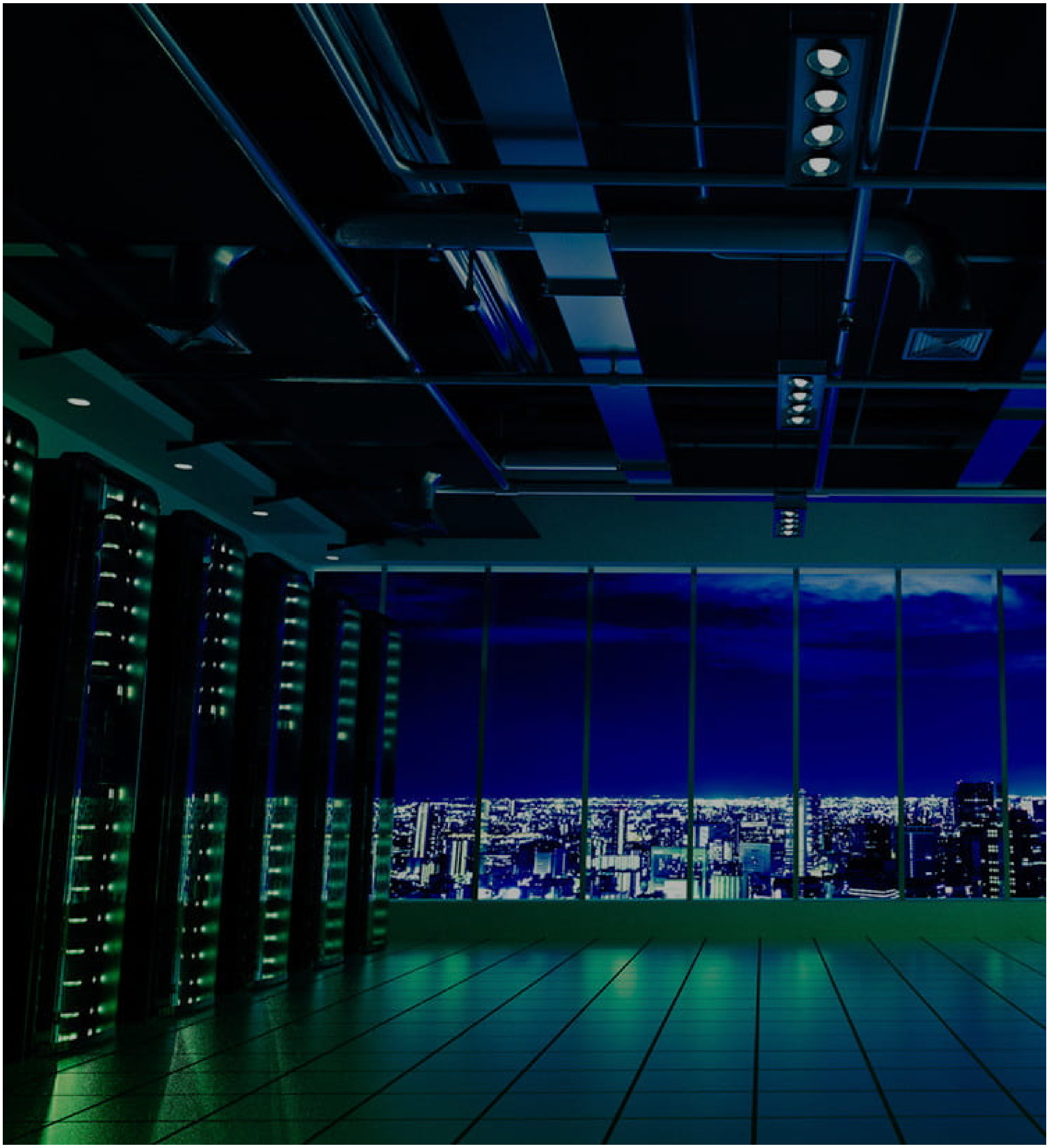
SUPERNOVA Web Shell Deployment Linked to SPIRAL Threat Group

secureworks.com/blog/supernova-web-shell-deployment-linked-to-spiral-threat-group

Counter Threat Unit Research Team

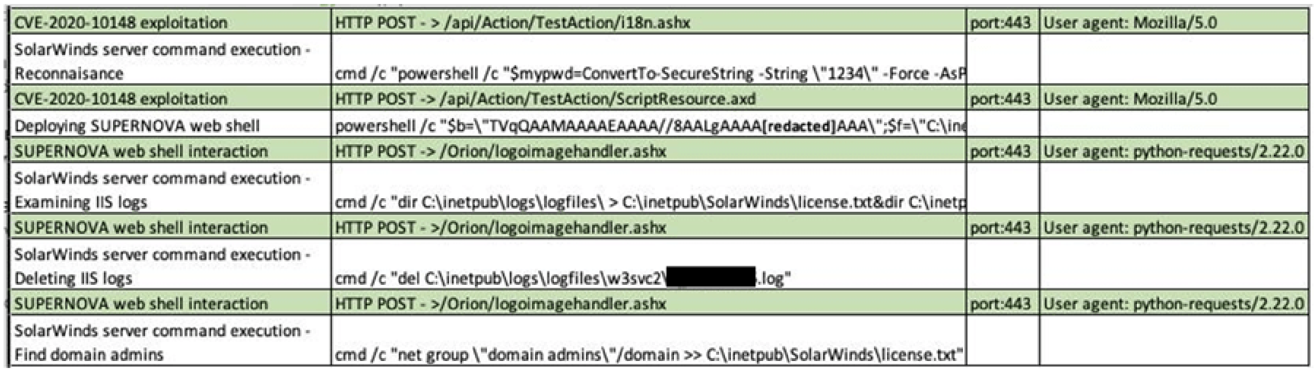


In late 2020, Secureworks® Counter Threat Unit™ (CTU) researchers observed a threat actor exploiting an internet-facing SolarWinds server to deploy the SUPERNOVA web shell. Additional analysis revealed similarities to intrusion activity identified on the same network earlier in 2020, suggesting the two intrusions are linked. CTU™ researchers attribute the intrusions to the SPIRAL threat group. Characteristics of the activity suggest the group is based in China.

SPIRAL threat group's SUPERNOVA deployment

During a November 2020 incident response engagement, Secureworks analysts observed a threat actor exploiting a vulnerability in the SolarWinds Orion Platform to deliver the SUPERNOVA web shell. CTU analysis indicates that this activity is unrelated to the SUNBURST supply chain attack that trojanized the SolarWinds Orion business software updates. CTU researchers attribute the SUPERNOVA activity to the SPIRAL espionage group.

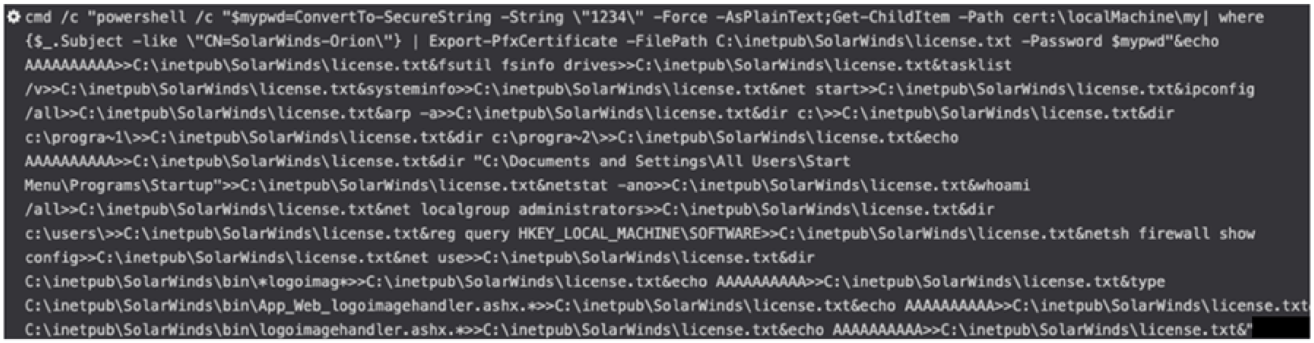
The threat actor exploited a SolarWinds Orion API authentication bypass vulnerability (CVE-2020-10148) to execute a reconnaissance script and then write the SUPERNOVA web shell to disk (see Figure 1).



CVE-2020-10148 exploitation	HTTP POST - > /api/Action/TestAction/i18n.ashx	port:443	User agent: Mozilla/5.0
SolarWinds server command execution - Reconnaisance	cmd /c "powershell /c "$mypwd=ConvertTo-SecureString -String \"1234\" -Force -AsP		
CVE-2020-10148 exploitation	HTTP POST -> /api/Action/TestAction/ScriptResource.axd	port:443	User agent: Mozilla/5.0
Deploying SUPERNOVA web shell	powershell /c "$b=\"TVqQAAMAAAAEAAAA//8AALgAAAA**[redacted]**AAA\";$f=\"C:\in		
SUPERNOVA web shell interaction	HTTP POST -> /Orion/logoimagehandler.ashx	port:443	User agent: python-requests/2.22.0
SolarWinds server command execution - Examining IIS logs	cmd /c "dir C:\inetpub\logs\logfiles\ > C:\inetpub\SolarWinds\license.txt&dir C:\inetp		
SUPERNOVA web shell interaction	HTTP POST - >/Orion/logoimagehandler.ashx	port:443	User agent: python-requests/2.22.0
SolarWinds server command execution - Deleting IIS logs	cmd /c "del C:\inetpub\logs\logfiles\w3svc2\[redacted].log"		
SUPERNOVA web shell interaction	HTTP POST - >/Orion/logoimagehandler.ashx	port:443	User agent: python-requests/2.22.0
SolarWinds server command execution - Find domain admins	cmd /c "net group \"domain admins\"/domain >> C:\inetpub\SolarWinds\license.txt"		

Figure 1. Sample HTTP POST requests sent to the SolarWinds server and corresponding commands executed on the host. (Source: Secureworks)

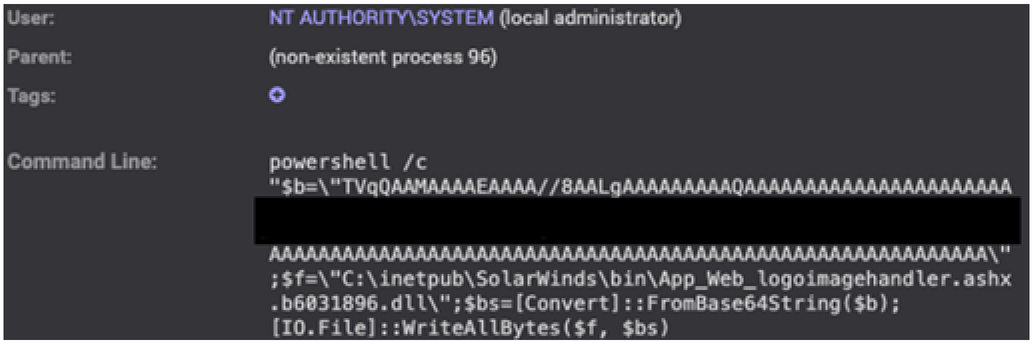
The reconnaissance script consisted of a series of commands concatenated using "&". The script wrote the output to C:\inetpub\SolarWinds\license.txt (see Figure 2).



```
cmd /c "powershell /c "$mypwd=ConvertTo-SecureString -String \"1234\" -Force -AsPlainText;Get-ChildItem -Path cert:\localMachine\my| where
 {$_.Subject -like \"CN=SolarWinds-Orion\"} | Export-PfxCertificate -FilePath C:\inetpub\SolarWinds\license.txt -Password $mypwd"&echo
 AAAAAAAAAA>>C:\inetpub\SolarWinds\license.txt&fsutil fsinfo drives>>C:\inetpub\SolarWinds\license.txt&tasklist
 /v>>C:\inetpub\SolarWinds\license.txt&systeminfo>>C:\inetpub\SolarWinds\license.txt&net start>>C:\inetpub\SolarWinds\license.txt&ipconfig
 /all>>C:\inetpub\SolarWinds\license.txt&arp -a>>C:\inetpub\SolarWinds\license.txt&dir c:\>>C:\inetpub\SolarWinds\license.txt&dir
 c:\progra~1\>>C:\inetpub\SolarWinds\license.txt&dir c:\progra~2\>>C:\inetpub\SolarWinds\license.txt&echo
 AAAAAAAAAA>>C:\inetpub\SolarWinds\license.txt&dir "C:\Documents and Settings\All Users\Start
 Menu\Programs\Startup">>C:\inetpub\SolarWinds\license.txt&netstat -ano>>C:\inetpub\SolarWinds\license.txt&whoami
 /all>>C:\inetpub\SolarWinds\license.txt&net localgroup administrators>>C:\inetpub\SolarWinds\license.txt&dir
 c:\users\>>C:\inetpub\SolarWinds\license.txt&reg query HKEY_LOCAL_MACHINE\SOFTWARE>>C:\inetpub\SolarWinds\license.txt&netsh firewall show
 config>>C:\inetpub\SolarWinds\license.txt&net use>>C:\inetpub\SolarWinds\license.txt&dir
 C:\inetpub\SolarWinds\bin\*logoimag*>>C:\inetpub\SolarWinds\license.txt&echo AAAAAAAAAA>>C:\inetpub\SolarWinds\license.txt&type
 C:\inetpub\SolarWinds\bin\App_Web_logoimagehandler.ashx.*>>C:\inetpub\SolarWinds\license.txt&echo AAAAAAAAAA>>C:\inetpub\SolarWinds\license.txt
 C:\inetpub\SolarWinds\bin\logoimagehandler.ashx.*>>C:\inetpub\SolarWinds\license.txt&echo AAAAAAAAAA>>C:\inetpub\SolarWinds\license.txt&"[redacted]
```

Figure 2. Reconnaissance script executed by exploiting CVE-2020-10148. (Source: Secureworks)

The SUPERNOVA web shell was written to disk using a PowerShell command (see Figure 3). SUPERNOVA is written in .NET C# and is a trojanized version of the legitimate DLL (app_web_logoimagehandler.ashx.b6031896.dll) used by the SolarWinds Orion Platform.

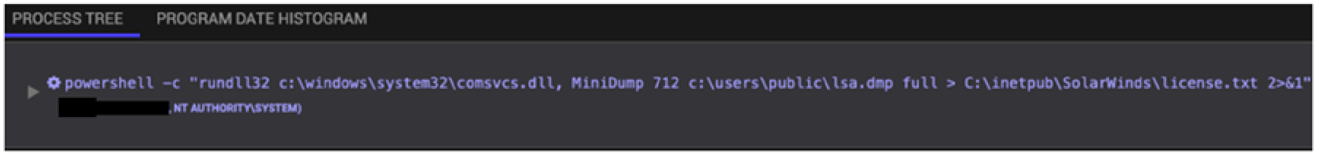


```
User:            NT AUTHORITY\SYSTEM (local administrator)
Parent:          (non-existent process 96)
Tags:            ○

Command Line:    powershell /c
                 "$b=\"TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAA
                 [redacted]
                 AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA\"
                 ;$f=\"C:\inetpub\SolarWinds\bin\App_Web_logoimagehandler.ashx
                 .b6031896.dll\";$bs=[Convert]::FromBase64String($b);
                 [IO.File]::WriteAllBytes($f, $bs)
```

Figure 3. Threat actor writing the SUPERNOVA web shell to disk. (Source: Secureworks)

The attacker interacted with the SUPERNOVA web shell to conduct additional reconnaissance activity using net, dir, and whoami commands. The threat actor obtained credentials by dumping the content of the LSASS process using the legitimate comsvcs.dll library (see Figure 4). The output of this process dump was also piped to the license.txt file, which the attacker subsequently retrieved and then deleted from disk.



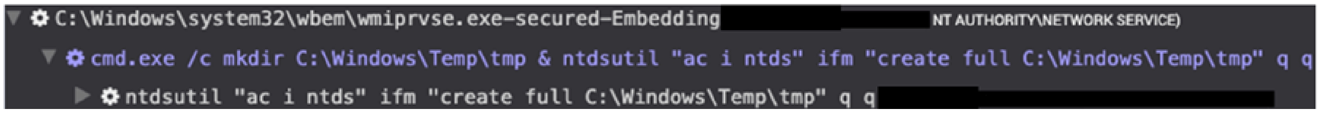
```
▶ powershell -c "rundll32 c:\windows\system32\comsvcs.dll, MiniDump 712 c:\users\public\lsa.dmp full > C:\inetpub\SolarWinds\license.txt 2>&1"
  [redacted], NT AUTHORITY\SYSTEM)
```

Figure 4. LSASS process dumped using comsvcs.dll library. (Source: Secureworks)

The threat actor then mapped network shares on two hosts: a domain controller and a server that could provide access to sensitive business information. The immediate and targeted nature of the lateral movement suggests that SPIRAL had prior knowledge of the network. Intervention and remediation by Secureworks incident responders blocked additional malicious activity.

Similarities to previous intrusion activity

Earlier in 2020, Secureworks incident responders identified intrusion activity on the same network. Analysis suggested that the threat actor initially gained access as early as 2018 by exploiting a vulnerable public-facing ManageEngine ServiceDesk server. The attacker used the access to periodically harvest and exfiltrate domain credentials. In August 2020, the threat actor returned to the network via the ManageEngine ServiceDesk server, harvested credentials from two servers (see Figure 5), likely exfiltrated these credentials through the ManageEngine server, and then used them to access files from Office 365-hosted SharePoint and OneDrive services.

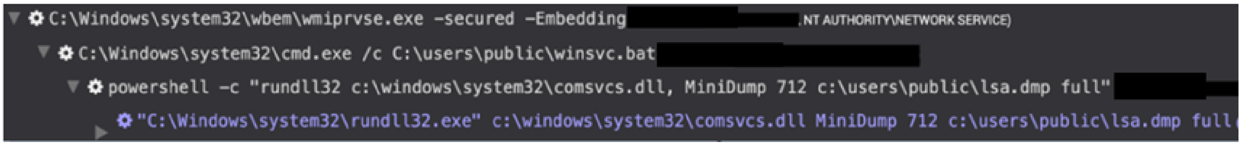


```
▼ ⚙ C:\Windows\system32\wbem\wmiprvse.exe-secured-Embedding [redacted] NT AUTHORITY\NETWORK SERVICE)
    ▼ ⚙ cmd.exe /c mkdir C:\Windows\Temp\tmp & ntdsutil "ac i ntds" ifm "create full C:\Windows\Temp\tmp" q q
        ▶ ⚙ ntdsutil "ac i ntds" ifm "create full C:\Windows\Temp\tmp" q q [redacted]
```

Figure 5. Threat actor running ntdsutil to dump the Active Directory database containing domain credentials. (Source: Secureworks)

CTU researchers were initially unable to attribute the August activity to any known threat groups. However, the following similarities to the SPIRAL intrusion in late 2020 suggest that the SPIRAL threat group was responsible for both intrusions:

- The threat actors used identical commands to dump the LSASS process via comsvcs.dll and used the same output file path (see Figure 6).

  ```
  ▼ ⚙ C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding [redacted] NT AUTHORITY\NETWORK SERVICE)
      ▼ ⚙ C:\Windows\system32\cmd.exe /c C:\users\public\winsvc.bat [redacted]
          ▼ ⚙ powershell -c "rundll32 c:\windows\system32\comsvcs.dll, MiniDump 712 c:\users\public\lsa.dmp full" [redacted]
              ▶ ⚙ "C:\Windows\system32\rundll32.exe" c:\windows\system32\comsvcs.dll MiniDump 712 c:\users\public\lsa.dmp full
  ```

  Figure 6. LSASS process dump from August 2020 using an identical command to the November 2020 incident. (Source: Secureworks)

- The same two servers were accessed: a domain controller and a server that could provide access to sensitive business data.
- The same ‘c:\users\public’ path (all lowercase) was used as a working directory.
- Three compromised administrator accounts were used in both intrusions.

Connections to China?

CTU researchers have associated Chinese threat groups with network intrusions involving the targeting of ManageEngine servers, maintenance of long-term access to periodically harvest credentials and exfiltrate data, and espionage or theft of intellectual property. Although SPIRAL activity shares these characteristics, the characteristics are insufficient for attributing SPIRAL’s country of origin. However, an additional characteristic of the August 2020 intrusion strengthens the Chinese connection.

A Secureworks endpoint detection and response (EDR) agent checked in from a host that did not belong to the compromised organization and used an IP address geolocated to China. The naming convention of this host was the same as another host used by the threat actor to connect to the network via a VPN connection. This ‘<*Username*>-PC’ naming convention is the default hostname for a Windows 7 host, but it is not the victim’s standard naming convention for hosts. CTU analysis suggests the threat group likely downloaded the endpoint agent installer from the network and executed it on the attacker-managed infrastructure. The exposure of the IP address was likely unintentional, so its geolocation supports the hypothesis that the SPIRAL threat group operates out of China.

Conclusion

Similarities between SUPERNOVA-related activity in November and activity that CTU researchers analyzed in August suggest that the SPIRAL threat group was responsible for both intrusions. Characteristics of these intrusions indicate a possible connection to China.

The abuse of vulnerabilities in both intrusions reinforces the importance of applying security updates as soon as possible. However, network breaches can occur even with preventative measures in place. Organizations should consider implementing an EDR solution for real-time network monitoring and alerting. CTU researchers also advise organizations to prepare and test a robust incident response plan.

Attribution is difficult, and members of the security community often have varying insights and perspectives. To facilitate information sharing, the CTU research team has published threat group profiles since May 2020. Fostering discussion within the community can lead to a better understanding of the threats. CTU researchers welcome insights about the SPIRAL threat group and its activity (threatgroupfeedback@secureworks.com).

Threat indicators

To mitigate exposure to this threat, CTU researchers recommend that organizations use available controls to review and restrict access using the indicators listed in Table 1. Note that IP addresses can be reallocated. The IP addresses may contain malicious content, so consider the risks before opening them in a browser.

Indicator	Type	Context
24.59.231.58	IP address	SPIRAL C2 server
24.59.231.62	IP address	SPIRAL C2 server
24.59.231.60	IP address	SPIRAL C2 server
24.59.231.61	IP address	SPIRAL C2 server

Indicator	Type	Context
24.59.231.59	IP address	SPIRAL C2 server
23.236.125.20	IP address	SPIRAL C2 server
76.237.140.245	IP address	SPIRAL C2 server
117.21.187.144	IP address	SPIRAL infrastructure located in China
56ceb6d0011d87b6e4d7023d7ef85676	MD5 hash	SUPERNOVA web shell delivered following exploitation of SolarWinds via CVE-2020-10148
75af292f34789a1c782ea36c7127bf6106f595e8	SHA1 hash	SUPERNOVA web shell delivered following exploitation of SolarWinds via CVE-2020-10148
c15abaf51e78ca56c0376522d699c978217bf041a3bd3c71d09193efa5717c71	SHA256 hash	SUPERNOVA web shell delivered following exploitation of SolarWinds via CVE-2020-10148

Table 1. Indicators for this threat.