Understanding the Risk of Ryuk Ransomware

SUMMARY

Ryuk is a type of ransomware known for targeting large, public-entity Microsoft Windows cyber-systems. It typically encrypts data on an infected system, rendering the data inaccessible until a ransom is paid via cryptocurrency. Ryuk ransomware is derived primarily from the popular Hermes commodity ransomware that has been widely available on the dark web and hacker forums. But unlike Hermes, the Ryuk code has been modified and upgraded to specifically target enterprise environments. The ransomware is almost exclusively disseminated via a malware program called TrickBot, entering the system as a Trojan horse.

As opposed to other more highly automated forms of ransomware, once inside, hackers manually navigate Ryuk to conduct reconnaissance and select the most high-value targets. Once the data is stolen or systems rendered inoperable, Ryuk attackers typically demand payment in Bitcoin or other cryptocurrencies as ransom payments. One of the biggest recent Ryuk attacks conducted by hacker group Wizard Spider disabled the computer systems of United Health Care, one of the largest healthcare providers in the world.

A Ryuk ransomware attack typically occurs in the following sequence of events:

a) Phishing: The ransomware is usually delivered to an unsuspecting user or users via a phishing attack. Ryuk is embedded in a legitimate-looking document or attachment, executing once the user opens it;
b) TrickBot: Once Ryuk is unleashed, the TrickBot script is activated, which is purpose-built to collect passwords and gain privileged access to higher levels of the system and network; and
c) Ransom: The attackers then use TrickBot to navigate laterally through the system and either shut it down completely or gain access to sensitive data. Ryuk will then deliver a message explaining that an attack is underway along with payment instructions.

With malicious emails up over 600% since the beginning of COVID-19, it is imperative that organizations have the right tools and cybersecurity posture to detect and mitigate Ryuk attacks at all three stages.

In many cases, days or weeks may elapse between the time hackers initially gain access to a system before the massive encryption occurs, as the criminals penetrate deeper into the network to inflict maximum damage. Ryuk is a destructive type of malware because it also finds and encrypts network drives and resources. It also disables the System Restore feature of Microsoft Windows that would otherwise

allow restoring the computer's system files, applications, and Windows Registry to their previous, unencrypted state.

Because of the complexity of Ryuk, only experienced IT teams should remove it. Only the threat actors hold the key to restoring the assets. It is possible to remove Ryuk in safe mode or via system restore, but ideally, the focus should be on preventing an attack before getting hold of critical assets.

To avoid this kind of ransomware, netizens should never click on unknown links or open any software downloads without first performing a virus scan. In addition, users should deny any User Account Control (UAC) request unless they are making modifications to their own system. Likewise, they should be cautious in visiting web pages with malicious code, for this will disallow the attacker to compromise through the infected system. It is best to install security software with warning signals for the detection of malicious software.

RECOMMENDATION

The public are advised to follow these tips in order to prevent Ryuk Ransomware:

- Install anti-malware software;
- Back-up regularly and keep a recent backup copy off-site;
- Do not enable macros in document attachments received via email;
- Update systems regularly; and
- Be cautious about unsolicited attachments.