USE CASE

INCIDENT RESPONSE

MARKET:

Healthcare

THREAT ACTOR:

Karakurt (“Black Wolf” in Turkish)

Threat Actor Profile:

- Karakurt focuses on attacking organizations that have already been compromised, obtaining stolen credentials from third party intrusion brokers and buying credentials via the Dark Web.
- Karakurt is believed to be an affiliate of Conti Ransomware Group.
- Karakurt moves laterally across victim networks by using valid stolen administrator credentials.
- This threat actor is highly focused on data extortion.

RISK/CHALLENGE:

A large International Accounting Firm was faced with impacts from a network and data security breach carried out by the Karakurt group.

- Client required immediate incident response, containment, and remediation to its global networks and infrastructure.
- International offices were impacted across the US and EMEA.
- Ransom demand was $5,500,000.
- Karakurt operators hit the firm with triple extortion tactics.

TOOLS & TECHNIQUES:

- **Immediate Response:** Redpoint coordinated scoping call with the client's Legal Counsel within minutes of being contacted to support incident response, investigation, and containment.
- **Containment:** Initiated countermeasures to contain active "hostile hosts" through technology deployment, routing updates, data center isolation, and targeted shutdowns of critical operations.
- **Threat Actor (TA) Negotiations:** Redpoint's seasoned negotiator established communications with the TA to gain valuable insight into the TA operations / TTP's.
- **Discovery:** Analyzed client physical/virtual server environment to identify recoverable systems and configurations to facilitate rebuild of critical infrastructure. Performed data integrity analysis on unencrypted data and exfiltrated data to shared storage solution for recovery after spinning up new server infrastructure.
- **Remediation:** Consulted with client leadership, technical staff, and 3rd-party provider(s) to plan and execute migration to cloud-based server infrastructure with proper backup policies established and in use; planned, organized, and executed re-imaging procedure for client workstations at all global locations using newly established infrastructure.

OUTCOMES:

- Rapid response – we began the initial engagement within the first hour of the reported incident and established critical "mass on target" within first 12 hours.
- Strategically contained and remediated the attack while being laser focused on prioritization of critical business functions in coordination with key stakeholders.
- Systematically identified, contained, and remediated "hostile hosts" while balancing business priorities.
- Conducted forensics and timeline analysis to confirm credential harvesting (Mimikatz and Rubeus) and primary propagation method was GPO (Group Policy Object).
- Restoration and reporting were concluded within 5 business days.