Mar 28 2024

NETMANAGEIT

Intelligence Report

Fake Browser Update Campaign

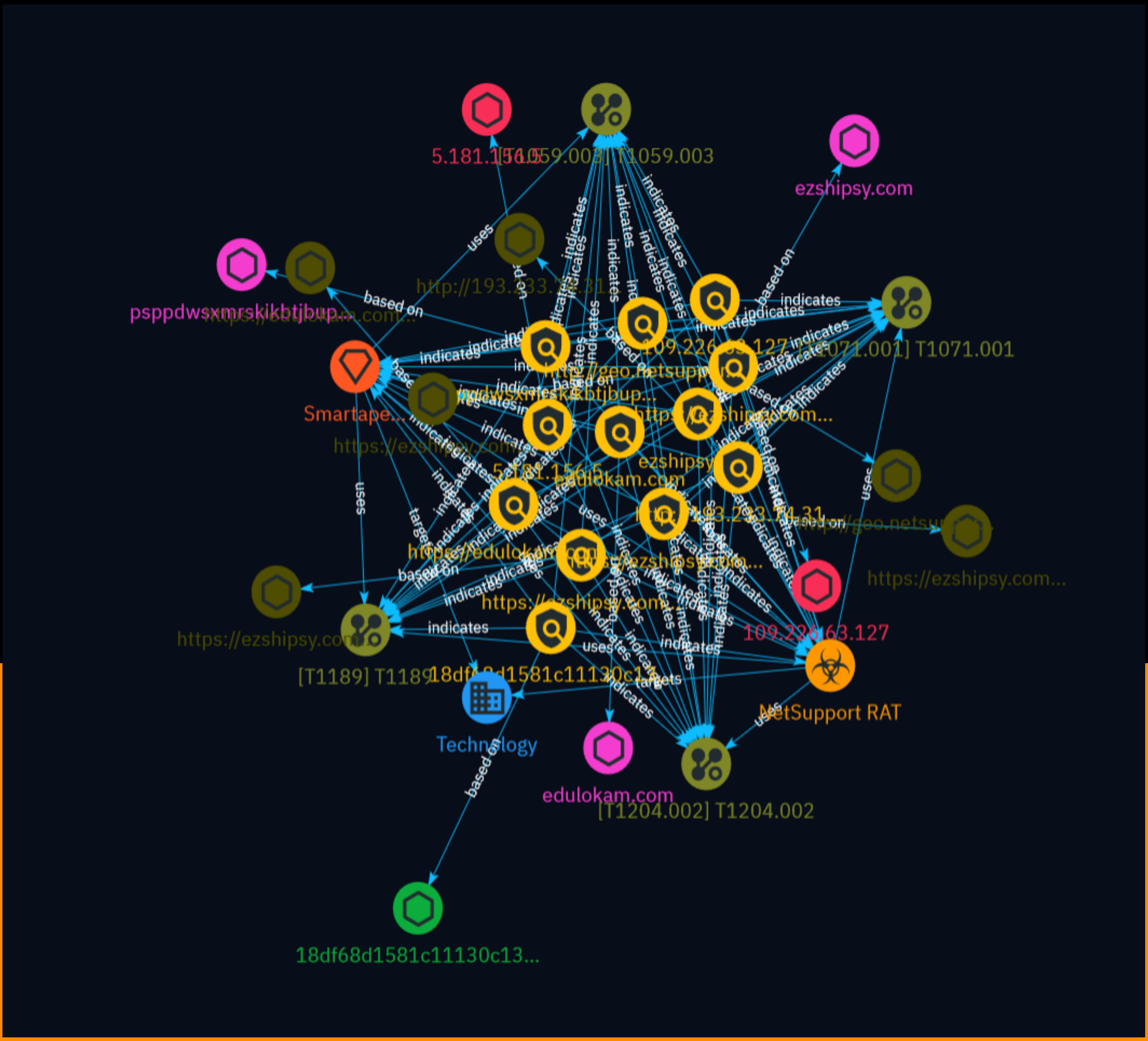

Table of contents

Overview

Entities

Observables

External References

Overview

Description

This report details a malware campaign distributing fake browser updates containing the NetSupport RAT remote access trojan. The attackers use staged web injections to ultimately download an executable payload which phones home to a command and control server.

Confidence

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

100 / 100

Content

N/A

Indicator

Name

psppdwsxmrskikbtjbupwcqajjzphmt.run

Pattern Type

stix

Pattern

[domain-name:value = 'psppdwsxmrskikbtjbupwcqajjzphmt.run']

Name

ezshipsy.com

Pattern Type

stix

Pattern

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

Name

edulokam.com

Pattern Type

stix

Pattern

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

Name

https://ezshipsy.com/help/zewmrgqnw.php?reqtime=1711551912405

Pattern Type

stix

Pattern

[url:value = 'https://ezshipsy.com/help/zewmrgqnw.php?reqtime=1711551912405']

Name

https://ezshipsy.com/help/helper.php

Pattern Type

stix

Pattern

[url:value = 'https://ezshipsy.com/help/helper.php']

Name

https://ezshipsy.com/cdn-vs/cache.php

Pattern Type

stix

Pattern

[url:value = 'https://ezshipsy.com/cdn-vs/cache.php']

Name

https://edulokam.com/data.php?9605

Pattern Type

stix

Pattern

[url:value = 'https://edulokam.com/data.php?9605']

Name

http://geo.netsupportsoftware.com/location/loca.asp

Pattern Type

stix

Pattern

[url:value = 'http://geo.netsupportsoftware.com/location/loca.asp']

Name

http://193.233.74.31/13cecbdad86667b0.php

Pattern Type

stix

Pattern

[url:value = 'http://193.233.74.31/13cecbdad86667b0.php']

Name

5.181.156.5

Description

ISP: MivoCloud SRL **OS:** Windows Server 2012 R2 -------------------------- Services:
22: ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.11 Key type: ssh-rsa Key:
AAAAB3NzaC1yc2EAAAADAQABAAABgQC9ollE/LaMqR2gyCbroCB3Y2/Z0tn5sk0osDovsSJj1Yoe
IUxGvY1ls0NPiItAuhQHjt4zF34Im4bGmx2KMMgVbjCI7IU737yg0gZ7o1AkDnrkwHmSpdUVfhZn
vowsj6h03MWPl8Ly498h5F+YSqosh8RFf/CyJkI9jGK2XD8fVFKxA5T9FItfLdOp0sq4uutjY5EV
IHnaIsDrlwQfH2bJvywaV6Kh9R3nFEq61JLf0ibMYQUtLENqNj4YF/wD0edH0AOubFCW1yB9J5J3
0koPFVVtjab0o0Ry+5wvG3bVZgYJiOpxYk/GwNVcJq/KUnwCHkMk/
PA1m+bfSNzmdpdKpjxM0hMr
DzbYPHUAMIkNcWFqnfPWzJ6EyxI5QxCVTNVZ2ZtprkycqamjDQTha0pYLHMmyyhAT/
gTmK1GbmSl FR8KKwBH/
xDVXaYmrSvalPhyAVS4WdKJyOEIGxjseybfUxpy94jrBEMQcHubvN5hIMUGQGML8P30
RE2WLlIKPfM= Fingerprint: 94:43:d7:7c:fe:19:d9:23:69:a0:8b:86:0b:f8:de:7d 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 kex-strict-s-v00@openssh.com 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 ```
------------------ **443:** ``` ``` ------------------ **3389:** ``` Remote Desktop Protocol
\x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x0f\x08\x00\x02\x00\x00\x00 Remote
Desktop Protocol NTLM Info: OS: Windows 8.1/Windows Server 2012 R2 OS Build: 6.3.9600
Target Name: NEWQ NetBIOS Domain Name: NEWQ NetBIOS Computer Name: NEWQ DNS

Domain Name: newq FQDN: newq Administrator am Windows Server 2012R2 ``` ------------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '5.181.156.5']

Name

109.226.63.127

Description

ISP: Triple C Cloud Computing Ltd. **OS:** Windows ------------------------- Services: **21:** ``` 220 Microsoft FTP Service 230 User logged in. 214-The following commands are recognized (* ==>'s unimplemented). ABOR ACCT ADAT * ALLO APPE AUTH CCC CDUP CWD DELE ENC * EPRT EPSV FEAT HELP HOST LANG LIST MDTM MIC * MKD MODE NLST NOOP OPTS PASS PASV PBSZ PORT PROT PWD QUIT REIN REST RETR RMD RNFR RNTO SITE SIZE SMNT STAT STOR STOU STRU SYST TYPE USER XCUP XCWD XMKD XPWD XRMD 214 HELP command successful. 211-Extended features supported: LANG EN* UTF8 AUTH TLS;TLS-C;SSL;TLS-P; PBSZ PROT C;P; CCC HOST SIZE MDTM REST STREAM 211 END ``` ------------------ **80:** ``` HTTP/1.1 200 OK Content-Type: text/html Last-Modified: Mon, 11 Jul 2016 06:24:26 GMT Accept-Ranges: bytes ETag: "6c9e67df3cdbd11:0" Server: Microsoft-IIS/8.5 Date: Tue, 26 Mar 2024 03:02:51 GMT Content-Length: 701 ``` ------------------ **3389:** ``` Remote Desktop Protocol \x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x0f\x08\x00\x02\x00\x00\x00 Remote Desktop Protocol NTLM Info: OS: Windows 8.1/Windows Server 2012 R2 OS Build: 6.3.9600 Target Name: BMW-162-10187 NetBIOS Domain Name: BMW-162-10187 NetBIOS Computer Name: BMW-162-10187 DNS Domain Name: BMW-162-10187 FQDN: BMW-162-10187 am Windows Server 2012R2 ``` ------------------

Pattern Type

stix

Pattern
[ipv4-addr:value = '109.226.63.127']

Name
18df68d1581c11130c139fa52abb74dfd098a9af698a250645d6a4a65efcbf2d

Description
SHA256 of c4f1b50e3111d29774f7525039ff7086

Pattern Type
stix

Pattern
[file:hashes.'SHA-256' = '18df68d1581c11130c139fa52abb74dfd098a9af698a250645d6a4a65efcbf2d']

Intrusion-Set

Name
Smartape SG/Haneymaney

Malware

Name
NetSupport RAT

Attack-Pattern

Name

T1071.001

ID

T1071.001

Description

Adversaries may communicate using application layer protocols associated with web traffic to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server. Protocols such as HTTP/S(Citation: CrowdStrike Putter Panda) and WebSocket(Citation: Brazking-Websockets) that carry web traffic may be very common in environments. HTTP/S packets have many fields and headers in which data can be concealed. An adversary may abuse these protocols to communicate with systems under their control within a victim network while also mimicking normal, expected traffic.

Name

T1189

ID

T1189

Description

Adversaries may gain access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is typically targeted for exploitation, but adversaries may also use compromised websites for non-exploitation behavior such as acquiring [Application Access Token](https://attack.mitre.org/techniques/T1550/001). Multiple ways of delivering exploit code to a browser exist (i.e., [Drive-by Target](https://attack.mitre.org/techniques/T1608/004)), including: * A legitimate website is compromised where adversaries have injected some form of malicious code such as JavaScript, iFrames, and cross-site scripting * Script files served to a legitimate website from a publicly writeable cloud storage bucket are modified by an adversary * Malicious ads are paid for and served through legitimate ad providers (i.e., [Malvertising](https://attack.mitre.org/techniques/T1583/008)) * Built-in web application interfaces are leveraged for the insertion of any other kind of object that can be used to display web content or contain a script that executes on the visiting client (e.g. forum posts, comments, and other user controllable web content). Often the website used by an adversary is one visited by a specific community, such as government, a particular industry, or region, where the goal is to compromise a specific user or set of users based on a shared interest. This kind of targeted campaign is often referred to a strategic web compromise or watering hole attack. There are several known examples of this occurring.(Citation: Shadowserver Strategic Web Compromise) Typical drive-by compromise process: 1. A user visits a website that is used to host the adversary controlled content. 2. Scripts automatically execute, typically searching versions of the browser and plugins for a potentially vulnerable version. * The user may be required to assist in this process by enabling scripting or active website components and ignoring warning dialog boxes. 3. Upon finding a vulnerable version, exploit code is delivered to the browser. 4. If exploitation is successful, then it will give the adversary code execution on the user's system unless other protections are in place. * In some cases a second visit to the website after the initial scan is required before exploit code is delivered. Unlike [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190), the focus of this technique is to exploit software on a client endpoint upon visiting a website. This will commonly give an adversary access to systems on the internal network instead of external systems that may be in a DMZ. Adversaries may also use compromised websites to deliver a user to a malicious application designed to [Steal Application Access Token](https://attack.mitre.org/techniques/T1528)s, like OAuth tokens, to gain access to protected applications and information. These malicious applications have been delivered through popups on legitimate websites.(Citation: Volexity OceanLotus Nov 2017)

Name

T1059.003

ID
T1059.003

Description
Adversaries may abuse the Windows command shell for execution. The Windows command shell ([cmd](https://attack.mitre.org/software/S0106)) is the primary command prompt on Windows systems. The Windows command prompt can be used to control almost any aspect of a system, with various permission levels required for different subsets of commands. The command prompt can be invoked remotely via [Remote Services](https://attack.mitre.org/techniques/T1021) such as [SSH](https://attack.mitre.org/techniques/T1021/004).(Citation: SSH in Windows) Batch files (ex: .bat or .cmd) also provide the shell with a list of sequential commands to run, as well as normal scripting operations such as conditionals and loops. Common uses of batch files include long or repetitive tasks, or the need to run the same set of commands on multiple systems. Adversaries may leverage [cmd](https://attack.mitre.org/software/S0106) to execute various commands and payloads. Common uses include [cmd](https://attack.mitre.org/software/S0106) to execute a single command, or abusing [cmd](https://attack.mitre.org/software/S0106) interactively with input and output forwarded over a command and control channel.

Name
T1204.002

ID
T1204.002

Description
An adversary may rely upon a user opening a malicious file in order to gain execution. Users may be subjected to social engineering to get them to open a file that will lead to code execution. This user action will typically be observed as follow-on behavior from [Spearphishing Attachment](https://attack.mitre.org/techniques/T1566/001). Adversaries may use several types of files that require a user to execute them, including .doc, .pdf, .xls, .rtf, .scr, .exe, .lnk, .pif, and .cpl. Adversaries may employ various forms of [Masquerading](https://attack.mitre.org/techniques/T1036) and [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) to increase the likelihood that a

user will open and successfully execute a malicious file. These methods may include using a familiar naming convention and/or password protecting the file and supplying instructions to a user on how to open it.(Citation: Password Protected Word Docs) While [Malicious File](https://attack.mitre.org/techniques/T1204/002) frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after [Internal Spearphishing](https://attack.mitre.org/techniques/T1534).

Sector

Name
Technology
Description
Private entities related to the research, development, manufacturing and distribution of electronics, softwares, computers and products related to information technologies.

Domain-Name

Value
psppdwsxmrskikbtjbupwcqajjzphmt.run
ezshipsy.com
edulokam.com

Url

Value
https://ezshipsy.com/help/zewmrgqnw.php?reqtime=1711551912405
https://ezshipsy.com/help/helper.php
https://ezshipsy.com/cdn-vs/cache.php
https://edulokam.com/data.php?9605
http://geo.netsupportsoftware.com/location/loca.asp
http://193.233.74.31/13cecbdad86667b0.php

IPv4-Addr

Value
5.181.156.5
109.226.63.127

StixFile

Value
18df68d1581c11130c139fa52abb74dfd098a9af698a250645d6a4a65efcbf2d

External References

- https://otx.alienvault.com/pulse/66056b207d671fbe55c79f19