

Threat Round Up for Oct 20 - Oct 27

blog.talosintelligence.com/2017/10/threat-round-up-1020-1017.html

AMP	✓
CWS	✓
Email Security	N/A
Network Security	N/A
Threat Grid	✓

Today, Talos is publishing a glimpse into the most prevalent threats we've observed between October 20 and October 27. As with previous round-ups, this post isn't meant to be an in-depth analysis. Instead, this post will summarize the threats we've observed by highlighting key behavior characteristics, indicators of compromise, and how our customers are automatically protected from these threats.

As a reminder, the information provided for the following threats in this post is non-exhaustive and current as of date of publication. Detection and coverage for the following threats is subject to updates pending additional threat or vulnerability analysis. For the most current information, please refer to your Firepower Management Center, Snort.org, or ClamAV.net.

The most prevalent threats highlighted in this round up are:

- **Doc.Macro.Downloader-6355564-0**

Office Macro

Word documents making use of VBA macros to download additional binaries to further compromise the system. This cluster focuses on VBA importing external Win32 API to download and execute a file with the presence of an obfuscated URL.

- **Doc.Macro.Obfuscation-6355576-0**

Office Macro

Word documents making use of VBA macro obfuscation techniques to evade detection and prevent quick analysis. This cluster focuses on the repeated use of base64 encoded data encapsulating a substring used to create the desired string for malicious use.

- **Win.Ransomware.Bucbi-6357228-0**

Ransomware

This is a ransomware variant that encrypts a user's data and demands that a Bitcoin ransom be paid. To achieve this, the malware performs code injection and set registry keys for persistence. Moreover, the samples contain anti-debugging techniques to hinder analysis.

- **Win.Trojan.Msil-6358223-2**

Trojan

This .NET trojan creates a shortcut file in the Windows Startup folder for persistence, drops and executes a malicious VBScript and a .bat file, and downloads additional files from different websites.

- **Win.Trojan.Tinba-6357827-1**

Trojan

Tinba (or TinyBanker, or Hupigon) is an information stealer and banking trojan. It is capable of hooking into several popular web browsers in order to gather credentials to send back to an attacker controlled C2. It is custom packed and code is injected into an instance of winver or Explorer (or both, in that consecutive order) before execution reaches its intended purpose.

- **Win.Trojan.Tovkater-6355575-0**

Trojan

This malware is able to download and upload files, inject malicious code, and install additional malware.

- **Win.Trojan.WillExec-6356235-0**

Trojan

This trojan injects into other processes, disables security features, and tries to contact several domains, waiting for instructions.

- **Win.Trojan.Zusy-6357526-0**

Trojan

This is a bank credential stealer which gathers online bank passwords, credit card numbers and social security numbers. The malware injects itself into winver.exe and explorer.exe.

Threats

Doc.Macro.Downloader-6355564-0

Indicators of Compromise

Registry Keys

N/A

Mutexes

N/A

IP Addresses

239[.]255[.]255[.]250

Domain Names

site[.]sitez3[.]com

Files and or directories created

- %WinDir%\SoftwareDistribution\DataStore\DataStore.edb
- %AppData%\Microsoft\Windows\Cookies\7OT1LGP2.txt
- %SystemDrive%\~\$1334139.doc
- \srvsvc
- %AppData%\Microsoft\Office\Recent\SAT_Documento741929.LNK
- \TEMP\SAT_Documento741929.doc

File Hashes

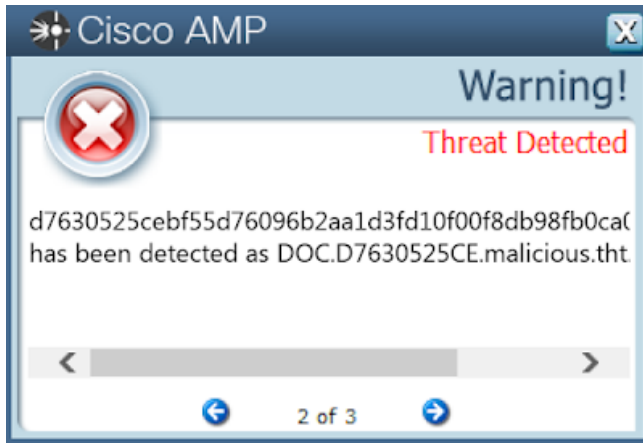
- d7630525cebf55d76096b2aa1d3fd10f00f8db98fb0ca0f9b5bdae5172913244
- 137dd479759fd525720874f4f94ee169950f46a41e7cc46b2159b10d28d61082
- 08d224602235aec498c31c1b1d16740d4ee294b5213a9236ff9ff09a8e07ae02
- 4922461d1524944042eb674ab0f04f43b9935c93c9cb6947f43dc546332161af
- 2d0b4e8f1d8f77838a97f1201fd114c63d19f67c7630725d04fd448c884e6b15
- 49cb1cde87383dc7b8feb70a3844cacb61bdbacbd67da19781be4ac67d8ca2f
- f18b9066ccb85df41cbd2686ce686324f7dadae23a0aecb58275dcbfa3db17b9
- 53c879eb61fa7079f1d78b97d79bf105dcd6eedbc65edf34634002c69c4a4db3
- 14da983e5dd73ca236f567fbbc09c7478f7575919b27b537cb0be0c87a1a808f
- 30a5a6f342fae27e81da59fa8a6c27e0730d0039bce9fbed961ec33e436f9961
- b6e105246ff47a3263900ca49c4ad8255b56f3a72edb9c98dcb605eb096c1d32
- 06d2b9d3ca2e2bfc445ebb738261b47ec02787add1aea864d202e12cbcf65d74
- 8af2f1175a4599c2c7bb5100a6fd6edf2f1094573aaf12b8d63bff1c4182059c
- bea666206a9648750da4653ca55159ba5cb1677a1cd4de1df9dd53c452890c49
- 0ce3c8f42aa43764e76fdf620e2b19abe70903d3aeb0302ab774535bfb6bc163
- 4bb72db17e61dae3990c448d88a4de41cc5ffc50ab64486d73bceb7ec2e92655
- a80d57a9b68a0cf17e21d23de8c9912ab08335f1ecf2f01470f51d65aad3fc98
- 20c4888614517caf7f87e79e4f1e83ab1aa518f8ad1c55fef0f3c9c031c34405
- c1f30a7bf8c953b6a75152b8c06c474682b8269a4422bebb5f44288e8abca6a0
- c965d63446d4f6a6a7f392c8497f8d4c121a80ca92027affda967d0edd342c62

Coverage

PRODUCT	PROTECTION
AMP	✓
CWS	✓
Email Security	N/A
Network Security	N/A
Threat Grid	✓
Umbrella	✓
WSA	✓

Screenshots of Detection

AMP

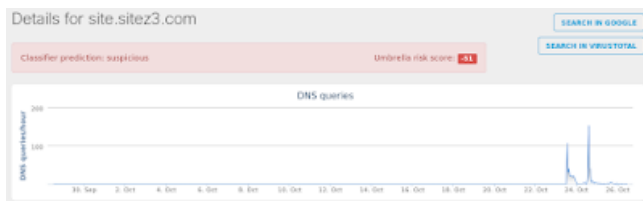


ThreatGrid

Behavioral indicators

Artifact Flagged Malicious by Antivirus Service	Severity: 100	Confidence: 100
A Document File with Embedded and Minimal Content Established Network Communications	Severity: 100	Confidence: 100
A Document File Established Network Communications	Severity: 100	Confidence: 100
Document Flagged by Antivirus	Severity: 100	Confidence: 100
VBA Macro Imports Function From External Library	Severity: 90	Confidence: 100
VBA Macro Reads Environment Variables	Severity: 80	Confidence: 100
Document Contains Embedded Material and Minimal Content	Severity: 80	Confidence: 100
Artifact Flagged by Antivirus	Severity: 80	Confidence: 100
VBA Macro Contains URL	Severity: 75	Confidence: 100
VBA Macro Has Action on Open	Severity: 70	Confidence: 100
Office Document Contains a VBA Macro	Severity: 70	Confidence: 100
Static Analysis Flagged Artifact As Anomalous	Severity: 60	Confidence: 100
DNS Response Contains Low Time to Live (TTL) Value	Severity: 30	Confidence: 100
Document Queried Domain	Severity: 20	Confidence: 100

Umbrella



Doc.Macro.Obfuscation-6355576-0

Indicators of Compromise

Registry Keys

N/A

Mutexes

- MC8D2645C
- Global\I98B68E3C
- MF4F51CA3
- Global\M98B68E3C

IP Addresses

- 81[.]169[.]145[.]76
- 194[.]88[.]246[.]9
- 239[.]255[.]255[.]250

Domain Names

puikprodukties[.]nl

Files and or directories created

- \Users\Administrator\Documents\20171025\PowerShell_transcript.PC.BQAZNa49.20171025072414.txt
- %SystemDrive%\Documents and Settings\Administrator\Local Settings\Temp\54180.exe
- %SystemDrive%\~\$690febddc8bf29d57cee5e527e3a386d0d32afa4ae9bc1fa4a18cf849f5be3.doc
- %WinDir%\AppCompat\Programs\RecentFileCache.bcf
- \TEMP\~\$690febddc8bf29d57cee5e527e3a386d0d32afa4ae9bc1fa4a18cf849f5be3.doc
- \TEMP\27690febddc8bf29d57cee5e527e3a386d0d32afa4ae9bc1fa4a18cf849f5be3.doc
- %WinDir%\SysWOW64\specsystem.exe

File Hashes

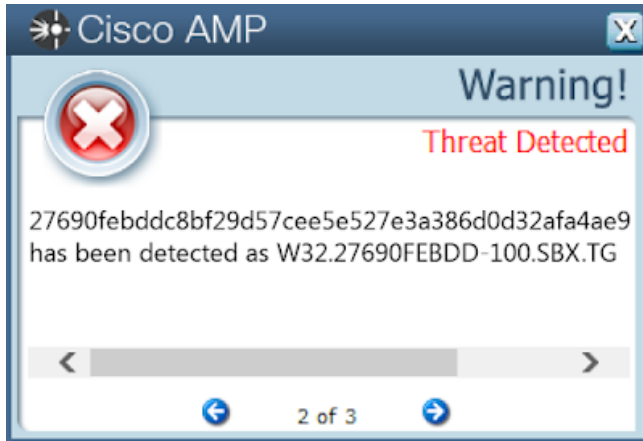
- 27690febddc8bf29d57cee5e527e3a386d0d32afa4ae9bc1fa4a18cf849f5be3
- 1ae79bf1ce63c3ea8d73f051cecb53d806bb477919d98257c363cb22d50410d1
- 74d3f7dc3417444e17a08c644807475c6b7b3e28316eb96a40877448417093c3
- 25aff8c96de125e1f922df676f3a117e07c0abb9e41b8d06bd6c995e614b8dec
- 664c26180cc669785d6e30140e07dfa538e66d8d9c38b9f1b8a94aecf9348fbe
- e135f8b2bd2588f94d47a084b75f0470fef7681c28fa0ddac71a80410beaea83
- 010e17653177339519c89f7ee9d67d4772928ae1c3eebaaf57191263ad2f4dbb
- 1f51f205991240c81a25d54d50cb05ffaa33a031560dea6d43e9423dc257c99d
- 61003d0b2697a5d457f8ef5fc219ec526dbdd41cb067230f3475edbb044ac649
- bb4795a99563991495f42f9b25395d5cc66d96cac7da4e4fbd1f6ae0f5019d18
- 31580e5f0462ce34241ab9d133edbaae3442840d1f5fd0a9958dd3cd0e750d7f
- 26bc8918448cc0fb9fb2d3f264006bb927ecc477b84f4f452606e2207e88f932
- 8aba5ce12e0df2f4fc6a58b4defbfc7fc0bae480740892d04f4fee9156f25ffd
- 9499a9a629a585fd75b7af3eacbc000c74a7eed240928a250ad580b8c8efc8d3
- 1e7de19e0636b8e224ce0d69b207d8bc5f8375b7bbc9228e43f426f5fdf05bc4
- a3fbecf3aa41c5b91274eb8c8319fd52c06fa5d20dc6c5f28bc535a8b17b2726
- 9131bc11a47c82ae466c719ab946fcac0a5e00e96e1bfc985d74e726526b4e84
- b6d69d0f0a3ee1dfb08f311c2ec0bab1b4e565ec4e03f23d555defdaf1b8dc9e
- 6e9d2d12a9d53fce2a16f63e18d970896f4a7f67bf40411c143fa3cf061ec4b8
- f1d99d9a6ff529ceba5bcfeffdea1aece875db4563838095f6382888842a7a
- 5f2eda2978e6da11ba9f29a398f100531ceda1ec44a49dc5b7e013f711a850ad
- 32453c24c8e36e93a594650554ecd730d5d00a466b764c1d774fc344b009d58a
- fc82b57b5f2aeafd2a602321afa4a7f9a33ea0575f0329786b5c2598abef57a7
- fdd0acbddd96dd0fb72ca78fa84dca24577796e1cd977206280bc5ac715f32d02
- 640976b9ad42936e9cc75778292bb28f402321883a124a674a5a6551df481781

Coverage

PRODUCT	PROTECTION
AMP	✓
CWS	✓
Email Security	N/A
Network Security	N/A
Threat Grid	✓
Umbrella	✓
WSA	✓

Screenshots of Detection

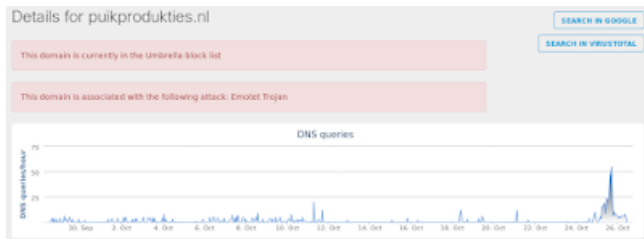
AMP



ThreatGrid

Behavioral Indicators	
Office Document Launches a Powershell	Severity: 100 Confidence: 100
Document with Random Variables Established Network Communications	Severity: 100 Confidence: 65
A Suspicious Document Containing Randomized Variable Names Detected	Severity: 65 Confidence: 100
Artifact Flagged Malicious by Antivirus	Severity: 100 Confidence: 65
Artifact Flagged as Known Trojan by Antivirus	Severity: 100 Confidence: 65
A Document File with Embedded and Minimal Content Established Network Communications	Severity: 100 Confidence: 65
A Document File Established Network Communications	Severity: 100 Confidence: 65
Document Launched Utility Application	Severity: 100 Confidence: 65
Document Flagged by Antivirus	Severity: 65 Confidence: 100
Office Document Launches a Command Shell	Severity: 65 Confidence: 100
Command Line Obfuscation Detected	Severity: 100 Confidence: 65
An Embedded VBA Macro Contains Randomly Generated Variables	Severity: 65 Confidence: 65
Antivirus Service Flagged Artifact As Likely Malicious	Severity: 65 Confidence: 65
Document Contains Embedded Material and Minimal Content	Severity: 65 Confidence: 65
Artifact Flagged by Antivirus	Severity: 65 Confidence: 65
Process Modified an Executable File	Severity: 65 Confidence: 100
VBA Macro Has Action on Open	Severity: 35 Confidence: 65
Outbound HTTP GET Request	Severity: 35 Confidence: 35
Antivirus Service Flagged Artifact As Containing A Macro	Severity: 35 Confidence: 65
Process Modified File in a User Directory	Severity: 35 Confidence: 65
Office Document Contains a VBA Macro	Severity: 35 Confidence: 65
PowerShell Used With Encoded Command	Severity: 65 Confidence: 35
HTTP Request with Blank or Missing User-Agent	Severity: 65 Confidence: 65
Dynamic Content Detected in Document	Severity: 65 Confidence: 65
Command Exe File Execution Detected	Severity: 65 Confidence: 65
Process Uses Very Large Command-Line	Severity: 65 Confidence: 65
File Downloaded to Disk	Severity: 35 Confidence: 65
Potential Code Injection Detected	Severity: 35 Confidence: 35
DNS Response Contains Low Time to Live (TTL) Value	Severity: 35 Confidence: 35
Document Queried Domain	Severity: 35 Confidence: 35

Umbrella



Win.Ransomware.Bucbi-6357228-0

Indicators of Compromise

Registry Keys

- <HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\CONNECTIONS
Value: SavedLegacySettings
- <HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP
Value: IntranetName
- <HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP
Value: AutoDetect
- <HKLM>\SOFTWARE\WOW6432NODE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP
Value: IntranetName
- <HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\5.0\CACHE\CONTENT
Value: CachePrefix
- <HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\5.0\CACHE\HISTORY
Value: CachePrefix
- <HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\5.0\CACHE\COOKIES
Value: CachePrefix
- <HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS
Value: ProxyServer
- <HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP
Value: UNCAAsIntranet
- <HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\CONNECTIONS
Value: DefaultConnectionSettings
- <HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP
Value: ProxyBypass
- <HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN
Value: internat.exe
- <HKLM>\SOFTWARE\WOW6432NODE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP
Value: ProxyBypass
- <HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS
Value: AutoConfigURL
- <HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS

Value: ProxyEnable

- <HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS
Value: AutoDetect
- <HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS
Value: ProxyOverride
- <HKCU>\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
- <HKU>\Software\Microsoft\Windows\CurrentVersion\Run
- <HKCU>\Software\Microsoft\Windows\CurrentVersion\Run
- <HKCU>\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\
- <HKLM>\System\CurrentControlSet\Services\Tcpip\Parameters
- <HKCU>\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings

Mutexes

- Local\ZonesCacheCounterMutex
- Local\ZonesLockedCacheCounterMutex

IP Addresses

N/A

Domain Names

- shalunishka12[.]org
- caprice-porn[.]com

Files and or directories created

- %SystemDrive%\Documents and Settings\Administrator\Local Settings\Application Data\lqwrnvdl.exe
- \Users\Administrator\AppData\Local\wikqsupt.exe
- \Users\Administrator\AppData\Local\lpcqdivf

File Hashes

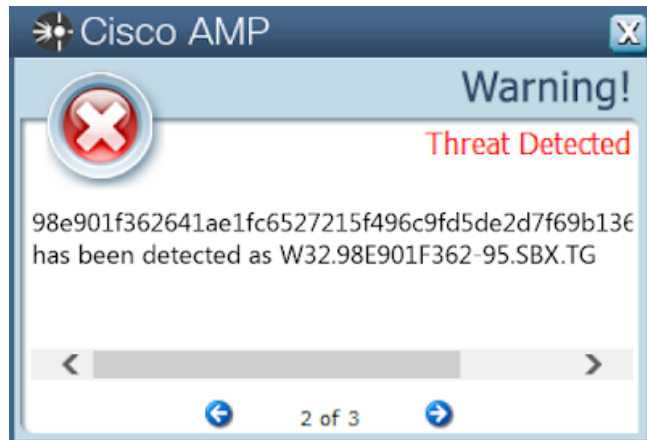
- 98e901f362641ae1fc6527215f496c9fd5de2d7f69b136ac610e453469831d07
- 6edf7c043348efe02d94c97a4d06ec735fb90a77ea290509e03991edadb24716
- f51719dfeac4f52a90d52188c3b3e9145d77f612da784510c968564aa0d46e9e
- 713413ee1a008b91a6afb29c52d2beda829778b8072c5ba5171bb50277104ebc
- a65293abd10e7c4a306ddfae94c67df2db411c4a29ca71a1ca8169ee640a8ed3
- feecc0baccecabeddc8f0e07b3a7aa54d7f13d60e232b7a538b10cd773b4c5e5

Coverage

PRODUCT	PROTECTION
AMP	✓
CWS	✓
Email Security	✓
Network Security	N/A
Threat Grid	✓
Umbrella	✓
WSA	✓

Screenshots of Detection

AMP



ThreatGrid

Behavioral indicators	
Artifact Flagged Malicious by Antivirus Service	Severity: 100 Confidence: 100
Registry Persistence Mechanism Refers to an Executable in a User Data Directory	Severity: 99 Confidence: 100
Process Deleted the Submitted File	Severity: 99 Confidence: 100
Process Modified an Executable File	Severity: 69 Confidence: 100
Process Modified File in a User Directory	Severity: 79 Confidence: 100
Process Modified Autorun Registry Key Value	Severity: 98 Confidence: 100
Potential Code Injection Detected	Severity: 98 Confidence: 100
PE Checksum is Invalid	Severity: 98 Confidence: 100
DNS Query Returned Non-Existent Domain	Severity: 25 Confidence: 15
PE Resource Indicates Russian Origin	Severity: 25 Confidence: 100
Sample flagged by antivirus service contacted domain	Severity: 25 Confidence: 100
Executable Imported the hDebuggerPresent Symbol	Severity: 25 Confidence: 100

Umbrella



Win.Trojan.Msil-6358223-2

Indicators of Compromise

Registry Keys

- <HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\5.0\CACHE\HISTORY
Value: CachePrefix
- <HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\5.0\CACHE\COOKIES
Value: CachePrefix
- <HKLM>\SAM\SAM\DOMAINS\ACCOUNT\USERS\000003E9
Value: F
- <HKLM>\SAM\SAM\DOMAINS\ACCOUNT\USERS\000003EC

Value: F

- <HKLM>\SAM\SAM\DOMAINS\ACCOUNT\USERS\000001F5

Value: F

- <HKCU>\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage2
- <HKCU>\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
- <HKLM>\System\CurrentControlSet\Control\SecurityProviders\Schannel
- <HKCU>\Software\Microsoft\GDIPPlus

Mutexes

RasPbFile

IP Addresses

- 185[.]182[.]56[.]160
- 104[.]18[.]48[.]20
- 104[.]27[.]162[.]68
- 104[.]27[.]163[.]68
- 104[.]18[.]49[.]20

Domain Names

- paste[.]ee
- artishoker[.]com
- c[.]lewd[.]se

Files and or directories created

- %SystemDrive%\Documents and Settings\Administrator\Start Menu\Programs\Startup\KiuFCoY1QO9PiPVC.vbs
- \srvsvc
- %AppData%\Microsoft\Windows\Start Menu\Programs\Startup\KiuFCoY1QO9PiPVC.Ink
- %AppData%\Microsoft\Windows\Start Menu\Programs\Startup\KiuFCoY1QO9PiPVC.vbs
- %SystemDrive%\Documents and Settings\Administrator\Start Menu\Programs\Startup\KiuFCoY1QO9PiPVC.Ink
- \TEMP\Scanned_Purchase_order_image277253491.exe
- %TEMP%\1861034378.bat
- %AppData%\KiuFCoY1QO9PiPVC.exe

File Hashes

- e32a39503459bad0542ccbb75e9fb1f9dcd97784f14a34ac5baac20875984c1d
- 2549362e299c04fd309af6034c8edca26cb4666de123d948a729a6bb98959a02
- 1948216f19bdb2e0cd2d09d89611eec211dca86618d4d7be5c743b1433bce38b
- 91c6d351305ee145d33df951155c6700294d1caec3a3738ba758d35e98cb9b75
- ceffc973720d74d3afebfd38a6af2edd8237a875e1b636e794ea060220aeb4d2
- 7cbc85a09bebdd5675e9ddb74496c60ffa67558a0978f9c619e963ca9ba7b9a6
- 34eaf73bb07d3d0f9577d79283975a42566f193f61fbcaee616a2a4a366dbb28
- fbcacee6765ed156ce5751205b67efc2d8fdd2ef76cdfa67e157db0d7688031a
- d3014617acb71109befeea10e57b4b8fb7b8df05f66a55bb47d85f904b1ee32c
- 3e98b03a47e0629f095fcdca6ca15dc48ec72b1af36711a41785547dfabfe1af9
- 9fd2b95cae0407e03575992690ffb155017fbdf9580b4466705f03601d01d0e3
- fbcacee6765ed156ce5751205b67efc2d8fdd2ef76cdfa67e157db0d7688031a
- 0cb8711d1f2a856178c34915f204a1af2b62b145c7817b9eee90ec1ae13ed6a2
- cab3246e2d185bb58c3e1163f520efe300832277f24336a647e5457380ef53d6
- ddc57143d6d212eecef60cb8ed95afa728425f976bc1db5eed74f2aa13228257
- c66c8be8191cefb7949fc13c7ef7f39bd2cd621c5d2f401bdec5d9e5ab738222
- b0b52c73ed116a84c16c1b71bab68fb1a669cbcafb0b06c676a6f3577ba7c555
- 411aff7bcef1f9b1f00b35f0d4fbf2ea42bea72931489fce1b3edaa327f44485b

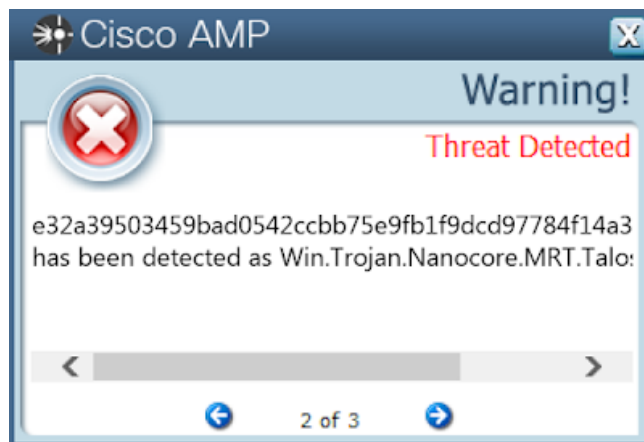
- b1149077c5a8c4f9730d5db86d0cb19229cf192768d3eb30de2778c6529bd0b7
- 88e4751e486257ae14bfc4cd1c7bc5f5af5568314c54be43b6e02c8c852e93f7
- f19685621ec16a3c2810852acd1219e4d386119e0902486361fd2aa0d5ed3add
- 87f9d1b5d26155470684a6410dad447ed93307428a71115bbbfce22dd34fb00c
- 8f65d213186372f0eccee43e3f00ac145e9080858f1b384bf8faf4a39797a979
- 251b9967ce0b664734a3fc072ec89a120df406b796364de84c83305d89a6d747
- 1948216f19bdb2e0cd2d09d89611eec211dca86618d4d7be5c743b1433bce38b
- b536330f0d2028e2d561582fd1d4053860d54fe09b40212f8cb8ac8359241dac
- 7e2a3692d653fa12120f96b10a03e9f2adb4fb009bb941c66a00182427723b79
- ac98dab0fa4cefa816e001737ae5a8f1f08c8851d8afb8c9e75f722366705b0e
- 56690111926e192663f3cdc04b540a1bfb6d498690d17d360082d57ec7569f5
- a611edd1273d31162da5a216b00d1460c433479719575018cd1cefd6a0fb297b
- 868ed435b09074e559bfc5dab4aeb3ff1d766d0f31132ea0c8010a1eeb7f1d
- dc38e69467f8d08621b498eb59f58f9139a4373c15c0567ad15d531f0aeb4766
- c51c9254f951f491aafb9b4fb2098189db4fed06b065162c4c288b072a85c60b

Coverage

PRODUCT	PROTECTION
AMP	✓
CWS	✓
Email Security	N/A
Network Security	N/A
Threat Grid	✓
Umbrella	✓
WSA	✓

Screenshots of Detection

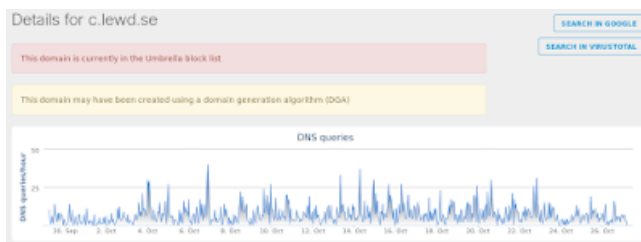
AMP



ThreatGrid

Behavioral indicators		
Excessive Remote Process Code Injection Detected	Severity: 85	Confidence: 100
Artifact Flagged Malicious by Antivirus Service	Severity: 100	Confidence: 85
Process Hollowing Detected	Severity: 100	Confidence: 85
Shortcut Added in the Windows Startup Folder	Severity: 95	Confidence: 75
A VBScript Invoked Run Method On Created Object	Severity: 85	Confidence: 85
Process Deleted the Submitted File	Severity: 85	Confidence: 85
VBScript May Call Shell	Severity: 85	Confidence: 85
Process Attempted to Access the Firefox Password Manager Local Database	Severity: 95	Confidence: 75
Process Modified an Executable File	Severity: 85	Confidence: 100
Outbound HTTP GET Request	Severity: 75	Confidence: 75
Process Modified File in a User Directory	Severity: 75	Confidence: 85
Command Exe File Execution Detected	Severity: 85	Confidence: 85
Process Created a File in the Windows Start Menu Folder	Severity: 85	Confidence: 85
Sample Created A Visual Basic Script	Severity: 85	Confidence: 85
Potential Code Injection Detected	Severity: 85	Confidence: 85
Sample Created A Batch File	Severity: 85	Confidence: 85
HTTP Client Error Response	Severity: 85	Confidence: 85
Executable Artifact Uses .NET	Severity: 85	Confidence: 85
Process Read IN File	Severity: 85	Confidence: 85
Executable with Encrypted Sections	Severity: 85	Confidence: 85
DNS Response Contains Low Time to Live (TTL) Value	Severity: 85	Confidence: 85

Umbrella



Win.Trojan.Tinba-6357827-1

Indicators of Compromise

Registry Keys

- <HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN
Value: F9E7DE7B
- <HKU>\Software\Microsoft\Windows\CurrentVersion\Run

Mutexes

- F9E7DE7B
- \BaseNamedObjects\5D79E0A3

IP Addresses

216[.]218[.]185[.]162

Domain Names

spaines[.]pw

Files and or directories created

- %AppData%\5D79E0A3\bin.exe
- %AppData%\F9E7DE7B\bin.exe

File Hashes

- 1a011db2ad073700f1ac9eaaf9760bf4c6569af894ff847520ea2918ea9228ee

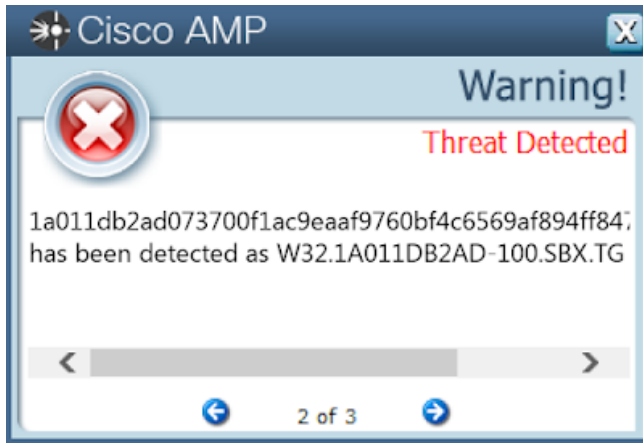
- 2e125dcdec21f24ec0834fea0df684a0db2fe1f3c6556694f7c1e44259c34bae
- 664cd8de35ff1318c294bdca6390aa4bd434bd0270ae997a60a1e6772a50626b
- 883939af8de0ceb28c3e4d508b7815a1518148a1e253e8df979e95f8a697c3f1
- fc5e9a478435e9dac68b036779cec6fea60be92e852ba2f31ca2234550937670
- e488fc3c2381c55fcc2a7a59c36b39bcba20e4a37640bb45238607cb7e2062a1
- fef91305f435a16413c87b1db1e0891fdebba6eaa06a6ab4f3464e86a274e36e
- 69c82a3f309d7727631925cafb134077613689a78143523a12a335af9c8014fd
- 683d8a111660b32f7b928d0375388a64bf4c1a709a20b5997f39f1649751b656
- 35f336aad0bb9ea07e8f49b0e10105a8bc31dc9d79c302ed594ca3d47f3aedf2
- d9f7dad10fe09eb4586b1156caf25f490dbe285eb6c5f5598cc6f525e559f319
- 9ff90fcb71b6d0c44de05e9bc909778ebdcb743ea7a0ce6da42b06ea9126153a
- c50c70f782a7027ddfb9f40cf7fa09ba026db2e966485532c698020feb5092e1
- feab7aea76929e0eea394f319ac9943431ac408ac04b0682ec28c5208d2c0143
- 719b78cd00d5d5fd5da3fa786e8f9093169517d6d376dff95572bdd64092a282
- 1f4524411c3d875259f8ab03d7d8d2e6eff55a603d2986cd36e006ad7091df97
- 96e7b9cdf921c06747e68e19ed01c32eb3b8b2cfabde164dd993c75ccecef917
- 0e00dd23c72c45f60eb7fc7581a93e5b4975997108969a28bddb1b1dfa170ace
- ad3fac8f3b7e49c251cf829817f4f077072b7d9e4e697638836e4fccfee5693d
- 373ce9827a9626148e5c343250015be1fd6df270141f37129586321ba72ee601
- 5dbf9fb9db064cdc48d0b7e23aa50f7c22341b11ab848efe90c7355ff2f9d030
- e6d9afa1df88be5c5bc05c9b1fa4744aa8118c22eebc898769a96ad835c5e6e8
- dd72936abfd9887928cec7649f427c676067f05cbd23ba0e85f50533af49b2dd
- 4ac17bc6cbd38f7e0a93e221abd71a1771804871adf6638eefae70a36693dba6
- b04c4527a35a70d945eed540a6373bb2db4cae3a5c8ed79266d40f527f7e74a8

Coverage

PRODUCT	PROTECTION
AMP	✓
CWS	✓
Email Security	✓
Network Security	✓
Threat Grid	✓
Umbrella	✓
WSA	✓

Screenshots of Detection

AMP



ThreatGrid

Behavioral indicators

TinyBanker Trojan Detected	Severity: 100 Confidence: 100
Excessive Remote Process Code Injection Detected	Severity: 95 Confidence: 100
Artifact Flagged Malicious by Avbivirus Service	Severity: 100 Confidence: 65
Registry Persistence Mechanism Refers to an Executable in a User Data Directory	Severity: 60 Confidence: 100
File Name of Executable on Disk Does Not Match Original File Name	Severity: 40 Confidence: 60
Process Modified an Executable File	Severity: 40 Confidence: 100
Process Modified File in a User Directory	Severity: 35 Confidence: 80
Decey Document Detected	Severity: 35 Confidence: 80
Process Modified Autorun Registry Key Value	Severity: 35 Confidence: 80
Task Creation Detected	Severity: 35 Confidence: 80
Potential Code Injection Detected	Severity: 35 Confidence: 35
Hook Procedure Detected in Executable	Severity: 35 Confidence: 80
Executable with Encrypted Sections	Severity: 35 Confidence: 35
Executable Imported the IsDebuggerPresent Symbol	Severity: 25 Confidence: 35

Umbrella



Win.Trojan.Tovkater-6355575-0

Indicators of Compromise

Registry Keys

- <HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP
Value: IntranetName
- <HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS
Value: ProxyServer

- <HKLM>\SOFTWARE\WOW6432NODE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP
Value: ProxyBypass
- <HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP
Value: ProxyBypass
- <HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS
Value: AutoConfigURL
- <HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS
Value: AutoDetect
- <HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS
Value: ProxyOverride

Mutexes

- !IECompat!Mutex
- Global\C::Users\Administrator\AppData\Local\Microsoft\Windows\Explorer:thumbcache_idx.db!rwReaderRefs
- Global\C::Users\Administrator\AppData\Local\Microsoft\Windows\Explorer:thumbcache_idx.db!ThumbnailCacheInit
- MutexNPA_UnitVersioning_1288
- \BaseNamedObjects\MutexNPA_UnitVersioning_1908

IP Addresses

- 185[.]80[.]54[.]18
- 239[.]255[.]255[.]250

Domain Names

chubbyoasis[.]top

Files and or directories created

- %TEMP%\nspB3BE.tmp\nsJSON.dll
- %TEMP%\nspB3BE.tmp\ihovet312.exe
- %Public%\Desktop\Download Download.lnk
- %TEMP%\nspB3BE.tmp\crub.exe

File Hashes

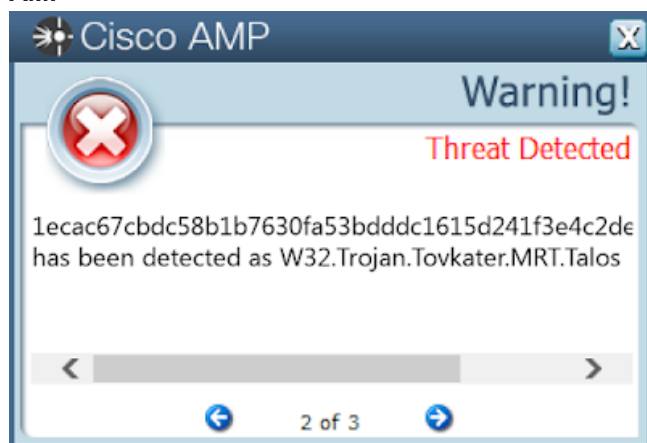
- 00e2316602cdc220d7d96b51ddb30c8686768172aa690dca61299599b432e4e1
- 09c6d7aa165da344e09575978d4ed279bfc7b538a21d19d8a983bf6c53f6fd63
- 0cc22fdb99248307ad676f62fdeea54bf531a4a736db87a68b5e99200fa22346
- 0d5abc8055d7075ddc380a2244c048be7df2e1528625f178bae28b9a385d8059
- 37e58e7f9c958a84bc1f9e993b88ac35b208835bcd78de647e61acca0674ffc5
- 390c133ff17c3dba9ad6a1f23300259a25bf347ce1871b7bda3137e2793dea9c
- 46266424dc446fa849f32e390c72f2158937de669596d1604e7debfe42d4b08c
- 4d1aa1730c5c825513dcab70b2d953f0b410a7d77ae24c37c80a6c7b064a84cc
- 5fe7ab0b58112c10da05503e9d16429bde3cfe4fc6a6084354ad2e53ce174ead
- 629988c5c0eca9431d34ec6c62966e0f524b60f9d958d34481bc7bd320ab530a
- 6daf4f85fd756c9f348bf6c37361933725c44866c9a0fd48f75b37459dc1c82f
- 6e302beef11ceff3ce6d7578f21bc5fb63ff95b30b3bc1bab6ee56d82aeaaa81
- 7aa4bc907b1db2373c3429b54f29ad7a8e2c26d8075dce51e2019b3908123d6b
- 993e6ca19189fc218aa72a58914fd44a18e928fd8d57cda419d5d707c80b8d56
- ac0cee4f6a3e327ea011b790f1bd279ff835e0af32f0f6a944c20ceee60ae65c
- acb488c1a11f6e4c74bb16677266f90136f636564660b3365b9cadf58a3b2fe0
- b3bf68fc33b354a9387dd582f348ce7c739a96cbf18a52398d8f67ecbcbdf04b0
- be030179649c3c286ba386ce87cf2a7db4257b463d40d2fffd571801099f2209
- c620f230d09552f28a405d77f0a0aec3503a59fe329b01150ad975651419929f
- d6f21beb7b1033bef5de62b26e6e378909ddd54104cd92b2a0d359ef62f8d020
- e2197aebd08c65fb547461f7d4f3a86a70008743701828fbad4ff58266850958

Coverage

PRODUCT	PROTECTION
AMP	✓
CWS	✓
Email Security	N/A
Network Security	✓
Threat Grid	✓
Umbrella	✓
WSA	✓

Screenshots of Detection

AMP



ThreatGrid

Behavioral indicators	
Artifact Flagged Malicious by Antivirus Service	Severity 100 Confidence 93
Downloaded Packed, Encrypted or Encoded PE	Severity 100 Confidence 83
File Name of Executable on Disk Does Not Match Original File Name	Severity 80 Confidence 83
Process Modified an Executable File	Severity 80 Confidence 100
Outbound HTTP GET Request	Severity 35 Confidence 35
Process Modified File in a User Directory	Severity 30 Confidence 80
Static Analysis Flagged Artifact As VM Aware	Severity 30 Confidence 80
Downloaded PE Executable	Severity 80 Confidence 80
File Uploaded to the Network	Severity 80 Confidence 80
File Downloaded to Disk	Severity 30 Confidence 80
Potential Code Injection Detected	Severity 80 Confidence 80
PE Has Sections Marked Executable and Writable	Severity 80 Confidence 80
PE Contains TLS Callback Entries	Severity 80 Confidence 80
Executable with Encrypted Sections	Severity 30 Confidence 80
Nullsoft Installer Detected	Severity 30 Confidence 80
Executable Packed with UPX	Severity 30 Confidence 80
Outbound HTTP POST Communications	Severity 35 Confidence 35
Outbound Communications to Nginx Web Server	Severity 35 Confidence 35
Sample Flagged by antivirus service contacted domain	Severity 35 Confidence 35
Executable Imported the IsDebuggerPresent Symbol	Severity 30 Confidence 35
PE COFF Header Timestamp is Set to Date Prior to 1999	Severity 3 Confidence 80

Umbrella



Win.Trojan.WillExec-6356235-0

Indicators of Compromise

Registry Keys

- <HKLM>\SYSTEM\CONTROLSET001\SERVICES\WUAUSERV
Value: DelayedAutostart
- <HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN
Value: dgprf
- <HKLM>\SOFTWARE\POLICIES\MICROSOFT\WINDOWS DEFENDER
Value: DisableAntiSpyware
- <HKLM>\SYSTEM\CONTROLSET001\SERVICES\WUAUSERV
Value: Start
- <HKCU>\Software\Microsoft\Windows\CurrentVersion\Run
- <HKLM>\SOFTWARE\Wow6432Node\Policies\Microsoft\Windows Defender

Mutexes

Hej2ffi2jd4slfe

IP Addresses

N/A

Domain Names

- LKEXIVL[.]RU
- HDYKVXN[.]RU
- ebfrtgx[.]ru
- PIBSCXI[.]RU
- indvaws[.]ru
- mfwvokl[.]ru
- UOEVSFM[.]RU
- JTPXQRU[.]RU
- KAQELMY[.]RU
- BGYMVRR[.]RU
- XQTNVLM[.]RU
- lkexivl[.]ru
- MFWVOKL[.]RU
- EBFRTGX[.]RU
- HTTHUED[.]RU
- dtrxcms[.]ru
- QTKIHPS[.]RU

- lqwuhot[.]ru
- bgymvrr[.]ru
- UPSCDOQ[.]RU
- DTRXCMS[.]RU
- qtkihps[.]ru
- FACJGHS[.]RU
- pibscxi[.]ru
- xlvudsp[.]ru
- rmcltni[.]ru
- LTYHVWD[.]RU
- ADOHBTT[.]RU
- hdykvxn[.]ru
- xqtnvlm[.]ru
- upscdoq[.]ru
- LQWUHOT[.]RU
- facjghs[.]ru
- INDVAWS[.]RU
- htthued[.]ru
- XLVUDSP[.]RU
- jtpxqru[.]ru
- RMCLTNI[.]RU
- ltyhwd[.]ru
- kaqelmy[.]ru
- uoevsfm[.]ru
- adohbtt[.]ru

Files and or directories created

- %TEMP%\dd.te
- %AppData%\xxudxudr\ucqupaug.exe

File Hashes

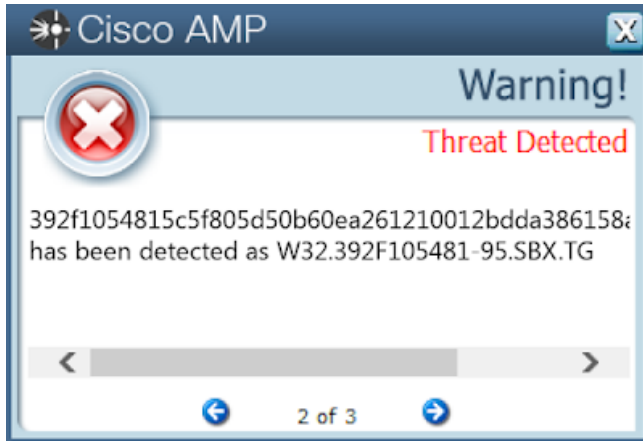
- 392f1054815c5f805d50b60ea261210012bdda386158a1da92d992a929eb77c2
- 03b2164da6318fff63b6cad2fc613c3d885bd65432a7b8744c2b1709f2f9a479
- 69a36e6f12b4e9b9cd15528a068385f2311b0c540336c142aabdd73c2a2e2015
- a63a5639d0cb6a10f7af5bd0dd30ca1800958a0f5bb47f358b6d37f51d0f0a31
- 2ae61c8c2a8e83cde33f38b89599032a6fb455256aa414a15f2724c94d3460d2
- 40cfb7b7fad1602276ebf3fa63514ba91be6186d5d3bd190f593bdec0b6d8d64
- 76d7a19cd2700dfe9e209f7a90b65f505ea14936dca3a5b00bd3b61c2c6ee386
- 9a339f2cbd25fcd821e6a1d37744280007f4ce016e93c6fb8c7c9e0ef8dfaf06
- a012c26e70ecdc13a644ef53d1202d3d1b2a53c70046ccedb12c97a00844ef73
- fa7e5cdf59d30ade201e91f0543a03f581ff5f95ddc74bccf7590663de3a6a01

Coverage

PRODUCT	PROTECTION
AMP	✓
CWS	✓
Email Security	✓
Network Security	N/A
Threat Grid	✓
Umbrella	✓
WSA	✓

Screenshots of Detection

AMP



ThreatGrid

Behavioral indicators	
Artifact Flagged Malicious by Antivirus Service	Severity 100 Confidence 65
Process Following Detected	Severity 100 Confidence 93
Excessive Number of DNS Queries Returned Non-Existent Domain	Severity 65 Confidence 100
Registry Persistence Mechanism Refers to an Executable in a User Data Directory	Severity 60 Confidence 100
Detected Attempts To Lookup Several Randomly Named Domains	Severity 100 Confidence 93
Excessive Number of DNS Queries	Severity 70 Confidence 100
Process Modified an Executable File	Severity 60 Confidence 100
Process Modified File in a User Directory	Severity 70 Confidence 85
Process Started a Service Using the SC Utility	Severity 80 Confidence 100
Process Stopped a Service Using the SC Utility	Severity 80 Confidence 100
Process Modified Autorun Registry Key Value	Severity 80 Confidence 80
Command Exe File Execution Detected	Severity 80 Confidence 80
Potential Code Injection Detected	Severity 50 Confidence 80
DNS Query Returned Non-Existent Domain	Severity 35 Confidence 35
Process Modified Registry Settings Using Reg Utility	Severity 30 Confidence 80
Executable Uses Armadillo	Severity 30 Confidence 30
Sample Flagged by antivirus service contacted domain	Severity 25 Confidence 35

Umbrella



Win.Trojan.Zusy-6357526-0

Indicators of Compromise

Registry Keys

- <HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN
Value: F9E7DE7B
- <HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN
Value: internat.exe
- <HKCU>\Software\Microsoft\Windows\CurrentVersion\Run
- <HKU>\Software\Microsoft\Windows\CurrentVersion\Run

Mutexes

- F9E7DE7B
- \BaseNamedObjects\5D79E0A3

IP Addresses

- 239[.]255[.]255[.]250
- 216[.]218[.]185[.]162

Domain Names

spaines[.]pw

Files and or directories created

- %AppData%\5D79E0A3\bin.exe
- %AppData%\F9E7DE7B\bin.exe

File Hashes

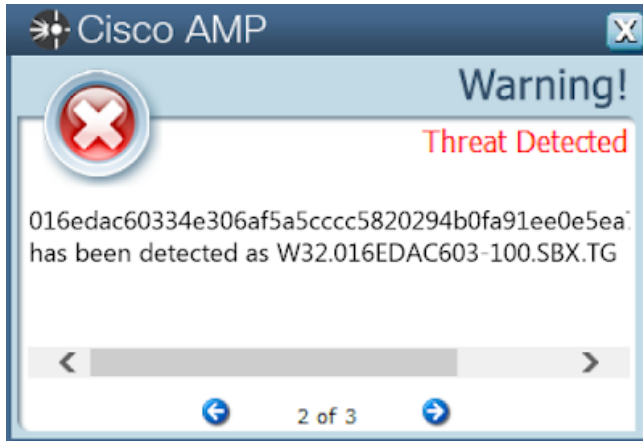
- 016edac60334e306af5a5cccc5820294b0fa91ee0e5ea71e655c4632e8998347
- bdd213dad416f81f8b76a7463c20500ee789c8d44371cf62c061a0aa6c232472
- b1fd5250ab7300da229a091f58e655e2aade24c38cd280af4cd8cb79af30203
- 1d2b1f2f844f40bcbdf614d4c38d3c4fde7a36d9102b7e13cc05abfa2c6bf593
- a27d0e059e9d56b31e06899bd7287ee8e05f10b8da04124d9ad1fbc633cff893
- 3c27beb77c3261ceb55eaae2d32a193ca4a53432a3a188fd9494202b94736522
- b5b46370c593ae3c32042355ff5d234b597d4f2685706f4f978006834483a689
- 13bf1d8d2fc96ec4ad92225a77d212e2d41ad09ffee5061de73124a6662aa792
- 1c5ba0cb523cd3c713c24c75cfa28885ef542f2226b25151ebafa3ecdde4e827
- eef6f6d965da6f45e376eb9e5e01451ea110466e4b02780625cd5170edad4119

Coverage

PRODUCT	PROTECTION
AMP	✓
CWS	✓
Email Security	✓
Network Security	✓
Threat Grid	✓
Umbrella	✓
WSA	✓

Screenshots of Detection

AMP



ThreatGrid

Behavioral indicators	
TinyBanker Trojan Detected	Severity: 100 Confidence: 100
Excessive Remote Process Code Injection Detected	Severity: 65 Confidence: 100
Artifact Flagged Malicious by Antivirus Service	Severity: 100 Confidence: 65
Registry Persistence Mechanism Refers to an Executable in a User Data Directory	Severity: 60 Confidence: 100
File Name of Executable on Disk Does Not Match Original File Name	Severity: 60 Confidence: 60
Process Modified an Executable File	Severity: 60 Confidence: 100
Process Modified File in a User Directory	Severity: 70 Confidence: 60
Decey Document Detected	Severity: 70 Confidence: 60
Process Modified Autorun Registry Key Value	Severity: 60 Confidence: 60
Process Uses Very Large Command-Line	Severity: 60 Confidence: 60
Task Creation Detected	Severity: 50 Confidence: 60
Potential Code Injection Detected	Severity: 50 Confidence: 60
Hook Procedure Detected in Executable	Severity: 30 Confidence: 60
Executable with Encrypted Sections	Severity: 30 Confidence: 60
Executable Imported the hDebuggerPresent Symbol	Severity: 20 Confidence: 60

Umbrella

Details for spaines.pw

SEARCH IN GOOGLE

SEARCH IN VIRUSTOTAL

One or more of the IP addresses that this domain resolves to are currently blocked by Umbrella:
216.238.385.162

This domain is currently in the Umbrella block list

This domain is associated with the following attack: Tinba Trojan

This domain has a suspicious prefix score

Classifier prediction: suspicious

Umbrella risk score: **63**

