Jul 03 2023

NETMANAGEIT

Intelligence Report

New Fast-Developing ThirdEye Infostealer Pries Open System Information | FortiGuard Labs

http://shlalala.ru/g...
2008bdd98d3dcb663335...
3d9aff07e4cb6c943aec...
http://glovatickets....
[T1539] Steal Web Session Cookie
[T1566] Phishing
0a798b4e7bd4853ec9f0...
5d211c47612b98426dd3...
610aff11acce8398f2b3...
9db721fa9ea9cdec98f1...
847cbe9457b001faf3c0...
263600712137c1465e0f...
[T1140] Deobfuscate/Decode Files or Information
[T1020] Automated Exfiltration
http://ohmycars.ru/g...
a9d98b15c94bb310cdb6...
c36c4a09bccdeda6e5d3...
f0e6d44137cb5fcee20b...
http://anime-clab.ru...
based on
indicates
targets

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A previously unseen infostealer that harvests information from compromised machines is being developed by FortiGuard Labs, who recently uncovered a new variant of the malware, which can be used as a stepping-stone for future attacks.

Confidence

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

15 / 100

Indicator

Name

http://glovatickets.ru/ch3ckState

Pattern Type

stix

Pattern

[url:value = 'http://glovatickets.ru/ch3ckState']

Name

http://anime-clab.ru/ch3ckState

Pattern Type

stix

Pattern

[url:value = 'http://anime-clab.ru/ch3ckState']

Name

http://shlalala.ru/general/ch3ckState

Pattern Type

stix

Pattern

[url:value = 'http://shlalala.ru/general/ch3ckState']

Name

610aff11acce8398f2b35e3742cb46c6a168a781c23a816de2aca471492161b2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '610aff11acce8398f2b35e3742cb46c6a168a781c23a816de2aca471492161b2']

Name

5d211c47612b98426dd3c8eac092ac5ce0527bda09afa34b9d0f628109e0c796

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5d211c47612b98426dd3c8eac092ac5ce0527bda09afa34b9d0f628109e0c796']

Name

2008bdd98d3dcb6633357b8d641c97812df916300222fc815066978090fa078f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2008bdd98d3dcb6633357b8d641c97812df916300222fc815066978090fa078f']

Name

9db721fa9ea9cdec98f113b81429db29ea47fb981795694d88959d8a9f1042e6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9db721fa9ea9cdec98f113b81429db29ea47fb981795694d88959d8a9f1042e6']

Name

847cbe9457b001faf3c09fde89ef95f9ca9e1f79c29091c4b5b08c5f5fe48337

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '847cbe9457b001faf3c09fde89ef95f9ca9e1f79c29091c4b5b08c5f5fe48337']

Name

263600712137c1465e0f28e1603b3e8feb9368a37503fa1c9edaaab245c63026

Description

stack_string

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '263600712137c1465e0f28e1603b3e8feb9368a37503fa1c9edaaab245c63026']

Name

http://ohmycars.ru/general/ch3ckState

Pattern Type

stix

Pattern

[url:value = 'http://ohmycars.ru/general/ch3ckState']

Name

a9d98b15c94bb310cdb61440fa2b11d0c7b4aa113702035156ce23f6b6c5eecf

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'a9d98b15c94bb310cdb61440fa2b11d0c7b4aa113702035156ce23f6b6c5eecf']

Name

f6e6d44137cb5fcee20bcde0a162768dadbb84a09cc680732d9e23ccd2e79494

Description

stack_string

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'f6e6d44137cb5fcee20bcde0a162768dadbb84a09cc680732d9e23ccd2e79494']

Name

3d9aff07e4cb6c943aec7fcd2d845d21d0261f6f8ae1c94aee4abdf4eef5924d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'3d9aff07e4cb6c943aec7fcd2d845d21d0261f6f8ae1c94aee4abdf4eef5924d']

Name

0a798b4e7bd4853ec9f0d3d84ad54a8d24170aa765db2591ed3a49e66323742c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'0a798b4e7bd4853ec9f0d3d84ad54a8d24170aa765db2591ed3a49e66323742c']

Name

c36c4a09bccdeda263a33bc87a166dfbad78c86b0f953fcd57e8ca42752af2fc

Description

stack_string

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'c36c4a09bccdeda263a33bc87a166dfbad78c86b0f953fcd57e8ca42752af2fc']

Attack-Pattern

Name

Web Cookies

ID

T1606.001

Description

Adversaries may forge web cookies that can be used to gain access to web applications or Internet services. Web applications and services (hosted in cloud SaaS environments or on-premise servers) often use session cookies to authenticate and authorize user access. Adversaries may generate these cookies in order to gain access to web resources. This differs from [Steal Web Session Cookie](https://attack.mitre.org/techniques/T1539) and other similar behaviors in that the cookies are new and forged by the adversary, rather than stolen or intercepted from legitimate users. Most common web applications have standardized and documented cookie values that can be generated using provided tools or interfaces.(Citation: Pass The Cookie) The generation of web cookies often requires secret values, such as passwords, [Private Keys](https://attack.mitre.org/techniques/T1552/004), or other cryptographic seed values. Once forged, adversaries may use these web cookies to access resources ([Web Session Cookie](https://attack.mitre.org/techniques/T1550/004)), which may bypass multi-factor and other authentication protection mechanisms.(Citation: Volexity SolarWinds)(Citation: Pass The Cookie)(Citation: Unit 42 Mac Crypto Cookies January 2019)

Name

Automated Exfiltration

ID

T1020

Description

Adversaries may exfiltrate data, such as sensitive documents, through the use of automated processing after being gathered during Collection. When automated exfiltration is used, other exfiltration techniques likely apply as well to transfer the information out of the network, such as [Exfiltration Over C2 Channel](https://attack.mitre.org/techniques/T1041) and [Exfiltration Over Alternative Protocol](https://attack.mitre.org/techniques/T1048).

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

Deobfuscate/Decode Files or Information

ID

T1140

Description

Adversaries may use [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware or by using utilities present on the system. One such example is the use of [certutil](https://attack.mitre.org/software/S0160) to decode a remote access tool portable executable file that has been hidden inside a certificate file.(Citation: Malwarebytes Targeted Attack against Saudi Arabia) Another example is using the Windows `copy /b` command to reassemble binary fragments into a malicious payload.(Citation: Carbon Black Obfuscation Sept 2016) Sometimes a user's action may be required to open it for deobfuscation or decryption as part of [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)

Vulnerability

Name
CVE-2023-34362

StixFile

Value
847cbe9457b001faf3c09fde89ef95f9ca9e1f79c29091c4b5b08c5f5fe48337
f6e6d44137cb5fcee20bcde0a162768dadbb84a09cc680732d9e23ccd2e79494
3d9aff07e4cb6c943aec7fcd2d845d21d0261f6f8ae1c94aee4abdf4eef5924d
263600712137c1465e0f28e1603b3e8feb9368a37503fa1c9edaaab245c63026
9db721fa9ea9cdec98f113b81429db29ea47fb981795694d88959d8a9f1042e6
610aff11acce8398f2b35e3742cb46c6a168a781c23a816de2aca471492161b2
a9d98b15c94bb310cdb61440fa2b11d0c7b4aa113702035156ce23f6b6c5eecf
2008bdd98d3dcb6633357b8d641c97812df916300222fc815066978090fa078f
c36c4a09bccdeda263a33bc87a166dfbad78c86b0f953fcd57e8ca42752af2fc
5d211c47612b98426dd3c8eac092ac5ce0527bda09afa34b9d0f628109e0c796
0a798b4e7bd4853ec9f0d3d84ad54a8d24170aa765db2591ed3a49e66323742c

Url

Value
http://glovatickets.ru/ch3ckState
http://anime-clab.ru/ch3ckState
http://shlalala.ru/general/ch3ckState
http://ohmycars.ru/general/ch3ckState

External References

- https://www.fortinet.com/blog/threat-research/new-fast-developing-thirdeye-infostealer-pries-open-system-information
- https://otx.alienvault.com/pulse/64a2fd5d41b0df8a9965bb6a