ESET Research discovers new Lazarus DreamJob campaign and links it to phone provider 3CX supply-chain attack

DUBAI, UNITED ARAB EMIRATES, May 9, 2023 /EINPresswire.com/ -- ESET researchers have discovered a new Lazarus Operation DreamJob campaign targeting Linux users. ESET Research was able to reconstruct the full chain, from the ZIP file that delivers a fake HSBC job offer as a decoy up until the final payload: the SimplexTea Linux backdoor distributed through an OpenDrive cloud storage account. It is the first time for this major North Korea–aligned threat actor to be using Linux malware as part of this operation. Similarities with this newly discovered Linux malware corroborate the theory that the infamous North Korea–aligned group is behind the 3CX supply-chain attack.

“This latest discovery provides corroborating evidence and reinforces our high level of confidence that the recent 3CX supply-chain attack was in fact conducted by Lazarus – a link that was suspected from the very beginning and demonstrated by several security researchers since,” says ESET researcher Peter Kálnai, who investigates Lazarus activities.

3CX is an international VoIP software developer and distributor that provides phone system services to many organizations. According to its website, 3CX has more than 600,000 customers and 12 million users in various sectors, including aerospace, healthcare, and hospitality. It provides client software to use its systems via a web browser, mobile app, or a desktop application. Late in March 2023, it was discovered that the desktop application for both Windows and macOS contained malicious code that enabled a group of attackers to download and run arbitrary code on all machines where the application was installed. 3CX itself was compromised and its software was used in a supply-chain attack driven by external threat actors to distribute additional malware to specific 3CX customers.

The perpetrators had planned the attacks long before execution – as early as December 2022. This suggests that they already had a foothold inside 3CX's network late last year. Several days before the attack was publicly revealed, a mysterious Linux downloader was submitted to VirusTotal. It downloads a new Lazarus backdoor for Linux, SimplexTea, which connects to the same Command & Control server as payloads involved in the 3CX compromise.

"This compromised software, deployed on various IT infrastructures, allows the download and execution of any kind of payload, which can have devastating impacts. The stealthiness of a supply-chain attack makes this method of distributing malware very appealing from an attacker's perspective, and Lazarus has already used this technique in the past," explains Kálnai. "It is also interesting to note that Lazarus can produce and use native malware for all major desktop operating systems: Windows, macOS, and Linux," adds Marc-Etienne M.Léveillé , ESET researcher who helped with the research.

Operation DreamJob is the name for a series of campaigns where Lazarus uses social engineering techniques to compromise its targets, with fake job offers as the lure. On March 20, a user in the country of Georgia submitted to VirusTotal a ZIP archive called HSBC job offer.pdf.zip. Given other DreamJob campaigns by Lazarus, this payload was probably distributed through spearphishing or direct messages on LinkedIn. The archive contains a single file: a native 64-bit Intel Linux binary written in Go and named HSBC job offer□pdf.

For more technical information about the latest Lazarus DreamJob campaign and links to the 3CX supply-chain attack, check out the blog post "Linux malware strengthens links between Lazarus and the 3CX supply-chain attack" 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
0559724623
email us here