Ransomware

US Government Alerts of Imminent Attacks Against the Healthcare Sector by Trickbot Group

Executive Summary

Last week, the Cybersecurity and Infrastructure Security Agency (CISA) in collaboration with the Federal Bureau of Investigation (FBI), and the Department of Health and Human Services (HHS) released the following alert: AA20-302A - Ransomware Activity Targeting the Healthcare and Public Health Sector.

The alert informs that there is credible intelligence of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers associated with the **Trickbot and BazarLoader trojans** that often leads to ransomware like the **Ryuk and Conti ransomware.** The alert also mentions the **Trickbot Anchor tool set** and **Anchor_DNS** tool developed by this group.

News of these attacks against the Healthcare sector are of special concern due to the recent increase of COVID-19 cases in the US and evidence that shows ransomware attacks against the healthcare sector have been associated with persons losing their lives due to services being routed to nearby hospitals and laboratory results not being quickly delivered electronically to the providers.

Arete statistics and Intel from Arete's Fusion Center and Open-source intelligence (OSINT) shows that this new wave of attacks since October 2020 have a slight change in TTPs and the BazarLoader malware has now been observed in systems compromised with Ryuk.

The Arete incident response (IR) practice has responded to more than ninety (90) Ryuk engagements since 2019 with more than six breach responses engagements just in the month of October 2020.

Based on Intelligence gathered from our DFIR cases, Arete's Fusion Center had developed countermeasures deployed in the SentinelOne EDR platform to detect these threats and our Managed Detection and Response (MDR) team has been handling detections at our client's sites.

This article is meant to share with the community Arete's statistics and our assessment based on breach response engagements.

Statistical Data from Arete's Metrics

The information listed below is based on Ryuk cases investigated by Arete IR since January 2019. Our IR and Data Analytics practices work together to track key data points for every ransomware engagement. Our IR practice tracks data points on the ransomware variant and collects statis-tics based on handled engagements:

- Since 2019, Arete has responded to Ryuk cases in some of the following sectors:
  Healthcare: 19 | Professional Service: 28 | Public services: 21 | Manufacturing: 11 | Technology/Engineing/ Telecom: 6 | Critical Infrastructure: 1
- Average duration of business downtime: 9.47 days
- Average original ransom demand in bitcoin: 125.39 BTC
- Average final ransom demand in bitcoin: 72.58 BTC
- Average ransom demand paid in US dollars: $621,064.05
- Minimum ransom demand paid in US dollars: $10,000.00
- Maximum ransom demand paid in US dollars: $5,177,510.78
- Remote access is the most common method of intrusion found 39.34% of the times
- During the Ryuk dwell time this year, Arete responded to ten (10) Conti ransomware engagements

Ryuk Ransomware Overview

Since August 2018, a Russian-based cybercrime group has been operating a ransomware known as Ryuk (a customized version of Hermes commodity ransomware).

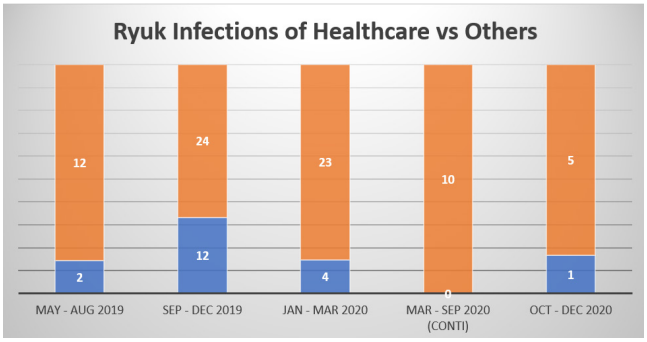
The industry saw a sudden drop of Ryuk, starting around the time that COVID-19 had its major impact in March 2020. This is also around the same time that a very similar, Conti ransomware, began to kick-off, leading many to believe that Conti was merely a rebrand of Ryuk. The data suggests though that it is possible that Conti was a failed rebrand since Arete IR has not been engaged with Conti infected clients since Ryuk attacks started again in October 2020.

Ryuk typically compromises networks through Trickbot, or Emotet then delivering Trickbot. Trickbot has recently been in the news in the cyber industry due to Microsoft's approval via a court order to engage in disruption efforts of this botnet. With this active disruption campaign, it is possible that the sudden return and up-tick of Ryuk infections is due to the Russian cybercrime group acting in retaliation utilizing their more mature ransomware product, Ryuk, as opposed to the potentially rebranded, Conti, which could still have been in a testing phase. This is based on the sudden stop of Conti and up-rise of Ryuk in line with the disruption efforts from Microsoft.

According to Microsoft, they initially disabled sixty-two (62) of the initially identified sixty-nine (69) Trickbot servers. Almost immediately, fifty-nine (59) new servers were attempted to be added to the Trickbot infrastructure. As of October 20, 2020, fifty-eight (58) of the new servers have also been disabled leaving a total number of eight (8) known active Trickbot servers.

Ryuk Wave Crashing on US Healthcare

Of the more than ninety (90) total Ryuk ransomware engagements that Arete IR has led since May 2019, nineteen (19) of those engagements were for a client in the healthcare industry (23%). Out of the seven (7) engagements of Ryuk ransomware that Arete IR has led since it re-emerged in October 2020, the most recent case is the only client that is in the healthcare industry (14%). This evidence shows it is not typical for Ryuk attacks to be focused primarily on the healthcare industry. This could further backup the theory that the impending Ryuk wave of attacks on the healthcare industry could be retaliation for Microsoft's disruption campaign against the Trickbot infrastructure that Ryuk is known for utilizing for initial intrusion.



Recommendations

- Install an Endpoint Detection and Response (EDR) solution with the capability to halt detected processes and isolate systems on the network, based on identified conditions
- Block: Any known attacker C2s in the firewall; A high number of SMB connection attempts from one system to others in the network over a short period of time
- Implement: A system enforced password policy to force users into changing passwords at least every 90 days; Multifactor authentication (MFA) on RDP and VPN access
- If not needed, eliminate vulnerable RDP ports exposed to the internet
- Perform: Dark web monitoring periodically to verify if data from the organization is available for sell in the black market; Penetration tests
- Periodically patch systems and update tools
- Monitor: Connections to the network from suspicious locations; Downloads\uploads of files to file sharing services over non-standard hours, not commonly used in the organization, etc; Uploads of files from Domain Controllers to the internet; Network scans from uncommon servers (e.g. RDP server)

References

ttps://blogs.microsoft.com/on-the-issues/2020/10/12/trickbot-ransomware-cyberthreat-us-elections/
https://blogs.microsoft.com/on-the-issues/2020/10/20/trickbot-ransomware-disruption-update/
https://us-cert.cisa.gov/ncas/alerts/aa20-302a