BLACKSWAN
CYBERSECURITY

THREAT ADVISORY

June 22, 2023

RDStealer Malware Targeting Remote Desktops

SUMMARY

Bitdefender researchers published a warning related to new malware that is actively targeting the remote desktop protocol in an effort to steal client data.

The Bitdefender warning comes after the malware's first appearance as part of a cyber espionage operation called RedClouds, which targeted an east Asian IT company. The malware, written in Golang, is called RDStealer and looks for RDP connections with client drive mapping enabled. It then infects connecting RDP clients with a Logutil backdoor and begins exfiltrating data. The RedClouds operation was active for more than a year with the end goal of compromising credentials and data exfiltration.

TECHNICAL DETAILS

The attack employs an evasion tactic of using Microsoft Windows folders that are likely to be excluded from scanning by security software, like System32 and Program Files, to store the Logutil backdoor payload. In addition, the sub-folder "C:Program FilesDellCommandUpdate," has also been observed, which is a legitimate folder containing the Dell application called Dell Command | Update.   Researchers at Bitdefender said all the machines infected over the course of the incident were Dell computers, suggesting that the threat actors deliberately chose this folder to hide the malicious activity. Threat actors also registered command-and-control (C2) domains such as "dell-a[.]ntp-update[.]com".

A server-side backdoor called RDStealer is the primary data harvester, which specializes in continuously gathering clipboard content and keystroke data from the host. In this case, however, RDStealer is also "monitoring incoming RDP [Remote Desktop Protocol] connections and compromising remote machines if client drive mapping is enabled".   When a new RDP client connection is detected, commands are issued by RDStealer to exfiltrate sensitive data, such as browsing history, credentials, and private keys from apps like mRemoteNG, KeePass, and Google Chrome. In addition, the connecting RDP clients are infected with another Golang-based custom malware known as Logutil to maintain a persistent foothold on the victim network using DLL side-loading techniques and facilitate command execution.

INDICATORS OF COMPROMISE (IOCs)

MD5

- e89cb63e1352a1c9f86e03e4c744b5cd
- f51e88b159b5661f0b83c3947f3e0b24
- 61ac19b0f812b10e7690109430cba4a5
- d80827879b2e15b18a9c0feaf5a3c859
- 1d6b37bd2dfc9d6b4a811f90f6f48dce
- 2af313bdd3c54d95303c14786a3ad58d
- d5cdeba19d1a31b5be424a82210e3417
- de9233ed6689f84286fe0b7da8bc89e9
- e7121980263c08d2a759df827f97ecae
- 78a7df158236edd372946347a156e5bc
- 2b1130775c44be96990b2916ba071f40

- 211ffebfbf679b713148c6dad94ec1df
- 3b8424499183af6f886f722d85353abf
- 5a5e02256c0a8b65b2db8a0f88887744
- 1325ad15712a875ff61de3bbb0eccebd
- dec5b1c097b8d547666f76b55c5d0fdc
- b7538226437cea21297b94f37d2c2813
- 6cf0007b0d487f899fbd05ffc3401211
- 3294710063ee0dc7d6dfffc4de337b68
- 003d6351a2a2a2835f2b64a999963ec1
- e89cb63e1352a1c9f86e03e4c744b5cd
- 20ef20fd88dc7a5e90908f1667c08d11
- f18eb7a820f75e51b619b14967c83bb2
- b7538226437cea21297b94f37d2c2813
- 43b238bf6829e6f1056749bebdc01dbe
- a83cdb7efbe7bbc4dafa1c11578e6372
- f14a812c6c377e52fb98f8d4c1ed0abd
- 2a421eec6784f1675585e9b428c1b68c
- 5c613c1f1f426d7b4630673966a125ba
- ea4cee8027df495c0da7b22e5a9d8457
- 32efbf302aaa2845d3a2b76a50840dc2
- 47a02b5f59bbc62b7f4be0f4ce7574cd
- 13f5490acf5f5fab2f43f71999563bb9
- 9fc12edb2e5f193ed4ae365a57c47ffb

File Paths

- %SYSTEM32%\wbem\ncobjapi.dll
- %SYSTEM32%\wbem\ncobjapi.dll
- vcruntime140.dll
- %PROGRAM_FILES%\dell\md storage software\mdconfiguration utility\modular disk service daemon.exe
- %SYSTEM32%\wbem\lzsrv64.dll
- %SYSTEM32%\mcpbroker.dll
- %SYSTEM32%\wbem\efsmgr32.dll
- %SYSTEM32%\wbem\secure64.dll
- %SYSTEM32%\splsys64.dll

- %SYSTEM32%\mcpbroker.dll
- %SYSTEM32%\bithostw.dll
- %SYSTEM32%\bithosts.dll
- %SYSTEM32%\efsmgr32.dll
- %SYSTEM32%\efsmgr32.dll
- %SYSTEM32%\lzsrv64.dll
- %SYSTEM32%\splsys64.dll
- %SYSTEM32%\efsmgr32.dll
- wspack.dll • %SYSTEM32%\bithostw.dll
- %SYSTEM32%\wbem\bithosts.dll
- %WINDOWS%\temp\__deleted.dat
- %PROGRAM_FILES%\f-secure\psb\diagnostics\fs_ui.exe
- %PROGRAM_FILES%\f-secure\psb\diagnostics\fs_ui.exe
- %PROGRAM_FILES_x86%\dell\commandupdate\wbemwork.dll
- %WINDOWS%\temp\__to_be_deleted.dat
- %SYSTEM32%\bithostw.dll
- %SYSTEM32%\winrpc32.dll
- %PROGRAM_FILES_x86%\dell\commandupdate\wbemwork2.dll
- %PROGRAM_FILES_x86%\dell\commandupdate\dellcommandservice.exe
- %SYSTEM32%\msvcp150.dll
- %SYSTEM32%\edbr.dat • %PROGRAM_FILES_x86%\dell\commandupdate\dellcommandupdate.exe
- %PROGRAM_FILES_x86%\dell\commandupdate\msvcp140.dll
- ea4cee8027df495c0da7b22e5a9d8457 %SYSTEM32%\msvcp150.dll
- %WINDOWS%\security\database\msvcp150.dll
- %WINDOWS%\security\database\msprotect.dll
- %WINDOWS%\security\database\edbt.dat Domains
- a-ad-tml[.]ntp-update[.]com • rps-a[.]ntp-update[.]com
- a-rps[.]ntp-update[.]com • dns-a[.]ntp-update[.]com
- a-tb[.]ntp-update[.]com • alast[.]sun-java[.]com
- alast[.]ntp-update[.]com • dell-a[.]ntp-update[.]com
- a-sp-rps[.]0g6666[.]com • og8888[.]0g6666[.]com
- windows[.]javaupdate-cdn[.]com
- adobe[.]javaupdate-cdn[.]com
- flash[.]javaupdate-cdn[.]com

- linux[.]0g6666[.]com
- ad[.]ntp-update[.]com
- linux[.]ntp-update[.]com
- windows[.]0g6666[.]com
- www[.]0g6666[.]com
- wt[.]ntp-update[.]com
- aliyun[.]ntp-update[.]com
- cloud[.]ntp-update[.]com
- fe[.]ntp-update[.]com
- wtech[.]ntp-update[.]com
- imp[.]ntp-update[.]com
- ogplus[.]ntp-update[.]com
- organization[.]0g6666[.]com
- global[.]ntp-update[.]com
- kaiy[.]0g6666[.]com
- kaiy[.]ntp-update[.]com
- ky[.]0g6666[.]com
- oriental[.]ntp-update[.]com
- guard[.]ntp-update[.]com
- oglive[.]ntp-update[.]com
- guard[.]0g6666[.]com
- plus[.]ntp-update[.]com
- oglty[.]0g6666[.]com
- oglty[.]ntp-update[.]com
- oglty-ml[.]ntp-update[.]com
- esxi-lty[.]ntp-update[.]com
- ml-lty[.]ntp-update[.]com
- telegram[.]ntp-update[.]com
- easyh[.]ntp-update[.]com
- weblog[.]ntp-update[.]com
- weblog-ml[.]ntp-update[.]com
- o-fsh[.]ntp-update[.]com
- idn-tb[.]ntp-update[.]com
- tb-ndi2[.]ntp-update[.]com

- ml-ndi[.]ntp-update[.]com
- vct[.]0g6666[.]com
- windows-i-tb[.]ntp-update[.]com
- ubuntu-ndi[.]ntp-update[.]com
- windows-qc-tb-i[.]ntp-update[.]com
- windows-tb-i[.]ntp-update[.]com
- a-fms[.]ntp-update[.]com
- plus[.]0g6666[.]com
- aprotect[.]sun-java[.]com

IP Addresses

- 34.96.222[.]22
- 35.220.144[.]179
- 35.220.202[.]191
- 34.96.235[.]162
- 35.220.190[.]145
- 35.220.183[.]209
- 35.208.179[.]162
- 34.92.13[.]119

RECOMMENDATIONS

- Minimize your exposed attack surfaces.
- Utilize tools and technologies that provide behavioral and anomaly detection.

REFERENCES

- https://www.bleepingcomputer.com/news/security/new-rdstealer-malware-steals-from-drives-shared-over-remote-desktop/
- https://www.bitdefender.com/files/News/CaseStudies/study/431/Bitdefender-Labs-Report-X-creat6958-en-EN.pdf
- https://www.itpro.com/security/malware/researchers-uncover-novel-rdstealer-malware-targeting-remote-desktop-protocol
- https://siliconangle.com/2023/06/20/bitdefender-warns-new-exfiltration-malware-targeting-rdp-workloads/
- https://thehackernews.com/2023/06/experts-uncover-year-long-cyber-attack.htm