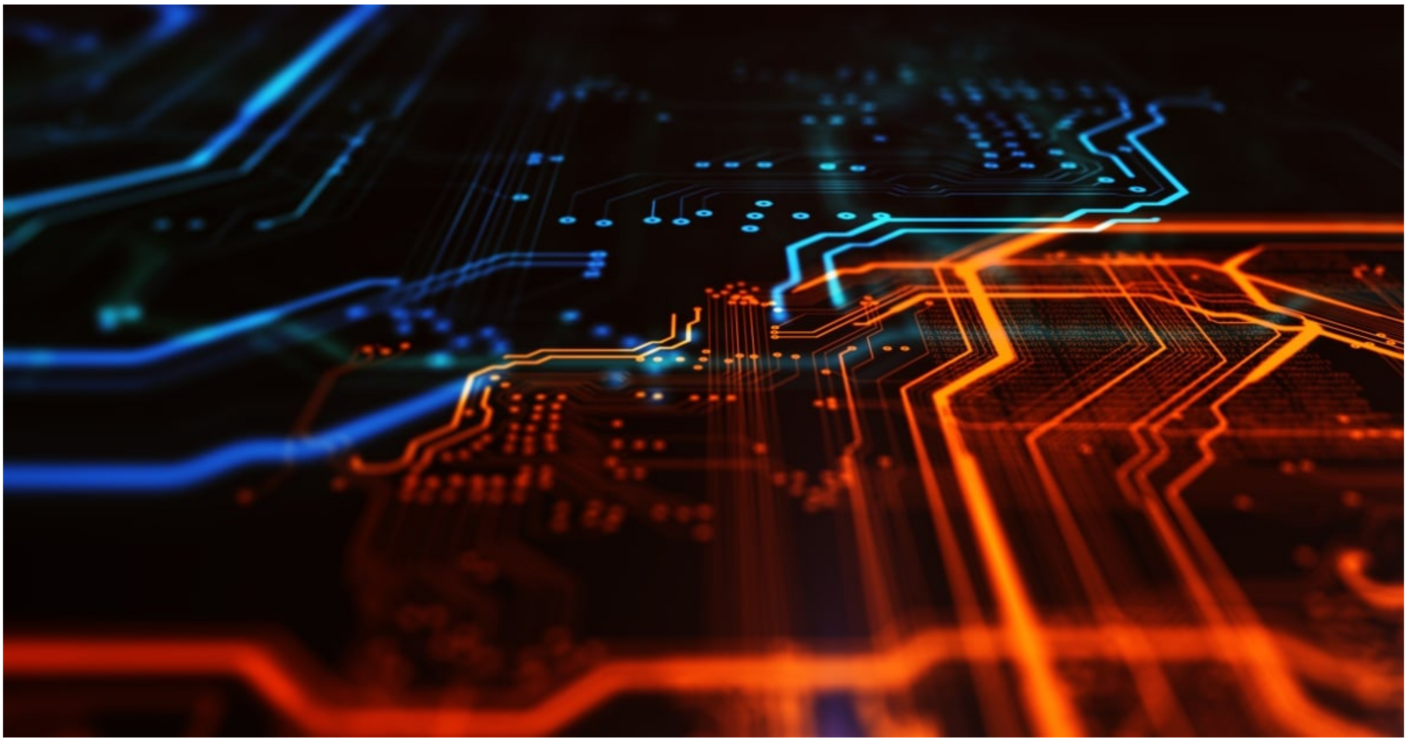
Budworm: APT Group Uses Updated Custom Tool in Attacks on Government and Telecoms Org



The Budworm advanced persistent threat (APT) group continues to actively develop its toolset. Most recently, the Threat Hunter Team in Symantec, part of Broadcom, discovered Budworm using an updated version of one of its key tools to target a Middle Eastern telecommunications organization and an Asian government.

Both attacks occurred in August 2023. Budworm (aka LuckyMouse, Emissary Panda, APT27) deployed a previously unseen variant of its SysUpdate backdoor (SysUpdate DLL inicore_v2.3.30.dll). SysUpdate is exclusively used by Budworm.

As well as its custom malware, Budworm also used a variety of living-off-the-land and publicly available tools in these attacks. It appears the activity by the group may have been stopped early in the attack chain as the only malicious activity seen on infected machines is credential harvesting.

Tools Used

Budworm executes SysUpdate on victim networks by DLL sideloading the payload using the legitimate INISafeWebSSO application. This technique has been used by the group for some time, with reports of INISafeWebSSO being leveraged dating as far back as 2018. DLL sideloading attacks use the DLL search order mechanism in Windows to plant and then invoke a legitimate application that executes a malicious payload. It can help attackers evade detection.

SysUpdate is a feature-rich backdoor that has multiple capabilities, including:

- List, start, stop, and delete services
- Take screenshots
- Browse and terminate processes
- Drive information retrieval
- File management (finds, deletes, renames, uploads, downloads files, and browses a directory)
- Command execution

Trend Micro reported in March 2023 that Budworm had developed a Linux version of SysUpdate with similar capabilities to the Windows version. SysUpdate has been in use by Budworm since at least 2020, and the attackers appear to continually develop the tool to improve its capabilities and avoid detection.

As well as SysUpdate, the attackers used a number of legitimate or publicly available tools to map the network and dump credentials. Tools used by the attackers in this campaign included:

- **AdFind:** A publicly available tool that is used to query Active Directory. It has legitimate uses but is widely used by attackers to help map a network.
- **Curl:** An open-source command-line tool for transferring data using various network protocols.
- **SecretsDump:** A publicly available tool that can perform various techniques to dump secrets from the remote machine without executing any agent. Techniques include reading SAM and LSA secrets from registries, dumping NTLM hashes, plaintext credentials, and Kerberos keys, as well as dumping the NTDS.dit Active Directory database.
- **PasswordDumper:** A password-dumping tool.

Budworm Background

Budworm is a long-running APT group that is believed to have been active since at least 2013. The attackers are known for their targeting of high-value victims, often focusing on organizations in the government, technology, and defense sectors. Budworm has targeted victims in many countries in Southeast Asia and the Middle East, among other locations, including the U.S. Symantec's Threat Hunter Team published a blog in October 2022 detailing how Budworm activity was seen on the network of a U.S. state legislature. In that campaign, the attackers also targeted the government of a Middle Eastern country, a multinational electronics manufacturer, and a hospital in Southeast Asia. The attackers also leveraged DLL sideloading in that campaign to load their HyperBro malware.

The victims in this campaign — a government in Asia and a telecommunications company in the Middle East — do align with the kinds of victims we often see Budworm targeting. The targeting of a telecommunications company and government also point to the motivation behind the campaign being intelligence gathering, which is the motivation that generally drives Budworm activity.

That Budworm continues to use a known malware (SysUpdate), alongside techniques it is known to favor, such as DLL sideloading using an application it has used for this purpose before, indicate that the group isn't too concerned about having this activity associated with it if it is discovered.

The use of a previously unseen version of the SysUpdate tool also demonstrates that the group is continuing to actively develop its toolset. The fact that this activity occurred as recently as August 2023 suggests that the group is currently active, and that those organizations that may be of interest to Budworm should be aware of this activity and the group’s current toolset.

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.

SHA256 file hashes

c501203ff3335fbfc258b2729a72e82638719f60f7e6361fc1ca3c8560365a0e — Legitimate INISafeWebSSO application

c4f7ec0c03bcacaaa8864b715eb617d5a86b5b3ca6ee1e69ac766773c4eb00e6 — SysUpdate backdoor

551397b680da0573a85423fbb0bd10dac017f061a73f2b8ebc11084c1b364466 — Password dumper

df571c233c3c10462f4d88469bababe4c57c21a52cca80f2b1e1af848a2b4d23 — Hacktool

c3405d9c9d593d75d773c0615254e69d0362954384058ee970a3ec0944519c37 — SecretsDump

f157090fd3ccd4220298c06ce8734361b724d80459592b10ac632acc624f455e — AdFind

ee9dfcea61282b4c662085418c7ad63a0cbbeb3a057b6c9f794bb32455c3a79e — Curl