MANDIANT
NOW PART OF Google Cloud

THREAT INTELLIGENCE
WHITE PAPER

Establishing Resilience Against Edge Device Attacks

The content in this document was originally published in The Defender's Advantage Cyber Snapshot Issue 4.

Over the past 10 years, organizations have increased visibility throughout their digital environments. As a result, they are detecting attackers faster[1] and have made significant progress in proactively securing their environments from threats like password reuse and brute force attacks as they continue to move towards defense in depth style architecture.

While this trend progresses in the right direction, most organizations center detection and response around the visibility provided by their endpoint detection and response (EDR) solutions. However, EDR solutions are deployed, as the name implies, on endpoints. In other words, firewalls, IOT devices, VPNs, hypervisors, and many other devices are not typically supported by EDR, and are therefore commonly referred to as "edge devices." What happens when malicious actors start targeting those devices?

Because edge devices by definition sit outside the typical detection range of most organizations, they provide attackers with enormous value during intrusions. Edge devices will always be targets to adversaries, just in different ways. These edge devices provide many valuable services to organizations such as monitoring internal security tools, but historically have not been supported by EDR solutions and are rarely monitored at the system level. This type of system-level monitoring is needed to identify if code changes or targeted malware is installed.

Edge devices are leveraged for security hunting and protection and are not inherently protected themselves. More to the point, vendors typically do not enable direct access to the operating system or filesystem for users. Because detections aren't extended to these edge devices and systems, defenders are limited in their capacity to perform analysis into underlying, potentially anomalous behavior.

Over the past five years, Mandiant has seen increasing evidence to suggest nation-backed adversaries are targeting edge devices. This focus on edge devices is as concerning for defenders as it is advantageous for attackers. Malicious intrusions are targeting edge devices likely to gain a foothold or maintain persistence in the target environment. Beyond a simple foothold, edge devices offer malicious actors a host of advantages. First among them being that edge devices have elevated visibility and privileges within the environment to provide network monitoring or a secure point of access. Access to these devices also allows the attacker to control the timing of the operation and can reduce the chances of detection. Edge devices, by definition, are not visible to EDR solutions, meaning that all these advantages are conferred on attacks as well as the ability to remain hidden from defenders.

Nation-backed adversaries often dedicate considerable time and effort for extensive research and development cycles to identify and create exploits for previously unknown vulnerabilities. Mandiant has investigated dozens of intrusions over the years where suspected China-nexus groups have exploited zero-day vulnerabilities and deployed custom malware to steal user credentials and maintain long-term access to the victim environments. For example in 2022, UNC3886 targeted edge devices such as firewalls and later in the attack life cycle, hypervisor technologies.

[1] M-Trends 2023, Mandiant April 2023

UNC3886 Case Study

Multiple components of the Fortinet[2] ecosystem were targeted by UNC3886 before they moved laterally to VMWare infrastructure. These components and their associated versions, at the time of compromise, are listed as follows:

- **FortiGate: 6.2.7** – FortiGate units are network firewall devices which allow for the control and monitoring of network traffic passing through the devices.
- **FortiManager 6.4.7** – The FortiManager acts as a centralized management platform for managing Fortinet devices.
- **FortiAnalyzer 6.4.7** – The FortiAnalyzer acts as a centralized log management solution for Fortinet devices as well as a reporting platform.

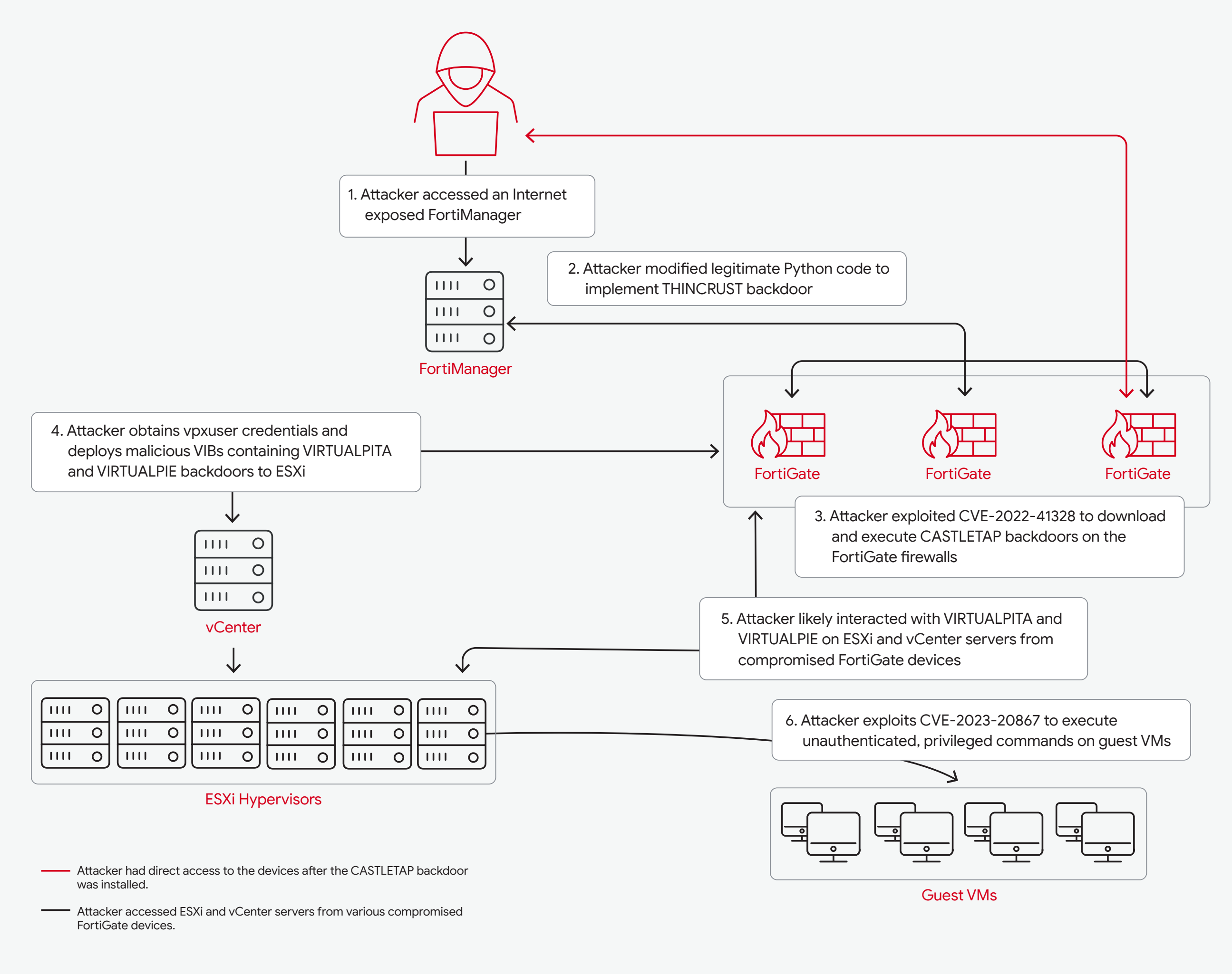
1. Attacker accessed an Internet exposed FortiManager
2. Attacker modified legitimate Python code to implement THINCRUST backdoor
FortiManager
4. Attacker obtains vpxuser credentials and deploys malicious VIBs containing VIRTUALPITA and VIRTUALPIE backdoors to ESXi
FortiGate
FortiGate
FortiGate
3. Attacker exploited CVE-2022-41328 to download and execute CASTLETAP backdoors on the FortiGate firewalls
vCenter
5. Attacker likely interacted with VIRTUALPITA and VIRTUALPIE on ESXi and vCenter servers from compromised FortiGate devices
6. Attacker exploits CVE-2023-20867 to execute unauthenticated, privileged commands on guest VMs
ESXi Hypervisors
Guest VMs
Attacker had direct access to the devices after the CASTLETAP backdoor was installed.
Attacker accessed ESXi and vCenter servers from various compromised FortiGate devices.

FIGURE 1: Activity after internet access restrictions implemented to FortiManager

[2] https://www.mandiant.com/resources/blog/fortinet-malware-ecosystem

In 2022, Mandiant began tracking UNC3886, a group with a suspected China-nexus. This group specifically targeted the Fortinet ecosystem and eventually moved laterally to access VMWare Infrastructure within targeted environments. To gain this access, UNC3886 proved to have sufficient knowledge of multiple Fortinet solutions including FortiGate (firewall), FortiManager (centralized management solution), and FortiAnalyzer (log management, analytics and reporting platform). With this knowledge, UNC3886 deployed a backdoor, tracked by Mandiant as **THINCRUST**, across FortiManager and FortiAnalyzer devices to gain persistence. Then UNC3886 leveraged access to FortiManager native scripts to exploit CVE-2022-41328 to download and execute another backdoor, **CASTLETAP**, across FortiGate devices to further maintain access within the environment.

Mandiant observed SSH connections from the Fortinet devices to ESXi servers within the target environment followed by the installation of vSphere Installation Bundles[3] that contained **VIRTUALPITA** and **VIRTUALPIE** backdoors.

In another scenario, where the FortiManager was restricted from the internet, UNC3886 leveraged previously established access to install a network traffic redirection utility Mandiant tracks as **TABLEFLIP**, and a reverse shell backdoor variant of **REPTILE**, on the FortiManager. This combined use of malware allowed UNC3886 to circumvent network access control lists (ACLs) in place to restrict external access.

In both of these scenarios, malicious activity was detected following a full compromise of both the Fortinet ecosystem and the VMware hypervisor, once UNC3886 began performing reconnaissance commands and exfiltrating data using legitimate system processes.

For a detailed account of this case study, please refer to: the blog "Fortinet Zero-Day and Custom Malware Used by Suspected Chinese Actor in Espionage Operation".

CASTLETAP is a Linux binary that passively listens for packets and activates the backdoor functionality when it receives an ICMP Echo packet. Within these packets, the malware also searches for C2 server information that it can connect back to over SSL socket. Its capabilities include uploading and downloading files, spawning normal, and busybox-based shell.

THINCRUST is a Python backdoor embedded in a third-party library code that allows remote command execution, reading, and writing files via HTTP requests. The encrypted commands are stored in HTTP cookies.

VIRTUALPITA is a 64-bit passive backdoor for Linux and VMware ESXi that creates a listener on a hardcoded TCP or VMCI port numbers. It supports arbitrary command execution, file upload and download, and the ability to start and stop vmsyslogd.

VIRTUALPIE is a backdoor written in Python that spawns a demonized IPv6 listener on a hardcoded TCP port. It supports file transfer, arbitrary command execution, and reverse shell capabilities. It communicates using a custom protocol and the data is encrypted using RC4.

TABLEFLIP is a Linux utility that performs traffic redirection. It passively listens on all active interfaces for specialized command packets. These packets contain XOR encoded IP address and port number to redirect traffic to using iptable commands.

REPTILE is a publicly available Linux rootkit written in C. It supports backdoor functionality which can be activated through ICMP, UDP or TCP packets via port-knocking. Additional capabilities include reverse shell and file transfer.

[3] https://blogs.vmware.com/vsphere/2011/09/whats-in-a-vib.html

APT29 Case Study

Mandiant has also observed nation-backed actors, like APT29, targeting similar types of edge device appliances with a novel tunneler.

In early 2022, after gaining access to the target environment, APT29 deployed **QUIETEXIT** to endpoints throughout the environment. In one case, APT29 hijacked legitimate application specific startup scripts to enable **QUIETTEXT** to run at startup, as it does not have native persistent mechanisms. **QUIETEXIT** supports full SSH functionality and APT29 leveraged a SOCKS tunnel into the target environment. This allowed APT29 to execute tools to steal data with little to no evidence on the target computer. APT29 targeted network attached storage (NAS) masquerading the binary name to blend in with legitimate files on the file system. To maintain additional access, APT29 deployed a secondary backdoor, **REGEORG** web shell, on a DMZ web server. This, combined with a lack of supported anti-virus or EDR solutions, aided in a prolonged dwell time.

QUIETEXIT is a reverse SSH tunneler that connects out to a remote C2, but requires a password to authenticate. QUIETEXIT can execute commands or proxy traffic via SOCKS. QUIETEXIT is derived from the open source DROPBEAR SSL client-server software.

REGEORG is an open-source utility used to tunnel webshell traffic.

QUIETEXIT. Mandiant observed command and control (C2) systems were primarily legacy conference room camera systems, which were likely infected with the server component of QUIETTEXT. By targeting these trusted systems, APT29 remained undetected in target environments for at least 18 months.

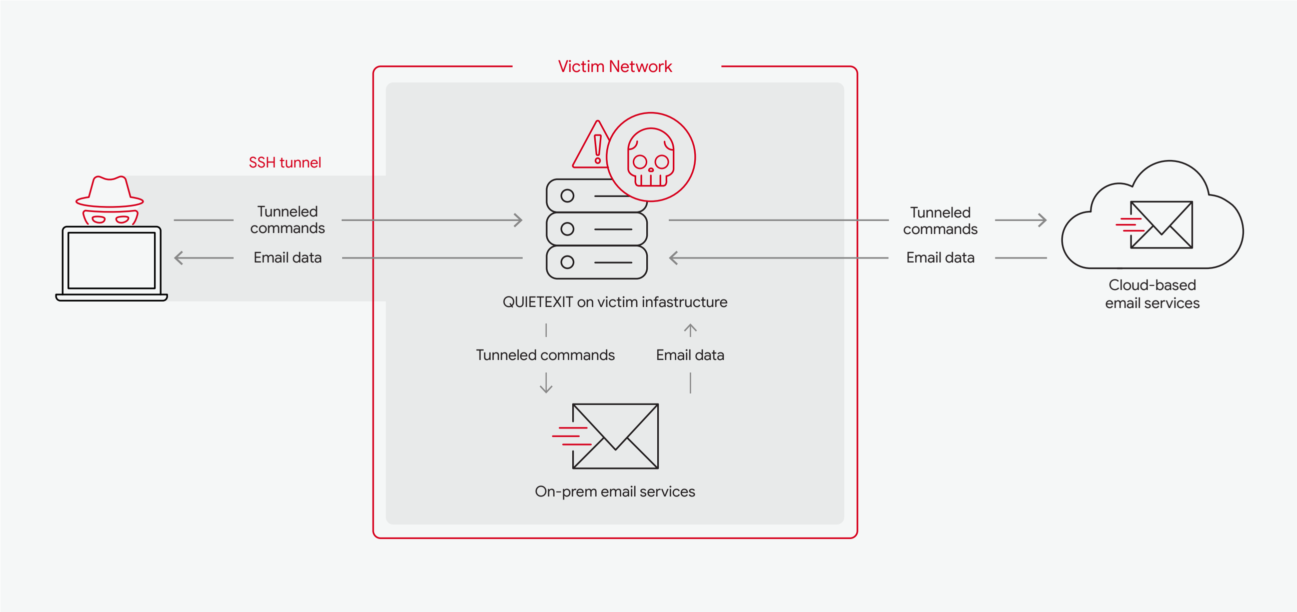

FIGURE 2: Tunneling though QUIETTEXIT

Completing the mission, APT29 successfully obtained privileged credentials to the target's email environment and focused efforts on executive teams and employees who work with corporate development, mergers and acquisitions, or the IT security staff. In some cases, APT29 leveraged the same eDiscovery and Graph API tools used to perform programmatic searching and access to email data that investigators use to conduct response efforts. These tools allowed APT29 to conduct bulk email exfiltration.

For a detailed account of this case study, please refer to: the blog
"Eye Spy on Your Email".

APT28 Case Study

In 2022, Mandiant observed APT28 deviate from historic activity. This group demonstrated a preference towards compromising edge infrastructure to conduct a variety of operations, a technique referred to as "Living on the Edge." Since the outset of the war in Ukraine, the Russian Military Intelligence, or known as the GRU, has attempted to conduct successive and almost constant campaigns of cyber espionage and disruption aimed against key services and organizations within Ukraine. This balance of access to and actions against target organizations relies on the compromise of edge infrastructure such as routers and other internet connected devices.

For a detailed account of this case study, please refer to:
M-Trends 2023, "The Invasion of Ukraine: Cyber Operations During Wartime".

Key takeaways

In these case studies, evidence of compromise was detected within the environment during post exploitation activity, as by design, actors target edge networks to remain undetected. During the investigations, Mandiant conducted thorough reviews of impacted systems to identify the initial entry vector. In these cases, evidence existed to trace access back to edge device IP addresses. This led investigators down the path of working with vendors to collect forensic images of these devices to perform further analysis. Cross organizational communication and collaboration is key to providing both manufacturers with early notice of new attack methods in the wild before they are made public and investigators with expertise to better shed light on these new attacks.

What you can do to protect against these attacks

Cyber espionage related actors have increased their investment in research and development of tooling and exploits against systems that do not generally support EDR. These types of tooling and exploits require a deep understanding of the targeted operating systems. While organizations continue to build out security operations centers (SOCs), organizations should also continue to expand visibility further than endpoint detection. Visibility gaps allow threat actors to evade detection with minimal effort. Determining those visibility gaps is the next step to build an efficient SOC to support the security of the organization. Organizations should inventory devices on the network and evaluate if monitoring tools are available for each. Each device that does not support monitoring tools likely has vendor-specific hardening actions to ensure proper logging is enabled. Organizations should also ensure that these vendor-specific logs are forwarded to a central repository. Utilizing network access controls to limit or completely restrict egress traffic from these devices should also be evaluated. Implementing additional network monitoring and hunting for anomalous traffic to and from edge devices and other non-EDR enabled technologies allows further detection capabilities if these network controls are not feasible.

For additional resources please refer to the following:

Mandiant's Microsoft 365 Hardening Guide

Detection and Hardening within ESXi Hypervisors

Read more articles from **The Defender's Advantage Cyber Snapshot**.

Mandiant
11951 Freedom Dr, 6th Fl, Reston, VA 20190
(703) 935-1700
833.3MANDIANT (362.6342)
info@mandiant.com

About Mandiant
Mandiant is a recognized leader in dynamic cyber defense, threat intelligence and incident response services. By scaling decades of frontline experience, Mandiant helps organizations to be confident in their readiness to defend against and respond to cyber threats. Mandiant is now part of Google Cloud.

MANDIANT® NOW PART OF Google Cloud