ESET uncovers new Linux backdoor from SparklingGoblin APT group, targeting a Hong Kong university again

DUBAI, DUBAI, UNITED ARAB EMIRATES, September 21, 2022 /EINPresswire.com/ -- ESET researchers have discovered a Linux variant of the SideWalk backdoor, one of the multiple custom implants used by the SparklingGoblin APT group. This variant was first deployed against a Hong Kong university in February 2021 — the same university that had already been targeted by SparklingGoblin during the student protests in May 2020. SparklingGoblin is an APT group with targets mostly in East and Southeast Asia, though ESET Research has seen SparklingGoblin targeting a broad range of organizations and verticals around the world, with a particular focus on the academic sector.

“The SideWalk backdoor is exclusive to SparklingGoblin. In addition to the multiple code similarities between the Linux variants of SideWalk and various SparklingGoblin tools, one of the SideWalk Linux samples uses a C&C address that was previously used by SparklingGoblin. Considering all of these factors, we attribute with high confidence SideWalk Linux to the SparklingGoblin APT group,” explains Vladislav Hrčka, an ESET researcher who made the discovery along with Thibault Passilly and Mathieu Tartare.

SparklingGoblin first compromised the particular Hong Kong university in May 2020, and we first detected the Linux variant of SideWalk in that university’s network in February 2021. The group continuously targeted this organization over a long period of time, successfully compromising multiple servers, including a print server, an email server, and a server used to manage student schedules and course registrations. This time, it is a Linux variant of the original backdoor. This Linux version exhibits several similarities with its Windows counterpart, along with some technical novelties.

One particularity with SideWalk is the use of multiple threads to execute a single specific task.

We noticed that in both variants there are exactly five threads executed simultaneously, with each of them having a specific task. Four commands are not implemented or are implemented differently in the Linux variant. “Considering the numerous code overlaps between the samples, we believe that we actually found a Linux variant of SideWalk, which we dubbed SideWalk Linux. The similarities include the same customized ChaCha20, software architecture, configuration, and dead-drop resolver implementation,” says Hrčka.

“The Windows variant of SideWalk goes to great lengths to conceal the objectives of its code. It trimmed out all data and code that was unnecessary for its execution and encrypted the rest. On the other hand, the Linux variants contain symbols and leave some unique authentication keys and other artifacts unencrypted, which makes the detection and analysis significantly easier,” concludes Hrčka.

For more technical information about SideWalk Linux, check out the blog post “You never walk alone: SideWalk backdoor gets a Linux variant” on WeLiveSecurity. Make sure to follow ESET Research on Twitter for the latest news from ESET Research.

About ESET
For more than 30 years, ESET® has been developing industry-leading IT security software and services to protect businesses, critical infrastructure and consumers worldwide from increasingly sophisticated digital threats. From endpoint and mobile security to endpoint detection and response, as well as encryption and multifactor authentication, ESET’s high-performing, easy-to-use solutions unobtrusively protect and monitor 24/7, updating defenses in real time to keep users safe and businesses running without interruption. Evolving threats require an evolving IT security company that enables the safe use of technology. This is backed by ESET’s R&D centers worldwide, working in support of our shared future. For more information, visit www.eset.com or follow us on LinkedIn, Facebook, and Twitter.

Sanjeev Kant
Vistar Communications
+971 55 972 4623
email us here
