ESET Research discovers UEFI-compatible HybridPetya ransomware capable of Secure Boot bypass

DUBAI , DUBAI, UNITED ARAB EMIRATES, September 15, 2025 /EINPresswire.com/ -- ESET Research has discovered a HybridPetya bootkit and ransomware uploaded from Poland to the malware-scanning platform VirusTotal. The sample is a copycat of the infamous Petya/NotPetya malware; however, it adds the capability of compromising UEFI-based systems and weaponizing CVE-2024-7344 to bypass UEFI Secure Boot on outdated systems.

“Late in July 2025, we encountered suspicious ransomware samples under various filenames, including notpetyanew.exe and other similar ones, suggesting a connection with the infamously destructive malware that struck Ukraine and many other countries back in 2017. The NotPetya attack is believed to be the most destructive cyberattack in history, with more than $10 billion in total damages. Due to the shared characteristics of the newly discovered samples with both Petya and NotPetya, we named this new malware HybridPetya,” says ESET researcher Martin Smolár, who made the discovery.

The algorithm used to generate the victim’s personal installation key, unlike in the original NotPetya, allows the malware operator to reconstruct the decryption key from the victim’s personal installation keys. Thus, HybridPetya remains viable as regular ransomware – more like Petya. Additionally, HybridPetya is also capable of compromising modern UEFI-based systems by installing a malicious EFI application to the EFI System Partition. The deployed UEFI application is then responsible for encryption of the NTFS-related Master File Table (MFT) file – an important metadata file containing information about all the files on the NTFS-formatted partition.

“After a bit more digging, we discovered something even more interesting on VirusTotal: an archive containing the whole EFI System Partition contents, including a very similar HybridPetya UEFI application, but this time bundled in a specially formatted cloak.dat file, vulnerable to CVE-

2024-7344 – the UEFI Secure Boot bypass vulnerability that our team disclosed in early 2025," adds Smolár. ESET publications from January 2025 purposely refrained from detailing the exploitation; thus, the malware author probably reconstructed the correct cloak.dat file format based on reverse engineering the vulnerable application on their own.

ESET telemetry shows no active use of HybridPetya in the wild yet; thus, HybridPetya may just be a proof of concept developed by a security researcher or an unknown threat actor. Furthermore, this malware does not exhibit the aggressive network propagation seen in the original NotPetya.

For a more detailed analysis and technical breakdown of HybridPetya, check out the latest ESET Research blogpost: "Introducing HybridPetya: Petya/NotPetya copycat with UEFI Secure Boot bypass," on WeLiveSecurity.com. Make sure to follow ESET Research on Twitter (today known as X), BlueSky, and Mastodon for the latest news from ESET Research.

About ESET
ESET® provides cutting-edge cybersecurity to prevent attacks before they happen. By combining the power of AI and human expertise, ESET stays ahead of emerging global cyberthreats, both known and unknown—securing businesses, critical infrastructure, and individuals. Whether it's endpoint, cloud, or mobile protection, our AI-native, cloud-first solutions and services remain highly effective and easy to use. ESET technology includes robust detection and response, ultra-secure encryption, and multifactor authentication. With 24/7 real-time defense and strong local support, we keep users safe and businesses running without interruption. The ever-evolving digital landscape demands a progressive approach to security: ESET is committed to world-class research and powerful threat intelligence, backed by R&D centers and a strong global partner network. For more information, visit www.eset.com or follow our social media, podcasts, and blogs.

Sanjeev Kant
Vistar Communications
+971 55 972 4623
email us here