THREAT BULLETINS

Russian State Hackers Targeted Centreon Servers in Years-Long Campaign

TLP:WHITE

Feb 16, 2021

The French Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), is stating that a group of Russian military hackers, known as the Sandworm group, have been behind a three-years-long operation during which they breached the internal networks of several French entities running the Centreon IT monitoring software.

On compromised systems, ANSSI discovered the presence of a backdoor in the form of a webshell dropped on several Centreon servers exposed to the internet. Centreon is a software developed by a company of the same name, its purpose is to monitor applications, networks and systems, similarly to SolarWinds Orion products. An open-source version exists under the GPL 2.0 license. The backdoor to Centreon systems was identified as being the P.A.S. webshell, version number 3.1.4. On the same servers, ANSSI found another backdoor identical to one described by ESET and named Exaramel.

P.A.S. can handle file operations, search the file system, interact with SQL databases, carry out brute-force password attacks against SSH, FTP, POP3, and MySQL, create a reverse shell, and run arbitrary PHP commands. Exaramel functions as a remote administration tool capable of shell command execution and copying files to and fro between an attacker-controlled server and the infected system. It also communicates using HTTPS with its C2 server to retrieve a list of commands to run.

The combination of these two methodologies has been linked to the Russia-linked state-sponsored threat actor known as Sandworm, which the Agence Nationale de la Sécurité des Systèmes d'Information has directly accused of initiating the attack. Cyber-attacks previously carried out by this group included the energy grid crashes across Ukraine in 2015 and 2016, the NotPetya ransomware outbreak of 2017, the attacks on the PyeongChang Winter Olympics opening ceremony in 2018, and a mass defacement of Georgian websites in 2019.

The first Centreon victim seems to have been compromised from late 2017. The campaign lasted until late 2020, but the ANSSI is now warning and urging both French and international organizations to inspect their Centreon installations for the presence of the two P.A.S. and Exaramel malware strains.

Reference(s)	ZDNet, CERT-FR, The Hacker News

Recommendations

- **System and security administrators should review the yara rules listed below and manually check their own Centreon systems for the malicious P.A.S. and Exaramel malware strains**
- Monitoring systems such as Centreon need to be highly intertwined with the monitored information system and therefore are a prime target for intrusion sets seeking lateralization.
    - It is recommended either not to expose these tools' web interfaces to Internet or to restrict such access using non-applicative authentication (TLS client certificate, basic authentication on the web server).

Yara Rules:

The Yara rules found below are just a collection found in the complete report from the ANSSI report, which can be accessed via the attached file. The four rules found below are related towards the three initial methodologies used by attackers to breach an organization.

```
rule PAS_webshell {

meta:

 author = "FR/ANSSI/SDO"

 description = "Detects P.A.S. PHP webshell - Based on DHS/FBI JAR-16-2029 (GrizzlySteppe)",

 TLP = "White

strings:

 $php = "<?php"

 $base64decode = /='base'\.\(\d+(\*|\/)\d+\)\.'_de'\.'code'/

 $strreplace = "(str_replace("

 $md5 = ".substr(md5(strrev($" nocase

 $gzinflate = "gzinflate"
```

```
 $cookie = "_COOKIE"

  $isset = "isset

condition:

 (filesize > 20KB and filesize < 200KB) and

 #cookie == 2 and

 #isset == 3 and

 all of them

}

rule PAS_webshell_ZIPArchiveFile {

meta:

 author = "FR/ANSSI/SDO"

 description = "Detects an archive file created by P.A.S. for download
operation"

 TLP = "White"

strings:

 $ = /Archive created by P\.A\.S\. v.{1,30}\nHost: : .{1,200}\nDate :[0-
9]{1,2}-[0-9]{1,2}-[0-9]{4}/

 condition:

 all of them

}

rule PAS_webshell_PerlNetworkScript {

meta:

 author = "FR/ANSSI/SDO"
```

```
 description = "Detects PERL scripts created by P.A.S. webshell to
supports network functionnalities"

 TLP = "White"

 strings:

 $pl_start = "#!/usr/bin/perl\n$SIG{'CHLD'}='IGNORE'; use
IO::Socket; use FileHandle;"

 $pl_status = "$o=\" [OK]\";$e=\"Error: \""

 $pl_socket = "socket(SOCKET, PF_INET, SOCK_STREAM,$tcp) or
die print \"$l$e$!$l"

 $msg1 = "print \"$lOK! I\\'m successful connected.$l\""

 $msg2 = "print \"$lOK! I\\'m accept connection.$l\""

condition:

 filesize < 6000 and

 ($pl_start at 0 and all of ($pl*)) or

 any of ($msg*)

}

rule PAS_webshell_SQLDumpFile {

meta:

 author = "FR/ANSSI/SDO"

 description = "Detects SQL dump file created by P.A.S. webshell"

 TLP = "White"

strings:

 $ = "-- [  SQL Dump created by P.A.S.  ] --"
```

condition:

all of them

}

Sources
France: Russian state hackers targeted Centreon servers in years-long campaign

CERT-FR: Rapport Menaces et Incidents du CERT-FR

Hacker News: Hackers Exploit IT Monitoring Tool Centreon to Target Several French Entities

Alert ID e8f2dacc

This Alert has 1 attachment(s). To view or download the attachment(s), click "View Alert" to login to the web portal.

View Alert

Tags ANSSI, Sandworm

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions or Comments Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.

For more update and alerts, visit: **https://health-isac.cyware.com**