Monitoring Pulse Connect Secure With Splunk (CISA Emergency Directive 21-03)

splunk.com/en_us/blog/security/monitoring-pulse-connect-secure-with-splunk-cisa-emergency-directive-21-03.html

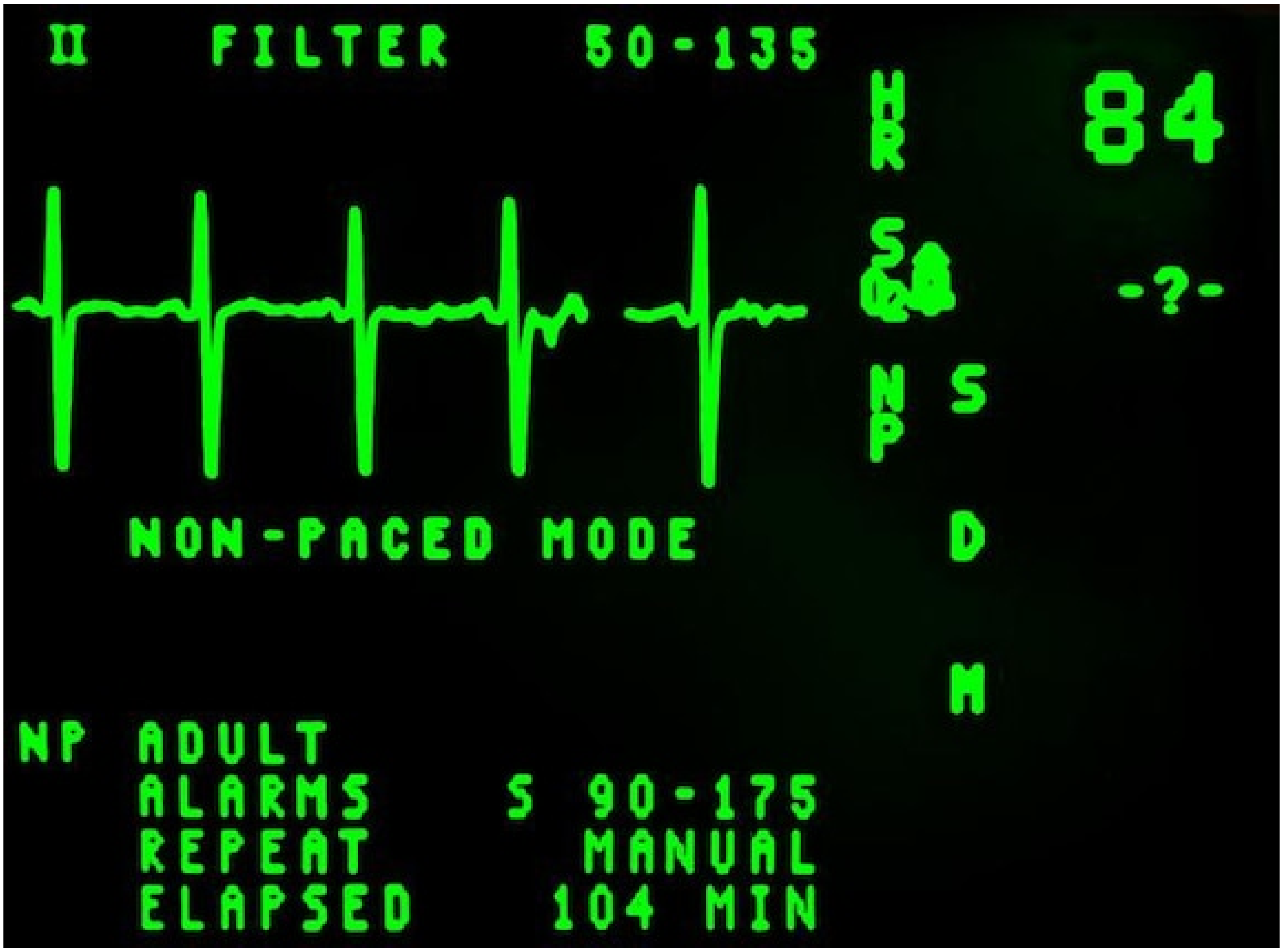
April 21, 2021

By Dave Herrald April 21, 2021

Contributors: Mick Baccio, James Brodsky, Tamara Chacon, Shannon Davis, Dave Herrald, Kelly Huang, Ryan Kovar, Marcus LaFerrerra, Michael Natkin, John Stoner and Bill Wright

Update May 4, 2021: Over the last two weeks, there have been several significant developments. First and most importantly, Pulse Secure issued an update on May 3 addressing multiple vulnerabilities. Splunk recommends that all Pulse Secure users review and install the update as soon as possible. On April 30, CISA updated Alert (AA21-110A) with new detections, including the "Impossible Travel" detection and JA3 analysis. We have updated our Splunk-friendly collection of indicators to include the latest from CISA.

To immediately see how to find potential vulnerabilities or exploits in your Pulse Connect Secure appliance, skip down to the *"Identifying, Monitoring and Hunting with Splunk"* section. Otherwise, read on for a quick breakdown of what happened, how to detect it, and MITRE ATT&CK mappings.



https://snappygoat.com/b/29e92459abc8f20ebaa4fffd7921b8f67513db9e

What You Need to Know About the Pulse Connect Secure Attacks

Over the past few weeks, there has been increasing chatter regarding adversary groups exploiting multiple vulnerabilities in the Pulse Connect Secure (PCS) virtual private network (VPN) appliance. On April 20, 2021, the Mandiant team at FireEye released a blog detailing their findings from multiple recent incidents involving compromised PCS appliances. This report prompted a flurry of activity from various organizations, including government agencies and security vendors. That same day, DHS Cybersecurity and Infrastructure Security Agency (CISA) released Alert (AA21-110A) and Emergency Directive 21-03, the latter requiring all US Federal agencies to take specific action concerning PCS appliances in their environments. Splunk recommends all US Federal agencies refer to the DHS directive to ensure compliance.

According to a blog post by Pulse Secure, the incidents disclosed this week involve vulnerabilities that were patched in 2019 and 2020, plus a new issue (CVE-2021-22893 Security Advisory SA44784) discovered this month. The vendor notes that a software update for this new issue will be available in early May. The post contains valuable information on all the vulnerabilities and recommended mitigation measures, and customer support information. Of particular importance is the Pulse Connect Secure Integrity Tool, which allows you to check if essential components of your PCS appliance software have been tampered with. Splunk recommends all PCS customers follow this vendor-published guidance in its entirety.

The PCS appliance is a popular VPN solution that offers workers secure access to an organization's internal networks from anywhere in the world. Because VPN appliances play a critical role in securing an organization's network perimeter and, by design, exposed directly to the Internet, they are often targeted by adversaries. Although the latest news is specific to Pulse Secure products, attacks of this nature are not limited to one vendor. Adversaries commonly return to vulnerabilities in VPN products to gain unauthorized access to organizations. As recently as April 16, 2021, the US National Security Agency released a cybersecurity advisory warning that older vulnerabilities in at least five different remote access products were being actively exploited.

Identifying, Monitoring, and Hunting with Splunk

Here are some **hot-off-the-press** searches to help find some of the badness described in the FireEye/Mandiant blog and other sources. If we have coverage for these searches in Splunk Security Content, we call them out in the MITRE ATT&CK section.

Note that proof of concept (POC) exploits are only available for some of the vulnerabilities involved in this attack. The detections below are all derived from a lab environment and informed by the context provided in the FireEye/Mandiant report. If we uncover more information, we will publish updates!

Ingesting PCS Appliance Data into Splunk

Several of the following techniques require logs from your PCS appliances to be ingested into Splunk for analysis. PCS appliances use syslog to log to external systems like Splunk. Ivanti publishes configuration details in the PCS appliance Admin guide; here is a link to

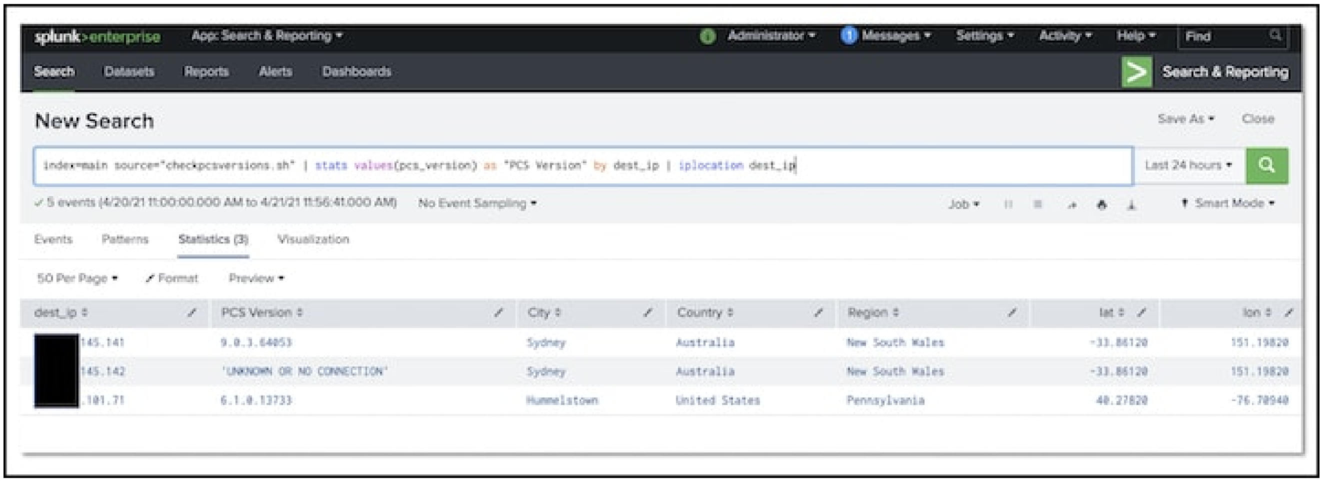
Admin Guide version 9.1R11 (the latest available at the time of publication). PCS appliances support multiple log export formats ("standard," "WELF," "W3C"). Each of these formats yields slightly different data and results. In 2015, Juniper Networks divested the JunOS Pulse product line to Pulse Secure, LLC, now owned by Ivanti. Early versions of the Splunk Add-on for Juniper included support for the IVE/SA (now PCS) product line, with a sourcetype of "juniper_sslvpn" or "juniper:ive." Since this time, third parties have published their own TAs on SplunkBase (such as this one) or GitHub (such as this one) to continue to support the PCS appliance log data. BOTS V's RWI scenario made use of WELF-formatted log data from a Juniper SA utilizing this TA. Note that some examples in this blog use a sourcetype of 'juniper:ive,' some use a sourcetype of 'pulse:connectsecure', and some use a sourcetype of 'syslog.' This emulates the variety of formatting we've observed in the wild. You should determine the sourcetype in use in your environment and substitute it in these example searches when necessary.

Additionally, we recommend enabling logging for "Unauthenticated Requests" (this setting is disabled by default on PCS appliances). While this may slightly increase the log volume, the CISA alert demonstrates that it is vital in revealing evidence of tampering and potentially ongoing malevolent activity.

Version Checking

According to this week's advisories, certain versions of the Pulse Secure appliance software contain critical vulnerabilities. Therefore, it is important to catalog the versions of all Pulse Secure Connect appliances you have on your network so that you can create a mitigation plan. You can use Splunk to do this if you don't have an alternative method. If you already have a list of IP addresses for your PCS appliances, you can feed that list as a lookup into a simple Splunk Technical Add-On that we have created, which will sequentially probe each appliance in the list and report the PCS version found into Splunk for reporting or alerting.

```
index=main source="checkpcsversions.sh"
| stats values(pcs_version) as "PCS Version" by dest_ip
| iplocation dest_ip
```



```
index=main source="checkpcsversions.sh" | stats values(pcs_version) as "PCS Version" by dest_ip | iplocation dest_ip
```

✓ 5 events (4/20/21 11:00:00.000 AM to 4/21/21 11:56:41.000 AM)

dest_ip	PCS Version	City	Country	Region	lat	lon
[redacted]145.141	9.0.3.64053	Sydney	Australia	New South Wales	-33.86120	151.19820
[redacted]145.142	'UNKNOWN OR NO CONNECTION'	Sydney	Australia	New South Wales	-33.86120	151.19820
[redacted].101.71	6.1.0.13733	Hummelstown	United States	Pennsylvania	40.27820	-76.70940

CVE-2021-22893 Mitigation Monitoring

This technique can be employed to assess your exposure by finding appliances that may still require mitigation according to the Pulse Secure guidance. We suggest you search through those logs for evidence of the following:

- Windows File Share Browse
- Pulse Secure Collaboration

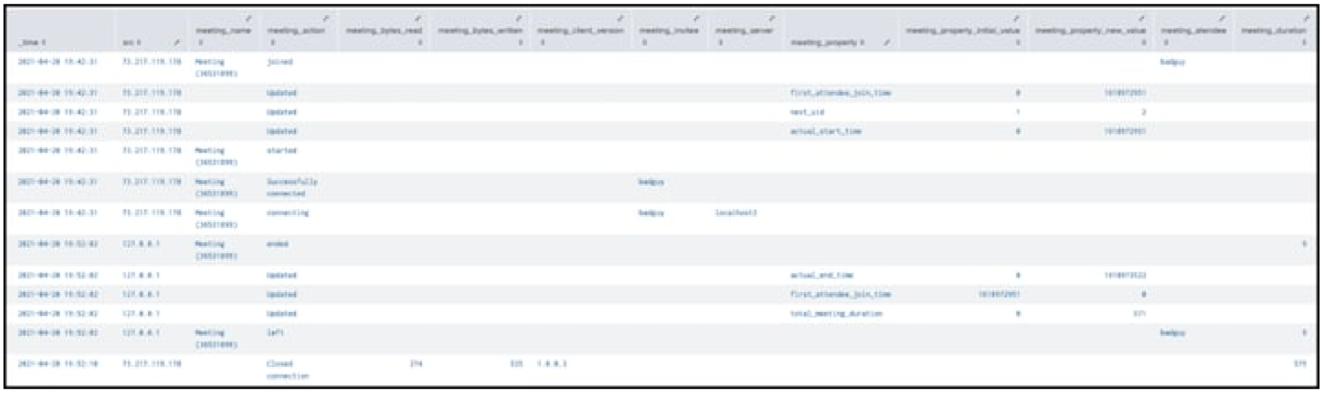
Why? Because both of those services are vulnerable, and the temporary "workaround" mitigation that you should have already applied turns both of these functions off. **Therefore, if you are still seeing activity from either function in the logs, and you know that your appliance is running a vulnerable Pulse Secure version, you must apply the appropriate workaround via application of the "workaround-2104.xml" file. You** can create a report or alerts based on any appliances still logging file sharing or collaboration activity, and provide the report or alerts to your network team to implement the workaround. Pulse Secure has committed to releasing an update in early May 2021, at which time this workaround can be reverted, thereby restoring these two capabilities if necessary.

Pulse Secure Collaboration Activity

Here is a quick and easy search to determine if Pulse Secure Collaboration is currently being used. You might look at the search and think, what is this reference to "meetings?" Well, "Secure Meetings" is what the original functionality in the appliance was called. Not all of the meeting fields are displayed here nor are they all required to determine if it is running, but it is meant to show you what can be seen in the events.

```
sourcetype=pulse:connectsecure dest=<IP Address of Pulse devices> meeting_id=*

| table _time src meeting_name meeting_action meeting_bytes_read
meeting_bytes_written meeting_client_version meeting_invitee meeting_server
meeting_property meeting_property_initial_value meeting_property_new_value
meeting_atendee meeting_duration
```

```
| sort + _time
```



_time	src	meeting_name	meeting_action	meeting_bytes_read	meeting_bytes_written	meeting_client_version	meeting_invitee	meeting_server	meeting_property	meeting_property_initial_value	meeting_property_new_value	meeting_attendee	meeting_duration
2021-04-28 15:42:31	73.217.119.178	Meeting (36531899)	joined									badguy	
2021-04-28 15:42:31	73.217.119.178		Updated						first_attendee_join_time	0	1618972951		
2021-04-28 15:42:31	73.217.119.178		Updated						next_uid	1	2		
2021-04-28 15:42:31	73.217.119.178		Updated						actual_start_time	0	1618972951		
2021-04-28 15:42:31	73.217.119.178	Meeting (36531899)	started										
2021-04-28 15:42:31	73.217.119.178	Meeting (36531899)	Successfully connected				badguy						
2021-04-28 15:42:31	73.217.119.178	Meeting (36531899)	connecting				badguy	localhost3					
2021-04-28 15:52:02	127.0.0.1	Meeting (36531899)	ended										0
2021-04-28 15:52:02	127.0.0.1		Updated						actual_end_time	0	1618973522		
2021-04-28 15:52:02	127.0.0.1		Updated						first_attendee_join_time	1618972951	0		
2021-04-28 15:52:02	127.0.0.1		Updated						total_meeting_duration	0	571		
2021-04-28 15:52:02	127.0.0.1	Meeting (36531899)	left									badguy	0
2021-04-28 15:52:16	73.217.119.178		Closed connection	274	325	1.0.0.1							575

__Note:__ You should determine the sourcetype in use in your environment and substitute it in these example searches as applicable.

Windows File Share Activity

As stated, you're also going to want to track Windows File Share activity. If your PCS appliance is configured to use WebTrends Enhanced Log Format (WELF) formatting for syslog events, this activity will be captured in the proto field. Search your logs for:

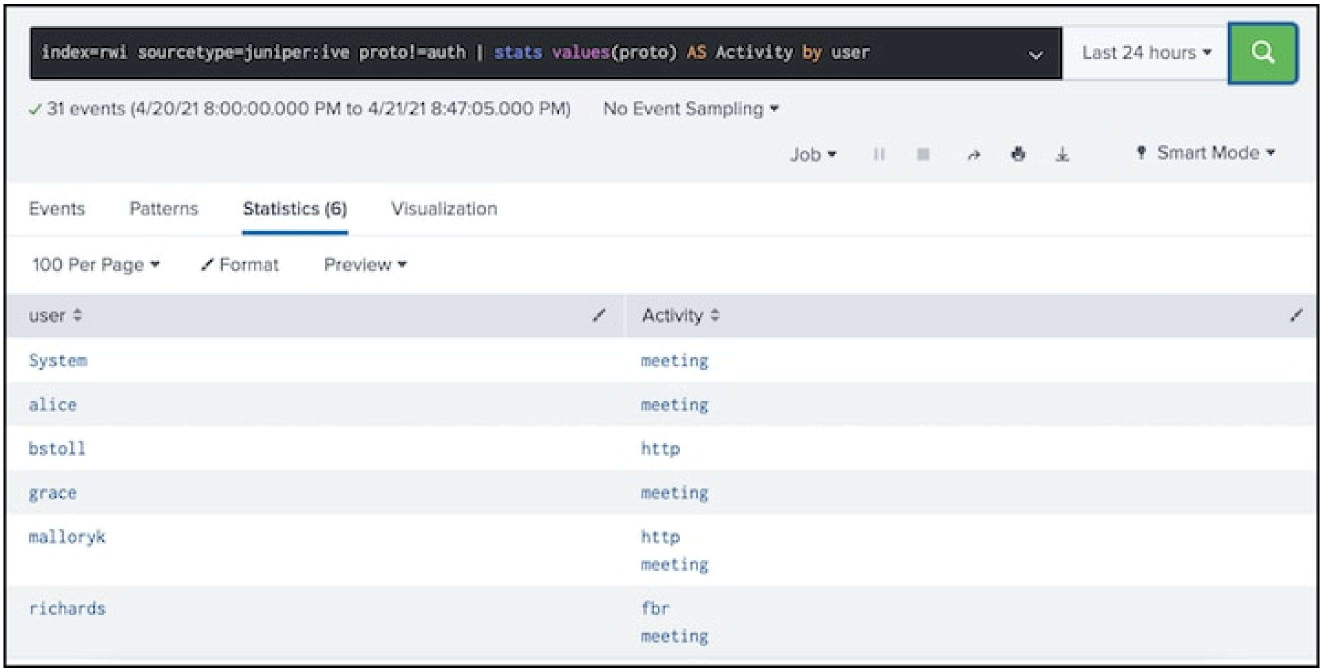
proto=fbr for Windows File Share activity

And as an alternative to the meeting search above, you can also search:

proto=meeting for Pulse Secure Collaboration activity

An example of this, combining both kinds of activity in the same search, is as follows:

```
search sourcetype=juniper:ive proto!=auth
| stats values(proto) AS Activity by user
```



```
index=rwi sourcetype=juniper:ive proto!=auth | stats values(proto) AS Activity by user
```

✓ 31 events (4/20/21 8:00:00.000 PM to 4/21/21 8:47:05.000 PM)

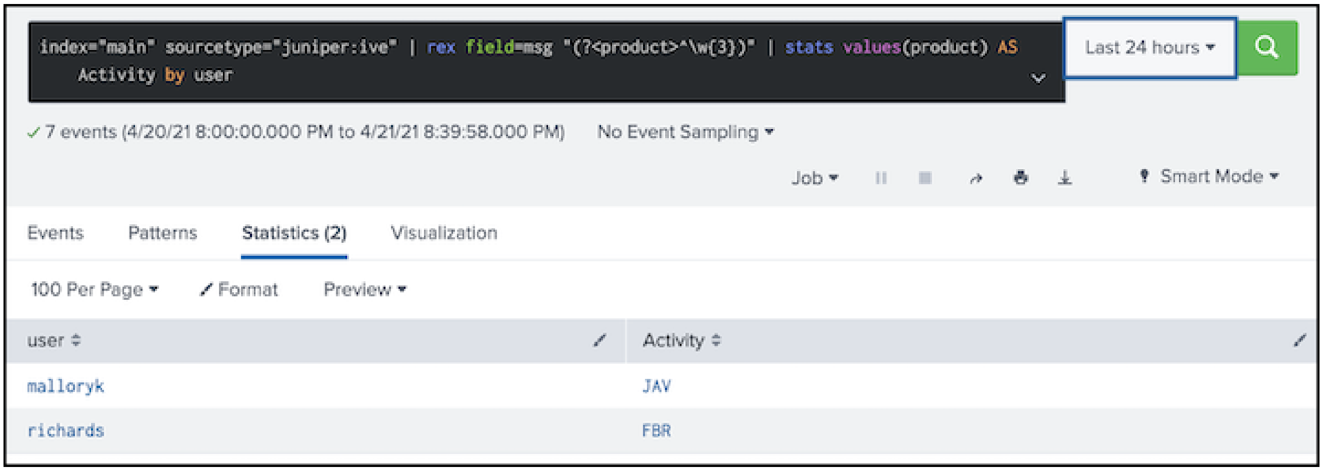
user	Activity
System	meeting
alice	meeting
bstoll	http
grace	meeting
malloryk	http meeting
richards	fbr meeting

Note: *You should determine the sourcetype in use in your environment and substitute it in these example searches as applicable.*

However, if your PCS appliance is configured for "standard" formatting for your syslog, PCS may identify activity based on a message code within the "msg" field. The format is three letters followed by five numbers (e.g. "MTG20035" or "FBR20503"). The examples below extract only the three letter code which indicates the feature being used. As previously noted, FBR denotes Windows File Share activity.

Examples of this are as follows:

```
sourcetype="juniper:ive"
| rex field=msg "(?<product>^\w{3})"
| stats values(product) AS Activity by user
```



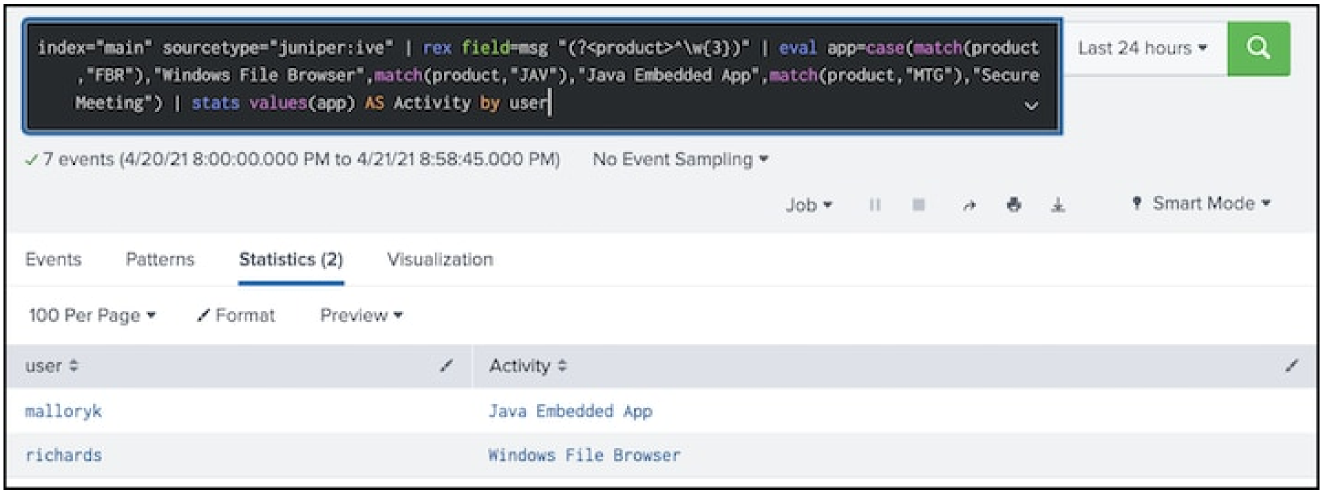
```
index="main" sourcetype="juniper:ive" | rex field=msg "(?<product>^\w{3})" | stats values(product) AS
    Activity by user
```

✓ 7 events (4/20/21 8:00:00.000 PM to 4/21/21 8:39:58.000 PM)

user	Activity
malloryk	JAV
richards	FBR

In the following example, we’re substituting the activity code in-line (though this could be accomplished with a lookup as well):

```
sourcetype="juniper:ive"
| rex field=msg "(?<product>^\w{3})"
| eval app=case(match(product,"FBR"),"Windows File
Browser",match(product,"JAV"),"Java Embedded App",match(product,"MTG"),"Secure
Meeting")
| stats values(app) AS Activity by user
```



```
index="main" sourcetype="juniper:ive" | rex field=msg "(?<product>^\w{3})" | eval app=case(match(product
    ,"FBR"),"Windows File Browser",match(product,"JAV"),"Java Embedded App",match(product,"MTG"),"Secure
    Meeting") | stats values(app) AS Activity by user
```

✓ 7 events (4/20/21 8:00:00.000 PM to 4/21/21 8:58:45.000 PM)

user	Activity
malloryk	Java Embedded App
richards	Windows File Browser

Note: *You should determine the sourcetype in use in your environment and substitute it in these example searches as applicable.*

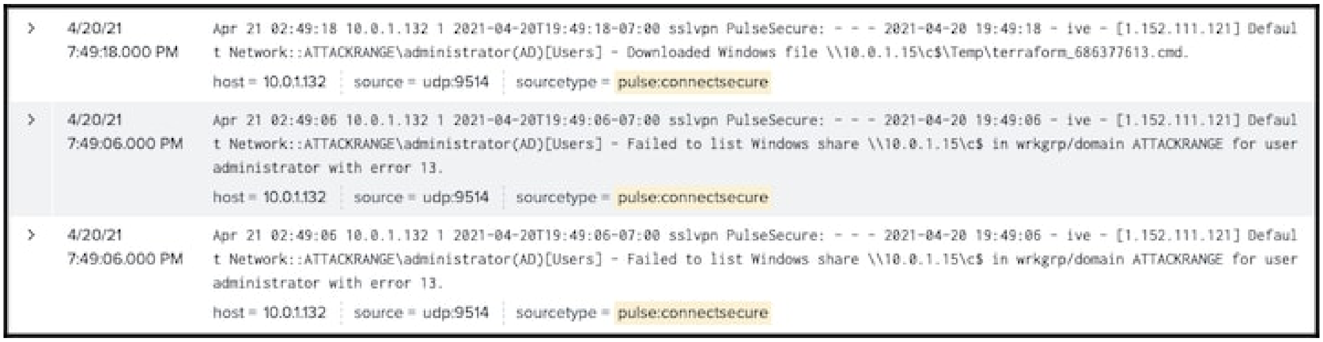
Alternatively, if your logging includes URIs, you may search for the following:

```
/dana/fb/smb/wfb.cgi for Windows File Share browsing activity
```

```
/dana/fb/smb/swsh.cgi   for Windows File Share activity
```

```
/dana-na/{meeting_base_URL}/meetingrun.cgi for Pulse Secure Collaboration activity
(where {meeting_base_URL} is the administrator-configured base URL for secure
meetings)
```

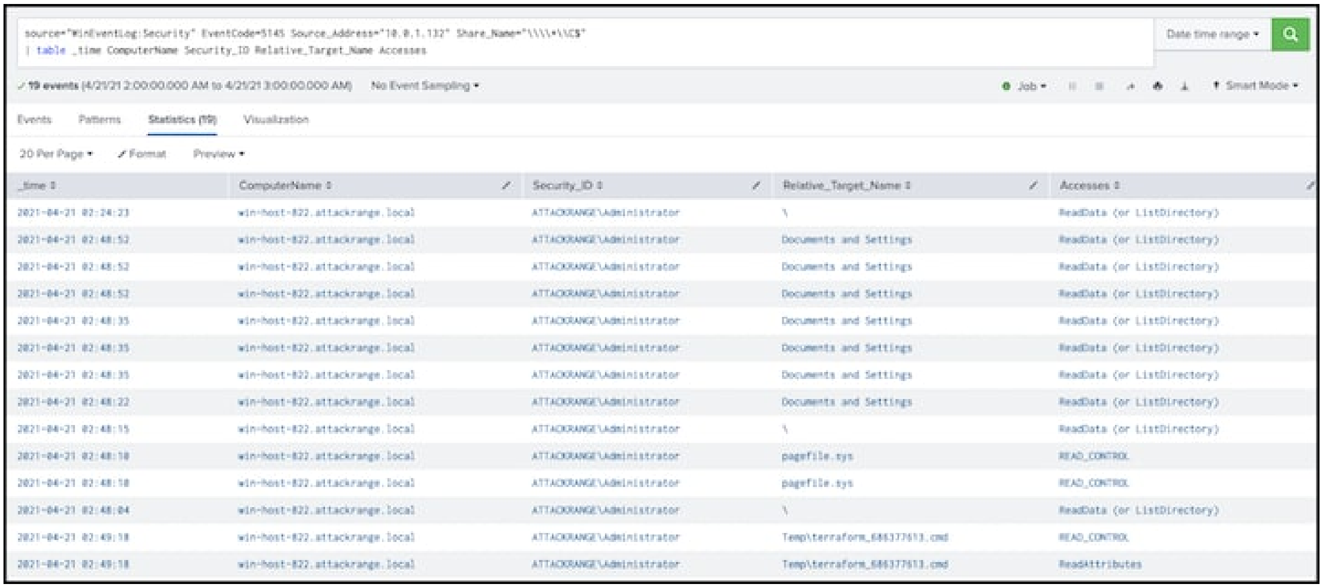
Depending on the logging configuration on the PCS appliance, events such as the ones below are logged when connections are attempted to access files on the Windows servers.



```
>  4/20/21          Apr 21 02:49:18 10.0.1.132 1 2021-04-20T19:49:18-07:00 sslvpn PulseSecure: - - - 2021-04-20 19:49:18 - ive - [1.152.111.121] Defaul
   7:49:18.000 PM   t Network::ATTACKRANGE\administrator(AD)[Users] - Downloaded Windows file \\10.0.1.15\c$\Temp\terraform_686377613.cmd.
                    host = 10.0.1.132 | source = udp:9514 | sourcetype = pulse:connectsecure
>  4/20/21          Apr 21 02:49:06 10.0.1.132 1 2021-04-20T19:49:06-07:00 sslvpn PulseSecure: - - - 2021-04-20 19:49:06 - ive - [1.152.111.121] Defaul
   7:49:06.000 PM   t Network::ATTACKRANGE\administrator(AD)[Users] - Failed to list Windows share \\10.0.1.15\c$ in wrkgrp/domain ATTACKRANGE for user
                    administrator with error 13.
                    host = 10.0.1.132 | source = udp:9514 | sourcetype = pulse:connectsecure
>  4/20/21          Apr 21 02:49:06 10.0.1.132 1 2021-04-20T19:49:06-07:00 sslvpn PulseSecure: - - - 2021-04-20 19:49:06 - ive - [1.152.111.121] Defaul
   7:49:06.000 PM   t Network::ATTACKRANGE\administrator(AD)[Users] - Failed to list Windows share \\10.0.1.15\c$ in wrkgrp/domain ATTACKRANGE for user
                    administrator with error 13.
                    host = 10.0.1.132 | source = udp:9514 | sourcetype = pulse:connectsecure
```

Turning to a familiar source of data that you may also be collecting, Windows Security event logs, the search below provides a way to gain insight into files being accessed through a share directly from Windows. This can be useful in case the PCS appliance is not logging this level of fidelity.

```
source="WinEventLog:Security" EventCode=5145 Source_Address=<IP Address of Pulse
devices> Share_Name="\\\\*\\C$"

| table _time ComputerName Security_ID Relative_Target_Name Accesses
```

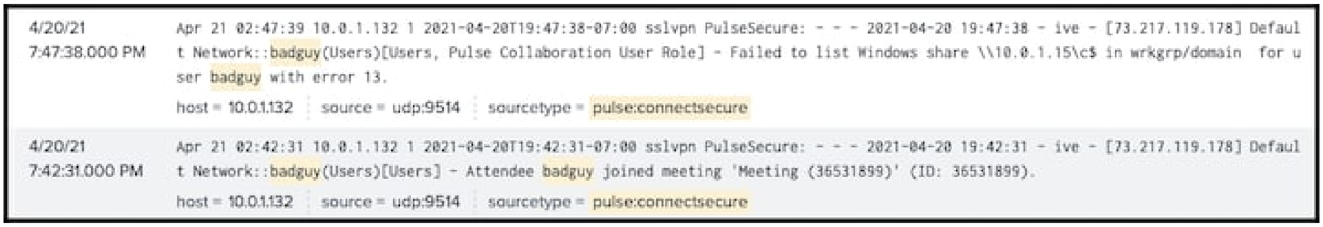


```
source="WinEventLog:Security" EventCode=5145 Source_Address="10.0.1.132" Share_Name="\\\\*\\C$"
| table _time ComputerName Security_ID Relative_Target_Name Accesses
```

✓ 19 events (4/21/21 2:00:00.000 AM to 4/21/21 3:00:00.000 AM)   No Event Sampling ▾

_time	ComputerName	Security_ID	Relative_Target_Name	Accesses
2021-04-21 02:24:23	win-host-822.attackrange.local	ATTACKRANGE\Administrator	\	ReadData (or ListDirectory)
2021-04-21 02:48:52	win-host-822.attackrange.local	ATTACKRANGE\Administrator	Documents and Settings	ReadData (or ListDirectory)
2021-04-21 02:48:52	win-host-822.attackrange.local	ATTACKRANGE\Administrator	Documents and Settings	ReadData (or ListDirectory)
2021-04-21 02:48:52	win-host-822.attackrange.local	ATTACKRANGE\Administrator	Documents and Settings	ReadData (or ListDirectory)
2021-04-21 02:48:35	win-host-822.attackrange.local	ATTACKRANGE\Administrator	Documents and Settings	ReadData (or ListDirectory)
2021-04-21 02:48:35	win-host-822.attackrange.local	ATTACKRANGE\Administrator	Documents and Settings	ReadData (or ListDirectory)
2021-04-21 02:48:35	win-host-822.attackrange.local	ATTACKRANGE\Administrator	Documents and Settings	ReadData (or ListDirectory)
2021-04-21 02:48:22	win-host-822.attackrange.local	ATTACKRANGE\Administrator	Documents and Settings	ReadData (or ListDirectory)
2021-04-21 02:48:15	win-host-822.attackrange.local	ATTACKRANGE\Administrator	\	ReadData (or ListDirectory)
2021-04-21 02:48:10	win-host-822.attackrange.local	ATTACKRANGE\Administrator	pagefile.sys	READ_CONTROL
2021-04-21 02:48:10	win-host-822.attackrange.local	ATTACKRANGE\Administrator	pagefile.sys	READ_CONTROL
2021-04-21 02:48:04	win-host-822.attackrange.local	ATTACKRANGE\Administrator	\	ReadData (or ListDirectory)
2021-04-21 02:49:18	win-host-822.attackrange.local	ATTACKRANGE\Administrator	Temp\terraform_686377613.cmd	READ_CONTROL
2021-04-21 02:49:18	win-host-822.attackrange.local	ATTACKRANGE\Administrator	Temp\terraform_686377613.cmd	ReadAttributes

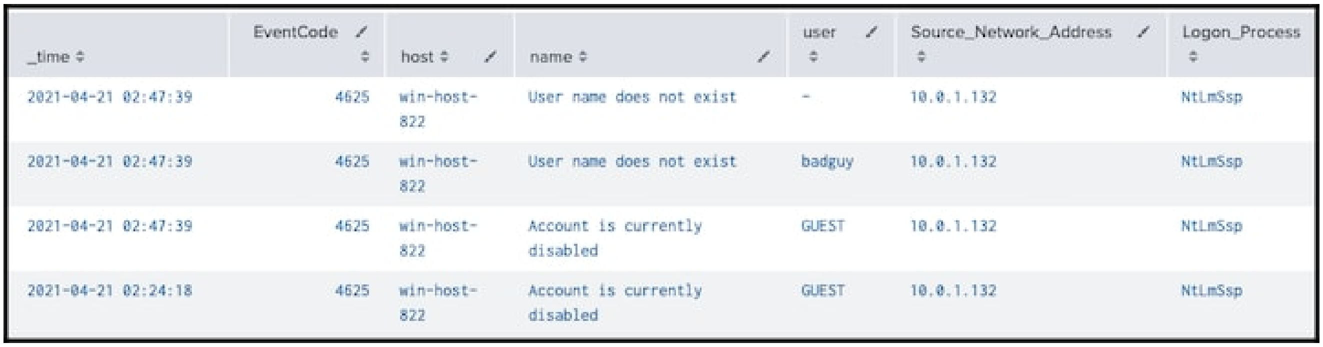
Similarly, if a share is attempted to be accessed without proper permissions, a Windows EventCode 4625 will trigger. Turning back to the Pulse Secure logs, in the example below, the user "badguy" successfully joins as shown in these events:



```
4/20/21          Apr 21 02:47:39 10.0.1.132 1 2021-04-20T19:47:38-07:00 sslvpn PulseSecure: - - - 2021-04-20 19:47:38 - ive - [73.217.119.178] Defaul
7:47:38.000 PM   t Network::badguy(Users)[Users, Pulse Collaboration User Role] - Failed to list Windows share \\10.0.1.15\c$ in wrkgrp/domain  for u
                 ser badguy with error 13.
                 host = 10.0.1.132   source = udp:9514   sourcetype = pulse:connectsecure

4/20/21          Apr 21 02:42:31 10.0.1.132 1 2021-04-20T19:42:31-07:00 sslvpn PulseSecure: - - - 2021-04-20 19:42:31 - ive - [73.217.119.178] Defaul
7:42:31.000 PM   t Network::badguy(Users)[Users] - Attendee badguy joined meeting 'Meeting (36531899)' (ID: 36531899).
                 host = 10.0.1.132   source = udp:9514   sourcetype = pulse:connectsecure
```

However, “badguy” tries to connect to a file share and is rejected. The following search sheds light on why he was not able to access the desired resource. In this example with LDAP configured on the Windows device, the "user name does not exist." This search can be used to determine why login events from that originate from the Pulse Server(s) are not authenticating successfully.

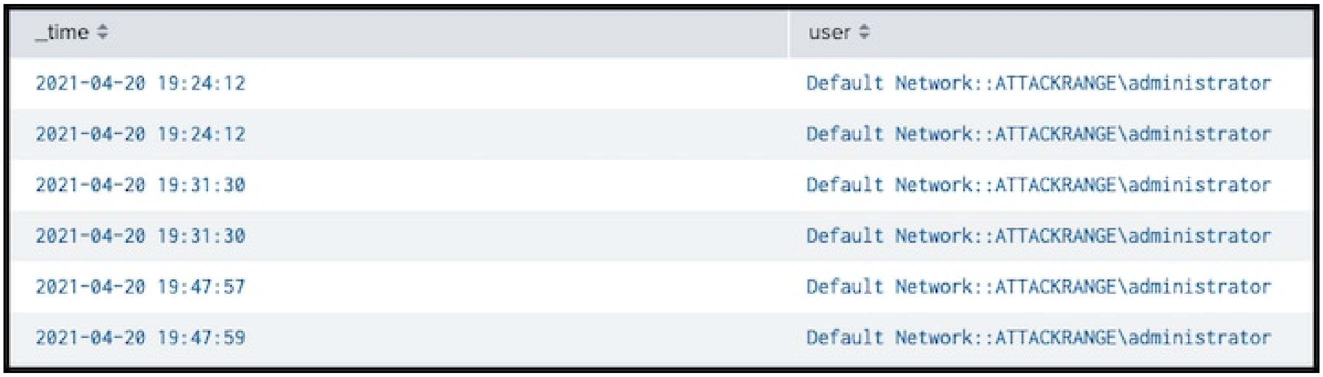
```
source="WinEventLog:Security" EventCode=4625  Source_Network_Address=<IP Address of
Pulse devices>

| table  _time EventCode hostname user Source_Network_Address Logon_Process
```



_time	EventCode	host	name	user	Source_Network_Address	Logon_Process
2021-04-21 02:47:39	4625	win-host-822	User name does not exist	-	10.0.1.132	NtLmSsp
2021-04-21 02:47:39	4625	win-host-822	User name does not exist	badguy	10.0.1.132	NtLmSsp
2021-04-21 02:47:39	4625	win-host-822	Account is currently disabled	GUEST	10.0.1.132	NtLmSsp
2021-04-21 02:24:18	4625	win-host-822	Account is currently disabled	GUEST	10.0.1.132	NtLmSsp

Why is all of that important? Because, it enables another potential detection. FireEye noted in their blog that “the malicious operations of SLOWPULSE can be detected via log correlation between the authentication servers responsible for LDAP and RADIUS auth and the VPN server. Authentication failures in either LDAP or RADIUS logs with the associated VPN logins showing success would be an anomalous event worthy of flagging.” The following search will return a listing of login events from Pulse that are tied into LDAP; in our case we are using Active Directory for LDAP so our realm is called AD.

```
sourcetype=pulse:connectsecure dest=<IP Address of Pulse devices> action=success
realm=AD
| table _time user
| sort + _time
```



_time	user
2021-04-20 19:24:12	Default Network::ATTACKRANGE\administrator
2021-04-20 19:24:12	Default Network::ATTACKRANGE\administrator
2021-04-20 19:31:30	Default Network::ATTACKRANGE\administrator
2021-04-20 19:31:30	Default Network::ATTACKRANGE\administrator
2021-04-20 19:47:57	Default Network::ATTACKRANGE\administrator
2021-04-20 19:47:59	Default Network::ATTACKRANGE\administrator

From there, we could take those Pulse logins and look for the failed login events, Event Code 4625. That search is above. Timestamps should be very close to one another, within seconds.

Note: *You should determine the sourcetype in use in your environment and substitute it in these example searches as applicable.*

Indicators of Compromise (IOCs)

FireEye/Mandiant published IOCs, including files, hashes, web shells, and sed patterns in their blog posts. Ivanti and CISA published additional IOCs (including additional hashes and affected URIs) in their respective posts. We have consolidated and converted these indicators into simple CSV format so that you may use them as lookup tables — and posted to Github here for review and consumption. But what's a lookup table, and how does it help with security detection in Splunk? Got you covered there, too.

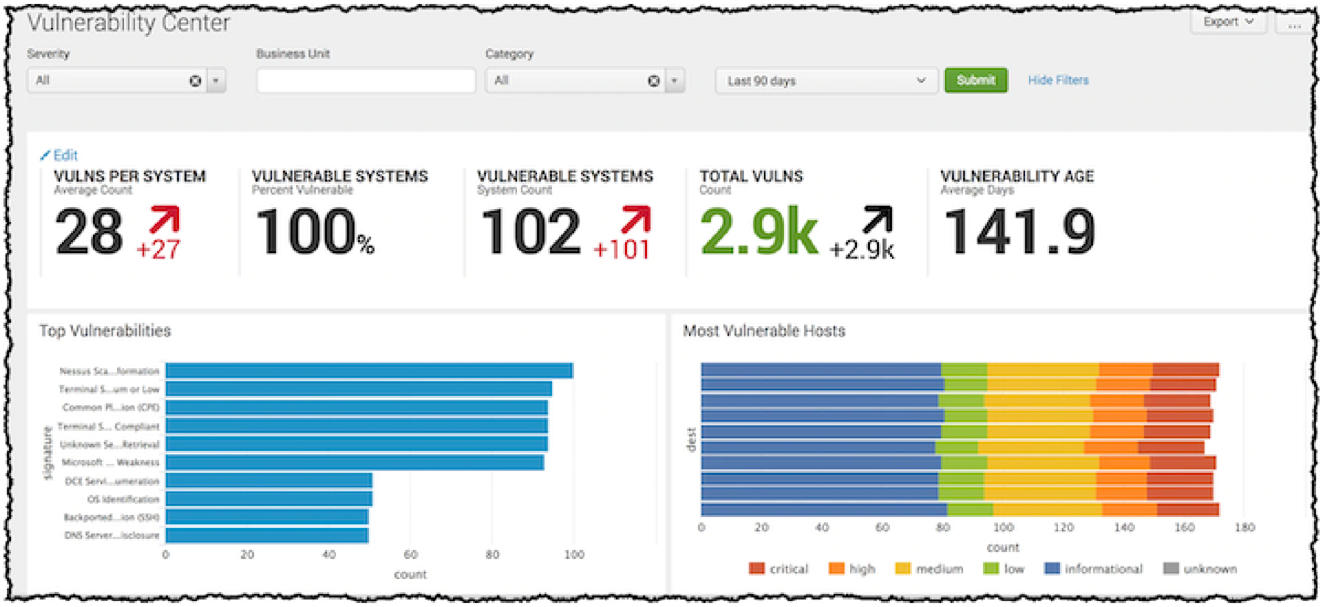
Webshells

Many of the attacks disclosed this week result in the installation of webshells on the PCS appliance. We felt it valuable to include a reference to this classic Youtube video from James Bower about how to hunt web shells with Splunk.

Splunk Enterprise Security

Know Thyself

While we have spent some time explaining this attack and effort needs to be put toward investigating this, it is also important to note that the basics are important. Basic asset management, hopefully via your asset and identity framework, will tell you where your vulnerable systems reside. Running regular vulnerability scans that integrate into Splunk will display which systems are vulnerable and can help you prioritize your patching schedule and better focus your detection efforts.



Vulnerability Center

Severity: All

Business Unit:

Category: All

Last 90 days

VULNS PER SYSTEM
Average Count
28 +27

VULNERABLE SYSTEMS
Percent Vulnerable
100%

VULNERABLE SYSTEMS
System Count
102 +101

TOTAL VULNS
Count
2.9k +2.9k

VULNERABILITY AGE
Average Days
141.9

Threat Intelligence Framework

You can also leverage the IOCs above (for those that don't want to scroll up, here they are) with Splunk Enterprise Security. The Threat Intelligence Framework can easily ingest these IOCs and Splunk Enterprise Security will let you know if any of them are identified. If you aren't sure how to do this, check out our recent blog post that walks you through the process of onboarding IOCs in Splunk Enterprise Security.

MITRE ATT&CK

Reviewing the blog posts from FireEye/Mandiant, we mapped the adversary's activity to MITRE ATT&CK. Each tactic is then linked to Splunk Content to help you hunt for that information. Be aware; these searches are provided as a way to accelerate your hunting. We recommend you configure them via the Splunk Security Essentials App. You may need to modify them to work in your environment! Many of these searches are optimized for use with the tstats command.

Finally, as more information becomes available, we will update these searches if more ATT&CK TTPs become known.

ATT&CK Tactic	Title	Splunk Searches
T1003	OS Credential Dumping	Many Detections

T1016	System Network Configuration Discovery	Detect processes used for System Network Configuration Discovery
T1021.001	Remote Desktop Protocol	Remote Desktop Network Bruteforce Remote Desktop Process Running On System Remote Desktop Network Traffic
T1027	Obfuscated Files or Information	Malicious PowerShell Process - Encoded Command
T1048	Exfiltration Over Alternative Protocol	Many Detections
T1053	Scheduled Task/Job	Many Detections
T1057	Process Discovery	Reconnaissance and Access to Processes and Services via Mimikatz modules Reconnaissance and Access to Operating System Elements via PowerSploit modules
T1059	Command and Scripting Interpreter	Many Detections
T1059.003	Windows Command Shell	Many Detections
T1070	Indicator Removal on Host	Many Detections
T1070.001	Clear Windows Event Logs	Windows Event Log Cleared

T1071.001	Web Protocols	TOR Traffic
T1082	System Information Discovery	System Information Discovery Detection Web Servers Executing Suspicious Processes
T1098	Account Manipulation	Many detections
T1105	Ingress Tool Transfer	CertUtil Download With URLCache and Split Arguments CertUtil Download With VerifyCtl and Split Arguments BITSAdmin Download File
T1136	Create Account	Many detections
T1140	Deobfuscate/Decode Files or Information	CertUtil With Decode Argument
T1190	Exploit Public Facing Application	SQL Injection with Long URLs
T1505.003	Web Shell	Supernova Webshell W3WP Spawning Shell Detect Exchange Web Shell
T1518	Software Discovery	Reconnaissance and Access to Operating System Elements via PowerSploit modules

T1554	Compromise Client Software Binary	Applying Stolen Credentials via Mimikatz modules Applying Stolen Credentials via PowerSploit modules
T1562	Impair Defenses	Many detections
T1569.002	Service Execution	Malicious Powershell Executed As A Service Create Service In Suspicious File Path First Time Seen Running Windows Service
T1574	Hijack Execution Flow	Detect Path Interception By Creation Of program exe Reg exe Manipulating Windows Services Registry Keys

Here is the full list of all the MITRE ATT&CK TTP’s that FireEye/Mandiant reported as being associated with malware/groups identified in this attack:

```
T1003,T1016, T1021.001, T1027, T1036.005, T1048, T1049, T1053, T1057, T1059,
T1059.003, T1070, T1070.001, T1070.004, T1071.001, T1082, T1098,
T1105,T1111,T1133,T1134.001,
T1136,T1140,T1190,T1505.003,T1518,T1554,T1556.004,T1592.004, T1562,T1569.002,T1574,
T1600
```

Conclusion

We know that these are significant vulnerabilities and that customers will want to patch as soon as possible and determine if they were affected by this attack. If you haven’t patched yet (we’ve all been there), hopefully, these searches will provide you the ability to have more visibility into your environment and any malicious activity that you might be experiencing. If they don’t work perfectly, think of them as "SplunkSpiration" :-). **As soon as we have more**

information, we will update this blog. Need Help? Splunk experts are here for you! Customers should reach out to their customer success manager, sales engineer, or regional sales manager.