ShadowPad: How Attackers hide Backdoor in Software used by Hundreds of Large Companies around the World

By Kaspersky

Published: 2017-08-15 · Archived: 2026-04-05 16:19:53 UTC

ShadowPad is one of the largest known supply-chain attacks. Had it not been detected and patched so quickly, it could potentially have targeted hundreds of organizations worldwide.

Kaspersky Lab experts have discovered a backdoor planted in a server management software product used by hundreds of large businesses around the world. When activated, the backdoor allows attackers to download further malicious modules or steal data. Kaspersky Lab has alerted NetSarang, the vendor of the affected software, and it has promptly removed the malicious code and released an update for customers.

ShadowPad is one of the largest known supply-chain attacks. Had it not been detected and patched so quickly, it could potentially have targeted hundreds of organizations worldwide.

In July, 2017 Kaspersky Lab's Global Research and Analysis (GReAT) team was approached by one of its partners – a financial institution. The organization's security specialists were worried about suspicious DNS (domain name server) requests originating on a system involved in the processing of financial transactions. Further investigation showed that the source of these requests was server management software produced by a legitimate company and used by hundreds of customers in industries like financial services, education, telecoms, manufacturing, energy, and transportation. The most worrying finding was the fact that the vendor did not mean for the software to make these requests.

Further Kaspersky Lab analysis showed that the suspicious requests were actually the result of the activity of a malicious module hidden inside a recent version of the legitimate software. Following the installation of an infected software update, the malicious module would start sending DNS-queries to specific domains (its command and control server) at a frequency of once every eight hours. The request would contain basic information about the victim system (user name, domain name, host name). If the attackers considered the system to be "interesting", the command server would reply and activate a fully-fledged backdoor platform that would silently deploy itself inside the attacked computer. After that, on command from the attackers, the backdoor platform would be able to download and execute further malicious code.

Following the discovery, Kaspersky Lab researchers immediately contacted NetSarang. The company reacted fast and released an updated version of the software without the malicious code.

So far, according to Kaspersky Lab research, the malicious module has been activated in Hong Kong, but it could be lying dormant on many other systems worldwide, especially if the users have not installed the updated version of the affected software.

While analyzing the tools, techniques and procedures used by the attackers, KL researchers came to the conclusion that some similarities exist that point to PlugX malware variants used by the Winnti APT, a known Chinese-speaking cyberespionage group. This information, however, is not enough to establish a precise connection to these actors.

"ShadowPad is an example of how dangerous and wide-scale a successful supply-chain attack can be. Given the opportunities for reach and data collection it gives to the attackers, most likely it will be reproduced again and again with some other widely used software component. Luckily NetSarang was fast to react to our notification and released a clean software update, most likely preventing hundreds of data stealing attacks against its clients. However, this case shows that large companies should rely on advanced solutions capable of monitoring network activity and detecting anomalies. This is where you can spot malicious activity even if the attackers were sophisticated enough to hide their malware inside legitimate software," said Igor Soumenkov, security expert, Global Research and Analysis Team, Kaspersky Lab.

NetSarang Statement

"To combat the ever-changing landscape of cyberattacks NetSarang has incorporated various methods and measures to prevent our line of products from being compromised, infected, or utilized by cyberespionage groups. Regretfully, the Build release of our full line of products on July 18th, 2017 was unknowingly shipped with a backdoor which had the potential to be exploited by its creator.

The security of our customers and user base is our highest priority and ultimately, our responsibility. The fact that malicious groups and entities are utilizing commercial and legitimate software for illicit gain is an ever-growing concern and one that NetSarang, as well as others in the computer software industry, is taking very seriously.

NetSarang is committed to its users' privacy and has incorporated a more robust system to ensure that never again will a compromised product be delivered to its users. NetSarang will continue to evaluate and improve our security not only to combat the efforts of cyber espionage groups around the world but also in order to regain the trust of its loyal user base."

All Kaspersky Lab products detect and protect against the ShadowPad malware as "Backdoor.Win32.ShadowPad.a".

Kaspersky Lab advises users to updateimmediately to the latest version of the NetSarang software, from which the malicious module has been removed, and to check their systems for signs of DNS queries to unusual domains. A list of the command server domains used by the malicious module can be found in the Securelist blogpost, which also includes further technical information on the backdoor.

About Kaspersky Lab

Kaspersky Lab is a global cybersecurity company celebrating its 20 year anniversary in 2017. Kaspersky Lab's deep threat intelligence and security expertise is constantly transforming into security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by

Kaspersky Lab technologies and we help 270,000 corporate clients protect what matters most to them. Learn more at www.kaspersky.com.

About NetSarang

NetSarang Computer, Inc. develops, markets and supports secure connectivity solution in the global market. The company develops a family of PC X server and SSH client software for PC-to-Unix and PC-to-Linux, and is expanding its TCP/IP network technologies to other Internet businesses. The company offers its products and services to more than 90 countries around the world.
