
**ID:** 886219
**Sample Name:**
HkObDPju6Z.exe
**Cookbook:** default.jbs
**Time:** 21:16:06
**Date:** 12/06/2023
**Version:** 37.1.0 Beryl

# Table of Contents

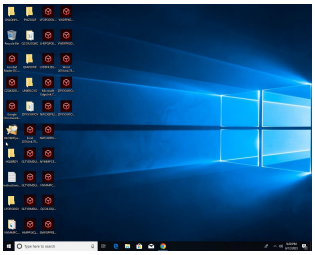
# Windows Analysis Report

## HkObDPju6Z.exe

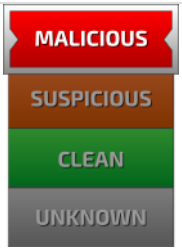
## Overview

### General Information

| | |
|---|---|
| Sample Name: | HkObDPju6Z.exe |
| Original Sample Name: | 723d1cf3d74fb… |
| Analysis ID: | 886219 |
| MD5: | 6441d7260944… |
| SHA1: | 462579828404… |
| SHA256: | 723d1cf3d74fb… |
| Tags: | exe |
| Infos: | |



### Detection



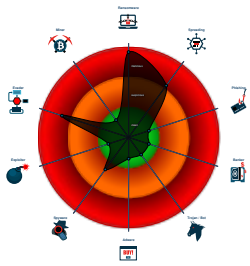

BlackBasta

| | |
|---|---|
| Score: | 100 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 100% |

### Signatures

- Multi AV Scanner detection for subm…
- Yara detected BlackBasta ransomw…
- Found ransom note / readme
- Antivirus / Scanner detection for sub…
- Detected unpacking (creates a PE f…
- Infects executable files (exe, dll, sy…
- Found Tor onion address
- Machine Learning detection for sam…
- May disable shadow drive data (use…
- Writes many files with high entropy
- Writes a notice file (html or txt) to de…
- Deletes shadow drive data (may be …

### Classification



## Process Tree

- **System is w10x64**
- HkObDPju6Z.exe (PID: 6028 cmdline: C:\Users\user\Desktop\HkObDPju6Z.exe MD5: 6441D7260944BCEDC5958C5C8A05D16D)
  - cmd.exe (PID: 4148 cmdline: C:\Windows\system32\cmd.exe /c C:\Windows\SysNative\vssadmin.exe delete shadows /all /quiet MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 1572 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - vssadmin.exe (PID: 7056 cmdline: C:\Windows\SysNative\vssadmin.exe delete shadows /all /quiet MD5: 47D51216EF45075B5F7EAA117CC70E40)
- HkObDPju6Z.exe (PID: 7028 cmdline: "C:\Users\user\Desktop\HkObDPju6Z.exe" MD5: 6441D7260944BCEDC5958C5C8A05D16D)
  - cmd.exe (PID: 1852 cmdline: C:\Windows\system32\cmd.exe /c C:\Windows\SysNative\vssadmin.exe delete shadows /all /quiet MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6824 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - vssadmin.exe (PID: 6840 cmdline: C:\Windows\SysNative\vssadmin.exe delete shadows /all /quiet MD5: 47D51216EF45075B5F7EAA117CC70E40)
- HkObDPju6Z.exe (PID: 4652 cmdline: "C:\Users\user\Desktop\HkObDPju6Z.exe" MD5: 6441D7260944BCEDC5958C5C8A05D16D)
  - cmd.exe (PID: 5708 cmdline: C:\Windows\system32\cmd.exe /c C:\Windows\SysNative\vssadmin.exe delete shadows /all /quiet MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 5688 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - vssadmin.exe (PID: 5700 cmdline: C:\Windows\SysNative\vssadmin.exe delete shadows /all /quiet MD5: 47D51216EF45075B5F7EAA117CC70E40)
- **cleanup**

## Malware Threat Intel

Provided by malpedia

| Name | Description | Attribution | Blogpost URLs | Link |
|---|---|---|---|---|

| Name | Description | Attribution | Blogpost URLs | Link |
|---|---|---|---|---|
| **Black Basta** | "Black Basta" is a new ransomware strain discovered during April 2022 - looks in dev since at least early February 2022 - and due to their ability to quickly amass new victims and the style of their negotiations, this is likely not a new operation but rather a rebrand of a previous top-tier ransomware gang that brought along their affiliates. | No Attribution | http://https://assets.sentinelone.com/sentinellabs22/sentinellabs-blackbastahttps://gbhackers.com/black-basta-ransomware/https://mandiant.widen.net/s/pkffwrbjlz/m-trends-2023https://noticeofpleadings.com/crackedcobaltstrike/files/ComplaintAndSummons/1%20-Microsoft%20Cobalt%20Strike%20-%20Complaint(907040021.9).pdfhttps://quadrantsec.com/resource/technical-analysis/black-basta-malware-overview | http://https://malpedia.caad.fkie.fraunhofer.de/details/win.blackbasta |

# Malware Configuration

**No configs have been found**

# Yara Signatures

## Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000000.00000003.371931160.00000000034E0000.00000004.00001000.00020000.00000000.sdmp | JoeSecurity_BlackBasta | Yara detected BlackBasta ransomware | Joe Security | |
| 00000008.00000002.477620370.0000000003220000.00000040.00001000.00020000.00000000.sdmp | JoeSecurity_BlackBasta | Yara detected BlackBasta ransomware | Joe Security | |
| 00000006.00000002.463365199.0000000003600000.00000040.00001000.00020000.00000000.sdmp | JoeSecurity_BlackBasta | Yara detected BlackBasta ransomware | Joe Security | |
| Process Memory Space: HkObDPju6Z.exe PID: 6028 | JoeSecurity_BlackBasta | Yara detected BlackBasta ransomware | Joe Security | |
| Process Memory Space: HkObDPju6Z.exe PID: 7028 | JoeSecurity_BlackBasta | Yara detected BlackBasta ransomware | Joe Security | |

Click to see the 1 entries

## Unpacked PEs

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 6.2.HkObDPju6Z.exe.3600000.1.raw.unpack | JoeSecurity_BlackBasta | Yara detected BlackBasta ransomware | Joe Security | |
| 6.2.HkObDPju6Z.exe.3600000.1.unpack | JoeSecurity_BlackBasta | Yara detected BlackBasta ransomware | Joe Security | |
| 8.2.HkObDPju6Z.exe.3220000.1.unpack | JoeSecurity_BlackBasta | Yara detected BlackBasta ransomware | Joe Security | |
| 8.2.HkObDPju6Z.exe.3220000.1.raw.unpack | JoeSecurity_BlackBasta | Yara detected BlackBasta ransomware | Joe Security | |
| 0.3.HkObDPju6Z.exe.34e0000.0.unpack | JoeSecurity_BlackBasta | Yara detected BlackBasta ransomware | Joe Security | |

Click to see the 1 entries

## Sigma Signatures

No Sigma rule has matched

## Snort Signatures

No Snort rule has matched

## Joe Sandbox Signatures

### AV Detection

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Machine Learning detection for sample

### Compliance

Detected unpacking (creates a PE file in dynamic memory)

### Spreading

Infects executable files (exe, dll, sys, html)

### Networking

Found Tor onion address

### Spam, unwanted Advertisements and Ransom Demands

Yara detected BlackBasta ransomware

Found ransom note / readme

May disable shadow drive data (uses vssadmin)

Writes many files with high entropy

Writes a notice file (html or txt) to demand a ransom

Deletes shadow drive data (may be related to ransomware)

### Data Obfuscation

Detected unpacking (creates a PE file in dynamic memory)

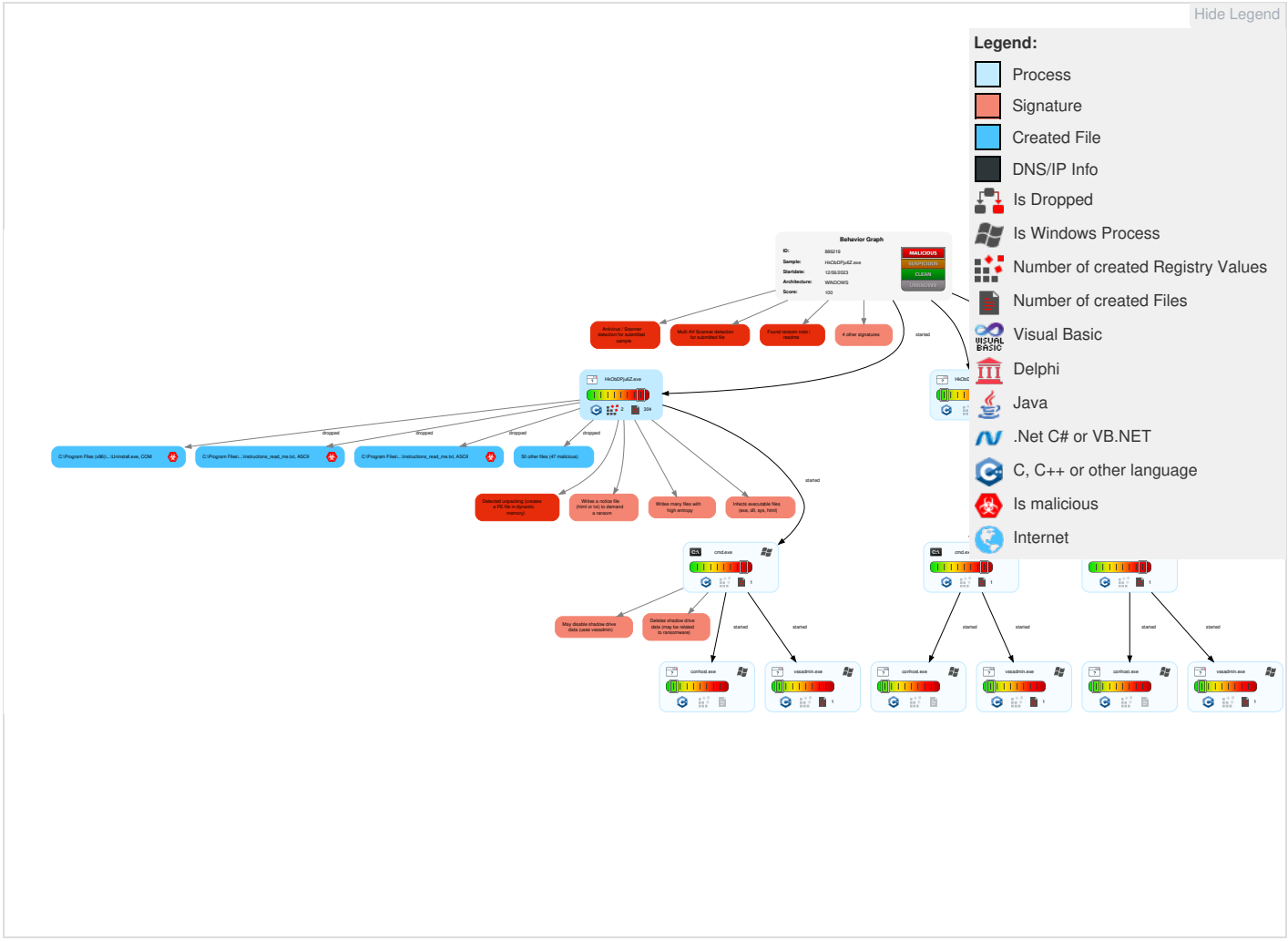
### Persistence and Installation Behavior

Infects executable files (exe, dll, sys, html)

## Mitre Att&ck Matrix

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Network Effects | Remote Service Effects | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Valid Accounts | 2 Command and Scripting Interpreter | 1 Registry Run Keys / Startup Folder | 1 2 Process Injection | 3 Masquerading | OS Credential Dumping | 2 1 Security Software Discovery | 1 Taint Shared Content | 1 Archive Collected Data | Exfiltration Over Other Network Medium | 1 Encrypted Channel | Eavesdrop on Insecure Network Communication | Remotely Track Device Without Authorization | 1 Data Encrypted for Impact |
| Default Accounts | 1 Native API | 1 DLL Side-Loading | 1 Registry Run Keys / Startup Folder | 1 Virtualization/Sandbox Evasion | LSASS Memory | 1 Virtualization/Sandbox Evasion | Remote Desktop Protocol | Data from Removable Media | Exfiltration Over Bluetooth | 1 Proxy | Exploit SS7 to Redirect Phone Calls/SMS | Remotely Wipe Data Without Authorization | Device Lockout |
| Domain Accounts | At (Linux) | Logon Script (Windows) | 1 DLL Side-Loading | 1 2 Process Injection | Security Account Manager | 1 Process Discovery | SMB/Windows Admin Shares | Data from Network Shared Drive | Automated Exfiltration | Steganography | Exploit SS7 to Track Device Location | Obtain Device Cloud Backups | Delete Device Data |
| Local Accounts | At (Windows) | Logon Script (Mac) | Logon Script (Mac) | 1 Deobfuscate/Decode Files or Information | NTDS | 1 1 Application Window Discovery | Distributed Component Object Model | Input Capture | Scheduled Transfer | Protocol Impersonation | SIM Card Swap | | Carrier Billing Fraud |
| Cloud Accounts | Cron | Network Logon Script | Network Logon Script | 3 Obfuscated Files or Information | LSA Secrets | 1 File and Directory Discovery | SSH | Keylogging | Data Transfer Size Limits | Fallback Channels | Manipulate Device Communication | | Manipulate App Store Rankings or Ratings |
| Replication Through Removable Media | Launchd | Rc.common | Rc.common | 1 1 Software Packing | Cached Domain Credentials | 2 4 System Information Discovery | VNC | GUI Input Capture | Exfiltration Over C2 Channel | Multiband Communication | Jamming or Denial of Service | | Abuse Accessibility Features |
| External Remote Services | Scheduled Task | Startup Items | Startup Items | 1 DLL Side-Loading | DCSync | Network Sniffing | Windows Remote Management | Web Portal Capture | Exfiltration Over Alternative Protocol | Commonly Used Port | Rogue Wi-Fi Access Points | | Data Encrypted for Impact |
| Drive-by Compromise | Command and Scripting Interpreter | Scheduled Task/Job | Scheduled Task/Job | 1 File Deletion | Proc Filesystem | Network Service Scanning | Shared Webroot | Credential API Hooking | Exfiltration Over Symmetric Encrypted Non-C2 Protocol | Application Layer Protocol | Downgrade to Insecure Protocols | | Generate Fraudulent Advertising Revenue |

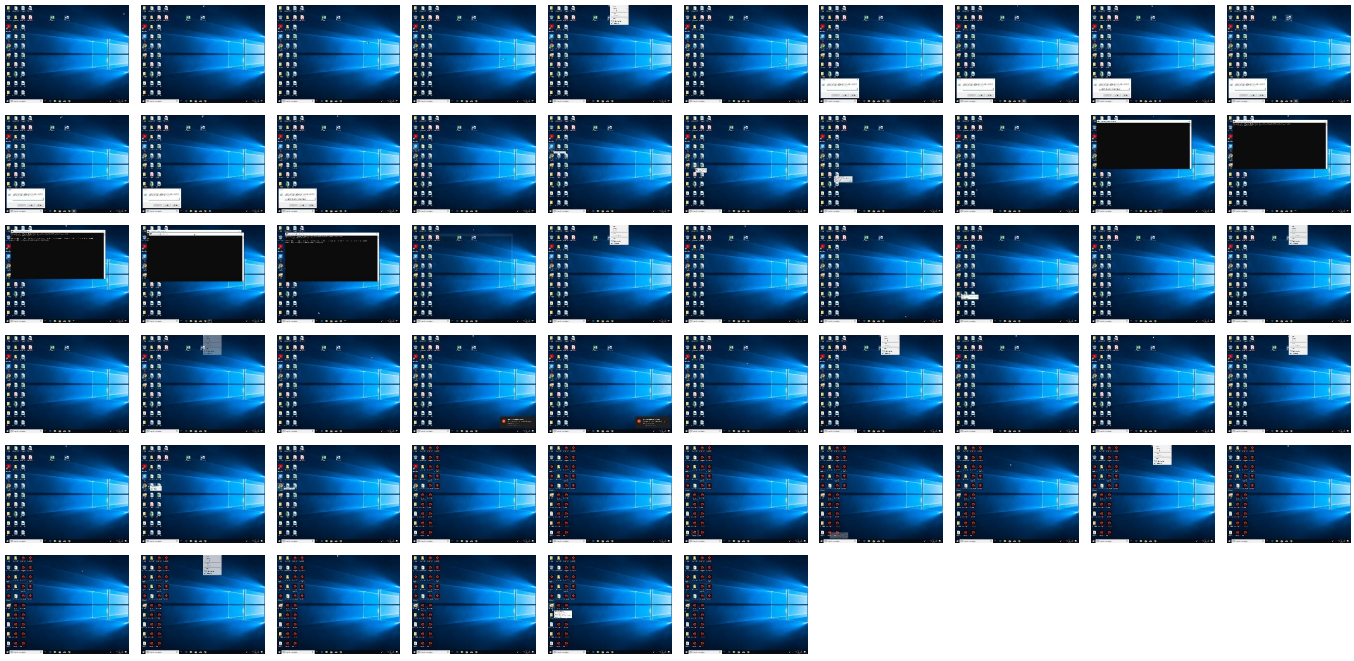
## Behavior Graph




# Screenshots

## Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.




## Antivirus, Machine Learning and Genetic Malware Detection

### Initial Sample

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| HkObDPju6Z.exe | 59% | ReversingLabs | Win32.Ransomware.Basta | |
| HkObDPju6Z.exe | 64% | Virustotal | | Browse |
| HkObDPju6Z.exe | 100% | Avira | TR/AD.PrestigeRansom.byoon | |
| HkObDPju6Z.exe | 100% | Joe Sandbox ML | | |

### Dropped Files

No Antivirus matches

### Unpacked PE Files

No Antivirus matches

### Domains

No Antivirus matches

### URLs

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://https://www.flos-freeware.chopenmailto:florian.balmer | 0% | Avira URL Cloud | safe | |
| http://https://bastad5huzwkepdixedg2gekg7jk22ato24zyllp6lnjx7wdtyctgvyd.onion/ | 0% | Virustotal | | Browse |
| http://https://bastad5huzwkepdixedg2gekg7jk22ato24zyllp6lnjx7wdtyctgvyd.onion/ | 0% | Avira URL Cloud | safe | |
| http://office.micro | 0% | Avira URL Cloud | safe | |

# Domains and IPs

## Contacted Domains

No contacted domains info

## URLs from Memory and Binaries

| Name | Source | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|
| http://https://www.rizonesoft.com | HkObDPju6Z.exe | false | | high |
| http://https://www.torproject.org/ | HkObDPju6Z.exe, 00000000.00000003.371931160.00000000034E0000.00000004.00001000.00020000.00000000.sdmp, HkObDPju6Z.exe, 00000006.00000002.463365199.0000000003600000.00000040.00001000.00020000.00000000.sdmp, HkObDPju6Z.exe, 00000008.00000002.477620370.0000000003220000.00000040.00001000.00020000.00000000.sdmp, instructions_read_me.txt59.0.dr, instructions_read_me.txt56.0.dr, instructions_read_me.txt74.0.dr, instructions_read_me.txt71.0.dr, instructions_read_me.txt65.0.dr, instructions_read_me.txt2.0.dr | false | | high |
| http://office.micro | PptLR.cab.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://bastad5huzwkepdixedg2gekg7jk22ato24zyllp6lnjx7wdtyctgvyd.onion/ | HkObDPju6Z.exe, 00000000.00000003.371931160.00000000034E0000.00000004.00001000.00020000.00000000.sdmp, HkObDPju6Z.exe, 00000006.00000002.463365199.0000000003600000.00000040.00001000.00020000.00000000.sdmp, HkObDPju6Z.exe, 00000006.00000002.463304811.0000000003440000.00000004.00001000.00020000.00000000.sdmp, HkObDPju6Z.exe, 00000008.00000002.477620370.0000000003220000.00000040.00001000.00020000.00000000.sdmp, HkObDPju6Z.exe, 00000008.00000002.477563045.00000000030C0000.00000004.00001000.00020000.00000000.sdmp, instructions_read_me.txt59.0.dr, instructions_read_me.txt56.0.dr, instructions_read_me.txt74.0.dr, instructions_read_me.txt71.0.dr, instructions_read_me.txt65.0.dr, instructions_read_me.txt2.0.dr | true | • 0%, Virustotal, Browse<br>• Avira URL Cloud: safe | unknown |
| http://https://www.flos-freeware.chopenmailto:florian.balmer | HkObDPju6Z.exe | false | • Avira URL Cloud: safe | low |
| http://https://www.flos-freeware.ch | HkObDPju6Z.exe | false | | high |

## World Map of Contacted IPs

No contacted IP infos

# General Information

| | |
|---|---|
| Joe Sandbox Version: | 37.1.0 Beryl |
| Analysis ID: | 886219 |
| Start date and time: | 2023-06-12 21:16:06 +02:00 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 13m 47s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Cookbook file name: | default.jbs |
| Analysis system description: | Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211 |

| | |
|---|---|
| Number of analysed new started processes analysed: | 18 |
| Number of new started drivers analysed: | 0 |
| Number of existing processes analysed: | 0 |
| Number of existing drivers analysed: | 0 |
| Number of injected processes analysed: | 0 |
| Technologies: | • HCA enabled<br>• EGA enabled<br>• HDC enabled<br>• AMSI enabled |
| Analysis Mode: | default |
| Analysis stop reason: | Timeout |
| Sample file name: | HkObDPju6Z.exe |
| Original Sample Name: | 723d1cf3d74fb3ce95a77ed9dff257a78c8af8e67a82963230dd073781074224.exe |
| Detection: | MAL |
| Classification: | mal100.rans.spre.evad.winEXE@18/400@0/0 |
| EGA Information: | • Successful, ratio: 50% |
| HDC Information: | Failed |
| HCA Information: | • Successful, ratio: 71%<br>• Number of executed functions: 0<br>• Number of non-executed functions: 0 |
| Cookbook Comments: | • Found application associated with file extension: .exe<br>• Override analysis time to 240s for sample files taking high CPU consumption |

### Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, conhost.exe, VSSVC.exe, svchost.exe
- Created / dropped Files have been reduced to 100
- Execution Graph export aborted for target HkObDPju6Z.exe, PID 6028 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtSetInformationFile calls found.

## Simulations

### Behavior and APIs

| Time | Type | Description |
|---|---|---|
| 21:17:08 | Autostart | Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Skype C:\Users\user\Desktop\HkObDPju6Z.exe |
| 21:17:17 | Autostart | Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Skype C:\Users\user\Desktop\HkObDPju6Z.exe |

## Joe Sandbox View / Context

### IPs

No context

### Domains

No context

### ASNs

No context

### JA3 Fingerprints

No context

## Dropped Files

No context

# Created / dropped Files

### C:\MSOCache\All Users\instructions_read_me.txt

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 1091 |
| Entropy (8bit): | 4.804750185554599 |
| Encrypted: | false |
| SSDEEP: | 24:F6SGOzWKJa3XWOCYj1C1PpiyE/xVHpmjxNkX0lOhA5:VGOzW6CwRNsxV0jVOK5 |
| MD5: | BA21D49977850F54961EDE73B7E9E480 |
| SHA1: | BD630B3DBE9D7139527C1FFDBB2161E7A9067AE0 |
| SHA-256: | 34757273C5E041F07B0352C51CFAB2998AB676F3A39BC0F16A1B4D68F3FAC4F8 |
| SHA-512: | 4BF9BE5F41F7258357E838BA94F0AA2B7F17D8FE3266174AAF123156B422C4FB72E4D3FD36DB7B2E3E9D13202202D2A6B0ECCA06EE2A2A043CE6AD27FFD751E2 |
| Malicious: | false |
| Preview: | ATTENTION!..Your network has been breached and all data was encrypted. Please contact us at:..https://bastad5huzwkepdixedg2gekg7jk22ato24zyllp6lnjx7wdtyctgvyd.onion/ .....Login ID: 26d371a9-efda-4e82-9989-01e292244d65.....*!* To access .onion websites download and install Tor Browser at:.... https://www.torproject.org/ (Tor Browser is not related to us)....*!* To restore all your PCs and get your network working again, follow these instructions:....- Any attempts to modify, decrypt or rename the files will lead to its fatal corruption. It doesn't matter, who are trying to do this, either it will be your IT guys or a recovery agency.....Please follow these simple rules to avoid data corruption:....- Do not modify, rename or delete files. Any attempts to modify, decrypt or rename the files will lead to its fatal corruption. ....- Do not hire a recovery company. They can't decrypt without the key. ..They also don't care about your business. They believe that they are ..good negotiator |

### C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\OWOW64WW.cab

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | modified |
| Size (bytes): | 30592502 |
| Entropy (8bit): | **7.999941422906834** |
| Encrypted: | **true** |
| SSDEEP: | 786432:8rEtPAhzlsR3KvYQJnbJ+9UwbXgWDRNIWhkXLOC:YEGhzw8PJI1TPIuuLOC |
| MD5: | 98DC2C73FEE92897B8A36947C711DF7F |
| SHA1: | 6B74915B1B5125E683AE09081639272141 76AC77 |
| SHA-256: | 43158309F90C1420F08DF067C89459B43A1CC4CB4BC4791DEFAE46104B58CD75 |
| SHA-512: | 8F2704707219AF6783771250DD7E3543C7BDCC45AF09C1DBA9866D3E59257E5C481D6CF09BC6A1E971001CF19542003DF1AF36E929D81CAB1F8DAFD8722A799 |
| Malicious: | **true** |
| Preview: | ..kl.X...+1l!9<...G...4.p@..d..P+..x.S..$...2+...).0.....ybw+i.....n.....FM. .ActionsPane3.xsd_x86.3643236F_FC70_11D3_A536_0090278A1BB8.41B86362_9D8B_4D9B_B426_8A6D1F809A25..(....(*..W.X..)QPc..0..L.[...M.....5tw.'....P.Y.....o.C...vB._B824_C9816882FA56..&..')....F.R .api_ms_win_core_datetime_l1_1_0.dll.A38EBF59_3A35_3759_B824_C9816882FA56..&...O.....F.R .api_..w].6Nbe..E\^..+..".....B@.S...m..'....k....ul...v...3.....6.6..&..gv.....F.R .api_ms_win_core_errorhandling_l1_1_0.dll.A38EBF59_3A35_3759_B824_C9816882FA56..4.....F.R .api_ms_win_core_..DO.4 ^;..fEUP.....U...B..[.S..itY.J.....h...)....w:.7Aw.F.R .api_ms_win_core_file_l1_2_0.dll.A38EBF59_3A35_3759_B824_C9816882FA56..&..G.....F.R .api_ms_win_core_file_l2_1_0.dll.A38EBF..w..k$^9..q~{....."...C.o[.`?.P+..y.S.2r.g..K^...Z.G.I...E$(Candle_l1_1_0.dll.A38EBF59_3A35_3759_B824_C9816882FA56..(...E.....F.R .api_ms_win_core_heap_l1_1_0.dll.A38EBF59_3A35_3759_B824_C9.....jW@?....9<...G....QBO..?...\r.'.< |

### C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\OWOW64WW.cab.7878kr5jx (copy)

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 30592502 |
| Entropy (8bit): | **7.999941422906834** |
| Encrypted: | **true** |
| SSDEEP: | 786432:8rEtPAhzlsR3KvYQJnbJ+9UwbXgWDRNIWhkXLOC:YEGhzw8PJI1TPIuuLOC |
| MD5: | 98DC2C73FEE92897B8A36947C711DF7F |
| SHA1: | 6B74915B1B5125E683AE09081639272141 76AC77 |
| SHA-256: | 43158309F90C1420F08DF067C89459B43A1CC4CB4BC4791DEFAE46104B58CD75 |
| SHA-512: | 8F2704707219AF6783771250DD7E3543C7BDCC45AF09C1DBA9866D3E59257E5C481D6CF09BC6A1E971001CF19542003DF1AF36E929D81CAB1F8DAFD8722A799 |

| | |
|---|---|
| Malicious: | **true** |
| Preview: | ..kl.X...+1I!9<...G...4.p@..d..P+..x.S..$...2+...).0.....ybw+i.....n.....FM. .ActionsPane3.xsd_x86.3643236F_FC70_11D3_A536_0090278A1BB8.41B86362_9D8B_4D9B_B426_8A6D1F809A25..(....(*..W.X..)QPc..0..L.[...M.....5tw.'....P.Y.....o.C...vB._B824_C9816882FA56..&..').....F.R .api_ms_win_core_datetime_l1_1_0.dll.A38EBF59_3A35_3759_B824_C9816882FA56..&...O.....F.R .api_..w].6Nbe..E\^..+..".....B@.S...m..'....k....ul...v...3.....6.6..&..gv.....F.R .api_ms_win_core_errorhandling_l1_1_0.dll.A38EBF59_3A35_3759_B824_C9816882FA56..4.....F.R .api_ms_win_core_..DO.4 ^;..fEUP.....U...B..[.S..itY.J.....h...)....w:.7Aw.F.R .api_ms_win_core_file_l1_2_0.dll.A38EBF59_3A35_3759_B824_C9816882FA56..&..G.....F.R .api_ms_win_core_file_l2_1_0.dll.A38EBF..w..k$^9..q~{....."...C.o[.`?.P+..y.S.2r.g..K^...Z.G.l...E$(Candle_l1_1_0.dll.A38EBF59_3A35_3759_B824_C9816882FA56..(...E.....F.R .api_ms_win_core_heap_l1_1_0.dll.A38EBF59_3A35_3759_B824_C9.....jW@?....9<...G....QBO..?...\r.'.< |

**C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\Office64WW.msi**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 3944762 |
| Entropy (8bit): | 7.113572129312687 |
| Encrypted: | false |
| SSDEEP: | 49152:sokGeClV9xd/lQwkqMgv1ivQ1J0XcEF1Q+OKKx8mG0C9RDHDtQAZUgyI2jN5XwBD:MWrP/lTNv1TvEF16KKKQC9RxT283uW |
| MD5: | D4BDA25196DF2CD081A302FAEA33ECAE |
| SHA1: | F6D9FADAFC4FD2B8FAC090F5F09720F9F65E6C94 |
| SHA-256: | FE6965946DC8311E3431DAAEF58CF7D5325991D6C5998C2BB6FEC01CDA247208 |
| SHA-512: | 733452957530D9B6DC45B3BF045E978FF191A1268283071803F3D292B962A7A43E0DE8B5F285DDAB62EB4DD5DDB1F700CD6ECC626761C448F91F9F9FEEA5ACI6 |
| Malicious: | false |
| Preview: | q.).~.....8q:...P\|.f.....w....,X+..3l..~+.....-.+#.Fd..;5.....^....0..9.BC..[s.r..,<_'....#E.r...X.....(..W....{..Jk.....872..%....8q:...P\|.f.....lq.w....,X+..3l..~+.....-.+#.Fd..;5.....872..%....8q:...P\|.f.....lq.w....,X+ |

**C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\Office64WW.msi.7878kr5jx (copy)**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 3944762 |
| Entropy (8bit): | 7.113572129312687 |
| Encrypted: | false |
| SSDEEP: | 49152:sokGeClV9xd/lQwkqMgv1ivQ1J0XcEF1Q+OKKx8mG0C9RDHDtQAZUgyI2jN5XwBD:MWrP/lTNv1TvEF16KKKQC9RxT283uW |
| MD5: | D4BDA25196DF2CD081A302FAEA33ECAE |
| SHA1: | F6D9FADAFC4FD2B8FAC090F5F09720F9F65E6C94 |
| SHA-256: | FE6965946DC8311E3431DAAEF58CF7D5325991D6C5998C2BB6FEC01CDA247208 |
| SHA-512: | 733452957530D9B6DC45B3BF045E978FF191A1268283071803F3D292B962A7A43E0DE8B5F285DDAB62EB4DD5DDB1F700CD6ECC626761C448F91F9F9FEEA5ACI6 |
| Malicious: | false |
| Preview: | q.).~.....8q:...P\|.f.....w....,X+..3l..~+.....-.+#.Fd..;5.....^....0..9.BC..[s.r..,<_'....#E.r...X.....(..W....{..Jk.....872..%....8q:...P\|.f.....lq.w....,X+..3l..~+.....-.+#.Fd..;5.....872..%....8q:...P\|.f.....lq.w....,X+ |

**C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\Office64WW.xml**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 5306 |
| Entropy (8bit): | 7.886160779314717 |
| Encrypted: | false |
| SSDEEP: | 96:P20Ylpy3PUURzGjOfnBWXKNvzMOy58H57Xw6k3KziFcXlNzAwB/HswQYezeNnlTk:PUpy3PL3ZWXc7K6A6k3KQQzJ/H9ugnlI |
| MD5: | DBBFDEC29EC5467FA8FCCEFFA11D6D37 |
| SHA1: | 947910199E6A7B31247A1A553AB6122203C5D983 |
| SHA-256: | 22FC6739D05242E05A016B436F03702365824F3FFF382969D27B7087DFA97ED0 |
| SHA-512: | 88EF11858753D66497C73B094BCD31898CA4CC33E0BB74639489F07683CC33F6ABCF627652AB339D60E0D6A88DE02045454A8F2134FCAFD99BF68C506688EC4 |
| Malicious: | false |

| | |
|---|---|
| Preview: | .[.db.M.3..x<(....mqOJ;.C.....s..Mv..}M..&..-..U.1.C.E.e.wt..].\|<.j....=\|6n...."XyC9.~.....f...(J.C.E.s...F..0....C.Q.f.=Z....px.t.....pE%.....s.q$.e....M...f]..^G.@..&..c....u...f.;H.&.<g.\|<br>..$..WIY...*SiA2.f.....,(..QD%.V\..X...%..I..3...@.I.k...<.eL.W....x*G...)vIz.....Q....U..;Q.y...1..F....~.I.....j}.H..w.*#LC....<B.ad.x....\|...3]...q.e.....a....z.g.E..Z....e;.Y.w.]!0s....<br>(QOj.....k)..."N..Qt.6.....e.. ...\|.E.a...-.)^.O..b..phi.....!z.....{..^g..W!O.o...*..e.....I...V.$>....q.X&,:....}$goe.o....(C... @.JS..%..[.....G...x.Z.)]....n{.\..b.J6Qf....?y..,.....y...=F<br>..%O.e....."....C.a...V7....}{.^..$.JFse.....{Ok;.^....W!..,&\.JS..8...K.....K._.A.[.9X....+^.T.#...mo...@.(.{.O..._...S.J...O.+...K..c../.C.L.A.9L..P.)M.H..b.J(.....=`HF:.O....CP<br>...%w..4Y....."..z.&...P.(K.Z....}.4..s!C....>{bF9.E....]...%J.AE_.....=..C.....Q4..X.yz.T.%.H_e7...)aB]..F...I...@.J...O.5..U..a.....L....Q...Og.^..t.HUny...u"..e.....h)... @.% |

**C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\Office64WW.xml.7878kr5jx (copy)**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 5306 |
| Entropy (8bit): | 7.886160779314717 |
| Encrypted: | false |
| SSDEEP: | 96:P20Ylpy3PUURzGjOfnBWXKNvzMOy58H57Xw6k3KziFcXlNzAwB/HswQYezeNnlTk:PUpy3PL3ZWXc7K6A6k3KQQzJ/H9ugnlI |
| MD5: | DBBFDEC29EC5467FA8FCCEFFA11D6D37 |
| SHA1: | 947910199E6A7B31247A1A553AB6122203C5D983 |
| SHA-256: | 22FC6739D05242E05A016B436F03702365824F3FFF382969D27B7087DFA97ED0 |
| SHA-512: | 88EF11858753D66497C73B094BCD31898CA4CC33E0BB74639489F07683CC33F6ABCF627652AB339D60E0D6A88DE02045454A8F2134FCAFD99BF68C506688EC4 |
| Malicious: | false |
| Preview: | .[.db.M.3..x<(....mqOJ;.C.....s..Mv..}M..&..-..U.1.C.E.e.wt..].\|<.j....=\|6n...."XyC9.~.....f...(J.C.E.s...F..0....C.Q.f.=Z....px.t.....pE%.....s.q$.e....M...f]..^G.@..&..c....u...f.;H.&.<g.\|<br>..$..WIY...*SiA2.f.....,(..QD%.V\..X...%..I..3...@.I.k...<.eL.W....x*G...)vIz.....Q....U..;Q.y...1..F....~.I.....j}.H..w.*#LC....<B.ad.x....\|...3]...q.e.....a....z.g.E..Z....e;.Y.w.]!0s....<br>(QOj.....k)..."N..Qt.6.....e.. ...\|.E.a...-.)^.O..b..phi.....!z.....{..^g..W!O.o...*..e.....I...V.$>....q.X&,:....}$goe.o....(C... @.JS..%..[.....G...x.Z.)]....n{.\..b.J6Qf....?y..,.....y...=F<br>..%O.e....."....C.a...V7....}{.^..$.JFse.....{Ok;.^....W!..,&\.JS..8...K.....K._.A.[.9X....+^.T.#...mo...@.(.{.O..._...S.J...O.+...K..c../.C.L.A.9L..P.)M.H..b.J(.....=`HF:.O....CP<br>...%w..4Y....."..z.&...P.(K.Z....}.4..s!C....>{bF9.E....]...%J.AE_.....=..C.....Q4..X.yz.T.%.H_e7...)aB]..F...I...@.J...O.5..U..a.....L....Q...Og.^..t.HUny...u"..e.....h)... @.% |

**C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\PidGenX.dll**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 1274770 |
| Entropy (8bit): | 7.512951123194743 |
| Encrypted: | false |
| SSDEEP: | 24576:f2TJLcxCqNlyS3hrFfSLtgS/EP3mRa3CuGgSSKVx5RD+CCnVqmiHvPCrvIucch2B:fScgZuqTVHtmKRIaHpgAKwtt3kEgZKie |
| MD5: | F728CF82E2FB15902C1E2247A1840F69 |
| SHA1: | 65AE9C720A05D4C32DE56DA80B28CAFB3F10588A |
| SHA-256: | 4C425A1447D49A5787CA4904ACC637E437755686F3F7E3DFDD060BDF9F5D4B8A |
| SHA-512: | FCBE6BE131E2FCE3A989731B3A7A2DF4842B6CC083D52EFCD1E7EAAACE9F74FAAACF9795727318A09AD13C804A99FA096C1E2DBB2F567BE2A83FAC3AA8F57F10 |
| Malicious: | false |
| Preview: | Z....`..').\.....c._.....q...S).Y..\|.;v.....y...8.....!..L.!This program cannot be run in DOS mode....$.....m)A..G...G...G..^....G..t....G...F.>.G..t....G..t....G..t....G.....l..w...<br>...:.M.u.....M.....S).Y..\|.;v.....y...8PE..L....$.O.....!.....h.....Pc.....CS P.....f....@.....XX..]..._.C..`..#.:.....:._@....q..__.Y..\|.;v.<br>.....y...8.....@.....text....f.....h..... ..`.data.....I.....S..`.7..Z.]...\.....g._.....q...S).Y.\|.....8.h.....@..H.....<br>.....S..`..#.).>.....c._.....q...S).Y..\|.;v.....y...8.....<br>.....S..`..#.).>.....c._.....q... |

**C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\PidGenX.dll.7878kr5jx (copy)**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 1274770 |
| Entropy (8bit): | 7.512951123194743 |
| Encrypted: | false |
| SSDEEP: | 24576:f2TJLcxCqNlyS3hrFfSLtgS/EP3mRa3CuGgSSKVx5RD+CCnVqmiHvPCrvIucch2B:fScgZuqTVHtmKRIaHpgAKwtt3kEgZKie |
| MD5: | F728CF82E2FB15902C1E2247A1840F69 |
| SHA1: | 65AE9C720A05D4C32DE56DA80B28CAFB3F10588A |
| SHA-256: | 4C425A1447D49A5787CA4904ACC637E437755686F3F7E3DFDD060BDF9F5D4B8A |
| SHA-512: | FCBE6BE131E2FCE3A989731B3A7A2DF4842B6CC083D52EFCD1E7EAAACE9F74FAAACF9795727318A09AD13C804A99FA096C1E2DBB2F567BE2A83FAC3AA8F57F10 |
| Malicious: | false |
| Preview: | Z....`..').\.....c._.....q...S).Y..\|.;v.....y...8.....!..L.!This program cannot be run in DOS mode....$.....m)A..G...G...G..^....G..t....G...F.>.G..t....G..t....G..t....G.....l..w...<br>...:.M.u.....M.....S).Y..\|.;v.....y...8PE..L....$.O.....!.....h.....Pc.....CS P.....f....@.....XX..]..._.C..`..#.:.....:._@....q..__.Y..\|.;v.<br>.....y...8.....@.....text....f.....h..... ..`.data.....I.....S..`.7..Z.]...\.....g._.....q...S).Y.\|.....8.h.....@..H.....<br>.....S..`..#.).>.....c._.....q...S).Y..\|.;v.....y...8.....<br>.....S..`..#.).>.....c._.....q... |

**C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ProPlusWW.msi**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 28983610 |
| Entropy (8bit): | 6.311677848898019 |
| Encrypted: | false |
| SSDEEP: | 393216:+vfwbsMbPzX1sgMai8VDwxTvali5aK+nkF:qfwYAXx9nGxTvalAaFkF |
| MD5: | D94E3C74A0DC8DD4C1F191EDCC02961C |
| SHA1: | 269F434281A7079C9C7CFB2672933E22402B81EA |
| SHA-256: | A3C4B2CE075243E49CAD0BD4717BEADF387FA8F6F79606081D16DE7742AF00E7 |
| SHA-512: | A22700B1236C801EE7E57353B9685594CB01D3D54621ACE8AB7266B3D578D3FDDABD3FF09480F83511CBDDC170E58EE5FB1D2384C43E7E20C3C3C359035B359 |
| Malicious: | false |
| Preview: | .z \.b...4(.,..<.Z."Z.....}...3.6PCj....*.-..j.....?....p9..\.r..U...6.P.He\|.q..3.....7L..4h.]..C.$.\.v.:..V.$.....?....p9..\.r..U...6.P.He\|.q..3.....7L..4h.]..C.$.\.v.:..V.$.....7ck..\xS..4(.,..<.Z."Z.....5.6PCj....*.-..j.....7ck..\xS..4(.,..<.Z."Z.....5.6PCj....*.-..j.....7ck..\xS..4(.,..<.Z."Z.....5.6PCj.. |

**C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ProPlusWW.msi.7878kr5jx (copy)**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 28983610 |
| Entropy (8bit): | 6.311677848898019 |
| Encrypted: | false |
| SSDEEP: | 393216:+vfwbsMbPzX1sgMai8VDwxTvali5aK+nkF:qfwYAXx9nGxTvalAaFkF |
| MD5: | D94E3C74A0DC8DD4C1F191EDCC02961C |
| SHA1: | 269F434281A7079C9C7CFB2672933E22402B81EA |
| SHA-256: | A3C4B2CE075243E49CAD0BD4717BEADF387FA8F6F79606081D16DE7742AF00E7 |
| SHA-512: | A22700B1236C801EE7E57353B9685594CB01D3D54621ACE8AB7266B3D578D3FDDABD3FF09480F83511CBDDC170E58EE5FB1D2384C43E7E20C3C3C359035B359 |
| Malicious: | false |
| Preview: | .z \.b...4(.,..<.Z."Z.....}...3.6PCj....*.-..j.....?....p9..\.r..U...6.P.He\|.q..3.....7L..4h.]..C.$.\.v.:..V.$.....?....p9..\.r..U...6.P.He\|.q..3.....7L..4h.]..C.$.\.v.:..V.$.....7ck..\xS..4(.,..<.Z."Z.....5.6PCj....*.-..j.....7ck..\xS..4(.,..<.Z."Z.....5.6PCj....*.-..j.....7ck..\xS..4(.,..<.Z."Z.....5.6PCj.. |

**C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ProPlusWW.xml**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 17422 |
| Entropy (8bit): | 6.785529037683763 |
| Encrypted: | false |
| SSDEEP: | 384:cgeiFfFhG92uf/YdGNQXvvrAhof6fG95yc+H:FeIfG2uf2GCfEBfG95yc+H |
| MD5: | D193A7719787D6FB03003BC8D1FBBBF5 |
| SHA1: | 7FAE49BA6131DE5F500B5E840811FCD8AC60C817 |
| SHA-256: | 116E6DE38A370951C8AC208DACE2292B4C71F3A632F55F5DB16E9E9E89CC700E |
| SHA-512: | 2EDD60F758AD8234F12A3CC7A6A34F932B5E9E9381F2A2B481C35190F719B6677247124025C23CA4D81D545A1F0B9709741665C4DC2EF68713179F9700284700 |
| Malicious: | false |
| Preview: | ...Z}..*W..d?=..'...n.{.`.9\...8.t.<..tvn._..@8.F.I.{.....g.%nDjOQbzgDObLJSNTgntLRjr76QOQWKY42r25vol1N8yE5Nz8bDippwsY/y1v1IWxVYAYqSZMbKKNf3B5VGnLzSufEMU00Bk/aTVAfSv5od9+Yn83yNcCrkdyt73vvlgr..f!./.WU.ocDS.p..@!O..G.i8_...8.h...Tez..I...-..$.ZI`.....*fYt6JR53OQnP0ZZS5mH6zfKCr0gE7OnQnMmwSVcr7DXoNV03nuWbcy6jVwEbMKppAIWkjmNmEwZw6gqnjtQws1r6b58dfEeWiHuuWv1f0yP+kAMGBruBCZdNFWxNEgZuw..o:..;`..?.Hk.e..lCa..~.sL...E.5.c..h.'."..E..f.\....8...AI" Path="ProPlusWW.MSI" Version="1.0" ProductCode="{90160000-0011-0000-0000-0000000FF1CE}" MSIVersion="16.0.4266.1001" ProductLaC.Vv.Bm.\.[=aW.f..). ..). 1.Z...t.?.I..)90.o...7'.p.gkc..W...wature Id="RhdInspector" Cost="63776">....<OptionRef Id="ProductFiles"/>...</Feature>...<Feature Id="MsoInstalledPackagesScoped" n.C,.Om.s..X<l.}.OY.~..m.\| W..f.8.v..$2'./...H.S.jJ_...P.<.Teature Id="VSTOCLR35" Cost="4906912">....<OptionRef Id="VSTOCLR35"/>...</Feature>...<Feature Id="VBAFiles" Cost="11486152">....<b.^~.-*C^.ol"u.H.Mn.:....W]...a.$.<.. |

**C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ProPlusWW.xml.7878kr5jx (copy)**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |

| | |
|---|---|
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 17422 |
| Entropy (8bit): | 6.785529037683763 |
| Encrypted: | false |
| SSDEEP: | 384:cgeiFfFhG92uf/YdGNQXvvrAhof6fG95yc+H:FeIfG2uf2GCfEBfG95yc+H |
| MD5: | D193A7719787D6FB03003BC8D1FBBBF5 |
| SHA1: | 7FAE49BA6131DE5F500B5E840811FCD8AC60C817 |
| SHA-256: | 116E6DE38A370951C8AC208DACE2292B4C71F3A632F55F5DB16E9E9E89CC700E |
| SHA-512: | 2EDD60F758AD8234F12A3CC7A6A34F932B5E9E9381F2A2B481C35190F719B6677247124025C23CA4D81D545A1F0B9709741665C4DC2EF68713179F9700284700 |
| Malicious: | false |
| Preview: | ...Z}..*W..d?=..'...n.{.`.9\...8.t.<..tvn._..@8.F.I.{.....g.%nDjOQbzgDObLJSNTgntLRjr76QOQWKY42r25vol1N8yE5Nz8bDippwsY/y1v1IWxVYAYqSZMbKKNf3B5VGnLzSufE MU00Bk/aTVAfSv5od9+Yn83yNcCrkdyt73vvlgr..f!./.WU.ocDS.p..@!O..G.i8_...8.h...Tez..I...-..$.ZI`.....*fYt6JR53OQnP0ZZS5mH6zfKCr0gE7OnQnMmwSVcr7 DXoNV03nuWbcy6jVwEbMKppAIWkjmNmEwZw6gqnjtQws1r6b58dfEeWiHuuWv1f0yP+kAMGBruBCZdNFWxNEgZuw..o:..;`..?.Hk.e..lCa..~.sL...E.5.c..h.'."..E..f.\....8...AI" Path="ProPlusWW.MSI" Version="1.0" ProductCode="{90160000-0011-0000-0000-0000000FF1CE}" MSIVersion="16.0.4266.1001" ProductLaC.Vv.Bm.\.[=aW.f..). ..). 1.Z...t.?.I..)90.o...7'.p.gkc..W...wature Id="RhdInspector" Cost="63776">....<OptionRef Id="ProductFiles"/>...</Feature>...<Feature Id="MsoInstalledPackagesScoped" n.C,.Om.s..X<l.}.OY.~..m.| W..f.8.v..$2'./...H.S.jJ_...P.<.Teature Id="VSTOCLR35" Cost="4906912">....<OptionRef Id="VSTOCLR35"/>...</Feature>...<Feature Id= "VBAFiles" Cost="11486152">....<b.^~.-*C^.ol"u.H.Mn.:....W]...a.$.<.. |

### C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ProPsWW.cab

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 323579288 |
| Entropy (8bit): | **7.99992937711017** |
| Encrypted: | **true** |
| SSDEEP: | 6291456:IvTS8/jU9LWir8NG/du4HQLeL7u0IR0KY26cMashYFRX4Mbip4IsW7:IzSLD4cHkRM2PMDhYFRXT7nW7 |
| MD5: | FA26DFA649511F61A0426256FBB10732 |
| SHA1: | D6FE84C280C4A9660EC97B2EE70D13107353BF0E |
| SHA-256: | A9F6E84B367D35F2DCCEB30C3CD059C154890A873961065FF9E96735BB59F2E3 |
| SHA-512: | CF3F6819A94C2AED7FF42087A08FCEC03CF0E73727AEB5460F6045F6FDEA86463F3ED5AB37717EE01908D8266789A101AAC28A94D702E0F8F001D26ED1E54FD 7 |
| Malicious: | **true** |
| Preview: | .V.....k..e.MJ...y...k.2.....=.:`G`D....&D....O+R.:...:....L...I.....(.....Z.....P.....:.....a...t.'....I.r.....>...&.....,.6....#3.....V..RM..8tM...I...I.3..H.....(! {t@.D..g.h2q.....T$S.9....5.....~G.....a.y.....I.....I.....I.....J.I.....F.O .ACACEDAO.DLL.....F.. .ACC12PL.DLL.....F.. .ACC.1...W.P..e.GM.....K.r[...9Z..= 5.&GPu.....s...J..n....3..L....%....F.. .ACCESSCOMPARE.RDLC.x86.....f.'....F.. .ACCESSPL.CFG.....'....F.O .ACECORE.DLL.....F.O .ACEDAO.DLL.....kU.S.D. ..d.. yo^.ki.....'Q...=....8..=.5.....C+S...I..:ACEODBC.DLL..C.....F.O .ACEODEXL.DLL.....=.....F.O .ACEOLEDB.DLL..~...6.....F.O .ACETXT.DLL.....F.O .ACEWDAT.DLL..... }.....Q..e.....W...k..D.....M{..G!..I..V...H..+R.!...3:...F.. .ACWZLIB.ACCDE..._.`.....F.. .AD.DPV.....i.....F.. .AD.XML.....s.....F.O .ADAL.DLL.....F.. .ADAO12PL.CFG. .....D...jU"..D.$.|x.=....2...{.....<..:. |

### C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ProPsWW.cab.7878kr5jx (copy)

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 323579288 |
| Entropy (8bit): | **7.99992937711017** |
| Encrypted: | **true** |
| SSDEEP: | |
| MD5: | FA26DFA649511F61A0426256FBB10732 |
| SHA1: | D6FE84C280C4A9660EC97B2EE70D13107353BF0E |
| SHA-256: | A9F6E84B367D35F2DCCEB30C3CD059C154890A873961065FF9E96735BB59F2E3 |
| SHA-512: | CF3F6819A94C2AED7FF42087A08FCEC03CF0E73727AEB5460F6045F6FDEA86463F3ED5AB37717EE01908D8266789A101AAC28A94D702E0F8F001D26ED1E54FD 7 |
| Malicious: | **true** |
| Preview: | .V.....k..e.MJ...y...k.2.....=.:`G`D....&D....O+R.:...:....L...I.....(.....Z.....P.....:.....a...t.'....I.r.....>...&.....,.6....#3.....V..RM..8tM...I...I.3..H.....(! {t@.D..g.h2q.....T$S.9....5.....~G.....a.y.....I.....I.....I.....J.I.....F.O .ACACEDAO.DLL.....F.. .ACC12PL.DLL.....F.. .ACC.1...W.P..e.GM.....K.r[...9Z..= 5.&GPu.....s...J..n....3..L....%....F.. .ACCESSCOMPARE.RDLC.x86.....f.'....F.. .ACCESSPL.CFG.....'....F.O .ACECORE.DLL.....F.O .ACEDAO.DLL.....kU.S.D. ..d.. yo^.ki.....'Q...=....8..=.5.....C+S...I..:ACEODBC.DLL..C.....F.O .ACEODEXL.DLL.....=.....F.O .ACEOLEDB.DLL..~...6.....F.O .ACETXT.DLL.....F.O .ACEWDAT.DLL..... }.....Q..e.....W...k..D.....M{..G!..I..V...H..+R.!...3:...F.. .ACWZLIB.ACCDE..._.`.....F.. .AD.DPV.....i.....F.. .AD.XML.....s.....F.O .ADAL.DLL.....F.. .ADAO12PL.CFG. .....D...jU"..D.$.|x.=....2...{.....<..:. |

### C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ProPsWW2.cab

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |

| | |
|---|---|
| Category: | dropped |
| Size (bytes): | 249155585 |
| Entropy (8bit): | **7.999931605163267** |
| Encrypted: | **true** |
| SSDEEP: | |
| MD5: | 9E09A048941F51DAF21DB78B77A028B3 |
| SHA1: | BEEFD213E782788AC7048F38B43FAF945D397952 |
| SHA-256: | 6248E5AF7CE2C8420E4144A6304B762B65F8B4D85C9A98B837921EEDEC764E07 |
| SHA-512: | 6C9562BC18679CE151D4A6A1EA71F4D6CC5D9D23EAEA850B545764D18D76EF0FE3F9B608B847D27613DFB3F7619813CF42F6645D9D5EF864B52189282C44496 |
| Malicious: | **true** |
| Preview: | ....o....\|....4.....,..`.....<2.PX...g3w..c...@..:b..\| h.....+.....1..@.....E.....g...;...^...#.....!M].....k.$.....e.A.....q.....k.....5.....[..._.r.:..5.g...../...a....7.>..iq.aj ....x]...C..:b...I.ACC14PL.CFG.....F.. .ACCESSPL.DLL..49..5.....F.O .ACCICONS.EXE.....Hj9....F.O .ACCOLK.DLL..-....;....F.. .ACCSBAR.POC....C..qo..S}.....\|.. .a.....Hn&.pX.....z....'.k.... .ACDAOPIA.DLL.....?....F.O .ACEERR.DLL.."...;@....F.O .ACEEXCL.DLL..C...^F....F.O .ACEODTXT.DLL.....F....F.. .ActionsPanep..9.... .;.....P.....g`.....m..<y.Z.[X.4.X.B_B39D_A7A9EB6A7951..P....F....F.. .ACWZMAIN.ACCDE.....F.. .ACWZTOOL.ACCDE..@4...`....F.. .ACWZUSR12.A CCDU.Z.....F .c...V...tV.....+'.....A.....kt.P...=l;..^..Z..{&X.Z.9..DLL..%.....F.. .ADDINS.STORE..j..`#.....F#O .AdHocReportingExcelClient_resources_dll_32_1026.9 4CF6D16_6C48_4FC6_8570_3E1DCAp..\|]...Y..(ul..M.....).....Ow.3 |

**C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ProPsWW2.cab.7878kr5jx (copy)**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 249155585 |
| Entropy (8bit): | **7.999931605163267** |
| Encrypted: | **true** |
| SSDEEP: | |
| MD5: | 9E09A048941F51DAF21DB78B77A028B3 |
| SHA1: | BEEFD213E782788AC7048F38B43FAF945D397952 |
| SHA-256: | 6248E5AF7CE2C8420E4144A6304B762B65F8B4D85C9A98B837921EEDEC764E07 |
| SHA-512: | 6C9562BC18679CE151D4A6A1EA71F4D6CC5D9D23EAEA850B545764D18D76EF0FE3F9B608B847D27613DFB3F7619813CF42F6645D9D5EF864B52189282C44496 |
| Malicious: | **true** |
| Preview: | ....o....\|....4.....,..`.....<2.PX...g3w..c...@..:b..\| h.....+.....1..@.....E.....g...;...^...#.....!M].....k.$.....e.A.....q.....k.....5.....[..._.r.:..5.g...../...a....7.>..iq.aj ....x]...C..:b...I.ACC14PL.CFG.....F.. .ACCESSPL.DLL..49..5.....F.O .ACCICONS.EXE.....Hj9....F.O .ACCOLK.DLL..-....;....F.. .ACCSBAR.POC....C..qo..S}.....\|.. .a.....Hn&.pX.....z....'.k.... .ACDAOPIA.DLL.....?....F.O .ACEERR.DLL.."...;@....F.O .ACEEXCL.DLL..C...^F....F.O .ACEODTXT.DLL.....F....F.. .ActionsPanep..9.... .;.....P.....g`.....m..<y.Z.[X.4.X.B_B39D_A7A9EB6A7951..P....F....F.. .ACWZMAIN.ACCDE.....F.. .ACWZTOOL.ACCDE..@4...`....F.. .ACWZUSR12.A CCDU.Z.....F .c...V...tV.....+'.....A.....kt.P...=l;..^..Z..{&X.Z.9..DLL..%.....F.. .ADDINS.STORE..j..`#.....F#O .AdHocReportingExcelClient_resources_dll_32_1026.9 4CF6D16_6C48_4FC6_8570_3E1DCAp..\|]...Y..(ul..M.....).....Ow.3 |

**C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\Setup.xml**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | OpenPGP Secret Key |
| Category: | dropped |
| Size (bytes): | 28096 |
| Entropy (8bit): | 6.801218487789588 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | BF6FE01153AC3566C9379D96D32EFABC |
| SHA1: | A98A3B53BF1062798E39D28D388F5031D2F7A24A |
| SHA-256: | 8AB40A2A3385217054045720867A837136E7AFDD8E466A8220E9CD6E106DB764 |
| SHA-512: | FE987BDC5159E34680DAA47C73CA7159D7D227FE8FB7329922D68FD4F7646D5D148DC2C148EA6F9FE035B6B6F11FD4331D72EE11F5DAF44A34015BC4EFD6B3 A1 |
| Malicious: | false |
| Preview: | .UU../E..x...Q.D....t8.p..?...C....3;X..hF....9.u._.....+.....Z1Rr28qghARqLdvYs4i2aUebCkINmnoD5nuDfBALSnEN8LJNteqBeAfK8bNy0fA98n11k9iFq7JlGPQeCVP2e9kl hS8ixzDS0oUwyNWMEmg4hfXHS8vot+S/DO2dFJr6..Z..Ka)*n.....C....B..Y.....rMD../.I..d4.....=n.9...p....nNBhadFX+gqIwh/45B0U6kMPswkN5T7jO585oeh26atONRLiqBA tC23W8N7vEwZWdnfN08yryNTEsyQW+tDuGrgx2UMXKhwOGcM9fXfbWAQUqwy8XJdS6lorLXTXHuuz..d..Ci.8X..#..<..P..p..I...;.E.eq....tI. >..,J\|t6..."....."....t" ProductCode=" {90160000-0011-0000-0000-0000000FF1CE}">...<PIDTemplate Value="82503<````=````=````=````=````=`````&am.QJ..Os32K..Na.\|....x9.?..I.A....w....,..r...8L2 1....=....." DisallowAbsent="yes" DisallowAdvertise="yes" Hidden="yes"/>...<Option Id="OSpp" DefaultState="Local" DisallowAbsent="yes" Disa..B..kE.....Q.....Y?.{..I.E WV....Z.. ..r..@{v.$.>...e.....ultState="Local" DisallowAbsent="yes" DisallowAdvertise="yes" Hidden="yes"/>...<Option Id="Gimme_OnDemandData" DefaultState="Loc. ....f@..g..1.....h3.=..8...Z....ga.. |

**C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\Setup.xml.7878kr5jx (copy)**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | OpenPGP Secret Key |
| Category: | dropped |
| Size (bytes): | 28096 |

| | |
|---|---|
| Entropy (8bit): | 6.801218487789588 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | BF6FE01153AC3566C9379D96D32EFABC |
| SHA1: | A98A3B53BF1062798E39D28D388F5031D2F7A24A |
| SHA-256: | 8AB40A2A3385217054045720867A837136E7AFDD8E466A8220E9CD6E106DB764 |
| SHA-512: | FE987BDC5159E34680DAA47C73CA7159D7D227FE8FB7329922D68FD4F7646D5D148DC2C148EA6F9FE035B6B6F11FD4331D72EE11F5DAF44A34015BC4EFD6B3A1 |
| Malicious: | false |
| Preview: | .UU../E..x...Q.D....t8.p..?...C....3;X..hF....9.u.._....+.....Z1Rr28qghARqLdvYs4i2aUebCklNmnoD5nuDfBALSnEN8LJNteqBeAfK8bNy0fA98n11k9iFq7JlGPQeCVP2e9kl hS8ixzDS0oUwyNWMEmg4hfXHS8vot+S/DO2dFJr6..Z..Ka)*n.....C....B..Y.....rMD../.l..d4.....=n.9...p....nNBhadFX+gqlwh/45B0U6kMPswkN5T7jO585oeh26atONRLiqBA tC23W8N7vEwZWdnfN08yryNTEsyQW+tDuGrgx2UMXKhwOGcM9fXfbWAQUqwy8XJdS6lorLXTXHuuz..d..Ci.8X..#..<..P..p..l...;.E.eq....tl. >..,Jjt6..."".....t" ProductCode="{90160000-0011-0000-0000-0000000FF1CE}">...<PIDTemplate Value="82503<````=````=````=````=`````&am.QJ..Os32K..Na.|....x9.?..l.A....w.....,..r...8L2 1....=....." DisallowAbsent="yes" DisallowAdvertise="yes" Hidden="yes"/>...<Option Id="OSpp" DefaultState="Local" DisallowAbsent="yes" Disa..B..kE.....Q.....Y?.{..l.E WV....Z.. ..r..@{v.$.>...e.....ultState="Local" DisallowAbsent="yes" DisallowAdvertise="yes" Hidden="yes"/>...<Option Id="Gimme_OnDemandData" DefaultState="Loc. ....f@..g..1.....h3.=..8...Z....ga.. |

**C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\instructions_read_me.txt**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 1091 |
| Entropy (8bit): | 4.804750185554599 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | BA21D49977850F54961EDE73B7E9E480 |
| SHA1: | BD630B3DBE9D7139527C1FFDBB2161E7A9067AE0 |
| SHA-256: | 34757273C5E041F07B0352C51CFAB2998AB676F3A39BC0F16A1B4D68F3FAC4F8 |
| SHA-512: | 4BF9BE5F41F7258357E838BA94F0AA2B7F17D8FE3266174AAF123156B422C4FB72E4D3FD36DB7B2E3E9D13202202D2A6B0ECCA06EE2A2A043CE6AD27FFD751E2 |
| Malicious: | false |
| Preview: | ATTENTION!..Your network has been breached and all data was encrypted. Please contact us at:..https://bastad5huzwkepdixedg2gekg7jk22ato24zyllp6lnjx7wdtyctgvyd.onion/ .....Login ID: 26d371a9-efda-4e82-9989-01e292244d65.....*!* To access .onion websites download and install Tor Browser at:.... https://www.torproject.org/ (Tor Browser is not related to us)....*!* To restore all your PCs and get your network working again, follow these instructions:....- Any attempts to modify, decrypt or rename the files will lead to its fatal corruption. It doesn't matter, who are trying to do this, either it will be your IT guys or a recovery agency.....Please follow these simple rules to avoid data corruption:....- Do not modify, rename or delete files. Any attempts to modify, decrypt or rename the files will lead to its fatal corruption. ....- Do not hire a recovery company. They can't decrypt without the key. ..They also don't care about your business. They believe that they are ..good negotiator |

**C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ose.exe**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 203242 |
| Entropy (8bit): | 7.226275049150236 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | E023A8F754E20D7866045CAAB9EC2083 |
| SHA1: | FDC5873E2E87A40A0E83F30299664F855B374C8A |
| SHA-256: | 94A3C5C9FAC0502D2CE268B678F1F98D9853C100BBA716BF7A72EDCACEF4E76A |
| SHA-512: | 4CD4532D35328A5123CA6DC22721A457FC3965CBF01FC1A78BCCFDB6B8FBB3286B145E316ACAAC725689CD4DA81ECF878EBFBD6B55EB241C3E3A982BCF350C2 |
| Malicious: | false |
| Preview: | .b...<.%I..XG..B.....b.b.t.}e4..i.j.{:u .S...h.W.|x...Qnb3[e.Oi.....!..L.!This program cannot be run in DOS mode....$.....%..v..v..v-..w..vk..v..vk..v..v..v..vk..v..vk..v... v(!Q.U.mSw\./t..49. ...v.....:.....a....BK....z%.....'<.P3.....PE..L.....U.....<.....`....@.....0.....@.....C8D..<.%M..X.I.B[...jb.b.t.}. 2..i.j.{:u `Q...h.W..x...Q.(1[!.Oi.....@.....P.....text...;.....<..... ..`.rdata..\....P..C.D..|.%M..X.I.B....Nb.".....4..~.j..8u .S...j.W.|x...Qnb3 [5.O..rsrc.....@..@.reloc.....@..B.....C8D..<.%M..X.I.B.....b.b.t.}e4..i.j.{:u .S...h.W.|x...Qnb3[u.Oi..... .....C8D..<.%M..X.I.B.....b.b.t.}e4..i.j.{:u |

**C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ose.exe.7878kr5jx (copy)**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 203242 |
| Entropy (8bit): | 7.226275049150236 |

| | |
|---|---|
| Encrypted: | false |
| SSDEEP: | |
| MD5: | E023A8F754E20D7866045CAAB9EC2083 |
| SHA1: | FDC5873E2E87A40A0E83F30299664F855B374C8A |
| SHA-256: | 94A3C5C9FAC0502D2CE268B678F1F98D9853C100BBA716BF7A72EDCACEF4E76A |
| SHA-512: | 4CD4532D35328A5123CA6DC22721A457FC3965CBF01FC1A78BCCFDB6B8FBB3286B145E316ACAAC725689CD4DA81ECF878EBFBD6B55EB241C3E3A982BCF35<br>0C2 |
| Malicious: | false |
| Preview: | .b...<.%I..XG..B.....b.b.t.}e4..i.j.{:u .S...h.W.\|x...Qnb3[e.Oi.....!..L.!This program cannot be run in DOS mode....$.....%..v..v..v-..w..vk..v..vk..v..v..v..vk..v..vk..v...<br>v(!Q.U.mSw\./t..49. ...v.....:.....a....BK....z%.....'<.P3.....PE..L.....U.....<.....`....@.....0.....@.....C8D..<.%M..X.I.B[...jb.b.t.}.<br>2..i.j.{:u `Q...h.W..x...Q.(1[!.Oi.....@.....P.....text....;.....<..... ..`.rdata..\....P..C.D..\|.%M..X.I.B....Nb.".....4..~.j..8u .S...j.W.\|x...Qnb3<br>[5.O..rsrc.....@..@.reloc.....@..B.....C8D..<.%M..X.I.B.....b.b.t.}e4..i.j.{:u .S...h.W.\|x...Qnb3[u.Oi.....<br>.....C8D..<.%M..X.I.B.....b.b.t.}e4..i.j.{:u |

**C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\osetup.dll**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 9833442 |
| Entropy (8bit): | 6.386071762477098 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | FC1232628D6CFAC9DB6488C87C5A73A7 |
| SHA1: | 5354858DFBCC17306986FFC6D276C3134CC7D670 |
| SHA-256: | 31F38A8050E07B0B826C94A6FC81A326C21E9FA89A5AA71CAF31A3FE3339C7D5 |
| SHA-512: | 8D92F7BD6BDC52BB441B479C602C7C825FA8326307CE478ACEA3CAE11308E1E1A67DDF518E0B6C9FDEF53EE64F656356F9937727089A53F46E589737C6CAF5<br>B |
| Malicious: | false |
| Preview: | x%...i.FT+.....Z.k..... .....<G.F.z..S....o.V.y...,..'...l.p.....!..L.!This program cannot be run in DOS mode....$.....U....n..n..n...+.#n..7..n..7.`n..7.Rn...)..n..7..n...e.....MT.5<br>.U....T..:"m.....S..-a.Rh.....G.O.....9.7.(j..7%..n..7..n.Rich.n.....PE..L.....U.....-.....3...b.....'.....P3.....3.K..i.FP...Bc.Z..d...J.`.....<G.F.z..S.....<br>V.",,...'.nal-q.....p....3.T.....\._.....@..... 3.....D.c.....text.....3.....5yy..m.FP+..Bg.ZKk.....Ni..ob<G...z..`..>.o.e.y..,..'...l.q...data.....c<br>.....c.....@....tls.....t.....@....rsrc.....v.....@..@.reloc....N...HFPY..B.~ZKk.....`...[.<..F.z..S....o.V.y..,..'...l.q.....<br>.....5.J..i.FP+..Bg.ZKk.....`.....<G.F.z..S. |

**C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\osetup.dll.7878kr5jx (copy)**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 9833442 |
| Entropy (8bit): | 6.386071762477098 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | FC1232628D6CFAC9DB6488C87C5A73A7 |
| SHA1: | 5354858DFBCC17306986FFC6D276C3134CC7D670 |
| SHA-256: | 31F38A8050E07B0B826C94A6FC81A326C21E9FA89A5AA71CAF31A3FE3339C7D5 |
| SHA-512: | 8D92F7BD6BDC52BB441B479C602C7C825FA8326307CE478ACEA3CAE11308E1E1A67DDF518E0B6C9FDEF53EE64F656356F9937727089A53F46E589737C6CAF5<br>B |
| Malicious: | false |
| Preview: | x%...i.FT+.....Z.k..... .....<G.F.z..S....o.V.y...,..'...l.p.....!..L.!This program cannot be run in DOS mode....$.....U....n..n..n...+.#n..7..n..7.`n..7.Rn...)..n..7..n...e.....MT.5<br>.U....T..:"m.....S..-a.Rh.....G.O.....9.7.(j..7%..n..7..n.Rich.n.....PE..L.....U.....-.....3...b.....'.....P3.....3.K..i.FP...Bc.Z..d...J.`.....<G.F.z..S.....<br>V.",,...'.nal-q.....p....3.T.....\._.....@..... 3.....D.c.....text.....3.....5yy..m.FP+..Bg.ZKk.....Ni..ob<G...z..`..>.o.e.y..,..'...l.q...data.....c<br>.....c.....@....tls.....t.....@....rsrc.....v.....@..@.reloc....N...HFPY..B.~ZKk.....`...[.<..F.z..S....o.V.y..,..'...l.q.....<br>.....5.J..i.FP+..Bg.ZKk.....`.....<G.F.z..S. |

**C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\pkeyconfig-office.xrm-ms**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 590837 |
| Entropy (8bit): | 7.077041178843877 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | F5136C873EF328692841FEF7DD8DC104 |

| | |
|---|---|
| SHA1: | 5F83C8CA13A4F1C3F853F668EF98FE0402D2BEB1 |
| SHA-256: | 3016A0F68E190B9548B4D04C51AB1EDCEA5787F6AF1DF73271506C2BEA6DDB63 |
| SHA-512: | 04B087A0D29940F426BE166357CAB128DD04DF0F76F8AE7FA31F828A030FBD0C54A9B2AF966E65BFB48B15ADB808B6E5A2135A538618DD9DFC5ABB4E290D6734 |
| Malicious: | false |
| Preview: | ..g.'yk.....u.v....p.(*[R..Ylb'..y..PR...s.;.[.<...e.....*9:.rg="urn:mpeg:mpeg21:2003:01-REL-R-NS"><r:license xmlns:r="urn:mpeg:mpeg21:2003:01-REL-R-NS" licenseId="{6040a6e7-445d-4609-b6c4-Du.z66.N.....:.&.O.!.pfMO.Z{:b..o..@\.^.z.b....?.D.Z....>:%.s:mx="urn:mpeg:mpeg21:2003:01-REL-MX-NS" xmlns:sl="http://www.microsoft.com/DRM/XrML2/SL/v2" xmlns:tm="http://www.microsoft.com/8F..@sK.....(.u....;.!!.e..{+m+..S.....N.i. .Z.,..\..... >..ration</r:title><r:issuer><Signature xmlns="http://www.w3.org/2000/09/xmldsig#"><SignedInfo><CanonicalizationMethod Algorithm="h.`..7.q.Z....u.$...=.b<JP.[|<4..=..N>....=. .s.;..s.6.../#!.="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/><Reference><Transforms><Transform Algorithm="urn:mpeg:mpeg21:2003:01-REL-R-NS:lic.z..Lsg.^....5.w.].!."6U...Pd-l..r.....T.f.%...&..x.....):f.rml/lwc14n"/></Transforms><DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><DigestValue>6X/xqRuE0xDP15xTDTpGJlpJ'..%=).D....{.>.....+!JX..R5c*..x...$ |

**C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\pkeyconfig-office.xrm-ms.7878kr5jx (copy)**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 590837 |
| Entropy (8bit): | 7.077041178843877 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | F5136C873EF328692841FEF7DD8DC104 |
| SHA1: | 5F83C8CA13A4F1C3F853F668EF98FE0402D2BEB1 |
| SHA-256: | 3016A0F68E190B9548B4D04C51AB1EDCEA5787F6AF1DF73271506C2BEA6DDB63 |
| SHA-512: | 04B087A0D29940F426BE166357CAB128DD04DF0F76F8AE7FA31F828A030FBD0C54A9B2AF966E65BFB48B15ADB808B6E5A2135A538618DD9DFC5ABB4E290D6734 |
| Malicious: | false |
| Preview: | ..g.'yk.....u.v....p.(*[R..Ylb'..y..PR...s.;.[.<...e.....*9:.rg="urn:mpeg:mpeg21:2003:01-REL-R-NS"><r:license xmlns:r="urn:mpeg:mpeg21:2003:01-REL-R-NS" licenseId="{6040a6e7-445d-4609-b6c4-Du.z66.N.....:.&.O.!.pfMO.Z{:b..o..@\.^.z.b....?.D.Z....>:%.s:mx="urn:mpeg:mpeg21:2003:01-REL-MX-NS" xmlns:sl="http://www.microsoft.com/DRM/XrML2/SL/v2" xmlns:tm="http://www.microsoft.com/8F..@sK.....(.u....;.!!.e..{+m+..S.....N.i. .Z.,..\..... >..ration</r:title><r:issuer><Signature xmlns="http://www.w3.org/2000/09/xmldsig#"><SignedInfo><CanonicalizationMethod Algorithm="h.`..7.q.Z....u.$...=.b<JP.[|<4..=..N>....=. .s.;..s.6.../#!.="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/><Reference><Transforms><Transform Algorithm="urn:mpeg:mpeg21:2003:01-REL-R-NS:lic.z..Lsg.^....5.w.].!."6U...Pd-l..r.....T.f.%...&..x.....):f.rml/lwc14n"/></Transforms><DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><DigestValue>6X/xqRuE0xDP15xTDTpGJlpJ'..%=).D....{.>.....+!JX..R5c*..x...$ |

**C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\setup.dll**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 608250 |
| Entropy (8bit): | 6.46323965715756 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | 75BAA8DFF6DA95D6F5CE17AF43BD6EFE |
| SHA1: | CED6B5606B35252088A708F357B903F14BBFDC96 |
| SHA-256: | 7A225849BD3914AD587042651CD873F421988A27426213E894EDCC6C151C455D |
| SHA-512: | 3B7ECD1425C2BBF2FD3E5F73920EF8821B18A08AD8947C563928E69AD130A48360B1FB0618F2D26A7074F3E55BFC945204D5D880AAD31B39DDD830CA4CE23F2 |
| Malicious: | false |
| Preview: | (.A.v..e.....NRu..J')..-.9.PUO..S....Q..*[.>..f.:.....Q...a.....!..L.!This program cannot be run in DOS mode....$.....\|zI.8.'.8.'..8.'..B#.>.'..J.?.'..Z.:.'....0.'....-.'.8.&...'.....C....*3..7..f.x.o<.uIo..+Kr.,.qL..0C..k%.:...F..X.....B..9.'..B%.9.'.Rich8.'.....PE..L...Y..U.....-.....w..d....[<.N.u..J7)..-.9.PUO..U..Q..,[i>..fS<...}....Q...a.,.....0..8F.....T.....P.....Xy..@.....X...d.....text.....eD..U.....`/M.N....J.*..E.9..VO..S....Q..*[Q>.H.[.....Q...a.R..@....tls.....P.....@....rsrc...X.....R.....@..@.reloc..8F...0...H.....eD..u..e.....,..u..J')..-.9.PUO..S....Q..*[.>..f.:.....Q...a.....eD..u..e....[,.N.u..J')..-.9.PUO..S....Q |

**C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\setup.dll.7878kr5jx (copy)**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 608250 |
| Entropy (8bit): | 6.46323965715756 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | 75BAA8DFF6DA95D6F5CE17AF43BD6EFE |
| SHA1: | CED6B5606B35252088A708F357B903F14BBFDC96 |

| | |
|---|---|
| SHA-256: | 7A225849BD3914AD587042651CD873F421988A27426213E894EDCC6C151C455D |
| SHA-512: | 3B7ECD1425C2BBF2FD3E5F73920EF8821B18A08AD8947C563928E69AD130A48360B1FB0618F2D26A7074F3E55BFC945204D5D880AAD31B39DDD830CA4CE23F<br>2 |
| Malicious: | false |
| Preview: | (.A.v..e.....NRu..J').-.9.PUO..S....Q..*[.>..f.:.....Q...a.....!..L.!This program cannot be run in DOS mode....$.....\|zI.8.'.8.'.8.'..B#.>.'..J.?.'..Z.:.'....0.'....-.'.8.&...'.....C....*3..<br>7..f.x.o<.uIo..+Kr.,.qL..0C..k%.:...F..X.....B..9.'..B%.9.'..Rich8.'.....PE..L...Y..U.....-.....w..d....[<.N.u..J7)..-.9.PUO..U..Q..,<br>[i>..fS<...}....Q...a.,.....0..8F.....T.....P.....Xy..@.....X...d.....text.....eD..U.....`/M.N....J.*..E.9..VO..S....Q..*[Q>.H.[.....Q...a.R..<br>.....@....tls.....P.....@....rsrc...X.....R.....@..@.reloc..8F...0...H.....eD..u..e....,..u..J')..-.9.PUO..S....Q..*[.>..f.:.....Q...a.....<br>.....eD..u..e....[,.N.u..J')..-.9.PUO..S....Q |

**C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\setup.exe**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 237050 |
| Entropy (8bit): | 5.401030939777094 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | EFDBD54FAC46EF08CD56D3147F7027C9 |
| SHA1: | A57C67D87A4E1BD66B5338A28AE5516F31F1FAE1 |
| SHA-256: | 8E775E4EC8A8A47961CCB264CB39FD0EFB9E32CCB714A531AAE430C0A80A5AAB |
| SHA-512: | 785B5AE5D8A549CC93490A4981A6D91EFAB832185053156DB2FFE4DC4DBDBC89E3D22586174E268686EA3031C30ED84E5EE8DF75E9B9FEA7BCE5C86BF2ED2<br>430 |
| Malicious: | false |
| Preview: | sO.E_P... ....4.be...Ku.....~..O;.#...<{..>.....AV}.1.;.<..a.7.....!..L.!This program cannot be run in DOS mode....$.....Z..Z..Z....(.S....*. ....+.B.....K.....x.....K....r...K..d.T.<br>.1r.o~..A.."g%.(.(.HZn..\|..V.:&Y..AV}.1.;.<..`.7.....PE..L...?..U.....@.....~....@.....>.DE\P.."...yF4..u...w.T...~..O;v ...<br><{.g.>....c.AV).1.;.<..`.7.....@.....(.....@.....text..... ..`.rdata..>G.....H.....>.DE\P... ...F4.....Ku.....~o.O;.#..1<{..>.....AV=.1D.<br>.O..`.7X.....@..@.reloc.....t.....@..B.....>.DE\P... ..QF4..e...Ku.T...~..O;.#...<{..>.....AV}.1.;.<..`.7.....<br>.....>.DE\P... ..QF4..e...Ku.T...~..O;.#...<{ |

**C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\setup.exe.7878kr5jx (copy)**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 237050 |
| Entropy (8bit): | 5.401030939777094 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | EFDBD54FAC46EF08CD56D3147F7027C9 |
| SHA1: | A57C67D87A4E1BD66B5338A28AE5516F31F1FAE1 |
| SHA-256: | 8E775E4EC8A8A47961CCB264CB39FD0EFB9E32CCB714A531AAE430C0A80A5AAB |
| SHA-512: | 785B5AE5D8A549CC93490A4981A6D91EFAB832185053156DB2FFE4DC4DBDBC89E3D22586174E268686EA3031C30ED84E5EE8DF75E9B9FEA7BCE5C86BF2ED2<br>430 |
| Malicious: | false |
| Preview: | sO.E_P... ....4.be...Ku.....~..O;.#...<{..>.....AV}.1.;.<..a.7.....!..L.!This program cannot be run in DOS mode....$.....Z..Z..Z....(.S....*. ....+.B.....K.....x.....K....r...K..d.T.<br>.1r.o~..A.."g%.(.(.HZn..\|..V.:&Y..AV}.1.;.<..`.7.....PE..L...?..U.....@.....~....@.....>.DE\P.."...yF4..u...w.T...~..O;v ...<br><{.g.>....c.AV).1.;.<..`.7.....@.....(.....@.....text..... ..`.rdata..>G.....H.....>.DE\P... ...F4.....Ku.....~o.O;.#..1<{..>.....AV=.1D.<br>.O..`.7X.....@..@.reloc.....t.....@..B.....>.DE\P... ..QF4..e...Ku.T...~..O;.#...<{..>.....AV}.1.;.<..`.7.....<br>.....>.DE\P... ..QF4..e...Ku.T...~..O;.#...<{ |

**C:\MSOCache\All Users\{90160000-0016-0409-0000-0000000FF1CE}-C\ExcelLR.cab**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 5769880 |
| Entropy (8bit): | **7.999656053069699** |
| Encrypted: | **true** |
| SSDEEP: | |
| MD5: | B552A9089ED105BE914E9AB54D5948DB |
| SHA1: | 70550DB9ED93F9A40BE9FF799DF5416846F0DA9A |
| SHA-256: | A50CF2AF0C47CCDDF34C34B99262F0AA11BC0DEF1C100EAA0CE7E94ADF4B3D06 |
| SHA-512: | 52983966A46CE6B1D42E9B0D042108810E0B22E453217552618C0205398D73D1FB46D064044E33C223015DB8C0E76BA313D41B9AC5A1DBAE9A66C2281F86E6C |
| Malicious: | **true** |

| | |
|---|---|
| Preview: | ..t.....}.?...4.&.N.....w.@..D...T.6.d.G.9.]..Uz.q.....4.....F"O .ANALYS32.XLL_1033..2.....F.O .AS_ClientMsmdsrv_rll_32_1033.591605AC_46A6_49C2_9395_A3F7477D339D..&..xM.....D.|...MU.*.t.....s...U.g.F,U-..c%.2...!.+.u.F7477D339D.(7..Ht%....F.O .AS_msolui110_rll_32_1033.591605AC_46A6_49C2_9395_A3F7477D339D.P...p.%....F"O .ATPVBAEN.XLAM_1033..G..T....?XB..?...9Na...R...#....t...x...<...X^:*.....5. .BLOODPRESSURETRACKER_TP10073878.XLTX_1033..=....'....F.. .EXCEL.HXS_1033.m....O>....F.. .EXCEL_COL.HXC_1033.....CR>....F.. .EX..{...0.O.`....pr&.N.U.....A.D.....i.;...)'RR..el..... .4..F.. .EXCEL_K_COL.HXK_1033.k....S>....F.. .EXCEL12.XLSX_1033.MJ..^j>....F.. .EXPENSEREPORT_TP10073879.XLTX_1033.Ov....>....F"O ...y...0.[.r....C..5N.....wQ..d...w.+...].^P.....A..*./.l.TX_1033..u...!B....F.. .PERSONALMONTHLYBUDGET_TP10073882.XLTX_1033.....N.B....F"O .PROCDB.XLAM_1033..N....M....F.. .PROTTPLN.DOC.....<C.....F&.n.V...'.....p... |

## C:\MSOCache\All Users\{90160000-0016-0409-0000-0000000FF1CE}-C\ExcelLR.cab.7878kr5jx (copy)

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 5769880 |
| Entropy (8bit): | **7.999656053069699** |
| Encrypted: | **true** |
| SSDEEP: | |
| MD5: | B552A9089ED105BE914E9AB54D5948DB |
| SHA1: | 70550DB9ED93F9A40BE9FF799DF5416846F0DA9A |
| SHA-256: | A50CF2AF0C47CCDDF34C34B99262F0AA11BC0DEF1C100EAA0CE7E94ADF4B3D06 |
| SHA-512: | 52983966A46CE6B1D42E9B0D042108810E0B22E453217552618C0205398D73D1FB46D064044E33C223015DB8C0E76BA313D41B9AC5A1DBAE9A66C2281F86E6C( |
| Malicious: | **true** |
| Preview: | ..t.....}.?...4.&.N.....w.@..D...T.6.d.G.9.]..Uz.q.....4.....F"O .ANALYS32.XLL_1033..2.....F.O .AS_ClientMsmdsrv_rll_32_1033.591605AC_46A6_49C2_9395_A3F7477D339D..&..xM.....D.|...MU.*.t.....s...U.g.F,U-..c%.2...!.+.u.F7477D339D.(7..Ht%....F.O .AS_msolui110_rll_32_1033.591605AC_46A6_49C2_9395_A3F7477D339D.P...p.%....F"O .ATPVBAEN.XLAM_1033..G..T....?XB..?...9Na...R...#....t...x...<...X^:*.....5. .BLOODPRESSURETRACKER_TP10073878.XLTX_1033..=....'....F.. .EXCEL.HXS_1033.m....O>....F.. .EXCEL_COL.HXC_1033.....CR>....F.. .EX..{...0.O.`....pr&.N.U.....A.D.....i.;...)'RR..el..... .4..F.. .EXCEL_K_COL.HXK_1033.k....S>....F.. .EXCEL12.XLSX_1033.MJ..^j>....F.. .EXPENSEREPORT_TP10073879.XLTX_1033.Ov....>....F"O ...y...0.[.r....C..5N.....wQ..d...w.+...].^P.....A..*./.l.TX_1033..u...!B....F.. .PERSONALMONTHLYBUDGET_TP10073882.XLTX_1033.....N.B....F"O .PROCDB.XLAM_1033..N....M....F.. .PROTTPLN.DOC.....<C.....F&.n.V...'.....p... |

## C:\MSOCache\All Users\{90160000-0016-0409-0000-0000000FF1CE}-C\ExcelMUI.msi

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 2388282 |
| Entropy (8bit): | 7.117799486726264 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | 4FEFD7150B1C8B6471D67D4F9E4C80AA |
| SHA1: | 78928BF50FBF8D69E2FACBA141EB4350FDA97052 |
| SHA-256: | 0DEBA169F69B6B348D1811A35DCD67BE93342E9D0D83F61517E7F336E78D0A9B |
| SHA-512: | 78BA8977114ADE92B055242DB51B3FBBD920BDAFACB9A49744699D1620D13FC4217D5E11C7D1D90DD0B01B50A99E91AEE50764B6A4F35481F67D46E0390DCDBB |
| Malicious: | false |
| Preview: | ...k....H0.(.a....7...&...U..~.,..\..G.....<.X"Tac,.p.Q.).....7.t..m.Y..9.Q...3..?..Mp....UR9.{._q.!8.mM"\-s.2.....?.*.....7.t..m.Y..9.Q...3..?..Mp....UR9.{._q.!8.mM"\-s.2.....?.*.....RZ...H0.(.a....7...&..W...x.,..\..E.....<.X"Tac,.p.S.).....RZ...H0.(.a....7...&..W...x.,..\..E.....<.X"Tac,.p.S.).....RZ...H0.(.a....7...&..W...x.,..\.. |

## C:\MSOCache\All Users\{90160000-0016-0409-0000-0000000FF1CE}-C\ExcelMUI.msi.7878kr5jx (copy)

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 2388282 |
| Entropy (8bit): | 7.117799486726264 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | 4FEFD7150B1C8B6471D67D4F9E4C80AA |
| SHA1: | 78928BF50FBF8D69E2FACBA141EB4350FDA97052 |
| SHA-256: | 0DEBA169F69B6B348D1811A35DCD67BE93342E9D0D83F61517E7F336E78D0A9B |
| SHA-512: | 78BA8977114ADE92B055242DB51B3FBBD920BDAFACB9A49744699D1620D13FC4217D5E11C7D1D90DD0B01B50A99E91AEE50764B6A4F35481F67D46E0390DCDBB |
| Malicious: | false |

| | |
|---|---|
| Preview: | ...k....H0.(.a....7...&...U..~.,..\..G.....<.X"Tac,.p.Q.).....7.t..m.Y..9.Q...3..?..Mp....UR9.{._q.!8.mM'\-s.2.....?.*.....RZ...H0.(.a....7...&..W...x.,..\..E.....<.X"Tac,.p.S.).....RZ...H0.(.a....7...&..W...x.,..\..E.....<.X"Tac,.p.S.).....RZ...H0.(.a....7...&..W...x.,..\.. |

**C:\MSOCache\All Users\{90160000-0016-0409-0000-0000000FF1CE}-C\ExcelMUI.xml**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 2094 |
| Entropy (8bit): | 7.766127127438384 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | F318DD3E3868D62228AC331D5C584C3E |
| SHA1: | F0E4D3D03B137671B20D6E37EEF685426B6DBDA4 |
| SHA-256: | 2FA97A785704825C1A244EF0EEEDB4C168A6BDA259E44A5B4DA246CCD83520E7 |
| SHA-512: | 3F8BD778ABE7B014ED6A9AC3DCC4FF8EFD0300ADE7BD765B13F7DAAEFBDCE9E90D0C586C1C1FDA9EB31840FBC04E70CCD269D68135D8D042905129C32C6<br>755B |
| Malicious: | false |
| Preview: | .t.V)L...}....I...f*.c...<..)..^..9.<..q<.Q.L.[..yX...b.p."..8...^?U?..,.....'W..Tb./G..y.}mFE..!+.?.03x:.V9....d.z..O.f.9.p.<....n...!..%\|*p...1.-<..n.dT.1..&*./.X.K..Mj..J.,\..^.q.3.U2<br>/)...L...+..+)*s.....g.....%....`0./.F\{8`y^..8.`.Z.fn.k...K".....V.....3.%Q..71..S..p.LnMe...P...T5Nxo.F....M.S..E.P...M,T;..I.....>.U..(...Z..r.ysOx...v.:.N(P.*i~....l.~..D.^.z.at..<br>...m.....%.n..o.o5....UxHc..mT.A.D.\|+5a^....8.B.tc.c.v.v.%\..`.....9...+p..n..Q.Z&.3..o=...e.\|:.Co..P.,...d..#.{..sAN...9....U...v.@0..S..?)..k.b~Qq..# .M./Q1zk.=..B.$...&X.f<br>.?.Z+....)....K...*..f...o.:3....>..D..9h...H."l.Th..3.q._...g.z...r+....'.....d~A2.[j.\|..1.{kWk...x.\.e\=.!On....\|.p..q...8..{at...R.....LFLF...'.'+....csJv..,....I.{*<BB....$...v..\|.?..p[M...*....D../<br>.R..B...)..Q.QIB`..9U...d.=ag!...].p.E.&R...B.} ....4....?..#.?n...3.&O..Y..XLq..o-.B..h.r.\....p...0..T.&.^.#...u.....xBz..$7.6~....>..D..9h...H."l.Th..!.x.]..^.v...O)3O...6.....w<br>wG8._..K...H.]tMP.. |

**C:\MSOCache\All Users\{90160000-0016-0409-0000-0000000FF1CE}-C\ExcelMUI.xml.7878kr5jx (copy)**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 2094 |
| Entropy (8bit): | 7.766127127438384 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | F318DD3E3868D62228AC331D5C584C3E |
| SHA1: | F0E4D3D03B137671B20D6E37EEF685426B6DBDA4 |
| SHA-256: | 2FA97A785704825C1A244EF0EEEDB4C168A6BDA259E44A5B4DA246CCD83520E7 |
| SHA-512: | 3F8BD778ABE7B014ED6A9AC3DCC4FF8EFD0300ADE7BD765B13F7DAAEFBDCE9E90D0C586C1C1FDA9EB31840FBC04E70CCD269D68135D8D042905129C32C6<br>755B |
| Malicious: | false |
| Preview: | .t.V)L...}....I...f*.c...<..)..^..9.<..q<.Q.L.[..yX...b.p."..8...^?U?..,.....'W..Tb./G..y.}mFE..!+.?.03x:.V9....d.z..O.f.9.p.<....n...!..%\|*p...1.-<..n.dT.1..&*./.X.K..Mj..J.,\..^.q.3.U2<br>/)...L...+..+)*s.....g.....%....`0./.F\{8`y^..8.`.Z.fn.k...K".....V.....3.%Q..71..S..p.LnMe...P...T5Nxo.F....M.S..E.P...M,T;..I.....>.U..(...Z..r.ysOx...v.:.N(P.*i~....l.~..D.^.z.at..<br>...m.....%.n..o.o5....UxHc..mT.A.D.\|+5a^....8.B.tc.c.v.v.%\..`.....9...+p..n..Q.Z&.3..o=...e.\|:.Co..P.,...d..#.{..sAN...9....U...v.@0..S..?)..k.b~Qq..# .M./Q1zk.=..B.$...&X.f<br>.?.Z+....)....K...*..f...o.:3....>..D..9h...H."l.Th..3.q._...g.z...r+....'.....d~A2.[j.\|..1.{kWk...x.\.e\=.!On....\|.p..q...8..{at...R.....LFLF...'.'+....csJv..,....I.{*<BB....$...v..\|.?..p[M...*....D../<br>.R..B...)..Q.QIB`..9U...d.=ag!...].p.E.&R...B.} ....4....?..#.?n...3.&O..Y..XLq..o-.B..h.r.\....p...0..T.&.^.#...u.....xBz..$7.6~....>..D..9h...H."l.Th..!.x.]..^.v...O)3O...6.....w<br>wG8._..K...H.]tMP.. |

**C:\MSOCache\All Users\{90160000-0016-0409-0000-0000000FF1CE}-C\Setup.xml**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 2796 |
| Entropy (8bit): | 7.834624537450112 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | 9FF45CD0F7311F8F29AC2E6DF823A404 |
| SHA1: | 3CB386C4CF396144037CA2042292E9D1EFE0C526 |
| SHA-256: | 73B45C99B14126A8F54D5E693B301CDF34ACF13ED03B6A688AB51035DF363202 |
| SHA-512: | C0AD018ED34D6BBE7CCB73BF4644C78FFACF79C53B1B32E227BC8A6EE6F288858D89EB3B2A53F14F9BDDC55010ADA8C7A4624FDEF3F31645E9A85560B4BEA<br>FC3 |
| Malicious: | false |

| | |
|---|---|
| Preview: | ....OjCMr....'.x.....u.N...uE...V.*..4.XH....8..t...Af.....PL.r_T...V..+.Q....=N6....**.U>.F..A.@\|.....p)...^N.....6A.LpC..V..g.m....PN<4...f...j;..h.T.Dq#..1....7...Bx.....Q.ymaG...U...<br>.H.....4i.&...E..7b....F.NBg.....+...P.....Wz.zOc.....4..*.e.....S ....&..._>.RP.u.~F5.....$$...CG.....,k+tqu....H..'.A.....o.A...C...v...s.S.`T.../...9...r}.....sy..I....1..*.....>&K^../;.O..i\.;<br>..f?..$...3`...WR.....@..PQw.....@..-.n.....w.....1...O...5...Hu.../M..}`..FN.....F...D....q..).F.....wDS...r..M).S].m.%\|?..a)..!...fS....._.3P["....`..j.F....m.Z<...\|...^U.gQ.t.XJ4..,<br>....#....s.....B>P."....'..!.B....h.....j.....,SY.u.pD>..3...%...T....._.3P["....9..<.L...EK.....g..._...\|...ri... ...b...K.....T.W[e...`..h.J.....Z.....z.....9...(....&....t.....@..PNa....d..u<br>.o...G_.....\|..I..T..w.%%... ...7...UC.....@.G?!....I..h.G.....w'....U..lJ.d].x.kq...5...-.....b(FMn....'..!.B....m.....vU..UJ.- |

**C:\MSOCache\All Users\{90160000-0016-0409-0000-0000000FF1CE}-C\Setup.xml.7878kr5jx (copy)**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 2796 |
| Entropy (8bit): | 7.834624537450112 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | 9FF45CD0F7311F8F29AC2E6DF823A404 |
| SHA1: | 3CB386C4CF396144037CA2042292E9D1EFE0C526 |
| SHA-256: | 73B45C99B14126A8F54D5E693B301CDF34ACF13ED03B6A688AB51035DF363202 |
| SHA-512: | C0AD018ED34D6BBE7CCB73BF4644C78FFACF79C53B1B32E227BC8A6EE6F288858D89EB3B2A53F14F9BDDC55010ADA8C7A4624FDEF3F31645E9A85560B4BEA<br>FC3 |
| Malicious: | false |
| Preview: | ....OjCMr....'.x.....u.N...uE...V.*..4.XH....8..t...Af.....PL.r_T...V..+.Q....=N6....**.U>.F..A.@\|.....p)...^N.....6A.LpC..V..g.m....PN<4...f...j;..h.T.Dq#..1....7...Bx.....Q.ymaG...U...<br>.H.....4i.&...E..7b....F.NBg.....+...P.....Wz.zOc.....4..*.e.....S ....&..._>.RP.u.~F5.....$$...CG.....,k+tqu....H..'.A.....o.A...C...v...s.S.`T.../...9...r}.....sy..I....1..*.....>&K^../;.O..i\.;<br>..f?..$...3`...WR.....@..PQw.....@..-.n.....w.....1...O...5...Hu.../M..}`..FN.....F...D....q..).F.....wDS...r..M).S].m.%\|?..a)..!...fS....._.3P["....`..j.F....m.Z<...\|...^U.gQ.t.XJ4..,<br>....#....s.....B>P."....'..!.B....h.....j.....,SY.u.pD>..3...%...T....._.3P["....9..<.L...EK.....g..._...\|...ri... ...b...K.....T.W[e...`..h.J.....Z.....z.....9...(....&....t.....@..PNa....d..u<br>.o...G_.....\|..I..T..w.%%... ...7...UC.....@.G?!....I..h.G.....w'....U..lJ.d].x.kq...5...-.....b(FMn....'..!.B....m.....vU..UJ.- |

**C:\MSOCache\All Users\{90160000-0016-0409-0000-0000000FF1CE}-C\instructions_read_me.txt**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 1091 |
| Entropy (8bit): | 4.804750185554599 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | BA21D49977850F54961EDE73B7E9E480 |
| SHA1: | BD630B3DBE9D7139527C1FFDBB2161E7A9067AE0 |
| SHA-256: | 34757273C5E041F07B0352C51CFAB2998AB676F3A39BC0F16A1B4D68F3FAC4F8 |
| SHA-512: | 4BF9BE5F41F7258357E838BA94F0AA2B7F17D8FE3266174AAF123156B422C4FB72E4D3FD36DB7B2E3E9D13202202D2A6B0ECCA06EE2A2A043CE6AD27FFD751<br>E2 |
| Malicious: | false |
| Preview: | ATTENTION!..Your network has been breached and all data was encrypted. Please contact us at:..https://bastad5huzwkepdixedg2gekg7jk22ato24zyllp6lnjx7wdtyctgvyd.o<br>nion/ .....Login ID: 26d371a9-efda-4e82-9989-01e292244d65.....*!* To access .onion websites download and install Tor Browser at:.... https://www.torproject.org/ (Tor<br>Browser is not related to us)....*!* To restore all your PCs and get your network working again, follow these instructions:....- Any attempts to modify, decrypt or rename the<br>files will lead to its fatal corruption. It doesn't matter, who are trying to do this, either it will be your IT guys or a recovery agency.....Please follow these simple rules to avoid<br>data corruption:....- Do not modify, rename or delete files. Any attempts to modify, decrypt or rename the files will lead to its fatal corruption. ....- Do not hire a recovery<br>company. They can't decrypt without the key. ..They also don't care about your business. They believe that they are ..good negotiator |

**C:\MSOCache\All Users\{90160000-0018-0409-0000-0000000FF1CE}-C\PowerPointMUI.msi**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 2388282 |
| Entropy (8bit): | 7.137544887266395 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | A52874989F5FDB723F4E63BA44E5CBD9 |
| SHA1: | C1AC7741AA32D4B083D498DDA2E669DAD76FA564 |
| SHA-256: | B6A7A176FAED678A81CF380ED58B05D3F1D90F9A79668D1EE7D51E5BDD2EB95E |
| SHA-512: | B74FB4FFF97CFDA5B5FEE5F4D0B1ED3AE5C5D23419E3FA6211ABD968FC73E16BAB62869F5AE6A9E1696E0E63B8003351D64306B638C708EFAC63A51605BB00<br>C1 |
| Malicious: | false |

| | |
|---|---|
| Preview: | P... .L:.XC._.N.cl...v....-.....(.H.....&j..q-D..M.].$y(x:.....4..~..$.!...@..9..J2.eu.-2wE.oM<br>.".bM.P.X.fB...). .....:.....<br>.....=.RV..XC._.N.cl...v.....(.H.....&j..q-D..M.].$y*x:.....<br>.....=.RV..XC._.N.cl...v.....(.H.....&j..q-D..M.].$y*x:.....<br>...=.RV..XC._.N.cl...v.....(.H. |

**C:\MSOCache\All Users\{90160000-0018-0409-0000-0000000FF1CE}-C\PowerPointMUI.msi.7878kr5jx (copy)**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 2388282 |
| Entropy (8bit): | 7.137544887266395 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | A52874989F5FDB723F4E63BA44E5CBD9 |
| SHA1: | C1AC7741AA32D4B083D498DDA2E669DAD76FA564 |
| SHA-256: | B6A7A176FAED678A81CF380ED58B05D3F1D90F9A79668D1EE7D51E5BDD2EB95E |
| SHA-512: | B74FB4FFF97CFDA5B5FEE5F4D0B1ED3AE5C5D23419E3FA6211ABD968FC73E16BAB62869F5AE6A9E1696E0E63B8003351D64306B638C708EFAC63A51605BB00C1 |
| Malicious: | false |
| Preview: | P... .L:.XC._.N.cl...v....-.....(.H.....&j..q-D..M.].$y(x:.....4..~..$.!...@..9..J2.eu.-2wE.oM<br>.".bM.P.X.fB...). .....:.....<br>.....=.RV..XC._.N.cl...v.....(.H.....&j..q-D..M.].$y*x:.....<br>.....=.RV..XC._.N.cl...v.....(.H.....&j..q-D..M.].$y*x:.....<br>...=.RV..XC._.N.cl...v.....(.H. |

**C:\MSOCache\All Users\{90160000-0018-0409-0000-0000000FF1CE}-C\PowerPointMUI.xml**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 1975 |
| Entropy (8bit): | 7.737544643314397 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | C6BBD3B4EA05B7CDAADEC3C89E4DFF0A |
| SHA1: | 5DFED85C22819F31BB1E59B1EF5CFFB3D26B6C9C |
| SHA-256: | F9EB9A2FF0B0A2B4652976FCE982FCB73D284D833D17289982A5D7DA71687D89 |
| SHA-512: | CF7120557DAA0A9BD4967E7F55CF09CAD3CA8F3646790B43A348AF6972D442C907136AF7552BC3235D3A3B555D4B60A44735AD8C61BCAA6F00C4E12B9A4BA78 |
| Malicious: | false |
| Preview: | VU..Y....j....QX.9.....lp(z.\fY.. ?....%..@=.8-...O.. .....X..^w.>...3....3..Q|.....s}!.BnSM.Up....]...y....,...'.."......%.<W.!..q...('.c....AZ.+SDui..Fh....g...cG.'O...m.....By....:...../<br>u....1,=6Sx&...<....)...JO..A...!+.C....%'..a.%..6...5.._v.....n\?=Sjpw..[x..n..?;..!....%.....^.... ..h....S..~N.....WL.!..Er..oF...7...?...D=...Z.....>.!_.1...`../F.ie.....P#bj.$...ak....M...<br>]....(...a>.;.....HJ..E.H..J.....9v.....jw!3h|[...K"...w...0P..DZ...z.....H..]..E.....MF.+.....(..w.."...3C....I...h.....#].\....ZZ.O.....`.....|C....6<o.IHfY.o=....&...N.....5:.O.....)...P.....1...?<br>G.(.....q#mv.. ...2".....y..&....qN.3.....Y....=...O0.zR.....s.@HfJ.."I...T...c0..>...f:.....HJ..F.H...6...m|.....kL*!.`v...RT...w...x..[>...`..L.....P.<..D...?9._C.....dj.e.j}L.. 0....<br>...}...*...\..P....%...X....w....m|.'.....w{qJ/ .y.vu....`.....y..;....YY.Mv....2...PT..,...qw )wLt...?"... |

**C:\MSOCache\All Users\{90160000-0018-0409-0000-0000000FF1CE}-C\PowerPointMUI.xml.7878kr5jx (copy)**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 1975 |
| Entropy (8bit): | 7.737544643314397 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | C6BBD3B4EA05B7CDAADEC3C89E4DFF0A |
| SHA1: | 5DFED85C22819F31BB1E59B1EF5CFFB3D26B6C9C |
| SHA-256: | F9EB9A2FF0B0A2B4652976FCE982FCB73D284D833D17289982A5D7DA71687D89 |
| SHA-512: | CF7120557DAA0A9BD4967E7F55CF09CAD3CA8F3646790B43A348AF6972D442C907136AF7552BC3235D3A3B555D4B60A44735AD8C61BCAA6F00C4E12B9A4BA78 |
| Malicious: | false |
| Preview: | VU..Y....j....QX.9.....lp(z.\fY.. ?....%..@=.8-...O.. .....X..^w.>...3....3..Q|.....s}!.BnSM.Up....]...y....,...'.."......%.<W.!..q...('.c....AZ.+SDui..Fh....g...cG.'O...m.....By....:...../<br>u....1,=6Sx&...<....)...JO..A...!+.C....%'..a.%..6...5.._v.....n\?=Sjpw..[x..n..?;..!....%.....^.... ..h....S..~N.....WL.!..Er..oF...7...?...D=...Z.....>.!_.1...`../F.ie.....P#bj.$...ak....M...<br>]....(...a>.;.....HJ..E.H..J.....9v.....jw!3h|[...K"...w...0P..DZ...z.....H..]..E.....MF.+.....(..w.."...3C....I...h.....#].\....ZZ.O.....`.....|C....6<o.IHfY.o=....&...N.....5:.O.....)...P.....1...?<br>G.(.....q#mv.. ...2".....y..&....qN.3.....Y....=...O0.zR.....s.@HfJ.."I...T...c0..>...f:.....HJ..F.H...6...m|.....kL*!.`v...RT...w...x..[>...`..L.....P.<..D...?9._C.....dj.e.j}L.. 0....<br>...}...*...\..P....%...X....w....m|.'.....w{qJ/ .y.vu....`.....y..;....YY.Mv....2...PT..,...qw )wLt...?"... |

### C:\MSOCache\All Users\{90160000-0018-0409-0000-0000000FF1CE}-C\PptLR.cab

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 6310440 |
| Entropy (8bit): | **7.999677078446772** |
| Encrypted: | **true** |
| SSDEEP: | |
| MD5: | FF92DEEB59288681212D5615863DFC48 |
| SHA1: | 194E193F6CFE81C89EA1632019D101C45D382141 |
| SHA-256: | AF3124560597B5D578861F5FBD18D96CC110081F4FE005A6631BC5CACD60FDAA |
| SHA-512: | 0A3105DAB307C9F0E0F282B63218152B6ADE890255582952E8E480B6DCB21F0C6A97890280E42F1608C02E68CB6FFD5661C57237D8FBF61706B5036AEF9337BE |
| Malicious: | **true** |
| Preview: | .c....S.E.j.UDm..~q.gf.".Z...Hz.dcxFZ.....{...g.\|Z....7rh.....F.P .CHART.XLSRVINTL.DLL_1033..T.....F.. .CLASSICPHOTOALBUM.POTX_1033..T...L.....F.. .CONTEMPORARYPHOTOALBUM.....`'N`*.U....~q.!\|.....;Q0M;..F=...{...g..E...nq.8.w.INTL.DLL_1033..... ....F.. .PITCHBK.POT_1033.v....v#....F.. .POWERPNT.HXS_1033.\|.....*....F.. .POWERPNT_COL.HXC_1033.....*.....[..8...2..2_B?2...h..Lz.2.RRZ....[;.00....z..h1'..p.1033.q....*....F.. .POWERPNT_K_COL.HXK_1033..Z..9.*....F.P .PPINTL.DLL_1033..W....<....F.. .PREVIEWTEMPLATE.POTX_1033.>....5A.....F..#...(..20^"T.q.....\|0dcHRZ\...{..z\|.A..a..g>&..h..033.."..E.E....F.. .PROTTPLN.XLS_1033..0..E.F....F.. .PROTTPLV.PPT_1033.."..EDF....F.. .PROTTPLV.XLS_1033..v..EfF....F.. .QUIZSH.g.....%~.Y...i.r.6.gf\|g.@...6O)&(..\^...5o.15..k....j.z.....F.. .TRAINING.POTX_1033.4....._....F.. .WIDESCREENPRESENTATION16X9.POTX_1033..&...jb....F"O .XLINTL32.DLL_1033..\|..y.e....F"O .h....X..[.fwm..{..4f.zT.q..L0.d!xRN.. |

### C:\MSOCache\All Users\{90160000-0018-0409-0000-0000000FF1CE}-C\PptLR.cab.7878kr5jx (copy)

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 6310440 |
| Entropy (8bit): | **7.999677078446772** |
| Encrypted: | **true** |
| SSDEEP: | |
| MD5: | FF92DEEB59288681212D5615863DFC48 |
| SHA1: | 194E193F6CFE81C89EA1632019D101C45D382141 |
| SHA-256: | AF3124560597B5D578861F5FBD18D96CC110081F4FE005A6631BC5CACD60FDAA |
| SHA-512: | 0A3105DAB307C9F0E0F282B63218152B6ADE890255582952E8E480B6DCB21F0C6A97890280E42F1608C02E68CB6FFD5661C57237D8FBF61706B5036AEF9337BE |
| Malicious: | **true** |
| Preview: | .c....S.E.j.UDm..~q.gf.".Z...Hz.dcxFZ.....{...g.\|Z....7rh.....F.P .CHART.XLSRVINTL.DLL_1033..T.....F.. .CLASSICPHOTOALBUM.POTX_1033..T...L.....F.. .CONTEMPORARYPHOTOALBUM.....`'N`*.U....~q.!\|.....;Q0M;..F=...{...g..E...nq.8.w.INTL.DLL_1033..... ....F.. .PITCHBK.POT_1033.v....v#....F.. .POWERPNT.HXS_1033.\|.....*....F.. .POWERPNT_COL.HXC_1033.....*.....[..8...2..2_B?2...h..Lz.2.RRZ....[;.00....z..h1'..p.1033.q....*....F.. .POWERPNT_K_COL.HXK_1033..Z..9.*....F.P .PPINTL.DLL_1033..W....<....F.. .PREVIEWTEMPLATE.POTX_1033.>....5A.....F..#...(..20^"T.q.....\|0dcHRZ\...{..z\|.A..a..g>&..h..033.."..E.E....F.. .PROTTPLN.XLS_1033..0..E.F....F.. .PROTTPLV.PPT_1033.."..EDF....F.. .PROTTPLV.XLS_1033..v..EfF....F.. .QUIZSH.g.....%~.Y...i.r.6.gf\|g.@...6O)&(..\^...5o.15..k....j.z.....F.. .TRAINING.POTX_1033.4....._....F.. .WIDESCREENPRESENTATION16X9.POTX_1033..&...jb....F"O .XLINTL32.DLL_1033..\|..y.e....F"O .h....X..[.fwm..{..4f.zT.q..L0.d!xRN.. |

### C:\MSOCache\All Users\{90160000-0018-0409-0000-0000000FF1CE}-C\Setup.xml

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 2386 |
| Entropy (8bit): | 7.776618243979623 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | 3DCE076CBB5BC80031F80DA08DC44B48 |
| SHA1: | EE545CF0EDB35F72352001E28253790476003CBF |
| SHA-256: | 483E131849C77AED9A1BCC489D349502930623C11F24D83D19E3B5FAA237C3F7 |
| SHA-512: | 0DB18552918B55F7FF3E71A50F4741B4619407664A98EB41DA5B85D809BCBAD3672AC22600831634DAAD7B5445DA09A2C9E09F774A1F7C5799B296536A09E978 |
| Malicious: | false |
| Preview: | E..,....H...QY*.>'.\....}..z.g..Tk....$.N.a..U...a:-..N"..YFZ(..(..7.I...v.F.uA...P...r.%6.x.....M..`*.[..@..Q....I...3@..ydA!.5'../.^...S.d.#c.7.J..-.76.e..."j,.....[..d...6E...TF..gR?...w..7.k...~ ;. V.7.3..U..6.K..Aw...85.<..k..X...0e0..3u..MKI..,.....}...f.F.UM.9....I.\..e...(..N..P^.&.....K...sc.../A..drb2..8 ...V...]3K.Yc...5..y.56.=....(j..Rv.P..t..H....@...+j..EQj=.....O...Y._.D~.3.)...M.@j.....=V..P\|.A..[..P...(!!..c.[\...^.&.6....F.g.t*.,....{..3.G../<O..k}.A.....".U3.....FA2[..6#...T...S.m.27.....G..3./....(O..]q....C..b...(2f...2..fVn...6....H...ZY*.ud.\.....z.O>.a..aC*..il....e.."...1j...%u..aAK...cb...[...l.i.u*.0.....4..4.~..-+P..m%.....i...0`3...u..fVjD..$1.Y.S...QY*.ud.S.v...[....\|...Qks..}m....@..".....n1..2d..j.-5.. ..Y.S...S...rd...F..g.M..a...>b..\|j.....o...V.M...d..a.F..^...?.V.... m.qb.....).!(.s..( P..uw."..I..=...~/..../...\|..xdk...5+.....i.....3....4..z.]...(Q..pt....h..a....{%..\2..\|@a..\.+...V...].m.d*...Y..g..+.e...;W..\| |

### C:\MSOCache\All Users\{90160000-0018-0409-0000-0000000FF1CE}-C\Setup.xml.7878kr5jx (copy)

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |

| | |
|---|---|
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 2386 |
| Entropy (8bit): | 7.776618243979623 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | 3DCE076CBB5BC80031F80DA08DC44B48 |
| SHA1: | EE545CF0EDB35F72352001E28253790476003CBF |
| SHA-256: | 483E131849C77AED9A1BCC489D349502930623C11F24D83D19E3B5FAA237C3F7 |
| SHA-512: | 0DB18552918B55F7FF3E71A50F4741B4619407664A98EB41DA5B85D809BCBAD3672AC22600831634DAAD7B5445DA09A2C9E09F774A1F7C5799B296536A09E978 |
| Malicious: | false |
| Preview: | E..,....H...QY*.>'.\....}..z.g..Tk....$.N.a..U...a:-..N"..YFZ(..(..7.I...v.F.uA...P...r.%6.x.....M..`*.[..@..Q....I...3@..ydA!.5'../.^...S.d.#c.7.J..-.76.e..."j,.....[..d...6E...TF..gR?...w ..7.k...~ ;. V.7.3..U..6.K..Aw...85.<..k..X...0e0..3u..MKI..,.....}...f.F.UM.9....I.\..e...(.N..P^.&.....K...sc.../A..drb2..8 ...V...]3K.Yc...5..y.56.=....(j..Rv.P..t..H....@...+j..EQj=..... ..O...Y._.D~.3.)...M.@j.....=V..P\|.A..[..P...(!!..c.[\...^.&.6....F.g.t*.,....{..3.G../<O..k}.A.....".U3.....FA2[..6#...T...S.m.27.....G..3./....(O..]q....C..b...(2f...2..fVn...6....H...ZY*.ud.\.. ..z.O>.a..aC*..il....e.."...1j...%u..aAK...cb...[...l.i.u*.0.....4..4.~..-+P..m%.....i...0`3...u..fVjD..$1.Y.S...QY*.ud.S.v...[....|...Qks..}m....@.."...:n1..2d..j.-5.. ..Y.S...S...rd...F. .g.M..a...>b..|j.....o...V.M...d..a.F..^...?.V.... m.qb.....).!(.s..( P..uw."..I..=...~/....|..xdk...5+.....i.....3....4..z.]...(Q..pt....h..a....{%..\2..|@a..\.+...V...].m.d*...Y..g..+.e...;W..\| |

**C:\MSOCache\All Users\{90160000-0018-0409-0000-0000000FF1CE}-C\instructions_read_me.txt**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 1091 |
| Entropy (8bit): | 4.804750185554599 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | BA21D49977850F54961EDE73B7E9E480 |
| SHA1: | BD630B3DBE9D7139527C1FFDBB2161E7A9067AE0 |
| SHA-256: | 34757273C5E041F07B0352C51CFAB2998AB676F3A39BC0F16A1B4D68F3FAC4F8 |
| SHA-512: | 4BF9BE5F41F7258357E838BA94F0AA2B7F17D8FE3266174AAF123156B422C4FB72E4D3FD36DB7B2E3E9D13202202D2A6B0ECCA06EE2A2A043CE6AD27FFD751E2 |
| Malicious: | false |
| Preview: | ATTENTION!..Your network has been breached and all data was encrypted. Please contact us at:..https://bastad5huzwkepdixedg2gekg7jk22ato24zyllp6lnjx7wdtyctgvyd.onion/ .....Login ID: 26d371a9-efda-4e82-9989-01e292244d65.....*!* To access .onion websites download and install Tor Browser at:.... https://www.torproject.org/ (Tor Browser is not related to us)....*!* To restore all your PCs and get your network working again, follow these instructions:....- Any attempts to modify, decrypt or rename the files will lead to its fatal corruption. It doesn't matter, who are trying to do this, either it will be your IT guys or a recovery agency.....Please follow these simple rules to avoid data corruption:....- Do not modify, rename or delete files. Any attempts to modify, decrypt or rename the files will lead to its fatal corruption. ....- Do not hire a recovery company. They can't decrypt without the key. ..They also don't care about your business. They believe that they are ..good negotiator |

**C:\MSOCache\All Users\{90160000-0019-0409-0000-0000000FF1CE}-C\PubLR.cab**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 3561961 |
| Entropy (8bit): | **7.999436914411064** |
| Encrypted: | **true** |
| SSDEEP: | |
| MD5: | 763112C51BB1AC58F9713280CD066F7F |
| SHA1: | 9BCF8DC47A506BD7AB9FBEA3E23AC0AFBAF78281 |
| SHA-256: | 386268A204588801616AE03355FFD38046D37F87A093F2D4F047386A6F2C8F97 |
| SHA-512: | 3C1FF763419600CE6E09A250FF7E60BC97A42709F1458F9BDF06CEB8675B629CD89F87FD6E267F2B4DD3603F363812437B2F0CD2345DF090B33937ED974BC8D |
| Malicious: | **true** |
| Preview: | .j.....-.. i.....5..6..1...!$....]...r...w,.....Bk..CO_>.....F{. .FONTSCHM.INI_1033.....F.Q .MOR6INT.DLL_1033.p..._.....F.. .MSPUB.HXS_1033.....F.. .MSPUB.OPG_.....Y..7.s. i.....f...r...i|.....n...b...M,.....8.]~..qL.HXT_1033.r.....F.. .MSPUB_F_COL.HXK_1033.q...}.....F.. .MSPUB_K_COL.HXK_1033.+.....F.. .PAPERS.INI_1033..;.....2..~..e.....O.8....".ba...!.....S.v'.e..1.6.o.k..X^_>..F.. .PDIR12F.GIF_1033..C.....F.. .PDIR13F.GIF_1033..\.....F.. .PDIR14F.GIF_1033.....K.....F.. .PDIR15F.GIF_1033..9..X..)....,...d .8cO.rg.....1q..!.....B.`M.~.F.B...s[.;<..>.....F.. .PDIR18F.GIF_1033.O.....F.. .PDIR19F.GIF_1033.....F.. .PDIR1B.GIF_1033.m....).....F.. .PDIR1F.GIF_1033....)Y.!..7..;I.Y.@.....q.....!Z..e.R...;.a,..I.7...".W.cl.....|.....F.. .PDIR22F.GIF_1033.;1..S.....F.. .PDIR23F.GIF_1033.....F.. .PDIR24F.GIF_1033..1..;.....F.. .PDIR25F.GIF_.....7... i.....w.g{..... |

**C:\MSOCache\All Users\{90160000-0019-0409-0000-0000000FF1CE}-C\PubLR.cab.7878kr5jx (copy)**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 3561961 |

| | |
|---|---|
| Entropy (8bit): | **7.999436914411064** |
| Encrypted: | **true** |
| SSDEEP: | |
| MD5: | 763112C51BB1AC58F9713280CD066F7F |
| SHA1: | 9BCF8DC47A506BD7AB9FBEA3E23AC0AFBAF78281 |
| SHA-256: | 386268A204588801616AE03355FFD38046D37F87A093F2D4F047386A6F2C8F97 |
| SHA-512: | 3C1FF763419600CE6E09A250FF7E60BC97A42709F1458F9BDF06CEB8675B629CD89F87FD6E267F2B4DD3603F363812437B2F0CD2345DF090B33937ED974BC8D |
| Malicious: | **true** |
| Preview: | .j.....-.. i.....5..6..1...!$....]...r...w,.....Bk..CO_>.....F{. .FONTSCHM.INI_1033.....F.Q .MOR6INT.DLL_1033.p..._.....F.. .MSPUB.HXS_1033.....F.. .MSPUB.OPG_.....Y..7.s. i.....f...r...i|.....n...b...M,.....8.]~..qL.HXT_1033.r.....F.. .MSPUB_F_COL.HXK_1033.q...}.....F.. .MSPUB_K_COL.HXK_1033.+.....F.. .PAPERS.INI_1033..;.....2..~..e.....O.8...."..ba...!.....S.v'.e..1.6.o.k..X^_>..F.. .PDIR12F.GIF_1033..C.....F.. .PDIR13F.GIF_1033..\.....F.. .PDIR14F.GIF_1033.....K.....F.. .PDIR15F.GIF_1033..9..X..)....,...d .8cO.rg.....1q..!.....B.`M.~.F.B...s[.;<..>.....F.. .PDIR18F.GIF_1033.O.....F.. .PDIR19F.GIF_1033.....F.. .PDIR1B.GIF_1033.m....).....F.. .PDIR1F.GIF_1033....)Y.!..7..;I.Y.@.....q.....!Z..e.R...;.a,..I.7...".W.cl.....|.....F.. .PDIR22F.GIF_1033.;1..S.....F.. .PDIR23F.GIF_1033.....F.. .PDIR24F.GIF_1033..1..;.....F.. .PDIR25F.GIF_.....7... i.....w.g{..... |

**C:\MSOCache\All Users\{90160000-0019-0409-0000-0000000FF1CE}-C\PublisherMUI.msi**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 2408762 |
| Entropy (8bit): | 7.112066530806255 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | F3E4687F1A70CFC79927E5D3168FB202 |
| SHA1: | A258C03DFCD934B5E36D453545E07000084D4509 |
| SHA-256: | 4F0F609BC8E12A371D059F3C238ECFCDB6668E8B81049FB721749E779685303C |
| SHA-512: | EF27094168A2127646C55A76C82425112B5D42202B181251FC87281C579A39D65C1C0CED4B3E053BD149FA28A650632DC2DFDA5F107DC8ABE9C12E98B0C97C |
| Malicious: | false |
| Preview: | ..(....4...1aj....^...8.~.....9...f....."zw0...uO..K..`Y.....7.....v[...o.#.c...>-..:...=.#p..]....ZD..Tx.Z...~!.....7.....v[...o.#.c...>-..:...=.#p..]....ZD..Tx.Z...~!.....7w..nC..4...1aj....^...8.~..n....9...f....."zw1...uO..K..`[.....7w..nC..4...1aj....^...8.~..n....9...f....."zw1...uO..K..`[.....7w..nC..4...1aj....^...8.~..n....9...f.. |

**C:\MSOCache\All Users\{90160000-0019-0409-0000-0000000FF1CE}-C\PublisherMUI.msi.7878kr5jx (copy)**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 2408762 |
| Entropy (8bit): | 7.112066530806255 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | F3E4687F1A70CFC79927E5D3168FB202 |
| SHA1: | A258C03DFCD934B5E36D453545E07000084D4509 |
| SHA-256: | 4F0F609BC8E12A371D059F3C238ECFCDB6668E8B81049FB721749E779685303C |
| SHA-512: | EF27094168A2127646C55A76C82425112B5D42202B181251FC87281C579A39D65C1C0CED4B3E053BD149FA28A650632DC2DFDA5F107DC8ABE9C12E98B0C97C |
| Malicious: | false |
| Preview: | ..(....4...1aj....^...8.~.....9...f....."zw0...uO..K..`Y.....7.....v[...o.#.c...>-..:...=.#p..]....ZD..Tx.Z...~!.....7.....v[...o.#.c...>-..:...=.#p..]....ZD..Tx.Z...~!.....7w..nC..4...1aj....^...8.~..n....9...f....."zw1...uO..K..`[.....7w..nC..4...1aj....^...8.~..n....9...f....."zw1...uO..K..`[.....7w..nC..4...1aj....^...8.~..n....9...f.. |

**C:\MSOCache\All Users\{90160000-0019-0409-0000-0000000FF1CE}-C\PublisherMUI.xml**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 1976 |
| Entropy (8bit): | 7.77163005338989 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | BC8487D06DCBFD8662A4BC93CF556B28 |
| SHA1: | DB479A5DCF2FDE5C4DEFCDC898A3FA22F91A8645 |

| | |
|---|---|
| SHA-256: | 52E3843105946F4D5AB140CA7FFEB22790EEFF9A6DF3E8F640D842186B32C175 |
| SHA-512: | 025878B05492175A7C405E4A88693F57A42B1F11475EC1FC708C666FA228714D4587EA3AB3292186428C0256E3C0FA93F4D742C844DFAE63360731638F76E722 |
| Malicious: | false |
| Preview: | ...FW...0tB..F....<.X..=...\|t...;~k.....&....[.Y..VC.5c...1LC'..(Pk.V6.....c..b.[.@8...Cfw!.....8B.k=$K.....9).X9..wNl.\|.....a.V...9...]3...\|O*6.....7...[..;I.H15qo.Y...-,L6R..)<br>x{..3...=.]....B._IM...JZ.....>..rR.g..kj.F.....dOK..4k@.KK.....!.v.gr...s~"5....)...A..mF."8.TE.E...J?[4...*{h..3...?....6.P.mH_..]t!I.....z.....O.`'.GQ.?....?.....!*..b.....(.k..n.....L..<br>Wo!.....0e.Xe.p...u....OJ_...?..M.....;.R..!.v.'M#...R%.....s...J..&].e..zE.T,.LO.GM..s-...T....i.....c...9F6..qybF.....1...W...I..%y[(..Fg.])X....7QL.K.....h.....B.oo....\|xP.....<br>.....L.3..\|L..?..5.F.;..&nd.X.....{.x...n...83A...Jo.....-.....d).wS..%....I....a2..&m....-.I...Y...la...Q$.....#.....!\.%..jL.Gg._Yi....a,...Q.....S.2...'.L.[e...P9b6.....#...E...K..W..jU..<br>i.tEl....1x..HY....+.V.....W.V1@..$.....{.Z...H!.-..jl.....]0NJ_..!M_..A.....T.2.6.W.{eN.=8.....-..'w....sA.....[.4...~?...i...).R..6...m=R..Yi%9. |

**C:\MSOCache\All Users\{90160000-0019-0409-0000-0000000FF1CE}-C\PublisherMUI.xml.7878kr5jx (copy)**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 1976 |
| Entropy (8bit): | 7.77163005338989 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | BC8487D06DCBFD8662A4BC93CF556B28 |
| SHA1: | DB479A5DCF2FDE5C4DEFCDC898A3FA22F91A8645 |
| SHA-256: | 52E3843105946F4D5AB140CA7FFEB22790EEFF9A6DF3E8F640D842186B32C175 |
| SHA-512: | 025878B05492175A7C405E4A88693F57A42B1F11475EC1FC708C666FA228714D4587EA3AB3292186428C0256E3C0FA93F4D742C844DFAE63360731638F76E722 |
| Malicious: | false |
| Preview: | ...FW...0tB..F....<.X..=...\|t...;~k.....&....[.Y..VC.5c...1LC'..(Pk.V6.....c..b.[.@8...Cfw!.....8B.k=$K.....9).X9..wNl.\|.....a.V...9...]3...\|O*6.....7...[..;I.H15qo.Y...-,L6R..)<br>x{..3...=.]....B._IM...JZ.....>..rR.g..kj.F.....dOK..4k@.KK.....!.v.gr...s~"5....)...A..mF."8.TE.E...J?[4...*{h..3...?....6.P.mH_..]t!I.....z.....O.`'.GQ.?....?.....!*..b.....(.k..n.....L..<br>Wo!.....0e.Xe.p...u....OJ_...?..M.....;.R..!.v.'M#...R%.....s...J..&].e..zE.T,.LO.GM..s-...T....i.....c...9F6..qybF.....1...W...I..%y[(..Fg.])X....7QL.K.....h.....B.oo....\|xP.....<br>.....L.3..\|L..?..5.F.;..&nd.X.....{.x...n...83A...Jo.....-.....d).wS..%....I....a2..&m....-.I...Y...la...Q$.....#.....!\.%..jL.Gg._Yi....a,...Q.....S.2...'.L.[e...P9b6.....#...E...K..W..jU..<br>i.tEl....1x..HY....+.V.....W.V1@..$.....{.Z...H!.-..jl.....]0NJ_..!M_..A.....T.2.6.W.{eN.=8.....-..'w....sA.....[.4...~?...i...).R..6...m=R..Yi%9. |

**C:\MSOCache\All Users\{90160000-0019-0409-0000-0000000FF1CE}-C\Setup.xml**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 2109 |
| Entropy (8bit): | 7.773415931495382 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | D1EE69B440B7E6348B142CF75DF61B76 |
| SHA1: | AA7BA21273F58D54E56BC045C67C09493012EC63 |
| SHA-256: | F11E1555EAF535A18ACE9E06C5DB47AC5CB8AE94EC720312B4C628C22FE7CB01 |
| SHA-512: | 11E31C8561B77DAFDC2E3855511B9583973E74750D494824BA384EE999B72686C96E594D96E1AB03E9445351480894CBA3E9312DF9A60AEB40E06DFB0079B60B |
| Malicious: | false |
| Preview: | [5<IIZ.....*./b}A.....=p.s..G.8..?g..G.?.Z.Q..86nW..zu.....as*VU.....\.W9.i.\L...Z..A...R..}9.>.6.s4A..1*#n..!j...y.b!LD>.....J.4.I\.&M...s..V..-.i..@^..X...[.K...v.`z..iy...%.R}J.6..<br>...].q..f./+..fO....G.$...L..5.).(v\|...P/.7.2\|...a#:.tt>.....Q.z.rl.8J..&8..G....i...>..:...{.k...1..a...5...fTc.NA.....+.zt.J..0..bc..6.....,..f...&.!.A.o..DW$}.h*....%;.Y\/.....J.x..h.. ..n:..<br>...9.n...$..H...y(w..+.95..s:...3Z(.eA5.....=.(F.....!Z..$....n..WP.....7.....J.#q..qS....}%xV3.....;.z&<Q..+..'r.J....8..[.....w2a...'.2k...s...:.}.eS.....h.?.4@.....*r..)..`.&..F..J...7.m.<br>.Z+9\..0t...".(dE@.....&.S/>E.KX.. v..i.....O...@.\|2e..r%3n..%s...t.o7#.2.....h.0~P..U7..:x..O.H.h..G.....7a@..p.#K..%....9.k(#.>.....h.q4`.....~..j....~..@....B.zc:....X.h..<br>>t..kEZ1cu.....}.j,)w.....q[..g.J.s..^..+...{59..'D.q..=v...2.o6uL.....\|.T.....s.V....i..@%.....p2&..c."t..%{...t!e(mJ.....r.~,1K.(...=c....H.^..S. |

**C:\MSOCache\All Users\{90160000-0019-0409-0000-0000000FF1CE}-C\Setup.xml.7878kr5jx (copy)**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 2109 |
| Entropy (8bit): | 7.773415931495382 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | D1EE69B440B7E6348B142CF75DF61B76 |
| SHA1: | AA7BA21273F58D54E56BC045C67C09493012EC63 |
| SHA-256: | F11E1555EAF535A18ACE9E06C5DB47AC5CB8AE94EC720312B4C628C22FE7CB01 |
| SHA-512: | 11E31C8561B77DAFDC2E3855511B9583973E74750D494824BA384EE999B72686C96E594D96E1AB03E9445351480894CBA3E9312DF9A60AEB40E06DFB0079B60B |
| Malicious: | false |

| | |
|---|---|
| Preview: | [5<IIZ.....*./b}A.....=p.s..G.8..?g..G.?.Z.Q..86nW..zu.....as*VU.....\.W9.i.\L...Z..A...R..}9.>.6.s4A..1*#n..!j...y.b!LD>.....J.4.I\.&M...s..V..-.i..@^..X...[.K...v.`z..iy...%.R}J.6.. ...].q..f./+..fO....G.$...L..5.).(v\|...P/.7.2\|...a#:.tt>.....Q.z.rl.8J..&8..G....i...>..:...{.k...1..a...5...fTc.NA.....+.zt.J..0..bc..6....,..f...&.!.A.o..DW$}.h*....%;.Y\/.....J.x..h.. ..n:.. ...9.n...$..H...y(w..+.95..s:...3Z(.eA5.....=.(F.....!Z..$....n..WP.....7.....J.#q..qS....}%xV3.....:.z&<Q..+..'r.J....8..[.....w2a...'.2k...s...:.}.eS.....h.?.4@.....*r..)..`.&..F..J...7.m. .Z+9\..0t..".(dE@.....&.S/>E.KX.. v..i.....O...@.\|2e..r%3n..%s...t.o7#.2.....h.0~P..U7..:x..O.H.h..G.....7a@..p.#K..%....9.k(#.>.....h.q4`.....~..j....~..@....B.zc:....X.h.. >t..kEZ1cu.....}.j,)w.....q[..g.J.s..^..+...{59..'D.q..=v...2.o6uL.....\|.T.....s.V....i..@%.....p2&..c."t..%{...t!e(mJ.....r.~,1K.(...=c....H.^..S. |

**C:\MSOCache\All Users\{90160000-0019-0409-0000-0000000FF1CE}-C\instructions_read_me.txt**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 1091 |
| Entropy (8bit): | 4.804750185554599 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | BA21D49977850F54961EDE73B7E9E480 |
| SHA1: | BD630B3DBE9D7139527C1FFDBB2161E7A9067AE0 |
| SHA-256: | 34757273C5E041F07B0352C51CFAB2998AB676F3A39BC0F16A1B4D68F3FAC4F8 |
| SHA-512: | 4BF9BE5F41F7258357E838BA94F0AA2B7F17D8FE3266174AAF123156B422C4FB72E4D3FD36DB7B2E3E9D13202202D2A6B0ECCA06EE2A2A043CE6AD27FFD751E2 |
| Malicious: | false |
| Preview: | ATTENTION!..Your network has been breached and all data was encrypted. Please contact us at:..https://bastad5huzwkepdixedg2gekg7jk22ato24zyllp6lnjx7wdtyctgvyd.onion/ .....Login ID: 26d371a9-efda-4e82-9989-01e292244d65.....*!* To access .onion websites download and install Tor Browser at:.... https://www.torproject.org/ (Tor Browser is not related to us)....*!* To restore all your PCs and get your network working again, follow these instructions:....- Any attempts to modify, decrypt or rename the files will lead to its fatal corruption. It doesn't matter, who are trying to do this, either it will be your IT guys or a recovery agency.....Please follow these simple rules to avoid data corruption:....- Do not modify, rename or delete files. Any attempts to modify, decrypt or rename the files will lead to its fatal corruption. ....- Do not hire a recovery company. They can't decrypt without the key. ..They also don't care about your business. They believe that they are ..good negotiator |

**C:\MSOCache\All Users\{90160000-001A-0409-0000-0000000FF1CE}-C\OutlkLR.cab**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 4009499 |
| Entropy (8bit): | **7.999809964829567** |
| Encrypted: | **true** |
| SSDEEP: | |
| MD5: | AF40559312DCC311014EC876740806E1 |
| SHA1: | DB7033F4303DE879A02F49CF874C684DDC7A99B7 |
| SHA-256: | 90DC15961EED94E4C3E263A7835C043E47449211911706D6462BAE4A80B223D5 |
| SHA-512: | 4AB7DF839831B7881377B89D4FDC125F29A603597AB426946C8B12A638DE5D2105761AE0D2D2D61BCFC27B92D4B425F08149DEC52A2E289FD61437A7FD114F8 |
| Malicious: | **true** |
| Preview: | 0..;...5V.."....+U.>...\u5P..j.a}.8.....@.....t#d..j.....6.....F.. .ACTIVITL.ICO_1033.....6.....F.. .ACTIVITS.ICO_1033.....F.. .ACTIVITY.CFG_1033.....F.. .APPT.C;..L..-5.C9"....oU.x....$d.H..).>L....H...PC5...P...@.$w7s.)._1033.@....&.....F.. .CNFNOT.CFG_1033.6....'.....F.. .CNFNOT.ICO_1033.R...+,.....F.. .CNFRES.CFG_1033.....}-.....F.. .CONFLICT.I>..L..-5.D9".1..oU.xNn...;z.E..D.':.....9.@J.....!.7I*..).L.ICO_1033.....x@.....F.. .CONTACTS.ICO_1033.o....L.....F.. .CURRENCY.GIF_1033.$....c.....F.. .CURRENCY.HTM_1033.....e.....F.. }..9..Wg.i~k.WN>\f.....:t4P..../A}.m..].n..x..%.....Dd].j8F.P .DELIMR.FAE_1033.%.....F.. .DISTLIST.CFG_1033.6.....F.. .DISTLSTL.ICO_1033.....F.. .DISTLSTS.ICO_1033.....^.}..X.2g9f.KQM).D.....ip4P.@.j.a..%....@..d.v...&..U..t..].j..F.. .DOCS.ICO_1033..D.....F.P .ENVELOPR.DLL_1033.F.....F.. .EXITEM.CFG_1033.6.....F.. .EXITEML.ICO_1033.....}..t...p..mg.[QG,.D.....aw4P...j.a...?.. |

**C:\MSOCache\All Users\{90160000-001A-0409-0000-0000000FF1CE}-C\OutlkLR.cab.7878kr5jx (copy)**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 4009499 |
| Entropy (8bit): | **7.999809964829567** |
| Encrypted: | **true** |
| SSDEEP: | |
| MD5: | AF40559312DCC311014EC876740806E1 |
| SHA1: | DB7033F4303DE879A02F49CF874C684DDC7A99B7 |
| SHA-256: | 90DC15961EED94E4C3E263A7835C043E47449211911706D6462BAE4A80B223D5 |
| SHA-512: | 4AB7DF839831B7881377B89D4FDC125F29A603597AB426946C8B12A638DE5D2105761AE0D2D2D61BCFC27B92D4B425F08149DEC52A2E289FD61437A7FD114F8 |
| Malicious: | **true** |

| | |
|---|---|
| Preview: | 0..;...5V.."....+U.>...\u5P..j.a}.8.....@.....t#d..j.....6.....F.. .ACTIVITL.ICO_1033.....6.....F.. .ACTIVITS.ICO_1033.....F.. .ACTIVITY.CFG_1033.....F.. .APPT.C;..L..-5.C9"....oU.x....$d.H..).>L....H...PC5...P...@.$w7s.)._1033.@....&.....F.. .CNFNOT.CFG_1033.6...'.....F.. .CNFNOT.ICO_1033.R...+,.....F.. .CNFR ES.CFG_1033.....}-.....F.. .CONFLICT.I>..L..-5.D9".1..oU.xNn...;z.E..D.':.....9.@J.....!.7I*..).L.ICO_1033.....x@.....F.. .CONTACTS.ICO_1033.o....L.....F.. .CURRENC Y.GIF_1033.$....c.....F.. .CURRENCY.HTM_1033.....e.....F.. }..9..Wg.i~k.WN>\f.....:t4P..../A}.m..].n..x..%.....Dd].j8F.P .DELIMR.FAE_1033.%.....F.. .DISTLIST.CFG_1 033.6.....F.. .DISTLSTL.ICO_1033.....F.. .DISTLSTS.ICO_1033.....^.}..X.2g9f.KQM).D.....ip4P.@.j.a..%....@..d.v...&..U..t..].j..F.. .DOCS.ICO_1033..D.....F.P .ENVELOPR.DLL_1033.F.....F.. .EXITEM.CFG_1033.6.....F.. .EXITEML.ICO_1033.....}..t...p..mg.[QG,.D.....aw4P...j.a...?.. |

**C:\MSOCache\All Users\{90160000-001A-0409-0000-0000000FF1CE}-C\OutlookMUI.msi**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 2830650 |
| Entropy (8bit): | 7.11015231966488 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | F71D0958366B6758D85E16E7865E3671 |
| SHA1: | 4C8BF2A2A983841D99F594CCC8F2DAE4E9F37E37 |
| SHA-256: | D01C376CE05ABB6990128878AF27F8BC1A91AB370001C9D33A66D77DDB23E19E |
| SHA-512: | E6F7C36690D0CA7FFCA92EC5D7837742F94DBC8629D6A736FF37555E352A50D7D67131A5672E5A1ABFBFCDADC35138F12AD58C62C8680E8B9279B33C7F3AFC 77 |
| Malicious: | false |
| Preview: | 6...h....Z=P%q}.k5fP.....R;....C.=.w..y1h,g\f.....9..oz...U.....&.6.U.....j...2\|..Zo....GKG.V. (.B6.....=..].;.]v.....&.6.U.....j...2\|..Zo....GKG.V.(.B6.....=..].;.]v..... ...../.....Z=P%q}.k5fP.....V;?1...C.=.w..{1h,f\f.....9..oj...U..... ...../.....Z=P%q}.k5fP.....V;?1...C.=.w..{1h,f\f.....9..oj...U...../ .....Z=P%q}.k5fP.....V;?1...C.=.w.. |

**C:\MSOCache\All Users\{90160000-001A-0409-0000-0000000FF1CE}-C\OutlookMUI.msi.7878kr5jx (copy)**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 2830650 |
| Entropy (8bit): | 7.11015231966488 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | F71D0958366B6758D85E16E7865E3671 |
| SHA1: | 4C8BF2A2A983841D99F594CCC8F2DAE4E9F37E37 |
| SHA-256: | D01C376CE05ABB6990128878AF27F8BC1A91AB370001C9D33A66D77DDB23E19E |
| SHA-512: | E6F7C36690D0CA7FFCA92EC5D7837742F94DBC8629D6A736FF37555E352A50D7D67131A5672E5A1ABFBFCDADC35138F12AD58C62C8680E8B9279B33C7F3AFC 77 |
| Malicious: | false |
| Preview: | 6...h....Z=P%q}.k5fP.....R;....C.=.w..y1h,g\f.....9..oz...U.....&.6.U.....j...2\|..Zo....GKG.V. (.B6.....=..].;.]v.....&.6.U.....j...2\|..Zo....GKG.V.(.B6.....=..].;.]v..... ...../.....Z=P%q}.k5fP.....V;?1...C.=.w..{1h,f\f.....9..oj...U..... ...../.....Z=P%q}.k5fP.....V;?1...C.=.w..{1h,f\f.....9..oj...U...../ .....Z=P%q}.k5fP.....V;?1...C.=.w.. |

**C:\MSOCache\All Users\{90160000-001A-0409-0000-0000000FF1CE}-C\OutlookMUI.xml**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 3151 |
| Entropy (8bit): | 7.8215922793625206 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | B023DEA1554917AA94B749155F17F146 |
| SHA1: | 95C2752986700E7272766F156D45410106EDB05C |
| SHA-256: | E122AAB020E8A0238B2965536903604CCE9150D4B177F065B9F47454E3FA8F35 |
| SHA-512: | C725D1EB46C7B68F295E1B66748916476CD0D1ED62D453C1D30010C7E8D424DD88A799582A76B0D6C7DEBF4DA81E78C4DD76121EA8FB0174273032E983BE50 9 |
| Malicious: | false |

| | |
|---|---|
| Preview: | .^%..7.A.%k....9........)..8...].}...a.%.<.....z.....8..E.v...t.2..z..m.... ...l..V.!.8.Y.i.z..*...)........4.....*-._2...0.5..S..X.....y.c.."...;.../x'..*...?..5.....>.....8...'.}.~0....md.X...2..%.J7.<br>[.H.O.N.p.W.*....u.....$B....<..r I...~.5..o..^...5./.I|.....!...2zC..-.....(...../.V....h.p..ta.O...38.<.Df.....lzl.);.....C.....W...{:^.$3.0..SZ.]....43.c..@.Z...)...}pl.A....5.....p...<br>...8..Z"m...e.*..X_.P..(3...oo.0...+.....&.Ao...>..3.....Qm..'A...|0.{..'.....MJ.....E...$./Ja..r...t..s....mB.....9..c=E..9e.'..&.....!.Kp...S.|.x.a.m..:.....e.....1<..v.A./k.'..y^<br>.c...._Z.!.Rp.V.[.H.{..I|..!...z..z....$.....1..5^...E8....c_.Y...A<./.S?.F...`...(IK..;...6.....}1....Uk..)|...pK.6..yx.Z...._;.9._>.....6.iF...?..2.....TN.....8..sL..8h.-..rY.]..4.."..}.U.E.-.....?<br>.V|...W..N.....2.....`..b.H..'I.1..pC.[...ws.a.C,.....O.{..\i..=..>.....6?.....)..&A...lG.1..5....._D.D./q.....,... |

**C:\MSOCache\All Users\{90160000-001A-0409-0000-0000000FF1CE}-C\OutlookMUI.xml.7878kr5jx (copy)**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 3151 |
| Entropy (8bit): | 7.8215922793625206 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | B023DEA1554917AA94B749155F17F146 |
| SHA1: | 95C2752986700E7272766F156D45410106EDB05C |
| SHA-256: | E122AAB020E8A0238B2965536903604CCE9150D4B177F065B9F47454E3FA8F35 |
| SHA-512: | C725D1EB46C7B68F295E1B66748916476CD0D1ED62D453C1D30010C7E8D424DD88A799582A76B0D6C7DEBF4DA81E78C4DD76121EA8FB0174273032E983BE509 |
| Malicious: | false |
| Preview: | .^%..7.A.%k....9........)..8...].}...a.%.<.....z.....8..E.v...t.2..z..m.... ...l..V.!.8.Y.i.z..*...)........4.....*-._2...0.5..S..X.....y.c.."...;.../x'..*...?..5.....>.....8...'.}.~0....md.X...2..%.J7.<br>[.H.O.N.p.W.*....u.....$B....<..r I...~.5..o..^...5./.I|.....!...2zC..-.....(...../.V....h.p..ta.O...38.<.Df.....lzl.);.....C.....W...{:^.$3.0..SZ.]....43.c..@.Z...)...}pl.A....5.....p...<br>...8..Z"m...e.*..X_.P..(3...oo.0...+.....&.Ao...>..3.....Qm..'A...|0.{..'.....MJ.....E...$./Ja..r...t..s....mB.....9..c=E..9e.'..&.....!.Kp...S.|.x.a.m..:.....e.....1<..v.A./k.'..y^<br>.c...._Z.!.Rp.V.[.H.{..I|..!...z..z....$.....1..5^...E8....c_.Y...A<./.S?.F...`...(IK..;...6.....}1....Uk..)|...pK.6..yx.Z...._;.9._>.....6.iF...?..2.....TN.....8..sL..8h.-..rY.]..4.."..}.U.E.-.....?<br>.V|...W..N.....2.....`..b.H..'I.1..pC.[...ws.a.C,.....O.{..\i..=..>.....6?.....)..&A...lG.1..5....._D.D./q.....,... |

**C:\MSOCache\All Users\{90160000-001A-0409-0000-0000000FF1CE}-C\Setup.xml**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 4184 |
| Entropy (8bit): | 7.855392584606368 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | A18649A849F7A26FC449D9A9DBA4BFFD |
| SHA1: | 05006DD9DB50314A981B2F7B5DB1D3960C35A7AF |
| SHA-256: | 0F6F2A09E0A780D653B45F1B2FBAF09A3A626C3214302F308C948E9665A677DA |
| SHA-512: | 2417766BD1E0B7FCFE8904BFE5D26261A0FF3D77339AC1B870C37014EEFFD2EFAF3A4EC0B2FD18E4106187E9394210CD887E673B0C15077A552DAD0DAAC7438 |
| Malicious: | false |
| Preview: | 0.S_...^..B4..)h.c...3K%..!.N.@-..>l..p.{.;;Z.2..(X!.H...F.:..o.|Y.m.I..[*...k .....p.L)..T.cv.3<.8.=...X.7...(].i..7#....{.Ft.s,J..R0...w.V....if.....v.Up..ib....0. .%.7..H"r.s.....|.C.../k...?.<br>..U!E+..hOs.J...y..-...X..a...-0(....OW^.qd..;. ..E.`t.K!^..Jt...Z!b....f..!!..V.UW.Ke..t.=...f....NQ"....>..?..:.Gk.."J..m4.../.G'...J...<..w.U4.b0..x...W\W....MRE.S...0....h.CY.s#...f/...`<br>.`....o,.Fk.6..S.t".(.t...y.....;.Kr....3.M.O}..Ip..\4..:.A5..;i..Yf..W.Sr..#7..9.t.i}..(....x.q4.f2.!....EA.[.W...{...y3X5..$A|.7)..W..D.`>..;.4...a.E...G6.Q#.(..!..z.YF.I....N(...q"P$..)A2<br>.Tx.2.ip.n<.(.t...x.8..?.{.V4.%..t..i.JG.N:O..Nf...{'Xc...#E-..1..H.Ht..x7..l.?...y.....d.Q#.yQ.3..,.BV._....N(....L=}..9K/.2".k.Id.u...).t. .s....(.w.]m....7..,.BA.V.T..I(...%dM$....M2..*.<br>.z.Pe.h!..n.9.Zz..n.....Vp. N....@.dy.S.^.....m*@...5.c..%....bi.m>....%...(...[!..Y<.+..2..~.BA..KU...V....z{1..>...Fd..O.Io.d>..%.3.FWQ.....E.Y$.yQ.9..c.{S._.O..o2...t)C....><br>P|..#....Os.m=.. |

**C:\MSOCache\All Users\{90160000-001A-0409-0000-0000000FF1CE}-C\Setup.xml.7878kr5jx (copy)**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 4184 |
| Entropy (8bit): | 7.855392584606368 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | A18649A849F7A26FC449D9A9DBA4BFFD |
| SHA1: | 05006DD9DB50314A981B2F7B5DB1D3960C35A7AF |
| SHA-256: | 0F6F2A09E0A780D653B45F1B2FBAF09A3A626C3214302F308C948E9665A677DA |
| SHA-512: | 2417766BD1E0B7FCFE8904BFE5D26261A0FF3D77339AC1B870C37014EEFFD2EFAF3A4EC0B2FD18E4106187E9394210CD887E673B0C15077A552DAD0DAAC7438 |
| Malicious: | false |

| | |
|---|---|
| Preview: | 0.S_...^..B4..)h.c...3K%..!.N.@-..>l..p.{.;:Z.2..(X!.H...F.:..o.|Y.m.I..[*...k .....p.L)..T.cv.3<.8.=...X.7...(].i..7#....{.Ft.s,J..R0...w.V....if.....v.Up..ib....0. .%.7..H"r.s.....|.C.../k...?. ..U!E+..hOs.J...y..-...X..a...-0(....OW^.qd..:. ..E.`t.K!^.Jt...Z!b....f..!!..V.UW.Ke..t.=...f....NQ"....>..?..:.Gk.."J..m4.../.G'...J...<..w.U4.b0..x...W\W....MRE.S...0....h.CY.s#...f/..` .`....o,.Fk.6..S.t".(.t...y.....;.Kr....3.M.O}..Ip..\4..:.A5..;i..Yf..W.Sr..#7..9.t.i}..(....x.q4.f2.!....EA.[.W...{...y3X5..$A\|.7)..W..D.`>..;.4...a.E...G6.Q#.(..!..z.YF.I....N(...q"P$..)A2 .Tx.2.ip.n<.(.t...x.8..?.{.V4.%..t..i.JG.N:O..Nf...{'Xc...#E-..1..H.Ht..x7..l.?...y.....d.Q#.yQ.3..,.BV._....N(....L=}..9K/.2".k.Id.u...).t. .s....(.w.]m....7..,.BA.V.T..I(...%dM$....M2..*. .z.Pe.h!..n.9.Zz..n.....Vp. N....@.dy.S.^.....m*@...5.c..%....bi.m>....%...(...[!..Y<.+..2..~.BA..KU...V....z{1..>...Fd..O.Io.d>..%.3.FWQ.....E.Y$.yQ.9..c.{S._.O..o2...t)C....> P\|..#....Os.m=.. |

**C:\MSOCache\All Users\{90160000-001A-0409-0000-0000000FF1CE}-C\instructions_read_me.txt**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 1091 |
| Entropy (8bit): | 4.804750185554599 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | BA21D49977850F54961EDE73B7E9E480 |
| SHA1: | BD630B3DBE9D7139527C1FFDBB2161E7A9067AE0 |
| SHA-256: | 34757273C5E041F07B0352C51CFAB2998AB676F3A39BC0F16A1B4D68F3FAC4F8 |
| SHA-512: | 4BF9BE5F41F7258357E838BA94F0AA2B7F17D8FE3266174AAF123156B422C4FB72E4D3FD36DB7B2E3E9D13202202D2A6B0ECCA06EE2A2A043CE6AD27FFD751E2 |
| Malicious: | false |
| Preview: | ATTENTION!..Your network has been breached and all data was encrypted. Please contact us at:..https://bastad5huzwkepdixedg2gekg7jk22ato24zyllp6lnjx7wdtyctgvyd.onion/ .....Login ID: 26d371a9-efda-4e82-9989-01e292244d65.....*!* To access .onion websites download and install Tor Browser at:.... https://www.torproject.org/ (Tor Browser is not related to us)....*!* To restore all your PCs and get your network working again, follow these instructions:....- Any attempts to modify, decrypt or rename the files will lead to its fatal corruption. It doesn't matter, who are trying to do this, either it will be your IT guys or a recovery agency.....Please follow these simple rules to avoid data corruption:.....- Do not modify, rename or delete files. Any attempts to modify, decrypt or rename the files will lead to its fatal corruption. ....- Do not hire a recovery company. They can't decrypt without the key. ..They also don't care about your business. They believe that they are ..good negotiator |

**C:\MSOCache\All Users\{90160000-001B-0409-0000-0000000FF1CE}-C\Setup.xml**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 3086 |
| Entropy (8bit): | 7.831666533764893 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | C9B2FF88EA40365BC09426D33A7D57E6 |
| SHA1: | F9E271BF6038E2081544A50250CFCD447DA16556 |
| SHA-256: | 490774D14098A359EB4E3CE59FEE932F376AE4159A7F5765260766C34F1A5E98 |
| SHA-512: | 89F550167EA4E201FC085D74FE9DE878F3198552B9AF98D129C5FBFDA585CC6ED704B70B5516F5513E45D0785B3B03596682A64B36A5723974E3161CC70D946D |
| Malicious: | false |
| Preview: | .`..`...VMmq.....V..<...n...`..-U.....g....='..4....*.?Zz*.%..8....V.Uu..{...^.....?..X(....);..1.!q.(B.V.....e.....j....Mcm....i....W..5..,....5..>Y.....r6.....}..Y...4..!dT.>..{.....SDZ..Y... A.....2>...;..1g.....8...<?=;.%Q.?.K..;Q.....4.....Ha-.....1....R..Z-.....=...9#....t...1.#.&..(..._...ciq)..V.....4...e..^.....:....P.+...L.....?.,6.p..9....U.Ix...D....i..3..U~...:..{.....% _=.d.....J"p..1..G....W@?=..J.....4...6...h.\|H.....:...H..u..Y.....`..3.....DQnk..Z....W..4.<:...j..N.....3....,".).*Z.'.....}..b.i...L@fz...W.....Q...'...&..2H.....%...2T.F.....x..+..i...F En=...]...O..+...n...u..K.....".-.dL...[...p..b.i....(..#...G....\.....&...o..\|H....&.....Oj.)V...[...u..0..n.....{z..j....T.....!...c..a.....v>...%R..{..).?...q.....j....vPck...b.....1...?...d..a.....$...0 P.....UAz..a.....UPkp...J..J..1...<...v..l...../.....).#.. .....D..:.....DHnp..].....z... ...i..k.... |

**C:\MSOCache\All Users\{90160000-001B-0409-0000-0000000FF1CE}-C\Setup.xml.7878kr5jx (copy)**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 3086 |
| Entropy (8bit): | 7.831666533764893 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | C9B2FF88EA40365BC09426D33A7D57E6 |
| SHA1: | F9E271BF6038E2081544A50250CFCD447DA16556 |
| SHA-256: | 490774D14098A359EB4E3CE59FEE932F376AE4159A7F5765260766C34F1A5E98 |
| SHA-512: | 89F550167EA4E201FC085D74FE9DE878F3198552B9AF98D129C5FBFDA585CC6ED704B70B5516F5513E45D0785B3B03596682A64B36A5723974E3161CC70D946D |
| Malicious: | false |
| Preview: | .`..`...VMmq.....V..<...n...`..-U.....g....='..4....*.?Zz*.%..8....V.Uu..{...^.....?..X(....);..1.!q.(B.V.....e.....j....Mcm....i....W..5..,....5..>Y.....r6.....}..Y...4..!dT.>..{.....SDZ..Y... A.....2>...;..1g.....8...<?=;.%Q.?.K..;Q.....4.....Ha-.....1....R..Z-.....=...9#....t...1.#.&..(..._...ciq)..V.....4...e..^.....:....P.+...L.....?.,6.p..9....U.Ix...D....i..3..U~...:..{.....% _=.d.....J"p..1..G....W@?=..J.....4...6...h.\|H.....:...H..u..Y.....`..3.....DQnk..Z....W..4.<:...j..N.....3....,".).*Z.'.....}..b.i...L@fz...W.....Q...'...&..2H.....%...2T.F.....x..+..i...F En=...]...O..+...n...u..K.....".-.dL...[...p..b.i....(..#...G....\.....&...o..\|H....&.....Oj.)V...[...u..0..n.....{z..j....T.....!...c..a.....v>...%R..{..).?...q.....j....vPck...b.....1...?...d..a.....$...0 P.....UAz..a.....UPkp...J..J..1...<...v..l...../.....).#.. .....D..:.....DHnp..].....z... ...i..k.... |

### C:\MSOCache\All Users\{90160000-001B-0409-0000-0000000FF1CE}-C\WordLR.cab

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 10080047 |
| Entropy (8bit): | **7.999121789035516** |
| Encrypted: | **true** |
| SSDEEP: | |
| MD5: | D59BABCAA7FFF0E85102F3EDFC9A5EA3 |
| SHA1: | C75F79E77636475DA4B5D8644BDEC046F56B7A91 |
| SHA-256: | E13475CF353DA2E26E5FFF9685C4599DB66004B89239668864251119A4015DCE |
| SHA-512: | 8539D401C529E7CC59D52A3877F285157BC7E004C222C85C7EC68EC5858AC3225A937B25473B29E56C95E86E9F45ADC2ED26CC8CC52E38F680D680AA7FF2B92 |
| Malicious: | **true** |
| Preview: | .-....*.^....3P.....N7...!2..%Fm..=.n..t..C..r)t/...K&....U..;.....F.. .ADJACENCYLETTER.DOTX_1033...6.....F.. .ADJACENCYREPORT.DOTX_1033.....:....F.. .ADJACENCYRESUME.DOTX_103.~.5.../.<...u.....@.c...aa..`.9....5MZ+*.`8.b.w..,K&.h..]..r.RTHECARYNEWSLETTER.DOTX_1033..`....C....F.. .APOTHECARYRESUME.DOTX_1033.Q/....F....F.. .BASICELEGANT.DOTX_1033../...)G....F.. .BA.7....z......k..'..[....xt..%.+....8XQ=X..RA..<!.F..y..8UTz2...G....F.. .BIBFORM.XML_1033../...:l....F.. .BWCAPITALIZED.DOTX_1033.....il....F.. .BWCLASSIC.DOTX_1033.64....I....F.. .BWNUMBER.:....r.....H....\|YN7.../(..f.>.q.>VV,D.c8>.4[..Qy.&...MZ..3.XNTERED.DOTX_1033.....+J....F.P .CHART.XLSRVINTL.DLL_1033.p....$M....F.. .CHRONOLOGICALLETTER.DOTX_1033.....N....F.. .CHRONOLO.7....o..q..\|...%.#}7}.. ...%BmF.2.Z.A8Z..BN..;[.V.{...$U..q.....F.. .DEFAULT.DOTX_1033..8.wqO....F.. .DOCUMENT_PARTS.DOT_1033.6...>.....F.. .ESSENTIALLETTER.DOTX_1033....t.....F.. .ESSE.*....o..n..\|...%.#}7.. n.)%BmG...Z.G' |

### C:\MSOCache\All Users\{90160000-001B-0409-0000-0000000FF1CE}-C\WordLR.cab.7878kr5jx (copy)

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 10080047 |
| Entropy (8bit): | **7.999121789035516** |
| Encrypted: | **true** |
| SSDEEP: | |
| MD5: | D59BABCAA7FFF0E85102F3EDFC9A5EA3 |
| SHA1: | C75F79E77636475DA4B5D8644BDEC046F56B7A91 |
| SHA-256: | E13475CF353DA2E26E5FFF9685C4599DB66004B89239668864251119A4015DCE |
| SHA-512: | 8539D401C529E7CC59D52A3877F285157BC7E004C222C85C7EC68EC5858AC3225A937B25473B29E56C95E86E9F45ADC2ED26CC8CC52E38F680D680AA7FF2B92 |
| Malicious: | **true** |
| Preview: | .-....*.^....3P.....N7...!2..%Fm..=.n..t..C..r)t/...K&....U..;.....F.. .ADJACENCYLETTER.DOTX_1033...6.....F.. .ADJACENCYREPORT.DOTX_1033.....:....F.. .ADJACENCYRESUME.DOTX_103.~.5.../.<...u.....@.c...aa..`.9....5MZ+*.`8.b.w..,K&.h..]..r.RTHECARYNEWSLETTER.DOTX_1033..`....C....F.. .APOTHECARYRESUME.DOTX_1033.Q/....F....F.. .BASICELEGANT.DOTX_1033../...)G....F.. .BA.7....z......k..'..[....xt..%.+....8XQ=X..RA..<!.F..y..8UTz2...G....F.. .BIBFORM.XML_1033../...:l....F.. .BWCAPITALIZED.DOTX_1033.....il....F.. .BWCLASSIC.DOTX_1033.64....I....F.. .BWNUMBER.:....r.....H....\|YN7.../(..f.>.q.>VV,D.c8>.4[..Qy.&...MZ..3.XNTERED.DOTX_1033.....+J....F.P .CHART.XLSRVINTL.DLL_1033.p....$M....F.. .CHRONOLOGICALLETTER.DOTX_1033.....N....F.. .CHRONOLO.7....o..q..\|...%.#}7}.. ...%BmF.2.Z.A8Z..BN..;[.V.{...$U..q.....F.. .DEFAULT.DOTX_1033..8.wqO....F.. .DOCUMENT_PARTS.DOT_1033.6...>.....F.. .ESSENTIALLETTER.DOTX_1033....t.....F.. .ESSE.*....o..n..\|...%.#}7.. n.)%BmG...Z.G' |

### C:\MSOCache\All Users\{90160000-001B-0409-0000-0000000FF1CE}-C\WordMUI.msi

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 2404666 |
| Entropy (8bit): | 7.119635899619627 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | 6CA448FA970E0E1AAA1786539B0C4A74 |
| SHA1: | 4CDEA6817C72421B21A0FEF5CCD8584370FAB86F |
| SHA-256: | B29D0C4067E7322E5F60C21007011B549D1EC8B499A5D51CBBB9C696CE4C18B3 |
| SHA-512: | 07B72FD03356C222C9E04ADB22B295CB856AEC8069DA7BF64CFD2863FC1BBF17E3C70B1A90FE898A180A2B0BE4E137F68AFD48A3D2AE6E46FE18FCD872F34D57 |
| Malicious: | false |
| Preview: | ^.`.b...x ...`...$.ch'Q.....T...(/...w9.t*v..Q.N.....+.-.....q>..<.....7.tK.x.....%<..:...../..zSI..8..`w...fEiy.vR].....q>..<.....7.tK.x.....%<..:...../..zSI..8..`w...fEiy.vR].....q..p.#x ...`...$.ch'Q4...T....T...(/...w9.t*v..Q.N.....+.-.....q..p.#x ...`...$.ch'Q4...T....T...(/...w9.t*v..Q.N.....+.-.....q..p.#x ...`...$.ch'Q4...T....T...(/. |

| C:\MSOCache\All Users\{90160000-001B-0409-0000-0000000FF1CE}-C\WordMUI.msi.7878kr5jx (copy) | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 2404666 |
| Entropy (8bit): | 7.119635899619627 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | 6CA448FA970E0E1AAA1786539B0C4A74 |
| SHA1: | 4CDEA6817C72421B21A0FEF5CCD8584370FAB86F |
| SHA-256: | B29D0C4067E7322E5F60C21007011B549D1EC8B499A5D51CBBB9C696CE4C18B3 |
| SHA-512: | 07B72FD03356C222C9E04ADB22B295CB856AEC8069DA7BF64CFD2863FC1BBF17E3C70B1A90FE898A180A2B0BE4E137F68AFD48A3D2AE6E46FE18FCD872F34D57 |
| Malicious: | false |
| Preview: | ^.`.b...x ...`...$.ch'Q.....T...(/...w9.t*v..Q.N.....+.-.....q>..<.....7.tK.x.....%<..:...../..zSl..8..`w...fEiy.vR].....q>..<.....7.tK.x.....%<..:...../..zSl..8..`w...fEiy.vR].....q..p.#x ...`...$.ch'Q4...T....T...(/...w9.t*v..Q.N.....+.-.....q..p.#x ...`...$.ch'Q4...T....T...(/...w9.t*v..Q.N.....+.-.....q..p.#x ...`...$.ch'Q4...T....T...(/. |

| C:\MSOCache\All Users\{90160000-001B-0409-0000-0000000FF1CE}-C\WordMUI.xml | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 2422 |
| Entropy (8bit): | 7.806574624046372 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | ACCA347585DBBA663DB4760FCA500809 |
| SHA1: | 78043BA2DD4FA5AFC4F9C63654DCC3828453EB29 |
| SHA-256: | E6E998E33490E5EF557E19EE7B8782B757FA4279EF87ED3ED71D7DE48E41D143 |
| SHA-512: | 8B1E589C76B9EEF51BAECD19F70A52E687C8F50F71D73ABBC194600741DEE129BF596755389C4ED1F28705DE807740F190FB4D6C99148F3C5A5BD7C66133EA88 |
| Malicious: | false |
| Preview: | ..4..)9.....F.B..r!8...*s....dWT>%..h....._.B..U.".O.....n2.....H.:...b58..5.....n..$l..*.....t.^'.9.H.8..}.....o.&.....=.\...'"7...tX.....U.-*(..0....3.].^....q.D...\...n.^p.....F.....*....?WA"...C.....i.x..".M.n...~.....s;.....&... |c..+y....O2'nq.W.....k.Y%...c."..c.....o.....4... <.....|.....:7.~).....6.".y6.C.X./..G.....n...._..4.6....)e..4 .....>*..q.....i.C..F.g.b...e.....,.....j....cK....IGN-4..B....1.X.j6.J.0.&.....t..oe..[.V.C..bt.....`.....T..os._...|.).8}.X.8.7.U....>.K89..Z.H.S...&"9...ae....sPZ.....o.V.a....h.{..P.....E/9.....$.C..r.9...a-....F#ln.....6.9.b$...@.d..]....S..p.....~...!7...&=...g..lY..... .r.k .H.f.c.....P.e/(.....:...(!....s....g.N3$..k....&.i.0^.a.O.v..T.....!.O3.....<0:...p.....vGN--..U..._...2....f.E..x....8.Y.2.....Q..XMj.."i...sPZ.....o.L.\....{.s.T...h..l~.....F.B..ctn...I.....k..N...+ |

| C:\MSOCache\All Users\{90160000-001B-0409-0000-0000000FF1CE}-C\WordMUI.xml.7878kr5jx (copy) | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 2422 |
| Entropy (8bit): | 7.806574624046372 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | ACCA347585DBBA663DB4760FCA500809 |
| SHA1: | 78043BA2DD4FA5AFC4F9C63654DCC3828453EB29 |
| SHA-256: | E6E998E33490E5EF557E19EE7B8782B757FA4279EF87ED3ED71D7DE48E41D143 |
| SHA-512: | 8B1E589C76B9EEF51BAECD19F70A52E687C8F50F71D73ABBC194600741DEE129BF596755389C4ED1F28705DE807740F190FB4D6C99148F3C5A5BD7C66133EA88 |
| Malicious: | false |
| Preview: | ..4..)9.....F.B..r!8...*s....dWT>%..h....._.B..U.".O.....n2.....H.:...b58..5.....n..$l..*.....t.^'.9.H.8..}.....o.&.....=.\...'"7...tX.....U.-*(..0....3.].^....q.D...\...n.^p.....F.....*....?WA"...C.....i.x..".M.n...~.....s;.....&... |c..+y....O2'nq.W.....k.Y%...c."..c.....o.....4... <.....|.....:7.~).....6.".y6.C.X./..G.....n...._..4.6....)e..4 .....>*..q.....i.C..F.g.b...e.....,.....j....cK....IGN-4..B....1.X.j6.J.0.&.....t..oe..[.V.C..bt.....`.....T..os._...|.).8}.X.8.7.U....>.K89..Z.H.S...&"9...ae....sPZ.....o.V.a....h.{..P.....E/9.....$.C..r.9...a-....F#ln.....6.9.b$...@.d..]....S..p.....~...!7...&=...g..lY..... .r.k .H.f.c.....P.e/(.....:...(!....s....g.N3$..k....&.i.0^.a.O.v..T.....!.O3.....<0:...p.....vGN--..U..._...2....f.E..x....8.Y.2.....Q..XMj.."i...sPZ.....o.L.\....{.s.T...h..l~.....F.B..ctn...I.....k..N...+ |

| C:\MSOCache\All Users\{90160000-001B-0409-0000-0000000FF1CE}-C\instructions_read_me.txt | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | ASCII text, with CRLF line terminators |

| | |
|---|---|
| Category: | dropped |
| Size (bytes): | 1091 |
| Entropy (8bit): | 4.804750185554599 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | BA21D49977850F54961EDE73B7E9E480 |
| SHA1: | BD630B3DBE9D7139527C1FFDBB2161E7A9067AE0 |
| SHA-256: | 34757273C5E041F07B0352C51CFAB2998AB676F3A39BC0F16A1B4D68F3FAC4F8 |
| SHA-512: | 4BF9BE5F41F7258357E838BA94F0AA2B7F17D8FE3266174AAF123156B422C4FB72E4D3FD36DB7B2E3E9D13202202D2A6B0ECCA06EE2A2A043CE6AD27FFD751E2 |
| Malicious: | **true** |
| Preview: | ATTENTION!..Your network has been breached and all data was encrypted. Please contact us at:..https://bastad5huzwkepdixedg2gekg7jk22ato24zyllp6lnjx7wdtyctgvyd.onion/ .....Login ID: 26d371a9-efda-4e82-9989-01e292244d65.....*!* To access .onion websites download and install Tor Browser at:.... https://www.torproject.org/ (Tor Browser is not related to us)....*!* To restore all your PCs and get your network working again, follow these instructions:....- Any attempts to modify, decrypt or rename the files will lead to its fatal corruption. It doesn't matter, who are trying to do this, either it will be your IT guys or a recovery agency.....Please follow these simple rules to avoid data corruption:....- Do not modify, rename or delete files. Any attempts to modify, decrypt or rename the files will lead to its fatal corruption. ....- Do not hire a recovery company. They can't decrypt without the key. ..They also don't care about your business. They believe that they are ..good negotiator |

**C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Proofing.msi**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 1061178 |
| Entropy (8bit): | 7.067253408762128 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | 04EDED780CED2D690A2AED977FD9E877 |
| SHA1: | FB9C32FFDBB75F5D1978EF18FFAE439D427E6784 |
| SHA-256: | 73E1BBC11EE3D2E1D11CBE912540F83892F64CD561F2AA6192BDC0181A062862 |
| SHA-512: | BA600D0EA065262F132EA9DB49453A1029C635062F8C97DD348ACF10DD295C80A40E846815743BFB113AF6F69B051DDC8E59F347E71E60378FA4EBB61CF4D99E |
| Malicious: | false |
| Preview: | ....@9..e.7.".....[...Zp..g_.|i....=.....BWT)1....pM..#a.....w~....I...|.W.H.~..~I...|.[.4.O.z~g!KDt.t.....1.,:..OV.8.....w~....I...|.W.H.~..~I...|.[.4.O.z~g!KDt.t.....1.,:..OV.8.....|8...Be.7.".....[...Zp..c_..e....=.....BWU)1....pM..#c.....|8...Be.7.".....[...Zp..c_..e....=.....BWU)1....pM..#c.....|8...Be.7.".....[...Zp..c_..e....=... |

**C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Proofing.msi.7878kr5jx (copy)**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 1061178 |
| Entropy (8bit): | 7.067253408762128 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | 04EDED780CED2D690A2AED977FD9E877 |
| SHA1: | FB9C32FFDBB75F5D1978EF18FFAE439D427E6784 |
| SHA-256: | 73E1BBC11EE3D2E1D11CBE912540F83892F64CD561F2AA6192BDC0181A062862 |
| SHA-512: | BA600D0EA065262F132EA9DB49453A1029C635062F8C97DD348ACF10DD295C80A40E846815743BFB113AF6F69B051DDC8E59F347E71E60378FA4EBB61CF4D99E |
| Malicious: | false |
| Preview: | ....@9..e.7.".....[...Zp..g_.|i....=.....BWT)1....pM..#a.....w~....I...|.W.H.~..~I...|.[.4.O.z~g!KDt.t.....1.,:..OV.8.....w~....I...|.W.H.~..~I...|.[.4.O.z~g!KDt.t.....1.,:..OV.8.....|8...Be.7.".....[...Zp..c_..e....=.....BWU)1....pM..#c.....|8...Be.7.".....[...Zp..c_..e....=.....BWU)1....pM..#c.....|8...Be.7.".....[...Zp..c_..e....=... |

**C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Proofing.xml**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | OpenPGP Secret Key |
| Category: | dropped |
| Size (bytes): | 1338 |

| | |
|---|---|
| Entropy (8bit): | 7.599982589525571 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | A31FD34218D861A805110097508FD454 |
| SHA1: | 75AB217EADCBBACF0B1A61796D90885B5CAB8CB8 |
| SHA-256: | F6B3A0FEA45E7997BAA14B807155FC01D89625C717C319F01CCFE31AE00515DC |
| SHA-512: | 429645A495687C4CFAF43A789860D1A23907C52F126AAC86551C81A75AA781E939D541A4B484474F0D1CD3B6E17D2E2239A5391BCB7D97B243799DA7D94A442F |
| Malicious: | false |
| Preview: | .I..Oo..o.....Z\....R...Z....E....S...~...9x3..B?d.D..*.;.w...Q....."....r.....3....q...'.#..4YEd~.#....v9.sx..E..."/.....Ys....[....L....M...C....\|..8<\.Z..!.e..U..'/.. ....."(.....a.....q. ...!....X.....[Ia%..(....g...z..&.....@-...9]....F.....6....^.....SO.b....=.....j..-.....K.....O....t....K.....n....?...7LM.b.....[*..R./F....:.....O.....U...."T..\\]]p0....n..p..kM...H.... .....P.....U..J.....Y.... G..H9.d ..V.c..`b..-..GE...HL.....1p....o.....\.....\kK..@+..b...'..M(.*z..UD...(.....O.....=.....0....OG>u.F.<...m.}%..z.....;Q...K.....Vj<... \|\7...o....W:..=..JW.....V....O.....6...A+._...Z.#..L!..{..H.....P....1....=.....3....1...Q@Jo2....#..M;.$q...3....X?.....D...5.....$....zZ3\|....\|..)F.d[.....q@.... .....{....$.....[..J....L+.p...o.o..W&.%O..W<.....T....H..v.. |

**C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Proofing.xml.7878kr5jx (copy)**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | OpenPGP Secret Key |
| Category: | dropped |
| Size (bytes): | 1338 |
| Entropy (8bit): | 7.599982589525571 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | A31FD34218D861A805110097508FD454 |
| SHA1: | 75AB217EADCBBACF0B1A61796D90885B5CAB8CB8 |
| SHA-256: | F6B3A0FEA45E7997BAA14B807155FC01D89625C717C319F01CCFE31AE00515DC |
| SHA-512: | 429645A495687C4CFAF43A789860D1A23907C52F126AAC86551C81A75AA781E939D541A4B484474F0D1CD3B6E17D2E2239A5391BCB7D97B243799DA7D94A442F |
| Malicious: | false |
| Preview: | .I..Oo..o.....Z\....R...Z....E....S...~...9x3..B?d.D..*.;.w...Q....."....r.....3....q...'.#..4YEd~.#....v9.sx..E..."/.....Ys....[....L....M...C....\|..8<\.Z..!.e..U..'/.. ....."(.....a.....q. ...!....X.....[Ia%..(....g...z..&.....@-...9]....F.....6....^.....SO.b....=.....j..-.....K.....O....t....K.....n....?...7LM.b.....[*..R./F....:.....O.....U...."T..\\]]p0....n..p..kM...H.... .....P.....U..J.....Y.... G..H9.d ..V.c..`b..-..GE...HL.....1p....o.....\.....\kK..@+..b...'..M(.*z..UD...(.....O.....=.....0....OG>u.F.<...m.}%..z.....;Q...K.....Vj<... \|\7...o....W:..=..JW.....V....O.....6...A+._...Z.#..L!..{..H.....P....1....=.....3....1...Q@Jo2....#..M;.$q...3....X?.....D...5.....$....zZ3\|....\|..)F.d[.....q@.... .....{....$.....[..J....L+.p...o.o..W&.%O..W<.....T....H..v.. |

**C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Setup.xml**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 6381 |
| Entropy (8bit): | 6.964907921570851 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | 49C7340EEEF938604BD8DDB3A48A1F94 |
| SHA1: | 57F7C203078D69C9D0237ECF12AC4748450B473E |
| SHA-256: | B3727301DA790137B597826902BC07FB9C389BC2490757EA7BA0A821083A9654 |
| SHA-512: | 070CD78169FF39F1A9D8FB708FC1105CB0BF91EE806DF3F4AED49487D27C483E4715320FCF8CF07009ECCAB5B911391698D064BE3CE5CCCD3A2D503DA18C5520 |
| Malicious: | false |
| Preview: | ..bh.\|...0..S..j+o...F...6...S.mZ.v."...8.>.....o..R.z....nUrh4zfOhAXu2dmPJCbN9UmOU+lUqcy4R0mUOC0tbze4r4JRogbF600syyUPsEf4+wSe0yKVn6avR88AlLKNSsNyibq ZG/SZfQx+D8fsIGp3+vGZkZsVMjBJhgpEQP4F..Y}..=.....Vck+....f\..S...S.qh.G.3.....L..u..bq..w..M..../GBoAyiIbQA29X2CrOi7d22vp8rl43O5cUUSn2D3IeOcVqZ2Wk sQj9FraBEpLUmo/VBfAaM2Eesg2kfui5gmljnP/aTRO6mLqaW2/sRocxpPo3c6ZPuXulqvEL58LEg..o}..y....._..~7b9...R:R.&...-.;..[.z.....-..EX.k..]..."AddOn" Keywor d="Proofing" Culture="en-us">...<Option Id="AlwaysInstalled" DefaultState="Local" DisallowAbsent="yes" DisallowAdv..nl..7..*..&..[?gr.....DQ..... ..2.#.....-..MW..\. .h....faultState="Local" DisallowAbsent="yes" DisallowAdvertise="yes" Hidden="yes"/>...<Option Id="ProductFiles" DefaultState="Local" ..id..e...*....F?zm....C...\|....&..F .p.j.x.....IY..Q..+....EDFiles" DefaultState="Local" DisallowAbsent="no" DisallowAdvertise="no">.....<Option Id="ProofingTools" DefaultState="Local" Di..vi..K...7..L...zM &...M...}....rG... |

**C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Setup.xml.7878kr5jx (copy)**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 6381 |
| Entropy (8bit): | 6.964907921570851 |
| Encrypted: | false |
| SSDEEP: | |

| | |
|---|---|
| MD5: | 49C7340EEEF938604BD8DDB3A48A1F94 |
| SHA1: | 57F7C203078D69C9D0237ECF12AC4748450B473E |
| SHA-256: | B3727301DA790137B597826902BC07FB9C389BC2490757EA7BA0A821083A9654 |
| SHA-512: | 070CD78169FF39F1A9D8FB708FC1105CB0BF91EE806DF3F4AED49487D27C483E4715320FCF8CF07009ECCAB5B911391698D064BE3CE5CCCD3A2D503DA18C5<br>20 |
| Malicious: | false |
| Preview: | ..bh.\|...0..S..j+o...F...6...S.mZ.v."...8.>.....o..R.z....nUrh4zfOhAXu2dmPJCbN9UmOU+lUqcy4R0mUOC0tbze4r4JRogbF600syyUPsEf4+wSe0yKVn6avR88AlLKNSsNyibq<br>ZG/SZfQx+D8fsIGp3+vGZkZsVMjBJhgpEQP4F..Y}..=.....Vck+....f\..S...S.qh.G.3.....L..u..bq..w..M..../GBoAyiIbQA29X2CrOi7d22vp8rl43O5cUUSn2D3IeOcVqZ2Wk<br>sQj9FraBEpLUmo/VBfAaM2Esg2kfui5gmljnP/aTRO6mLqaW2/sRocxpPo3c6ZPuXulqvEL58LEg..o}..y....._..~7b9...R:R.&...-.;..[.z.....-..EX.k..]..."AddOn" Keywor<br>d="Proofing" Culture="en-us">...<Option Id="AlwaysInstalled" DefaultState="Local" DisallowAbsent="yes" DisallowAdv..nl..7..*..&..[?gr.....DQ..... ..2.#.....-..MW..\.<br>.h....faultState="Local" DisallowAbsent="yes" DisallowAdvertise="yes" Hidden="yes"/>...<Option Id="ProductFiles" DefaultState="Local" ..id..e...*....F?zm....C...\|....&..F<br>.p.j.x.....IY..Q..+....EDFiles" DefaultState="Local" DisallowAbsent="no" DisallowAdvertise="no">.....<Option Id="ProofingTools" DefaultState="Local" Di..vi..K...7..L...zM<br>&...M...}....rG... |

### C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\instructions_read_me.txt

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 1091 |
| Entropy (8bit): | 4.804750185554599 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | BA21D49977850F54961EDE73B7E9E480 |
| SHA1: | BD630B3DBE9D7139527C1FFDBB2161E7A9067AE0 |
| SHA-256: | 34757273C5E041F07B0352C51CFAB2998AB676F3A39BC0F16A1B4D68F3FAC4F8 |
| SHA-512: | 4BF9BE5F41F7258357E838BA94F0AA2B7F17D8FE3266174AAF123156B422C4FB72E4D3FD36DB7B2E3E9D13202202D2A6B0ECCA06EE2A2A043CE6AD27FFD751<br>E2 |
| Malicious: | **true** |
| Preview: | ATTENTION!..Your network has been breached and all data was encrypted. Please contact us at:..https://bastad5huzwkepdixedg2gekg7jk22ato24zyllp6lnjx7wdtyctgvyd.o<br>nion/ .....Login ID: 26d371a9-efda-4e82-9989-01e292244d65.....*!* To access .onion websites download and install Tor Browser at:.... https://www.torproject.org/ (Tor<br>Browser is not related to us)....*!* To restore all your PCs and get your network working again, follow these instructions:....- Any attempts to modify, decrypt or rename the<br>files will lead to its fatal corruption. It doesn't matter, who are trying to do this, either it will be your IT guys or a recovery agency.....Please follow these simple rules to avoid<br>data corruption:....- Do not modify, rename or delete files. Any attempts to modify, decrypt or rename the files will lead to its fatal corruption. ....- Do not hire a recovery<br>company. They can't decrypt without the key. ..They also don't care about your business. They believe that they are ..good negotiator |

### C:\MSOCache\All Users\{90160000-0044-0409-0000-0000000FF1CE}-C\InfLR.cab

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 3911964 |
| Entropy (8bit): | **7.999825451372041** |
| Encrypted: | **true** |
| SSDEEP: | |
| MD5: | A25A3023942AE336CC7219D5B8975753 |
| SHA1: | 57BD302252A7535D2E163CACFBB9A83A83748582 |
| SHA-256: | 59614002E536157338933E3EA0FE3B8292322C648780514CCA045B225110DA9D |
| SHA-512: | DA8EE68B9F0F5BDEF4713354217C32065C42933549FE46F98B4AFAA51365423AE4D1E0BC0C6478C706108564D20670E28377EC27810F36E19746294BC023274D |
| Malicious: | **true** |
| Preview: | ....u[(#..2)'..OIF..8.;.6t-([.../w... .$.f.h.).s.TC.....`.Rg....0.....bd.....B.....FPO .CONTACTPICKERINTL.DLL_1033.....B.....F.. .INFOPATH.HXS_1033.....F..<br>.INFOPAT..9u`{:.8.....F..7.;.5.o,P-.\a1DB.t.{.).Fb..,.Yp.....`..R.F.. .INFOPATH_F_COL.HXK_1033.q.....F.. .INFOPATH_K_COL.HXK_1033..2..q.....F.. .IN<br>FOPATHEDITOR.HXS_1033.....i3.....F.. .INF....=.lj-.[vd..a].E.....5.)(K.../u...$.../..e..',.....NR..81033.r.....F.. .INFOPATHEDITOR_F_COL.HXK_1033.q.....F..<br>.INFOPATHEDITOR_K_COL.HXK_1033.....F.. .IPATHDSG.XML_10..'W(...*`.K.f..h.w.b'y..@.J.G8!...'...}*X..mX.....2^..*L_1033..7..@.....F.. .IPXMLPOL.XML_103<br>3.".4..T!....F.. .XMLSDK5.CHM_1033.L...d...[.... .&uU.P..#Q.f...O.j..!!"..*.rv..TZ;).v.i....+Q....+=#o}6_Q).....M../.....+._.?....}.._...c..m.S.....aH..l.r_..;..nT.h.:.-.}..N.V^...xF.g..<br>.....'..}..(..@.....dn..HD.....&.....5 ..U.....c..\|".....8.._...^..?.h&.c`{.{."cc@=..T.$.a....3...6!_.....s |

### C:\MSOCache\All Users\{90160000-0044-0409-0000-0000000FF1CE}-C\InfLR.cab.7878kr5jx (copy)

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 3911964 |
| Entropy (8bit): | **7.999825451372041** |
| Encrypted: | **true** |
| SSDEEP: | |
| MD5: | A25A3023942AE336CC7219D5B8975753 |

| | |
|---|---|
| SHA1: | 57BD302252A7535D2E163CACFBB9A83A83748582 |
| SHA-256: | 59614002E536157338933E3EA0FE3B8292322C648780514CCA045B225110DA9D |
| SHA-512: | DA8EE68B9F0F5BDEF4713354217C32065C42933549FE46F98B4AFAA51365423AE4D1E0BC0C6478C706108564D20670E28377EC27810F36E19746294BC023274D |
| Malicious: | **true** |
| Preview: | ....u[(#..2)'..OIF..8.;.6t-([.../w... .$.f.h.).s.TC.....`.Rg....0.....bd.....B.....FPO .CONTACTPICKERINTL.DLL_1033.....B.....F.. .INFOPATH.HXS_1033.....F.. .INFOPAT..9u`{:.8.....F..7.;.5.o,P-.\a1DB.t.{.).Fb..,.Yp.....`..R.F.. .INFOPATH_F_COL.HXK_1033.q.....F.. .INFOPATH_K_COL.HXK_1033..2..q.....F.. .IN FOPATHEDITOR.HXS_1033.....i3.....F.. .INF....=.lj-.[vd..a].E.....5.)(K.../u...$.../..e..',.....NR..81033.r.....F.. .INFOPATHEDITOR_F_COL.HXK_1033.q.....F.. .INFOPATHEDITOR_K_COL.HXK_1033.....F.. .IPATHDSG.XML_10..'W(...*`.K.f..h.w.b'y..@.J.G8!...'...}*X..mX.....2^..*L_1033..7..@.....F.. .IPXMLPOL.XML_103 3.".4..T!....F.. .XMLSDK5.CHM_1033.L...d...[.... .&uU.P..#Q.f...O.j..!!"..*.rv..TZ;).v.i....+Q....+=#o}6_Q).....M../.....+._.?....}..._...c..m.S.....aH..l.r_..;..nT.h.:.-.}..N.V^...xF.g.. .....'..}..(..@.....dn..HD.....&.....5 ..U.....c..|".....8.._...^..?.h&.c`{.{."cc@=..T.$.a....3...6!_.....s |

**C:\MSOCache\All Users\{90160000-0044-0409-0000-0000000FF1CE}-C\InfoPathMUI.msi**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 2384186 |
| Entropy (8bit): | 7.107434701094617 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | 374FD4630788C034DAD3010C111BC324 |
| SHA1: | A49D41FA65ACD16D8707A193C40499BB9076E628 |
| SHA-256: | 310F8C7C806E26254F0CE6D06E1AFF6FE78EBEDF300DF4BB4606E83097D5454A |
| SHA-512: | 558CAEE1C3FA5A9313B9270B341C611661B805A12E8FB5694042F53508FA0205B2102D232D458873F5FF7D82CC814B6FEE27674BF62908F4E7571726FC58D1BA |
| Malicious: | false |
| Preview: | uv..`.....HC...4..B..*.....8q..0yU .zE.@..0<-\|.U.....\|.....ZF..>Q.'...8@.G.+st.:4c.J<...>m).e..X... .....a.Me.J,.....ZF..>Q.'...8@.G.+st.:4c.J<...>m).e..X... .....a.Me.J,.....Z..HC...4..B.....:.....8q..0{U .{E.@..0<-\|.U.....\|.....Z..HC...4..B.....:.....8q..0{U .{E.@..0<-\|.U.....\|.....Z..H C...4..B.....:.....8q..0 |

**C:\MSOCache\All Users\{90160000-0044-0409-0000-0000000FF1CE}-C\InfoPathMUI.msi.7878kr5jx (copy)**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 2384186 |
| Entropy (8bit): | 7.107434701094617 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | 374FD4630788C034DAD3010C111BC324 |
| SHA1: | A49D41FA65ACD16D8707A193C40499BB9076E628 |
| SHA-256: | 310F8C7C806E26254F0CE6D06E1AFF6FE78EBEDF300DF4BB4606E83097D5454A |
| SHA-512: | 558CAEE1C3FA5A9313B9270B341C611661B805A12E8FB5694042F53508FA0205B2102D232D458873F5FF7D82CC814B6FEE27674BF62908F4E7571726FC58D1BA |
| Malicious: | false |
| Preview: | uv..`.....HC...4..B..*.....8q..0yU .zE.@..0<-\|.U.....\|.....ZF..>Q.'...8@.G.+st.:4c.J<...>m).e..X... .....a.Me.J,.....ZF..>Q.'...8@.G.+st.:4c.J<...>m).e..X... .....a.Me.J,.....Z..HC...4..B.....:.....8q..0{U .{E.@..0<-\|.U.....\|.....Z..HC...4..B.....:.....8q..0{U .{E.@..0<-\|.U.....\|.....Z..H C...4..B.....:.....8q..0 |

**C:\MSOCache\All Users\{90160000-0044-0409-0000-0000000FF1CE}-C\InfoPathMUI.xml**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 1544 |
| Entropy (8bit): | 7.668723320369599 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | 9DF962CDFED624563B86C5CD9CD62BAF |
| SHA1: | 41894921C4F363006C91AFAD0C9DEC063381EFC9 |
| SHA-256: | 976DED3528CC01C156336B8A51B09C3C4EBB156A71148B32A542EB7184A02AE7 |
| SHA-512: | 12D047AE8520FD3944F2DD25234D782C7D554DA3F528D9C87505BE7E1735817D249E0641440C62EE448AB2A1D52F02FB6A622243872F61B433DB2F0C9D36487E |
| Malicious: | false |

| | |
|---|---|
| Preview: | @.....[Y.HVY.k..F.C.m$%.J.c'.-.k:.a89l.*7.....:.5.....,.\|^$.....p..y..1..=./.y..+h._4.^.~}^vJE1>&E....=...w.K...b..[&H.....Fs..v}.$...J.\|>4.O.a..m.bsz07r.lLF....*....}.{....8.D.....Z.vR P.....g.t.V.`..?..0:.}..x4;;....f.....@.F..30.h#.....Uu.~\Y.?.2.6.g-m.x.u/.i.5Uf"vBvBwt..l...E.M....<8._^.....[..Px`.g..C.%.J...t.[..~.>M..q~4,$N....4...u.X...j.i:-....Eq.y{o....C.2.M.$#w .0m.1..1GJ lf#p6_....5.....o.T....{4.<K(..`o...f."...J...g.'.F.X..B../7}&ut-zx+....y....r.u...kc.'[M.....b..E.Q.8gvQ..=p.I..NRVa'J.\@s....5.....7.5...gq./I\....NH.ZQQ.7..U.P.;ydA~.l4.` .05S{1%z...../....c.#...3..p/....LH...u.%..J.C..@Oh..}4.`..hq..c:fR.{....5.....c.`...hL..WS...._Y.65?.....(."\..I..\.agm*kb7\xb....h....t.<...gu.-IB.....bL.RPX.3..!.\.P.."}.h,.l.hd.l9.N.* 9.....G..$$.W.A.....]d.Wy_.3..H...\|wdU../~....1X[7nh*Gsp....y.....t.o..:$.<DB....kY.OJD.h..a.'.i>3.K.D$.-..BTx.nk!f_x....k.....h.u...fx.<Uq.....]H.TQd.0....C.L..2h.a%.-....".(A!t |

**C:\MSOCache\All Users\{90160000-0044-0409-0000-0000000FF1CE}-C\InfoPathMUI.xml.7878kr5jx (copy)**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 1544 |
| Entropy (8bit): | 7.668723320369599 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | 9DF962CDFED624563B86C5CD9CD62BAF |
| SHA1: | 41894921C4F363006C91AFAD0C9DEC063381EFC9 |
| SHA-256: | 976DED3528CC01C156336B8A51B09C3C4EBB156A71148B32A542EB7184A02AE7 |
| SHA-512: | 12D047AE8520FD3944F2DD25234D782C7D554DA3F528D9C87505BE7E1735817D249E0641440C62EE448AB2A1D52F02FB6A622243872F61B433DB2F0C9D36487E |
| Malicious: | false |
| Preview: | @.....[Y.HVY.k..F.C.m$%.J.c'.-.k:.a89l.*7.....:.5.....,.\|^$.....p..y..1..=./.y..+h._4.^.~}^vJE1>&E....=...w.K...b..[&H.....Fs..v}.$...J.\|>4.O.a..m.bsz07r.lLF....*....}.{....8.D.....Z.vR P.....g.t.V.`..?..0:.}..x4;;....f.....@.F..30.h#.....Uu.~\Y.?.2.6.g-m.x.u/.i.5Uf"vBvBwt..l...E.M....<8._^.....[..Px`.g..C.%.J...t.[..~.>M..q~4,$N....4...u.X...j.i:-....Eq.y{o....C.2.M.$#w .0m.1..1GJ lf#p6_....5.....o.T....{4.<K(..`o...f."...J...g.'.F.X..B../7}&ut-zx+....y....r.u...kc.'[M.....b..E.Q.8gvQ..=p.I..NRVa'J.\@s....5.....7.5...gq./I\....NH.ZQQ.7..U.P.;ydA~.l4.` .05S{1%z...../....c.#...3..p/....LH...u.%..J.C..@Oh..}4.`..hq..c:fR.{....5.....c.`...hL..WS...._Y.65?.....(."\..I..\.agm*kb7\xb....h....t.<...gu.-IB.....bL.RPX.3..!.\.P.."}.h,.l.hd.l9.N.* 9.....G..$$.W.A.....]d.Wy_.3..H...\|wdU../~....1X[7nh*Gsp....y.....t.o..:$.<DB....kY.OJD.h..a.'.i>3.K.D$.-..BTx.nk!f_x....k.....h.u...fx.<Uq.....]H.TQd.0....C.L..2h.a%.-....".(A!t |

**C:\MSOCache\All Users\{90160000-0044-0409-0000-0000000FF1CE}-C\Setup.xml**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 2109 |
| Entropy (8bit): | 7.780332001676361 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | 3330F10430686D507C6FD96D7CCC166D |
| SHA1: | D1CD17C84CFDBBF43EBE3F5D289ADB6E73C7DD93 |
| SHA-256: | C94EC903524FDBFDD76A42497055ACA5A9BE658C383D9F65690533A556C5AC80 |
| SHA-512: | E0F744228E94AB1A15C5A32EE204938A3A758502F2BB7D2DC824BBC1E7BB321B19062EA5F8982387D39BFEA9EFD74591B9E383A7E9B23FB541E6716F9F30F24 8 |
| Malicious: | false |
| Preview: | .c.....{O9.g..1Y.u5^$.u=..sQ.H..Clhx.47.....E.!.....V...e@.....F..CE...\|.J,.e#d{.~?.....%.1;..-c....%.$...d<...fw.....Bt...v.2T.x.h .]6M.;i.6....Q@.q#B....\|.....#Y.5.k_..i...9..k e#..7.u..B..`.N"M..T..H..qXYS.8Et....q.....\.[.._..2...2..?V5..'..S".c:v..**;.;U....83...q~~....[.....8`.D.vH..i.... ..Geo.....6M.@.tx.x.J.aF.1..0;.].S.d....X.,...../<...LK..&.....Np.... .KB.`5\|..knS.o)..6..."E;.(8n....q.....&,.;.^@.....T.m_!..!..H....\?.Q.7.qg.....oG..8oT.....;...uG.R.oI..%.....dC2....`..d.I*.yn\.>G.G...!...zmf....d.V....g...BJ..8.....5./..g..h..u5.i.y \.o)..Y...;...\~...}.+...4`.+.ZD.....\|G".g.b..2{y".}?..&e....Ap...7:c....\|.....!g....\..~.....5./..g...q..,M?.s=^.5.....1.4.y.T...v.....!k.M.AF..~.....gQ... .<Y.u(.k.u ..=K.....&...(8I.....}....:`.&.. .....*....$.u(.q/Xv.]1..?P..!...>...TxT....2.....4b...oA.....K.g.v..!.oF.i>Ni..Yw.X.....r,..7Bc....u.....w....OP.....K.gJ:....d..2{y".}?..&e....Ap.. |

**C:\MSOCache\All Users\{90160000-0044-0409-0000-0000000FF1CE}-C\Setup.xml.7878kr5jx (copy)**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 2109 |
| Entropy (8bit): | 7.780332001676361 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | 3330F10430686D507C6FD96D7CCC166D |
| SHA1: | D1CD17C84CFDBBF43EBE3F5D289ADB6E73C7DD93 |
| SHA-256: | C94EC903524FDBFDD76A42497055ACA5A9BE658C383D9F65690533A556C5AC80 |
| SHA-512: | E0F744228E94AB1A15C5A32EE204938A3A758502F2BB7D2DC824BBC1E7BB321B19062EA5F8982387D39BFEA9EFD74591B9E383A7E9B23FB541E6716F9F30F24 8 |
| Malicious: | false |
| Preview: | .c.....{O9.g..1Y.u5^$.u=..sQ.H..Clhx.47.....E.!.....V...e@.....F..CE...\|.J,.e#d{.~?.....%.1;..-c....%.$...d<...fw.....Bt...v.2T.x.h .]6M.;i.6....Q@.q#B....\|.....#Y.5.k_..i...9..k e#..7.u..B..`.N"M..T..H..qXYS.8Et....q.....\.[.._..2...2..?V5..'..S".c:v..**;.;U....83...q~~....[.....8`.D.vH..i.... ..Geo.....6M.@.tx.x.J.aF.1..0;.].S.d....X.,...../<...LK..&.....Np.... .KB.`5\|..knS.o)..6..."E;.(8n....q.....&,.;.^@.....T.m_!..!..H....\?.Q.7.qg.....oG..8oT.....;...uG.R.oI..%.....dC2....`..d.I*.yn\.>G.G...!...zmf....d.V....g...BJ..8.....5./..g..h..u5.i.y \.o)..Y...;...\~...}.+...4`.+.ZD.....\|G".g.b..2{y".}?..&e....Ap...7:c....\|.....!g....\..~.....5./..g...q..,M?.s=^.5.....1.4.y.T...v.....!k.M.AF..~.....gQ... .<Y.u(.k.u ..=K.....&...(8I.....}....:`.&.. .....*....$.u(.q/Xv.]1..?P..!...>...TxT....2.....4b...oA.....K.g.v..!.oF.i>Ni..Yw.X.....r,..7Bc....u.....w....OP.....K.gJ:....d..2{y".}?..&e....Ap.. |

| C:\MSOCache\All Users\{90160000-0044-0409-0000-0000000FF1CE}-C\instructions_read_me.txt | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 1091 |
| Entropy (8bit): | 4.804750185554599 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | BA21D49977850F54961EDE73B7E9E480 |
| SHA1: | BD630B3DBE9D7139527C1FFDBB2161E7A9067AE0 |
| SHA-256: | 34757273C5E041F07B0352C51CFAB2998AB676F3A39BC0F16A1B4D68F3FAC4F8 |
| SHA-512: | 4BF9BE5F41F7258357E838BA94F0AA2B7F17D8FE3266174AAF123156B422C4FB72E4D3FD36DB7B2E3E9D13202202D2A6B0ECCA06EE2A2A043CE6AD27FFD751E2 |
| Malicious: | false |
| Preview: | ATTENTION!..Your network has been breached and all data was encrypted. Please contact us at:..https://bastad5huzwkepdixedg2gekg7jk22ato24zyllp6lnjx7wdtyctgvyd.onion/ .....Login ID: 26d371a9-efda-4e82-9989-01e292244d65.....*!* To access .onion websites download and install Tor Browser at:.... https://www.torproject.org/ (Tor Browser is not related to us)....*!* To restore all your PCs and get your network working again, follow these instructions:....- Any attempts to modify, decrypt or rename the files will lead to its fatal corruption. It doesn't matter, who are trying to do this, either it will be your IT guys or a recovery agency.....Please follow these simple rules to avoid data corruption:....- Do not modify, rename or delete files. Any attempts to modify, decrypt or rename the files will lead to its fatal corruption. ....- Do not hire a recovery company. They can't decrypt without the key. ..They also don't care about your business. They believe that they are ..good negotiator |

| C:\MSOCache\All Users\{90160000-0090-0409-0000-0000000FF1CE}-C\DCFMUI.cab | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 641904 |
| Entropy (8bit): | **7.99920950933189** |
| Encrypted: | **true** |
| SSDEEP: | |
| MD5: | E0CDB3C2223FEC0C1640E72098F4FDF0 |
| SHA1: | 37D363A08CF1B6E6641289236FED0D9C65434C08 |
| SHA-256: | BA71870E7F8AAF89C016306D0B272AF3B1DC6DD2DEAADB9C7C2EBACE2B94E23B |
| SHA-512: | 873F0035F772EFAD5428AE0DB1E421DEC2ED417E78971EFF272C318EDBAC7253878903DB2270EC1024CF9B3B0215C599F21A6142A8D1784B77233A96D3C479C |
| Malicious: | **true** |
| Preview: | n.t...2...?.e6..`J..U..5..9.h....n.xOh%.8Hq"...XiE...y...*.+.....2.....F.O .COMMON.AUDITITEMS.RESOURCES.DLL.x86.1033..Z...2.....F.O .COMMON.CLIENTCONFIGURATION.q.d...qS.qr.)....N{(.f..t.../h....(.#ohf.u.>z...;..N../.....j..URCES.DLL.x86.1033.....P.....F.O .COMMON.FILEUTILS.RESOURCES.DLL.x86.1033.....F.O .COMMON.PASSWORDMANAGER.RESOURCES.DLL.[..}...%.'.e..`J..U.(6].m.*....!.<.:`.p."k...KT....1....*di.. .DATABASECOMPARE_COL.HXC_1033.....O.....F..DATABASECOMPARE_COL.HXT_1033.r.....F.. .DATABASECOMPARE_F_COL.HXK_1033.q....#.7Q.wt...6.$b..3.[..Gld\.r.+....6.3~X..8.34..xTG...j....k.f..SHIM.RESOURCES.DLL.1033..n...C.....F.. .SPREADSHEETCOMPARE.HXS_1033.....F.. .SPREADSHEETCOMPARE_COL.HXC_1033.....y.....F#..S..`S..e. s..-.Y..HKyU.q.<....]..Oh%.8Xq5.Y.xOe...+...b.j..OMPARE_F_COL.HXK_1033.q.....F.. .SPREADSHEETCOMPARE_K_COL.HXK_1033..R.....F.O .SPREADSHEETIQ.DIAGRAM.RESOURCES.DLL.x86....`.Ad...d.e5.z.s.8..GZsX.j.-....@.4.-i |

| C:\MSOCache\All Users\{90160000-0090-0409-0000-0000000FF1CE}-C\DCFMUI.cab.7878kr5jx (copy) | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 641904 |
| Entropy (8bit): | **7.99920950933189** |
| Encrypted: | **true** |
| SSDEEP: | |
| MD5: | E0CDB3C2223FEC0C1640E72098F4FDF0 |
| SHA1: | 37D363A08CF1B6E6641289236FED0D9C65434C08 |
| SHA-256: | BA71870E7F8AAF89C016306D0B272AF3B1DC6DD2DEAADB9C7C2EBACE2B94E23B |
| SHA-512: | 873F0035F772EFAD5428AE0DB1E421DEC2ED417E78971EFF272C318EDBAC7253878903DB2270EC1024CF9B3B0215C599F21A6142A8D1784B77233A96D3C479C |
| Malicious: | **true** |
| Preview: | n.t...2...?.e6..`J..U..5..9.h....n.xOh%.8Hq"...XiE...y...*.+.....2.....F.O .COMMON.AUDITITEMS.RESOURCES.DLL.x86.1033..Z...2.....F.O .COMMON.CLIENTCONFIGURATION.q.d...qS.qr.)....N{(.f..t.../h....(.#ohf.u.>z...;..N../.....j..URCES.DLL.x86.1033.....P.....F.O .COMMON.FILEUTILS.RESOURCES.DLL.x86.1033.....F.O .COMMON.PASSWORDMANAGER.RESOURCES.DLL.[..}...%.'.e..`J..U.(6].m.*....!.<.:`.p."k...KT....1....*di.. .DATABASECOMPARE_COL.HXC_1033.....O.....F..DATABASECOMPARE_COL.HXT_1033.r.....F.. .DATABASECOMPARE_F_COL.HXK_1033.q....#.7Q.wt...6.$b..3.[..Gld\.r.+....6.3~X..8.34..xTG...j....k.f..SHIM.RESOURCES.DLL.1033..n...C.....F.. .SPREADSHEETCOMPARE.HXS_1033.....F.. .SPREADSHEETCOMPARE_COL.HXC_1033.....y.....F#..S..`S..e. s..-.Y..HKyU.q.<....]..Oh%.8Xq5.Y.xOe...+...b.j..OMPARE_F_COL.HXK_1033.q.....F.. .SPREADSHEETCOMPARE_K_COL.HXK_1033..R.....F.O .SPREADSHEETIQ.DIAGRAM.RESOURCES.DLL.x86....`.Ad...d.e5.z.s.8..GZsX.j.-....@.4.-i |

**C:\MSOCache\All Users\{90160000-0090-0409-0000-0000000FF1CE}-C\DCFMUI.msi**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 2384186 |
| Entropy (8bit): | 7.114699347653902 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | 2AAE645411ABEFC6FB0978CD1010C05C |
| SHA1: | D932253A067156E89F24717B835CDB80A97668FD |
| SHA-256: | 52267B4D2620756289245136EDEF6B0D90DBD11E09CECC1808104A67783C9FBF |
| SHA-512: | E12DFE783B65FEAB3696A8DDBAA9E2EF43E7ADA8863B1B98BF976AD38B5DE1B01D6F4218CCFF3430456C09C9D358BAF8C5E6EB24D00433EE2C71EDBBD0964C6D |
| Malicious: | false |
| Preview: | ..cV...!.^.L3.y]...gv.x....kD..Yr..`c.R*...p.O.Y.K...z....-x.O.....!.I...?.....L._.....SQO.k.=....\..I..3.U....`.../.ICJ..V.....!.I...?.....L._.....SQO.k.=....\..I..3.U....`.../.ICJ..V.....Y.r.<....^.L3.y]...gv.x..6.H..Yr..`c.P*...p.O.Y.K...z..../x.O.....Y.r.<....^.L3.y]...gv.x..6.H..Yr..`c.P*...p.O.Y.K...z..../x.O.....Y.r.<....^.L3.y]...gv.x..6.H..Yr..`c. |

**C:\MSOCache\All Users\{90160000-0090-0409-0000-0000000FF1CE}-C\DCFMUI.msi.7878kr5jx (copy)**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 2384186 |
| Entropy (8bit): | 7.114699347653902 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | 2AAE645411ABEFC6FB0978CD1010C05C |
| SHA1: | D932253A067156E89F24717B835CDB80A97668FD |
| SHA-256: | 52267B4D2620756289245136EDEF6B0D90DBD11E09CECC1808104A67783C9FBF |
| SHA-512: | E12DFE783B65FEAB3696A8DDBAA9E2EF43E7ADA8863B1B98BF976AD38B5DE1B01D6F4218CCFF3430456C09C9D358BAF8C5E6EB24D00433EE2C71EDBBD0964C6D |
| Malicious: | false |
| Preview: | ..cV...!.^.L3.y]...gv.x....kD..Yr..`c.R*...p.O.Y.K...z....-x.O.....!.I...?.....L._.....SQO.k.=....\..I..3.U....`.../.ICJ..V.....!.I...?.....L._.....SQO.k.=....\..I..3.U....`.../.ICJ..V.....Y.r.<....^.L3.y]...gv.x..6.H..Yr..`c.P*...p.O.Y.K...z..../x.O.....Y.r.<....^.L3.y]...gv.x..6.H..Yr..`c.P*...p.O.Y.K...z..../x.O.....Y.r.<....^.L3.y]...gv.x..6.H..Yr..`c. |

**C:\MSOCache\All Users\{90160000-0090-0409-0000-0000000FF1CE}-C\DCFMUI.xml**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | OpenPGP Public Key |
| Category: | dropped |
| Size (bytes): | 1529 |
| Entropy (8bit): | 7.680670765970888 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | 4950C77D2A91C4C55A4E34CA815A97E6 |
| SHA1: | E2334485AF31DC6B000E5EDDA0E98008C1D3C55C |
| SHA-256: | D1209F26FC5302B8C19B667F991E650D0E289E2098DCC7866718A299176529CF |
| SHA-512: | 115E92A1D925941C9F6AA6837430498E9025C1D4D7FBD4B4AE517773A7C5F1F9A2DDD2C8826A47C87118F78C634F0C53FCACF79955550689BE681920E37DA56A |
| Malicious: | false |
| Preview: | .9.....0. W...,..<}.... ..J&..DT....4.. $.............Z.!.k....H..k....(Z...J..F...-....ey..~fi.c._..iG..u....s.....]...X...B..S. ...@...T..zm.....FT..suT.y.a.k-n..8../.1....b.Z,d..e...@.... L...^..K..Z1.v...m..G.....<1(.....5.n.....!.."x...)..m.#!.+i..G..k6.\...Q..L..UVM...I..eQ..'.....:.Rf.~p....6..I.-...{...S..X).>7.+..JI..H^U.O.@..j2..9..j.....V7.+t...A...O.C...m..T.X...+...6.:.S.O.k.x<L.....t.crQ.j....K.....6.t....P..0..!D....^r....2...*.osa.....>.c...h. `Ax>..+.....Er.y...-.....Y%.9X.`H..U@p.C.7.,*+...~..u.q...y.b?.=p....a..D.Ws.z...q..x2..[.<B..%..9.E.M...x<L.....6.....<.q>..r....E....E`.D2...R..w2.:..d3..9..]_f.c.N.p}k..8..t.L...v.u1.=a.....@..0.iq...Y..V8.. .(..du..o.3...*.roq...}..o.c...P.,..<z....`....%0.-Q...x.. P.aZ....Yn...?....o.iiw...(....5...4.V9.-`....u....M`.D2...R..w2.:..d3..9..GSz.e.y.|pi..c..Q.}..8.e".v....c..S.U..t....N..{<....!..|D...!.o.y. >4...t..y.L...e.`$.'}....O..q..&.(V..2...T.G .%.._~.:;?.I.~.o |

**C:\MSOCache\All Users\{90160000-0090-0409-0000-0000000FF1CE}-C\DCFMUI.xml.7878kr5jx (copy)**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | OpenPGP Public Key |

| | |
|---|---|
| Category: | dropped |
| Size (bytes): | 1529 |
| Entropy (8bit): | 7.680670765970888 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | 4950C77D2A91C4C55A4E34CA815A97E6 |
| SHA1: | E2334485AF31DC6B000E5EDDA0E98008C1D3C55C |
| SHA-256: | D1209F26FC5302B8C19B667F991E650D0E289E2098DCC7866718A299176529CF |
| SHA-512: | 115E92A1D925941C9F6AA6837430498E9025C1D4D7FBD4B4AE517773A7C5F1F9A2DDD2C8826A47C87118F78C634F0C53FCACF79955550689BE681920E37DA56A |
| Malicious: | false |
| Preview: | .9.....0. W...,..<}.... ..J&..DT....4.. $.............Z.!.k....H..k....(Z...J..F...-....ey..~fi.c._..iG..u....s.....]...X...B..S. ...@...T..zm.......FT..suT.y.a.k-n..8../.1....b.Z,d..e...@.... L...^..<br>K..Z1.v...m..G.......<1(......5.n.....!.."x...)..m.#!.+i..G..k6.\...Q..L..UVM...I..eQ..'.....:.Rf.~p....6..I.-...{...S..X).>7.+..JI..H^U.O.@..j2..9..j.....V7.+t...A...O.C...m..T.X...+...<br>..6.:.S.O.k.x<L.....t.crQ.j....K.....6.t....P..0..!D....^r....2...*.osa.....>.c...h. `Ax>..+.....Er.y...-.....Y%.9X.`H..U@p.C.7.,*+...~..u.q...y.b?.=p....a..D.Ws.z...q..x2..[.<B..%..9<br>.E.M...x<L.....6.....<.q>..r....E....E`.D2...R..w2.:..d3..9..]_f.c.N.p}k..8..t.L...v.u1.=a.....@..0.iq...Y..V8.. .(..du..o.3...*.roq...}..o.c...P.,...<z....`....%0.-Q...x.. P.aZ....Yn...?....o.iiw...(<br>....5...4.V9.-`....u....M`.D2...R..w2.:..d3..9..GSz.e.y.|pi..c..Q.}..8.e".v....c..S.U..t....N..{<....!..|D...!.o.y. >4...t..y.L...e.`$.'}....O..q..&.(V..2...T.G .%.._~.:;?.I.~.o |

| C:\MSOCache\All Users\{90160000-0090-0409-0000-0000000FF1CE}-C\Setup.xml | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 2122 |
| Entropy (8bit): | 7.782653398168922 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | 8DD8BAECD1C67272D8DC67681B025808 |
| SHA1: | 47C109713CE18DE030F816BF8FF28AA01AAC967A |
| SHA-256: | 85CD9BCB81156551EC7882B406B8BD43A3265E6AA329E3D52103F28251AAA37B |
| SHA-512: | 98E7C9CDA7AF248F0548CFC7E0B2F34D3A88786315BF3AE33F54D3FD2D629085BED6A817B74AA196D4F4EEF96D36115115D80829E1D463EF6D1D5225D36DDA7 |
| Malicious: | false |
| Preview: | .9..m'b.9.%X.L.O2..v*.B.|...jYB.I...$.E.].0M.;.^..].}.'.I.%..X..~..Jt_..16\.@PKr..3~.o.f....|Y.....[...=.(D...`..Z.W_..o.'.U..|..i,n.*>6D..h<V.o...E.s...@{..u..k..XK.q=...a..z.j.4...%.....s.<br>.KMd.r$.v..f.P..8...W.. ...I.....n.Q.N[.I.?..L.-.R.+.y._..`..6~U.">..0E;r.$...c.v...2Gy.1L..~..mH.Ze...|..].\.V...c.....@..5Em.#..Y..k&N..`v.{.]....}_.WA.5."JO.K}...g..m.s./.i.&.<br>.N..A...DP.:U'~..TI_.1;.g.b...v!<.7J.j..EA.YQ.Z.e..}.> ..?.3..^..$..d~c.9.q..2f3l..v..Y.g...-B.........sn..t}.T.o..O.i.....b..V..b..Ebr.>.8d..T.!..9,...Q..$@Y.%M.t.r...n0.0.x..b.i5..?.e._...<br>..#'\./.)Y.SY.o..hB....e..&...Y..w.*~3.Yw...o..z.<T$.<.d..i..r..#K{.*.n...S.p.!..H.a...-_. F.v. V=.kw...x.,.{.B...u..T.....#(*.Anpx..I.r..2r._.q...EZ.........T..Nf...6..a...B...b..V..G..di`<br>.i.)D.Qd.o.: .I.p...;I...@....F(@.mf...+..3.J;/...x..I..B..`rx...-C.L.2s.:m..D.t..?mT..A..8. .\.ta...d..j.{...).,.U.....(.;.%X.Qi.!..$ .L.v....IP..C.n.;DA.Q}...)..g.....-.s..T.$..#'P.8. [..a.j."&....<br>I...v!<.m&..U.; |

| C:\MSOCache\All Users\{90160000-0090-0409-0000-0000000FF1CE}-C\Setup.xml.7878kr5jx (copy) | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 2122 |
| Entropy (8bit): | 7.782653398168922 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | 8DD8BAECD1C67272D8DC67681B025808 |
| SHA1: | 47C109713CE18DE030F816BF8FF28AA01AAC967A |
| SHA-256: | 85CD9BCB81156551EC7882B406B8BD43A3265E6AA329E3D52103F28251AAA37B |
| SHA-512: | 98E7C9CDA7AF248F0548CFC7E0B2F34D3A88786315BF3AE33F54D3FD2D629085BED6A817B74AA196D4F4EEF96D36115115D80829E1D463EF6D1D5225D36DDA7 |
| Malicious: | false |
| Preview: | .9..m'b.9.%X.L.O2..v*.B.|...jYB.I...$.E.].0M.;.^..].}.'.I.%..X..~..Jt_..16\.@PKr..3~.o.f....|Y.....[...=.(D...`..Z.W_..o.'.U..|..i,n.*>6D..h<V.o...E.s...@{..u..k..XK.q=...a..z.j.4...%.....s.<br>.KMd.r$.v..f.P..8...W.. ...I.....n.Q.N[.I.?..L.-.R.+.y._..`..6~U.">..0E;r.$...c.v...2Gy.1L..~..mH.Ze...|..].\.V...c.....@..5Em.#..Y..k&N..`v.{.]....}_.WA.5."JO.K}...g..m.s./.i.&.<br>.N..A...DP.:U'~..TI_.1;.g.b...v!<.7J.j..EA.YQ.Z.e..}.> ..?.3..^..$..d~c.9.q..2f3l..v..Y.g...-B.........sn..t}.T.o..O.i.....b..V..b..Ebr.>.8d..T.!..9,...Q..$@Y.%M.t.r...n0.0.x..b.i5..?.e._...<br>..#'\./.)Y.SY.o..hB....e..&...Y..w.*~3.Yw...o..z.<T$.<.d..i..r..#K{.*.n...S.p.!..H.a...-_. F.v. V=.kw...x.,.{.B...u..T.....#(*.Anpx..I.r..2r._.q...EZ.........T..Nf...6..a...B...b..V..G..di`<br>.i.)D.Qd.o.: .I.p...;I...@....F(@.mf...+..3.J;/...x..I..B..`rx...-C.L.2s.:m..D.t..?mT..A..8. .\.ta...d..j.{...).,.U.....(.;.%X.Qi.!..$ .L.v....IP..C.n.;DA.Q}...)..g.....-.s..T.$..#'P.8. [..a.j."&....<br>I...v!<.m&..U.; |

| C:\MSOCache\All Users\{90160000-0090-0409-0000-0000000FF1CE}-C\instructions_read_me.txt | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 1091 |
| Entropy (8bit): | 4.804750185554599 |

| | |
|---|---|
| Encrypted: | false |
| SSDEEP: | |
| MD5: | BA21D49977850F54961EDE73B7E9E480 |
| SHA1: | BD630B3DBE9D7139527C1FFDBB2161E7A9067AE0 |
| SHA-256: | 34757273C5E041F07B0352C51CFAB2998AB676F3A39BC0F16A1B4D68F3FAC4F8 |
| SHA-512: | 4BF9BE5F41F7258357E838BA94F0AA2B7F17D8FE3266174AAF123156B422C4FB72E4D3FD36DB7B2E3E9D13202202D2A6B0ECCA06EE2A2A043CE6AD27FFD751E2 |
| Malicious: | false |
| Preview: | ATTENTION!..Your network has been breached and all data was encrypted. Please contact us at:..https://bastad5huzwkepdixedg2gekg7jk22ato24zyllp6lnjx7wdtyctgvyd.onion/ .....Login ID: 26d371a9-efda-4e82-9989-01e292244d65.....*!* To access .onion websites download and install Tor Browser at:.... https://www.torproject.org/ (Tor Browser is not related to us)....*!* To restore all your PCs and get your network working again, follow these instructions:....- Any attempts to modify, decrypt or rename the files will lead to its fatal corruption. It doesn't matter, who are trying to do this, either it will be your IT guys or a recovery agency.....Please follow these simple rules to avoid data corruption:....- Do not modify, rename or delete files. Any attempts to modify, decrypt or rename the files will lead to its fatal corruption. ....- Do not hire a recovery company. They can't decrypt without the key. ..They also don't care about your business. They believe that they are ..good negotiator |

# Static File Info

## General

| | |
|---|---|
| File type: | PE32 executable (GUI) Intel 80386, for MS Windows |
| Entropy (8bit): | 7.044268283359809 |
| TrID: | • Win32 Executable (generic) a (10002005/4) 99.94%<br>• Win16/32 Executable Delphi generic (2074/23) 0.02%<br>• Generic Win/DOS Executable (2004/3) 0.02%<br>• DOS Executable Generic (2002/1) 0.02%<br>• Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00% |
| File name: | HkObDPju6Z.exe |
| File size: | 1489920 |
| MD5: | 6441d7260944bcedc5958c5c8a05d16d |
| SHA1: | 46257982840493eca90e051ff1749e7040895584 |
| SHA256: | 723d1cf3d74fb3ce95a77ed9dff257a78c8af8e67a82963230dd073781074224 |
| SHA512: | af88fd3a0a2728c811be524feee575d8d2d9623b7944021c83173e40dbec6b1fbe7bea64dcdd8f1dbebc7d8df76b40e5c9647e2586316ea46ceb191ebcf14d89 |
| SSDEEP: | 24576:1p2gwjk6ikYhJ9lvGnYZvy48/V33ck7LnBAyldFu8hod/Qodly:1AgxkmvGnYWccjBAwFadRd |
| TLSH: | 9B65D000B680C036FA722870556AABB2897EBC30976555CF23C43D7B6E726D19D3672F |
| File Content Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....W.....L.....7.....@.....P.....@..... |

## File Icon

| | |
|---|---|
| Icon Hash: | 3fc7a3c665f3c37d |

## Static PE Info

### General

| | |
|---|---|
| Entrypoint: | 0x4237d9 |
| Entrypoint Section: | .text |
| Digitally signed: | false |
| Imagebase: | 0x400000 |
| Subsystem: | windows gui |
| Image File Characteristics: | EXECUTABLE_IMAGE, 32BIT_MACHINE |
| DLL Characteristics: | DYNAMIC_BASE, NX_COMPAT, TERMINAL_SERVER_AWARE |
| Time Stamp: | 0x5717C407 [Wed Apr 20 18:01:43 2016 UTC] |
| TLS Callbacks: | |
| CLR (.Net) Version: | |
| OS Version Major: | 6 |
| OS Version Minor: | 0 |
| File Version Major: | 6 |
| File Version Minor: | 0 |
| Subsystem Version Major: | 6 |
| Subsystem Version Minor: | 0 |

| | |
|---|---|
| Import Hash: | e7481059b799ac586859298d4788584d |

| Entrypoint Preview |
|---|
| **Instruction** |
| call 00007F0D4C6EC74Dh |
| jmp 00007F0D4C6EBEA8h |
| retn 0000h |
| push ebp |
| mov ebp, esp |
| mov eax, dword ptr [ebp+08h] |
| mov eax, dword ptr [eax] |
| pop ebp |
| ret |
| push ebp |
| mov ebp, esp |
| mov eax, dword ptr [ebp+08h] |
| mov eax, dword ptr [eax] |
| pop ebp |
| ret |
| push ebp |
| mov ebp, esp |
| mov eax, dword ptr [ebp+08h] |
| mov edx, 0048E840h |
| mov ecx, 0048E840h |
| sub eax, edx |
| sub ecx, edx |
| cmp eax, ecx |
| jnbe 00007F0D4C6EC083h |
| int3 |
| pop ebp |
| ret |
| push ebp |
| mov ebp, esp |
| mov eax, dword ptr [ebp+08h] |
| mov edx, 0048E840h |
| mov ecx, 0048E840h |
| sub eax, edx |
| sub ecx, edx |
| cmp eax, ecx |
| jnbe 00007F0D4C6EC087h |
| push 00000041h |
| pop ecx |
| int 29h |
| pop ebp |
| ret |
| retn 0000h |
| push ebp |
| mov ebp, esp |
| mov eax, dword ptr [ebp+08h] |
| mov edx, 0048E840h |
| mov ecx, 0048E840h |
| sub eax, edx |
| sub ecx, edx |
| cmp eax, ecx |
| jnbe 00007F0D4C6EC093h |
| cmp dword ptr [0047E620h], 00000000h |
| je 00007F0D4C6EC08Ah |
| mov eax, dword ptr [0047E620h] |
| pop ebp |
| jmp eax |

| Instruction |
|---|
| pop ebp |
| ret |
| push ebp |
| mov ebp, esp |
| cmp dword ptr [0047E620h], 00000000h |
| je 00007F0D4C6EC08Ah |
| mov eax, dword ptr [0047E620h] |
| pop ebp |
| jmp eax |
| pop ebp |
| ret |
| push ebp |
| mov ebp, esp |
| mov eax, dword ptr [ebp+08h] |
| mov edx, 0048E840h |
| mov ecx, 0048E840h |
| sub eax, edx |
| sub ecx, edx |
| cmp ecx, eax |
| sbb eax, eax |
| inc eax |
| pop ebp |
| ret |
| push ebp |
| mov ebp, esp |
| mov ecx, dword ptr [ebp+08h] |
| mov eax, ecx |
| sub eax, dword ptr [ebp+0Ch] |
| sub eax, 0000E800h |

**Data Directories**

| Name | Virtual Address | Virtual Size | Is in Section |
|---|---|---|---|
| IMAGE_DIRECTORY_ENTRY_EXPORT | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_IMPORT | 0x90c70 | 0xf0 | .rdata |
| IMAGE_DIRECTORY_ENTRY_RESOURCE | 0x11e000 | 0x50378 | .rsrc |
| IMAGE_DIRECTORY_ENTRY_EXCEPTION | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_SECURITY | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_BASERELOC | 0x16f000 | 0x5110 | .reloc |
| IMAGE_DIRECTORY_ENTRY_DEBUG | 0x8e780 | 0x70 | .rdata |
| IMAGE_DIRECTORY_ENTRY_COPYRIGHT | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_GLOBALPTR | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_TLS | 0x8e880 | 0x18 | .rdata |
| IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG | 0x85578 | 0x40 | .rdata |
| IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_IAT | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT | 0x90b68 | 0x40 | .rdata |
| IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_RESERVED | 0x0 | 0x0 | |

**Sections**

| Name | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy | Characteristics |
|---|---|---|---|---|---|---|---|---|
| .text | 0x1000 | 0x7c9ea | 0x7ca00 | False | 0.41879348984453363 | data | 6.631020869912357 | IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ |
| .rdata | 0x7e000 | 0x14e72 | 0x15000 | False | 0.5792178199404762 | data | 6.1426369171952455 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |

| Name | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy | Characteristics |
|---|---|---|---|---|---|---|---|---|
| .data | 0x93000 | 0x8a5b0 | 0x84800 | False | 0.9093639445754716 | data | 7.357984406581138 | IMAGE_SCN_CNT_CODE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE |
| .rsrc | 0x11e000 | 0x50378 | 0x50400 | False | 0.501323379088785 | data | 5.824284929352815 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .reloc | 0x16f000 | 0x5110 | 0x5200 | False | 0.784108231707317 | data | 6.756606998856607 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ |

**Resources**

| Name | RVA | Size | Type | Language | Country |
|---|---|---|---|---|---|
| RT_CURSOR | 0x147588 | 0x134 | Targa image data 64 x 65536 x 1 +32 "\001" | English | United States |
| RT_BITMAP | 0x1476d8 | 0x3c28 | Device independent bitmap graphic, 240 x 16 x 32, image size 15360, resolution 3779 x 3779 px/m | English | United States |
| RT_BITMAP | 0x14b300 | 0x428 | Device independent bitmap graphic, 16 x 16 x 32, image size 1024, resolution 3779 x 3779 px/m | English | United States |
| RT_ICON | 0x11ec00 | 0x1011a | PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced | English | United States |
| RT_ICON | 0x12ed20 | 0x10828 | Device independent bitmap graphic, 128 x 256 x 32, image size 67584 | English | United States |
| RT_ICON | 0x13f548 | 0x4228 | Device independent bitmap graphic, 64 x 128 x 32, image size 16896 | English | United States |
| RT_ICON | 0x143770 | 0x25a8 | Device independent bitmap graphic, 48 x 96 x 32, image size 9600 | English | United States |
| RT_ICON | 0x145d18 | 0x10a8 | Device independent bitmap graphic, 32 x 64 x 32, image size 4224 | English | United States |
| RT_ICON | 0x146dc0 | 0x468 | Device independent bitmap graphic, 16 x 32 x 32, image size 1088 | English | United States |
| RT_ICON | 0x147288 | 0x2e8 | Device independent bitmap graphic, 32 x 64 x 4, image size 512, 16 important colors | English | United States |
| RT_ICON | 0x14baf8 | 0x10828 | Device independent bitmap graphic, 128 x 256 x 32, image size 0 | English | United States |
| RT_ICON | 0x15c320 | 0x4228 | Device independent bitmap graphic, 64 x 128 x 32, image size 0 | English | United States |
| RT_ICON | 0x160548 | 0x25a8 | Device independent bitmap graphic, 48 x 96 x 32, image size 0 | English | United States |
| RT_ICON | 0x162af0 | 0x10a8 | Device independent bitmap graphic, 32 x 64 x 32, image size 0 | English | United States |
| RT_ICON | 0x163b98 | 0x468 | Device independent bitmap graphic, 16 x 32 x 32, image size 0 | English | United States |
| RT_ICON | 0x164050 | 0x10a8 | Device independent bitmap graphic, 32 x 64 x 32, image size 4224 | English | United States |
| RT_ICON | 0x165110 | 0x10a8 | Device independent bitmap graphic, 32 x 64 x 32, image size 4224 | English | United States |
| RT_ICON | 0x1661d0 | 0x10a8 | Device independent bitmap graphic, 32 x 64 x 32, image size 4224 | English | United States |
| RT_ICON | 0x167290 | 0x10a8 | Device independent bitmap graphic, 32 x 64 x 32, image size 4224 | English | United States |
| RT_ICON | 0x168350 | 0x2e8 | Device independent bitmap graphic, 32 x 64 x 4, image size 512, 16 important colors | English | United States |
| RT_ICON | 0x168650 | 0x10a8 | Device independent bitmap graphic, 32 x 64 x 32, image size 4224 | English | United States |
| RT_ICON | 0x169710 | 0x2e8 | Device independent bitmap graphic, 32 x 64 x 4, image size 512, 16 important colors | English | United States |
| RT_MENU | 0x169a10 | 0x53e | data | English | United States |
| RT_DIALOG | 0x169f50 | 0x1a8 | data | English | United States |
| RT_DIALOG | 0x16a0f8 | 0x1b0 | data | English | United States |
| RT_DIALOG | 0x16a480 | 0x1dc | data | English | United States |
| RT_DIALOG | 0x16a660 | 0x1dc | data | English | United States |
| RT_DIALOG | 0x16a840 | 0x130 | data | English | United States |
| RT_DIALOG | 0x16aaa0 | 0x210 | data | English | United States |
| RT_DIALOG | 0x16a2a8 | 0x1d4 | data | English | United States |

| Name | RVA | Size | Type | Language | Country |
|---|---|---|---|---|---|
| RT_DIALOG | 0x16a970 | 0x130 | data | English | United States |
| RT_DIALOG | 0x16bbe0 | 0x560 | data | English | United States |
| RT_DIALOG | 0x16c140 | 0x244 | data | English | United States |
| RT_DIALOG | 0x16acb0 | 0x4a2 | data | English | United States |
| RT_DIALOG | 0x16b158 | 0x4ae | data | English | United States |
| RT_DIALOG | 0x16b608 | 0x3ba | data | English | United States |
| RT_DIALOG | 0x16b9c8 | 0x218 | data | English | United States |
| RT_STRING | 0x16c928 | 0xa6 | data | English | United States |
| RT_STRING | 0x16d510 | 0x1e0 | Matlab v4 mat-file (little endian) i, numeric, rows 0, columns 0 | English | United States |
| RT_STRING | 0x16d738 | 0x1b0 | data | English | United States |
| RT_STRING | 0x16c800 | 0x124 | data | English | United States |
| RT_STRING | 0x16c9d0 | 0xb3e | data | English | United States |
| RT_STRING | 0x16c388 | 0x478 | data | English | United States |
| RT_STRING | 0x16d6f0 | 0x48 | data | English | United States |
| RT_ACCELERATOR | 0x14b728 | 0x1a0 | data | English | United States |
| RT_GROUP_CURSOR | 0x1476c0 | 0x14 | Lotus unknown worksheet or configuration, revision 0x1 | English | United States |
| RT_GROUP_ICON | 0x147228 | 0x5a | Targa image data - Map 32 x 282 x 1 +1 | English | United States |
| RT_GROUP_ICON | 0x1650f8 | 0x14 | data | English | United States |
| RT_GROUP_ICON | 0x168638 | 0x14 | data | English | United States |
| RT_GROUP_ICON | 0x167278 | 0x14 | data | English | United States |
| RT_GROUP_ICON | 0x168338 | 0x14 | data | English | United States |
| RT_GROUP_ICON | 0x1696f8 | 0x14 | data | English | United States |
| RT_GROUP_ICON | 0x1661b8 | 0x14 | data | English | United States |
| RT_GROUP_ICON | 0x1699f8 | 0x14 | data | English | United States |
| RT_GROUP_ICON | 0x147570 | 0x14 | data | English | United States |
| RT_GROUP_ICON | 0x164000 | 0x4c | data | English | United States |
| RT_VERSION | 0x14b8c8 | 0x22c | data | English | United States |
| RT_MANIFEST | 0x16d8e8 | 0xa90 | XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with very long lines (2644), with CRLF line terminators | English | United States |

**Imports**

| DLL | Import |
|---|---|
| SHLWAPI.dll | PathGetDriveNumberW, StrCmpNIW, StrDupW, StrChrA, PathRelativePathToW, PathIsPrefixW, PathFindFileNameW, PathUnExpandEnvStringsW, PathIsRootW, PathCanonicalizeW, PathFindExtensionW, PathCommonPrefixW, PathCompactPathExW, PathRemoveExtensionW, StrFormatByteSizeW, PathStripPathW, PathRemoveBackslashW, StrRetToBufW, PathMatchSpecW, StrCatBuffW, PathUnquoteSpacesW, StrChrW, StrTrimW, SHAutoComplete, StrCpyNW, PathQuoteSpacesW, PathRenameExtensionW, PathIsDirectoryW, StrRChrW, PathAppendW, PathIsRelativeW, PathFileExistsW, PathAddBackslashW, PathRemoveFileSpecW, PathIsSameRootW |
| PSAPI.DLL | EnumProcessModules, GetModuleFileNameExW |
| USER32.dll | OffsetRect, OpenClipboard, BeginDeferWindowPos, GetSubMenu, TrackPopupMenu, LoadAcceleratorsW, DeleteMenu, ShowOwnedPopups, CopyImage, MessageBoxW, EqualRect, IsWindowVisible, ShowWindowAsync, GetMessagePos, LoadMenuW, CharUpperW, GetKeyState, DefWindowProcW, GetMenuItemInfoW, DeferWindowPos, GetMessageW, CloseClipboard, SetMenuItemInfoW, EmptyClipboard, RegisterClassW, SetWindowPlacement, FrameRect, SetMenuDefaultItem, EnumWindows, GetMessageTime, IntersectRect, SetFocus, BringWindowToTop, TranslateAcceleratorW, GetWindowDC, EndDeferWindowPos, SetClipboardData, CheckMenuItem, IsZoomed, KillTimer, PostQuitMessage, GetSysColorBrush, EnableMenuItem, RegisterWindowMessageW, UpdateWindow, IsIconic, GetWindowThreadProcessId, DrawAnimatedRects, FindWindowExW, GetDC, MonitorFromRect, SetActiveWindow, LoadStringA, SetWindowTextW, LoadStringW, DdeCreateStringHandleW, DdeConnect, GetMonitorInfoW, DdeInitializeW, SetTimer, SetWindowCompositionAttribute, SystemParametersInfoW, SetPropW, RedrawWindow, SendMessageW, wsprintfW, GetSysColor, CharPrevW, GetWindowPlacement, GetSystemMetrics, DdeUninitialize, DialogBoxIndirectParamW, DdeClientTransaction, SetLayeredWindowAttributes, CharUpperBuffW, SetRect, DdeDisconnect, SetForegroundWindow, LoadImageW, ReleaseDC, GetPropW, RemovePropW, DispatchMessageW, PeekMessageW, TranslateMessage, GetWindowLongW, GetWindowTextLengthW, GetSystemMenu, AdjustWindowRectEx, PostMessageW, CheckMenuRadioItem, GetWindowRect, GetFocus, DestroyWindow, SetWindowPos, CheckRadioButton, MessageBoxExW, CreateWindowExW, EndDialog, MessageBeep, CreatePopupMenu, WindowFromPoint, DestroyCursor, ShowWindow, DestroyIcon, GetDlgCtrlID, SetDlgItemTextW, MapWindowPoints, GetDlgItemTextW, SendDlgItemMessageW, IsWindowEnabled, IsDlgButtonChecked, DestroyMenu, GetMenuStringW, CharNextW, LoadIconW, LoadCursorW, GetClassNameW, SetCapture, InsertMenuW, SetCursor, SetWindowLongW, TrackPopupMenuEx, GetComboBoxInfo, GetClientRect, GetDlgItem, AppendMenuW, CheckDlgButton, GetParent, ReleaseCapture, InvalidateRect, ChildWindowFromPoint, GetCursorPos, EnableWindow, GetWindowTextW, DdeFreeStringHandle |

| DLL | Import |
|---|---|
| KERNEL32.dll | RaiseException, GetSystemInfo, VirtualQuery, GetModuleHandleW, LoadLibraryExA, EnterCriticalSection, LeaveCriticalSection, DecodePointer, InitializeCriticalSectionAndSpinCount, DeleteCriticalSection, WaitForSingleObjectEx, ReadConsoleW, GetConsoleMode, VirtualProtect, CompareStringOrdinal, FreeLibrary, LoadLibraryExW, ReadFile, lstrlenW, WriteFile, lstrcpynW, ExpandEnvironmentStringsW, GetModuleFileNameW, SetFilePointer, SetEndOfFile, UnlockFileEx, CreateFileW, GetSystemDirectoryW, MultiByteToWideChar, lstrcatW, CloseHandle, LockFileEx, GetFileSize, WideCharToMultiByte, lstrcpyW, lstrcmpiW, lstrcmpW, FlushFileBuffers, GetShortPathNameW, LocalAlloc, GetFileAttributesW, SetFileAttributesW, FormatMessageW, GetLastError, GetCurrentDirectoryW, LocalFree, WaitForSingleObject, CreateEventW, SetEvent, GlobalAlloc, GlobalFree, ResetEvent, SizeofResource, SearchPathW, GetLocaleInfoEx, FreeResource, OpenProcess, LockResource, LoadLibraryW, LoadResource, FindResourceW, GetWindowsDirectoryW, GetProcAddress, GlobalLock, GlobalUnlock, MulDiv, CreateDirectoryW, FindFirstFileW, GetCommandLineW, SetErrorMode, FindClose, GetUserPreferredUILanguages, FindFirstChangeNotificationW, GetVersion, ResolveLocaleName, GlobalSize, FileTimeToSystemTime, FindCloseChangeNotification, LoadLibraryA, FileTimeToLocalFileTime, FindNextChangeNotification, SetCurrentDirectoryW, GetTimeFormatW, ExitProcess, VerSetConditionMask, CopyFileW, VerifyVersionInfoW, GetDateFormatW, MapViewOfFile, CreateFileMappingW, LocaleNameToLCID, FindResourceExW, LCIDToLocaleName, UnmapViewOfFile, GetVersionExW, GetLocaleInfoW, GetUserDefaultUILanguage, GetSystemDefaultUILanguage, SetLastError, UnhandledExceptionFilter, GetConsoleOutputCP, HeapReAlloc, HeapSize, SetFilePointerEx, GetFileSizeEx, GetStringTypeW, SetStdHandle, OutputDebugStringW, SetConsoleCtrlHandler, GetProcessHeap, SetEnvironmentVariableW, FreeEnvironmentStringsW, GetEnvironmentStringsW, GetCommandLineA, GetCPInfo, GetOEMCP, GetACP, IsValidCodePage, FindNextFileW, FindFirstFileExW, EnumSystemLocalesW, GetUserDefaultLCID, IsValidLocale, LCMapStringW, CompareStringW, GetFileType, HeapAlloc, HeapFree, GetCurrentThread, GetStdHandle, GetModuleHandleExW, FreeLibraryAndExitThread, ResumeThread, ExitThread, CreateThread, TlsFree, TlsSetValue, TlsGetValue, TlsAlloc, EncodePointer, InterlockedFlushSList, InterlockedPushEntrySList, RtlUnwind, InitializeSListHead, GetSystemTimeAsFileTime, GetCurrentThreadId, GetCurrentProcessId, QueryPerformanceCounter, GetStartupInfoW, IsDebuggerPresent, IsProcessorFeaturePresent, TerminateProcess, GetCurrentProcess, SetUnhandledExceptionFilter, WriteConsoleW |
| GDI32.dll | GetStockObject, SetBkColor, ExtTextOutW, EnumFontsW, GetDeviceCaps, SetTextColor, GetObjectW, DeleteObject, CreateSolidBrush, CreateFontIndirectW |
| COMDLG32.dll | GetSaveFileNameW, ChooseColorW, GetOpenFileNameW |
| ADVAPI32.dll | RegOpenKeyExW, RegQueryValueExW, RegCloseKey |
| SHELL32.dll | SHGetFolderPathW, SHGetSpecialFolderPathW, ShellExecuteW, SHCreateDirectoryExW, SHFileOperationW, SHBrowseForFolderW, SHGetSpecialFolderLocation, ShellExecuteExW, SHGetPathFromIDListW, SHGetFileInfoW, SHGetDesktopFolder, SHAppBarMessage, DragQueryFileW, Shell_NotifyIconW, DragAcceptFiles, DragFinish, SHGetDataFromIDListW |
| ole32.dll | OleUninitialize, CoCreateInstance, OleInitialize, CoUninitialize, CoTaskMemAlloc, CoTaskMemFree, CoInitialize, DoDragDrop |
| ntdll.dll | RtlGetNtVersionNumbers |
| COMCTL32.dll | ImageList_AddMasked, InitCommonControlsEx, ImageList_Create, ImageList_Destroy, PropertySheetW |

**Possible Origin**

| Language of compilation system | Country where language is spoken | Map |
|---|---|---|
| English | United States |  |

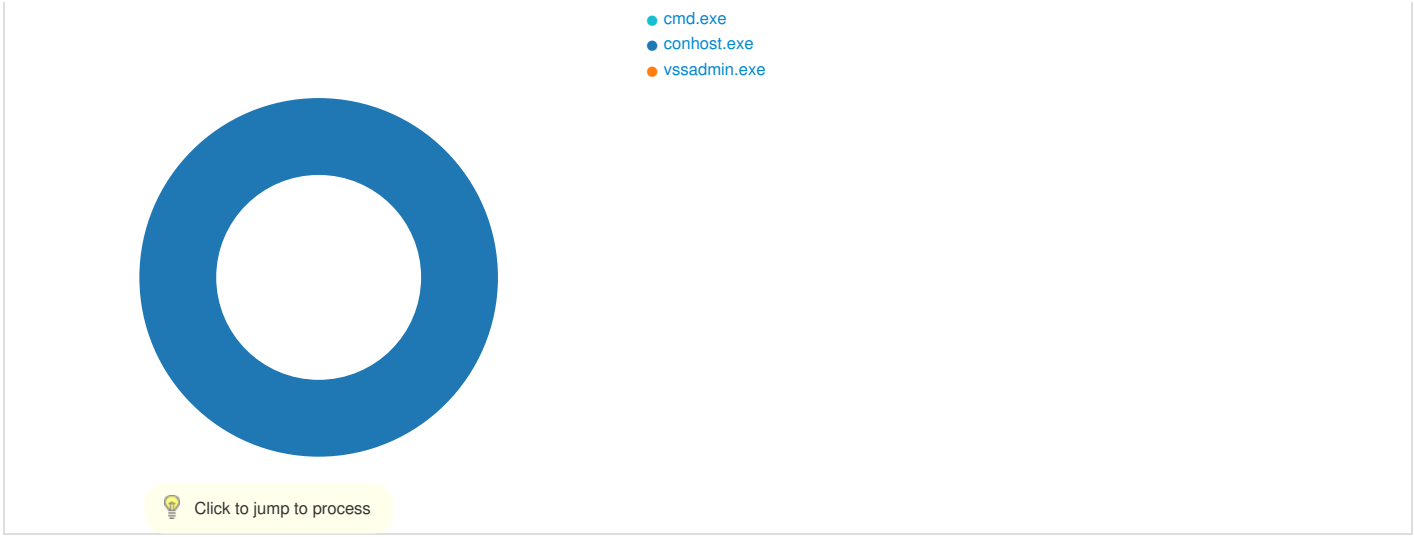
# Network Behavior

No network behavior found

# Statistics

## Behavior

- HkObDPju6Z.exe
- cmd.exe
- conhost.exe
- vssadmin.exe
- HkObDPju6Z.exe
- HkObDPju6Z.exe
- cmd.exe
- conhost.exe
- vssadmin.exe




# System Behavior

## Analysis Process: HkObDPju6Z.exe PID: 6028, Parent PID: 3452

### General

| | |
|---|---|
| Target ID: | 0 |
| Start time: | 21:16:58 |
| Start date: | 12/06/2023 |
| Path: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| Imagebase: | 0x1f0000 |
| File size: | 1489920 bytes |
| MD5 hash: | 6441D7260944BCEDC5958C5C8A05D16D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_BlackBasta, Description: Yara detected BlackBasta ransomware, Source: 00000000.00000003.371931160.00000000034E0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security |
| Reputation: | low |

### File Activities

### Registry Activities

#### Key Created

| Key Path | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|
| HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.7878kr5jx | success or wait | 1 | 35CE004 | RegCreateKeyExW |
| HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.7878kr5jx\DefaultIcon | success or wait | 1 | 35CE004 | RegCreateKeyExW |

#### Key Value Created

| Key Path | Name | Type | Data | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|
| HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.7878kr5jx\DefaultIcon | NULL | unicode | C:\Users\user\AppData\Local\Temp\fkdjsadasd.ico | success or wait | 1 | 35CE032 | RegSetValueExW |
| HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run | Skype | unicode | C:\Users\user\Desktop\HkObDPju6Z.exe | success or wait | 1 | 35E1AC7 | RegSetValueExW |

| Key Path | Name | Type | Old Data | New Data | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|

## Analysis Process: cmd.exe PID: **4148**, Parent PID: **6028**

| General | |
|---|---|
| Target ID: | 1 |
| Start time: | 21:17:06 |
| Start date: | 12/06/2023 |
| Path: | C:\Windows\SysWOW64\cmd.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\system32\cmd.exe /c C:\Windows\SysNative\vssadmin.exe delete shadows /all /quiet |
| Imagebase: | 0xb0000 |
| File size: | 232960 bytes |
| MD5 hash: | F3BDBE3BB6F734E357235F4D5898582D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

**File Activities**

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

## Analysis Process: conhost.exe PID: **1572**, Parent PID: **4148**

| General | |
|---|---|
| Target ID: | 2 |
| Start time: | 21:17:06 |
| Start date: | 12/06/2023 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff745070000 |
| File size: | 625664 bytes |
| MD5 hash: | EA777DEEA782E8B4D7C7C33BBF8A4496 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

## Analysis Process: vssadmin.exe PID: **7056**, Parent PID: **4148**

| General | |
|---|---|
| Target ID: | 3 |
| Start time: | 21:17:06 |
| Start date: | 12/06/2023 |
| Path: | C:\Windows\System32\vssadmin.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\SysNative\vssadmin.exe  delete shadows /all /quiet |
| Imagebase: | 0x7ff6484d0000 |
| File size: | 145920 bytes |
| MD5 hash: | 47D51216EF45075B5F7EAA117CC70E40 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

### File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

## Analysis Process: HkObDPju6Z.exe PID: 7028, Parent PID: 3452

### General

| | |
|---|---|
| Target ID: | 6 |
| Start time: | 21:17:17 |
| Start date: | 12/06/2023 |
| Path: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| Wow64 process (32bit): | true |
| Commandline: | "C:\Users\user\Desktop\HkObDPju6Z.exe" |
| Imagebase: | 0x1f0000 |
| File size: | 1489920 bytes |
| MD5 hash: | 6441D7260944BCEDC5958C5C8A05D16D |
| Has elevated privileges: | false |
| Has administrator privileges: | false |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_BlackBasta, Description: Yara detected BlackBasta ransomware, Source: 00000006.00000002.463365199.0000000003600000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security |
| Reputation: | low |

### File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

## Analysis Process: HkObDPju6Z.exe PID: 4652, Parent PID: 3452

### General

| | |
|---|---|
| Target ID: | 8 |
| Start time: | 21:17:26 |
| Start date: | 12/06/2023 |
| Path: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| Wow64 process (32bit): | true |
| Commandline: | "C:\Users\user\Desktop\HkObDPju6Z.exe" |
| Imagebase: | 0x1f0000 |
| File size: | 1489920 bytes |
| MD5 hash: | 6441D7260944BCEDC5958C5C8A05D16D |
| Has elevated privileges: | false |
| Has administrator privileges: | false |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_BlackBasta, Description: Yara detected BlackBasta ransomware, Source: 00000008.00000002.477620370.0000000003220000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security |
| Reputation: | low |

### File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

## Analysis Process: cmd.exe PID: 1852, Parent PID: 7028

### General

| | |
|---|---|
| Target ID: | 10 |

| | |
|---|---|
| Start time: | 21:17:40 |
| Start date: | 12/06/2023 |
| Path: | C:\Windows\SysWOW64\cmd.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\system32\cmd.exe /c C:\Windows\SysNative\vssadmin.exe delete shadows /all /quiet |
| Imagebase: | 0xb0000 |
| File size: | 232960 bytes |
| MD5 hash: | F3BDBE3BB6F734E357235F4D5898582D |
| Has elevated privileges: | false |
| Has administrator privileges: | false |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

**File Activities**

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

## Analysis Process: conhost.exe PID: **6824**, Parent PID: **1852**

**General**

| | |
|---|---|
| Target ID: | 11 |
| Start time: | 21:17:40 |
| Start date: | 12/06/2023 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff745070000 |
| File size: | 625664 bytes |
| MD5 hash: | EA777DEEA782E8B4D7C7C33BBF8A4496 |
| Has elevated privileges: | false |
| Has administrator privileges: | false |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

## Analysis Process: vssadmin.exe PID: **6840**, Parent PID: **1852**

**General**

| | |
|---|---|
| Target ID: | 12 |
| Start time: | 21:17:42 |
| Start date: | 12/06/2023 |
| Path: | C:\Windows\System32\vssadmin.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\SysNative\vssadmin.exe delete shadows /all /quiet |
| Imagebase: | 0x7ff6484d0000 |
| File size: | 145920 bytes |
| MD5 hash: | 47D51216EF45075B5F7EAA117CC70E40 |
| Has elevated privileges: | false |
| Has administrator privileges: | false |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

**File Activities**

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

## Analysis Process: cmd.exe PID: **5708**, Parent PID: **4652**

| General | |
|---|---|
| Target ID: | 13 |
| Start time: | 21:17:47 |
| Start date: | 12/06/2023 |
| Path: | C:\Windows\SysWOW64\cmd.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\system32\cmd.exe /c C:\Windows\SysNative\vssadmin.exe delete shadows /all /quiet |
| Imagebase: | 0xb0000 |
| File size: | 232960 bytes |
| MD5 hash: | F3BDBE3BB6F734E357235F4D5898582D |
| Has elevated privileges: | false |
| Has administrator privileges: | false |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

### File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

## Analysis Process: conhost.exe PID: **5688**, Parent PID: **5708**

| General | |
|---|---|
| Target ID: | 14 |
| Start time: | 21:17:47 |
| Start date: | 12/06/2023 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff745070000 |
| File size: | 625664 bytes |
| MD5 hash: | EA777DEEA782E8B4D7C7C33BBF8A4496 |
| Has elevated privileges: | false |
| Has administrator privileges: | false |
| Programmed in: | C, C++ or other language |

## Analysis Process: vssadmin.exe PID: **5700**, Parent PID: **5708**

| General | |
|---|---|
| Target ID: | 15 |
| Start time: | 21:17:48 |
| Start date: | 12/06/2023 |
| Path: | C:\Windows\System32\vssadmin.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\SysNative\vssadmin.exe  delete shadows /all /quiet |
| Imagebase: | 0x7ff6484d0000 |
| File size: | 145920 bytes |
| MD5 hash: | 47D51216EF45075B5F7EAA117CC70E40 |
| Has elevated privileges: | false |
| Has administrator privileges: | false |
| Programmed in: | C, C++ or other language |

### File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

## Disassembly

No disassembly