DTrack: previously unknown spy-tool by Lazarus hits financial institutions and research centers

By Kaspersky

Published: 2019-09-23 · Archived: 2026-04-05 17:21:57 UTC

Woburn, MA – September 23, 2019 -Kaspersky Global Research and Analysis Team have discovered a previously unknown spy tool, which had been spotted in Indian financial institutions and research centers. Called Dtrack, this spyware reportedly was created by the Lazarus group and is being used to upload and download files to victims' systems, record key strokes and conduct other actions typical of a malicious remote administration tool (RAT).

In 2018, Kaspersky researchers discovered ATMDtrack – malware created to infiltrate Indian ATMs and steal customer card data. Following further investigation using the Kaspersky Attribution Engine and other tools, the researchers found more than 180 new malware samples that had code sequence similarities with the ATMDtrack, but at the same time were not aimed at ATMs. Instead, its list of functions defined it as spy tools, now known as Dtrack. Moreover, not only did the two strains share similarities with each other, but also with the 2013 DarkSeoul campaign, which was attributed to Lazarus – an infamous advanced persistence threat actor responsible for multiple cyberespionage and cyber sabotage operations.

Dtrack can be used as a RAT, giving threat actors complete control over infected devices. Criminals can then perform different operations, such as uploading and downloading files and executing key processes.

Entities targeted by threat actors using Dtrack RAT often have weak network security policies and password standards, while also failing to track traffic across the organization. If successfully implemented, the spyware is able to list all available files and running processes, key logging, browser history and host IP addresses, including information about available networks and active connections.

The newly discovered malware is active and based on Kaspersky telemetry, and is still used in cyberattacks.

"Lazarus is a rather unusual nation state sponsored group. On one hand, as many other similar groups do, it focuses on conducting cyberespionage or sabotage operations. Yet on the other hand, it has also been found to influence attacks that are clearly aimed at stealing money. The latter is quite unique for such a high profile threat actor because generally, other actors do not have financial motivations in their operations," said Konstantin Zykov security researcher, Kaspersky Global Research and Analysis Team. "The vast amount of Dtrack samples we found demonstrate how Lazarus is one of the most active APT groups, constantly developing and evolving threats in a bid to affect large-scale industries. Their successful execution of Dtrack RAT proves that even when a threat seems to disappear, it can be resurrected in a different guise to attack new targets. Even if you are a research center, or a financial organization that operates solely in commercial sector with no government affiliates, you should still consider the possibility of being attacked by a sophisticated threat actor in your threat model and prepare respectively."

Kaspersky products successfully detect and block the Dtrack malware.

To avoid being affected by malware, such as Dtrack RAT, Kaspersky recommends:

- Using traffic monitoring software like Kaspersky Anti Targeted Attack Platform (KATA)
- Adopting proven security solutions equipped with behavior-based detection technologies, like Kaspersky Endpoint Security for Business
- Performing regular security audit of an organization's IT infrastructure
- Conducting regular security training sessions for staff

More information about the new malware, used by Lazarus group, can be found on Securelist.

About Kaspersky

Kaspersky is a global cybersecurity company founded in 1997. Kaspersky's deep threat intelligence and security expertise is constantly transforming into innovative 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 technologies and we help 270,000 corporate clients protect what matters most to them. Learn more at www.kaspersky.com.

Media Contact:
Sarah Kitsos
781.503.2615
Sarah.kitsos@kaspersky.com
