ESET discovers WinorDLL64 backdoor, likely part of the Lazarus arsenal

DUBAI, UNITED ARAB EMIRATES, February 28, 2023 /EINPresswire.com/ -- ESET researchers have discovered the WinorDLL64 backdoor, one of the payloads of the Wslink downloader. The targeted region, and overlap in behavior and code, suggest the tool is used by the infamous North Korea-aligned APT group Lazarus. Wslink's payload can exfiltrate, overwrite, and remove files, execute commands, and obtain extensive information about the underlying system.

"Wslink, which has the filename WinorLoaderDLL64.dll, is a loader for Windows binaries that, unlike other such loaders, runs as a server and executes received modules in memory. As the wording suggests, a loader serves as a tool to load a payload, or the actual malware, onto the already compromised system," explains Vladislav Hrčka, the ESET researcher who made the discovery. "The Wslink payload can be leveraged later for lateral movement, due to its specific interest in network sessions. The Wslink loader listens on a port specified in the configuration and can serve additional connecting clients, and even load various payloads," he adds.

WinorDLL64 contains overlaps in both behavior and code with several Lazarus samples, which indicates that it might be a tool from the vast arsenal of this North Korea-aligned APT group.

The initially unknown Wslink payload was uploaded to VirusTotal from South Korea shortly after the publication of an ESET Research blog post on the Wslink loader. ESET telemetry has seen only a few detections of the Wslink loader in Central Europe, North America, and the Middle East. Researchers from AhnLab confirmed South Korean victims of Wslink in their telemetry, which is a relevant indicator, considering the traditional Lazarus targets and that ESET Research observed only a few detections.

Active since at least 2009, this infamous North Korea-aligned group is responsible for high-

profile incidents such as the Sony Pictures Entertainment hack, the tens-of-millions-of-dollars cyberheists in 2016, the WannaCryptor (aka WannaCry) outbreak in 2017, and a long history of disruptive attacks against South Korean public and critical infrastructure since at least 2011. US-CERT and the FBI call this group HIDDEN COBRA.

For more technical information about WinorDLL64, check out the blog post “WinorDLL64: A backdoor from the vast Lazarus arsenal?” 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, or Twitter.

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