Revisiting UNC3886 Tactics to Defend Against Present Risk

Published: 2025-07-28 · Archived: 2026-04-05 15:07:10 UTC

APT & Targeted Attacks

We examine the past tactics used by UNC3886 to gain insight on how to best strengthen defenses against the ongoing and emerging threats of this APT group.

By: Cj Arsley Mateo, Ieriz Nicolle Gonzalez, Jacob Santos, Paul John Bardon, Angelo Junio, Rayven Cervantes
Jul 28, 2025 Read time: 8 min (2193 words)

Key Takeaways

- UNC3886 is an APT group that has historically targeted critical infrastructure, including telecommunications, government, technology, and defense, with a recent attack against Singapore.
- The group is known for rapidly exploiting zero-day and high-impact vulnerabilities in network and virtualization devices such as VMware vCenter/ESXi, Fortinet FortiOS, and Juniper Junos OS.
- UNC3886 deploys custom toolsets including TinyShell (a covert remote access tool) and Reptile (a stealthy Linux rootkit), and Medusa, leveraging layered persistence and advanced defense evasion methods such as rootkit deployment, living-off-the-land tactics, and replacement/backdooring of core system binaries.
- Trend Vision One™ detects and blocks the indicators of compromise (IOCs) highlighted in this blog. Trend Vision One customers can also access hunting queries, threat insights, and threat intelligence reports to gain rich context and the latest updates on UNC3886.

On July 18, Singapore's Coordinating Minister for National Security K. Shanmugam revealed that the country was facing a highly sophisticated threat actoropen on a new tab targeting critical infrastructure—UNC3886. First reportedopen on a new tab in 2022, this advanced persistent threat (APT) group has been targeting essential services in Singapore, posing a severe risk to their national security.

In this entry, we draw on observations and the tactics, techniques, and procedures (TTPs) from previously recorded UNC3886 attacks. Our aim is to get a good understanding of this threat group and enhance overall defensive posture against similar tactics.

An overview of UNC3886

UNC3886 is a cyber espionage group whose targets include the US, Europe, and Singapore, where it currently represents a significant threat. Known for its persistent attack methods, the group homes in on critical sectors such as government, telecommunications, technology, defense, energy, and utilities. While first reported in 2022, there have been evidence of its activity dating back to late 2021open on a new tab.

The Cyber Security Agency (CSA) of Singapore has been actively investigating UNC3886's activities and monitoring all critical service sectors. The group's activities have been detected in parts of Singapore's critical

information infrastructure that power essential services, highlighting the severe threat they pose to national security. Although the specific sectors affected have not been disclosed, the agency has emphasized the need to preserve operational security by not disclosing further information at this stage.

Tactics, Techniques and Procedures (TTPs)

UNC3886 operates using advanced techniques and primarily targets network devices, virtualization systems (e.g. VMware vCenter/ESXi, Fortinet FortiOS, and Juniper Junos OS), and critical information infrastructure. The group is also known for using zero-day exploits and deploying custom open-source malware specifically developed to evade detection and maintain persistence within the target networks. Additionally, UNC3886 leverages tools already present on the victim's system to further evade detection.

Even when detected and removed, the group is persistent and often attempts re-entry into the network. The group's attack chain involves several advanced techniques including:

- Exploiting public-facing applications for initial access (T1190)
- Using valid accounts for persistence (T1078)
- Employing remote access tools (T1219) and application layer protocols (T1071) for command and control.

This combination of advanced and persistent techniques with strategic targets makes UNC3886 a group that warrants heightened vigilance. Its past activities offer insight into the group’s capabilities, tools, as well as effective defenses that could derail their operation.

We take a closer look at the techniques, vulnerabilities, and other tactics UNC3886 have used in the past to get an idea of what could still be their current operations.

TACTIC	TECHNIQUE
Initial Access (TA0001)	T1190: Exploit Public-Facing Application
Execution (TA0002)	T1203: Exploitation for Client Execution
	T1059.004: Command and Scripting Interpreter: Unix Shell
	T1059.008: Command and Scripting Interpreter: Network Device CLI
Persistence (TA0003)	T1547: Boot or Logon Autostart Execution
	T1078: Valid Accounts
Privilege Escalation (TA0004)	T1078: Valid Accounts
	T1601: Modify System Image
	T1562.003: Impair Defenses: Impair Command History Logging
Defense Evasion (TA0005)	T1036.005: Masquerading: Match Legitimate Resource Name or Location

TACTIC	TECHNIQUE
	T1055.009: Process Injection: Proc Memory
	T1140: Deobfuscate/Decode Files or Information
	T1014: Rootkit
	T1027: Obfuscated Files or Information
	T1601: Modify System Image
	T1562.003: Impair Defenses: Impair Command History Logging
Credential Access (TA0006)	T1003: OS Credential Dumping
	T1056: Input Capture
Lateral Movement (TA0008)	T1563.001: Remote Service Session Hijacking: SSH Hijacking
Collection (TA0009)	T1074: Data Staged
Exfiltration (TA0010)	T1041: Exfiltration Over C2 Channel
Command and Control (TA0011)	T1573: Encrypted Channel
	T1090: Proxy
	T1205.002: Traffic Signaling: Socket Filters
	T1219: Remote Access Tools
	T1071: Application Layer Protocol

Table 1. Summary of UNC3886 TTPs

Malware and rootkits

As mentioned earlier, UNC3886 have used open-source custom malware designed for stealth and persistence, and often use legitimate tools found on compromised hosts to evade detection. The group's use of TinyShell, Reptile, and Medusa are indicative of its advanced capabilities, showcasing their ability to develop and deploy sophisticated tools tailored for Linux environments. Trend™ Research analyzed and revisited the malware and rootkits used by the group, to get a better understanding of how they operate.

TinyShell

TinyShell is a lightweight, Python-based remote access tool (RAT) or backdoor. It provides threat actors with remote command execution over HTTP/HTTPS and simple, encrypted communications, making it well-suited for stealthy operations. The use of TinyShell by UNC3886 demonstrates a focus on lightweight, agile attack tools that are highly effective in targeted, post-exploitation operations.

Reptile Linux rootkit

UNC3886 uses the Reptile Linux rootkit, which operates at the kernel level. This rootkit's core capabilities include hiding files, processes, and network activity. It can also provide attackers with a hidden backdoor, allowing them to regain access to a compromised system even if other access methods are discovered and removed. Notably, Reptile is often used in attacks to establish a persistent and stealthy foothold in the targeted system. It features functionalities such as port knocking (a method to secretly open ports by sending a specific sequence of connection attempts) and the ability to execute commands with root privileges.

Installation:

During the installation process the rootkit prompts what capabilities should be enabled, as seen below:

```
└─# make config
make[1]: Entering directory '/root/Reptile'
/root/Reptile/scripts/kconfig/conf --oldaskconfig Kconfig
*
* Reptile's configuration
*
*
* Chose the features you wanna enable
*
Backdoor (CONFIG_BACKDOOR) [Y/n] y
  *
  * Backdoor configuration
  *
  Magic value to magic packets (MAGIC_VALUE) [hax0r]
  Backdoor password (PASSWORD) [s3cr3t]
  Source port of magic packets (SRCPORT) [666]
  *
  * END
  *
Hide specific file contents (CONFIG_FILE_TAMPERING) [Y/n] y
  *
  * Name used in file tampering tags
  *
  Tag name that hide file contents (TAG_NAME) [reptile]
  *
  * END
  *
Hide process (CONFIG_HIDE_PROC) [Y/n] y
Hide files and directories (CONFIG_HIDE_DIR) [Y/n] y
*
* Hide name (needed to create Reptile's folder)
*
Hide name (HIDE) [reptile]
*
* END
*
Hide TCP and UDP connections (CONFIG_HIDE_CONN) [Y/n] y
Hide kernel module itself (CONFIG_AUTO_HIDE) [Y/n] y
Enable give root to a process run by an unprivileged user (CONFIG_GIVE_ROOT)
[Y/n] y
Would you like to launch the reverse shell daemon on start? (CONFIG_RSHELL_ON
_START) [Y/n] n
#
# configuration written to .config
#
make[1]: Leaving directory '/root/Reptile'
```

Figure 1. Configuration setup for the Reptile rootkit

Capabilities:

Reptile rootkit uses multiple script files to build a single executable using the “CMake” tool on Linux machines.

- Hide process: the rootkit can hide process by checking task flags and changing them. This can be done using PID or Filename as input.
- Hide directory: the rootkit can hide directories by changing flags.
- File content tampering: rootkit has the capability to tamper/change file content.
- Hide connections: the rootkit has the capability to hide/unhide connections done via a list system. The rootkit creates a list of network connections that are then hidden.
- Backdoor: if the backdoor capability is initialized during installation the following config are created automatically. The backdoor can execute commands using this credential and connections.
- Encrypt: the rootkit can be used to encrypt files using a randomly generated key.

Medusa rootkit

Medusa is another kernel-level rootkit specifically designed for Linux systems, that has been reportedly used by UNC3886 alongside Reptile. Similar to Reptile, its primary functions include hiding malicious activities, such as processes, files, and network connections, from administrators and security tools.

By operating within the kernel, Medusa can intercept system calls and manipulate their output, effectively cloaking the presence of other malware and the attacker's actions. Most notably, Medusa is used in maintaining covert persistence on compromised Linux servers, allowing UNC3886 to operate undetected for extended periods. It is often used in conjunction with other tools to facilitate command and control (C&C) communication and data exfiltration.

Capabilities:

- PAM Backdoor: Hook libpam authentication system calls for persisting with a hidden root user
- Process Hiding: Hooks rootkit can intercept the 'kill' function to prevent the user from terminating the rootkit process. By hiding itself from the system, the rootkit can remain undetected and achieve persistence on the system.
- File Hiding: Hooks 'stat' and 'readdir' to hide files and directories.
- Network Hiding: Hooks the 'getaddrinfo' function to filter out addresses of remote hosts that it wants to hide. By using these techniques, the rootkit can effectively hide network activity from the user and other programs.
- Anti-Debugging: Also Hooks 'kill' system call can be intercepted to prevent the debugger from sending signals to the rootkit process. By evading debugging, the rootkit can make it more difficult for security researchers to discover and analyze its behavior.
- Auth Logging: Hooks pam_prompt(), pam_vprompt and pam_syslog to log all successful authentications locally, or remotely via SSH to Medusa home directory
- Execution Logging : Hooks syslog() and pam_syslog to log all successful authentications locally, or remotely via SSH to Medusa home directory

MopSled

MopSled is a modular, shellcode-based backdoor capable of communicating with its C&C server over HTTP or a custom binary protocol via TCP. Its core functionality centers around extending its capabilities by downloading and executing plugins from the C&C server. Additionally, MOPSLED employs a custom implementation of the ChaCha20 encryption algorithm to decrypt both embedded and external configuration files.

RifleSpine

RifleSpine is a cross-platform backdoor that uses Google Drive for file transfer and command execution. It employs the CryptoPP library to implement the AES encryption algorithm, securing data transmitted between the compromised system and the threat actor.

CastleTap

CastleTap is a passive backdoor that targets FortiGate firewalls, disguised as the legitimate file '/bin/fgfm' to mimic the authentic 'fgfmd' service. The malware activates when it detects specially crafted ICMP packets containing specific magic strings, then establishes an encrypted SSL connection to a command-and-control server. Once connected, CastleTap provides attackers with comprehensive remote access capabilities including file upload/download, command shell access, and persistent control over the compromised firewall system.

Known CVEs used

The common thread among the CVEs used by the group is that they target highly privileged, broadly deployed, often-overlooked systems to enable impactful techniques (RCE, privilege escalation, persistence, lateral movement). This aligns with the APT group’s goal to maximize stealth, impact, and persistence in high-value targets.

Organizations are advised to apply the latest vendor patches for the CVEs used by UNC3886. Based on their reported past activitiesopen on a new tab, we list them here:

1. CVE-2023-34048open on a new tab
    - vCenter Server contains an out-of-bounds write vulnerability in the implementation of the DCERPC protocol. A malicious actor with network access to vCenter Server may trigger an out-of-bounds write potentially leading to remote code execution.
    - The exploitation enables unauthenticated remote command execution on vulnerable vCenter servers. Mandiant observed deployment of attacker backdoors minutes after crashing of the vulnerable VMware service.
2. CVE-2022-41328open on a new tab
    - An improper limitation of a pathname to a restricted directory vulnerability ('path traversal') [CWE-22] in Fortinet FortiOS version 7.2.0 through 7.2.3, 7.0.0 through 7.0.9 and before 6.4.11 allows a privileged attacker to read and write files on the underlying Linux system via crafted CLI commands.
    - In FortiOS was exploited to download and execute backdoors on FortiGate devices.
3. CVE-2022-22948open on a new tab
    - The vCenter Server contains an information disclosure vulnerability due to improper permission of files. A malicious actor with non-administrative access to the vCenter Server may exploit this issue

to gain access to sensitive information.
    - In VMware vCenter was exploited to obtain encrypted credentials in the vCenter's postgresDB for further access.
4. CVE-2023-20867open on a new tab
    - A fully compromised ESXi host can force VMware Tools to fail to authenticate host-to-guest operations, impacting the confidentiality and integrity of the guest virtual machine.
    - In VMware Tools was exploited to execute unauthenticated Guest Operations from ESXi host to guest virtual machines.
5. CVE-2022-42475open on a new tab
    - Allows a remote unauthenticated attacker to execute arbitrary code or commands via specifically crafted requests.
6. CVE-2025–21590open on a new tab
    - A security flaw involving insufficient system separation in Juniper Networks Junos OS kernel permits an authenticated local user with administrative rights to damage device security. An attacker who gains shell-level access can insert malicious code that may lead to full system compromise. This vulnerability cannot be triggered through the Junos command-line interface and is limited to Junos OS platforms.
7. Bring Your Own SSH Server (BYOSSH)
    - Beyond deploying backdoored SSH binaries to harvest credentials, the threat actor was also observed using the MEDUSA rootkit to install a custom SSH server, serving the same malicious purpose.

Proactive security with Trend Vision One™

Trend Vision One™products is the only AI-powered enterprise cybersecurity platform that centralizes cyber risk exposure management, security operations, and robust layered protection. This comprehensive approach helps you predict and prevent threats, accelerating proactive security outcomes across your entire digital estate. With Trend Vision One, you’re enabled to eliminate security blind spots, focus on what matters most, and elevate security into a strategic partner for innovation.

Trend protection rules and filters

TippingPoint

- 42855: HTTP: Fortinet FortiOS Heap Buffer Overflow Vulnerability CVE-2022-42475
- 44482: File Propagation Filter for Trojan.Linux.EfPSixSSH.A
- 45162: C2 filter for Trojan.Linux.Tableflip.A
- 45756: C2 filter for TinyShell/Backdoor.Linux.Lmpad.A
- 45768: File Propagation Filter for TinyShell/Backdoor.Linux.Jdosd.A
- 45770: C2 filter for TinyShell / Backdoor.Linux.Irad.A

Deep Discovery Inspector (DDI)

- 4525: CVE-2021-21972 - VSPHERE RCE EXPLOIT - HTTP (REQUEST)

Trend Vision One™ Threat Intelligence

To stay ahead of evolving threats, Trend customers can access Threat Insightsproducts which provide the latest insights from Trend Research on emerging threats and threat actors.

Threat Insights

Emerging Threats: Advanced Threat Actors on the Rise: UNC3886's Persistent Operations Revealed

Hunting Queries

Trend Vision One Search App

Trend Vision One customers can use the Search App to match or hunt the malicious indicators mentioned in this blog post with data in their environment.

UNC3886 APT detection

malName:*TINYSHELL* AND eventName:MALWARE_DETECTION AND LogType: detection

More hunting queries are available for Trend Vision One customers with Threat Insights entitlement enabled.

Indicators of Compromise (IoCs)

The indicators of compromise for this entry can be found here.

Tags
