Hive Pro

Threat Level

Amber

THREAT ADVISORY

ATTACK REPORT

Woody RAT leverages Follina to target Russia

Date of Publication	Admilarity Code	TA Number
August 5, 2022	A1	TA2022165

Summary

The unknown threat actor employs the Woody RAT to spear-phish Russian organizations. The malware was distributed via archive files and later switched to Microsoft Office documents leveraging the now-patched CVE-2022-30190 vulnerability.

CVE Table

CVE	NAME	PATCH
CVE-2022-30190	Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability	✓

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**T1566** Phishing	**TA0002** Execution	**T1059** Command and Scripting Interpreter
TA0005 Defense Evasion	**T1055** Process Injection	**T1055.012** Process Hollowing	**TA0007** Discovery
T1057 Process Discovery	**T1083** File and Directory Discovery	**T1082** System Information Discovery	**TA0009** Collection
T1560 Archive Collected Data	**TA0011** Command and Control	**T1105** Ingress Tool Transfer	**T1106** Native API
T1102 Web Service	**T1573** Encrypted Channel		

Technical Details

#1 After being deployed on the infected system, the malware uses the process hollowing technique to feed itself into the suspended notepad processes and removes traces from disks as a defensive evasion tactic.

#2 The malware is embedded with two .NET-based libraries, one to run .NET code and another to run PowerShell commands received via a C2 server. To avoid network-based detection, the RAT encrypts its C2 communication channels with combinations of RSA-4096 and AES-CBC encryption standards.

#3 Woody RAT can write arbitrary files to the machine, run additional malware, delete files, enumerate directories, capture screenshots, and gather a list of running processes.

Vulnerability Details

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2022-30190	Windows Server: 2008 - 2022 and Windows: 7 - 11 21H2	cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:*	CWE-78

Indicator of Compromise (IOC)

TYPE	VALUE
SHA-256	982ec24b5599373b65d7fec3b7b66e6afff4872847791cf3c5688f47bfcb8bf0 66378c18e9da070629a2dbbf39e5277e539e043b2b912cc3fed0209c48215d0b b65bc098b475996eaabbb02bb5fee19a18c6ff2eee0062353aff696356e73b7a 43b15071268f757027cf27dd94675fdd8e771cdcd77df6d2530cb8e218acc2ce 408f314b0a76a0d41c99db0cb957d10ea8367700c757b0160ea925d6d7b5dd8e 0588c52582aad248cf0c43aa44a33980e3485f0621dba30445d8da45bba4f834 5c5020ee0f7a5b78a6da74a3f58710cba62f727959f8ece795b0f47828e33e80 3ba32825177d7c2aac957ff1fc5e78b64279aeb748790bc90634e792541de8d3 9bc071fb6a1d9e72c50aec88b4317c3eb7c0f5ff5906b00aa00d9e720cbc828d
Domains	kurmakata.duckdns[.]org microsoft-ru-data[.]ru microsoft-telemetry[.]ru oakrussia[.]ru
IPV4	194.36.189.179

Patch Links

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30190

References

https://blog-malwarebytes-com.cdn.ampproject.org/c/s/blog.malwarebytes.com/threat-intelligence/2022/08/woody-rat-a-new-feature-rich-malware-spotted-in-the-wild/amp/

What Next?

Book a free demo with **HivePro Uni5** to check your exposure to this advisory. HivePro Uni5 is a Threat Exposure Management Solution that proactively reduces an organization's attack surface before it gets exploited.

At Hive Pro we take a long hard look at your vulnerabilities so you can bolster your defenses and fine-tune your offensive cybersecurity tactics.

REPORT GENERATED ON

August 5, 2022 • 2:41 AM

More at www.hivepro.com