**MALICIOUS**

Classifications: Injector, Downloader

Threat Names: SmokeLoader, Mal/HTMLGen-A

Verdict Reason: -

| | |
|---|---|
| **Sample Type** | **Windows Exe (x86-32)** |
| **File Name** | **eb24b3b9375f0b3272fac6eecc9329f79eab274d802b2ad37037cc83a46fa3f1.exe** |
| ID | #3212181 |
| MD5 | 720b195655e0a571c4d511088b51202b |
| SHA1 | f171845fe7b3ae9576ea0f698edd8d65d6bf6ead |
| SHA256 | eb24b3b9375f0b3272fac6eecc9329f79eab274d802b2ad37037cc83a46fa3f1 |
| File Size | 339.00 KB |
| Report Created | 2021-12-31 20:54 (UTC+1) |
| Target Environment | win7_64_sp1_en_mso2016 \| exe |

# OVERVIEW

## VMRay Threat Identifiers (17 rules, 30 matches)

| Score | Category | Operation | Count | Classification |
|---|---|---|---|---|
| 5/5 | YARA | Malicious content matched by YARA rules | 3 | Downloader |
| | • Rule "SmokeLoader" from ruleset "Malware" has matched on a memory dump for (process #2) eb24b3b9375f0b3272fac6eecc9329f79eab274d802b2ad37037cc83a46fa3f1.exe.<br>• Rule "SmokeLoader" from ruleset "Malware" has matched on a memory dump for (process #3) explorer.exe.<br>• Rule "SmokeLoaderStrings" from ruleset "Malware" has matched on the function strings for (process #3) explorer.exe. | | | |
| 4/5 | Defense Evasion | Obscures a file's origin | 1 | - |
| | • (Process #3) explorer.exe tries to delete zone identifier of file "C:\Users\kEecfMwgj\AppData\Roaming\cdieedr". | | | |
| 4/5 | Reputation | Contacts known malicious URL | 1 | - |
| | • Reputation analysis labels the URL "host-data-coin-11.com/" which was contacted by (process #3) explorer.exe as "Mal/HTMLGen-A". | | | |
| 4/5 | Injection | Writes into the memory of another process | 2 | Injector |
| | • (Process #2) eb24b3b9375f0b3272fac6eecc9329f79eab274d802b2ad37037cc83a46fa3f1.exe modifies memory of (process #3) explorer.exe.<br>• (Process #8) cdieedr modifies memory of (process #3) explorer.exe. | | | |
| 4/5 | Injection | Modifies control flow of another process | 2 | Injector |
| | • (Process #2) eb24b3b9375f0b3272fac6eecc9329f79eab274d802b2ad37037cc83a46fa3f1.exe creates thread in (process #3) explorer.exe.<br>• (Process #8) cdieedr creates thread in (process #3) explorer.exe. | | | |
| 2/5 | Anti Analysis | Tries to detect debugger | 1 | - |
| | • (Process #2) eb24b3b9375f0b3272fac6eecc9329f79eab274d802b2ad37037cc83a46fa3f1.exe tries to detect a debugger via API "NtQueryInformationProcess". | | | |
| 2/5 | Hide Tracks | Deletes file after execution | 2 | - |
| | • (Process #3) explorer.exe deletes executed executable "c:\users\keecfmwgj\appdata\roaming\cdieedr".<br>• (Process #3) explorer.exe deletes executed executable "c:\users\keecfmwgj\desktop\eb24b3b9375f0b3272fac6eecc9329f79eab274d802b2ad37037cc83a46fa3f1.exe". | | | |
| 2/5 | Anti Analysis | Delays execution | 1 | - |
| | • (Process #3) explorer.exe has a thread which sleeps more than 5 minutes. | | | |
| 2/5 | Injection | Writes into the memory of a process started from a created or modified executable | 2 | - |
| | • (Process #1) eb24b3b9375f0b3272fac6eecc9329f79eab274d802b2ad37037cc83a46fa3f1.exe modifies memory of (process #2) eb24b3b9375f0b3272fac6eecc9329f79eab274d802b2ad37037cc83a46fa3f1.exe.<br>• (Process #5) cdieedr modifies memory of (process #8) cdieedr. | | | |
| 2/5 | Injection | Modifies control flow of a process started from a created or modified executable | 2 | - |
| | • (Process #1) eb24b3b9375f0b3272fac6eecc9329f79eab274d802b2ad37037cc83a46fa3f1.exe alters context of (process #2) eb24b3b9375f0b3272fac6eecc9329f79eab274d802b2ad37037cc83a46fa3f1.exe.<br>• (Process #5) cdieedr alters context of (process #8) cdieedr. | | | |
| 2/5 | Task Scheduling | Schedules task | 2 | - |
| | • Schedules task for command "C:\Users\kEecfMwgj\AppData\Roaming\cdieedr", to be triggered by Logon.<br>• Schedules task for command "C:\Users\kEecfMwgj\AppData\Roaming\cdieedr", to be triggered by Time. Task has been rescheduled by the analyzer. | | | |
| 1/5 | Obfuscation | Reads from memory of another process | 2 | - |

| Score | Category | Operation | Count | Classification |
|---|---|---|---|---|
| | • (Process #1) eb24b3b9375f0b3272fac6eecc9329f79eab274d802b2ad37037cc83a46fa3f1.exe reads from (process #2) eb24b3b9375f0b3272fac6eecc9329f79eab274d802b2ad37037cc83a46fa3f1.exe.<br>• (Process #5) cdieedr reads from (process #8) cdieedr. | | | |
| 1/5 | Obfuscation | Creates a page with write and execute permissions | 2 | - |
| | • (Process #1) eb24b3b9375f0b3272fac6eecc9329f79eab274d802b2ad37037cc83a46fa3f1.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.<br>• (Process #5) cdieedr allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code. | | | |
| 1/5 | Discovery | Enumerates running processes | 1 | - |
| | • (Process #3) explorer.exe enumerates running processes. | | | |
| 1/5 | Mutex | Creates mutex | 1 | - |
| | • (Process #3) explorer.exe creates mutex with name "4BCD659AD8F347B5B451918CD891C8238443A5AF". | | | |
| 1/5 | Execution | Executes itself | 3 | - |
| | • (Process #1) eb24b3b9375f0b3272fac6eecc9329f79eab274d802b2ad37037cc83a46fa3f1.exe executes a copy of the sample at C:\Users\kEecfMwgj\Desktop\eb24b3b9375f0b3272fac6eecc9329f79eab274d802b2ad37037cc83a46fa3f1.exe.<br>• (Process #4) taskeng.exe executes a copy of the sample at C:\Users\kEecfMwgj\Desktop\eb24b3b9375f0b3272fac6eecc9329f79eab274d802b2ad37037cc83a46fa3f1.exe.<br>• (Process #5) cdieedr executes a copy of the sample at C:\Users\kEecfMwgj\Desktop\eb24b3b9375f0b3272fac6eecc9329f79eab274d802b2ad37037cc83a46fa3f1.exe. | | | |
| 1/5 | Obfuscation | Resolves API functions dynamically | 2 | - |
| | • (Process #1) eb24b3b9375f0b3272fac6eecc9329f79eab274d802b2ad37037cc83a46fa3f1.exe resolves 39 API functions by name.<br>• (Process #5) cdieedr resolves 39 API functions by name. | | | |

### Mitre ATT&CK Matrix

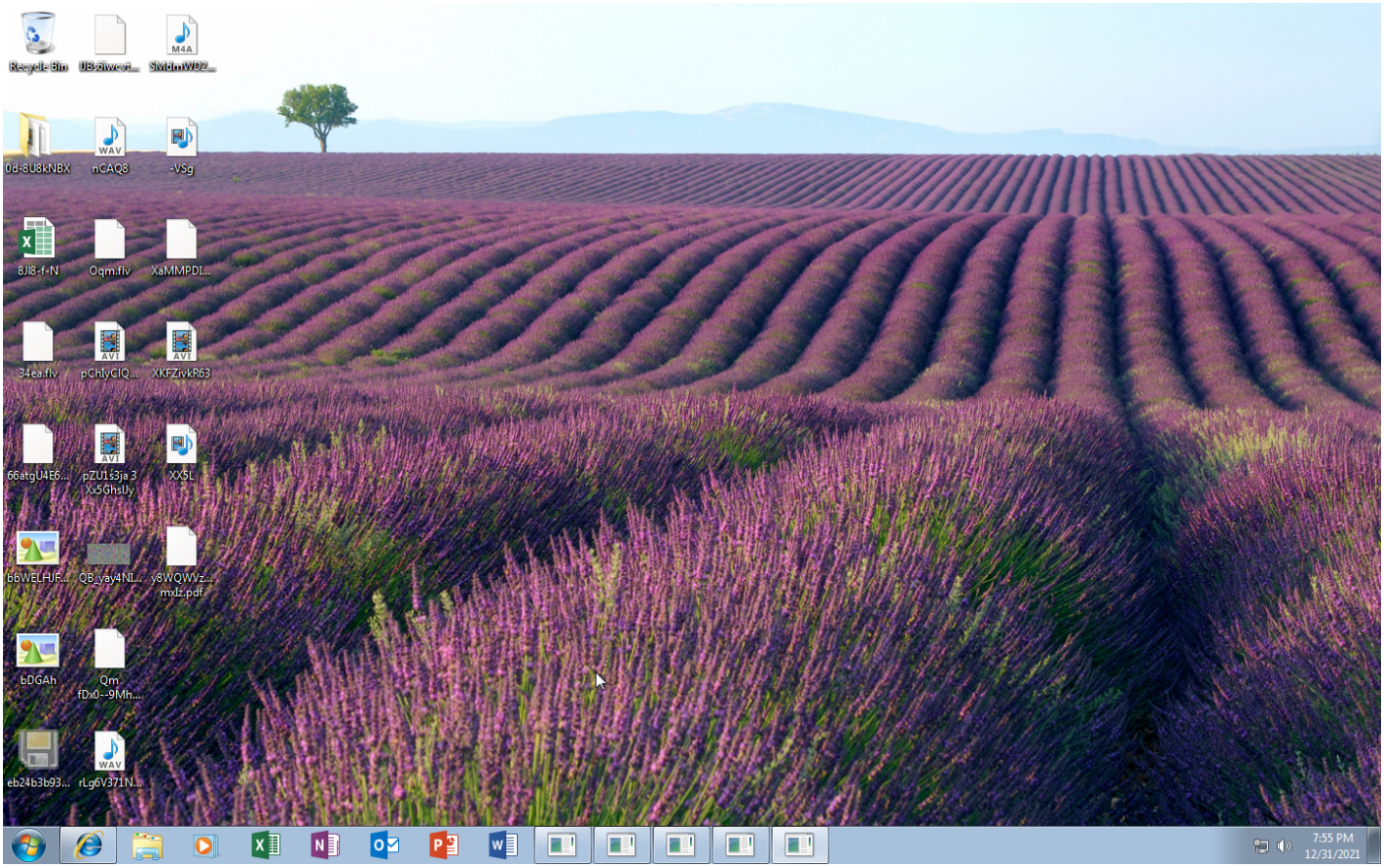
| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Command and Control | Exfiltration | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | #T1053 Scheduled Task | #T1053 Scheduled Task | #T1053 Scheduled Task | #T1045 Software Packing | | #T1057 Process Discovery | | | | | |
| | | | | #T1096 NTFS File Attributes | | | | | | | |

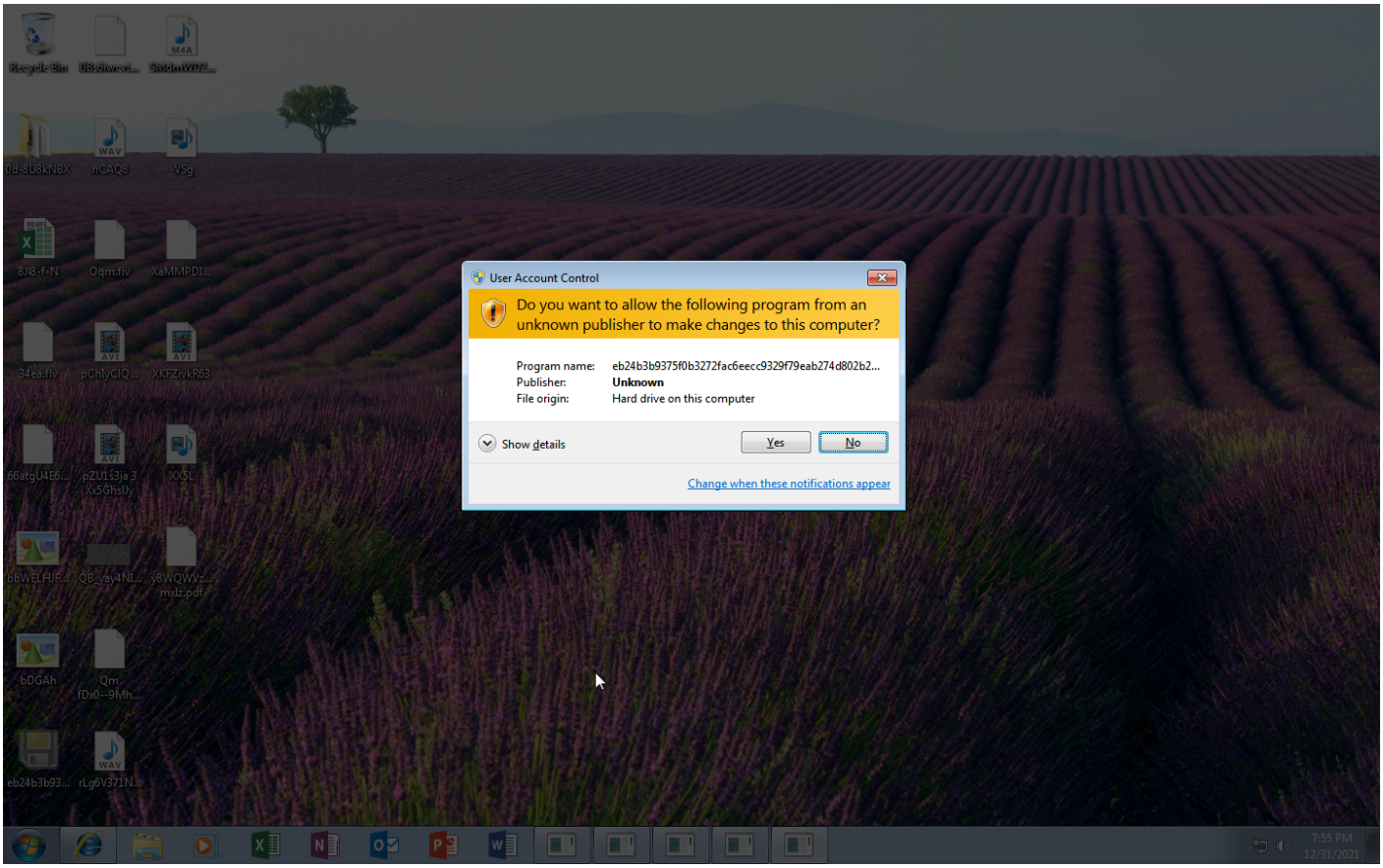
## Sample Information

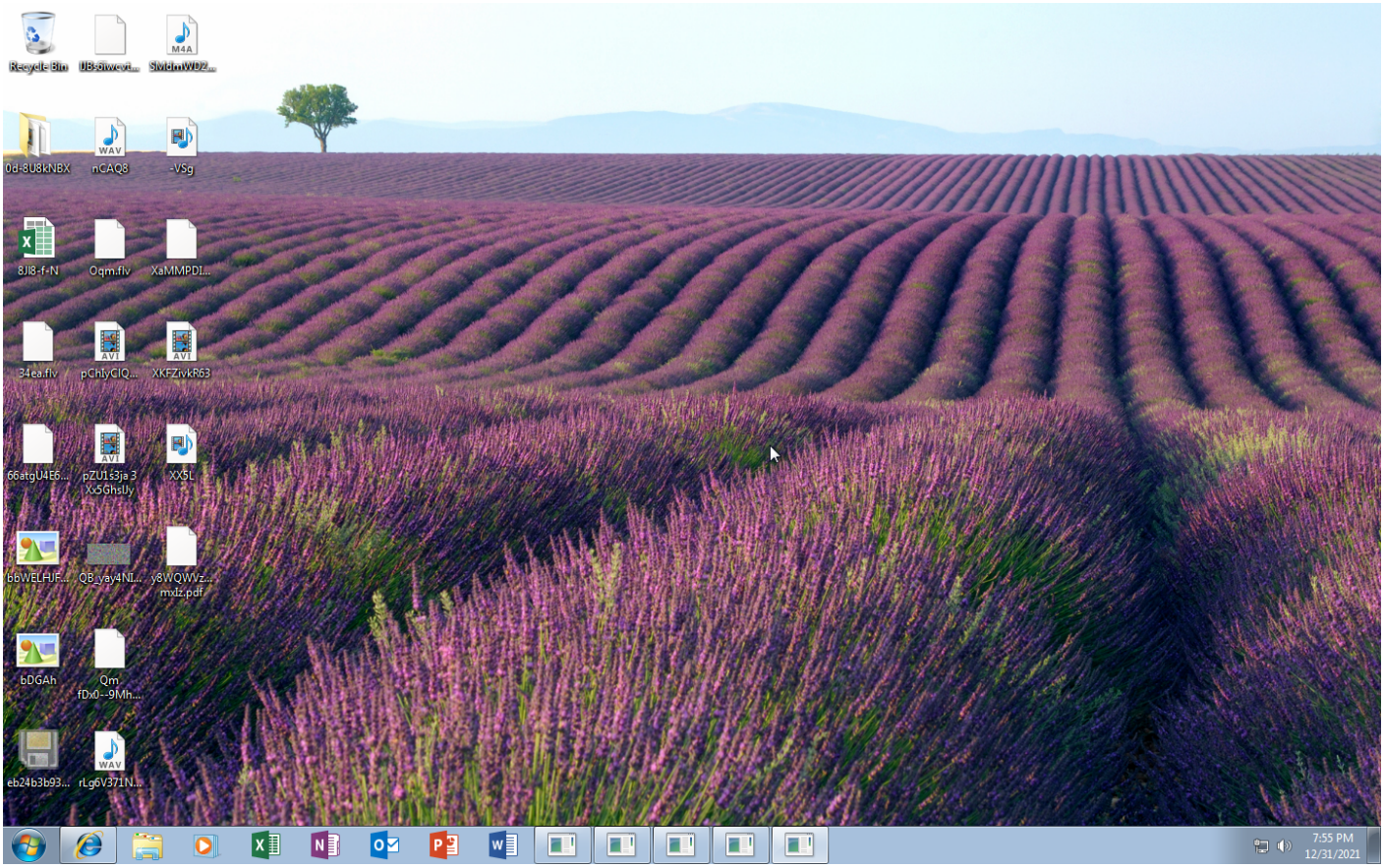
| | |
|---|---|
| ID | #3212181 |
| MD5 | 720b195655e0a571c4d511088b51202b |
| SHA1 | f171845fe7b3ae9576ea0f698edd8d65d6bf6ead |
| SHA256 | eb24b3b9375f0b3272fac6eecc9329f79eab274d802b2ad37037cc83a46fa3f1 |
| SSDeep | 6144:gnjd+ZnJMz+HPYYys+J7hulPCUrM/YbKwj4Fy9FVUHc1FEu:gnjdZz2Qmm7hulPCUQ/YbKwjRFVUwFEu |
| ImpHash | c613013e8ec93eae360257b5231d0949 |
| File Name | eb24b3b9375f0b3272fac6eecc9329f79eab274d802b2ad37037cc83a46fa3f1.exe |
| File Size | 339.00 KB |
| Sample Type | Windows Exe (x86-32) |
| Has Macros | ✓ |

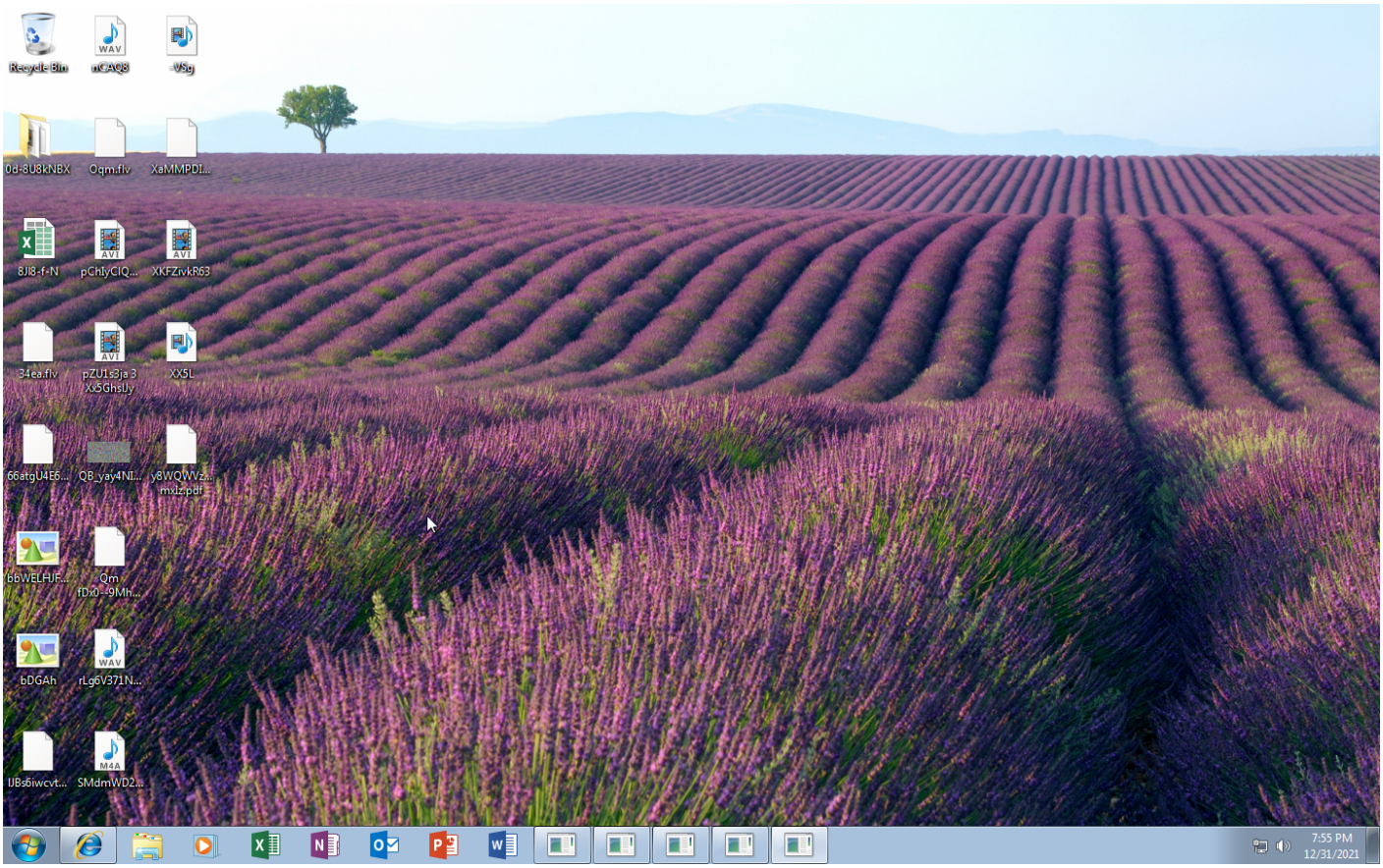
## Analysis Information

| | |
|---|---|
| Creation Time | 2021-12-31 20:54 (UTC+1) |
| Analysis Duration | 00:04:00 |
| Termination Reason | Timeout |
| Number of Monitored Processes | 6 |
| Execution Successful | False |
| Reputation Enabled | ✓ |
| WHOIS Enabled | ✓ |
| Built-in AV Enabled | ✗ |
| Built-in AV Applied On | Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files |
| Number of AV Matches | 0 |
| YARA Enabled | ✓ |
| YARA Applied On | Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files |
| Number of YARA Matches | 4 |




User Account Control
Do you want to allow the following program from an unknown publisher to make changes to this computer?
Program name: eb24b3b9375f0b3272fac6eecc9329f79eab274d802b2...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear




Screenshots truncated

# NETWORK

## General

5.91 KB total sent

3.03 KB total received

1 ports 80

1 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

## DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

## HTTP/S

1 URLs contacted, 1 servers

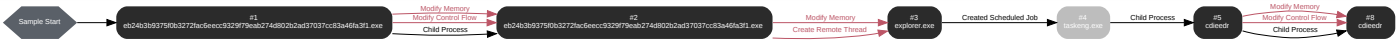
8 sessions, 5.91 KB sent, 3.03 KB received

## HTTP Requests

| Method | URL | Dest. IP | Dest. Port | Status Code | Response Size | Verdict |
|---|---|---|---|---|---|---|
| POST | host-data-coin-11.com/ | - | - | | 0 bytes | NA |

## BEHAVIOR

### Process Graph



### Process #1: eb24b3b9375f0b3272fac6eecc9329f79eab274d802b2ad37037cc83a46fa3f1.exe

| | |
|---|---|
| ID | 1 |
| File Name | c:\users\keecfmwgj\desktop\eb24b3b9375f0b3272fac6eecc9329f79eab274d802b2ad37037cc83a46fa3f1.exe |
| Command Line | "C:\Users\kEecfMwgj\Desktop\eb24b3b9375f0b3272fac6eecc9329f79eab274d802b2ad37037cc83a46fa3f1.exe" |
| Initial Working Directory | C:\Users\kEecfMwgj\Desktop\ |
| Monitor Start Time | Start Time: 43296, Reason: Analysis Target |
| Unmonitor End Time | End Time: 61856, Reason: Terminated |
| Monitor duration | 18.56s |
| Return Code | 0 |
| PID | 3600 |
| Parent PID | 912 |
| Bitness | 32 Bit |

### Host Behavior

| Type | Count |
|---|---|
| System | 252 |
| Module | 51 |
| File | 6 |
| Environment | 1 |
| Window | 1 |
| Process | 1 |
| - | 3 |
| - | 5 |

### Process #2: eb24b3b9375f0b3272fac6eecc9329f79eab274d802b2ad37037cc83a46fa3f1.exe

| | |
|---|---|
| ID | 2 |
| File Name | c:\users\keecfmwgj\desktop\eb24b3b9375f0b3272fac6eecc9329f79eab274d802b2ad37037cc83a46fa3f1.exe |
| Command Line | "C:\Users\kEecfMwgj\Desktop\eb24b3b9375f0b3272fac6eecc9329f79eab274d802b2ad37037cc83a46fa3f1.exe" |
| Initial Working Directory | C:\Users\kEecfMwgj\Desktop\ |
| Monitor Start Time | Start Time: 56602, Reason: Child Process |
| Unmonitor End Time | End Time: 69172, Reason: Terminated |
| Monitor duration | 12.57s |
| Return Code | 0 |
| PID | 3620 |
| Parent PID | 3600 |
| Bitness | 32 Bit |

### Injection Information (4)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Modify Memory | #1: c:\users\keecfmwgj\desktop\eb24b3b9375f0b3272fac6eecc9329f79eab274d802b2ad37037cc83a46fa3f1.exe | 0xe14 | 0x400000(4194304) | 0x200 | ✓ | 1 |
| Modify Memory | #1: c:\users\keecfmwgj\desktop\eb24b3b9375f0b3272fac6eecc9329f79eab274d802b2ad37037cc83a46fa3f1.exe | 0xe14 | 0x401000(4198400) | 0x7200 | ✓ | 1 |
| Modify Memory | #1: c:\users\keecfmwgj\desktop\eb24b3b9375f0b3272fac6eecc9329f79eab274d802b2ad37037cc83a46fa3f1.exe | 0xe14 | 0x7efde008(2130567176) | 0x4 | ✓ | 1 |
| Modify Control Flow | #1: c:\users\keecfmwgj\desktop\eb24b3b9375f0b3272fac6eecc9329f79eab274d802b2ad37037cc83a46fa3f1.exe | 0xe14 / 0xe28 | 0x779f01c4(2006909380) | - | ✓ | 1 |

### Host Behavior

| Type | Count |
|---|---|
| Module | 17 |
| Keyboard | 2 |
| Process | 1 |
| File | 1 |
| System | 6 |
| - | 1 |
| Registry | 18 |
| - | 1 |

### Process #3: explorer.exe

| | |
|---|---|
| ID | 3 |
| File Name | c:\windows\explorer.exe |
| Command Line | C:\Windows\Explorer.EXE |
| Initial Working Directory | C:\Windows\system32\ |
| Monitor Start Time | Start Time: 65859, Reason: Injection |
| Unmonitor End Time | End Time: 283688, Reason: Terminated by Timeout |
| Monitor duration | 217.83s |
| Return Code | Unknown |
| PID | 912 |
| Parent PID | 18446744073709551615 |
| Bitness | 64 Bit |

### Injection Information (6)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Modify Memory | #2: c:\users\keecfmwgj\desktop\eb24b3b9375f0b3272fac6eecc9329f79eab274d802b2ad37037cc83a46fa3f1.exe | 0xe28 | 0x3900000(59768832) | 0x5000 | ✓ | 1 |
| Modify Memory | #2: c:\users\keecfmwgj\desktop\eb24b3b9375f0b3272fac6eecc9329f79eab274d802b2ad37037cc83a46fa3f1.exe | 0xe28 | 0x3930000(59965440) | 0x16000 | ✓ | 1 |
| Create Remote Thread | #2: c:\users\keecfmwgj\desktop\eb24b3b9375f0b3272fac6eecc9329f79eab274d802b2ad37037cc83a46fa3f1.exe | 0xe28 | 0x3931930(59971888) | - | ✓ | 1 |
| Modify Memory | #8: c:\users\keecfmwgj\appdata\roaming\cdieedr | 0xe84 | 0x3950000(60096512) | 0x5000 | ✓ | 1 |
| Modify Memory | #8: c:\users\keecfmwgj\appdata\roaming\cdieedr | 0xe84 | 0x3960000(60162048) | 0x16000 | ✓ | 1 |
| Create Remote Thread | #8: c:\users\keecfmwgj\appdata\roaming\cdieedr | 0xe84 | 0x3961930(60168496) | - | ✓ | 1 |

### Dropped Files (1)

| File Name | File Size | SHA256 | YARA Match |
|---|---|---|---|
| C:\Users\kEecfMwgj\AppData\Roaming\cdieedr | 339.00 KB | eb24b3b9375f0b3272fac6eecc9329f79eab274d802b2ad37037cc83a46fa3f1 | ✗ |

### Host Behavior

| Type | Count |
|---|---|
| Module | 35 |
| System | 8415 |
| Process | 538 |
| Mutex | 2 |
| Registry | 3 |
| File | 23 |
| User | 1 |

| Type | Count |
| --- | --- |
| COM | 1 |

### Network Behavior

| Type | Count |
| --- | --- |
| HTTP | 8 |
| TCP | 8 |

### Process #4: taskeng.exe

| | |
|---|---|
| ID | 4 |
| File Name | c:\windows\system32\taskeng.exe |
| Command Line | taskeng.exe {DE00562E-A1A7-4FF8-A10B-5BE85423C482} S-1-5-21-4219442223-4223814209-3835049652-1000:Q9IATRKPRH\kEecfMwgj:Interactive:LUA[1] |
| Initial Working Directory | C:\Windows\system32\ |
| Monitor Start Time | Start Time: 99287, Reason: Created Scheduled Job |
| Unmonitor End Time | End Time: 283688, Reason: Terminated by Timeout |
| Monitor duration | 184.40s |
| Return Code | Unknown |
| PID | 3672 |
| Parent PID | 864 |
| Bitness | 64 Bit |

### Process #5: cdieedr

| | |
|---|---|
| ID | 5 |
| File Name | c:\users\keecfmwgj\appdata\roaming\cdieedr |
| Command Line | C:\Users\kEecfMwgj\AppData\Roaming\cdieedr |
| Initial Working Directory | C:\Windows\system32\ |
| Monitor Start Time | Start Time: 100918, Reason: Child Process |
| Unmonitor End Time | End Time: 112353, Reason: Terminated |
| Monitor duration | 11.44s |
| Return Code | 0 |
| PID | 3704 |
| Parent PID | 3672 |
| Bitness | 32 Bit |

### Host Behavior

| Type | Count |
|---|---|
| System | 252 |
| Module | 51 |
| File | 6 |
| Environment | 1 |
| Window | 1 |
| Process | 1 |
| - | 3 |
| - | 5 |

### Process #8: cdieedr

| | |
|---|---|
| ID | 8 |
| File Name | c:\users\keecfmwgj\appdata\roaming\cdieedr |
| Command Line | C:\Users\kEecfMwgj\AppData\Roaming\cdieedr |
| Initial Working Directory | C:\Windows\system32\ |
| Monitor Start Time | Start Time: 110125, Reason: Child Process |
| Unmonitor End Time | End Time: 117722, Reason: Terminated |
| Monitor duration | 7.60s |
| Return Code | 0 |
| PID | 3712 |
| Parent PID | 3704 |
| Bitness | 32 Bit |

### Injection Information (3)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Modify Memory | #5: c:\users\keecfmwgj\appdata\roaming\cdieedr | 0xe7c | 0x400000(4194304) | 0x200 | ✓ | 1 |
| Modify Memory | #5: c:\users\keecfmwgj\appdata\roaming\cdieedr | 0xe7c | 0x7efde008(2130567176) | 0x4 | ✓ | 1 |
| Modify Control Flow | #5: c:\users\keecfmwgj\appdata\roaming\cdieedr | 0xe7c / 0xe84 | 0x779f01c4(2006909380) | - | ✓ | 1 |

### Host Behavior

| Type | Count |
|---|---|
| Module | 17 |
| Keyboard | 2 |
| Process | 1 |
| File | 1 |
| System | 6 |
| - | 1 |
| Registry | 18 |
| - | 1 |

# ARTIFACTS

## File

| SHA256 | File Names | Category | File Size | MIME Type | Operations | Verdict |
|---|---|---|---|---|---|---|
| eb24b3b9375f0b3272fac6eecc9329f79eab274d802b2ad37037cc83a46fa3f1 | C:\Users\kEecfMwgj\AppData\Roaming\cdieedr, C:\Users\kEecfMwgj\Desktop\eb24b3b9375f0b3272fac6eecc9329f79eab274d802b2ad37037cc83a46fa3f1.exe | Sample File | 339.00 KB | application/vnd.microsoft.portable-executable | Create, Delete, Write, Access | MALICIOUS |

## Filename

| File Name | Category | Operations | Verdict |
|---|---|---|---|
| C:\Users\kEecfMwgj\Desktop\eb24b3b9375f0b3272fac6eecc9329f79eab274d802b2ad37037cc83a46fa3f1.exe | Sample File | Delete, Access | CLEAN |
| apfHQ | Accessed File | Access | CLEAN |
| C:\Windows\system32\ntdll.dll | Accessed File | Access | CLEAN |
| C:\Users\kEecfMwgj\AppData\Roaming\cdieedr | Sample File | Create, Delete, Write, Access | CLEAN |
| C:\Users\kEecfMwgj\AppData\Roaming\cdieedr:Zone.Identifier | Accessed File | Delete, Access | CLEAN |
| C:\Windows\system32\advapi32.dll | Accessed File | Access | CLEAN |
| C:\Users\kEecfMwgj\AppData\Roaming\estugfj | Accessed File | Access | CLEAN |

## URL

| URL | Category | IP Address | Country | HTTP Methods | Verdict |
|---|---|---|---|---|---|
| http://host-data-coin-11.com | - | 31.28.27.130 | - | POST | MALICIOUS |

## Domain

| Domain | IP Address | Country | Protocols | Verdict |
|---|---|---|---|---|
| host-data-coin-11.com | 31.28.27.130 | - | HTTP | CLEAN |

## IP

| IP Address | Domains | Country | Protocols | Verdict |
|---|---|---|---|---|
| 31.28.27.130 | host-data-coin-11.com | Russia | DNS, TCP, HTTP | CLEAN |

## Mutex

| Name | Operations | Parent Process Name | Verdict |
|---|---|---|---|
| 4BCD659AD8F347B5B451918CD891C8238443A5AF | access | explorer.exe | CLEAN |

## Registry

| Registry Key | Operations | Parent Process Name | Verdict |
|---|---|---|---|
| \REGISTRY\MACHINE\System\CurrentControlSet\Enum\IDE | access | cdieedr, eb24b3b9375f0b3272fac6eecc9329f79eab274d802b2ad37037cc83a46fa3f1.exe | CLEAN |
| \REGISTRY\MACHINE\System\CurrentControlSet\Enum\SCSI | access | cdieedr, eb24b3b9375f0b3272fac6eecc9329f79eab274d802b2ad37037cc83a46fa3f1.exe | CLEAN |
| HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer | access | explorer.exe | CLEAN |
| HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\svcVersion | read, access | explorer.exe | CLEAN |
| HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Version | read, access | explorer.exe | CLEAN |

## Process

| Process Name | Commandline | Verdict |
|---|---|---|
| eb24b3b9375f0b3272fac6eecc9329f79eab274d802b2ad37037cc83a46fa3f1.exe | "C:\Users\kEecfMwgj\Desktop\eb24b3b9375f0b3272fac6eecc9329f79eab274d802b2ad37037cc83a46fa3f1.exe" | MALICIOUS |
| cdieedr | C:\Users\kEecfMwgj\AppData\Roaming\cdieedr | MALICIOUS |
| explorer.exe | C:\Windows\Explorer.EXE | SUSPICIOUS |
| taskeng.exe | taskeng.exe {DE00562E-A1A7-4FF8-A10B-5BE85423C482} S-1-5-21-4219442223-4223814209-3835049652-1000:Q9IATRKPRH\kEecfMwgj:Interactive:LUA[1] | CLEAN |

## YARA / AV

### YARA (4)

| Ruleset Name | Rule Name | Rule Description | File Type | File Name | Classification | Verdict |
|---|---|---|---|---|---|---|
| Malware | SmokeLoader | SmokeLoader memory dump | Memory Dump | - | Downloader | 5/5 |
| Malware | SmokeLoader | SmokeLoader memory dump | Memory Dump | - | Downloader | 5/5 |
| Malware | SmokeLoader | SmokeLoader memory dump | Memory Dump | - | Downloader | 5/5 |
| Malware | SmokeLoaderStrings | SmokeLoader strings | Function Strings | function_strings_process_3.txt | Downloader | 5/5 |

# ENVIRONMENT

### Virtual Machine Information

| | |
|---|---|
| Name | win7_64_sp1_en_mso2016 |
| Description | win7_64_sp1_en_mso2016 |
| Architecture | x86 64-bit |
| Operating System | Windows 7 |
| Kernel Version | 6.1.7601.18741 (2e37f962-d699-492c-aaf3-f9f4e9770b1d) |
| Network Scheme Name | Local Gateway |
| Network Config Name | Local Gateway |

### Platform Information

| | |
|---|---|
| Platform Version | 4.4.0 |
| Dynamic Engine Version | 4.4.0 / 12/08/2021 19:04 |
| Static Engine Version | 4.4.0.0 / 2021-12-08 18:00:20 |
| AV Exceptions Version | 4.4.1.6 / 2021-12-14 15:06:27 |
| Link Detonation Heuristics Version | 4.4.1.7 / 2021-12-15 19:11:26 |
| Smart Memory Dumping Rules Version | 4.4.0.0 / 2021-12-08 18:00:20 |
| Signature Trust Store Version | 4.4.1.6 / 2021-12-14 15:06:27 |
| VMRay Threat Identifiers Version | 4.4.1.7 / 2021-12-15 19:11:26 |
| YARA Built-in Ruleset Version | 4.4.1.7 |

### Software Information

| | |
|---|---|
| Adobe Acrobat Reader Version | Not installed |
| Microsoft Office | 2016 |
| Microsoft Office Version | 16.0.4266.1003 |
| Hangul Office | Not installed |
| Hangul Office Version | Not installed |
| Internet Explorer Version | 8.0.7601.17514 |
| Chrome Version | Not installed |
| Firefox Version | Not installed |
| Flash Version | Not installed |
| Java Version | Not installed |

### System Information

| | |
|---|---|
| Sample Directory | C:\Users\kEecfMwgj\Desktop |
| Computer Name | Q9IATRKPRH |
| User Domain | Q9IATRKPRH |
| User Name | kEecfMwgj |
| User Profile | C:\Users\kEecfMwgj |
| Temp Directory | C:\Users\KEECFM~1\AppData\Local\Temp |
| System Root | C:\Windows |