THREAT ALERTS

MULTI-STAGE RANSOMWARE

OVERVIEW

THREAT TYPE:
RANSOMWARE

TARGET INDUSTRY:
CRITICAL INFRASTRUCTURE

ATTACK GOAL:
STEAL SENSITIVE DATA
& SPREAD RANSOMWARE

IMPACTED GEO:
NORTH AMERICA, SUSPECTED GLOBAL

REMEDIATION STEPS

Reimage any affected machines because of the different persistence mechanisms used.

Change all passwords related to affected services, both browser-based and local applications.

Harden remote access interfaces (RDP, SSH).

EXPERIENCED A BREACH?
EMAIL US AT

INFO@CYBEREASON.COM

WHAT'S HAPPENING?

Over the past few months, the Cybereason team has been investigating multiple instances of ransomware attacks against large critical infrastructure providers. This attack highlights an ongoing trend where ransomware attacks are no longer just deploying and detonating; they are taking their time to maximize their profit per targeted organization by impacting the availability of multiple machines and the confidentiality of proprietary data.

KEY OBSERVATIONS & TTPS

- This attack exfiltrates victim's data and credentials and uses stolen credentials to spread across the network before detonating ransomware.
- Following initial access, this attack immediately establishes persistence and starts to move laterally across the network.
- The malware establishes itself on multiple machines and scans the network. It deploys the ransomware early in the operation, exfiltrates data and credentials, and once that is completed, it detonates the ransomware.
- Ransomware attacks are no longer limited to requesting a ransom; they are now being used for more damaging hacking operations that can lead to data breaches, brand degredation, and ultimately, ransomware attacks.

CYBEREASON CUSTOMERS

PREVENTED & DETECTED BY
THE CYBEREASON DEFENSE PLATFORM

We highly recommend every customer consider the following:

- The Cybereason Defense Platform was able to detect the preliminary stages of the attack and analyze and prevent the execution of the malicious ransomware payload.
- If you do not have Cybereason NGAV activated, consider doing so to prevent against threats like these.
- For Cybereason MDR customers, the Cybereason team will monitor and triage as well as assist in the mitigation of potential infections.