Ransomware

Arete Analysis: AKO Ransomware

Executive Summary

Since January 2020, Arete's incident response (IR) team has responded to various AKO ransomware engagements. Recently, we have encountered these specific attacks against the Finance, Healthcare, and Manufacturing sectors. This article is meant to provide information on the ransomware behavior observed during one of these engagements. Our intention is to summa-rize the high-level information from AKO ransomware events for general awareness, as well as provide security recommendations to better defend against this threat.

Statistical Data on AKO ransomware from Arete's metrics

The information listed below is based on AKO cases investigated by Arete IR since January 2020. 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 statistics based on handled engagements:

- Arete has responded to AKO cases since January 2020 in the Finance, Healthcare, and Manufacturing sectors
- The average ransom demand is 8 BTC
- The maximum ransom demand paid in US dollars has been $150,000
- The minimum ransom demand paid in US dollars has been $2,000
- Data exfiltration was observed in incidents involving the Healthcare sector
- The major infection vector has been Remote Access (RDP) at 66.67% of the time

Background

AKO ransomware has been around since at least January 2020 and is distributed via a ransomware-as-a-service (RaaS), which mirrors the software-as-a-service (SaaS) model offered by legitimate vendors. Like SaaS, RaaS is offered via cloud-based subscription models for a subscription fee and several RaaS groups use a partner, or franchise-like, structure. This structure is where the RaaS operator keeps a percentage of commission from every victim infected through their partners and pays the rest of the extorted funds to the partner or "franchise owner." What makes the RaaS model so appealing and lucrative is they are specifically built to be easy to use and deploy. Typically, RaaS variants employ a portal where the partner only needs to download the ransomware, with no development or coding skills required. Most RaaS models even provide a fully staffed technical and customer support service, like you would find with a legitimate SaaS offering. The support is meant to help the franchise owner or partner get off the ground with their ransomware campaign.

There are various blogs [1-2] that have been written on AKO ransomware, so we will not go into detail in this section. In some of these reports, the malware was observed encrypting files on Windows systems and adding a .m9V742 files extension, Windows Defender is stopped, and the registry modified to prevent the antivirus software from starting again. Some antivirus tools detect the malware as MedusaLocker or MedusaReborn, but the AKO ransomware operators deny association with MedusaLocker and say that AKO is their own product. The threat actors also confirmed that it is part of their job to steal data from the compromised networks.

At the time of this writing, no known free decryptors for this ransomware variant were available.

Recommendations

- Install an Endpoint Detection and Response 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
- Implement a system enforced password policy to force users into changing passwords at least every 90 days
- Implement multifactor authentication on RDP and VPN access
- If not needed, eliminate vulnerable RDP ports exposed to the internet
- Block a high number of SMB connection attempts from one system to others in the network over a short period of time
- Perform dark web monitoring periodically to verify if data from the organization is available for sell in the black market
- Perform penetration tests
- Periodically patch systems and update tools
- Monitor connections to the network from suspicious locations
- Monitor downloads\uploads of files to file sharing services over non-standard hours, not commonly used in the organization, etc.
- Monitor uploads of files from domain controllers to the internet
- Monitor network scans from uncommon servers (e.g. RDP server)

[1] https://www.bleepingcomputer.com/news/security/ako-ransomware-another-day-another-infection-attacking-businesses/

[2] https://www.bleepingcomputer.com/news/security/ako-ransomware-uses-spam-to-infect-its-victims/