Falcon Complete MDR Thwarts VANGUARD PANDA Tradecraft

crowdstrike.com/blog/falcon-complete-thwarts-vanguard-panda-tradecraft/

Falcon Complete Team June 22, 2023

VANGUARD PANDA Background

On May 24, 2023, industry and government sources detailed China-nexus activity in which the threat actor dubbed Volt Typhoon targeted U.S.-based critical infrastructure entities. CrowdStrike Intelligence tracks this actor as VANGUARD PANDA.

Since at least mid-2020, the CrowdStrike Falcon® Complete managed detection and response (MDR) team and the CrowdStrike® Falcon OverWatch™ threat hunting team have observed related historical activity in multiple sectors. The adversary consistently employed ManageEngine Self-service Plus exploits to gain initial access, followed by custom webshells for persistent access, and living-off-the-land (LOTL) techniques for lateral movement.

Collaboration between Falcon Complete, Falcon OverWatch and the CrowdStrike Intelligence team is a force multiplier protecting customers from the latest threats to ultimately stop breaches.

Incident Case Study

One specific VANGUARD PANDA incident stands out to review in detail. Falcon Complete responded to a detection that was triggered by suspicious reconnaissance commands executed under an Apache Tomcat web server running ManageEngine ADSelfService Plus.

The malicious activity detailed in the detection included listing processes, network connectivity testing, gathering user and group information, mounting shares, enumeration of domain trust over WMI, and listing DNS zones over WMI. VANGUARD PANDA's actions indicated a familiarity with the target environment, due to the rapid succession of their commands, as well as having specific internal hostnames and IPs to ping, remote shares to mount, and plaintext credentials to use for WMI.

```
cmd /C "tasklist /svc"
cmd /C "ping -n 1 [redacted]"
cmd /C "ping -n 1 -a [redacted]"
cmd /C "net group "domain controllers" /dom"
cmd /C "net use \\[redacted]\admin$ REDACTED /u:[redacted]"
cmd /C "dir \\[redacted]\c$\Users"
cmd /C "wmic /node:[redacted] /user:[redacted] /password:"<removed>" process call
create "cmd /c nltest /DOMAIN_TRUSTS >>C:\Users\[redacted]\AppData\Local\
[redacted].tmp""
cmd /C "dir \\[redacted]\c$\users\[redacted]\AppData\Local\Temp\[redacted].tmp"
cmd /C "type \\[redacted]\c$\users\[redacted]\AppData\Local\Temp\[redacted].tmp"
cmd /C "wmic /node:[redacted] /user:[redacted] /password:"<removed>" process call
create "cmd /c Dnscmd . /EnumZones >>C:\Users\[redacted]\AppData\Local\Temp\
[redacted].tmp""
cmd /C "dir \\[redacted]\c$\users\[redacted]\AppData\Local\Temp\[redacted].tmp"
cmd /C "type \\[redacted]\c$\users\[redacted]\AppData\Local\Temp\[redacted].tmp"
```

Upon notification from Falcon OverWatch of the reconnaissance activity taking place underneath the ManageEngine AD SelfService Plus process, Falcon Complete quickly contained the host using the CrowdStrike Falcon® sensor's Network Containment capability. In doing so, Falcon Complete isolated the host and prevented the adversary from interacting with it.

Following successful containment, Falcon Complete quickly triaged the host, ultimately calling the impacted customer to notify them of this critical incident and the measures being taken to defend against the suspected adversary tradecraft.

Simultaneously, Falcon Complete began technical analysis of the Apache Tomcat access logs located in `C:\ManageEngine\ADSelfService Plus\logs`.

Upon review of the access logs, multiple HTTP POST requests to `/html/promotion/selfsdp.jspx` were found with timestamps matching the enumeration and reconnaissance commands seen spawning from the Apache Tomcat web server.

```
- /html/promotion/selfsdp.jspx "-" [redacted] [redacted] POST [redacted +0000] 203
2043 200 "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:68.0) Gecko/20100101 Firefox/68.0"
```

Based on the URI from the access logs, Falcon Complete identified the folder and file on disk located at `C:\ManageEngine\ADSelfService Plus\webapps\adssp\html\promotion\selfsdp.jspx`.

Upon analysis of the `.jspx` file, Falcon Complete identified it to be a webshell. This is based on Java code that converts the bytes 99, 109 and 100, respectively, into `cmd`; and the bytes 47 and 67 into `/C`. Execution of the command `cmd /C` is a common method by which webshells run commands under the Command Prompt process.

```
ProcessBuilder pb = new ProcessBuilder(new String(new byte[]{99, 109, 100}), new
String(new byte[]{47, 67}), command);
```

Additionally, the webshell was attempting to masquerade as a legitimate file of ManageEngine ADSelfService Plus by setting its title to ManageEngine ADSelfService Plus and adding links to legitimate enterprise help desk software http[:]//www.manageengine[.]com/products/adself-service/help-desk-software.html and ADSelfService http[:]//www.manageengine[.]com/products/adself-service/index.html.

Now, a retrospective review of the `selfsdp.jspx` webshell will return successful matches of the EncryptJSP YARA rule released by CISA reporting on Volt Typhoon activity.

```
rule EncryptJSP {
    strings:
        $s1 = "AEScrypt"
        $s2 = "AES/CBC/PKCS5Padding"
        $s3 = "SecretKeySpec"
        $s4 = "FileOutputStream"
        $s5 = "getParameter"
        $s6 = "new ProcessBuilder"
        $s7 = "new BufferedReader"
        $s8 = "readLine()"
    condition:
        filesize < 50KB and 6 of them
}
```

CISA also now reports that the following User-Agent (spaces included) was used by VANGUARD PANDA. However, at the time of CrowdStrike's initial investigation, this information had not yet been reported.

```
Mozilla/5.0 (Windows NT 6.1; WOW64; rv:68.0)              Gecko/20100101
Firefox/68.0
```

Retrospective review of the User-Agent that Falcon Complete observed making POST requests to the webshell is an exact match for this User-Agent without the mistake in spacing.

```
Mozilla/5.0 (Windows NT 6.1; WOW64; rv:68.0) Gecko/20100101 Firefox/68.0
```

Falcon Complete assessed the activity was malicious and rapidly remediated the webshell on behalf of the customer and provided the customer with further actionable recommendations for patching and user credential resets.

Investigation Follow-Through

This is where an investigation might typically end, but the expected access log artifacts that would indicate CVE-2021-40539 were not present, even though the TTPs of the malicious activity were a match for this CVE.

Additionally, Falcon Complete's experience with similar advanced intrusions combined with VANGUARD PANDA's apparent familiarity with the target environment and potential indicators of log tampering, Falcon Complete determined a deeper dive into the associated activity was an important next step to determine if other artifacts remained and could confirm the use of CVE-2021-40539 or possibly indicate another form of exploitation altogether.

More Tradecraft Unearthed

The number of remaining loose ends at this point in the investigation relative to a typical event became a red flag in itself, warranting further investigation because:

1. VANGUARD PANDA had clearly performed extensive prior recon and enumeration (based on its knowledge and use of remote hosts within the environment);
2. Administrator credentials had already been acquired/compromised;
3. Expected access log artifacts for CVE-2021-40539 did not appear to exist; and
4. The Falcon sensor was only recently installed on the targeted host

A review of existing evidence showed the identified webshell `selfsdp.jspx` was written to disk almost 6 months prior to the installation of the Falcon sensor as well as the witnessed hands-on-keyboard adversary activity.

Using the Apache Tomcat access logs, CrowdStrike was able to correlate the timing of the `selfsdp.jspx` disk write to a HTTP POST request to a URI `/html/error.jsp`, where the actor then performed an HTTP GET request to `/html/promotion/selfsdp.jspx` to confirm its presence.

Falcon Complete investigated the host for the suspected webshell at `/html/error.jsp`, but this file was not on disk — an important fact that will come up later in the investigation.

Even though the timing of this activity lined up with CVE-2021-40539 exploitation, no such exploitation artifacts were left in the access logs, ManageEngine serverOut logs, or the ManageEngine adslog. The lack of all of these log artifacts combined with the lack of `error.jsp` on disk suggested that the adversary might be attempting to cover their tracks.

Further review of the Apache Tomcat access logs showed the use of the `selfsdp.jspx` webshell across multiple months. On one particular day the access log was wiped clean for the first 12 hours of the day, and the first log message recorded of that day being to the `selfsdp.jspx` webshell.

Now with a specific 12-hour time period in focus, Falcon Complete triaged the host for any further signs of malicious activity that might be connected to the intrusion. This is where CrowdStrike discovered the adversary's misstep.

The Giveaway: JSP Compilation

A component of Apache Tomcat, the Jasper 2 JSP Engine, is responsible for the generation of Java source code from JSP files and the subsequent compilation of those files into classes.

The Jasper 2 JSP Engine has a configuration setting named "keepGenerated" with the following description:

```
"Should we keep the generated Java source code for each page instead of deleting it? true or false, default true."
```

An important piece of information is that these Java and Class files get created in a separate directory structure.

Where HTML and JSP files may be in `C:\ManageEngine\ADSelfService Plus\webapps\adssp\html.`
The Java and Class files are written to a separate directory, `C:\ManageEngine\ADSelfService Plus\work\Catalina\localhost\ROOT\org\apache\jsp\[foldername]`

VANGUARD PANDA went through extensive lengths to clear out multiple log files and remove excess files from disk — but they didn't clear out the generated Java source or compiled Class files. As a result, Falcon Complete discovered numerous webshells and backdoors all connected to this same attack.

One Java source code file, `ListName_jsp.java`, was critically important. The Jasper Engine generated this source code file just prior to known log clearing via the `selfsdp.jspx` webshell.

i.e.

ListName_jsp.java

```
/*
* Generated by the Jasper component of Apache Tomcat
* Version: Apache Tomcat/@VERSION@
* Generated at: [redacted] 11:[redacted]UTC
* Note: The last modified time of this file was set to
* the last modified time of the source file after
* generation to assist with modification tracking.
*/
```

JSP Backdoor Preparation

`ListName_jsp.java` is the generated Java source code for a deleted file that was named `ListName.jsp`. Analysis of `ListName.jsp` reveals its purpose is to deploy a backdoored version of the `tomcat-websocket.jar` Apache Tomcat library containing a webshell.

First, `ListName.jsp` tries to load the following three Classes:

```
/org/apache/tomcat/websocket/server/A.class
/org/apache/tomcat/websocket/server/B.class
/org/apache/tomcat/websocket/server/C.class
```

Then `ListName.jsp` moves the following Class files from a JAR archive `C:/users/public/tomcat-ant.jar` to `C:/users/public/tomcat-websocket.jar`:

```
/org/apache/tomcat/websocket/server/WsSci.class
/org/apache/tomcat/websocket/server/A.class
/org/apache/tomcat/websocket/server/B.class
/org/apache/tomcat/websocket/server/C.class
```

Armed with this knowledge, Falcon Complete confirmed that the version of `tomcat-websocket.jar` installed in the Apache Tomcat library on disk was backdoored. The `tomcat-websocket.jar` file timestamp was timestomped to appear unmodified, but unpacking the Java Archive showed the A, B, and C class files with timestamps matching the `ListName.jsp` timeframe.

The `C:/users/public/tomcat-ant.jar` was not available on disk, and not located anywhere within the installed Apache Tomcat directory structure.

While unconfirmed due to log clearing and occurring prior to the Falcon sensor installation, VANGUARD PANDA's workflow likely follows these approximate steps to backdoor `apache-tomcat.jar`:

1. Use webshell to retrieve `ListName.jsp` from a remote source, and place in web server directory
2. Use webshell to retrieve `tomcat-ant.jar` from a remote source and move to `C:/users/public/`

3. Use webshell to copy `tomcat-websocket.jar` out of the Apache Tomcat library directory into `C:/users/public`
4. Make an HTTP GET request to `ListName.jsp`, which would move A, B, and C classes from `tomcat-ant.jar` to `tomcat-websocket.jar`
5. Use webshell to replace the `tomcat-websocket.jar` in the Apache Tomcat library with the backdoored version
6. Cleanup
    1. Delete JARs out of `C:/users/public`
    2. Delete `ListName.jsp` out of the web server directory
    3. Clear Apache Tomcat access logs

JAR Backdoor

Falcon Intelligence reviewed the backdoored `tomcat-websocket.jar` to understand its purpose. The backdoored library provided VANGUARD PANDA with several possible commands triggered via HTTP URIs containing `/addEndpoint/html/lookup.gif`.

- C.class adds a new endpoint for B.class, which is reachable under `/addEndpoint/html/lookup.gif`.
- B.class instantiates A.class, which will handle requests to the previously registered endpoint under `/addEndpoint/html/lookup.gif`.
- A.class acts as the webshell. The webshell command data is Base64-encoded and AES-encrypted using the provided key. Command arguments are split using the ampersand ('`&`') character.

Command	Description
`first&<aes_key>`	Initializes the webshell class using the given data as the AES key for future requests and responses.
`<command_data>&0`	Executes the decrypted shell command and returns encrypted command output via the webshell session.
`exit&0`	If the decrypted command is exit, the webshell session is terminated
`<string_data>&1`	Writes the decrypted value of the string to the log file `C:/users/public/tmp.log`

The use of a backdoored Apache Tomcat library is a previously undisclosed persistence TTP in use by VANGUARD PANDA. This backdoor was likely used by VANGUARD PANDA to enable persistent access to high-value targets downselected after the initial access phase of operations using then zero-day vulnerabilities. CrowdStrike Intelligence's assessment is made with moderate confidence based on:

- The additional session management options provided by this backdoor compared to the webshell associated with VANGUARD PANDA initial access operations
- Extensive use of log clearing and artifact deletion to hinder forensic analysis
- Use of filenames masquerading as legitimate server files to avoid detection

The Falcon Complete MDR Way

Falcon Complete's subject matter expertise in responding to sophisticated adversaries allowed for the quick containment, identification and remediation of this pre-sensor-installation VANGUARD PANDA intrusion. The first time VANGUARD PANDA became active after the Falcon sensor was installed, Falcon Complete was prepared to investigate, contain and remediate.

Falcon Complete, Falcon OverWatch and CrowdStrike Intelligence continually partner to proactively hunt, identify, and remediate malicious activity from adversaries. By working together, these teams take full advantage of CrowdStrike's expertise and keep CrowdStrike customers protected 24/7/365.

Recommendations to Detect and Defend against VANGUARD PANDA

Falcon Complete recommends the following indicators and rules to detect and defend against the malicious VANGUARD PANDA components outlined in this blog.

In ManageEngine ADSelfService Plus, or Apache Tomcat access logs, any requests to the following URI:

```
/addEndpoint/html/lookup.gif
```

Files on disk:

- C:/users/public/*.jar
- C:/users/public/tmp.log

Review for unexpected .java or .class files or unexpected timestamps in the following directory and its subdirectories:

```
C:\ManageEngine\ADSelfService
Plus\work\Catalina\localhost\ROOT\org\apache\jsp\
```

YARA rule from CISA AA23-144a

```
rule EncryptJSP {
    strings:
        $s1 = "AEScrypt"
        $s2 = "AES/CBC/PKCS5Padding"
        $s3 = "SecretKeySpec"
        $s4 = "FileOutputStream"
        $s5 = "getParameter"
        $s6 = "new ProcessBuilder"
        $s7 = "new BufferedReader"
        $s8 = "readLine()"
    condition:
        filesize < 50KB and 6 of them
}
```

CrowdStrike Intelligence YARA rules:

```
rule CrowdStrike_VANGUARD_PANDA_timewarp_webshell : webshell vanguard_panda
{
    meta:
        copyright = "(c) 2023 CrowdStrike Inc."
        description = "Timewarp Java webshell in malicious Tomcat module"
        version = "202306131008"
        last_modified = "2023-06-13"
        actor = "VANGUARD PANDA"
    strings:
        $ = "setKey"
        $ = "ProcessBuilder"
        $ = "AES/ECB/PKCS5Padding"
        $ = "tmp.log"
        $ = "byteKey"
        $ = "method0"
        $ = "failed to read output from process"
    condition:
        filesize<50KB and 4 of them
}

rule CrowdStrike_VANGUARD_PANDA_timewarp_webshell_jar : java vanguard_panda
{
    meta:
        copyright = "(c) 2023 CrowdStrike Inc."
        description = "JAR file containing Timewarp webshell"
        version = "202306131011"
        last_modified = "2023-06-13"
        actor = "VANGUARD PANDA"
    strings:
        $WsSci = "/WsSci.class"
        $abc1 = "/A.class"
        $abc2 = "/B.class"
        $abc3 = "/C.class"
        $timewarp1 = "/Timewarp.class"
        $timewarp2 = "/Timewarp2.class"
        $timewarp3 = "/Timewarp3.class"
    condition:
        uint16(0)==0x4b50 and filesize<1MB and $WsSci and (all of ($abc*) or all of
($timewarp*))
}

rule CrowdStrike_VANGUARD_PANDA_webshell_installer : java vanguard_panda
{
    meta:
        copyright = "(c) 2023 CrowdStrike Inc."
        description = "ClassLoader - Java webshell install and execute script"
        version = "202306131012"
        last_modified = "2023-06-13"
        actor = "VANGUARD PANDA"
    strings:
        $ = "<title>class loader</title>"
        $ = "customEndpoint1"
```

```
        $ = "move true <br>"
        $ = "inject true <br>"
        $ = "ListName_jsp"
        $ = "photohelp_jsp"
        $ = "photoparse_jsp"
        $ = "Timewarp.class"
        $ = "WsSci.class"
        $ = "/A.class"
        $ = "srcZipfs.getPath"
    condition:
        filesize<50KB and 4 of them
}
```

Additional Resources

- *Learn how any size organization can achieve optimal security with Falcon Complete by visiting the product webpage.*
- *Request a free CrowdStrike Intelligence threat briefing and learn how to stop adversaries targeting your organization.*
- *The industry-leading CrowdStrike Falcon platform sets the new standard in cybersecurity. Watch this demo to see the Falcon platform in action.*
- *Experience how the industry-leading CrowdStrike Falcon platform protects against modern threats. Start your 15-day free trial today.*