THREAT REPORT: Two Regionally Novel Ransomware Groups Active in Alberta

March 20, 2024

TLP: GREEN ○○●

Source: Internal Closed Source

Overview:

Threat actor groups have been targeting municipalities and organizations at anomalous rates across Canada and within Alberta. Amongst the observed attackers are two ransomware groups—Cloak and Play—who are novel to the Alberta region.

- The **Play ransomware group** (also known as Playcrypt, DEV-0882, and storm-0882) first emerged in August of 2022.
  - As of October 2023, the Federal Bureau of Investigations is aware of approximately 300 victims.
  - When selecting targets, Play does not appear to distinguish between industries. To name a few, they have targeted information technology, transportation, government, education, construction, manufacturing, real estate, and financial industries.
  - Play appears to be financially motivated and employs the double extortion technique, exfiltrating data prior to encrypting target systems. This provides the attacker additional leverage, because even if they are flushed out of the system, they can threaten to publicize the targets data.
  - The group primarily gains initial access to target infrastructure through exploitation of public facing applications and services and by using valid accounts. The Play group has been known to target FortiNet and Microsoft Exchange server products.
  - After gaining initial access, Play establishes command and control with their infrastructure to download additional post-compromise tooling. An extensive list of tools they have used in the past can be found here.

- The **Cloak ransomware group** has been active since late 2022 and there is relatively little public information on their tactics.
  - Cloak appears to target primarily small to medium sized businesses. Like Play, their targets are diverse, and it cannot be assumed that they preferentially target any industry. However, they also appear to also be financially motivated.
  - Cloak is suspected of relying on Initial Access Brokers (IABs) to gain initial access to target infrastructure. IABs specialize in compromising systems and networks, and then selling that access to threat actor groups, such as Play and Cloak.

Threat Analysis:

- **Vulnerability & Patch Management:** Play has been observed using both older and zero-day vulnerabilities (e.g., FortiNet and Microsoft Exchange server) to gain initial access, escalate privileges, and perform execution. Organizations should concentrate on patching old systems and software and prioritize known exploited vulnerabilities.

- **Monitor Popular IABs:** Due to Cloaks' reliance on IABs, it is recommended that organizations monitor known brokers, who may be selling access to their networks. Should one discover their data is being brokered, they must act swiftly and issue immediate changes which will nullify this data. Commonly, IAB's will sell valid user credentials, in such scenarios, nullifying action means blocking compromised users until their credentials have been updated. Additional controls include mandatory Multi-factor Authentication (MFA) wherever applicable, and securing services on your perimeter such as Virtual Private Networks (VPNs) and Remote Desktop Protocol (RDP).

- **Be Prepared:** The above recommendations are preventative in nature, but in today's day and age, incidents are seemingly inevitable. It is paramount that organizations arm themselves with mature and tested incident response, business continuity, and disaster recovery plans. Further, organizations must have detection capabilities which will help identify anomalous behaviors in their networks. Having these technologies and plans in-place reduces adversary dwell time, mean time to detection, and mean time to recovery.

Further Reading:

- Cloak Ransomware: Who's behind the Cloak? | cyberint.com
- #StopRansomware: Play Ransomware | CISA
- CloAk Ransomware: Complete Guide | SalvageData.com
- An In-depth Look at Play Ransomware | Avertium
- Play | SentinelOne