

Re-Checking Your Pulse: Updates on Chinese APT Actors Compromising Pulse Secure VPN Devices

fireeye.com/blog/threat-research/2021/05/updates-on-chinese-apt-compromising-pulse-secure-vpn-devices.html



Threat Research

Dan Perez, Sarah Jones, Greg Wood, Stephen Eckels, Emiel Haeghebaert

May 27, 2021

19 mins read

Advanced Persistent Threats (APTs)

Threat Actors

On April 20, 2021, Mandiant published detailed results of our investigations into [compromised Pulse Secure devices by suspected Chinese espionage operators](#). This blog post is intended to provide an update on our findings, give additional recommendations to network defenders, and discuss potential implications for U.S.-China strategic relations.

- Mandiant continues to gather evidence and respond to intrusions involving compromises of Pulse Secure VPN appliances at organizations across the defense, government, high tech, transportation, and financial sectors in the U.S. and Europe (Figure 1).
- Reverse engineers on the FLARE team have identified four additional code families specifically designed to manipulate Pulse Secure devices.
- We now assess that espionage activity by UNC2630 and UNC2717 supports key Chinese government priorities. Many compromised organizations operate in verticals and industries aligned with Beijing's strategic objectives outlined in China's recent 14th Five Year Plan.
- While there is evidence of data theft at many organizations, we have not directly observed the staging or exfiltration of any data by Chinese espionage actors that could be considered a violation of the Obama-Xi [agreement](#).
- Mandiant Threat Intelligence assesses that Chinese cyber espionage activity has demonstrated a higher tolerance for risk and is less constrained by diplomatic pressures than previously characterized.


 Organizations with compromised Pulse Secure devices by vertical and geographic location

Figure 1: Organizations with compromised Pulse Secure devices by vertical and geographic location

Pulse Secure continues to work closely with Mandiant, affected customers, government partners, and other forensic experts to address these issues. Pulse Secure's parent company, Ivanti, has released patches to proactively address software vulnerabilities and issued updated [Security Advisories](#) and [Knowledge Articles](#) to assist customers. (Please see the Forensics, Remediation, and Hardening Guidelines section for additional details.)

UNC2630 and UNC2717 Tradecraft and Response to Disclosure

Mandiant is tracking 16 malware families exclusively designed to infect Pulse Secure VPN appliances and used by several cyber espionage groups which we believe are affiliated with the Chinese government. Between April 17 and April 20, 2021, Mandiant incident responders observed UNC2630 access dozens of compromised devices and remove webshells like ATRIUM and SLIGHTPULSE.

- Under certain conditions, the Integrity Checker Tool (ICT) will show no evidence of compromise on appliances which may have had historical compromise. This false negative may be returned because the ICT cannot scan the rollback partition. If a backdoor or persistence patcher exists on the rollback partition and a Pulse Secure appliance is rolled back to the prior version, the backdoor(s) will be present on the appliance. Please see the Forensics, Remediation, and Hardening Guidelines section for important information regarding the ICT and upgrade process.
- In at least one instance, UNC2630 deleted their webshell(s) but did not remove the persistence patcher, making it possible to regain access when the device was upgraded. The remaining persistence patcher causes the malicious code to be executed later during a system upgrade, re-inserts webshell logic into various files on the appliance, and recompromises the device.
- It is unusual for Chinese espionage actors to remove a large number of backdoors across several victim environments on or around the time of public disclosure. This action displays an interesting concern for operational security and a sensitivity to publicity.

Both UNC2630 and UNC2717 display advanced tradecraft and go to impressive lengths to avoid detection. The actors modify file timestamps and regularly edit or delete forensic evidence such as logs, web server core dumps, and files staged for exfiltration. They also demonstrate a deep understanding of network appliances and advanced knowledge of a targeted network. This tradecraft can make it difficult for network defenders to establish a complete list of tools used, credentials stolen, the initial intrusion vector, or the intrusion start date.

Updates from Incident Response Investigations

We continue to suspect that multiple groups including UNC2630 and UNC2717 are responsible for this activity, despite the use of similar exploits and tools. There is a high degree of variation in attacker actions within victim environments, with actors inconsistently using a combination of tools and command and control IP addresses.

Reverse engineers on the FLARE team have identified four additional malware families specifically designed to manipulate Pulse Secure devices (Table 1). These utilities have similar functions to the 12 previously documented malware families: harvesting credentials and sensitive system data, allowing arbitrary file execution, and removing forensic evidence. Please see the Technical Annex for detailed analysis of these code families.

Malware Family	Description	Actor
----------------	-------------	-------

BLOODMINE	BLOODMINE is a utility for parsing Pulse Secure Connect log files. It extracts information related to logins, Message IDs and Web Requests and copies the relevant data to another file.	UNC2630
BLOODBANK	BLOODBANK is a credential theft utility that parses two files containing password hashes or plaintext passwords and expects an output file to be given at the command prompt.	UNC2630
CLEANPULSE	CLEANPULSE is a memory patching utility that may be used to prevent certain log events from occurring. It was found in close proximity to an ATRIUM webshell.	UNC2630
RAPIDPULSE	RAPIDPULSE is a webshell capable of arbitrary file read. As is common with other webshells, RAPIDPULSE exists as a modification to a legitimate Pulse Secure file. RAPIDPULSE can serve as an encrypted file downloader for the attacker.	UNC2630

Table 1: New malware families identified

Initial Compromise

The actors leveraged several vulnerabilities in Pulse Secure VPN appliances. Mandiant observed the use of the recently patched vulnerability CVE-2021-22893 to compromise fully patched Pulse Secure appliances as well as previously disclosed vulnerabilities from 2019 and 2020. In many cases, determining the initial exploitation vector and timeframe was not possible to determine because the actors altered or deleted forensic evidence, or the appliance had undergone subsequent code upgrades thereby destroying evidence related to the initial exploitation.

Establish Foothold

In some cases, Mandiant observed the actors create their own Local Administrator account outside of established credential management controls on Windows servers of strategic value. This allowed the actor to maintain access to systems with short-cycle credential rotation policies and provided a sufficient level of access to operate freely within their target environment. The actors also maintained their foothold into the targeted environments exclusively through Pulse Secure webshells and malware without relying on backdoors deployed on internal Windows or Linux endpoints.

Escalate Privileges

Mandiant observed the actors use three credential harvesting techniques on Windows systems:

- Targeting of clear text passwords and hashes from memory using the credential harvesting tool Mimikatz. Instead of being copied locally and executed on the target system, Mandiant saw evidence of the Mimikatz binary on the source system of an RDP session (i.e. the threat actor's system that was connected to the VPN) through an RDP mapped drive.
- Copying and exfiltration of the SAM, SECURITY, and SYSTEM registry hives which contained cached NTLM hashes for Local and Domain accounts.
- Leveraging the Windows Task Manager process to target the Local Security Authority Subsystem Service (LSASS) process memory for NTLM hashes.

In addition to these privilege escalation techniques, the actors specifically targeted separate privileged accounts belonging to individuals whose unprivileged accounts were previously compromised (likely through the Pulse Secure credential harvesting malware families). It is unclear how the account associations were made by the actor.

Internal Reconnaissance

Mandiant found evidence that the actors renamed their own workstations that they connected to the VPN of victim networks to mimic the naming convention of their target environment. This practice aligns with the actor's objective for long-term persistence and evading detection and demonstrates a familiarity with the internal hostnames in the victim environment.

The actors operated solely by utilizing Windows-based utilities to carry out tasks. Some of the utilities observed were net.exe, quser.exe, powershell.exe, powershell_ise.exe, findstr.exe, netstat.exe, cmd.exe, reg.exe and tasklist.exe.

Move Laterally

Most lateral movement originated from compromised Pulse Secure VPN appliances to internal systems within the environment. While connected to the Pulse VPN appliance, the actor's system was assigned an IP address from the Pulse VPN DHCP pool and they moved laterally throughout the environments by leveraging the Remote Desktop Protocol (RDP), the Secure Shell Protocol (SSH), and browser-based communication to HTTPS hosted resources. The actors also accessed other resources such as Microsoft M365 cloud environments using stolen credentials they had previously acquired.

Mandiant also observed the actors targeting ESXi host servers. The actor enabled SSH on ESXi hosts that were previously disabled via the web interface. When their operations on the system were finished, the actors disabled SSH on the ESXi host again and cleared or preemptively disabled all relevant logging associated with the performed activities. This includes authentication, command history, and message logging on the system.

Maintain Presence

Mandiant observed the threat actor maintain persistence by compromising the upgrade process on the Pulse Secure Appliance. Persistence was primarily achieved by modifying the legitimate DSUpgrade.pm file to install the ATRIUM webshell across each upgrade performed by an administrator. The actor likely chose DSUpgrade.pm to host their patch logic as it is a core file in the system upgrade procedure, ensuring the patch is applied during updates. The patcher modifies content in /tmp/data as this directory holds the extracted upgrade image the newly upgraded system will boot into. This results in a persistence mechanism which allows the actor to maintain access to the system across updates.

The actors also achieved persistence in other cases by prepending a bash script to the file /bin/umount normally used to unmount a Linux filesystem. This binary was targeted by the actor because it is executed by the Pulse Secure appliance during a system upgrade. The actor's script verifies that the umount binary executes with a specific set of arguments, which are identical to the arguments used by the Pulse Secure appliance to execute the binary. The inserted malicious bash script remounts the filesystem as read-write and iterates through a series of bash routines to inject the ATRIUM webshell, hide SLOWPULSE from a legacy file integrity bash script, remove or add itself from the umount file, and validate the web process was running after a reboot to return the filesystem back to read-only.

Complete Mission

The threat actor's objectives appear to be stealing credentials, maintaining long-term persistent access to victim networks, and accessing or exfiltrating sensitive data. Mandiant has observed the attackers:

- Staging data related to sensitive projects, often in C:\Users\Public
- Naming exfiltration archives to resemble Windows Updates (KB) or to match the format KB<digits>.zip
- Using the JAR/ZIP file format for data exfiltration
- Deleting exfiltrated archives

Analysis of new malware families is included in the Technical Annex to enable defenders to quickly assess if their respective appliances have been affected. Relevant MITRE ATT&CK techniques, Yara rules and hashes are published on [Mandiant's GitHub page](#).

Forensics, Remediation, and Hardening Guidelines

To begin an investigation, Pulse Secure users should contact their Customer Support Representative for assistance completing the following steps:

1. Capture memory and a forensic image of the appliance
2. Run the Pulse Integrity Checker Tool found online
3. Request a decrypted image of each partition and a memory dump

To remediate a compromised Pulse Secure appliance:

1. Caution must be taken when determining if a Pulse Secure device was compromised at any previous date. If the Integrity Checker Tool (ICT) was not run before the appliance was updated, the only evidence of compromise will exist in the system rollback partition which cannot be scanned by the ICT. If an upgrade was performed without first using the ICT, a manual inspection of the rollback partition is required to determine if the device was previously compromised.
2. To ensure that no malicious logic is copied to a clean device, users must perform upgrades from the appliance console rather than the web interface. The console upgrade process follows a separate code path that will not execute files such as DSUpgrade.pm.
3. Previous versions of the ICT will exit if run on an unsupported software version. For every ICT scan, ensure that the ICT would have supported the device's version number.
4. Reset all passwords in the environment.
5. Upgrade to the most recent software version.

To secure the appliance and assist with future investigations, consider implementing the following:

1. Enable unauthenticated logging and configure syslog for Events, User & Admin Access
2. Forward all logs to a central log repository
3. Review logs for unusual authentications and evidence of exploitation
4. Regularly run the Integrity Checker Tool
5. Apply patches as soon as they are made available

Geopolitical Context and Implications for U.S.-China Relations

In collaboration with intelligence analysts at BAE Systems Applied Intelligence, Mandiant has identified dozens of organizations across the defense, government, telecommunications, high tech, education, transportation, and financial sectors in the U.S. and Europe that have been compromised via vulnerabilities in Pulse Secure VPNs. Historic Mandiant and BAE investigations identified a significant number of these organizations as previous APT5 targets.

Notably, compromised organizations operate in verticals and industries aligned with Beijing's strategic objectives as outlined in China's 14th Five Year Plan. Many manufacturers also compete with Chinese businesses in the high tech, green energy, and telecommunications sectors. Despite this, we have not directly observed the staging or exfiltration of any data by Chinese espionage actors that could be considered a violation of the Obama-Xi agreement.

Targets of Chinese cyber espionage operations are often selected for their alignment with national strategic goals, and there is a strong correlation between pillar industries listed in policy white papers and targets of Chinese cyber espionage activity.

China has outlined eight key areas of vital economic interest for development and production which it views as essential to maintaining global competitiveness, under the following categories: energy, healthcare, railway transportation, telecommunications, national defense and stability, advanced manufacturing, network power, and sports and culture.

Historical Context

In the *Red Line Drawn* report, Mandiant documented a significant decline in the volume of Chinese cyberespionage activity in 2014 and assessed that the restructuring of China's military and civilian intelligence agencies significantly impacted Chinese cyber operations. Then, in September 2015, President Xi of China concluded a bilateral agreement with U.S. President Obama to prohibit state-sponsored theft of intellectual property for the purpose of providing commercial advantage. Commercial IP theft has historically been a prominent characteristic of Chinese cyber espionage activity.

In 2018 we conducted an extensive review of Chinese cyber espionage operations, both before and after the official announcement of the PLA reforms and bilateral agreement to determine if there were any corresponding changes in the tactics, techniques, and procedures (TTPs) used during Chinese cyberespionage operations. We observed two important changes in the type of information stolen and the geographic distribution of the targets.

- Despite examining hundreds of incidents from January 2016 through mid 2019, we did not find definitive evidence of purely commercial application intellectual property theft in the US. Recent indictments by the US Department of Justice suggest that this theft did occur. While we observed other malicious activity, including geopolitical targeting, theft of intellectual property with military applications, and theft of confidential business information, we did not find evidence that these cyber operations violated the Obama-Xi agreement.
- Between January 2016 and mid-2019, the geographic focus of Chinese cyber operations shifted dramatically to Asia and away from the U.S. and Europe. While the U.S. remained the single most frequently targeted country, it became a much smaller percentage of observed activity. From 2012–2015, U.S. targeting constituted nearly 70 percent of all observed Chinese cyber espionage, while from January 2016 through August 2019, U.S. targeting fell to approximately 20 percent of Chinese activity. Targeting of Europe represented a similar proportion of overall Chinese activity to targeting of the Americas.

Changes in Chinese Espionage Activity between 2019 and 2021

Based on developments observed between 2019-2021, Mandiant Threat Intelligence assesses that most Chinese APT actors now concentrate on lower-volume but more-sophisticated, stealthier operations collecting strategic intelligence to support Chinese

strategic political, military, and economic goals. While some of the technical changes may be the result of the restructuring of China's military and civilian organizations, some changes possibly reflect larger technical trends in cyber operations overall.

- Before the reorganization, it was common to observe multiple Chinese espionage groups targeting the same organization, often targeting the same types of information. Post-2015, this duplication of efforts is rare.
- Chinese espionage groups developed more efficient and purposeful targeting patterns by transitioning away from spearphishing and relying on end user software vulnerabilities and instead began exploiting networking devices and web facing applications in novel ways. Chinese APT actors also began to leverage supply chain vulnerabilities and to target third party providers to gain access to primary targets.
- Recently observed Chinese cyber espionage activity exhibits an increased diligence in operational security, familiarity with network defender investigation techniques, and cognizance of the forensic evidence they leave behind.
- We observe the resurgence of older Chinese espionage groups, including APT4 and APT5 after long periods of dormancy and currently active groups engage in frequent and widespread campaigns.

Redline Withdrawn?

The Obama-Xi agreement prohibits the theft of intellectual property with purely commercial applications for the purpose of gaining a competitive advantage. It does not cover government or diplomatic information, sensitive business communications, IT data, PII, or intellectual property with military or dual use applications.

- We have direct evidence of UNC2630, UNC2717 and other Chinese APT actors stealing credentials, email communications, and intellectual property with dual commercial and military applications.
- Throughout our investigations, we did not directly observe the staging or exfiltration of any data by Chinese espionage actors that could be considered a violation of the Obama-Xi agreement.

Given the narrow definition of commercial intellectual property theft and the limited availability of forensic evidence, it is possible that our assessment will change with the discovery of new information.

Evidence collected by Mandiant over the past decade suggests that norms and diplomatic agreements do not significantly limit China's use of its cyber threat capabilities, particularly when serving high-priority missions.

The greater ambition and risk tolerance demonstrated by Chinese policymakers since 2019 indicates that the tempo of Chinese state-sponsored activity may increase in the near future and that the Chinese cyber threat apparatus presents a renewed and serious threat to US

and European commercial entities.

Acknowledgements

Mandiant would like to thank analysts at BAE Systems Applied Intelligence, Stroz Friedberg, and Pulse Secure for their hard work, collaboration and partnership. The team would also like to thank Scott Henderson, Kelli Vanderlee, Jacqueline O'Leary, Michelle Cantos, and all the analysts who worked on Mandiant's *Red Line Redrawn* project. The team would also like to thank Mike Dockry, Josh Villanueva, Keith Knapp, and all the incident responders who worked on these engagements.

Additional Resources

Detecting the Techniques

The following table contains specific FireEye product detection names for the malware families associated with this updated information.

Platform(s)	Detection Name
Network Security	<ul style="list-style-type: none">FE_APT_Tool_Linux32_BLOODMINE_1
Email Security	<ul style="list-style-type: none">FE_APT_Tool_Linux_BLOODMINE_1
Detection On Demand	<ul style="list-style-type: none">FE_APT_Tool_Linux32_BLOODBANK_1FE_APT_Tool_Linux_BLOODBANK_1
Malware File Scanning	<ul style="list-style-type: none">FE_APT_Tool_Linux32_CLEANPULSE_1FE_APT_Tool_Linux_CLEANPULSE_1
Malware File Storage Scanning	<ul style="list-style-type: none">FE_APT_Webshell_PL_RAPIDPULSE_1FEC_APT_Webshell_PL_RAPIDPULSE_1
Endpoint Security	Real-Time Detection (IOC) <ul style="list-style-type: none">BLOODBANK (UTILITY)BLOODMINE (UTILITY)

Helix

Establish Foothold

- WINDOWS METHODOLOGY [User Account Created]
- WINDOWS METHODOLOGY [User Created - Net Command]

Escalate Privileges

- WINDOWS METHODOLOGY [Mimikatz Args]
- WINDOWS METHODOLOGY [Invoke-Mimikatz Powershell Artifacts]
- WINDOWS METHODOLOGY [LSASS Memory Access]
- WINDOWS METHODOLOGY [LSASS Generic Dump Activity]

Internal Reconnaissance

WINDOWS ANALYTICS [Recon Commands]

Move Laterally

- WINDOWS ANALYTICS [Abnormal RDP Logon]
- OFFICE 365 ANALYTICS [Abnormal Logon]

Technical Annex

BLOODMINE

BLOODMINE is a utility for parsing Pulse Secure Connect log files. It extracts information related to logins, Message IDs and Web Requests and copies the relevant data to another file.

The sample takes three command line arguments

1. Filename to read
2. Filename to write
3. Timeout interval

It parses the input file for login status codes:

AUT31504

AUT24414

AUT22673

AUT22886

AUT23574

It parses the input file for web results code WEB20174. If it finds a web result code, it looks for file extensions:

.css

.jpg

.png

.gif

.ico

.js

.jsp

These strings indicate the type of data that is collected from web requests:

Web login, IP: %s, User: %s, Realm: %s, Roles: %s, Browser: %s

Agent login, IP: %s, User: %s, Realm: %s, Roles: %s, Client: %s

Logout, IP: %s, User: %s, Realm: %s, Roles: %s

Session end, IP: %s, User: %s, Realm: %s, Roles: %s

New session, IP: %s, User: %s, Realm: %s, Roles: %s, New IP: %s

Host check, Policy: %s

WebRequest completed, IP: %s, User: %s, Realm: %s, Roles: %s, %s to %s://%s:%s/%s from %s

BLOODBANK

BLOODBANK is a credential theft utility that parses two LMDB (an in memory database) files and expects an output file to be given at the command prompt. BLOODBANK takes advantage of a legitimate process that supports Single Sign On functionality and looks for plaintext passwords when they are briefly loaded in memory.

The utility parses the following two files containing password hashes or plaintext passwords:

- /home/runtime/mtmp/lmdb/data0/data.mdb
- /home/runtime/mtmp/system

BLOODBANK expects an output file as a command line parameter, otherwise it prints file open error. It contains the following strings which it likely tries to extract and target.

PRIMARY

SECONDARY

remoteaddr

user@

logicUR

logicTim

passw@

userAge

realm

Sourc

CLEANPULSE

CLEANPULSE is a memory patching utility that may be used to prevent certain log events from occurring. The utility inserts two strings from the command line into the target process and patches code to conditionally circumvent a function call in the original executable.

File Name	File Type	Size	Compile Time
dsrlog	ELF.X86	13332	

The utility expects to be run from the command line as follows:

```
drslog <pid> <code2_string> <code3_string> <command>
```

Where <pid> is the pid process ID to patch in memory, <code2_string> and <code3_string> are two strings to write into the target process, and <command> is either 'e' or 'E' for installation or 'u' or 'U' for uninstallation.

During installation (using the 'e' or 'E' <command>), the <code2_string> <code3_string> command line strings are written to the target process at hard-coded memory addresses, a small amount of code is written, and a jump instruction to the code snippet is patched in memory of the target process. The added code checks whether an argument is equal to either <code2_string> <code3_string> strings, and if, so skips a function call in the target process.

During uninstall (using the 'u' or 'U' <command>) the patch jump location is overwritten with what appears to be the original 8 bytes of instructions, and the two additional memory buffers and the code snippet appear to be overwritten with zeros.

The CLEANPULSE utility is highly specific to a victim environment. It does not contain any validation code when patching (i.e. verifying that code is expected prior to modifying it), and it contains hard-coded addresses to patch.

The target code to patch appears to be the byte sequence: 89 4C 24 08 FF 52 04. This appears as the last bytes in the patched code, and is the 8-bytes written when the uninstall 'u' command is given.

These bytes correspond to the following two instructions:

```
.data:0804B138 89 4C 24 08      mov    [esp+8], ecx  
  
-----  
.data:0804B13C FF 52 04      call  dword ptr [edx+4]
```

This byte sequence occurs at the hard-coded patch address the utility expects, dslogserver. Based on status and error messages in nearby functions the executable dslogserver appears to be related to log event handling, and the purpose of the CLEANPULSE utility may be to prevent certain events from being logged.

There are several un-referenced functions that appear to have been taken from the open source project PUPYRAT. It is likely that the actor re-purposed this open source code, using PUPYRAT as a simple template project.

RAPIDPULSE

RAPIDPULSE is a webshell capable of arbitrary file read. As is common with other webshells, RAPIDPULSE exists as a modification to a legitimate Pulse Secure file.

The webshell modifies the legitimate file's main routine which compares the HTTP query parameter with key name: deviceid to a specific key with value. If the parameter matches, then the sample uses an RC4 key to decrypt HTTP query parameter with key name: hmacTime. This decrypted value is a filename which the sample then opens, reads, RC4 encrypts with the same key, base64 encodes, then writes to stdout. The appliance redirects stdout as the response to HTTP requests. This serves as an encrypted file download for the attacker.

Integrity Checker Tool and Other Validation Checks

In our public report, we noted two code families that manipulate check_integrity.sh, a legitimate script used during a normal system upgrade. This validation script was modified by the actor to exit early so that it would not perform the intended checks.

Per Ivanti, the validation provided by check_integrity.sh is a separate validation feature and not the same as the [Integrity Checker Tool \(ICT\)](#) available on their website. They recommend that organizations use the online ICT to confirm that hashes of files on their Pulse Secure devices match Ivanti's list of known good hashes. Please note that the ICT does not scan the rollback partition.