Recorded Future® Triage

Submit Reports

Overview overview 10 | Static static 3 | wwlib.dll windows7-x64 10 | wwlib.dll windows10-2004-x64

Report | Analysis Logs

Download Sample
Download PCAP
Download PCAPNG
Feedback
Print to PDF

Analysis

max time kernel
119s

max time network
122s

platform
windows7_x64

resource
win7-20231215-en

resource tags

ARCH:X64
ARCH:X86
IMAGE:WIN7-20231215-EN
LOCALE:EN-US
OS:WINDOWS7-X64
SYSTEM

submitted
23-01-2024 13:59

Sharing

Copy URL
Twitter
E-mail

General

Target
wwlib.dll

Size
26KB

MD5
f20ca31b829252aecabeae7ba2e3ec60

SHA1
2a06a4538bb981c33f64a28bdfefdbf6b536aba0

SHA256
6a39e41394e418f1d96fdded86c1a994ce359c4cfb943daad3cb97125c25f6ab

SHA512
42b7b68e141076382cca744ebc5ebb27e886e4cf8d2530e0e8e69bbaafc182e62fd16db17aa6f1223b679054ff9ee0baa4caa5c1a8124008eb5bca0351b91341

SSDEEP
384:h2EYLKywcbyMIRp7NH10MI6aCI2Ldnc/+h/rI//EZYGo9RsTZeGgaRZBpAG3YF8I:BYLI7IvBZZwuTg1IjAGYDROcRZS

Score
10/10
PERSISTENCE

Malware Config

Signatures

Execution | Persistence | Privilege Escalation | Defense Evasion | Discovery

Modifies WinLogon for persistence • 2 TTPs 1 IoCs
PERSISTENCE

Creates scheduled task(s) • 1 TTPs 1 IoCs
Schtasks is often used by malware for persistence or to perform post-infection execution.
PERSISTENCE

Suspicious use of WriteProcessMemory • 3 IoCs

Uses Task Scheduler COM API • 1 TTPs
The Task Scheduler COM API can be used to schedule applications to run on boot or at set times.
PERSISTENCE

PID:2216

C:\Windows\system32\SCHTASKS.exe PID:2480

```
SCHTASKS /CREATE /f /TN "OneDriver Re
porting Task" /TR "shutdown /l /f" /S
C WEEKLY /d TUE,FRI /ST 12:35
```

Network

MITRE ATT&CK Enterprise v15

Replay Monitor

Downloads