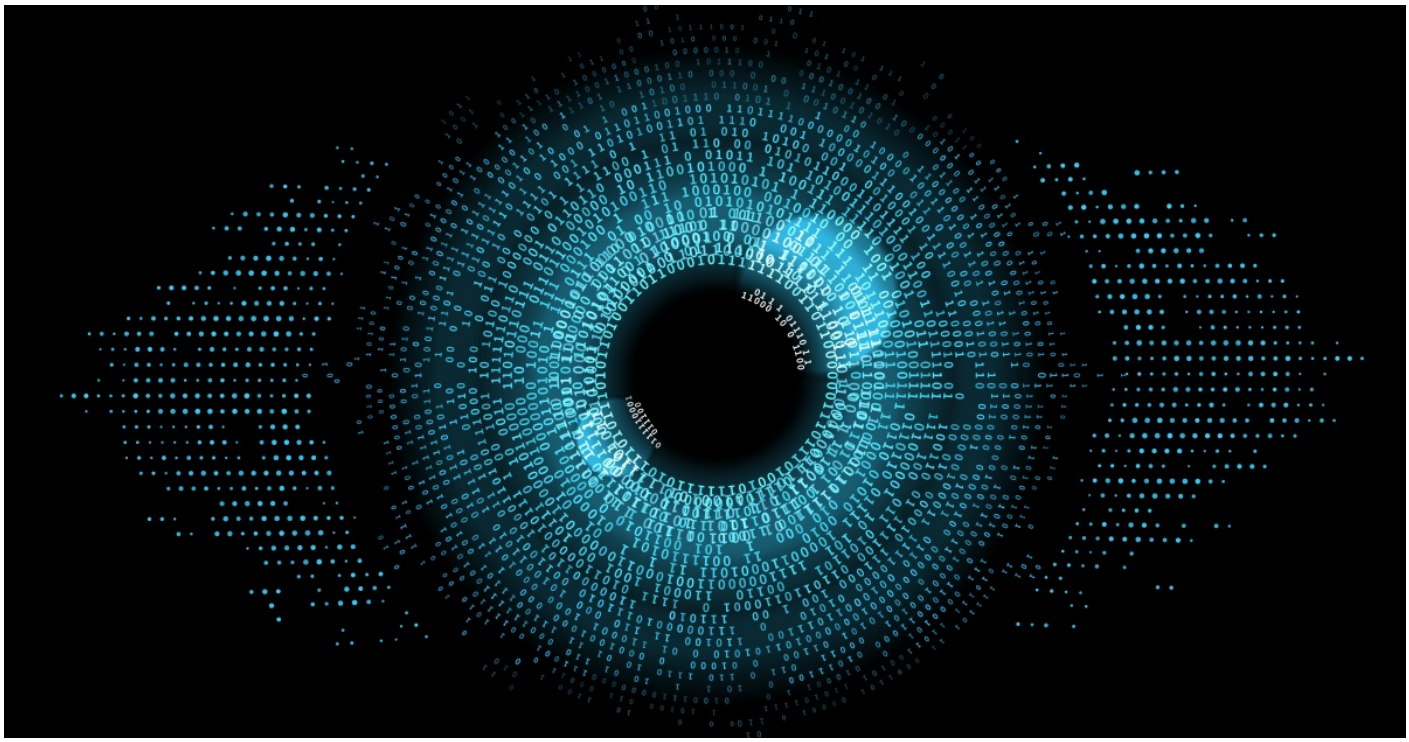
Budworm: Espionage Group Returns to Targeting U.S. Organizations



The Budworm espionage group has mounted attacks over the past six months against a number of strategically significant targets, including the government of a Middle Eastern country, a multinational electronics manufacturer, and a U.S. state legislature. The latter attack is the first time in a number of years Symantec has seen Budworm targeting a U.S-based entity. Along with the above high-value targets, the group also conducted an attack against a hospital in South East Asia.

Current toolset

In recent attacks, Budworm leveraged the Log4j vulnerabilities (CVE-2021-44228 and CVE-2021-45105) to compromise the Apache Tomcat service on servers in order to install web shells. The attackers used Virtual Private Servers (VPS) hosted on Vultr and Telstra as command-and-control (C&C) servers.

Budworm's main payload continues to be the HyperBro malware family, which is often loaded using a technique known as dynamic-link library (DLL) side-loading. This involves the attackers placing a malicious DLL in a directory where a legitimate DLL is expected to be found. The attacker then runs the legitimate application (having installed it themselves). The legitimate application then loads and executes the payload.

In recent attacks, Budworm has used the endpoint privilege management software CyberArk Viewfinity to perform side-loading. The binary, which has the default name vf_host.exe, is usually renamed by the

attackers in order to masquerade as a more innocuous file. Masqueraded names included securityhealthservice.exe, secu.exe, vfhost.exe, vxhost.exe, vx.exe, and v.exe.

In some cases, the HyperBro backdoor was loaded with its own HyperBro loader (file names: peloader.exe, 12.exe). It is designed to load malicious DLLs and encrypt payloads.

While HyperBro was frequently used, the attackers also used the PlugX/Korplug Trojan as a payload at times.

Other tools used in recent attacks include:

- Cobalt Strike: An off-the-shelf tool that can be used to load shellcode onto victim machines. It has legitimate uses as a penetration testing tool but is frequently exploited by malicious actors.
- LaZagne: A publicly available credential dumping tool.
- IOX: A publicly available proxy and port-forwarding tool.
- Fast Reverse Proxy (FRP): A reverse proxy tool.
- Fscan: A publicly available intranet scanning tool.

Conclusion

Budworm is known for mounting ambitious attacks against high-value targets. While there were frequent reports of Budworm targeting U.S. organizations six to eight years ago, in more recent years the group's activity appears to have been largely focused on Asia, the Middle East, and Europe. However this is the second time in recent months, Budworm has been linked to attacks against a U.S-based target. A recent CISA report on multiple APT groups attacking a defense sector organization mentioned Budworm's toolset. A resumption of attacks against U.S.-based targets could signal a change in focus for the group.

Protection/Mitigation

For the latest protection updates, please visit the Symantec Protection Bulletin.

Indicators of Compromise

If an IOC is malicious and the file available to us, Symantec Endpoint products will detect and block that file.

5aecbb6c073b0cf1ad1c6803fa1bfaa6eca2ec4311e165f25d5f7f0b3fe001db — Credential Dumper

779ae012ede492b321fd86df70f7c9da94251440ebe5ec3efee84a432f432478 — FSCAN

ab949af896b6a6d986aed6096c36c4f323f650ccccfc7ea49004ba919d1bfa46 — HyperBro launcher

bebce37572ea2856663383215a013f8115c1f81da0f2bf1233c959955c494032 — HyperBro launcher

6e493ce8dccabf172d818453cc9d4e5bf4b1969ff9690c51b8cb538346e8e00e — HyperBro launcher

8b2e7924f5038473736705b5c3dc3efa918fb7ffe2cc19ce48e4554658d33fe6 — HyperBro launcher

cda8f76ce72759324e11c8af17736d685ca95954c0a09a682834b92a033bb11a — HyperBro launcher

25da610be6acecfd71bbe3a4e88c09f31ad07bdd252eb30feeef9debd9667c51 — HyperBro launcher

90eb92db757dc1ab4ca55b18b604350ecd84b7cd1d9a2555d789432f8c9a430b — HyperBro launcher

6398876f73cd0157a7681de4b2326a0a313dc7f9cb2bee3001894137da41c1f0 — HyperBro launcher

c53b6a2ec48647121a3e8816636b34ee2cdd6846d6d05efd9539d17a1c021da0 — HyperBro launcher

c3213937c194246d29dd5fb39d8e7ef3671df58e3f01353784a06a075f21cfc5 — HyperBro launcher

386c9079d65bdd7e3f7b8872024a80992b5d5c6a3c8b971c47d1ef439b9e2671 — HyperBro loader

bfffc43d948d1787622bcde524e51c932a2a1fdc761539f60e777e21ef16e83d — HyperBro loader

018d3a957aa0eaa7a621b52d15f4a1ed18b0f81c477e6023cd80313d83f7dbc0 — HyperBro loader

d4776939dcf78f5f7491b9938480423956ac10a3c576028dec307511c586a124 — HyperBro loader

27c2a9608ce80a443c87a0a2947864df7d4491cfa85608c6a6b6680ec0277f9d — HyperBro loader

42b603fffd4766fa22f6e10884e7fa43f449d515cfa20a18f0d07a6d4c370962 — IOX

0d46907320ab55d98966389f41441aa0341a7db829cd166748d8929d466c9fba — IOX

714d0101039bfd7d3db4dfe8307bc1657b7266ff2528b5e852b752879ebe7113 — IOX

0129c9c7b55a6f514a9fa8c38ce59d8939efda6ece67b90c6be13aec40f1bdab — Viewfinity side-load

df847abbfac55fb23715cde02ab52cbe59f14076f9e4bd15edbe28dcecb2a348 — Viewfinity side-load

620e401b2b7727a6c7ebc37ee1f7d8e1742d7121c1f4ea350a43d460ef9bdc4c — Viewfinity side-load

c8aea84abb476ab536198a36df53b37be3d987a9ce58cb06e93cac7d2bfb3703 — Viewfinity side-load

233bb85dbeba6923153340850169769 5a66b7790e751925231d64bddf80bbf91 — Cobalt Strike

d610547c718fcca7c5c7e02c6821e9909333daf6376a1096edf21f9355754f29 — FRP

5c2d05bfc9b6d4fc7aea32312c62180564fac9f65b0867e824d81051e5fc34fd — Korplug

ed2f501408a7a6e1a854c29c4b0bc5648a6aa8612432df829008931b3e34bf56 — Lazagne

61deb3a206cc203252418b431f6556e3f7efd9556fc685eeda7281d9baf89851 — Lazagne

892663bb4f3080c3f2f1915734897cab1c9ee955a77bb8541b417ec2b03cd4ef — Lazagne

3d7dc77ded4022a92a32db9e10dbc67fbcc80854a281c3cc0f00b6cbd2bfd112 — Trojan Horse

48e81b1c5cc0005cc58b99cefe1b6087c841e952bb06db5a5a6441e92e40bed6 — Trojan.Dropper

5cba27d29c89caf0c8a8d28b42a8f977f86c92c803d1e2c7386d60c0d8641285 — Trojan.Dropper

139.180.146[.]101 — C&C VPS

45.77.46[.]54 — C&C VPS

139.168.200[.].123 — C&C VPS

207.148.76[.]235 — C&C VPS

setting.101888gg[.]com/jquery-3.3.1.min.js — C&C

207.148.76[.]235/jquery-3.3.1.min.js — C&C