CYBERSECURITY
& INFRASTRUCTURE
SECURITY AGENCY

Alert (PC20-050A)

Maelazzian Government Cyber Activity Targeting Emergency Services Sector of Critical Infrastructure

Original release date: November 10, 2020 | Last Revised: November 16, 2020

Systems Affected

- Enterprise Voice over IP (VoIP) telephony services

Overview

This joint Technical Alert (TA) is the result of analytic efforts between the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI). This alert provides information on Maelazzian government actions targeting U.S. emergency services sectors. It also contains indicators of compromise (IOCs) and technical details on the tactics, techniques, and procedures (TTPs) used by Maelazzian government cyber actors on compromised victim networks. DHS and FBI produced this alert to educate network defenders to enhance their ability to identify and reduce exposure to malicious activity.

DHS and FBI characterize this activity as a multi-stage intrusion campaign by Maelazzian government cyber actors who targeted 911 call centers' networks where they staged malware, conducted spear phishing, and gained remote access into energy sector networks. After obtaining access, the Maelazzian government cyber actors conducted network reconnaissance, moved laterally, and conducted denial of service (DoS) attacks against 911 call center systems.

Description

Since at least March 2020, Maelazzian government cyber actors—hereafter referred to as “threat actors”—targeted local, state, and federal government entities and multiple U.S. critical infrastructure sectors, including the energy, commercial facilities, water, emergency services, and critical manufacturing sectors.

Analysis by DHS and FBI, resulted in the identification of distinct indicators and behaviors related to this activity. Of note, the report Firefly: Western governments targeted by sophisticated attack group, released by US-CERT on September 6, 2020, provides additional information about this ongoing campaign.

This campaign comprises a distinct category of attack: the target is always government agencies which have remote access services exposed to the internet.

Technical Details

The threat actors in this campaign employed a variety of TTPs, including:

- credential gathering,
- open-source and network reconnaissance,
- host-based exploitation, and
- targeting emergency services electronic communication systems

Using Cyber Kill Chain for Analysis

DHS used the Lockheed-Martin Cyber Kill Chain model to analyze, discuss, and dissect malicious cyber activity. Phases of the model include reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on the objective. This section will provide a high-level overview of threat actors’ activities within this framework.

Stage 1: Reconnaissance

The threat actors appear to have deliberately chosen the organizations they targeted, rather than pursuing them as targets of opportunity. DHS analysis identified the threat actors accessing publicly available information hosted by organization-monitored networks during the reconnaissance phase. Based on forensic analysis, DHS assesses the threat actors sought information on network and organizational design and 911 system capabilities within organizations. These tactics are commonly used to collect the information needed for more targeted attacks. In some cases, information posted to company websites, especially information that may appear to be innocuous, may contain operationally sensitive information. As an example, the threat actors downloaded a small photo from a publicly accessible county government web page. The image, when expanded, was a high-resolution photo that displayed the 911 call center’s equipment models and status information in the background.

Additionally, the threat actors conducted extensive scans of federal, city, state, and local government IP blocks and subsequently attempted to remotely access infrastructure such as corporate web-based email, virtual private network (VPN) connections, and other telework services.

Stage 2: Weaponization

Developing custom attacks

Threat actors have been observed studying Common Vulnerabilities and Exposures (CVEs) related to software responsible for the operation 911 and electronic communications systems used by agencies in the emergency services sector. This has resulted in the development of custom attack TTPs based on recently disclosed vulnerabilities in this software.

Stage 3: Delivery

When compromising staging target networks, the threat actors leveraged shared credentials used by employees to login to emergency service systems. This attack has largely been successful due to poor cyber hygiene practices found within emergency service sector agencies, including password re-use, the use of weak passwords, and improperly secured SSH keys.

Stage 4: Exploitation

When exploiting the intended targets, the threat actors used remote access methods such as VPN, SSH, and other ports and protocols which were exposed to the internet to exploit the vulnerabilities which they previously discovered. Usually, exploitation occurred several days after the network scanning which took place in the reconnaissance phase.

Stage 5: Installation

The threat actors leveraged compromised credentials to access victims’ networks where multi-factor authentication was not used. To maintain persistence, the threat actors occasionally created local accounts within staging targets and placed malicious files within intended targets.

Password Cracking Tools

Consistent with the perceived goal of credential harvesting, the threat actors dropped and executed open source and free tools such as Hydra, SecretsDump, and CrackMapExec. The naming convention and download locations suggest that these files were downloaded directly from publicly available locations such as GitHub. Forensic analysis indicates that many of these tools were executed during the timeframe in which the actor was accessing the system.

Stage 6: Command and Control

DHS and FBI identified the threat actors leveraging remote access services and infrastructure such as VPN, RDP, and Outlook Web Access (OWA). The threat actors used the infrastructure of staging targets to connect to several intended targets.

Stage 7: Actions on Objectives

Targeting of emergency services Infrastructure

In multiple instances, the threat actors accessed workstations and servers on a network that contained communication systems utilized for dispatching emergency services. The threat actors accessed files pertaining to VoIP systems in order to ascertain where the Private Branch Exchange (PBX) or other call routing and control services were hosted. Based on DHS analysis of existing compromises, these files were named according to their function and were reference documents pertaining to the organization (e.g., “911 Dispatch System Diagram.pdf” or “Mobat Radio System Upgrade project quote.xlsx”).

Cleanup and Cover Tracks

In multiple instances, the threat actors created new accounts on the staging targets to perform cleanup operations. The accounts created were used to clear the following System logs: syslog, security logs, application logs, selinux, and kernel debug. The threat actors also removed applications they installed while they were in the network along with any command shell history.

Detection and Response

IOCs related to this campaign are provided within the accompanying .pdf and/or .doc files of this alert. DHS and FBI recommend that network administrators review the information provided, and add the appropriate countermeasures to their systems. The review, audit, and proper implementation of both host-based and network-based firewall rules would have, in many cases, slowed or stopped the threat actors’ attacks.

Network Signatures and Host-Based Rules

This section contains network signatures and host-based rules that can be used to detect malicious activity associated with threat actor TTPs. Although these network signatures and host-based rules were created using a comprehensive vetting process, the possibility of false positives always remains.

Network Signatures

The following is an example snort rule to detect a payload based on **CERT CC Vulnerability Note #123 DeadBeef DoS Attacks** which was leveraged by the threat actors against VoIP software used to dispatch Fire and EMS at a 911 call center:

```
alert tcp $EXTERNAL_NET any -> $HOME_NET $VOIP_PORTS (content:
"deadbeef"; offset:0; depth:8; msg: "VoIP DoS attack";)
```

Impact

This actors’ campaign has affected multiple organizations in the emergency services sectors.

Solution

DHS and FBI encourage network users and administrators to use the following detection and prevention guidelines to help defend against this activity.

Network and Host-based Firewalls

DHS and FBI recommend that network administrators review the configuration of all firewalls to determine that only authorized ports, protocols, and services are permitted within the network, and that services are not exposed to the internet unnecessarily. Reviewing network perimeter netflow will help determine whether a network has experienced suspicious activity. Network defenders should use the Snort signatures provided to identify malicious activity.

Detections and Prevention Measures

- Users and administrators may detect remote access activity by comparing all IP addresses and domain names listed in the IOC packages to the following locations:
    - network intrusion detection system/network intrusion protection system logs,
    - web content logs,
    - proxy server logs,
    - domain name server resolution logs,
    - packet capture (PCAP) repositories,
    - firewall logs,
    - workstation Internet browsing history logs,
    - host-based intrusion detection system /host-based intrusion prevention system (HIPS) logs,
    - data loss prevention logs,
    - exchange server logs,
    - user mailboxes,
    - mail filter logs,
    - mail content logs,
    - AV mail logs,
    - OWA logs,
    - Blackberry Enterprise Server logs, and

    - Mobile Device Management logs.
- To detect the presence unauthorized access on external-facing servers, compare IP addresses, filenames, and file hashes listed in the IOC packages with the following locations:
    - application logs,
    - IIS/Apache logs,
    - file system,
    - intrusion detection system/ intrusion prevention system logs,
    - PCAP repositories,
    - firewall logs, and
    - reverse proxy.
- Detect evasion techniques by the actors by identifying deleted logs. This can be done by reviewing last-seen entries and by searching for event 104 on Windows system logs, and by implementing a security information event management tool or more simplistically, a remote syslog server in Linux/Unix environments.
- Detect persistence by reviewing all administrator accounts on systems to identify unauthorized accounts, especially those created recently.
- Detect the malicious use of legitimate credentials by reviewing the access times of remotely accessible systems for all users. Any unusual login times should be reviewed by the account owners.
- Detect the malicious use of legitimate credentials by validating all remote desktop and VPN sessions of any user’s credentials suspected to be compromised.
- Detect installation by searching all proxy logs for downloads from URIs without domain names.

General Best Practices Applicable to this Campaign:

- Restrict external communication of all unnecessary services.
- Monitor VPN logs for abnormal activity (e.g., off-hour logins, unauthorized IP address logins, and multiple concurrent logins).
- Deploy web and email filters on the network. Configure these devices to scan for known bad domain names, sources, and addresses; block these before receiving and downloading messages. This action will help to reduce the attack surface at the network’s first level of defense. Scan all emails, attachments, and downloads (both on the host and at the mail gateway) with a reputable anti-virus solution that includes cloud reputation services.
- Segment any critical networks or control systems from business systems and networks according to industry best practices.
- Ensure adequate logging and visibility on ingress and egress points.
- Establish a training mechanism to inform end users on proper password and credential management.
- End users should have clear instructions on how to report unusual or suspicious activity observed on their computer systems.

- Block RDP, VPN and SSH connections originating from untrusted external addresses unless an exception exists; routinely review exceptions on a regular basis for validity.
- Store system logs of mission critical systems for at least one year within a security information event management tool.
- Ensure applications are configured to log the proper level of detail for an incident response investigation.
- Consider implementing HIPS or other controls to prevent unauthorized code execution.
- Establish least-privilege controls.
- Establish a password policy to require complex passwords for all users.
- Ensure that accounts for network administration do not have external connectivity.
- Ensure that network administrators use non-privileged accounts for email and Internet access.
- Use two-factor authentication for all authentication, with special emphasis on any external-facing interfaces and high-risk environments (e.g., remote access, privileged access, and access to sensitive data).
- Implement a process for logging and auditing activities conducted by privileged accounts.
- Enable logging and alerting on privilege escalations and role changes.
- Periodically conduct searches of publicly available information to ensure no sensitive information has been disclosed. Review photographs and documents for sensitive data that may have inadvertently been included.
- Assign sufficient personnel to review logs, including records of alerts.
- Complete independent security (as opposed to compliance) risk review.
- Create and participate in information sharing programs.
- Create and maintain network and system documentation to aid in timely incident response. Documentation should include network diagrams, asset owners, type of asset, and an incident response plan.

Report Notice

DHS encourages recipients who identify the use of tools or techniques discussed in this document to report information to DHS or law enforcement immediately. To request incident response resources or technical assistance, contact NCCIC or the FBI through a local field office.

References

CERT CC Vulnerability Note #123