What is the NotPetya Ransomware Attack? Get Protected Against it

crowdstrike.com/blog/fast-spreading-petrwrap-ransomware-attack-combines-eternalblue-exploit-credential-stealing/

June 28, 2017

CrowdStrike Protects Against NotPetya Attack

June 28, 2017

Falcon Intelligence Team From The Front Lines Research & Threat Intel

Update:

Due to naming convention consistency in the industry, CrowdStrike is now calling this variant of Petya – NotPetya.

On June 27 at approximately 10:30 UTC, a new ransomware family began propagating across multiple countries. The family, referred to as NotPetya, is noteworthy because it combines traditional ransomware behavior with stealthy propagation techniques and a destructive attack element. CrowdStrike Falcon® Endpoint Protection customers are protected against all currently identified variants of the threat. For more details, read:

NotPetya Technical Analysis — A Triple Threat: File Encryption, MFT Encryption, Credential Theft.

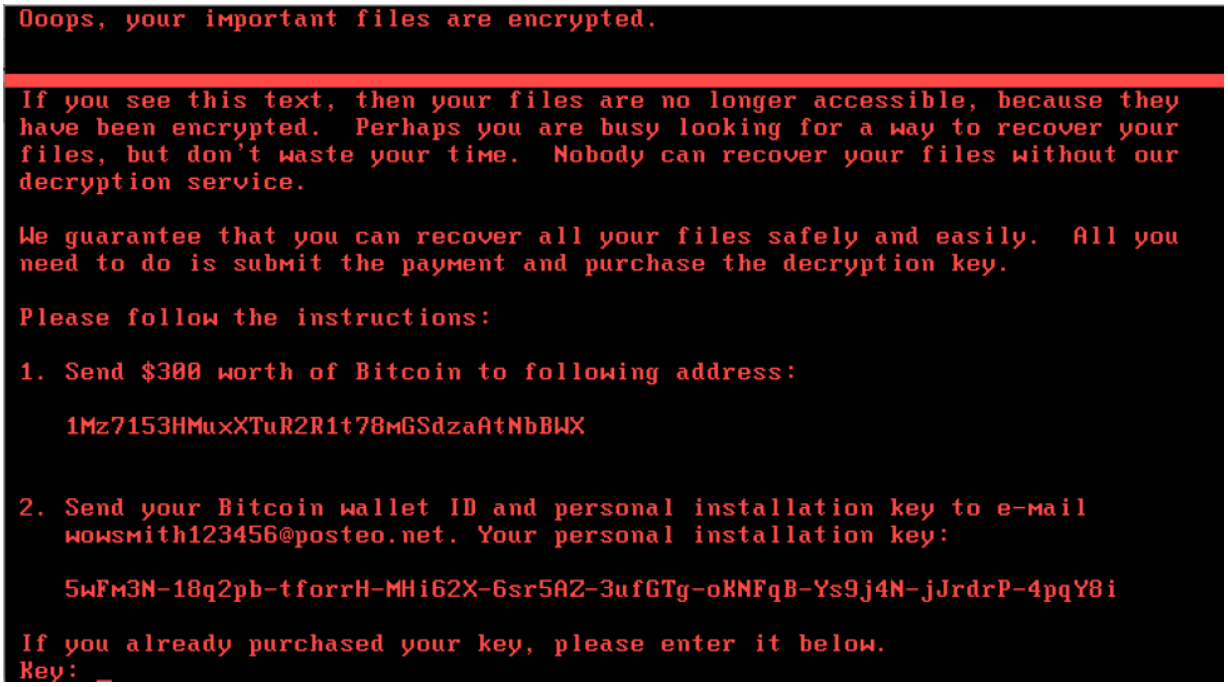
In addition to encrypting files on infected systems, NotPetya moves laterally to encrypt other systems in the organization by leveraging the same EternalBlue vulnerability that was popularized by WannaCry last month. It then uses another propagation technique that starts by stealing credentials, then uses those legitimate credentials to infect other systems on the network via built-in Microsoft tools (WMI and PSEXEC). Finally, NotPetya employs a destructive technique that prevents infected systems from booting by encrypting the master boot record (MBR).

Attacks have been reported in countries including Ukraine, Russia, Poland, France, Germany, Spain, the United Kingdom, the Netherlands, India, Israel, Australia and the United States. Sectors impacted by this attack include government, energy, finance, defense, telecom, media, maritime, aviation, and transportation.

NotPetya Summary

- Initial infection in Ukraine accomplished by exploiting vulnerability in M.E.Doc software
- Infected systems then attempt to propagate the infection to other systems
    - To infect other systems inside the organization, the malware steals credentials and propagates with built-in Windows tools WMI and PSEXEC:
      PSEXEC code snippet: C:\Windows\dllhost.dat \\IP ADDRESS -accepteula -s -d C:\Windows\System32\rundll32.exe “C:\Windows\perfc.dat”,#1 10 “USERNAME:PASSWORD”
      WMI code snippet: C:\Windows\system32\wbem\wmic.exe /node:”IP ADDRESS” /user:”USERNAME” /password:”PASSWORD” process call create “C:\Windows\System32\rundll32.exe \”C:\Windows\perfc.dat\” #1 XX \”USERNAME:PASSWORD\”
    - To infect additional systems outside the organization, the malware attempts to exploit the EternalBlue vulnerability
- The malicious payload then begins encrypting data, which includes the Master File Table and MBR
    - The attack creates a scheduled task to reboot the system after a certain amount of time has passed (up to 60 minutes):
    - Code snippet: schtasks /RU “SYSTEM” /Create /SC once /TN “” /TR “C:\Windows\system32\shutdown.exe /r /f” /ST XX:XX (where XX:XX is the time)
- It also attempts to cover its tracks by running commands to delete event logs and the disk change journal:
    - Code snippet 1: wevtutil cl Setup & wevtutil cl System & wevtutil cl Security & wevtutil cl Application
    - Code snippet 2: fsutil usn deletejournal /D C:

- Upon reboot the end user cannot get back into Windows, and instead they see a ransom note (screenshot below). This happens because NotPetya encrypted the MBR, thereby breaking the normal Windows boot process.



Initial Vector

According to multiple sources, infections of NotPetya were first identified on systems running a legitimate updater for the document management software M.E.Doc. This software is heavily used by Ukrainian companies, and companies operating in Ukraine, for maintaining information on tax and payroll accounting. From these infected systems, the ransomware can propagate to other systems using the techniques described above.

Based on analysis of the M.E.Doc software, and forensic analysis of initially infected hosts, it is believed that the malware was first deployed as a software update. Further third-party reporting suggests that the M.E.Doc update process started distributing a new binary containing a malicious payload at approximately 10:30 UTC. The deployment of NotPetya has also been reported by M.E.Doc users on the software company's forum in environments in which only this software was present.

Payment Mechanism

The ransomware operators demanded a ransom of $300 USD for each infected machine, and established Bitcoin payment workflow through an email address (wowsmith123456@posteo[.]net) provided by the third-party email service Posteo. Upon notification of this incident by the security community, the email provider announced that service to this address had been suspended as of 16:15 UTC (https://posteo.de/blog/info-zur-ransomware-petrwrappetya-betroffenes-postfach-bereits-seit-mittag-gesperrt). As a

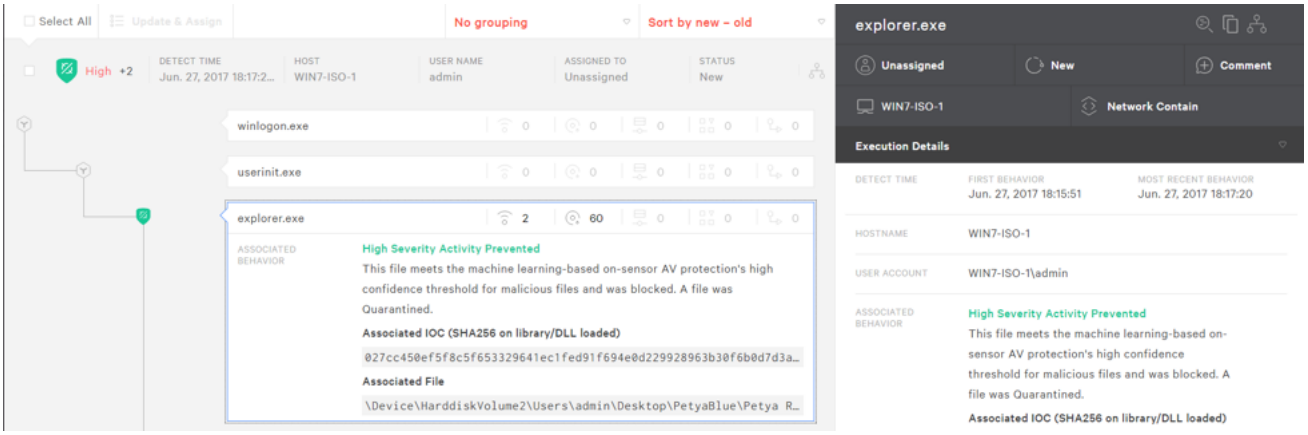
result, recovery of files upon payment of the ransom is no longer possible for impacted victims, as no mechanism currently exists for the ransomware operators to provide victims with decryption keys.

Once the malware is deployed on a victim machine, it creates a scheduled task to reboot the host an hour after the infection, likely in order to allow it to spread further before launching its destructive payload. To achieve this, the malware drops and runs either an x86 or an x64 version of a credential stealer executable from a resource that contains code similar to the well-known Mimikatz tool.

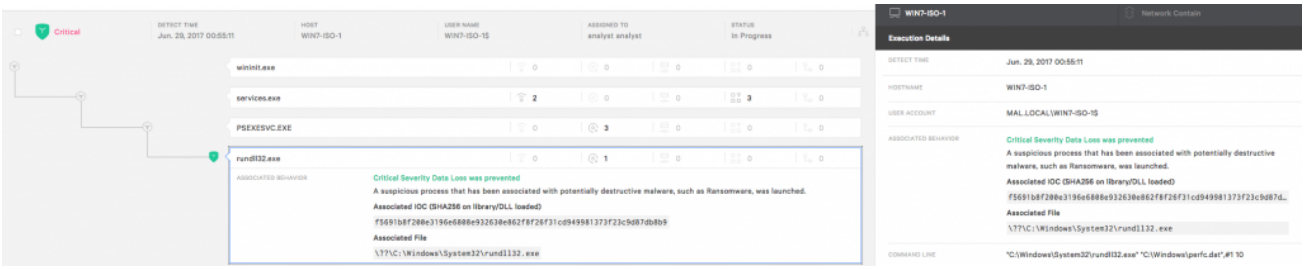
The ransomware payload uses a combination of 2048-bit RSA and 128-bit AES in Cipher Block Chaining (CBC) mode to encrypt files with extensions matching entries from a hard-coded list. Public reporting mentions similarities with the Petya ransomware; however, CrowdStrike was not able to confirm any links, and assesses that the code structure of this new family is different from Petya's.

Protection Against NotPetya

CrowdStrike Falcon Endpoint Protection can prevent both the initial NotPetya infection and subsequent propagation attempts. In the first example, Falcon is shown blocking the NotPetya malware from executing.

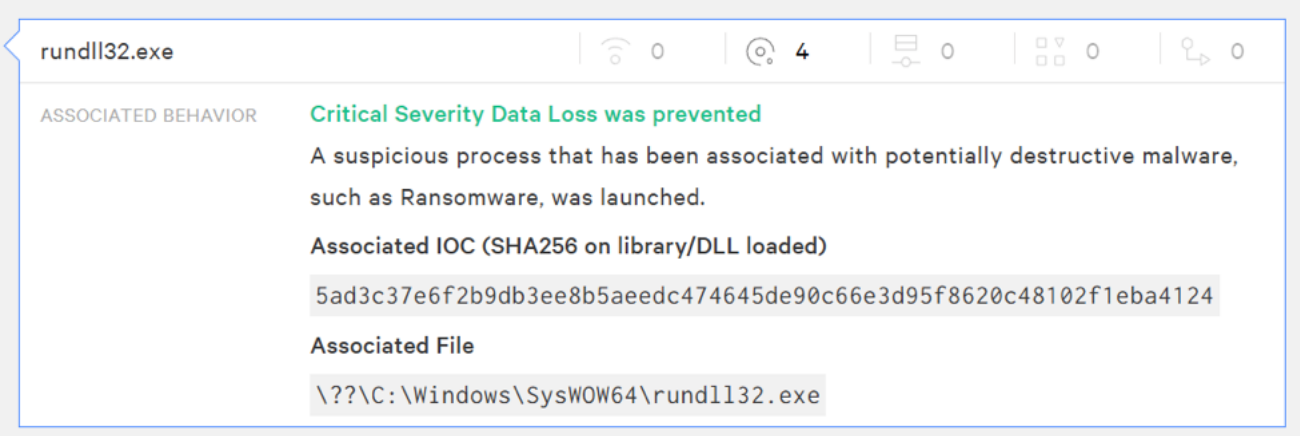


The second example shows a system on the same network as a system that is already infected. Because that second system is protected by Falcon, the propagation attempt fails and the second system is protected.

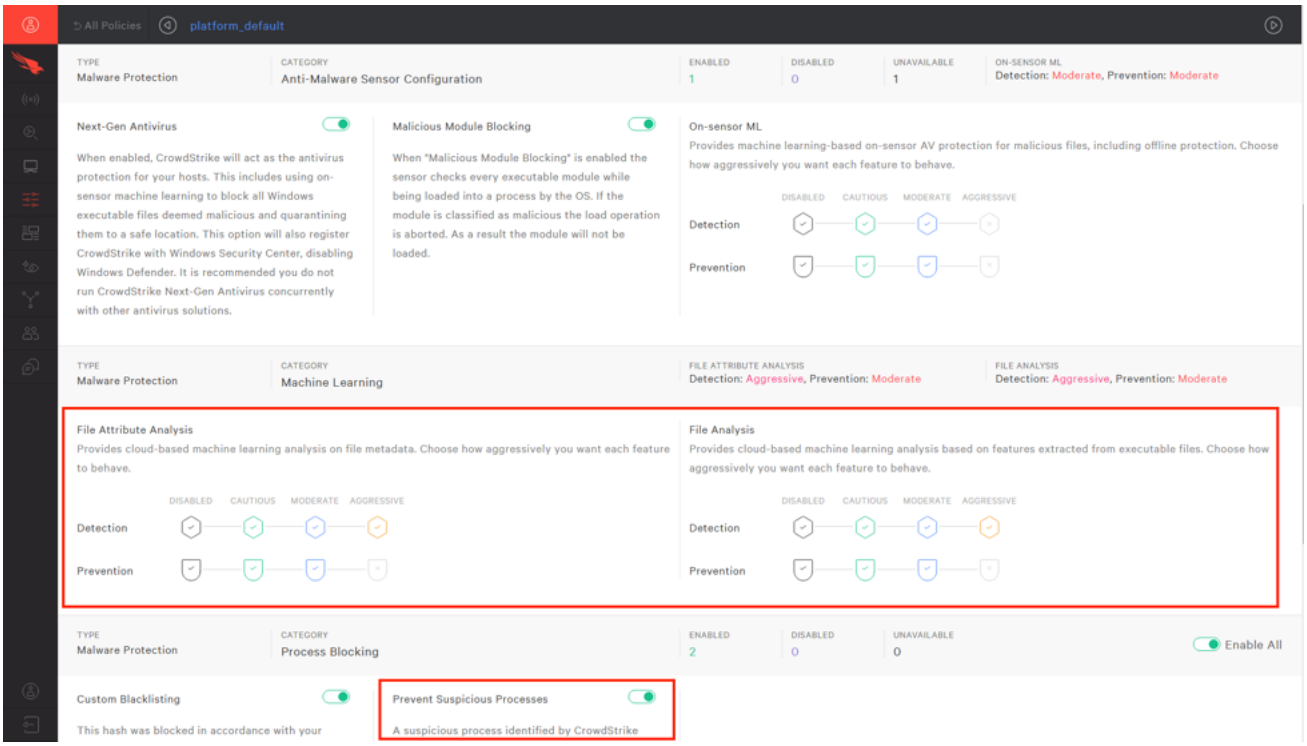


Falcon can also detect the threat based on its behavior. In the example below, RUNDLL32.EXE is exhibiting malicious behavior. It is attempting to execute a malicious DLL while simultaneously trying to steal credentials and write them to a temp file, as well as invoking a command to set the task scheduler to reboot the system in the near future.

The critical part of the attack is the RUNDLL32.EXE step (in orange). Because Falcon recognizes this collection of related behaviors as malicious, it prevents the execution of the process (as depicted below).



Falcon Endpoint Protection protects against NotPetya with both machine learning and behavioral protection. Falcon Prevent and Falcon Endpoint Protection customers can enable this protection by enabling “Moderate Prevention” settings on the machine learning engine sliders, including File Attribute, File Analysis, and On-Sensor Machine Learning under Process Blocking, please ensure Prevent Suspicious Processes is enabled.

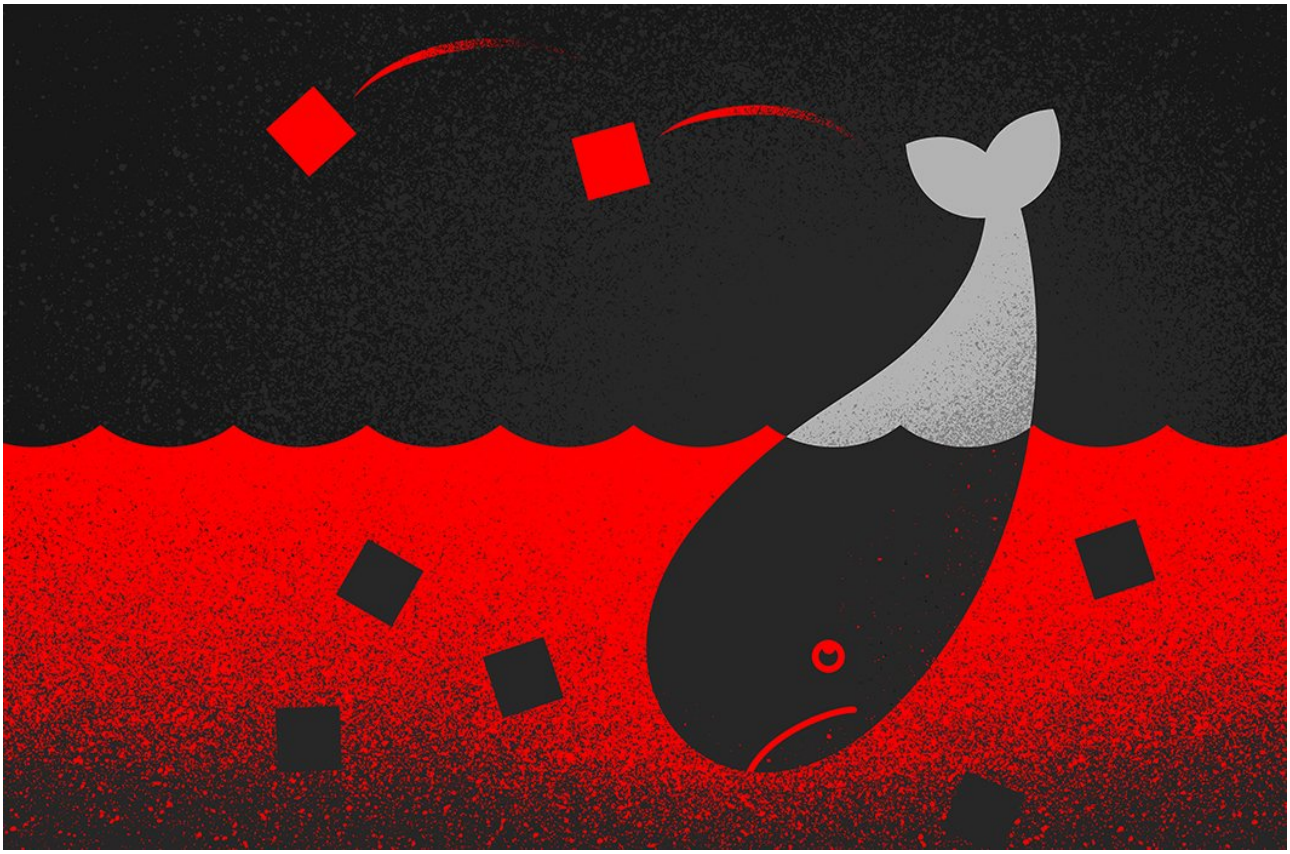


Falcon Endpoint Protection policy recommendation for blocking NotPetya

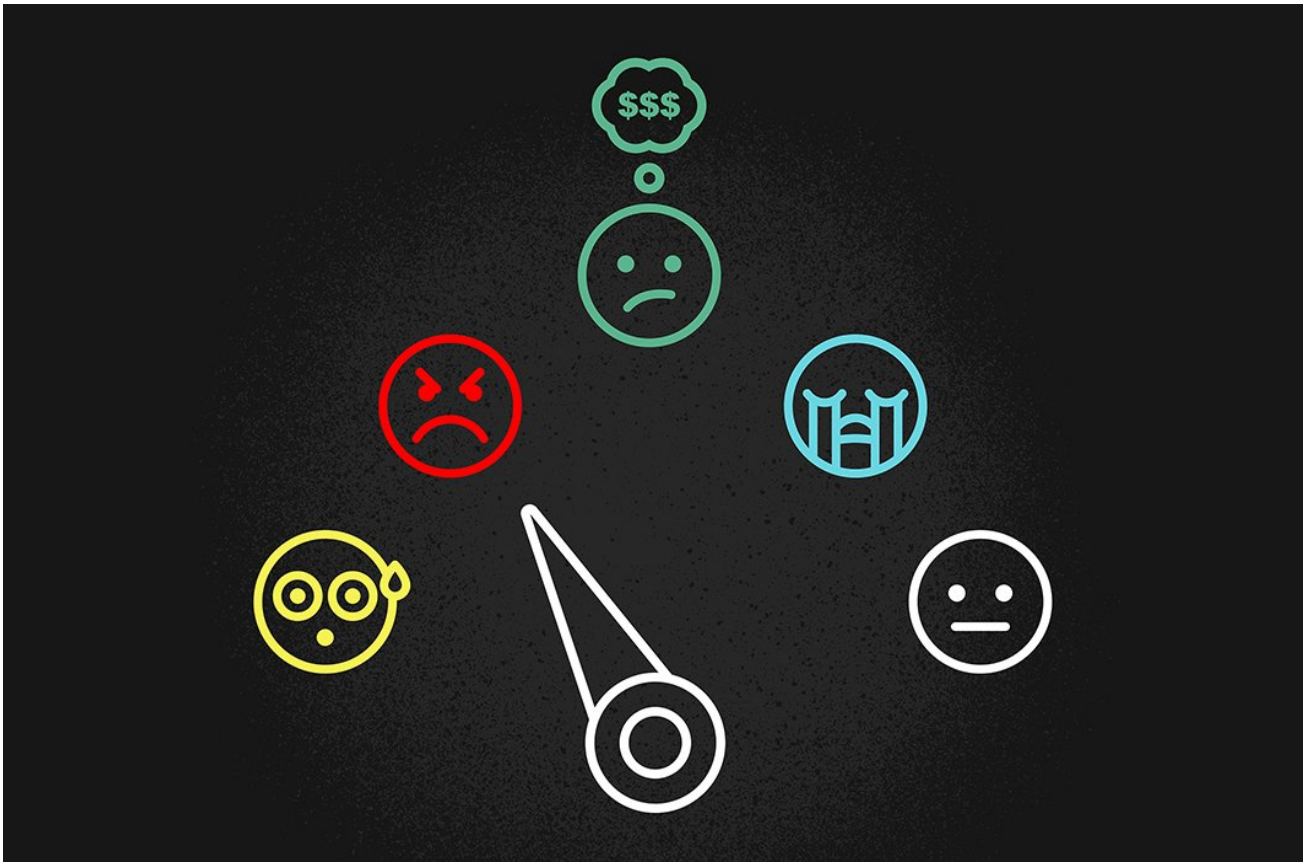
CrowdStrike Intelligence is actively monitoring the development of this ransomware and has published an in-depth technical analysis of NotPetya.

Click for more information on subscribing to Falcon Intelligence or to learn more about how Falcon prevents ransomware attacks.

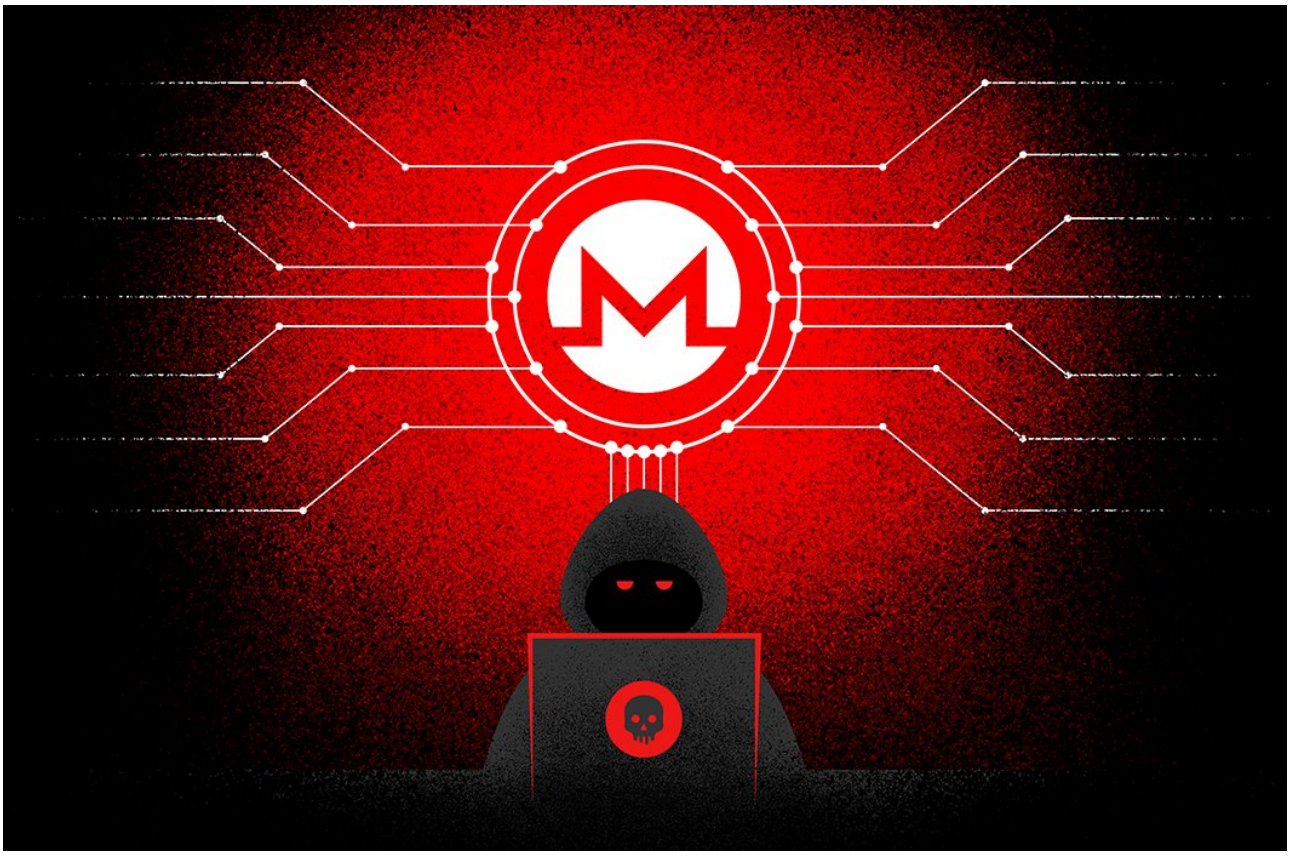
Related Content



Compromised Docker Honeypots Used for Pro-Ukrainian DoS Attack



Navigating the Five Stages of Grief During a Breach



LemonDuck Targets Docker for Cryptomining Operations