Kaspersky Lab finds new variant of SynAck ransomware using sophisticated Doppelgänging technique

By Kaspersky

Published: 2018-05-07 · Archived: 2026-04-05 22:51:19 UTC

Kaspersky Lab researchers have discovered a new variant of the SynAck ransomware Trojan using the Doppelgänging technique to bypass anti-virus security by hiding in legitimate processes.

Woburn, MA – May 7, 2018 – Kaspersky Lab researchers have discovered a new variant of the SynAck ransomware Trojan using the Doppelgänging technique to bypass anti-virus security by hiding in legitimate processes. This is the first time the Doppelgänging technique has been seen in ransomware in the wild. The developers behind SynAck also implement other tricks to evade detection and analysis, obfuscating all malware code prior to sample compilation and exiting if signs suggest it is being launched in a sandbox.

The SynAck ransomware has been known since fall 2017, and in December, it was observed targeting mainly English-speaking users with remote desktop protocol (RDP) brute-force attacks followed by the manual download and installation of malware. The new variant uncovered by Kaspersky Lab researchers implements a far more sophisticated approach, using the Process Doppelgänging technique to evade detection.

Reported in December 2017, Process Doppelgänging involves a fileless code injection that takes advantage of a built-in Windows function and an undocumented implementation of the Windows process loader. By manipulating how Windows handles file transactions, attackers can pass off malicious actions as harmless, legitimate processes, even if they are using known malicious code. Doppelgänging leaves no traceable evidence behind, making this type of intrusion extremely difficult to detect. This is the first time ransomware has been observed using this technique in-the-wild.

Other noteworthy features of the new variant of SynAck include:

- The Trojan obfuscates its executable code prior to compilation, rather than packing it like most other ransomware, making it harder for researchers to reverse engineer and analyze the malicious code.
- It also obscures the links to the necessary API function, and stores hashes to strings rather than the actual strings.
- Upon installation, the Trojan reviews the directory its executable is started from, and if it spots an attempt to launch it from an ‘incorrect’ directory – such as a potential automated sandbox – it exits.
- The malware also exits without execution if the victim PC has a keyboard set to Cyrillic script.
- Before encrypting files on a victim device, SynAck checks the hashes of all running processes and services against its own hard coded list. If it finds a match, it tries to kill the process. Processes blocked in this way include virtual machines, office applications, script interpreters, database applications, backup systems, gaming applications and more - possibly to make it easier to seize valuable files which might otherwise be tied up into the running processes.

Researchers believe attacks using this new variant of SynAck are highly targeted. To date, they have observed a limited number of attacks in the U.S., Kuwait, Germany and Iran, with ransom demands of $3,000.

“The race between attackers and defenders in cyberspace is a never-ending one. The ability of the Process Doppelgänging technique to sneak malware past the latest security measures represents a significant threat; one that has, not surprisingly, quickly been seized upon by attackers,” said Anton Ivanov, lead malware analyst, Kaspersky Lab. “Our research shows how the relatively low profile, targeted ransomware SynAck used the technique to upgrade its stealth and infection capability. Fortunately, the detection logic for this ransomware was implemented before it appeared in the wild.”

Kaspersky Lab detects this variant of the SynAck ransomware as:

- Trojan-Ransom.Win32.Agent.abwa
- Trojan-Ransom.Win32.Agent.abwb
- PDM:Trojan.Win32.Generic

Kaspersky Lab recommends the following actions to keep users and devices safe from ransomware:

- Back up data regularly.
- Use a reliable security solution that is powered with behavior detection and able to roll back malicious actions.
- Always keep software updated on all the devices you use.
- If you’re a business, you should also educate your employees as well as IT teams, and keep sensitive data separate with access restricted. Use dedicated security solution, such as Kaspersky Endpoint Security for Business.
- If you are unlucky enough to fall victim to an encryptor, don’t panic. Use a clean system to check our No More Ransom site; you may find a decryption tool that can help you get your files back.

To learn more about SynAck, read our blogpost on Securelist.com.

About Kaspersky Lab

Kaspersky Lab is a global cybersecurity company, which has been operating in the market for over 20 years. Kaspersky Lab’s deep threat intelligence and security expertise is constantly transforming into next generation 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

Media Contact

Jessica Bettencourt

781.503.7851

Jessica.Bettencourt@kaspersky.com

Source: https://usa.kaspersky.com/about/press-releases/2018_synack-doppelganging