Jan 04 2024

NETMANAGEIT

Intelligence Report

CVE-2017-11882 To Deliver Agent Tesla

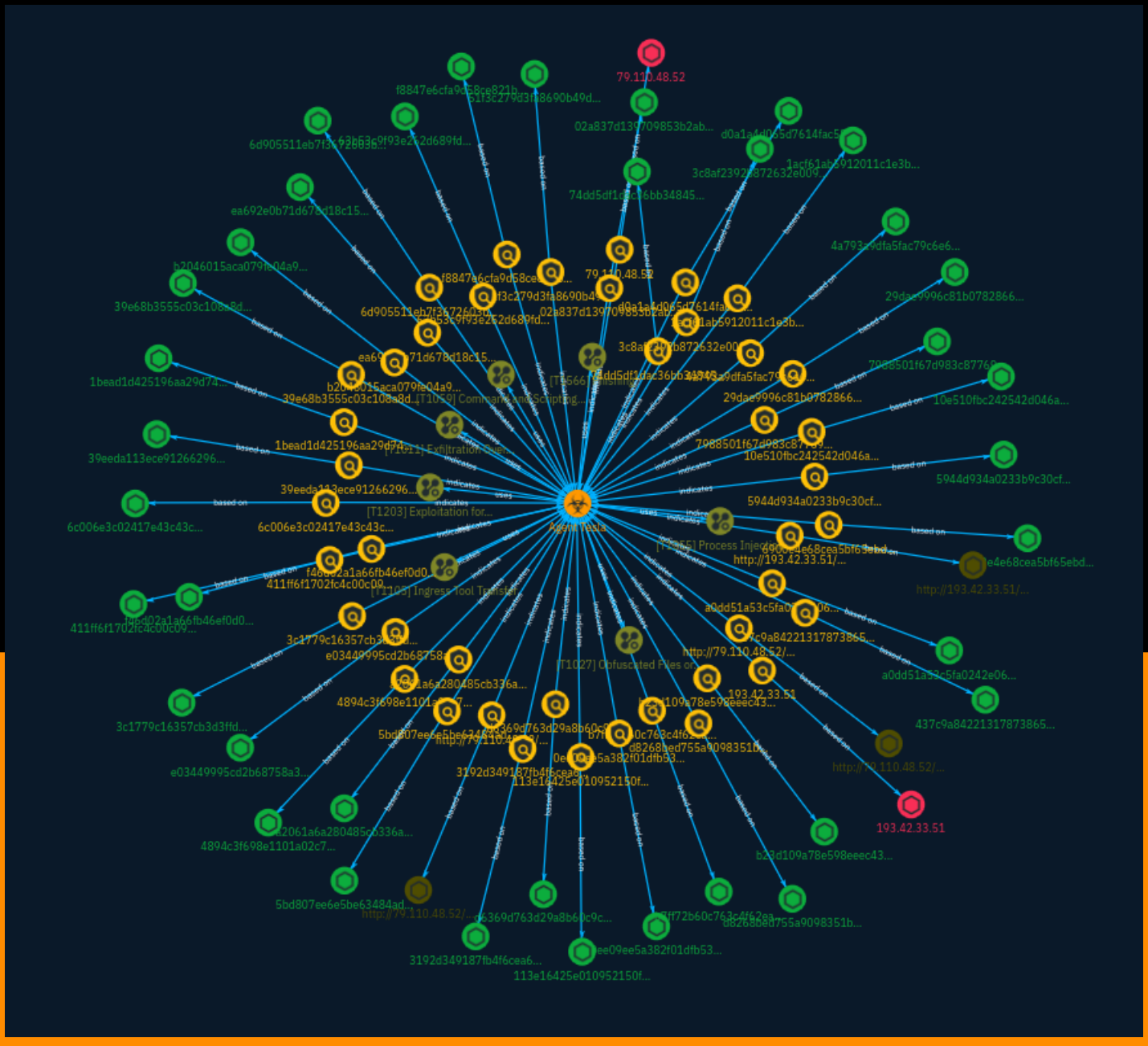

Table of contents

Overview

Entities

Observables

External References

Overview

Description

First discovered in 2014, Agent Tesla is an advanced keylogger with features like clipboard logging, screen keylogging, screen capturing, and extracting stored passwords from different web browsers. Recently, Zscaler ThreatLabz detected a threat campaign where threat actors leverage CVE-2017-11882 XLAM to spread Agent Tesla to users on vulnerable versions of Microsoft Office.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

15 / 100

Content

N/A

Attack-Pattern

Name
Process Injection
ID
T1055
Description
Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process. There are many different ways to inject code into a process, many of which abuse legitimate functionalities. These implementations exist for every major OS but are typically platform specific. More sophisticated samples may perform multiple process injections to segment modules and further evade detection, utilizing named pipes or other inter-process communication (IPC) mechanisms as a communication channel.
Name
Phishing
ID
T1566

Description

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name

Exfiltration Over Other Network Medium

ID

T1011

Description

Adversaries may attempt to exfiltrate data over a different network medium than the command and control channel. If the command and control network is a wired Internet connection, the exfiltration may occur, for example, over a WiFi connection, modem, cellular data connection, Bluetooth, or another radio frequency (RF) channel. Adversaries may choose to do this if they have sufficient access or proximity, and the connection might

not be secured or defended as well as the primary Internet-connected channel because it is not routed through the same enterprise network.

Name

Obfuscated Files or Information

ID

T1027

Description

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses. Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140) for [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016) Adversaries may also use compressed or archived scripts, such as JavaScript. Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. (Citation: Linux/Cdorked.A We Live Security Analysis) Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled. (Citation: Carbon Black Obfuscation Sept 2016) Adversaries may also abuse [Command Obfuscation](https://attack.mitre.org/techniques/T1027/010) to obscure commands executed from payloads or directly via [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Revoke-Obfuscation July 2017)(Citation: PaloAlto EncodedCommand March 2017)

Name

Ingress Tool Transfer

ID

T1105

Description

Adversaries may transfer tools or other files from an external system into a compromised environment. Tools or files may be copied from an external adversary-controlled system to the victim network through the command and control channel or through alternate protocols such as [ftp](https://attack.mitre.org/software/S0095). Once present, adversaries may also transfer/spread tools between victim devices within a compromised environment (i.e. [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570)). On Windows, adversaries may use various utilities to download tools, such as `copy`, `finger`, [certutil](https://attack.mitre.org/software/S0160), and [PowerShell](https://attack.mitre.org/techniques/T1059/001) commands such as `IEX(New-Object Net.WebClient).downloadString()` and `Invoke-WebRequest`. On Linux and macOS systems, a variety of utilities also exist, such as `curl`, `scp`, `sftp`, `tftp`, `rsync`, `finger`, and `wget`. (Citation: t1105_lolbas) Adversaries may also abuse installers and package managers, such as `yum` or `winget`, to download tools to victim hosts. Files can also be transferred using various [Web Service](https://attack.mitre.org/techniques/T1102)s as well as native or otherwise present tools on the victim system.(Citation: PTSecurity Cobalt Dec 2016) In some cases, adversaries may be able to leverage services that sync between a web-based and an on-premises client, such as Dropbox or OneDrive, to transfer files onto victim systems. For example, by compromising a cloud account and logging into the service's web portal, an adversary may be able to trigger an automatic syncing process that transfers the file onto the victim's machine.(Citation: Dropbox Malware Sync)

Name

Command and Scripting Interpreter

ID

T1059

Description

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer

systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](https://attack.mitre.org/techniques/T1059/004) while Windows installations include the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) and [PowerShell](https://attack.mitre.org/techniques/T1059/001). There are also cross-platform interpreters such as [Python](https://attack.mitre.org/techniques/T1059/006), as well as those commonly associated with client applications such as [JavaScript](https://attack.mitre.org/techniques/T1059/007) and [Visual Basic](https://attack.mitre.org/techniques/T1059/005). Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](https://attack.mitre.org/tactics/TA0001) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](https://attack.mitre.org/techniques/T1021) in order to achieve remote Execution. (Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

Name

Exploitation for Client Execution

ID

T1203

Description

Adversaries may exploit software vulnerabilities in client applications to execute code. Vulnerabilities can exist in software due to unsecure coding practices that can lead to unanticipated behavior. Adversaries can take advantage of certain vulnerabilities through targeted exploitation for the purpose of arbitrary code execution. Oftentimes the most valuable exploits to an offensive toolkit are those that can be used to obtain code execution on a remote system because they can be used to gain access to that system. Users will expect to see files related to the applications they commonly used to do work, so they are a useful target for exploit research and development because of their high utility. Several types exist: ### Browser-based Exploitation Web browsers are a common target through [Drive-by Compromise](https://attack.mitre.org/techniques/T1189) and [Spearphishing Link](https://attack.mitre.org/techniques/T1566/002). Endpoint systems may be compromised through normal web browsing or from certain users being targeted by links in spearphishing emails to adversary controlled sites used to exploit the web

browser. These often do not require an action by the user for the exploit to be executed. ### Office Applications Common office and productivity applications such as Microsoft Office are also targeted through [Phishing](https://attack.mitre.org/techniques/T1566). Malicious files will be transmitted directly as attachments or through links to download them. These require the user to open the document or file for the exploit to run. ### Common Third-party Applications Other applications that are commonly seen or are part of the software deployed in a target network may also be used for exploitation. Applications such as Adobe Reader and Flash, which are common in enterprise environments, have been routinely targeted by adversaries attempting to gain access to systems. Depending on the software and nature of the vulnerability, some may be exploited in the browser or require the user to open a file. For instance, some Flash exploits have been delivered as objects within Microsoft Office documents.

Indicator

Name

5944d934a0233b9c30cfa0b20afe86a09e6afa67030daad7d8c1f0534a9d629e

Description

Win.Packed.Msilperseus-9956591-0 SHA256 of 6bdb7a11d0eaa407e7a7f34d794fb567

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5944d934a0233b9c30cfa0b20afe86a09e6afa67030daad7d8c1f0534a9d629e']

Name

http://79.110.48.52/nix.txt

Description

Threat: malware_download - Reporter: James_inthe_box - Status: offline

Pattern Type

stix

Pattern

[url:value = 'http://79.110.48.52/nix.txt']

Name

http://193.42.33.51/knog.txt

Pattern Type

stix

Pattern

[url:value = 'http://193.42.33.51/knog.txt']

Name

74dd5df1dac36bb348452e5d084f1a10c692e1bad2b1491cc41c2980a002d8af

Description

ALF:HeraklezEval:Exploit:O97M/CVE-2017-11882.DR!rfn SHA256 of 38f6b4d5804de785b925eb46ddd86d6f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '74dd5df1dac36bb348452e5d084f1a10c692e1bad2b1491cc41c2980a002d8af']

Name

d6369d763d29a8b60c9cb16966ca213d6c1fbfc9cf97d96aa4f6c97fa324abe2

Description

Win.Packed.Msilperseus-9956591-0 SHA256 of e6c4636c331af09568a68dcf3614cfa4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd6369d763d29a8b60c9cb16966ca213d6c1fbfc9cf97d96aa4f6c97fa324abe2']

Name

d0a1a4d065d7614fac58c3e4ed5f52e8889372a2d6c3d5bfa5c291cc1f990100

Description

Win.Packed.Msilperseus-9956591-0 SHA256 of e6926fc50f40c5c5feb676b0adcb7655

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd0a1a4d065d7614fac58c3e4ed5f52e8889372a2d6c3d5bfa5c291cc1f990100']

Name

7988501f67d983c87769531838a8554a2fa186c3bb5ea76b9b697491c81ed7a0

Description

Win.Packed.Msilperseus-9956591-0 SHA256 of 935e75cbd0f207bfeb6d3b5d90e35685

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7988501f67d983c87769531838a8554a2fa186c3bb5ea76b9b697491c81ed7a0']

Name

4894c3f698e1101a02c7af04e0fd81e36a0d91c0ce7c7003234e7bc18906f024

Description

AgentTesla SHA256 of bbc7c66b301d3087cfdaa89528832895

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4894c3f698e1101a02c7af04e0fd81e36a0d91c0ce7c7003234e7bc18906f024']

Name

f8847e6cfa9d58ce821bca8d28dffabf0217bee958a71d1b1bcffbc44a48487d

Description

SHA256 of c1521547dea051bd7a007516511fb2ca

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f8847e6cfa9d58ce821bca8d28dffabf0217bee958a71d1b1bcffbc44a48487d']

Name

b7ff72b60c763c4f62ea0b572f261c5d87bd55f4b33903150ebd08b339fc72da

Description

Win.Packed.Msilperseus-9956591-0 SHA256 of 43ec3cc0836bd759260e8cf120b79a7b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b7ff72b60c763c4f62ea0b572f261c5d87bd55f4b33903150ebd08b339fc72da']

Name

1bead1d425196aa29d74a07fca9519db1e42242ad63e7a157979b83ee1722980

Description

Win.Packed.Msilperseus-9956591-0 SHA256 of b551da554933c2c064f96aaa6aa9ff55

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1bead1d425196aa29d74a07fca9519db1e42242ad63e7a157979b83ee1722980']

Name

193.42.33.51

Description

ISP: Xdeer Limited **OS:** Linux ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u3 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDYrb/AY1wwBEVUT/ubKuZVVCBgiT1l1zgVNL+k1AXhq/OoC4xPW+x6J0cVA1zIB22jcYaC8T1bVAHLXoqIqkUhpkzVWu4OMy9YJmZL7JGBfe9JoDOvtQ3+l6JY7mFbk6s3wqiipbI70Obe+MAy78hkLH4RSa3if7vp7nqos8acwz3z9iS27sZb2i/o4mGQP9hplWyQLZ1K5lCEOlyPBHf0IaYvVIC1TUCnYLZNW82dh4iqKgsu9RijfuYCH0eA1UFKivUZvKfsmL2OhrnKVN4xDm9ayLesSDzgNa/xfmTG9wqpiU/LOQ2yki0Lue8ghFmuP3fii8o7TWRulLdYxya3 Fingerprint: e6:34:fc:5e:49:1f:d0:d5:88:e1:8e:71:7b:10:6d:af Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 diffie-hellman-group14-sha1 Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ssh-rsa ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '193.42.33.51']

Name

5bd807ee6e5be63484adb9329a8143f44b7d09a15bb6b878912b3749bd371fd6

Description

Win.Packed.Msilperseus-9956591-0 SHA256 of f25da7cd5fb33e7a0967dbcdf008bd9a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5bd807ee6e5be63484adb9329a8143f44b7d09a15bb6b878912b3749bd371fd6']

Name

6d905511eb7f3672603bc86b2589df6c7b7a24a208e78cf6aa5a82501c3796cd

Description

Win.Packed.Msilperseus-9956591-0 SHA256 of 6e0dafacdeee6f2d9463d0052db5cce8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6d905511eb7f3672603bc86b2589df6c7b7a24a208e78cf6aa5a82501c3796cd']

Name

d8268bed755a9098351b3acfbfca2096882c89ae5517621d34580b4de8ee6120

Description

Win.Packed.Msilperseus-9956591-0 SHA256 of 1e22cd428f5baf23877a8189469ed92a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd8268bed755a9098351b3acfbfca2096882c89ae5517621d34580b4de8ee6120']

Name

f46d02a1a66fb46ef0d0fbeae13167d87329b22751868091fd7db732e509e914

Description

Win.Packed.Msilperseus-9956591-0 SHA256 of e9d4e5b8b80dcb4fcf5af8413066434e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f46d02a1a66fb46ef0d0fbeae13167d87329b22751868091fd7db732e509e914']

Name

51f3c279d3fa8690b49d1bd6b370ec18d055fcb10aa3cd83957afb1f7fd911f3

Description

Win.Packed.Msilperseus-9956591-0 SHA256 of f11d72bc4192b2ed698cc2b0200773bf

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '51f3c279d3fa8690b49d1bd6b370ec18d055fcb10aa3cd83957afb1f7fd911f3']

Name

113e16425e010952150f3c1f7ae615602cd4ca30826b0e7518aa058341058a94

Description

Win.Packed.Msilperseus-9956591-0 SHA256 of 547b88c4aa225377d7d65e912d81fe28

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '113e16425e010952150f3c1f7ae615602cd4ca30826b0e7518aa058341058a94']

Name

63b53c9f93e262d689fd45a2e2117e374e5ea602d27a9cb2e8d10b289a4d46d5

Description

Win.Packed.Msilperseus-9956591-0 SHA256 of 3c3580dfbc1f06636fe5696879cbdd85

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '63b53c9f93e262d689fd45a2e2117e374e5ea602d27a9cb2e8d10b289a4d46d5']

Name

b23d109a78e598eeec4375e08760c8e0ae961bdc117587e4e3f85c8c4058b842

Description

Win.Packed.Msilperseus-9956591-0 SHA256 of cb2b5646d68279aea516703df3c4c1e9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b23d109a78e598eeec4375e08760c8e0ae961bdc117587e4e3f85c8c4058b842']

Name

e03449995cd2b68758a3e44534fdb50f13070e743c9bd1e0d3b1f715c7e26e65

Description

Win.Packed.Msilperseus-9956591-0 SHA256 of 0708c52198a49bc7ab16bce19472598a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e03449995cd2b68758a3e44534fdb50f13070e743c9bd1e0d3b1f715c7e26e65']

Name

3c8af2392b872632e0090fa002ec74852697b8cfbfeccf6f238eb175d56aed14

Description

Win.Packed.Msilperseus-9956591-0 SHA256 of 2639c8b09f744e95ba612c89ef26e02c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3c8af2392b872632e0090fa002ec74852697b8cfbfeccf6f238eb175d56aed14']

Name

a2061a6a280485cb336a308d9906096b1417268aecce7d580e68049bcb59f18c

Description

Win.Packed.Msilperseus-9956591-0 SHA256 of 5373b6dce20bbb0218034aa9bf0c20df

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a2061a6a280485cb336a308d9906096b1417268aecce7d580e68049bcb59f18c']

Name

ea692e0b71d678d18c157a5980625e75f9060c97f9209a562691ebf92f726e84

Description

DotNET_Reactor SHA256 of 5630282a95afd2a5ceeecc5acf7ff053

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ea692e0b71d678d18c157a5980625e75f9060c97f9209a562691ebf92f726e84']

Name

29dae9996c81b0782866306c0faf4811226881061265b1c209a8ba02817c8892

Description

Win.Packed.Msilperseus-9956591-0 SHA256 of 92d1ece422670dbf9a3e1aef45612b5c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '29dae9996c81b0782866306c0faf4811226881061265b1c209a8ba02817c8892']

Name

3192d349187fb4f6cea676911f919ecc13e5b33db328d14ae7bddc0c9570ad8e

Description

Win.Packed.Msilperseus-9956591-0 SHA256 of e57882623add29cbfa8c93d011b52c44

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3192d349187fb4f6cea676911f919ecc13e5b33db328d14ae7bddc0c9570ad8e']

Name

1acf61ab5912011c1e3bed1fc4bca2b17f1d9098245976415e2d8d40ee3e472e

Description

Win.Packed.Msilperseus-9956591-0 SHA256 of b6f892c73fa0f491072592d7baf0c916

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1acf61ab5912011c1e3bed1fc4bca2b17f1d9098245976415e2d8d40ee3e472e']

Name

a0dd51a53c5fa0242e06b68f39fa55d9b21b703c5014098ce5a1889e41c3d357

Description

Win.Packed.Msilperseus-9956591-0 SHA256 of efc3a41ecae822eba861cb88c179c80e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a0dd51a53c5fa0242e06b68f39fa55d9b21b703c5014098ce5a1889e41c3d357']

Name

39eeda113ece91266296dfc3b9d00a6740bee7b0e695c277e49fa1966b8dfda9

Description

Win.Packed.Msilperseus-9956591-0 SHA256 of a8e8d4667f96ea847d18eb7830fb1dc6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '39eeda113ece91266296dfc3b9d00a6740bee7b0e695c277e49fa1966b8dfda9']

Name

10e510fbc242542d046a32efbdde7501b3c4f12211b77649b701769175687f63

Description

Win.Packed.Msilperseus-9956591-0 SHA256 of 0ada110f82ce64fcfab0eb0e5d8d948e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '10e510fbc242542d046a32efbdde7501b3c4f12211b77649b701769175687f63']

Name

0ee09ee5a382f01dfb53c94676b9c5676b1b82be91f46b6a2ffc1996c321a994

Description

Win.Packed.Msilperseus-9956591-0 SHA256 of f1a1542bbccea9a4e6746040d85eae1b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0ee09ee5a382f01dfb53c94676b9c5676b1b82be91f46b6a2ffc1996c321a994']

Name

39e68b3555c03c108a8dc3f9373a2031ba20ce5e0adc492ab3b2d2e5d3150d86

Description

Win.Packed.Msilperseus-9956591-0 SHA256 of f0af137175487b4d1249921ce506efe9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '39e68b3555c03c108a8dc3f9373a2031ba20ce5e0adc492ab3b2d2e5d3150d86']

Name

437c9a84221317873865c1a2e61fcb6011dafff7afb646c482dfefb400da0186

Description

Win.Packed.Msilperseus-9956591-0 SHA256 of c01e90db99bcc939f829a181aef2c348

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '437c9a84221317873865c1a2e61fcb6011dafff7afb646c482dfefb400da0186']

Name

411ff6f1702fc4c00c095688a3e3e7bc2a495bea2b50debc326d76ed9dcfec20

Description

SHA256 of f302addf3b4068888788d8edce8f52a0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '411ff6f1702fc4c00c095688a3e3e7bc2a495bea2b50debc326d76ed9dcfec20']

Name

4a793a9dfa5fac79c6e6b8f1d36e8719cc8f2849849259f364ee8e4af08d9613

Description

Win.Packed.Msilperseus-9956591-0 SHA256 of 00b28f548f14de4f53abd6651bf78b98

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4a793a9dfa5fac79c6e6b8f1d36e8719cc8f2849849259f364ee8e4af08d9613']

Name

http://79.110.48.52/nicko.vbs

Description

Threat: malware_download - Reporter: abuse_ch - Status: offline

Pattern Type

stix

Pattern

[url:value = 'http://79.110.48.52/nicko.vbs']

Name

b2046015aca079fe04a94f5aa2573c1ba678469c920a52cfe784547771a0b0ce

Description

Win.Packed.Msilperseus-9956591-0 SHA256 of 7b6ec969d4110722b427de45ca1c0d42

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b2046015aca079fe04a94f5aa2573c1ba678469c920a52cfe784547771a0b0ce']

Name

02a837d139709853b2ab7c3f1c55802c880fd133b731cfb2a15830230c5babd2

Description

SHA256 of dddabc8019a7184055301927239a9438

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '02a837d139709853b2ab7c3f1c55802c880fd133b731cfb2a15830230c5babd2']

Name

6c006e3c02417e43c43c66bf5e986a64b2bdced8cf62912e5d6e1de16ed90452

Description

Win.Packed.Msilperseus-9956591-0 SHA256 of 7ea06a0e6c1e5707a23364ae6984b4f3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6c006e3c02417e43c43c66bf5e986a64b2bdced8cf62912e5d6e1de16ed90452']

Name

79.110.48.52

Description

ISP: NPO G-net **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` Exceeded MaxStartups\r\n ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '79.110.48.52']

Name

6900e4e68cea5bf65ebd1d817d9408351539a8b152c80f88d70d6ff04479782e

Description

Win.Packed.Msilperseus-9956591-0 SHA256 of b7dba4e30a73f58740d316c46645b759

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6900e4e68cea5bf65ebd1d817d9408351539a8b152c80f88d70d6ff04479782e']

Name

3c1779c16357cb3d3ffdc0d66009f8fc0df7c618d189623f315e53887c11a453

Description

Win.Packed.Msilperseus-9956591-0 SHA256 of 3247ad04996dd2966800153e7ea14571

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3c1779c16357cb3d3ffdc0d66009f8fc0df7c618d189623f315e53887c11a453']

Malware

Name
Agent Tesla

Description
[Agent Tesla](https://attack.mitre.org/software/S0331) is a spyware Trojan written for the .NET framework that has been observed since at least 2014.(Citation: Fortinet Agent Tesla April 2018)(Citation: Bitdefender Agent Tesla April 2020)(Citation: Malwarebytes Agent Tesla April 2020)

StixFile

Value
0ee09ee5a382f01dfb53c94676b9c5676b1b82be91f46b6a2ffc1996c321a994
d0a1a4d065d7614fac58c3e4ed5f52e8889372a2d6c3d5bfa5c291cc1f990100
1bead1d425196aa29d74a07fca9519db1e42242ad63e7a157979b83ee1722980
d6369d763d29a8b60c9cb16966ca213d6c1fbfc9cf97d96aa4f6c97fa324abe2
3c1779c16357cb3d3ffdc0d66009f8fc0df7c618d189623f315e53887c11a453
6d905511eb7f3672603bc86b2589df6c7b7a24a208e78cf6aa5a82501c3796cd
5bd807ee6e5be63484adb9329a8143f44b7d09a15bb6b878912b3749bd371fd6
e03449995cd2b68758a3e44534fdb50f13070e743c9bd1e0d3b1f715c7e26e65
3c8af2392b872632e0090fa002ec74852697b8cfbfeccf6f238eb175d56aed14
f46d02a1a66fb46ef0d0fbeae13167d87329b22751868091fd7db732e509e914
437c9a84221317873865c1a2e61fcb6011dafff7afb646c482dfefb400da0186
6900e4e68cea5bf65ebd1d817d9408351539a8b152c80f88d70d6ff04479782e
d8268bed755a9098351b3acfbfca2096882c89ae5517621d34580b4de8ee6120

7988501f67d983c87769531838a8554a2fa186c3bb5ea76b9b697491c81ed7a0

4a793a9dfa5fac79c6e6b8f1d36e8719cc8f2849849259f364ee8e4af08d9613

39eeda113ece91266296dfc3b9d00a6740bee7b0e695c277e49fa1966b8dfda9

29dae9996c81b0782866306c0faf4811226881061265b1c209a8ba02817c8892

b7ff72b60c763c4f62ea0b572f261c5d87bd55f4b33903150ebd08b339fc72da

51f3c279d3fa8690b49d1bd6b370ec18d055fcb10aa3cd83957afb1f7fd911f3

a0dd51a53c5fa0242e06b68f39fa55d9b21b703c5014098ce5a1889e41c3d357

39e68b3555c03c108a8dc3f9373a2031ba20ce5e0adc492ab3b2d2e5d3150d86

f8847e6cfa9d58ce821bca8d28dffabf0217bee958a71d1b1bcffbc44a48487d

3192d349187fb4f6cea676911f919ecc13e5b33db328d14ae7bddc0c9570ad8e

74dd5df1dac36bb348452e5d084f1a10c692e1bad2b1491cc41c2980a002d8af

b2046015aca079fe04a94f5aa2573c1ba678469c920a52cfe784547771a0b0ce

113e16425e010952150f3c1f7ae615602cd4ca30826b0e7518aa058341058a94

6c006e3c02417e43c43c66bf5e986a64b2bdced8cf62912e5d6e1de16ed90452

1acf61ab5912011c1e3bed1fc4bca2b17f1d9098245976415e2d8d40ee3e472e

10e510fbc242542d046a32efbdde7501b3c4f12211b77649b701769175687f63

63b53c9f93e262d689fd45a2e2117e374e5ea602d27a9cb2e8d10b289a4d46d5

5944d934a0233b9c30cfa0b20afe86a09e6afa67030daad7d8c1f0534a9d629e

02a837d139709853b2ab7c3f1c55802c880fd133b731cfb2a15830230c5babd2
ea692e0b71d678d18c157a5980625e75f9060c97f9209a562691ebf92f726e84
b23d109a78e598eeec4375e08760c8e0ae961bdc117587e4e3f85c8c4058b842
a2061a6a280485cb336a308d9906096b1417268aecce7d580e68049bcb59f18c
4894c3f698e1101a02c7af04e0fd81e36a0d91c0ce7c7003234e7bc18906f024
411ff6f1702fc4c00c095688a3e3e7bc2a495bea2b50debc326d76ed9dcfec20

IPv4-Addr

Value
79.110.48.52
193.42.33.51

Url

Value
http://193.42.33.51/knog.txt
http://79.110.48.52/nix.txt
http://79.110.48.52/nicko.vbs

External References

- https://otx.alienvault.com/pulse/659590aec2e01294d509fc1e
- https://www.zscaler.com/blogs/security-research/threat-actors-exploit-cve-2017-11882-deliver-agent-tesla