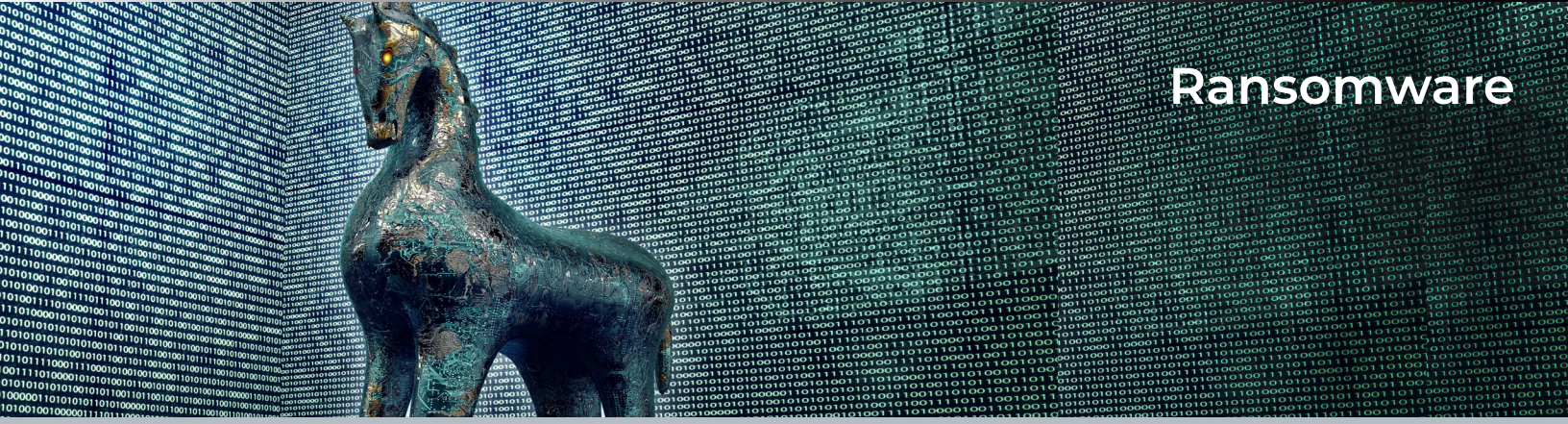


Is Conti the New Ryuk?

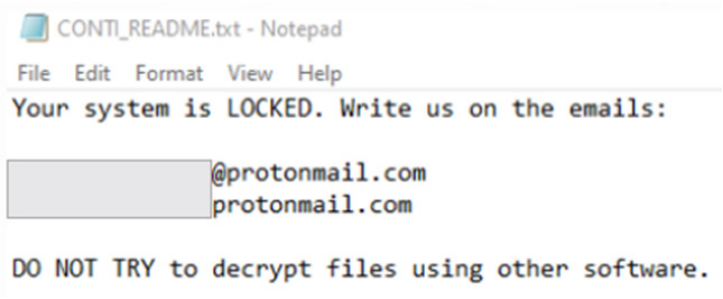
Background

Based on analysis of Conti ransomware, which was originally spotted in the wild in February of this year, the Arete Threat Intelligence team believes that this variant is being operated by the same group that conducted Ryuk ransomware attacks in the past. Digital forensics analysis of systems impacted by Conti ransomware revealed that it is generally being deployed by the attackers using the TrickBot banking trojan. Since early 2019, Ryuk ransomware operators exclusively used TrickBot trojan in their operations. In the 1st quarter of 2020, the number of Ryuk ransomware attacks significantly declined while the number of new Conti matters started to rise, which is a secondary indicator of a connection between both variants.

Conti Overview

Conti is a sophisticated ransomware variant that emerged in February 2020. Unlike most of its' peers, Conti ransomware encrypts files on victims' machines significantly faster by running 32 concurrent threads and utilizing all computing power that impacted systems have available. As a result of that, devices with multi-core CPUs get encrypted quicker. Conti has the capability to encrypt local hard drives, network shares and other devices on the local network. To encrypt the data, Conti uses the AES-256 encryption key, which is bundled with the RAS-4096 public encryption key (Note: this key is unique for each victim). Since the encryption key is unique for each victim, Conti operators cannot provide a decryption tool, which would work only on specific devices. The Conti decryption tool works on all encrypted systems within a victim's networks.

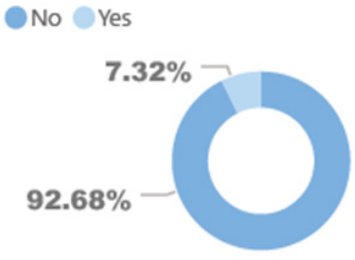
Prior to the start of the encryption, Conti leverages Windows Restart Manager to disable security, backups and other applications that may keep files locked on the impacted systems. Then it deletes Shadow Volume copies to make it impossible to use built-in Windows volume backups to restore data after the encryption.



Conti Ransom Note

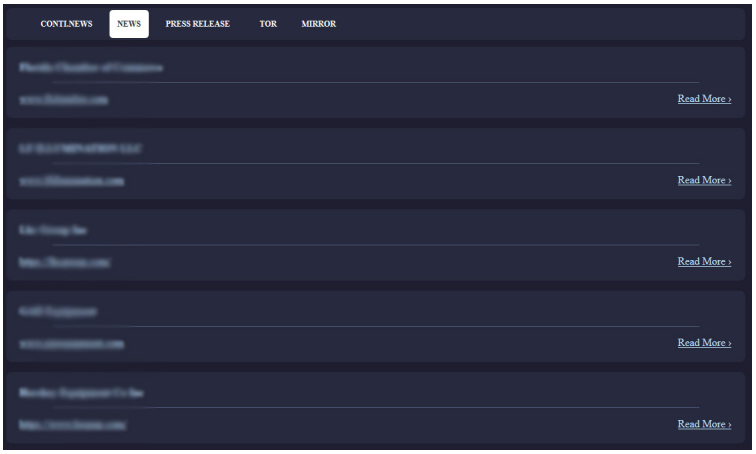
Conti Ransom Note

Once encryption completes, the .CONTI extension is **added to all encrypted files and the ransom note, CONTI_README.txt, is placed in each folder. Each ransom** note contains 2 email addresses to get in touch with the attackers, which are unique for each victim. This method is consistent with what Ryuk operators used in their attacks. Conti operators use a unique set of emails to identify each victim, so it does not matter if a victim responds from a corporate account or from a public email account – attackers still will know which victim they are communicating with. Just like Ryuk, Conti conducts research into information about their victims and sets ransom demands based on what they believe the victim can afford to pay.



% of Data Exfiltration in Ryuk matters

It was uncommon for Ryuk to exfiltrate data from victims' systems. Based on Arete analysis of previous matters, we only observed data exfiltration in 7% of cases. Unlike Ryuk, it appears that Conti ransomware operators decided to join the bandwagon of other 20+ variants that steal data from victims' environments prior to the encryption. Conti also created a web site where they publish lists of their victims in attempt to improve their chances of getting paid. In the last few weeks, Conti stepped up their extortion attempts and, in some cases, called the owner/managers of companies directly, to inform them that they have been compromised and threaten them to release the stolen data if they don't pay.



Screenshot of the Conti exfil site

Security Recommendations

Below are a few recommendations that will help to protect your organization from Conti ransomware attacks:

1. Implement a sophisticated Endpoint Detection & Response (EDR) solution that will rely on behavior analysis, instead of just malware signatures, and have tamper-proof capabilities.
2. Keep your systems updated and disable SMBv1, to protect against Windows EternalBlue vulnerability, which is actively being used by the TrickBot banking trojan to propagate within a victims' environment.
3. Block outbound traffic on your firewall for ports 447, 449 & 8082 (Note: along with 443 those ports are commonly used by TrickBot) and implement geo-blocking for foreign countries that you don't have any employees in and don't do business with.
4. Continuously educate your users on how to identify suspicious phishing emails and attachments.
5. Implement an off-site backup solution and test it regularly.