ESET Research: Tick cyberespionage group compromises data-loss prevention software developer in East Asia

DUBAI, DUBAI, UNITED ARAB EMIRATES, March 16, 2023 /EINPresswire.com/ -- ESET researchers have uncovered a compromise of an East Asian data-loss prevention (DLP) company. During the intrusion, the attackers deployed at least three malware families and compromised internal update servers and third-party tools used by the affected company. As a result, two customers of the company were subsequently compromised. ESET attributes the campaign with high confidence to the Tick APT group. Based on Tick's profile, the objective of the attack was most likely cyberespionage. The customer portfolio of the DLP company includes government and military entities, making the compromised company an especially attractive target for an APT group such as Tick.

"The attackers compromised the DLP company's internal update servers to deliver malware inside the software developer's network, and trojanized installers of legitimate third-party tools used by the company, which eventually resulted in the execution of malware on the computers of its customers," says ESET researcher Facundo Muñoz, who discovered Tick's latest operation. "During the intrusion, the attackers deployed a previously undocumented downloader, which we've named ShadowPy, and also deployed the Netboy backdoor (aka Invader) as well as the Ghostdown downloader," adds Muñoz.

The initial attack happened in March 2021, and ESET notified the company of the compromise. In 2022, ESET telemetry registered the execution of malicious code in the networks of two of the compromised company's customers. Since trojanized installers were transferred via remote support software, ESET Research hypothesizes that this took place while the DLP company was providing technical support. The attackers also compromised two internal update servers, which delivered malicious updates for the software developed by this DLP company on two occasions to machines inside the network of the DLP company.

The previously undocumented downloader ShadowPy was developed in Python and is loaded through a customized version of the open source project py2exe. ShadowPy contacts a remote server from where it receives new Python scripts that are decrypted and executed. The older Netboy backdoor supports 34 commands, including collecting system information, deleting a file downloading and executing programs, performing screen capture, and performing mouse and keyboard events requested by its controller.

Tick (also known as BRONZE BUTLER or REDBALDKNIGHT) is an APT group thought to have been active since at least 2006 and that mainly targets countries in the APAC region. This group is of interest for its cyberespionage operations, which focus on stealing classified information and intellectual property. Tick employs an exclusive custom malware toolset designed for persistent access to compromised machines, reconnaissance, data exfiltration, and download of tools.

For more technical information about the latest Tick campaign, check out the blogpost “The slow Tick-ing time bomb: Tick APT group compromise of a DLP software developer in East Asia” 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
email us here

This press release can be viewed online at: https://www.einpresswire.com/article/622579600

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2023 Newsmatics Inc. All Right Reserved.