Talos
Cisco Security Research

Ryuk remains a formidable ransomware threat

This malware family has been around for a few years, but as we saw in 2020, it's not going away soon

BACKGROUND

Ryuk ransomware has been around since at least mid-2018 and has consistently remained a top ransomware threat. Ryuk is usually delivered as a final payload by other threats, such Emotet and Trickbot. Adversaries tend to target organizations with high annual revenues and/or critical assets in hopes of extracting larger ransoms from the victims, an approach known as "big game hunting."

CAPABILITIES

- Ryuk operators extract information from the Active Directory (AD) by downloading and executing open-source tools and utilities.
- The actors use code injection to terminate processes and stop services for various security products.
- A Wake-on-LAN feature turns on powered-off devices to allow for more systems on the network to be encrypted.
- Ryuk actors send phishing emails containing malicious links or attachments that infect victims with Emotet, Trickbot, or other commodity trojans. After initial compromise, attackers gain a foothold in the victim environment and conduct extensive network reconnaissance before downloading Ryuk as a final payload.
- In addition to leveraging banking trojans, adversaries also rely on a range of open-source and native Windows tools during the attack process.
- Ryuk operators exploit the Zerologon vulnerability (CVE-2020-1472), allowing them to escalate privileges in less than two hours after an initial Ryuk phishing email.

INTELLIGENCE & RESPONSE

- Talos and Cisco Talos Incident Response (CTIR) researchers frequently respond to Ryuk-related incidents by conducting telemetry analysis and providing real-time intelligence support.
- Ryuk relies on several well-known tools and threats for infection, including Cobalt Strike and Trickbot, which Talos has years of insight and intelligence into.
- We blocklist all publicly reported indicators to ensure that our coverage remains up-to-date and enter all related open-source reports in the actor-tracking software MISP.
- All findings are crucial for Talos analysts writing expansive coverage for ClamAV®, SNORT®, OSQuery and Fireamp.

AFFECTED INDUSTRIES/GROUPS

- During the COVID-19 pandemic, Ryuk has targeted multiple health care entities in opportunistic attacks.
- The adversaries target a variety of countries across the globe, including those in North America, Europe, the Middle East, South America and Asia.
- In addition to targeting large organizations, the actors also target government and municipal networks, as well as critical infrastructure, including oil and gas entities.

COVERAGE

- Cisco AMP provides many layers of protections on the endpoint. It has multiple engines that detect and prevent initial infection, reconnaissance, lateral movement and file encryption.
- There are numerous ClamAV® and SNORT® signatures that protect users from many of Maze's malicious activities. Please refer to Snort.org or ClamAV.net to search for the full volume of specific rules or malware.
- Cisco Secure Network Analytics detects any changes in our customers' network and monitor both outbound and inbound traffic patterns that may point to a malware infection.
- Cisco Tetration provides multiple layers of visibility and control to reduce the attack surface and prevent lateral movement.
- Using multi-factor authentication protocols such as Cisco Duo can prevent credential-stealing, which often provides threat actors with an initial foothold on the targeted system.

talos-external@cisco.com | talosintelligence.com