

JOESandbox Cloud BASIC



ID: 719511

Sample Name:

diatomaceous.dat.dll

Cookbook: default.jbs

Time: 17:03:44

Date: 10/10/2022

Version: 36.0.0 Rainbow Opal

Table of Contents

| | |
|--|----|
| Table of Contents | 2 |
| Windows Analysis Report diatomaceous.dat.dll | 4 |
| Overview | 4 |
| General Information | 4 |
| Detection | 4 |
| Signatures | 4 |
| Classification | 4 |
| Process Tree | 4 |
| Malware Configuration | 4 |
| Threatname: Qbot | 4 |
| Yara Signatures | 5 |
| Memory Dumps | 5 |
| Unpacked PEs | 5 |
| Sigma Signatures | 6 |
| Data Obfuscation | 6 |
| Snort Signatures | 6 |
| Joe Sandbox Signatures | 6 |
| AV Detection | 6 |
| System Summary | 6 |
| Hooking and other Techniques for Hiding and Protection | 6 |
| Malware Analysis System Evasion | 6 |
| HIPS / PFW / Operating System Protection Evasion | 6 |
| Stealing of Sensitive Information | 7 |
| Remote Access Functionality | 7 |
| Mitre Att&ck Matrix | 7 |
| Behavior Graph | 7 |
| Screenshots | 8 |
| Thumbnails | 8 |
| Antivirus, Machine Learning and Genetic Malware Detection | 9 |
| Initial Sample | 9 |
| Dropped Files | 9 |
| Unpacked PE Files | 9 |
| Domains | 10 |
| URLs | 10 |
| Domains and IPs | 10 |
| Contacted Domains | 10 |
| World Map of Contacted IPs | 10 |
| General Information | 10 |
| Warnings | 11 |
| Simulations | 11 |
| Behavior and APIs | 11 |
| Joe Sandbox View / Context | 11 |
| IPs | 11 |
| Domains | 11 |
| ASNs | 11 |
| JA3 Fingerprints | 11 |
| Dropped Files | 11 |
| Created / dropped Files | 11 |
| C:\Users\user\Desktop\diatomaceous.dat.dll | 11 |
| Static File Info | 12 |
| General | 12 |
| File Icon | 12 |
| Static PE Info | 12 |
| General | 12 |
| Entrypoint Preview | 12 |
| Data Directories | 14 |
| Sections | 14 |
| Resources | 14 |
| Imports | 15 |
| Exports | 15 |
| Possible Origin | 15 |
| Network Behavior | 15 |
| Statistics | 16 |
| Behavior | 16 |
| System Behavior | 16 |
| Analysis Process: loaddll32.exePID: 5992, Parent PID: 3528 | 16 |
| General | 16 |
| File Activities | 16 |
| Analysis Process: conhost.exePID: 6064, Parent PID: 5992 | 16 |
| General | 16 |
| Analysis Process: cmd.exePID: 6116, Parent PID: 5992 | 17 |
| General | 17 |
| File Activities | 17 |

| | |
|---|----|
| Analysis Process: regsvr32.exePID: 6096, Parent PID: 5992 | 17 |
| General | 17 |
| File Activities | 17 |
| File Read | 17 |
| Analysis Process: rundll32.exePID: 244, Parent PID: 6116 | 18 |
| General | 18 |
| File Activities | 18 |
| File Read | 18 |
| Analysis Process: rundll32.exePID: 3908, Parent PID: 5992 | 18 |
| General | 18 |
| File Activities | 18 |
| File Read | 19 |
| Analysis Process: rundll32.exePID: 1540, Parent PID: 5992 | 19 |
| General | 19 |
| Analysis Process: wermgr.exePID: 5020, Parent PID: 6096 | 19 |
| General | 19 |
| File Activities | 19 |
| File Created | 19 |
| File Written | 19 |
| File Read | 20 |
| Registry Activities | 20 |
| Key Created | 20 |
| Key Value Created | 20 |
| Key Value Modified | 21 |
| Analysis Process: wermgr.exePID: 4860, Parent PID: 3908 | 21 |
| General | 21 |
| File Activities | 22 |
| File Written | 22 |
| File Read | 22 |
| Analysis Process: wermgr.exePID: 4768, Parent PID: 244 | 22 |
| General | 22 |
| File Activities | 23 |
| File Written | 23 |
| File Read | 23 |
| Disassembly | 23 |

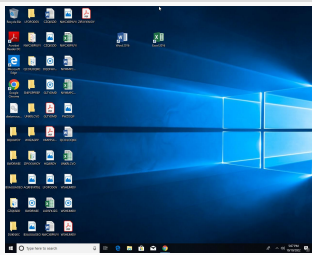
Windows Analysis Report

diatomaceous.dat.dll

Overview

General Information

| | |
|--------------|----------------------|
| Sample Name: | diatomaceous.dat.dll |
| Analysis ID: | 719511 |
| MD5: | 2e7f90e0c595d8.. |
| SHA1: | 8ff540ba601429c.. |
| SHA256: | e3a2c056c73066.. |
| Tags: | dll |
| Infos: | |



Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

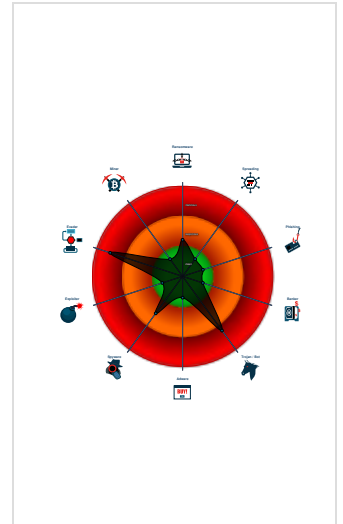
Qbot

| | |
|--------------|---------|
| Score: | 96 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 100% |

Signatures

- Yara detected Qbot
- Multi AV Scanner detection for subm...
- Malicious sample detected (through...
- Sigma detected: Execute DLL with s...
- Maps a DLL or memory area into an...
- Overwrites code with unconditional j...
- Writes to foreign memory regions
- Tries to detect sandboxes and other...
- Machine Learning detection for sam...
- Allocates memory in foreign process...
- Uses 32bit PE files
- Queries the volume information (nam...

Classification



Process Tree

- System is w10x64
- loadll32.exe (PID: 5992 cmdline: loadll32.exe "C:\Users\user\Desktop\diatomaceous.dat.dll" MD5: 1F562FBF37040EC6C43C8D5EF619EA39)
 - conhost.exe (PID: 6064 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
 - cmd.exe (PID: 6116 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\diatomaceous.dat.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
 - rundll32.exe (PID: 244 cmdline: rundll32.exe "C:\Users\user\Desktop\diatomaceous.dat.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
 - wermgr.exe (PID: 4768 cmdline: C:\Windows\SysWOW64\wermgr.exe MD5: CCF15E662ED5CE77B5FF1A7AAE305233)
 - regsvr32.exe (PID: 6096 cmdline: regsvr32.exe /s C:\Users\user\Desktop\diatomaceous.dat.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
 - wermgr.exe (PID: 5020 cmdline: C:\Windows\SysWOW64\wermgr.exe MD5: CCF15E662ED5CE77B5FF1A7AAE305233)
 - rundll32.exe (PID: 3908 cmdline: rundll32.exe C:\Users\user\Desktop\diatomaceous.dat.dll,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
 - wermgr.exe (PID: 4860 cmdline: C:\Windows\SysWOW64\wermgr.exe MD5: CCF15E662ED5CE77B5FF1A7AAE305233)
 - rundll32.exe (PID: 1540 cmdline: rundll32.exe C:\Users\user\Desktop\diatomaceous.dat.dll,DllUnregisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- cleanup

Malware Configuration

Threatname: Qbot

```

{
  "Bot id": "BB",
  "Campaign": "1664535088",
  "Version": "403.902",
  "C2 list": [
    "41.107.71.201:443",
    "105.101.230.16:443",
    "105.108.239.60:443",
    "196.64.227.5:8443",
    "41.249.158.221:995",
    "134.35.14.5:443",
    "113.170.117.251:443",
    "187.193.219.248:443",
    "122.166.244.116:443",
    "154.237.129.123:995",
    "41.98.229.81:443",
    "186.48.199.243:995",
    "102.156.3.13:443",
    "41.97.190.189:443",
    "197.207.191.164:443",
    "105.184.14.132:995",
    "196.207.146.151:443",
    "105.158.113.15:443",
    "196.89.42.89:995",
    "86.98.156.229:993",
    "177.174.119.195:32101",
    "81.156.194.147:2078",
    "80.253.189.55:443",
    "197.49.175.67:995",
    "177.45.78.52:993",
    "89.187.169.77:443",
    "196.92.59.242:995",
    "41.13.200.19:443",
    "41.97.195.237:443",
    "92.191.56.11:2222",
    "154.70.53.202:443",
    "210.186.37.98:50002"
  ]
}

```

Yara Signatures

Memory Dumps

| Source | Rule | Description | Author | Strings |
|--|------------------------------|--------------------|--------------|---|
| 00000004.00000003.312922602.0000000002FA0000.0000004.00000800.00020000.00000000.sdmp | JoeSecurity_Qbot_1 | Yara detected Qbot | Joe Security | |
| 00000004.00000003.312922602.0000000002FA0000.0000004.00000800.00020000.00000000.sdmp | Windows_Trojan_Qbot_92c67a6d | unknown | unknown | <ul style="list-style-type: none"> 0x1034f:\$a: 33 C0 59 85 F6 74 2D 83 66 0C 00 40 89 06 6A 20 89 46 04 C7 46 08 08 00 |
| 00000004.00000003.312922602.0000000002FA0000.0000004.00000800.00020000.00000000.sdmp | Windows_Trojan_Qbot_3074a8d4 | unknown | unknown | <ul style="list-style-type: none"> 0x1ba14:\$a4: %u;%u;%u; 0x1bf50:\$a5: %u.%u.%u.%u.%u.%u.%04x 0x1bdd8:\$a6: %u&%s&%u 0x80c6:\$get_string1: 33 D2 8B C6 6A 5A 5F F7 F7 8B 7D 08 8A 04 3A 8B 55 F8 8B 7D 10 3A 04 16 0x8404:\$set_key: 8D 87 00 04 00 00 50 56 E8 BF 15 00 00 59 8B D0 8B CE E8 0x2730:\$do_computer_use_russian_like_keyboard: B9 F F 03 00 00 66 23 C1 33 C9 0F B7 F8 66 3B 7C 4D 0x2187:\$execute_each_tasks: 8B 44 0E 0C 85 C0 74 04 FF D0 EB 12 6A 00 6A 00 6A 00 FF 74 0E 08 E8 F5 EF F F FF 83 C4 10 0xbcee:\$generate_random_alpha_num_string: 57 E8 DC DC FF FF 48 50 8D 85 30 F6 FF FF 6A 00 50 E8 D1 6D 0 0 00 8B 4D F8 83 C4 10 8A 04 38 88 04 0E 46 83 FE 0C |
| 00000005.00000003.313259350.000000000B90000.0000004.00000800.00020000.00000000.sdmp | JoeSecurity_Qbot_1 | Yara detected Qbot | Joe Security | |
| 00000005.00000003.313259350.000000000B90000.0000004.00000800.00020000.00000000.sdmp | Windows_Trojan_Qbot_92c67a6d | unknown | unknown | <ul style="list-style-type: none"> 0x1034f:\$a: 33 C0 59 85 F6 74 2D 83 66 0C 00 40 89 06 6A 20 89 46 04 C7 46 08 08 00 |

Click to see the 28 entries

Unpacked PEs

| Source | Rule | Description | Author | Strings |
|------------------------------------|------------------------------|--------------------|--------------|--|
| 8.0.wermgr.exe.e00000.0.raw.unpack | JoeSecurity_Qbot_1 | Yara detected Qbot | Joe Security | |
| 8.0.wermgr.exe.e00000.0.raw.unpack | Windows_Trojan_Qbot_92c67a6d | unknown | unknown | <ul style="list-style-type: none"> 0x10f4f:\$a: 33 C0 59 85 F6 74 2D 83 66 0C 00 40 89 06 6A 20 89 46 04 C7 46 08 08 00 |

| Source | Rule | Description | Author | Strings |
|---------------------------------------|------------------------------|--------------------|--------------|---|
| 8.0.wermgr.exe.e00000.0.raw.unpack | Windows_Trojan_Qbot_3074a8d4 | unknown | unknown | <ul style="list-style-type: none"> 0x1ca14:\$a4: %u;%u;%u; 0x1cf50:\$a5: %u.%u.%u.%u.%u.%u.%04x 0x1cdd8:\$a6: %u&%s&%u 0x8cc6:\$get_string1: 33 D2 8B C6 6A 5A 5F F7 F7 8B 7D 08 8A 04 3A 8B 55 F8 8B 7D 10 3A 04 16 0x9004:\$set_key: 8D 87 00 04 00 00 50 56 E8 BF 15 00 00 59 8B D0 8B CE E8 0x3330:\$do_computer_use_russian_like_keyboard: B9 F F 03 00 00 66 23 C1 33 C9 0F B7 F8 66 3B 7C 4D 0x2d87:\$execute_each_tasks: 8B 44 0E 0C 85 C0 74 04 FF D0 EB 12 6A 00 6A 00 6A 00 FF 74 0E 08 E8 F5 EF F F FF 83 C4 10 0xc8ee:\$generate_random_alpha_num_string: 57 E8 DC DC FF FF 48 50 8D 85 30 F6 FF FF 6A 00 50 E8 D1 6D 0 0 00 8B 4D F8 83 C4 10 8A 04 38 88 04 0E 46 83 FE 0C |
| 4.2.rundll32.exe.4820000.1.raw.unpack | JoeSecurity_Qbot_1 | Yara detected Qbot | Joe Security | |
| 4.2.rundll32.exe.4820000.1.raw.unpack | Windows_Trojan_Qbot_92c67a6d | unknown | unknown | <ul style="list-style-type: none"> 0x10f4f:\$a: 33 C0 59 85 F6 74 2D 83 66 0C 00 40 89 06 6A 20 89 46 04 C7 46 08 08 00 |

Click to see the 61 entries

Sigma Signatures

Data Obfuscation



Sigma detected: Execute DLL with spoofed extension

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection



Multi AV Scanner detection for submitted file

Machine Learning detection for sample

System Summary



Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection



Overwrites code with unconditional jumps - possibly settings hooks in foreign process

Malware Analysis System Evasion



Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion



Maps a DLL or memory area into another process

Writes to foreign memory regions

Stealing of Sensitive Information



Yara detected Qbot

Remote Access Functionality

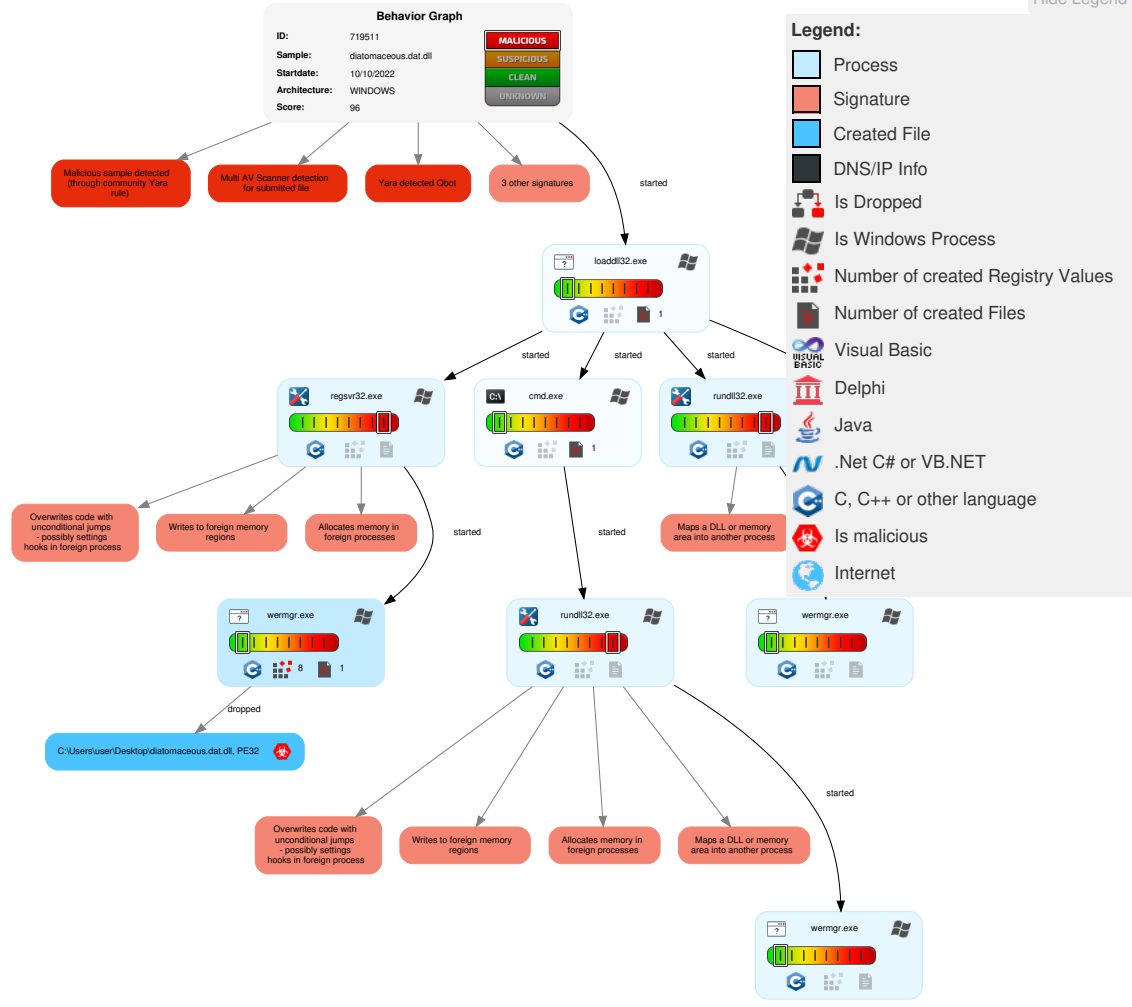


Yara detected Qbot

Mitre Att&ck Matrix

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Network Effects | Remote Service Effects | Impact |
|-------------------------------------|-----------------------------------|--------------------------------------|----------------------------|--|-----------------------------|-------------------------------------|------------------------------------|-----------------------------|---|----------------------------|---|---|--|
| Valid Accounts | 3 Native API | 1 DLL Side-Loading | 3 1 1 Process Injection | 1 Masquerading | 1 Credential API Hooking | 1 System Time Discovery | Remote Services | 1 Screen Capture | Exfiltration Over Other Network Medium | 2 Encrypted Channel | Eavesdrop on Insecure Network Communication | Remotely Track Device Without Authorization | Modify System Partition |
| Default Accounts | Scheduled Task/Job | Boot or Logon Initialization Scripts | 1 DLL Side-Loading | 2 Virtualization/Sandbox Evasion | LSASS Memory | 1 4 Security Software Discovery | Remote Desktop Protocol | 1 Credential API Hooking | Exfiltration Over Bluetooth | Junk Data | Exploit SS7 to Redirect Phone Calls/SMS | Remotely Wipe Data Without Authorization | Device Lockout |
| Domain Accounts | At (Linux) | Logon Script (Windows) | Logon Script (Windows) | 3 1 1 Process Injection | Security Account Manager | 2 Virtualization/Sandbox Evasion | SMB/Windows Admin Shares | 1 Archive Collected Data | Automated Exfiltration | Steganography | Exploit SS7 to Track Device Location | Obtain Device Cloud Backups | Delete Device Data |
| Local Accounts | At (Windows) | Logon Script (Mac) | Logon Script (Mac) | 1 Deobfuscate/Decode Files or Information | NTDS | 2 Process Discovery | Distributed Component Object Model | Input Capture | Scheduled Transfer | Protocol Impersonation | SIM Card Swap | | Carrier Billing Fraud |
| Cloud Accounts | Cron | Network Logon Script | Network Logon Script | 2 Obfuscated Files or Information | LSA Secrets | 1 File and Directory Discovery | SSH | Keylogging | Data Transfer Size Limits | Fallback Channels | Manipulate Device Communication | | Manipulate App Store Rankings or Ratings |
| Replication Through Removable Media | Launchd | Rc.common | Rc.common | 1 Regsvr32 | Cached Domain Credentials | 3 5 System Information Discovery | VNC | GUI Input Capture | Exfiltration Over C2 Channel | Multiband Communication | Jamming or Denial of Service | | Abuse Accessibility Features |
| External Remote Services | Scheduled Task | Startup Items | Startup Items | 1 Rundll32 | DCSync | Network Sniffing | Windows Remote Management | Web Portal Capture | Exfiltration Over Alternative Protocol | Commonly Used Port | Rogue Wi-Fi Access Points | | Data Encrypted for Impact |
| Drive-by Compromise | Command and Scripting Interpreter | Scheduled Task/Job | Scheduled Task/Job | 1 DLL Side-Loading | Proc Filesystem | Network Service Scanning | Shared Webroot | Credential API Hooking | Exfiltration Over Symmetric Encrypted Non-C2 Protocol | Application Layer Protocol | Downgrade to Insecure Protocols | | Generate Fraudulent Advertising Revenue |

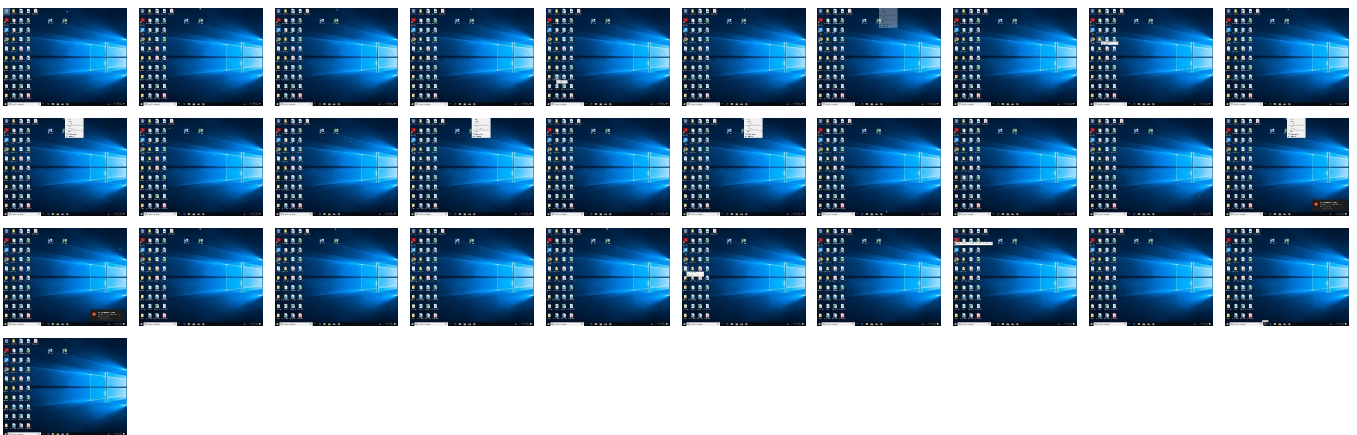
Behavior Graph



Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

| Source | Detection | Scanner | Label | Link |
|----------------------|-----------|----------------|----------------------------|------------------------|
| diatomaceous.dat.dll | 73% | ReversingLabs | Win32.Backdoor.Q uakbot | |
| diatomaceous.dat.dll | 77% | Virustotal | | Browse |
| diatomaceous.dat.dll | 44% | Metadefender | | Browse |
| diatomaceous.dat.dll | 100% | Joe Sandbox ML | | |

Dropped Files


| Source | Detection | Scanner | Label | Link |
|--|-----------|---------------|-------|------------------------|
| C:\Users\user\Desktop\diatomaceous.dat.dll | 3% | Virustotal | | Browse |
| C:\Users\user\Desktop\diatomaceous.dat.dll | 4% | ReversingLabs | | |
| C:\Users\user\Desktop\diatomaceous.dat.dll | NaN% | Metadefender | | Browse |

Unpacked PE Files

| Source | Detection | Scanner | Label | Link | Download |
|--------------------------------|-----------|---------|-----------------------|------|-------------------------------|
| 8.2.wermgr.exe.e00000.0.unpack | 100% | Avira | HEUR/AGEN.12 34562 | | Download File |
| 9.0.wermgr.exe.e00000.0.unpack | 100% | Avira | HEUR/AGEN.12 34562 | | Download File |

| Source | Detection | Scanner | Label | Link | Download |
|-----------------------------------|-----------|---------|-----------------------|------|-------------------------------|
| 5.2.rundll32.exe.2cc0000.1.unpack | 100% | Avira | HEUR/AGEN.12 34562 | | Download File |
| 9.2.wermgr.exe.e00000.0.unpack | 100% | Avira | HEUR/AGEN.12 34562 | | Download File |
| 8.0.wermgr.exe.e00000.0.unpack | 100% | Avira | HEUR/AGEN.12 34562 | | Download File |
| 3.2.regsvr32.exe.730000.1.unpack | 100% | Avira | HEUR/AGEN.12 34562 | | Download File |
| 7.0.wermgr.exe.1000000.0.unpack | 100% | Avira | HEUR/AGEN.12 34562 | | Download File |
| 4.2.rundll32.exe.4820000.1.unpack | 100% | Avira | HEUR/AGEN.12 34562 | | Download File |

Domains

 No Antivirus matches

URLs

 No Antivirus matches

Domains and IPs

Contacted Domains

 No contacted domains info

World Map of Contacted IPs

 No contacted IP infos

General Information

| | |
|--|---|
| Joe Sandbox Version: | 36.0.0 Rainbow Opal |
| Analysis ID: | 719511 |
| Start date and time: | 2022-10-10 17:03:44 +02:00 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 9m 22s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | diatomaceous.dat.dll |
| Cookbook file name: | default.jbs |
| Analysis system description: | Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211 |
| Run name: | Run with higher sleep bypass |
| Number of analysed new started processes analysed: | 15 |
| 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: | <ul style="list-style-type: none"> • HCA enabled • EGA enabled • HDC enabled • AMSI enabled |
| Analysis Mode: | default |
| Analysis stop reason: | Timeout |
| Detection: | MAL |
| Classification: | mal96.troj.evad.winDLL@18/1@0/0 |
| EGA Information: | <ul style="list-style-type: none"> • Successful, ratio: 100% |


| | |
|--------------------|---|
| HDC Information: | <ul style="list-style-type: none"> • Successful, ratio: 73.2% (good quality ratio 68.1%) • Quality average: 75.3% • Quality standard deviation: 29.8% |
| HCA Information: | <ul style="list-style-type: none"> • Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0 |
| Cookbook Comments: | <ul style="list-style-type: none"> • Found application associated with file extension: .dll • Sleeps bigger than 10000000ms are automatically reduced to 1000ms |

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe
- Not all processes were analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.


Simulations

Behavior and APIs


 No simulations

Joe Sandbox View / Context


IPs

 No context


Domains

 No context


ASNs

 No context



JA3 Fingerprints

 No context

Dropped Files

 No context

Created / dropped Files

C:\Users\user\Desktop\diatomaceous.dat.dll  

| | |
|-----------------|---|
| Process: | C:\Windows\SysWOW64\wermgr.exe |
| File Type: | PE32 executable (DLL) (console) Intel 80386, for MS Windows |
| Category: | dropped |
| Size (bytes): | 4096 |
| Entropy (8bit): | 4.5939701639198445 |
| Encrypted: | false |
| SSDEEP: | 48:LtlEsYew8vL36I8LgS72DsOA1dyqQrD1tXPFJhspwAOY5iRYgZX0dB1mkK52wRa:aesqt2Dk1dyqIF9JhsLwAOhf2ZW2wiPD |
| MD5: | C79A1334A3C60DACEE5E43B715236A17 |
| SHA1: | 825F4CA853E99E10B81ABE84A1EB2CB6CFD3E8E7 |
| SHA-256: | F892742F6C64A8991337FADDF84FBDB25C43022AC85C8BCC30D47FEBAFE1D87 |

| Instruction |
|------------------------------------|
| push ebp |
| mov ebp, esp |
| cmp dword ptr [ebp+0Ch], 01h |
| jne 00007F6C94BF9CF7h |
| call 00007F6C94BFA1B2h |
| push dword ptr [ebp+10h] |
| push dword ptr [ebp+0Ch] |
| push dword ptr [ebp+08h] |
| call 00007F6C94BF9BA3h |
| add esp, 0Ch |
| pop ebp |
| retn 000Ch |
| cmp ecx, dword ptr [10033014h] |
| jne 00007F6C94BF9CF3h |
| ret |
| jmp 00007F6C94BFA29Bh |
| mov ecx, dword ptr [ebp-0Ch] |
| mov dword ptr fs:[00000000h], ecx |
| pop ecx |
| pop edi |
| pop edi |
| pop esi |
| pop ebx |
| mov esp, ebp |
| pop ebp |
| push ecx |
| ret |
| push eax |
| push dword ptr fs:[00000000h] |
| lea eax, dword ptr [esp+0Ch] |
| sub esp, dword ptr [esp+0Ch] |
| push ebx |
| push esi |
| push edi |
| mov dword ptr [eax], ebp |
| mov ebp, eax |
| mov eax, dword ptr [10033014h] |
| xor eax, ebp |
| push eax |
| push dword ptr [ebp-04h] |
| mov dword ptr [ebp-04h], FFFFFFFFh |
| lea eax, dword ptr [ebp-0Ch] |
| mov dword ptr fs:[00000000h], eax |
| ret |
| push eax |
| push dword ptr fs:[00000000h] |
| lea eax, dword ptr [esp+0Ch] |
| sub esp, dword ptr [esp+0Ch] |
| push ebx |
| push esi |
| push edi |
| mov dword ptr [eax], ebp |
| mov ebp, eax |
| mov eax, dword ptr [10033014h] |
| xor eax, ebp |
| push eax |
| mov dword ptr [ebp-10h], esp |
| push dword ptr [ebp-04h] |
| mov dword ptr [ebp-04h], FFFFFFFFh |

| Instruction |
|-----------------------------------|
| lea eax, dword ptr [ebp-0Ch] |
| mov dword ptr fs:[00000000h], eax |
| ret |
| int3 |
| int3 |
| int3 |
| int3 |
| push ecx |
| lea ecx, dword ptr [esp+08h] |
| sub ecx, eax |
| and ecx, 0Fh |
| add eax, ecx |
| sbb ecx, ecx |
| or eax, ecx |
| pop ecx |
| jmp 00007F6C94BFA3DFh |

| Data Directories | | | |
|--------------------------------------|-----------------|--------------|---------------|
| Name | Virtual Address | Virtual Size | Is in Section |
| IMAGE_DIRECTORY_ENTRY_EXPORT | 0x31800 | 0x6c | .rdata |
| IMAGE_DIRECTORY_ENTRY_IMPORT | 0x3186c | 0x3c | .rdata |
| IMAGE_DIRECTORY_ENTRY_RESOURCE | 0x56000 | 0xb890 | .rsrc |
| IMAGE_DIRECTORY_ENTRY_EXCEPTION | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_SECURITY | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_BASERELOC | 0x62000 | 0x1da8 | .reloc |
| IMAGE_DIRECTORY_ENTRY_DEBUG | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_COPYRIGHT | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_GLOBALPTR | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_TLS | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG | 0x2fb70 | 0x40 | .rdata |
| IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_IAT | 0x24000 | 0x15c | .rdata |
| IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_RESERVED | 0x0 | 0x0 | |



| Sections | | | | | | | | |
|----------|-----------------|--------------|----------|----------|---------------------|---|-------------------|---|
| Name | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy | Characteristics |
| .text | 0x1000 | 0x2215c | 0x22200 | False | 0.555016597985348 | data | 6.649026882960341 | IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ |
| .rdata | 0x24000 | 0xe03c | 0xe200 | False | 0.5316993915929203 | data | 5.664939250342234 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .data | 0x33000 | 0x22ccc | 0x22000 | False | 0.8333668428308824 | DOS executable (block device driver \377\377\377\377\261) | 6.797248626276144 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE |
| .rsrc | 0x56000 | 0xb890 | 0xba00 | False | 0.17794438844086022 | data | 3.888171262767214 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .reloc | 0x62000 | 0x1da8 | 0x1e00 | False | 0.746484375 | data | 6.525986142096821 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ |


| Resources | | | | | |
|-----------|---------|-------|---|----------|---------|
| Name | RVA | Size | Type | Language | Country |
| RT_ICON | 0x56588 | 0xb13 | PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced | Russian | Russia |

| Name | RVA | Size | Type | Language | Country |
|---------------|---------|--------|---|----------|---------------|
| RT_ICON | 0x570a0 | 0xea8 | Device independent bitmap graphic, 48 x 96 x 8, image size 2304, 256 important colors | Russian | Russia |
| RT_ICON | 0x57f48 | 0x8a8 | Device independent bitmap graphic, 32 x 64 x 8, image size 1024, 256 important colors | Russian | Russia |
| RT_ICON | 0x587f0 | 0x568 | Device independent bitmap graphic, 16 x 32 x 8, image size 256, 256 important colors | Russian | Russia |
| RT_ICON | 0x58d58 | 0xc4a | PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced | Russian | Russia |
| RT_ICON | 0x599a8 | 0x4228 | Device independent bitmap graphic, 64 x 128 x 32, image size 16896 | Russian | Russia |
| RT_ICON | 0x5dbd0 | 0x25a8 | Device independent bitmap graphic, 48 x 96 x 32, image size 9600 | Russian | Russia |
| RT_ICON | 0x60178 | 0x10a8 | Device independent bitmap graphic, 32 x 64 x 32, image size 4224 | Russian | Russia |
| RT_ICON | 0x61220 | 0x468 | Device independent bitmap graphic, 16 x 32 x 32, image size 1088 | Russian | Russia |
| RT_GROUP_ICON | 0x61688 | 0x84 | data | Russian | Russia |
| RT_VERSION | 0x562b0 | 0x2d4 | data | Russian | Russia |
| RT_MANIFEST | 0x61710 | 0x17d | XML 1.0 document, ASCII text, with CRLF line terminators | English | United States |

| Imports | |
|--------------|--|
| DLL | Import |
| KERNEL32.dll | Sleep, VirtualAlloc, GetCommandLineA, CreateFileW, GetFileSize, CloseHandle, CreateFileA, LocalAlloc, GetModuleFileNameA, DebugBreak, ReadFile, WideCharToMultiByte, EnterCriticalSection, LeaveCriticalSection, InitializeCriticalSectionEx, DeleteCriticalSection, EncodePointer, DecodePointer, MultiByteToWideChar, LCMapStringEx, GetStringTypeW, GetCPInfo, IsProcessorFeaturePresent, IsDebuggerPresent, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetStartupInfoW, GetModuleHandleW, QueryPerformanceCounter, GetCurrentProcessId, GetCurrentThreadId, GetSystemTimeAsFileTime, InitializeSListHead, GetCurrentProcess, TerminateProcess, RtlUnwind, RaiseException, InterlockedFlushSList, GetLastError, SetLastError, InitializeCriticalSectionAndSpinCount, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, FreeLibrary, GetProcAddress, LoadLibraryExW, ExitProcess, GetModuleHandleExW, GetModuleFileNameW, HeapAlloc, HeapFree, GetStdHandle, GetFileType, LCMapStringW, GetLocaleInfoW, IsValidLocale, GetUserDefaultLCID, EnumSystemLocalesW, HeapReAlloc, FindClose, FindFirstFileExW, FindNextFileW, IsValidCodePage, GetACP, GetOEMCP, GetCommandLineW, GetEnvironmentStringsW, FreeEnvironmentStringsW, GetProcessHeap, SetFilePointerEx, SetStdHandle, HeapSize, FlushFileBuffers, WriteFile, GetConsoleOutputCP, GetConsoleMode, WriteConsoleW |
| ADVAPI32.dll | CryptCreateHash, CryptHashData, CryptDestroyHash, CryptGetHashParam, CryptReleaseContext, CryptAcquireContextA |

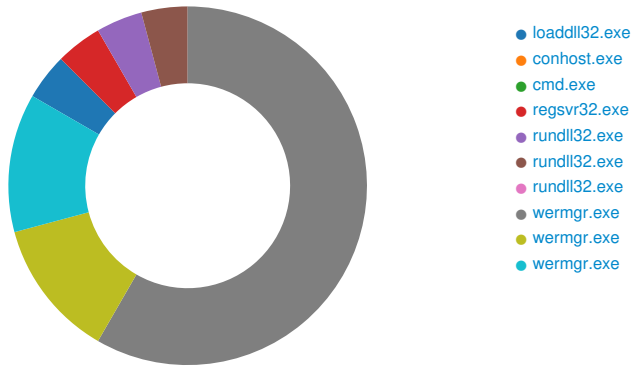
| Exports | | |
|---------------------|---------|------------|
| Name | Ordinal | Address |
| DllRegisterServer | 1 | 0x10006510 |
| DllUnregisterServer | 2 | 0x10007d50 |


| Possible Origin | | |
|--------------------------------|----------------------------------|---|
| Language of compilation system | Country where language is spoken | Map |
| Russian | Russia |  |
| English | United States |  |

| Network Behavior |
|---|
|  No network behavior found |

Statistics

Behavior



 Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 5992, Parent PID: 3528

General

| | |
|-------------------------------|--|
| Target ID: | 0 |
| Start time: | 17:04:39 |
| Start date: | 10/10/2022 |
| Path: | C:\Windows\System32\loaddll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | loaddll32.exe "C:\Users\user\Desktop\diatomaceous.dat.dll" |
| Imagebase: | 0xcc0000 |
| File size: | 116736 bytes |
| MD5 hash: | 1F562FBF37040EC6C43C8D5EF619EA39 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | moderate |

File Activities

Analysis Process: conhost.exe PID: 6064, Parent PID: 5992

General

| | |
|-------------------------------|---|
| Target ID: | 1 |
| Start time: | 17:04:39 |
| Start date: | 10/10/2022 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff7c72c0000 |
| File size: | 625664 bytes |
| MD5 hash: | EA777DEEA782E8B4D7C7C33BBF8A4496 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

| | |
|-------------|------|
| Reputation: | high |
|-------------|------|

Analysis Process: cmd.exe PID: 6116, Parent PID: 5992

General

| | |
|-------------------------------|---|
| Target ID: | 2 |
| Start time: | 17:04:39 |
| Start date: | 10/10/2022 |
| Path: | C:\Windows\SysWOW64\cmd.exe |
| Wow64 process (32bit): | true |
| Commandline: | cmd.exe /C rundll32.exe "C:\Users\user\Desktop\diatomaceous.dat.dll",#1 |
| Imagebase: | 0xd90000 |
| File size: | 232960 bytes |
| MD5 hash: | F3BDBE3BB6F734E357235F4D5898582D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

File Activities

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

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

Analysis Process: regsvr32.exe PID: 6096, Parent PID: 5992

General

| | |
|-------------------------------|--|
| Target ID: | 3 |
| Start time: | 17:04:39 |
| Start date: | 10/10/2022 |
| Path: | C:\Windows\SysWOW64\regsvr32.exe |
| Wow64 process (32bit): | true |
| Commandline: | regsvr32.exe /s C:\Users\user\Desktop\diatomaceous.dat.dll |
| Imagebase: | 0xe20000 |
| File size: | 20992 bytes |
| MD5 hash: | 426E7499F6A7346F0410DEAD0805586B |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | <ul style="list-style-type: none"> Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000003.00000002.320581974.0000000000730000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security Rule: Windows_Trojan_Qbot_92c67a6d, Description: unknown, Source: 00000003.00000002.320581974.0000000000730000.00000040.00000800.00020000.00000000.sdmp, Author: unknown Rule: Windows_Trojan_Qbot_3074a8d4, Description: unknown, Source: 00000003.00000002.320581974.0000000000730000.00000040.00000800.00020000.00000000.sdmp, Author: unknown Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000003.00000003.312800639.0000000004000000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security Rule: Windows_Trojan_Qbot_92c67a6d, Description: unknown, Source: 00000003.00000003.312800639.0000000004000000.00000004.00000800.00020000.00000000.sdmp, Author: unknown Rule: Windows_Trojan_Qbot_3074a8d4, Description: unknown, Source: 00000003.00000003.312800639.0000000004000000.00000004.00000800.00020000.00000000.sdmp, Author: unknown |
| Reputation: | high |

File Activities

File Read

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|----------------------------------|---------|--------|-----------------|-------|----------------|----------|
| C:\Windows\SysWOW64\regsvr32.exe | unknown | 20992 | success or wait | 1 | 6DA81581 | ReadFile |

Analysis Process: rundll32.exe PID: 244, Parent PID: 6116**General**

| | |
|-------------------------------|--|
| Target ID: | 4 |
| Start time: | 17:04:39 |
| Start date: | 10/10/2022 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | rundll32.exe "C:\Users\user\Desktop\diatomaceous.dat.dll",#1 |
| Imagebase: | 0xc50000 |
| File size: | 61952 bytes |
| MD5 hash: | D7CA562B0DB4F4DD0F03A89A1FDAD63D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | <ul style="list-style-type: none"> Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000004.00000003.312922602.0000000002FA0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security Rule: Windows_Trojan_Qbot_92c67a6d, Description: unknown, Source: 00000004.00000003.312922602.0000000002FA0000.00000004.00000800.00020000.00000000.sdmp, Author: unknown Rule: Windows_Trojan_Qbot_3074a8d4, Description: unknown, Source: 00000004.00000003.312922602.0000000002FA0000.00000004.00000800.00020000.00000000.sdmp, Author: unknown Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000004.00000002.320649129.0000000004820000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security Rule: Windows_Trojan_Qbot_92c67a6d, Description: unknown, Source: 00000004.00000002.320649129.0000000004820000.00000040.00000800.00020000.00000000.sdmp, Author: unknown Rule: Windows_Trojan_Qbot_3074a8d4, Description: unknown, Source: 00000004.00000002.320649129.0000000004820000.00000040.00000800.00020000.00000000.sdmp, Author: unknown |
| Reputation: | high |

File Activities**File Read**

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|----------------------------------|---------|--------|-----------------|-------|----------------|----------|
| C:\Windows\SysWOW64\rundll32.exe | unknown | 61952 | success or wait | 1 | 6DA81581 | ReadFile |

Analysis Process: rundll32.exe PID: 3908, Parent PID: 5992**General**

| | |
|-------------------------------|---|
| Target ID: | 5 |
| Start time: | 17:04:39 |
| Start date: | 10/10/2022 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | rundll32.exe C:\Users\user\Desktop\diatomaceous.dat.dll,DllRegisterServer |
| Imagebase: | 0xc50000 |
| File size: | 61952 bytes |
| MD5 hash: | D7CA562B0DB4F4DD0F03A89A1FDAD63D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | <ul style="list-style-type: none"> Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000005.00000003.313259350.000000000B90000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security Rule: Windows_Trojan_Qbot_92c67a6d, Description: unknown, Source: 00000005.00000003.313259350.000000000B90000.00000004.00000800.00020000.00000000.sdmp, Author: unknown Rule: Windows_Trojan_Qbot_3074a8d4, Description: unknown, Source: 00000005.00000003.313259350.000000000B90000.00000004.00000800.00020000.00000000.sdmp, Author: unknown Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000005.00000002.320603133.0000000002CC0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security Rule: Windows_Trojan_Qbot_92c67a6d, Description: unknown, Source: 00000005.00000002.320603133.0000000002CC0000.00000040.00000800.00020000.00000000.sdmp, Author: unknown Rule: Windows_Trojan_Qbot_3074a8d4, Description: unknown, Source: 00000005.00000002.320603133.0000000002CC0000.00000040.00000800.00020000.00000000.sdmp, Author: unknown |
| Reputation: | high |

File Activities

| File Read | | | | | | |
|----------------------------------|---------|--------|-----------------|-------|----------------|----------|
| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
| C:\Windows\SysWOW64\rundll32.exe | unknown | 61952 | success or wait | 1 | 6DA81581 | ReadFile |

Analysis Process: rundll32.exe PID: 1540, Parent PID: 5992

| General | |
|-------------------------------|---|
| Target ID: | 6 |
| Start time: | 17:04:42 |
| Start date: | 10/10/2022 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | rundll32.exe C:\Users\user\Desktop\diatomaceous.dat.dll,DllUnregisterServer |
| Imagebase: | 0xc50000 |
| File size: | 61952 bytes |
| MD5 hash: | D7CA562B0DB4F4DD0F03A89A1FDAD63D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

Analysis Process: wermgr.exe PID: 5020, Parent PID: 6096

| General | |
|-------------------------------|---|
| Target ID: | 7 |
| Start time: | 17:04:44 |
| Start date: | 10/10/2022 |
| Path: | C:\Windows\SysWOW64\wermgr.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\SysWOW64\wermgr.exe |
| Imagebase: | 0x1160000 |
| File size: | 191904 bytes |
| MD5 hash: | CCF15E662ED5CE77B5FF1A7AAE305233 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | <ul style="list-style-type: none"> Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000007.00000000.319688371.000000001000000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security Rule: Windows_Trojan_Qbot_92c67a6d, Description: unknown, Source: 00000007.00000000.319688371.000000001000000.00000040.80000000.00040000.00000000.sdmp, Author: unknown Rule: Windows_Trojan_Qbot_3074a8d4, Description: unknown, Source: 00000007.00000000.319688371.000000001000000.00000040.80000000.00040000.00000000.sdmp, Author: unknown |

File Activities

| File Created | | | | | | | |
|---|---|------------|--|-----------------|-------|----------------|------------------|
| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
| C:\Users\user\AppData\Roaming\Microsoft\Bwkwi | read data or list directory synchronize | device | directory file synchronous io non alert open for backup ident open reparse point | success or wait | 1 | 1003289 | CreateDirectoryW |

| File Written | | | | | | | | |
|--------------|--------|--------|-------|-------|------------|-------|----------------|--------|
| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |

| Key Path | Name | Type | Data | Completion | Count | Source Address | Symbol |
|---|----------|--------|---|-----------------|-------|----------------|--------------------|
| HKEY_CURRENT_USER\Software\Microsoft\fwliuvmg | e279be6c | binary | C3 AA 33 A9 BF E4 BD 27 7C 3D E5 F4 3C 29 2D 1D C2 B0 27 06 37 D0 BE 12 D4 25 01 A8 90 A4 32 C3 FD A0 ED 63 52 A9 28 84 1C 3C B5 86 BD 0F D0 CF 09 80 A4 39 DA 47 74 AC 4B E1 33 7B 6A 30 E6 07 07 F1 0B 32 0C 63 D9 62 26 03 5D 55 4F 70 E6 C6 9F 8F DD 3F 60 A4 3C 37 D9 7F F7 E5 DC 0E E9 69 1B C9 64 D3 6A 17 BC 42 13 76 7A 5B 5C 9D 1E C3 DB A2 | success or wait | 1 | 100AF2F | RegSetValueEx A |
| HKEY_CURRENT_USER\Software\Microsoft\fwliuvmg | 5ac5d909 | binary | F4 7E BA 78 5B EC 63 31 9E F0 CE F8 EA 44 33 57 35 AF 5F C7 4A B2 04 52 F5 07 2C 74 49 CA D1 20 CD 95 6F BA 4F 94 72 FF 36 63 03 98 5B DB 91 B4 E9 B4 CD 7F 2E 3A CC 2F 3E 49 E2 5A E8 E6 FE A1 A8 9C 50 | success or wait | 1 | 100AF2F | RegSetValueEx A |
| HKEY_CURRENT_USER\Software\Microsoft\fwliuvmg | 9d30d19a | binary | 79 22 CC F7 97 50 12 76 D3 5C B4 F2 02 4F 09 36 8A C4 C2 59 E8 AC CF 41 32 56 7F BD E3 66 B1 58 93 A6 91 34 7D DC D1 25 D0 43 A1 35 92 7A DA F6 42 4F 6C DA 60 47 74 DE 1F BE A9 2F CE 43 73 49 42 DC F1 1F 8C 46 84 D6 2B 44 78 0E 35 AD B9 17 4D 24 F0 56 62 22 D1 25 B0 C9 C0 95 29 5D B8 ED 4C AD 45 C3 4F D3 21 92 5C A5 4E 53 84 65 13 B1 43 F0 | success or wait | 1 | 100AF2F | RegSetValueEx A |
| HKEY_CURRENT_USER\Software\Microsoft\fwliuvmg | 6f5a0947 | binary | D2 D2 9F 71 70 AB 0F 4F DA B4 03 F1 13 DE F5 0E 9A 53 80 FD DD F7 24 0C 92 C4 6E 39 66 DF 50 B0 05 75 C9 CD F6 E4 94 70 EA B4 CE B1 62 | success or wait | 1 | 100AF2F | RegSetValueEx A |

| Key Value Modified | | | | | | | | |
|---|----------|--------|--|---|-----------------|-------|----------------|--------------------|
| Key Path | Name | Type | Old Data | New Data | Completion | Count | Source Address | Symbol |
| HKEY_CURRENT_USER\Software\Microsoft\fwliuvmg | 101366b1 | binary | 55 E6 56 8C 15 AC C1 2E 7F 0B ED C4 9A D2 68 0E B8 AA 19 55 69 CD 0F F6 CF EC 1A 95 A5 15 7A 9F 40 CE 76 FA A8 A4 0F 08 63 07 B4 4E 01 C5 5B A7 1E E9 E8 48 F4 4F 7E 24 EB CC 69 4B 0C CE 1D 10 79 E3 0D 88 C6 D7 BE 71 66 C2 E8 AB | 55 E6 41 8C 15 AC F2 B9 18 EC D3 8F 27 76 15 51 80 97 73 F6 3D 3F 7F 80 22 F8 24 70 90 08 2F 88 85 3A 2F D9 E4 2D 8D 62 F2 5A 3A 2A D6 C1 26 86 13 D4 FA FD F6 E8 AA 70 6C B5 32 A0 53 F4 15 29 32 3D CE 74 EC 80 BA 77 BA 57 13 92 57 9A 6E 29 B8 38 FC 52 1F 57 B0 AB 26 8E 04 F3 D8 FE 9C 67 4B | success or wait | 1 | 100AF2F | RegSetValueEx A |


Analysis Process: wermgr.exe PID: 4860, Parent PID: 3908

| General | |
|-------------------------------|----------------------------------|
| Target ID: | 8 |
| Start time: | 17:04:44 |
| Start date: | 10/10/2022 |
| Path: | C:\Windows\SysWOW64\wermgr.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\SysWOW64\wermgr.exe |
| Imagebase: | 0x1160000 |
| File size: | 191904 bytes |
| MD5 hash: | CCF15E662ED5CE77B5FF1A7AAE305233 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

| | |
|---------------|--|
| Yara matches: | <ul style="list-style-type: none"> • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000009.00000000.319924513.000000000E00000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Qbot_92c67a6d, Description: unknown, Source: 00000009.00000000.319924513.000000000E00000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Qbot_3074a8d4, Description: unknown, Source: 00000009.00000000.319924513.000000000E00000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000009.00000002.322491943.000000000E00000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Qbot_92c67a6d, Description: unknown, Source: 00000009.00000002.322491943.000000000E00000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Qbot_3074a8d4, Description: unknown, Source: 00000009.00000002.322491943.000000000E00000.00000040.80000000.00040000.00000000.sdmp, Author: unknown |
|---------------|--|

| File Activities | | | | | | | | | | | |
|--|--------|--------|---|--|-----------------|-------|----------------|-----------|--|--|--|
| File Written | | | | | | | | | | | |
| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol | | | |
| C:\Users\user\Desktop\diatomaceous.dat.dll | 0 | 4096 | 4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 10 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 1f fd 42 fd 5b fd 2c fd 5b fd 2c fd 5b fd 2c fd 2f fd 56 fd 2c fd fd 29 fd 91 2c fd fd 28 fd 4d fd 2c fd 09 fd 28 fd 54 fd 2c fd 09 fd 2f fd 48 fd 2c fd 09 fd 29 fd 18 fd 2c fd fd 2d fd 5e fd 2c fd 5b fd 2d fd 3d fd 2c fd fd 25 fd 5c fd 2c fd fd 2c fd 5a fd 2c fd fd fd 5a fd 2c fd 5b fd fd fd 5a fd 2c fd fd 2e fd 5a fd 2c fd 52 69 63 68 5b fd 2c | MZ@!LThis program cannot be run in DOS mode.\$B[.[./V),(M, (T,/H,)-^,[=-,%\,Z,Z, [Z.,Z,Rich[| success or wait | 1 | E0B4DE | WriteFile | | | |

| File Read | | | | | | | |
|--|---------|--------|-----------------|-------|----------------|----------|--|
| File Path | Offset | Length | Completion | Count | Source Address | Symbol | |
| C:\Users\user\Desktop\diatomaceous.dat.dll | unknown | 393216 | success or wait | 2 | E0B53C | ReadFile | |
| C:\Windows\SysWOW64\amstream.dll | unknown | 80896 | success or wait | 2 | E0B53C | ReadFile | |

| |
|--|
| <h2>Disassembly</h2> <p> No disassembly</p> |
|--|