Hive Pro

Threat Level

Red

THREAT ADVISORY

ATTACK REPORT

UNC4034 slips in a backdoor with trojanized PuTTY

Date of Publication	Admiralty Code	TA Number
September 19, 2022	A1	TA2022207

Summary

UNC4034, a North Korean threat actor, uses a fake job posting to trick victims into downloading a trojanized version of PuTTY. When the malicious PuTTY binary is executed on the host, a backdoor named AIRDRY is deployed, which establishes connections to the attacker's C2 server.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**T1566** Phishing	**T1566.001** Spearphishing Attachment	**T1566.003** Spearphishing via Service
TA0002 Execution	**T1059** Command and Scripting Interpreter	**T1059.003** Windows Command Shell	**T1053** Scheduled Task/Job
T1053.005 Scheduled Task/Job: Scheduled Task	**TA0003** Persistence	**T1574** Hijack Execution Flow	**T1574.001** DLL Search Order Hijacking
TA0005 Defense Evasion	**T1574** Process Injection	**T1574.001** Dynamic-link Library Injection	**T1218** System Binary Proxy Execution
T1620 Reflective Code Loading	**T1027** Obfuscated Files or Information	**T1027.002** Software Packing	**TA0011** Command and Control
T1071 Application Layer Protocol	**T1071.001** Web Protocols	**T1071.002** File Transfer Protocols	**T1132** Data Encoding
T1132.001 Standard Encoding	**T1573** Encrypted Channel	**T1573.002** Asymmetric Cryptography	**T1573.001** Symmetric Cryptography

Technical Details

#1

An attacker approaches their targets by email with a lucrative job offer from Amazon, then communicates with them via WhatsApp, sharing an ISO file ("amazon_assessment.iso"). As part of the ISO, there is a text file ("readme.txt") containing an IP address and login credentials, as well as a trojanized version of PuTTY (PuTTY.exe), one of the most popular SSH console applications.

#2

A malicious payload was included in the tampered PuTTY version, making the tampered version significantly larger than the legitimate one. The PuTTY executable was compiled from the legitimate program, so it is fully functional and appears exactly like the legitimate program.

#3

The hackers modified PuTTY's connect_to_host() function so that when the program is successfully connected to the host using the enclosed credentials, a DLL ("colorui.dll") with the DAVESHELL shellcode is deployed. In order to hide the shellcode launch, the malicious PuTTY uses a search order hijacking vulnerability in colorcpl.exe, the legitimate Windows Color Management tool. It drops the final payload, the AIRDRY.V2 backdoor malware, directly into memory.

#4

An AIRDRY.V2 instance can communicate via HTTP, file, or SMB over a named pipe, trying each hard-coded C2 address five times before going to sleep after 60 seconds.

Indicator of Compromise (IOC)

TYPE	VALUE
MD5	90adcfdaead2fda42b9353d44f7a8ceb 6d1a88fefd03f20d4180414e199eb23a 8368bb5c714202b27d7c493c9c0306d7 18c873c498f5b90025a3c33b17031223 c650b716f9eb0bd6b92b0784719081cd 4914bcbbe36dfa9d718d02f162de3da1
SHA256	8cc60b628bded497b11dbc04facc7b5d7160294cbe521764df1a9c cb219bba6b e03da0530a961a784fbba93154e9258776160e1394555d0752ac7 87f0182d3c0 1492fa04475b89484b5b0a02e6ba3e52544c264c294b57210404b 96b65e63266 cf22964951352c62d553b228cf4d2d9efe1ccb51729418c45dc488 01d36f69b4 aaad412aeb0f98c2c27bb817682f08673902a48b65213091534f96 fe6f5494d9 3ac82652cf969a890345db1862deff4ea8885fe72fb987904c0283a 2d5e6aac4
IPV4	137.184.15[.]189
URLs	https://hurricanepub[.]com/include/include.php https://turnscor[.]com/wp-includes/contacts.php https://www.elite4print[.]com/support/support.asp
File Path	C:\ProgramData\PackageColor\colorcpl.exe C:\ProgramData\PackageColor\colorui.dll

References

https://www.mandiant.com/resources/blog/dprk-whatsapp-phishing

What Next?

Book a free demo with **HivePro Uni5** to check your exposure to this advisory. HivePro Uni5 is a Continuous 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

September 19, 2022 . 7:00 AM

© 2022 All Rights are Reserved by HivePro

More at www.hivepro.com