7 Predictions of Ransomware's Evolution

September 22, 2017 / **BRIAN BASKIN PARAM SINGH**

During the past six months, the Carbon Black Threat Analysis Unit (TAU) analyzed more than 1,000 ransomware samples, categorizing them into 150 families, and found attackers are looking to make quick, easy money with unsophisticated malware, combined with sophisticated delivery methods.

Our sampling has given insight into the future direction of ransomware. Following our analysis, we compiled seven predictions for the evolution of ransomware.

1 – Based on the direction ransomware is trending in our sample set, we believe ransomware will increasingly target Linux systems in an effort to further extort larger enterprises. For example, attackers will increasingly look to conduct SQL injections to infect servers and charge a higher ransom price. We have already observed attacks hitting MongoDB earlier this year which provide an excellent foreshadowing.

2 – Ransomware will become more targeted by looking for certain file types and targeting specific companies such as legal, healthcare, and tax preparers rather than "spray and pray" attacks we largely see now. There is already ransomware that targets databases, preying on businesses, and small tweaks to their code can target critical, proprietary files such as AutoCAD designs. A focused targeting of extensions can allow many ransomware samples to hide under the radar of many defenders.

3 – While most ransomware samples we analyzed simply encrypt files in place and transmit encryption keys for the purpose of decryption, there will be ransomware samples that will take the extra step of exfiltrating data prior to encryption. Not only would such an evolution put stress on companies to restore their data but also incorporate the loss of proprietary data that could be sold on the black market.

4 – Ransomware will increasingly be used as a smokescreen. For example, in the past, Zeus botnet operators hit victims with DDoS attacks after an infection to take investigators off the trail. A similar trend is emerging with ransomware attacks where the encryption of files could take place after more damning actions are taken by adversaries. Using already existing techniques of deleting Volume Shadow Copies, which deletes potential file backups, and the deletion of Windows event logs, adversaries can thwart many incident response efforts by forcing responders to focus on decrypting files instead of investigating data and credentials exfiltrated.

5 – Ransomware will emerge as a secondary method when initial forms of attack fail. Adversaries that rely upon more crafted and targeted attacks may use ransomware as an attack of last resort. Failing to entrench in an environment with a Remote Access Tool (RAT) or exfiltrate data, adversaries can push a ransomware across the environment to ensure at least a minimum return for their effort invested.

6 – Ransomware will be used more commonly as a false flag, as seen with NotPetya. Solely from dynamic analysis it was perceived to be Petya, when more detailed analysis showed it wasn't. Such quick analysis also insinuated it to be obvious ransomware, but a greater depth of disassembly showed that data was not held at ransom; it was simply destroyed.

7 – Ransomware will increasingly leverage social media to spread either intentionally or unintentionally. Similar to malware such as Koobface, maliciously shared content on sites such as Facebook could lead victims to click enticing links. Intentionally shared ransomware, seen in prior concepts, such as Popcorn Time where victims could share to reduce or eliminate their ransom, could see larger-scale use.