Aug 03 2023

NETMANAGEIT

Intelligence Report

New Rilide Stealer Version Targets Banking Data and Works Around Google Chrome Manifest V3

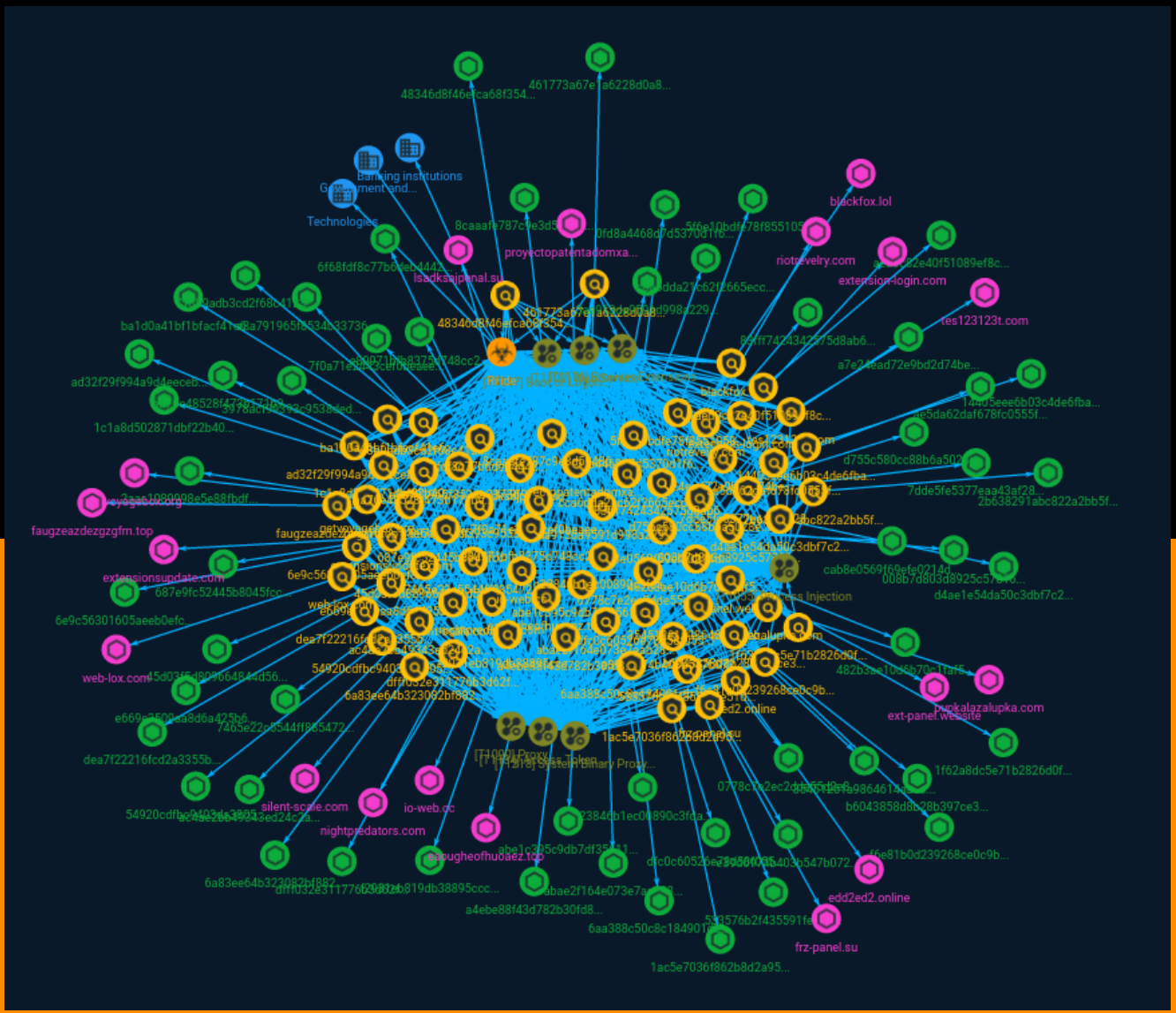

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Trustwave SpiderLabs discovered a new version of the Rilide Stealer extension targeting Chromium-based browsers such as Google Chrome, Microsoft Edge, Brave, and Opera. This malware uses a creative way to work around the Chrome Extension Manifest V3 from Google which is aimed at blocking the installation of malicious extensions for chromium browsers.

Confidence

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

15 / 100

Indicator

Name
7465e22c5544ff885472e36dd60beec5039c68c4728d804fea240bc36e8f6794
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '7465e22c5544ff885472e36dd60beec5039c68c4728d804fea240bc36e8f6794']
Name
482b3ae10d6b70c1faf55a9b3abd14bdc1b198b18d089a0aea6aa6ac6fd7ace1
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '482b3ae10d6b70c1faf55a9b3abd14bdc1b198b18d089a0aea6aa6ac6fd7ace1']
Name

lsadksajpenal.su

Pattern Type

stix

Pattern

[domain-name:value = 'lsadksajpenal.su']

Name

533576b2f435591fe51d0e09d479154fac13a6440c619085dc0a11ada0f69e12

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '533576b2f435591fe51d0e09d479154fac13a6440c619085dc0a11ada0f69e12']

Name

cab8e0569f69efe0214dea05461cba63c3abb9c255f17e2ae48e904dfce500fd

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'cab8e0569f69efe0214dea05461cba63c3abb9c255f17e2ae48e904dfce500fd']

Name

abe1c395c9db7df35611caf30fff0a18f23726505b2b51e4dce6547896ee6f76

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'abe1c395c9db7df35611caf30fff0a18f23726505b2b51e4dce6547896ee6f76']

Name

45d03f5d809664844d569d35431a147885d201ca151bda9bf66f282daec025a6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '45d03f5d809664844d569d35431a147885d201ca151bda9bf66f282daec025a6']

Name

718b9adb3cd2f68c41234870242e312cac6beb00444ed4e21dca5f21b6fbecb9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '718b9adb3cd2f68c41234870242e312cac6beb00444ed4e21dca5f21b6fbecb9']

Name

e39d0974b403b547b07282237f356061754375d1b70dacf731d8fa2add15d856

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e39d0974b403b547b07282237f356061754375d1b70dacf731d8fa2add15d856']

Name

2aac1089998e5e88fbdf539408be53570a4ed64a989885d1003bf73c723eea1d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2aac1089998e5e88fbdf539408be53570a4ed64a989885d1003bf73c723eea1d']

Name

eaougheofhuoaez.top

Pattern Type

stix

Pattern

[domain-name:value = 'eaougheofhuoaez.top']

Name

abae2f164e073e7aab2822b507de10e731cc1b396809728452e98be6618c149f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'abae2f164e073e7aab2822b507de10e731cc1b396809728452e98be6618c149f']

Name

extensionsupdate.com

Pattern Type

stix

Pattern

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

Name

a7e24ead72e9bd2d74be36c201e348d5c5aa29c1c0c4e972677ce12602a74158

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a7e24ead72e9bd2d74be36c201e348d5c5aa29c1c0c4e972677ce12602a74158']

Name

e669e3509aa8d6a425b61e77993b23f832071ba2f7def373af57417f661eb431

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e669e3509aa8d6a425b61e77993b23f832071ba2f7def373af57417f661eb431']

Name

riotrevelry.com

Pattern Type

stix

Pattern

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

Name

008b7d803d8925c578168a2bd757dd4a0b26b32b2f810ce91e3f062e1ed5cd0c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '008b7d803d8925c578168a2bd757dd4a0b26b32b2f810ce91e3f062e1ed5cd0c']

Name

6e9c56301605aeeb0efcbbfbf10008dba7a8b99963f02256d1b28fbc30df7907

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6e9c56301605aeeb0efcbbfbf10008dba7a8b99963f02256d1b28fbc30df7907']

Name

0778c7e2ec2dde55d2e88f31168a52d8e78ce5348ccab82c8e6b2c0f3bb0b3eb

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0778c7e2ec2dde55d2e88f31168a52d8e78ce5348ccab82c8e6b2c0f3bb0b3eb']

Name

3978acf99393c9538dedc22f97eb247bbcfe0791acead7f6c96d1079479286fd

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3978acf99393c9538dedc22f97eb247bbcfe0791acead7f6c96d1079479286fd']

Name

687e9fc52445b8045fccc308c30713395bdfba08dac83fc85355a5c94b2bbbde

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '687e9fc52445b8045fccc308c30713395bdfba08dac83fc85355a5c94b2bbbde']

Name

d755c580cc88b6a5028e843aeda3e3a50c8f025ef1dcf66027c0c1b671024d36

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd755c580cc88b6a5028e843aeda3e3a50c8f025ef1dcf66027c0c1b671024d36']

Name

silent-scale.com

Pattern Type

stix

Pattern

[domain-name:value = 'silent-scale.com']

Name

7f0a71e2443cef0beaeea10a78fbbdb3a612be6c4be206acf7c13849d593fad7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7f0a71e2443cef0beaeea10a78fbbdb3a612be6c4be206acf7c13849d593fad7']

Name

6aa388c50c8c184901db02eae71b1ec3d9e0ab9e636d22419f64a83c8b2c94b0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6aa388c50c8c184901db02eae71b1ec3d9e0ab9e636d22419f64a83c8b2c94b0']

Name

ad32f29f994a9d4eeceb39afeaa2a1dbda4f17931668d64026c225c738518cfd

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ad32f29f994a9d4eeceb39afeaa2a1dbda4f17931668d64026c225c738518cfd']

Name

extension-login.com

Pattern Type

stix

Pattern

[domain-name:value = 'extension-login.com']

Name

nightpredators.com

Pattern Type

stix

Pattern

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

Name

3aa913da9591d998a229acec529eb58b1fea14b403b92f56dde47a8425739473

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3aa913da9591d998a229acec529eb58b1fea14b403b92f56dde47a8425739473']

Name

1f62a8dc5e71b2826d0fe70588c4c4cbebb9518d3f1125807e6e6927b359458a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1f62a8dc5e71b2826d0fe70588c4c4cbebb9518d3f1125807e6e6927b359458a']

Name

54920cdfbc9403da38058b90bfb19a1af5caff2ca4584209d13e0f90b64c3b2c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '54920cdfbc9403da38058b90bfb19a1af5caff2ca4584209d13e0f90b64c3b2c']

Name

5f6e10bdfe78f855105843c67ff6ec69801caba328a8b1681425b06e359f888c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5f6e10bdfe78f855105843c67ff6ec69801caba328a8b1681425b06e359f888c']

Name

a4ebe88f43d782b30fd83e1fb79b26674827cc03db4aeb77540243c303b51a6a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a4ebe88f43d782b30fd83e1fb79b26674827cc03db4aeb77540243c303b51a6a']

Name

io-web.cc

Pattern Type

stix

Pattern

[domain-name:value = 'io-web.cc']

Name

ext-panel.website

Pattern Type

stix

Pattern

[domain-name:value = 'ext-panel.website']

Name

dfc0c60526e78d58f055ddace6cb91227958a0c5b413c88d00be175f084bd5da

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'dfc0c60526e78d58f055ddace6cb91227958a0c5b413c88d00be175f084bd5da']

Name

0fd8a4468d7d5370d1f67b01badb2e7e1aacb3e6cf1689cab4f678cc7868f520

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0fd8a4468d7d5370d1f67b01badb2e7e1aacb3e6cf1689cab4f678cc7868f520']

Name

2b638291abc822a2bb5f94b196022cae4b064487a71a8e067f8d8a2fb3c7acc5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2b638291abc822a2bb5f94b196022cae4b064487a71a8e067f8d8a2fb3c7acc5']

Name

e8a791965f8534b33736a0786ebeb0975002f3a03c31aefe2e4a64a1d4c70a34

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e8a791965f8534b33736a0786ebeb0975002f3a03c31aefe2e4a64a1d4c70a34']

Name

7dde5fe5377eaa43af2896f0aab7a6875ac88a34d0391c39d0979c3cf2861723

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7dde5fe5377eaa43af2896f0aab7a6875ac88a34d0391c39d0979c3cf2861723']

Name

e89971bfb8375d748cc233157537856c5598fcd513ed42e862261a99843f40d0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e89971bfb8375d748cc233157537856c5598fcd513ed42e862261a99843f40d0']

Name
proyectopatentadomxapostol.com
Pattern Type
stix
Pattern
[domain-name:value = 'proyectopatentadomxapostol.com']
Name
pupkalazalupka.com
Pattern Type
stix
Pattern
[domain-name:value = 'pupkalazalupka.com']
Name
dfff032e311776b3d62f70856a6d29ca8267beee614f756301b7f891c6325485
Pattern Type
stix
Pattern

[file:hashes.'SHA-256' = 'dfff032e311776b3d62f70856a6d29ca8267beee614f756301b7f891c6325485']

Name

461773a67e1a6228d0a8d02a45da72fc94ce0df97cd99aef33dcbf859d306a11

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '461773a67e1a6228d0a8d02a45da72fc94ce0df97cd99aef33dcbf859d306a11']

Name

edd2ed2.online

Pattern Type

stix

Pattern

[domain-name:value = 'edd2ed2.online']

Name

1c1a8d502871dbf22b404b6825b5219344a3d89ebb5da88380ba1ca158e2d92b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1c1a8d502871dbf22b404b6825b5219344a3d89ebb5da88380ba1ca158e2d92b']

Name

tes123123t.com

Pattern Type

stix

Pattern

[domain-name:value = 'tes123123t.com']

Name

ac4ae2bb49343ed24c2ae0d531cde04c3186dc4263a2352f2c2ac78812bb5c05

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ac4ae2bb49343ed24c2ae0d531cde04c3186dc4263a2352f2c2ac78812bb5c05']

Name

cca6dda21c62f2665eccdec2edff5e6dfa6260a217c02709b21b3e14670ca3b7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'cca6dda21c62f2665eccdec2edff5e6dfa6260a217c02709b21b3e14670ca3b7']

Name

35451261a9864614aaeb43cd8bfb8d166a483baaa4477c6e119ebcffffa0ba31

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '35451261a9864614aaeb43cd8bfb8d166a483baaa4477c6e119ebcffffa0ba31']

Name

getvoyagebox.org

Pattern Type

stix

Pattern

[domain-name:value = 'getvoyagebox.org']

Name

blackfox.lol

Pattern Type

stix

Pattern

[domain-name:value = 'blackfox.lol']

Name

1ac5e7036f862b8d2a951b1be262b498f0c9213d4d2f500e9c5f06ac8e8179b2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1ac5e7036f862b8d2a951b1be262b498f0c9213d4d2f500e9c5f06ac8e8179b2']

Name

48346d8f46efca68f354f0833c3cfc9e8931d5b655ec434725fcdffb03069460

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '48346d8f46efca68f354f0833c3cfc9e8931d5b655ec434725fcdffb03069460']

Name

ae5da62daf678fc0555f739c116f58fd26c5400257367dcd0f777997615a4b23

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ae5da62daf678fc0555f739c116f58fd26c5400257367dcd0f777997615a4b23']

Name

dea7f22216fcd2a3355b231d57dec37164c85faf3e9279beae6cdb153051a48a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'dea7f22216fcd2a3355b231d57dec37164c85faf3e9279beae6cdb153051a48a']

Name

c23846b1ec00890c3fda2b600b29b2fb717de6fa54b8c9bebe825aa4e0a7f2cc

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c23846b1ec00890c3fda2b600b29b2fb717de6fa54b8c9bebe825aa4e0a7f2cc']

Name

frz-panel.su

Pattern Type

stix

Pattern

[domain-name:value = 'frz-panel.su']

Name

faugzeazdezgzgfm.top

Pattern Type

stix

Pattern

[domain-name:value = 'faugzeazdezgzgfm.top']

Name

83fff7424342575d8ab6a9bd8eba71490e75a87ea825c8a84bb16945613467e1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '83fff7424342575d8ab6a9bd8eba71490e75a87ea825c8a84bb16945613467e1']

Name

f2931eb819db38895ccc016a6b04b90bb1456931164f2b7e15f4bc0c95fbd997

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f2931eb819db38895ccc016a6b04b90bb1456931164f2b7e15f4bc0c95fbd997']

Name

6f68fdf8c77b6deb44427322f82a6476a631ec6e4cdb0b18421bf5a0c895435e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6f68fdf8c77b6deb44427322f82a6476a631ec6e4cdb0b18421bf5a0c895435e']

Name

d4ae1e54da50c3dbf7c201a42537f42fc307c5ce7700ad32aceb60f69ed7d779

Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'd4ae1e54da50c3dbf7c201a42537f42fc307c5ce7700ad32aceb60f69ed7d779']
Name
aa76e48528f473b171b98bfc4d4e4d839a98c255e78382dc6f020e36ed00ea5b
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'aa76e48528f473b171b98bfc4d4e4d839a98c255e78382dc6f020e36ed00ea5b']
Name
aed0c82e40f51089ef8c08df53404d61a591db8f14f07a9ef38aeeef8f4e15a8
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'aed0c82e40f51089ef8c08df53404d61a591db8f14f07a9ef38aeeef8f4e15a8']

Name

b6043858d8b28b397ce364417a59167bb1afb32b5c8fcf0be428362af7952e27

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b6043858d8b28b397ce364417a59167bb1afb32b5c8fcf0be428362af7952e27']

Name

ba1d0a41bf1bfacf41e667857cbd24b9834631613de44124b95357cd5c7637c3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ba1d0a41bf1bfacf41e667857cbd24b9834631613de44124b95357cd5c7637c3']

Name

14405eee6b03c4de6fba6b68768a943120c092280e0763ee2672b7ffdf9358bc

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '14405eee6b03c4de6fba6b68768a943120c092280e0763ee2672b7ffdf9358bc']

Name

6a83ee64b323082bf8827deb6297d4d3895f346ff83e9d9d4d125e976df5e503

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6a83ee64b323082bf8827deb6297d4d3895f346ff83e9d9d4d125e976df5e503']

Name

8caaafe787c9e3d59486ec129b4259764641999b0f1de6b5b46d3773e96442c8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8caaafe787c9e3d59486ec129b4259764641999b0f1de6b5b46d3773e96442c8']

Name

f6e81b0d239268ce0c9bb6ba7dbe09fb67ffa273a85fdfe656b14b5ea9a94568

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f6e81b0d239268ce0c9bb6ba7dbe09fb67ffa273a85fdfe656b14b5ea9a94568']

Name

web-lox.com

Pattern Type

stix

Pattern

[domain-name:value = 'web-lox.com']

Malware

Name
Rilide

Sector

Name
Banking institutions
Description
Credit institutions whose business consists in receiving repayable funds from the public and granting credit. As the bank of banks, central banks are included in this scope.
Name
Technologies
Description
Private entities related to the research, development, manufacturing and distribution of electronics, softwares, computers and products related to information technologies.
Name
Government and administrations
Description
Civilian government institutions and administrations of the executive and legislative branches. The diplomatic and judicial branches are not included.

Attack-Pattern

Name
Browser Extensions
ID
T1176
Description
Adversaries may abuse Internet browser extensions to establish persistent access to victim systems. Browser extensions or plugins are small programs that can add functionality and customize aspects of Internet browsers. They can be installed directly or through a browser's app store and generally have access and permissions to everything that the browser can access.(Citation: Wikipedia Browser Extension)(Citation: Chrome Extensions Definition) Malicious extensions can be installed into a browser through malicious app store downloads masquerading as legitimate extensions, through social engineering, or by an adversary that has already compromised a system. Security can be limited on browser app stores so it may not be difficult for malicious extensions to defeat automated scanners.(Citation: Malicious Chrome Extension Numbers) Depending on the browser, adversaries may also manipulate an extension's update url to install updates from an adversary controlled server or manipulate the mobile configuration file to silently install additional extensions. Previous to macOS 11, adversaries could silently install browser extensions via the command line using the `profiles` tool to install malicious `.mobileconfig` files. In macOS 11+, the use of the `profiles` tool can no longer install configuration profiles, however `.mobileconfig` files can be planted and installed with user interaction.(Citation: xorrior chrome extensions macOS) Once the extension is installed, it can browse to websites in the background, steal all information that a user enters into a browser (including credentials), and be used as an installer for a RAT for persistence. (Citation: Chrome Extension Crypto Miner)(Citation: ICEBRG Chrome Extensions)(Citation: Banker Google Chrome Extension Steals Creds)(Citation: Catch All Chrome Extension) There

have also been instances of botnets using a persistent backdoor through malicious Chrome extensions.(Citation: Stantinko Botnet) There have also been similar examples of extensions being used for command & control.(Citation: Chrome Extension C2 Malware)

Name

Access Token Manipulation

ID

T1134

Description

Adversaries may modify access tokens to operate under a different user or system security context to perform actions and bypass access controls. Windows uses access tokens to determine the ownership of a running process. A user can manipulate access tokens to make a running process appear as though it is the child of a different process or belongs to someone other than the user that started the process. When this occurs, the process also takes on the security context associated with the new token. An adversary can use built-in Windows API functions to copy access tokens from existing processes; this is known as token stealing. These token can then be applied to an existing process (i.e. [Token Impersonation/Theft](https://attack.mitre.org/techniques/T1134/001)) or used to spawn a new process (i.e. [Create Process with Token](https://attack.mitre.org/techniques/T1134/002)). An adversary must already be in a privileged user context (i.e. administrator) to steal a token. However, adversaries commonly use token stealing to elevate their security context from the administrator level to the SYSTEM level. An adversary can then use a token to authenticate to a remote system as the account for that token if the account has appropriate permissions on the remote system.(Citation: Pentestlab Token Manipulation) Any standard user can use the `runas` command, and the Windows API functions, to create impersonation tokens; it does not require access to an administrator account. There are also other mechanisms, such as Active Directory fields, that can be used to modify access tokens.

Name

Boot or Logon Autostart Execution

ID

T1547

Description

Adversaries may configure system settings to automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges on compromised systems. Operating systems may have mechanisms for automatically running a program on system boot or account logon.(Citation: Microsoft Run Key)(Citation: MSDN Authentication Packages)(Citation: Microsoft TimeProvider)(Citation: Cylance Reg Persistence Sept 2013)(Citation: Linux Kernel Programming) These mechanisms may include automatically executing programs that are placed in specially designated directories or are referenced by repositories that store configuration information, such as the Windows Registry. An adversary may achieve the same goal by modifying or extending features of the kernel. Since some boot or logon autostart programs run with higher privileges, an adversary may leverage these to elevate privileges.

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

Proxy

ID

T1090

Description

Adversaries may use a connection proxy to direct network traffic between systems or act as an intermediary for network communications to a command and control server to avoid direct connections to their infrastructure. Many tools exist that enable traffic redirection through proxies or port redirection, including [HTRAN](https://attack.mitre.org/software/S0040), ZXProxy, and ZXPortMap. (Citation: Trend Micro APT Attack Tools) Adversaries use these types of proxies to manage command and control communications, reduce the number of simultaneous outbound network connections, provide resiliency in the face of connection loss, or to ride over existing trusted communications paths between victims to avoid suspicion. Adversaries may chain together multiple proxies to further disguise the source of malicious traffic. Adversaries can also take advantage of routing schemes in Content Delivery Networks (CDNs) to proxy command and control traffic.

Name

Web Service

ID

T1102

Description

Adversaries may use an existing, legitimate external Web service as a means for relaying data to/from a compromised system. Popular websites and social media acting as a mechanism for C2 may give a significant amount of cover due to the likelihood that hosts within a network are already communicating with them prior to a compromise. Using common services, such as those offered by Google or Twitter, makes it easier for adversaries to hide in expected noise. Web service providers commonly use SSL/TLS

encryption, giving adversaries an added level of protection. Use of Web services may also protect back-end C2 infrastructure from discovery through malware binary analysis while also enabling operational resiliency (since this infrastructure may be dynamically changed).

Name

System Binary Proxy Execution

ID

T1218

Description

Adversaries may bypass process and/or signature-based defenses by proxying execution of malicious content with signed, or otherwise trusted, binaries. Binaries used in this technique are often Microsoft-signed files, indicating that they have been either downloaded from Microsoft or are already native in the operating system.(Citation: LOLBAS Project) Binaries signed with trusted digital certificates can typically execute on Windows systems protected by digital signature validation. Several Microsoft signed binaries that are default on Windows installations can be used to proxy execution of other files or commands. Similarly, on Linux systems adversaries may abuse trusted binaries such as `split` to proxy execution of malicious commands.(Citation: split man page)(Citation: GTFO split)

Domain-Name

Value
frz-panel.su
eaougheofhuoaez.top
getvoyagebox.org
io-web.cc
extensionsupdate.com
tes123123t.com
silent-scale.com
blackfox.lol
edd2ed2.online
nightpredators.com
lsadksajpenal.su
proyectopatentadomxapostol.com
faugzeazdezgzgfm.top

riotrevelry.com

ext-panel.website

extension-login.com

pupkalazalupka.com

web-lox.com

StixFile

Value
0fd8a4468d7d5370d1f67b01badb2e7e1aacb3e6cf1689cab4f678cc7868f520
7dde5fe5377eaa43af2896f0aab7a6875ac88a34d0391c39d0979c3cf2861723
5f6e10bdfe78f855105843c67ff6ec69801caba328a8b1681425b06e359f888c
ba1d0a41bf1bfacf41e667857cbd24b9834631613de44124b95357cd5c7637c3
7f0a71e2443cef0beaeea10a78fbbdb3a612be6c4be206acf7c13849d593fad7
d755c580cc88b6a5028e843aeda3e3a50c8f025ef1dcf66027c0c1b671024d36
35451261a9864614aaeb43cd8bfb8d166a483baaa4477c6e119ebcffffa0ba31
45d03f5d809664844d569d35431a147885d201ca151bda9bf66f282daec025a6
2b638291abc822a2bb5f94b196022cae4b064487a71a8e067f8d8a2fb3c7acc5
c23846b1ec00890c3fda2b600b29b2fb717de6fa54b8c9bebe825aa4e0a7f2cc
ae5da62daf678fc0555f739c116f58fd26c5400257367dcd0f777997615a4b23
1f62a8dc5e71b2826d0fe70588c4c4cbebb9518d3f1125807e6e6927b359458a
7465e22c5544ff885472e36dd60beec5039c68c4728d804fea240bc36e8f6794

b6043858d8b28b397ce364417a59167bb1afb32b5c8fcf0be428362af7952e27

1ac5e7036f862b8d2a951b1be262b498f0c9213d4d2f500e9c5f06ac8e8179b2

461773a67e1a6228d0a8d02a45da72fc94ce0df97cd99aef33dcbf859d306a11

e8a791965f8534b33736a0786ebeb0975002f3a03c31aefe2e4a64a1d4c70a34

abe1c395c9db7df35611caf30fff0a18f23726505b2b51e4dce6547896ee6f76

e89971bfb8375d748cc233157537856c5598fcd513ed42e862261a99843f40d0

482b3ae10d6b70c1faf55a9b3abd14bdc1b198b18d089a0aea6aa6ac6fd7ace1

ad32f29f994a9d4eeceb39afeaa2a1dbda4f17931668d64026c225c738518cfd

d4ae1e54da50c3dbf7c201a42537f42fc307c5ce7700ad32aceb60f69ed7d779

e39d0974b403b547b07282237f356061754375d1b70dacf731d8fa2add15d856

ac4ae2bb49343ed24c2ae0d531cde04c3186dc4263a2352f2c2ac78812bb5c05

8caaafe787c9e3d59486ec129b4259764641999b0f1de6b5b46d3773e96442c8

6a83ee64b323082bf8827deb6297d4d3895f346ff83e9d9d4d125e976df5e503

a7e24ead72e9bd2d74be36c201e348d5c5aa29c1c0c4e972677ce12602a74158

1c1a8d502871dbf22b404b6825b5219344a3d89ebb5da88380ba1ca158e2d92b

2aac1089998e5e88fbdf539408be53570a4ed64a989885d1003bf73c723eea1d

aed0c82e40f51089ef8c08df53404d61a591db8f14f07a9ef38aeeef8f4e15a8

f2931eb819db38895ccc016a6b04b90bb1456931164f2b7e15f4bc0c95fbd997

48346d8f46efca68f354f0833c3cfc9e8931d5b655ec434725fcdffb03069460

dfff032e311776b3d62f70856a6d29ca8267beee614f756301b7f891c6325485

abae2f164e073e7aab2822b507de10e731cc1b396809728452e98be6618c149f

dea7f22216fcd2a3355b231d57dec37164c85faf3e9279beae6cdb153051a48a

14405eee6b03c4de6fba6b68768a943120c092280e0763ee2672b7ffdf9358bc

6e9c56301605aeeb0efcbbfbf10008dba7a8b99963f02256d1b28fbc30df7907

cab8e0569f69efe0214dea05461cba63c3abb9c255f17e2ae48e904dfce500fd

a4ebe88f43d782b30fd83e1fb79b26674827cc03db4aeb77540243c303b51a6a

3aa913da9591d998a229acec529eb58b1fea14b403b92f56dde47a8425739473

cca6dda21c62f2665eccdec2edff5e6dfa6260a217c02709b21b3e14670ca3b7

e669e3509aa8d6a425b61e77993b23f832071ba2f7def373af57417f661eb431

008b7d803d8925c578168a2bd757dd4a0b26b32b2f810ce91e3f062e1ed5cd0c

687e9fc52445b8045fccc308c30713395bdfba08dac83fc85355a5c94b2bbbde

718b9adb3cd2f68c41234870242e312cac6beb00444ed4e21dca5f21b6fbecb9

f6e81b0d239268ce0c9bb6ba7dbe09fb67ffa273a85fdfe656b14b5ea9a94568

54920cdfbc9403da38058b90bfb19a1af5caff2ca4584209d13e0f90b64c3b2c

aa76e48528f473b171b98bfc4d4e4d839a98c255e78382dc6f020e36ed00ea5b

533576b2f435591fe51d0e09d479154fac13a6440c619085dc0a11ada0f69e12

6f68fdf8c77b6deb44427322f82a6476a631ec6e4cdb0b18421bf5a0c895435e

dfc0c60526e78d58f055ddace6cb91227958a0c5b413c88d00be175f084bd5da

0778c7e2ec2dde55d2e88f31168a52d8e78ce5348ccab82c8e6b2c0f3bb0b3eb

3978acf99393c9538dedc22f97eb247bbcfe0791acead7f6c96d1079479286fd

6aa388c50c8c184901db02eae71b1ec3d9e0ab9e636d22419f64a83c8b2c94b0

83fff7424342575d8ab6a9bd8eba71490e75a87ea825c8a84bb16945613467e1

External References

- https://otx.alienvault.com/pulse/64cc04f4a7999cd603aad8d6
- https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/new-rilide-stealer-version-targets-banking-data-and-works-around-google-chrome-manifest-v3/