Case Study

US Municipality

AT&T Cybersecurity

AT&T Cybersecurity assists municipality hit by ransomware attack

Solutions

- AT&T Managed Threat Detection and Response
- AT&T Managed Firewall

Organization type

- State and local government

Overview

A large local government entity suffered a ransomware attack that affected several departments and temporarily disrupted critical communications and IT systems. The attack was subsequently found to have been carried out by the Royal ransomware group, a group that was first observed in September 2022 and that has impacted local government entities in the US and Europe.

AT&T Cybersecurity provided extensive after-hours support at the height of the attack and delivered a comprehensive report on the incident within 24 hours of the initial call from the customer.

Events

In Q2 2023, the AT&T Managed Threat Detection and Response (MTDR) team was made aware of a potential ransomware attack on a customer (“Customer X”). Analysts within the AT&T Cybersecurity Security Operations Center (SOC) received alerts that the PsExec utility tool was used within the customer’s environment. This tool allows users to remotely execute, and threat actors are known to abuse it to remotely execute commands or deploy malware and move laterally through an environment.

Analysts immediately created an investigation within AT&T USM Anywhere, an open XDR platform that extends threat detection and response across hybrid IT environments. The Investigations feature within USM Anywhere enables SOC analysts to automate the collection of data and initial findings such as alarms and events in support of an investigation. Customers are also able to log into the platform directly to view ongoing analysis and exchange communications with the SOC team.

The team conducted an in-depth review of log data from 90 days prior to the incident, performed open-source intelligence (OSINT) research, and observed encrypted file extensions that were being uploaded to OneDrive. From this work, AT&T analysts determined the attackers were members of the Royal ransomware group, known to be responsible for several high-visibility attacks since the end of 2022[1].

The incident was immediately escalated to an AT&T incident response (IR) team. The team was able to determine that the attackers had compromised an on-premises, external-facing Microsoft Exchange server running on a Windows Server that was past end-of-life (EOL) support. The attackers were using the server as their beachhead to perform reconnaissance and move laterally across the network before deploying encryption malware.

The IR team was also able to establish when the server was most likely compromised through the USM Anywhere platform's integration with ExtraHop, a third-party anomaly detection tool. Through AlienApps, the platform supports in excess of 600 integrations with third-party tools including more than 50 advanced integrations. The tool had detected large amounts of data being exfiltrated from multiple Windows assets to an IP address known to be a Cobalt Strike command-and-control server using a technique known as SSH tunneling. While Cobalt Strike is a legitimate penetration testing product, it is also used by threat actors to compromise networks.

The compromised server was observed using various known attacker tactics, techniques, and procedures (TTPs) to identify information sources and systems of interest and to perform suspicious and malicious actions in the customer's environment. These included ping sweeps to contact different IP addresses in the network and gather information as well as brute-force attacks against the FTP server, which is

Highlights

- Prompt investigation of incident
- Highly expeditious incident response
- Extensive after-hours support at peak of attack
- Detailed Incident Response Report provided to customer within 24 hours of initial contact

[1] https://www.securityweek.com/organizations-warned-of-royal-ransomware-attacks/

where an attacker uses multiple login and password combinations to crack login credentials.

The server was also observed searching for folders and shared drives on remote systems, scanning the web directory to discover files and networks, and initiating remote desktop protocol (RDP) connections to what appeared to be a laptop end-user host.

Solution

AT&T analysts served as vital first responders during the incident, quickly communicating the issue to Customer X and helping them accelerate their time to respond by providing recommendations on how to quarantine the attack and contain the damage.

AT&T analysts stayed in close communication with Customer X at the height of the attack, providing 24/7 support. As Customer X shared updates on which of its servers and services were impacted, the analysts gave detailed guidance on containment and remediation. This allowed Customer X to act quickly to contain the numerous affected hosts, reset the credentials for several accounts that were observed to have been used by attackers, and rebuild critical servers.

Within 24 hours of initial contact with Customer X, the AT&T team had issued Customer X a detailed report on the incident findings and provided recommendations to help protect against future ransomware attacks. The team also recommended actions to take for legal and compliance reasons and in the event that deeper post-incident forensic review is needed.

Customer X was also using AT&T's managed firewall services. This permitted the AT&T SOC team to provide multiple indicators of compromise (IOCs) including IP addresses and domains, which the AT&T Managed Firewall team blocked at the beginning of the investigation. These included:

- IP addresses that are known Cobalt Strike command-and-control servers
- Domains that were found to be newly registered
- Domains that had no traffic going back 90 days aside from to the compromised server.
- A free file hosting site that the compromised server was observed reaching out to, possibly to pull down malware or tools or upload staged data

Customer X was advised to continue working closely with the AT&T Managed Firewall team to review network firewall rules to prevent an attacker's lateral movement for internal only (i.e., "East/West") traffic and for external and internal (i.e., "North/South") traffic.

To protect against future attacks, AT&T analysts advised Customer X to:

- Replace EOL assets and software
- Routinely check assets for secure configurations
- Properly patch known vulnerabilities
- Use application whitelisting to prevent unknown applications from being executed in the environment
- Allow only known and approved remote access and management tools to be installed and executed

Because the attackers had compromised a domain controller, analysts also recommended that Customer X reset user credentials across the environment and closely monitor the environment for future findings. Additionally, since the attackers had access to the Customer X environment for a significant amount of time, AT&T analysts advised against Customer X restoring from recent backups and recommended instead rebuilding compromised or encrypted servers.

During the incident, AT&T analysts identified four new anomalous events. The AT&T Alien Labs threat intelligence team, which works in close collaboration with the AT&T SOC, has used these findings to develop four new, high-fidelity correlation rules that will generate alarms for similar anomalous activity across the AT&T Cybersecurity managed detection and response customer base.

These rules were subsequently deployed to the Customer X environment. Not only will they help protect the customer's fleet from similar attacks, but they will also help protect other AT&T Cybersecurity customers using the USM Anywhere platform.

> **"When the SOC identifies new patterns associated with malicious behavior, this is a win for all AT&T Cybersecurity customers because the Alien Labs threat intelligence team can use the insights to create new detections that will alarm on similar activity across our customer fleet."**
>
> **Santiago Cortes Diaz**
> Director, AT&T Alien Labs