Aug 09 2024

NETMANAGEIT

Intelligence Report

New Widespread Extension Trojan Malware Campaign

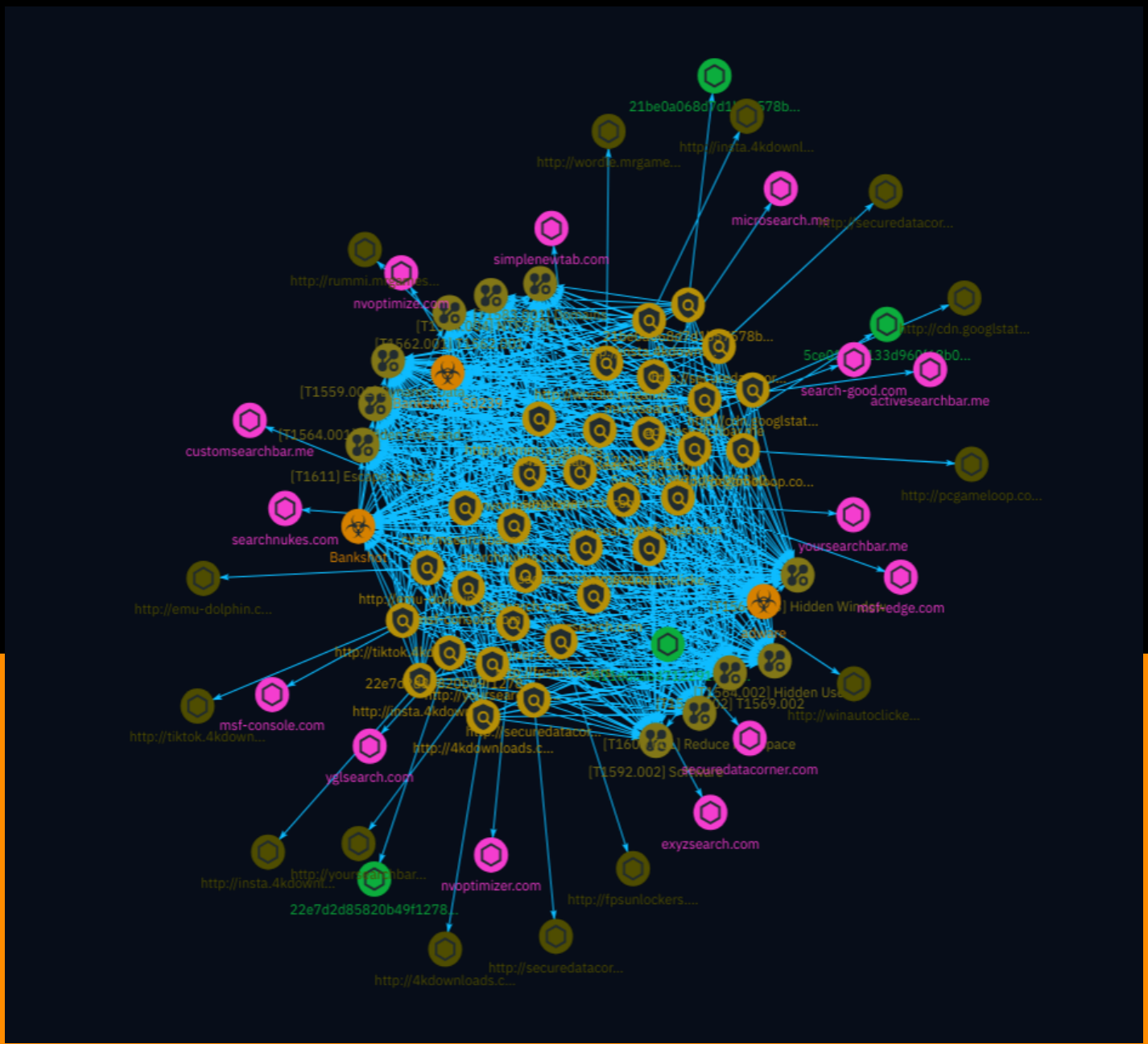

Table of contents

Overview

Entities

Observables

External References

Overview

Description

This report discusses a widespread polymorphic malware campaign that forcefully installs malicious browser extensions on endpoints. The malware, originating from imitations of download websites, delivers various malicious payloads, including adware extensions, data stealing scripts, and commands to execute. It hijacks searches, redirects traffic, and has affected over 300,000 users across Google Chrome and Microsoft Edge. The malicious actors employ obfuscation techniques, leverage PowerShell scripts, and communicate with command-and-control servers to receive instructions and download additional malicious components.

Confidence

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

100 / 100

Content

N/A

Attack-Pattern

Name

Escape to Host

ID

T1611

Description

Adversaries may break out of a container to gain access to the underlying host. This can allow an adversary access to other containerized resources from the host level or to the host itself. In principle, containerized resources should provide a clear separation of application functionality and be isolated from the host environment.(Citation: Docker Overview) There are multiple ways an adversary may escape to a host environment. Examples include creating a container configured to mount the host's filesystem using the bind parameter, which allows the adversary to drop payloads and execute control utilities such as cron on the host; utilizing a privileged container to run commands or load a malicious kernel module on the underlying host; or abusing system calls such as `unshare` and `keyctl` to escalate privileges and steal secrets.(Citation: Docker Bind Mounts)(Citation: Trend Micro Privileged Container)(Citation: Intezer Doki July 20)(Citation: Container Escape) (Citation: Crowdstrike Kubernetes Container Escape)(Citation: Keyctl-unmask) Additionally, an adversary may be able to exploit a compromised container with a mounted container management socket, such as `docker.sock`, to break out of the container via a [Container Administration Command](https://attack.mitre.org/techniques/T1609).(Citation: Container Escape) Adversaries may also escape via [Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068), such as exploiting vulnerabilities in global symbolic links in order to access the root directory of a host machine.(Citation: Windows Server Containers Are Open) Gaining access to the host may provide the adversary with the opportunity to achieve follow-on objectives, such as establishing persistence, moving

laterally within the environment, accessing other containers running on the host, or setting up a command and control channel on the host.

Name

Hidden Files and Directories

ID

T1564.001

Description

Adversaries may set files and directories to be hidden to evade detection mechanisms. To prevent normal users from accidentally changing special files on a system, most operating systems have the concept of a ‘hidden’ file. These files don’t show up when a user browses the file system with a GUI or when using normal commands on the command line. Users must explicitly ask to show the hidden files either via a series of Graphical User Interface (GUI) prompts or with command line switches (`dir /a` for Windows and `ls –a` for Linux and macOS). On Linux and Mac, users can mark specific files as hidden simply by putting a “.” as the first character in the file or folder name (Citation: Sofacy Komplex Trojan) (Citation: Antiquated Mac Malware). Files and folders that start with a period, ‘.’, are by default hidden from being viewed in the Finder application and standard command-line utilities like “ls”. Users must specifically change settings to have these files viewable. Files on macOS can also be marked with the UF_HIDDEN flag which prevents them from being seen in Finder.app, but still allows them to be seen in Terminal.app (Citation: WireLurker). On Windows, users can mark specific files as hidden by using the attrib.exe binary. Many applications create these hidden files and folders to store information so that it doesn’t clutter up the user’s workspace. For example, SSH utilities create a .ssh folder that’s hidden and contains the user’s known hosts and keys. Adversaries can use this to their advantage to hide files and folders anywhere on the system and evading a typical user or system analysis that does not incorporate investigation of hidden files.

Name

Hidden Users

ID

T1564.002

Description

Adversaries may use hidden users to hide the presence of user accounts they create or modify. Administrators may want to hide users when there are many user accounts on a given system or if they want to hide their administrative or other management accounts from other users. In macOS, adversaries can create or modify a user to be hidden through manipulating plist files, folder attributes, and user attributes. To prevent a user from being shown on the login screen and in System Preferences, adversaries can set the userID to be under 500 and set the key value `Hide500Users` to `TRUE` in the `/Library/Preferences/com.apple.loginwindow` plist file.(Citation: Cybereason OSX Pirrit) Every user has a userID associated with it. When the `Hide500Users` key value is set to `TRUE`, users with a userID under 500 do not appear on the login screen and in System Preferences. Using the command line, adversaries can use the `dscl` utility to create hidden user accounts by setting the `IsHidden` attribute to `1`. Adversaries can also hide a user's home folder by changing the `chflags` to hidden.(Citation: Apple Support Hide a User Account) Adversaries may similarly hide user accounts in Windows. Adversaries can set the `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList` Registry key value to `0` for a specific user to prevent that user from being listed on the logon screen.(Citation: FireEye SMOKEDHAM June 2021)(Citation: US-CERT TA18-074A) On Linux systems, adversaries may hide user accounts from the login screen, also referred to as the greeter. The method an adversary may use depends on which Display Manager the distribution is currently using. For example, on an Ubuntu system using the GNOME Display Manger (GDM), accounts may be hidden from the greeter using the `gsettings` command (ex: `sudo -u gdm gsettings set org.gnome.login-screen disable-user-list true`).(Citation: Hide GDM User Accounts) Display Managers are not anchored to specific distributions and may be changed by a user or adversary.

Name

Reduce Key Space

ID

T1600.001

Description

Adversaries may reduce the level of effort required to decrypt data transmitted over the network by reducing the cipher strength of encrypted communications.(Citation: Cisco Synful Knock Evolution) Adversaries can weaken the encryption software on a compromised network device by reducing the key size used by the software to convert plaintext to ciphertext (e.g., from hundreds or thousands of bytes to just a couple of bytes). As a result, adversaries dramatically reduce the amount of effort needed to decrypt the protected information without the key. Adversaries may modify the key size used and other encryption parameters using specialized commands in a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) introduced to the system through [Modify System Image](https://attack.mitre.org/techniques/T1601) to change the configuration of the device. (Citation: Cisco Blog Legacy Device Attacks)

Name

NTFS File Attributes

ID

T1564.004

Description

Adversaries may use NTFS file attributes to hide their malicious data in order to evade detection. Every New Technology File System (NTFS) formatted partition contains a Master File Table (MFT) that maintains a record for every file/directory on the partition. (Citation: SpectorOps Host-Based Jul 2017) Within MFT entries are file attributes, (Citation: Microsoft NTFS File Attributes Aug 2010) such as Extended Attributes (EA) and Data [known as Alternate Data Streams (ADSs) when more than one Data attribute is present], that can be used to store arbitrary data (and even complete files). (Citation: SpectorOps Host-Based Jul 2017) (Citation: Microsoft File Streams) (Citation: MalwareBytes ADS July 2015) (Citation: Microsoft ADS Mar 2014) Adversaries may store malicious data or binaries in file attribute metadata instead of directly in files. This may be done to evade some defenses, such as static indicator scanning tools and anti-virus. (Citation: Journey into IR ZeroAccess NTFS EA) (Citation: MalwareBytes ADS July 2015)

Name

Hidden Window

ID

T1564.003

Description

Adversaries may use hidden windows to conceal malicious activity from the plain sight of users. In some cases, windows that would typically be displayed when an application carries out an operation can be hidden. This may be utilized by system administrators to avoid disrupting user work environments when carrying out administrative tasks. Adversaries may abuse these functionalities to hide otherwise visible windows from users so as not to alert the user to adversary activity on the system.(Citation: Antiquated Mac Malware) On macOS, the configurations for how applications run are listed in property list (plist) files. One of the tags in these files can be `apple.awt.UIElement`, which allows for Java applications to prevent the application's icon from appearing in the Dock. A common use for this is when applications run in the system tray, but don't also want to show up in the Dock. Similarly, on Windows there are a variety of features in scripting languages, such as [PowerShell](https://attack.mitre.org/techniques/T1059/001), Jscript, and [Visual Basic](https://attack.mitre.org/techniques/T1059/005) to make windows hidden. One example of this is `powershell.exe -WindowStyle Hidden`.(Citation: PowerShell About 2019) In addition, Windows supports the `CreateDesktop()` API that can create a hidden desktop window with its own corresponding `explorer.exe` process.(Citation: Hidden VNC)(Citation: Anatomy of an hVNC Attack) All applications running on the hidden desktop window, such as a hidden VNC (hVNC) session,(Citation: Hidden VNC) will be invisible to other desktops windows.

Name

T1562.001

ID

T1562.001

Description

Adversaries may modify and/or disable security tools to avoid possible detection of their malware/tools and activities. This may take many forms, such as killing security software processes or services, modifying / deleting Registry keys or configuration files so that tools do not operate properly, or other methods to interfere with security tools scanning

or reporting information. Adversaries may also disable updates to prevent the latest security patches from reaching tools on victim systems.(Citation: SCADAfence_ransomware) Adversaries may also tamper with artifacts deployed and utilized by security tools. Security tools may make dynamic changes to system components in order to maintain visibility into specific events. For example, security products may load their own modules and/or modify those loaded by processes to facilitate data collection. Similar to [Indicator Blocking](https://attack.mitre.org/techniques/T1562/006), adversaries may unhook or otherwise modify these features added by tools (especially those that exist in userland or are otherwise potentially accessible to adversaries) to avoid detection.(Citation: OutFlank System Calls)(Citation: MDSec System Calls) Adversaries may also focus on specific applications such as Sysmon. For example, the “Start” and “Enable” values in `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WMI\Autologger\EventLog-Microsoft-Windows-Sysmon-Operational` may be modified to tamper with and potentially disable Sysmon logging.(Citation: disable_win_evt_logging) On network devices, adversaries may attempt to skip digital signature verification checks by altering startup configuration files and effectively disabling firmware verification that typically occurs at boot.(Citation: Fortinet Zero-Day and Custom Malware Used by Suspected Chinese Actor in Espionage Operation)(Citation: Analysis of FG-IR-22-369) In cloud environments, tools disabled by adversaries may include cloud monitoring agents that report back to services such as AWS CloudWatch or Google Cloud Monitor. Furthermore, although defensive tools may have anti-tampering mechanisms, adversaries may abuse tools such as legitimate rootkit removal kits to impair and/or disable these tools.(Citation: chasing_avaddon_ransomware)(Citation: dharma_ransomware)(Citation: demystifying_ryuk)(Citation: doppelpaymer_crowdstrike) For example, adversaries have used tools such as GMER to find and shut down hidden processes and antivirus software on infected systems.(Citation: demystifying_ryuk) Additionally, adversaries may exploit legitimate drivers from anti-virus software to gain access to kernel space (i.e. [Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068)), which may lead to bypassing anti-tampering features.(Citation: avoslocker_ransomware)

Name

Domains

ID

T1583.001

Description

Adversaries may acquire domains that can be used during targeting. Domain names are the human readable names used to represent one or more IP addresses. They can be purchased or, in some cases, acquired for free. Adversaries may use acquired domains for a variety of purposes, including for [Phishing](https://attack.mitre.org/techniques/T1566), [Drive-by Compromise](https://attack.mitre.org/techniques/T1189), and Command and Control.(Citation: CISA MSS Sep 2020) Adversaries may choose domains that are similar to legitimate domains, including through use of homoglyphs or use of a different top-level domain (TLD).(Citation: FireEye APT28)(Citation: PaypalScam) Typosquatting may be used to aid in delivery of payloads via [Drive-by Compromise](https://attack.mitre.org/techniques/T1189). Adversaries may also use internationalized domain names (IDNs) and different character sets (e.g. Cyrillic, Greek, etc.) to execute "IDN homograph attacks," creating visually similar lookalike domains used to deliver malware to victim machines.(Citation: CISA IDN ST05-016)(Citation: tt_httrack_fake_domains)(Citation: tt_obliqueRAT)(Citation: httrack_unhcr)(Citation: lazgroup_idn_phishing) Different URIs/URLs may also be dynamically generated to uniquely serve malicious content to victims (including one-time, single use domain names).(Citation: iOS URL Scheme)(Citation: URI)(Citation: URI Use)(Citation: URI Unique) Adversaries may also acquire and repurpose expired domains, which may be potentially already allowlisted/trusted by defenders based on an existing reputation/history.(Citation: Categorisation_not_boundary)(Citation: Domain_Steal_CC)(Citation: Redirectors_Domain_Fronting)(Citation: bypass_webproxy_filtering) Domain registrars each maintain a publicly viewable database that displays contact information for every registered domain. Private WHOIS services display alternative information, such as their own company data, rather than the owner of the domain. Adversaries may use such private WHOIS services to obscure information about who owns a purchased domain. Adversaries may further interrupt efforts to track their infrastructure by using varied registration information and purchasing domains with different domain registrars.(Citation: Mandiant APT1)

Name

T1569.002

ID

T1569.002

Description

Adversaries may abuse the Windows service control manager to execute malicious commands or payloads. The Windows service control manager (`services.exe`) is an

interface to manage and manipulate services.(Citation: Microsoft Service Control Manager) The service control manager is accessible to users via GUI components as well as system utilities such as `sc.exe` and [Net](https://attack.mitre.org/software/S0039). [PsExec](https://attack.mitre.org/software/S0029) can also be used to execute commands or payloads via a temporary Windows service created through the service control manager API.(Citation: Russinovich Sysinternals) Tools such as [PsExec](https://attack.mitre.org/software/S0029) and `sc.exe` can accept remote servers as arguments and may be used to conduct remote execution. Adversaries may leverage these mechanisms to execute malicious content. This can be done by either executing a new or modified service. This technique is the execution used in conjunction with [Windows Service](https://attack.mitre.org/techniques/T1543/003) during service persistence or privilege escalation.

Name

Software

ID

T1592.002

Description

Adversaries may gather information about the victim's host software that can be used during targeting. Information about installed software may include a variety of details such as types and versions on specific hosts, as well as the presence of additional components that might be indicative of added defensive protections (ex: antivirus, SIEMs, etc.). Adversaries may gather this information in various ways, such as direct collection actions via [Active Scanning](https://attack.mitre.org/techniques/T1595) (ex: listening ports, server banners, user agent strings) or [Phishing for Information](https://attack.mitre.org/techniques/T1598). Adversaries may also compromise sites then include malicious content designed to collect host information from visitors.(Citation: ATT ScanBox) Information about the installed software may also be exposed to adversaries via online or other accessible data sets (ex: job postings, network maps, assessment reports, resumes, or purchase invoices). Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593) or [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596)), establishing operational resources (ex: [Develop Capabilities](https://attack.mitre.org/techniques/T1587) or [Obtain Capabilities](https://attack.mitre.org/techniques/T1588)), and/or for initial access (ex: [Supply Chain

Compromise](https://attack.mitre.org/techniques/T1195) or [External Remote Services](https://attack.mitre.org/techniques/T1133)).

Name

Dynamic Data Exchange

ID

T1559.002

Description

Adversaries may use Windows Dynamic Data Exchange (DDE) to execute arbitrary commands. DDE is a client-server protocol for one-time and/or continuous inter-process communication (IPC) between applications. Once a link is established, applications can autonomously exchange transactions consisting of strings, warm data links (notifications when a data item changes), hot data links (duplications of changes to a data item), and requests for command execution. Object Linking and Embedding (OLE), or the ability to link data between documents, was originally implemented through DDE. Despite being superseded by [Component Object Model](https://attack.mitre.org/techniques/T1559/001), DDE may be enabled in Windows 10 and most of Microsoft Office 2016 via Registry keys.(Citation: BleepingComputer DDE Disabled in Word Dec 2017)(Citation: Microsoft ADV170021 Dec 2017)(Citation: Microsoft DDE Advisory Nov 2017) Microsoft Office documents can be poisoned with DDE commands, directly or through embedded files, and used to deliver execution via [Phishing](https://attack.mitre.org/techniques/T1566) campaigns or hosted Web content, avoiding the use of Visual Basic for Applications (VBA) macros.(Citation: SensePost PS DDE May 2016)(Citation: Kettle CSV DDE Aug 2014)(Citation: Enigma Reviving DDE Jan 2018)(Citation: SensePost MacroLess DDE Oct 2017) Similarly, adversaries may infect payloads to execute applications and/or commands on a victim device by way of embedding DDE formulas within a CSV file intended to be opened through a Windows spreadsheet program.(Citation: OWASP CSV Injection)(Citation: CSV Excel Macro Injection) DDE could also be leveraged by an adversary operating on a compromised machine who does not have direct access to a [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). DDE execution can be invoked remotely via [Remote Services](https://attack.mitre.org/techniques/T1021) such as [Distributed Component Object Model](https://attack.mitre.org/techniques/T1021/003) (DCOM).(Citation: Fireeye Hunting COM June 2019)

Indicator

Name
msf-console.com
Pattern Type
stix
Pattern
[domain-name:value = 'msf-console.com']
Name
http://tiktok.4kdownloads.com/app/TikTokDownloader_3.1_ex64LTS.exe
Pattern Type
stix
Pattern
[url:value = 'http://tiktok.4kdownloads.com/app/TikTokDownloader_3.1_ex64LTS.exe']
Name
http://securedatacorner.com/exe/download/ChromeSetup.exe

Pattern Type

stix

Pattern

[url:value = 'http://securedatacorner.com/exe/download/ChromeSetup.exe']

Name

d421d0cab4712291f54c15dd7d1a0dc02e498998f14b157bd11e1e6f43a54efe

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd421d0cab4712291f54c15dd7d1a0dc02e498998f14b157bd11e1e6f43a54efe']

Name

http://insta.4kdownloads.com/app/Insta4kDownloader_x64LTS.exe

Pattern Type

stix

Pattern

[url:value = 'http://insta.4kdownloads.com/app/Insta4kDownloader_x64LTS.exe']

Name

http://cdn.googlstaticontent.com/DesktopApp/YouTubeAppSetup.exe

Pattern Type

stix

Pattern

[url:value = 'http://cdn.googlstaticontent.com/DesktopApp/YouTubeAppSetup.exe']

Name

nvoptimizer.com

Pattern Type

stix

Pattern

[domain-name:value = 'nvoptimizer.com']

Name

yoursearchbar.me

Pattern Type

stix

Pattern

[domain-name:value = 'yoursearchbar.me']

Name

http://yoursearchbar.me/search?q=

Pattern Type

stix

Pattern

[url:value = 'http://yoursearchbar.me/search?q=']

Name

22e7d2d85820b49f1278ce152c5ed39fd88087c7a998dcf348b6164d5b33bb8d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '22e7d2d85820b49f1278ce152c5ed39fd88087c7a998dcf348b6164d5b33bb8d']

Name

5ce016d3133d960f68b0415d5bb825b143713ffaea751b098ffcf80353bc171b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5ce016d3133d960f68b0415d5bb825b143713ffaea751b098ffcf80353bc171b']

Name
microsearch.me
Pattern Type
stix
Pattern
[domain-name:value = 'microsearch.me']
Name
securedatacorner.com
Pattern Type
stix
Pattern
[domain-name:value = 'securedatacorner.com']
Name
http://insta.4kdownloads.com/app/Insta4kDownloader_ex64LTS.exe
Pattern Type
stix
Pattern
[url:value = 'http://insta.4kdownloads.com/app/Insta4kDownloader_ex64LTS.exe']

Name
customsearchbar.me
Pattern Type
stix
Pattern
[domain-name:value = 'customsearchbar.me']
Name
http://pcgameloop.com/app/GLP_installer_900221846.exe
Pattern Type
stix
Pattern
[url:value = 'http://pcgameloop.com/app/GLP_installer_900221846.exe']
Name
http://winautoclicker.com/app/AutoClicker_x64LTS.exe
Pattern Type
stix
Pattern
[url:value = 'http://winautoclicker.com/app/AutoClicker_x64LTS.exe']

Name
http://fpsunlockers.com/app/FPSUnlocker_4.1_x64LTS.exe
Pattern Type
stix
Pattern
[url:value = 'http://fpsunlockers.com/app/FPSUnlocker_4.1_x64LTS.exe']
Name
exyzsearch.com
Pattern Type
stix
Pattern
[domain-name:value = 'exyzsearch.com']
Name
activesearchbar.me
Pattern Type
stix
Pattern
[domain-name:value = 'activesearchbar.me']

Name

http://wordle.mrgameshub.com/app/Wordle_x64LTS.exe

Pattern Type

stix

Pattern

[url:value = 'http://wordle.mrgameshub.com/app/Wordle_x64LTS.exe']

Name

yglsearch.com

Pattern Type

stix

Pattern

[domain-name:value = 'yglsearch.com']

Name

http://4kdownloads.com/app/4kvideodownloader_4.1_x64LTS.exe

Pattern Type

stix

Pattern

[url:value = 'http://4kdownloads.com/app/4kvideodownloader_4.1_x64LTS.exe']

Name
http://securedatacorner.com/exe/download/SteamSetup.exe
Pattern Type
stix
Pattern
[url:value = 'http://securedatacorner.com/exe/download/SteamSetup.exe']
Name
search-good.com
Pattern Type
stix
Pattern
[domain-name:value = 'search-good.com']
Name
searchnukes.com
Pattern Type
stix
Pattern
[domain-name:value = 'searchnukes.com']

Name

21be0a068d7d1b57578bfb2ed850b3f3b1cfe4a4c47981ead95abdb8c20278fe

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '21be0a068d7d1b57578bfb2ed850b3f3b1cfe4a4c47981ead95abdb8c20278fe']

Name

simplenewtab.com

Pattern Type

stix

Pattern

[domain-name:value = 'simplenewtab.com']

Name

http://emu-dolphin.com/app/dolphin-x64-5.1.exe

Pattern Type

stix

Pattern

[url:value = 'http://emu-dolphin.com/app/dolphin-x64-5.1.exe']

Name

http://rummi.mrgameshub.com/app/RummikubSetup_ex64LTS.exe

Pattern Type

stix

Pattern

[url:value = 'http://rummi.mrgameshub.com/app/RummikubSetup_ex64LTS.exe']

Name

msf-edge.com

Pattern Type

stix

Pattern

[domain-name:value = 'msf-edge.com']

Name

nvoptimize.com

Pattern Type

stix

Pattern

```
[domain-name:value = 'nvoptimize.com']
```

Malware

Name
Bankshot
Description
[Bankshot](https://attack.mitre.org/software/S0239) is a remote access tool (RAT) that was first reported by the Department of Homeland Security in December of 2017. In 2018, [Lazarus Group](https://attack.mitre.org/groups/G0032) used the [Bankshot](https://attack.mitre.org/software/S0239) implant in attacks against the Turkish financial sector. (Citation: McAfee Bankshot)
Name
Bankshot - S0239
Name
adware

indicates

Name
Name
Name
Name
Name
Name
Name
Name
Name
Name

Name
Name
Name
Name
Name
Name
Name
Name
Name
Name
Name
Name

Name
Name
Name
Name
Name
Name
Name
Name
Name
Name

uses

Name
Name
Name
Name
Name

based-on

Name

Name

Domain-Name

Value
yoursearchbar.me
nvoptimizer.com
exyzsearch.com
microsearch.me
securedatacorner.com
search-good.com
yglsearch.com
customsearchbar.me
activesearchbar.me
nvoptimize.com
msf-console.com
searchnukes.com
simplenewtab.com

msf-edge.com

StixFile

Value
d421d0cab4712291f54c15dd7d1a0dc02e498998f14b157bd11e1e6f43a54efe
5ce016d3133d960f68b0415d5bb825b143713ffaea751b098ffcf80353bc171b
22e7d2d85820b49f1278ce152c5ed39fd88087c7a998dcf348b6164d5b33bb8d
21be0a068d7d1b57578bfb2ed850b3f3b1cfe4a4c47981ead95abdb8c20278fe

External References

- https://reasonlabs.com/research/new-widespread-extension-trojan-malware-campaign
- https://otx.alienvault.com/pulse/66b3316177bd9ddee5c69e13