THREAT BRIEF

Ryuk (Ransomware)

Ransomware Serving as a Devastating Final Stage • Winter 2020

Gartner COOL VENDOR 2020™

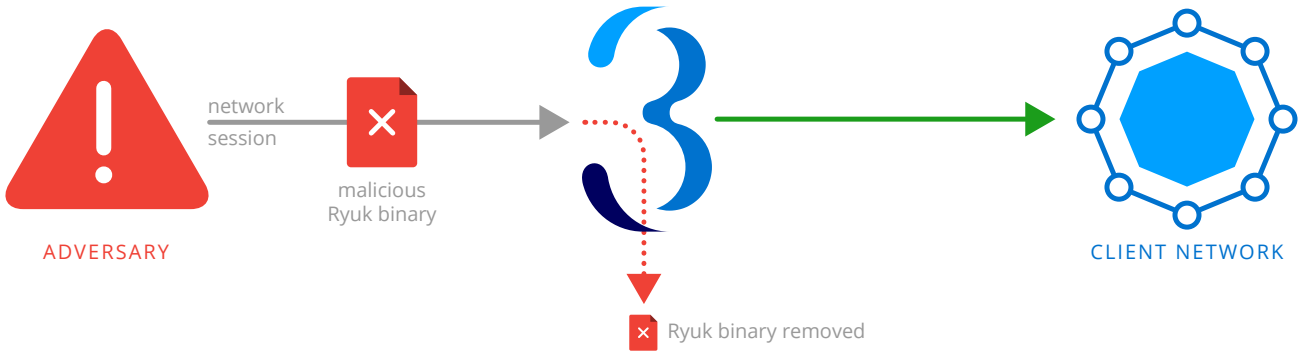
Ryuk is a ransomware campaign famous for re-emerging after long periods of quiet evolution. The gang responsible for this devastating cyber threat has also taken up the business of both selling their malicious code as a platform (AKA Ransomware-as-a-service (RaaS)) while simultaneously operating multiple campaigns against large enterprises. Because of this duality in business operations, Ryuk has appeared on enterprise networks in multiple industries: healthcare, local government, and many other sectors alike. Of particular note, Ryuk operators appear to be skilled at reducing the time from initial exploit to final stage infection. As a result, a simple spearphishing attempt can take just hours to unleash a multi-enterprise infection.

Because it is often deployed just as operators are exiting out of target networks, Ryuk ransomware has quickly evolved to be the final stage in many campaigns. This tactic is effective because it's preceded by extensive lateral movement, allowing attackers to establish a large foothold within the network from which they deploy Ryuk. To make matters worse for security professionals, these operators take extensive precautions to clean their forensic tracks as well—in some cases deleting backups so that even experienced IT admins can't access data encrypted by Ryuk without coughing up the ransom. To date, Ryuk operators have extorted over $61 million from their victims, according to FBI figures.

Rooting Out Ransomware at Every Stage of Attack

Trinity Cyber detects multiple variants of Ryuk binaries within full network sessions by applying our own unique and flexible logic that evolves as operators deploy new techniques and campaigns. Often, the very obfuscation techniques that Ryuk binaries contain give way to our ability to detect them within network sessions. We also identify the threat vectors that Ryuk is commonly delivered in, such as malicious documents with embedded CVE exploits or malicious macro content. We use our groundbreaking man-in-the-middle technology to address and prevent multiple stages in ransomware campaigns, which often mimic other malware campaigns.

When Ryuk binaries are detected, our advanced threat prevention service acts immediately by removing them from the offending network session. This prevents the delivery of sensitive information while providing valuable threat intelligence about where the attack came from within the internet. We also act on malicious documents in unique ways by surgically removing embedded exploits and malicious code (like macros) in flight before they have a chance to become a delivery vector for Ryuk. Trinity Cyber's immediate actions protect our customers from advanced threats such as Ryuk and provide a game-changing preventative control for network defense.



sales@trinitycyber.com • (240) 842-9900 • trinitycyber.com

Trinity Cyber