Ransomware: New exploit tool used in targeted attacks

Newly discovered tool exploits recently patched Windows privilege escalation vulnerability (CVE-2022-24521).

Summary

At least one ransomware group is using a new tool that exploits a recently patched Windows privilege escalation vulnerability. The vulnerability (CVE-2022-24521) was reported to Microsoft by the U.S. National Security Agency (NSA) and CrowdStrike, and was patched on April 12, 2022.

While the vulnerability was reportedly being exploited as a zero-day prior to patching, the first evidence of this exploit tool's use dates from late April.

The tool was used in attacks against a number of organizations in the healthcare, manufacturing, and education sectors. The pattern of malicious activity suggested ransomware attacks in preparation, with the attackers also deploying tools such as Cobalt Strike, AdFind, PC Hunter, and AD Explorer.

While the ransomware payload is unconfirmed, there is some evidence linking these attacks to older attacks involving Conti ransomware. The new exploit tool was used with exploit tools for an older elevation of privilege vulnerability, CVE-2020-0787. This was used in a number of Conti attacks in 2021 and may be the same as the SOURBITS exploit tool documented by Mandiant.

Targets

Targets include organizations in the following sectors:

- Healthcare
- Education
- Manufacturing

Tools

- CVE-2022-24521 exploit tool
- CVE-2020-0787 exploit tools
- Cobalt Strike
- PC Hunter
- AdFind
- AD Explorer
- PsExec

For IOCs, see next page.

Indicators of Compromise (IOCs):

SOC analysts should review this alert and hunt on their network for associated indicators of compromise (IOCs). Their presence may indicate a ransomware attack in preparation. If an IOC is malicious and the file available to us, Symantec Endpoint products will detect and block that file. If you discover any other unknown or unavailable files while hunting, you can submit them to Symantec for analysis. Symantec products will detect and alert against the behaviors and techniques detailed in this alert.

f94998b90a28c678e4ed6bdf851f339e02a58369435b20ad62858e0ea5bc8eba	CVE-2022-24521 exploit tool (Hacktool)
8dc79c12fe1e8aefb870049c16fd1d62051207310702b99428cd73987e299ca3	CVE-2022-24521 exploit tool (Hacktool)
ff5e7e7c8a82b92328376ef23ff0a2c6506c0876702a3dd9869878f886567741	CVE-2020-0787 exploit tool (Trojan Horse)
268a7f6e76f69abf56ec3899ea3ecacada45d4ce454a6d8fe93f6aff9c1d4327	CVE-2020-0787 exploit tool (Trojan Horse)
4096fbd1b0462e9a3c59b143778d202878b4e5473f45bf3fdbb119f3827dfea1	CVE-2020-0787 exploit tool (Heur.AdvML.B)
b3af3e97b503df85ee940044eb64ad482698bde256feee054d97879eac53780b	File executor (Heur.AdvML.B)
8b8af7040e2805fea7124f4a0dfc2d62484b16ab3db91152c57a346b94e3eb3e	File executor (Heur.AdvML.B)
51ddba2bfdccb9ae4e640ae2fa67594e51cc4303a2e8cefe5afde33cc2a37976	File executor (Heur.AdvML.B)
4d776151e8d82d56b92e4524f1af172c234b7bbfee19563b05fcebb4714ff38c	Cobalt Strike (Backdoor.Cobalt)
b7489d8d7416a2fe7aba34ffdca3a1a4eb20c829dea508df7c9d64de38747383	Cobalt Strike (Backdoor.Cobalt)
379408333035d7398792299e2748966458ccc795205c5621fc9b1d8527daffd4	Suspected Cobalt Strike
2b214bddaab130c274de6204af6dba5aeec7433da99aa950022fa306421a6d32	PC Hunter
32726fa33be861472d0b26286073b49500e3fd3bd1395f63bc114746a9195efb	PC Hunter
6dd21148f4e915174a2c65cd20fb83ddd75462d3f3f594e2a330cd85748154fd	AD Explorer
b1102ed4bca6dae6f2f498ade2f73f76af527fa803f0e0b46e100d4cf5150682	AdFind
3337e3875b05e0bfba69ab926532e3f179e8cfbf162ebb60ce58a0281437a7ef	PsExec
hxxp://burmesebleaker[.]com/templates?profiler=false	Cobalt Strike C&C
hxxps://www[.]molekraftness[.]com	Cobalt Strike C&C
hxxps://local[.]molekraftness[.]com	Cobalt Strike C&C
146.70.41[.]149	Cobalt Strike C&C
54.39.83[.]137	Suspected Cobalt Strike C&C