Mar 06 2024

NETMANAGEIT

Intelligence Report

WogRAT Malware Exploits aNotepad

WogRAT
Asia
w.linuxwork.net
Japan
newujs.com
http://w.linuxwork.n...
[T1036] T1036
http://newujs.com/dd...
js.domaiso.com
Singapore
[T1071] T1071
linuxwork.net
http://newujs.com/dd...
Hong Kong
newujs.com
t0rguard.net
Eastern Asia
w.newujs.com
w.linuxwork.net
China
http://newujs.com/cfs...
t0rguard.net
the eastern Asia
[T1035] T1035
http://w.linuxwork...
Technology
http://newujs.com/cf...
js.domaiso.com
w.newujs.com
linuxwork.net
WingOfGod
[T1204] User Execution
[T1027] Obfusc...
indicates
located at
uses
targets
based on

Table of contents

Overview

Entities

Observables

External References

Overview

Description

AhnLab Security intelligence Center (ASEC) has recently discovered the distribution of backdoor malware via aNotepad, a free online notepad platform. The malware, classified as WogRAT, supports both Windows and Linux systems. It has been used in attacks since late 2022, often disguised as legitimate software. WogRAT sends data to a command and control server, and can execute commands, upload/download files, etc. The Linux version connects to a Tiny Shell server to receive commands.

Confidence

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

100 / 100

Content

N/A

Indicator

Name
w.newujs.com
Pattern Type
stix
Pattern
[hostname:value = 'w.newujs.com']
Name
w.linuxwork.net
Pattern Type
stix
Pattern
[hostname:value = 'w.linuxwork.net']
Name
js.domaiso.com

Pattern Type

stix

Pattern

[hostname:value = 'js.domaiso.com']

Name

t0rguard.net

Description

- **Unsafe:** True - **Server:** cloudflare - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** True - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '11 months ago', 'timestamp': 1681381957, 'iso': '2023-04-13T06:32:37-04:00'} - **IPQS: Domain:** t0rguard.net - **IPQS: IP Address:** 104.21.75.222

Pattern Type

stix

Pattern

[domain-name:value = 't0rguard.net']

Name

newujs.com

Description

- **Unsafe:** True - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** True - **Phishing:** True - **Suspicious:** True -

Adult: False - **Category:** N/A - **Domain Age:** {'human': '1 year ago', 'timestamp': 1664548329, 'iso': '2022-09-30T10:32:09-04:00'} - **IPQS: Domain:** newujs.com - **IPQS: IP Address:** 45.32.18.189

Pattern Type

stix

Pattern

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

Name

linuxwork.net

Description

- **Unsafe:** True - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** True - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '1 year ago', 'timestamp': 1667279856, 'iso': '2022-11-01T01:17:36-04:00'} - **IPQS: Domain:** linuxwork.net - **IPQS: IP Address:** 45.77.175.245

Pattern Type

stix

Pattern

[domain-name:value = 'linuxwork.net']

Name

http://w.linuxwork.net:443

Description
- **Unsafe:** True - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** True - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '1 year ago', 'timestamp': 1667279856, 'iso': '2022-11-01T01:17:36-04:00'} - **IPQS: Domain:** w.linuxwork.net - **IPQS: IP Address:** 45.77.175.245

Pattern Type
stix

Pattern
[url:value = 'http://w.linuxwork.net:443']

Name
http://newujs.com/dddddd_oo

Description
- **Unsafe:** True - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** True - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '1 year ago', 'timestamp': 1664548329, 'iso': '2022-09-30T10:32:09-04:00'} - **IPQS: Domain:** newujs.com - **IPQS: IP Address:** 45.32.18.189

Pattern Type
stix

Pattern
[url:value = 'http://newujs.com/dddddd_oo']

Name

http://newujs.com/cff/wins.jpg

Description

- **Unsafe:** True - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** True - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '1 year ago', 'timestamp': 1664548329, 'iso': '2022-09-30T10:32:09-04:00'} - **IPQS: Domain:** newujs.com - **IPQS: IP Address:** 45.32.18.189

Pattern Type

stix

Pattern

[url:value = 'http://newujs.com/cff/wins.jpg']

Malware

Name
WogRAT

Intrusion-Set

Name
WingOfGod

Attack-Pattern

Name
T1035
ID
T1035
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

User Execution

ID

T1204

Description

An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behavior from forms of [Phishing](https://attack.mitre.org/techniques/T1566). While [User Execution](https://attack.mitre.org/techniques/T1204) 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). Adversaries may also deceive users into performing actions such as enabling [Remote Access Software](https://attack.mitre.org/techniques/T1219), allowing direct control of the system to the adversary, or downloading and executing malware for [User Execution](https://attack.mitre.org/techniques/T1204). For example, tech support scams can be facilitated through [Phishing](https://attack.mitre.org/techniques/T1566), vishing, or various forms of user interaction. Adversaries can use a combination of these methods, such as spoofing and promoting toll-free numbers or call centers that are used to direct victims to malicious websites, to deliver and execute payloads containing malware or [Remote Access Software](https://attack.mitre.org/techniques/T1219).(Citation: Telephone Attack Delivery)

Name

T1036

ID

T1036

Description

Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. Masquerading occurs when the name or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names. Renaming abusable system utilities to evade security monitoring is also a form of [Masquerading](https://attack.mitre.org/techniques/T1036).(Citation: LOLBAS Main Site) Masquerading may also include the use of [Proxy](https://attack.mitre.org/techniques/T1090) or VPNs to disguise IP addresses, which can allow adversaries to blend in with normal network traffic and bypass conditional access policies or anti-abuse protections.

Name

T1071

ID

T1071

Description

Adversaries may communicate using OSI application layer protocols 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. Adversaries may utilize many different protocols, including those used for web browsing, transferring files, electronic mail, or DNS. For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), commonly used protocols are SMB, SSH, or RDP.

Country

Name
Hong Kong

Name
Singapore

Name
Japan

Name
China

Region

Name
South-eastern Asia

Name
Eastern Asia

Name
Asia

Sector

Name
Technologies

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

Hostname

Value
w.newujs.com
w.linuxwork.net
js.domaiso.com

Domain-Name

Value
t0rguard.net
newujs.com
linuxwork.net

Url

Value
http://w.linuxwork.net:443
http://newujs.com/dddddd_oo
http://newujs.com/cff/wins.jpg

External References

- https://asec.ahnlab.com/en/62446/
- https://otx.alienvault.com/pulse/65e88e7ae77b71e99ddb944e