PYSA Ransomware Gang adds Linux Support

lacework.com/blog/pysa-ransomware-gang-adds-linux-support/

September 9, 2021

Lacework Labs

September 9, 2021

Key Take Aways

- The first Linux version of ChaChi, a Golang based DNS tunneling backdoor, was recently observed on VirusTotal.
- The malware is configured to use domains associated with ransomware actors known as PYSA, aka Menipoza Ransomware Gang.
- PYSA's ChaChi infrastructure appears to have been largely dormant for the past several weeks, mostly parked and apparently no longer operational.
- We assess with moderate confidence this sample represents the PYSA actor expanding into targeting Linux hosts with ChaChi backdoor.

Background

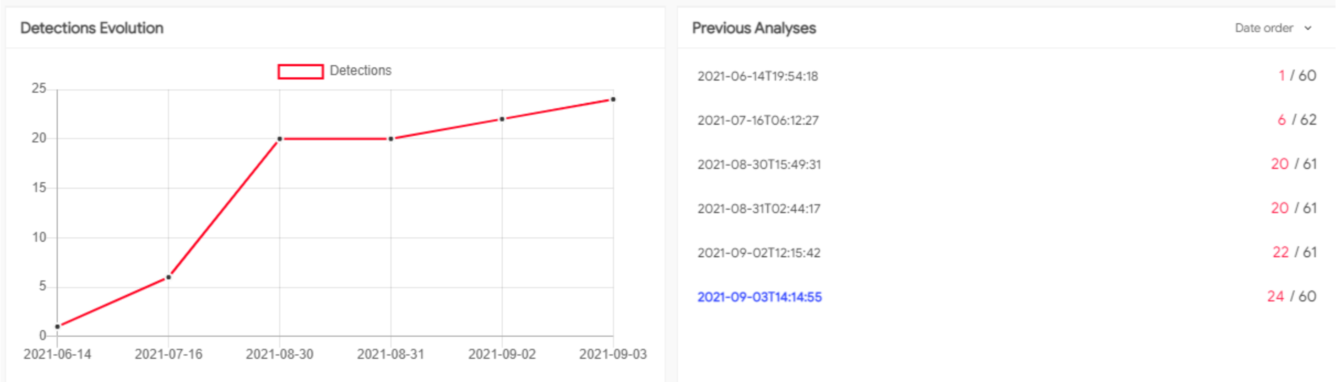
Ransomware is quickly expanding into Linux and Cloud networks as threat actors evolve their campaigns. For example, in recent weeks the BlackMatter ransomware gang, HelloKitty ransomware, and REvil ransomware were first observed expanding into Linux targeting through ESXi servers with ELF encryptors. Ransomware shifts to Linux targeting is an important trend to observe. Threat actors continue to evolve their campaigns by targeting Linux and cloud-centric networks.

Analysis

In August of 2021, Lacework Labs identified a Linux variant (MD5: 14abd57e8eb06191f12c0d84f9c1470b) of ChaChi. ChaChi refers to a customized variant of an open-source Golang based RAT that leverages DNS tunneling for C2 communication. The specimen was configured with domains that were reported by Palo Alto Networks in July:

- sbvjhs.xyz
- sbvjhs.club
- firefox-search.xyz

While the specimen was recently observed, it was uploaded to VirusTotal June 14th 2021, and only had 1/61 AV detections at the time. Following our tweet in late August, and as of this writing, it's currently at a 20/61 detection rate.

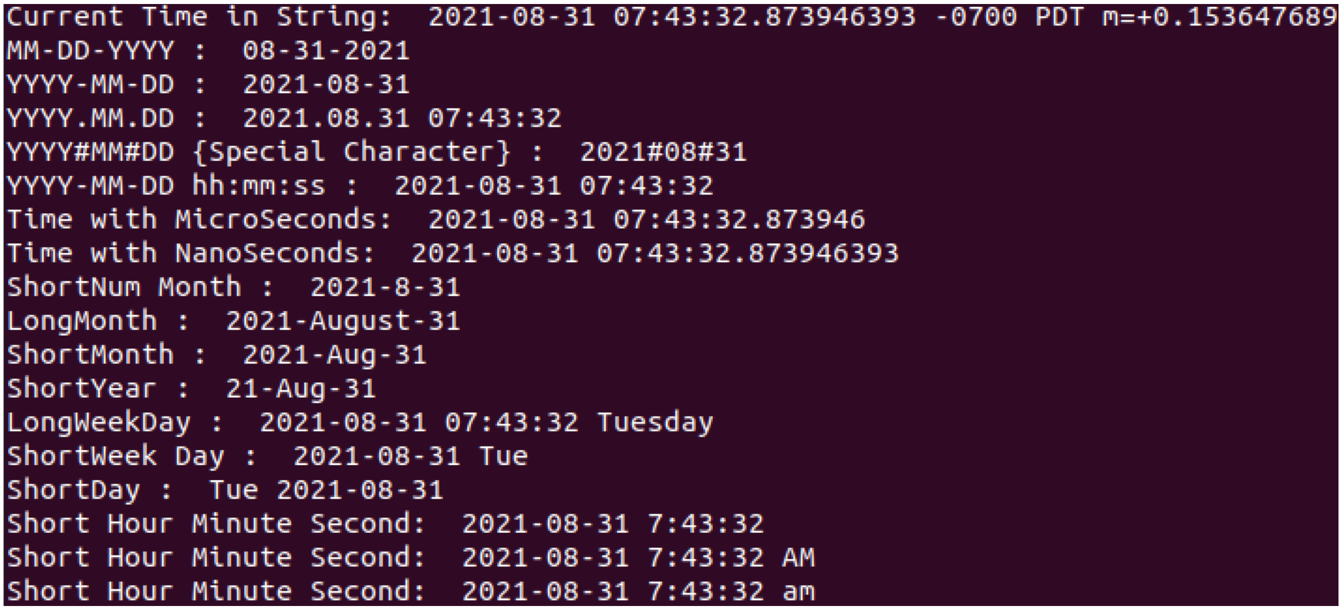

Detections Evolution

Previous Analyses

2021-06-14T19:54:18	1 / 60
2021-07-16T06:12:27	6 / 62
2021-08-30T15:49:31	20 / 61
2021-08-31T02:44:17	20 / 61
2021-09-02T12:15:42	22 / 61
2021-09-03T14:14:55	24 / 60

Figure 1. AV detection over time

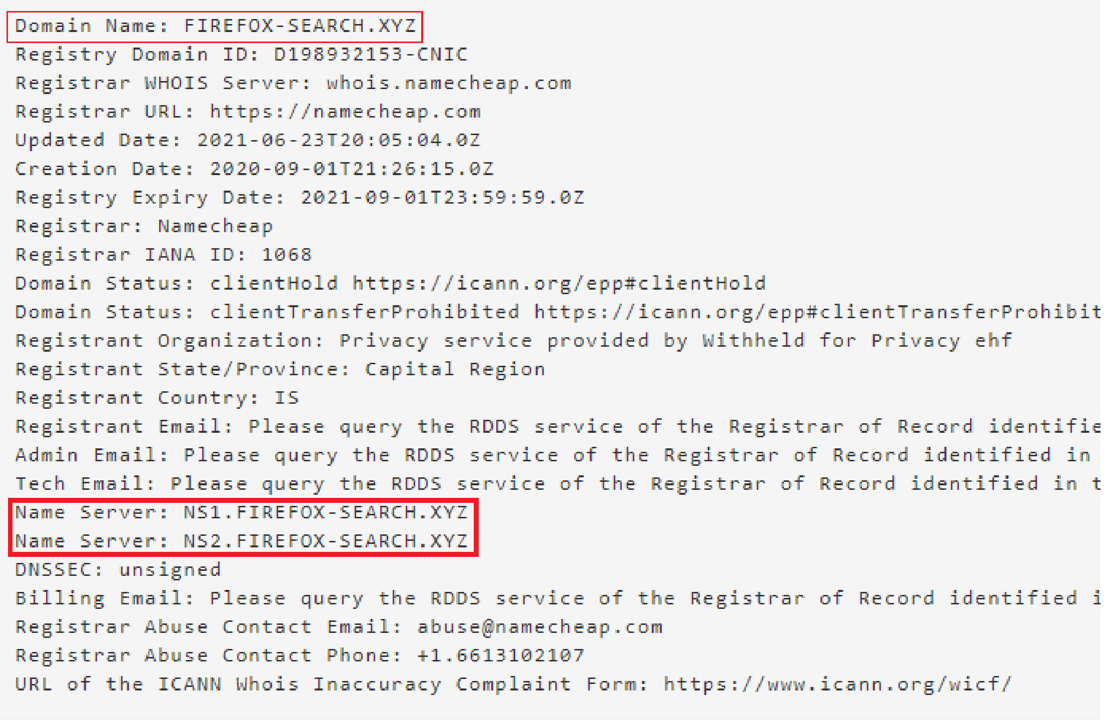
The Linux variant shares characteristics with its Windows counterpart, most notable being core functionality, the large file size (8MB +) and the use of Golang obfuscator Gobfuscate. A distinguishing characteristic of the Linux version was the presence of debug output containing datetime data.



```
Current Time in String:  2021-08-31 07:43:32.873946393 -0700 PDT m=+0.153647689
MM-DD-YYYY :  08-31-2021
YYYY-MM-DD :  2021-08-31
YYYY.MM.DD :  2021.08.31 07:43:32
YYYY#MM#DD {Special Character} :  2021#08#31
YYYY-MM-DD hh:mm:ss :  2021-08-31 07:43:32
Time with MicroSeconds:  2021-08-31 07:43:32.873946
Time with NanoSeconds:  2021-08-31 07:43:32.873946393
ShortNum Month :  2021-8-31
LongMonth :  2021-August-31
ShortMonth :  2021-Aug-31
ShortYear :  21-Aug-31
LongWeekDay :  2021-08-31 07:43:32 Tuesday
ShortWeek Day :  2021-08-31 Tue
ShortDay :  Tue 2021-08-31
Short Hour Minute Second:  2021-08-31 7:43:32
Short Hour Minute Second:  2021-08-31 7:43:32 AM
Short Hour Minute Second:  2021-08-31 7:43:32 am
```

Figure 2. Debug Output

ChaChi leverages custom nameservers that double as C2s to support the DNS tunneling protocol. As such the C2 hosts can be identified with passive DNS analysis of the name server domains. Analysis shows that the majority of ChaChi infrastructure has been parked or offline since 23-24 June 2021. The two exceptions to this appear to be domains ns1.ccenter.tech and ns2.spm.best.



```
Domain Name: FIREFOX-SEARCH.XYZ
Registry Domain ID: D198932153-CNIC
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: https://namecheap.com
Updated Date: 2021-06-23T20:05:04.0Z
Creation Date: 2020-09-01T21:26:15.0Z
Registry Expiry Date: 2021-09-01T23:59:59.0Z
Registrar: Namecheap
Registrar IANA ID: 1068
Domain Status: clientHold https://icann.org/epp#clientHold
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibit
Registrant Organization: Privacy service provided by Withheld for Privacy ehf
Registrant State/Province: Capital Region
Registrant Country: IS
Registrant Email: Please query the RDDS service of the Registrar of Record identifie
Admin Email: Please query the RDDS service of the Registrar of Record identified in
Tech Email: Please query the RDDS service of the Registrar of Record identified in t
Name Server: NS1.FIREFOX-SEARCH.XYZ
Name Server: NS2.FIREFOX-SEARCH.XYZ
DNSSEC: unsigned
Billing Email: Please query the RDDS service of the Registrar of Record identified i
Registrar Abuse Contact Email: abuse@namecheap.com
Registrar Abuse Contact Phone: +1.6613102107
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
```

Figure 3. C2 Whois and nameservers example

At the time of this blog, two domains from the Linux variant (sbvjhs.xyz and sbvjhs.club) resolved to Amazon IP address 99.83.154.118. This IP is an AWS Global accelerator host and has several AV detections on VirusTotal, however, our analysis indicates this is most likely used by Namecheap for domain parking purposes and should not be used as a ChaChi IOC. The following table lists known Chachi nameservers along with their resolutions. Several domains have been parked on either Amazon or Namecheap but these were filtered out.

HOSTNAME	IP_ADDR	ASN	COUNTRY	FIRST_SEEN	LAST_SEEN
ns1.englishdialoge.xyz	160.20.147.184	30823:"combahton GmbH"	Germany	Thu, 26 Nov 2020 23:27:18 -0800	Thu, 24 Jun 2021 09:22:03 -0700
ns2.englishdialoge.xyz	160.20.147.184	30823:"combahton GmbH"	Germany	Thu, 26 Nov 2020 23:27:18 -0800	Thu, 24 Jun 2021 09:22:03 -0700
ns1.englishdict.xyz	172.96.189.167	20068:"HAWKHOST"	Canada	Thu, 05 Nov 2020 03:39:33 -0800	Thu, 24 Jun 2021 06:26:43 -0700
ns2.englishdict.xyz	172.96.189.167	20068:"HAWKHOST"	Canada	Thu, 05 Nov 2020 03:39:33 -0800	Thu, 24 Jun 2021 06:26:43 -0700

ns1.english-breakfast.xyz	172.96.189.22	20068:”HAWKHOST”	Canada	Tue, 15 Dec 2020 15:45:14 -0800	Thu, 24 Jun 2021 13:38:42 -0700
ns1.english-breakfast.xyz	172.96.189.22	20068:”HAWKHOST”	Canada	Tue, 15 Dec 2020 15:45:14 -0800	Thu, 24 Jun 2021 13:38:42 -0700
ns1.pump-online.xyz	172.96.189.246	20068:”HAWKHOST”	Canada	Tue, 15 Dec 2020 15:45:55 -0800	Thu, 24 Jun 2021 05:00:38 -0700
ns2.english-breakfast.xyz	172.96.189.246	20068:”HAWKHOST”	Canada	Tue, 15 Dec 2020 15:45:14 -0800	Thu, 24 Jun 2021 13:38:42 -0700
ns2.english-breakfast.xyz	172.96.189.246	20068:”HAWKHOST”	Canada	Tue, 15 Dec 2020 15:45:14 -0800	Thu, 24 Jun 2021 13:38:42 -0700
ns2.pump-online.xyz	172.96.189.246	20068:”HAWKHOST”	Canada	Tue, 15 Dec 2020 15:45:55 -0800	Thu, 24 Jun 2021 05:00:38 -0700
ns1.blitzz.best	185.185.27.3	201206:”Droptop GmbH”	Germany	Sat, 06 Jun 2020 01:29:35 -0700	Wed, 02 Jun 2021 11:14:52 -0700
ns2.blitzz.best	185.185.27.3	201206:”Droptop GmbH”	Germany	Sat, 06 Jun 2020 01:29:35 -0700	Wed, 02 Jun 2021 11:14:52 -0700
ns1.firefox-search.xyz	185.186.245.85	40824:”WZCOM”	United States	Mon, 07 Sep 2020 15:35:41 -0700	Wed, 23 Jun 2021 07:31:39 -0700
ns2.firefox-search.xyz	185.186.245.85	40824:”WZCOM”	United States	Mon, 07 Sep 2020 15:35:41 -0700	Wed, 23 Jun 2021 07:31:39 -0700
ns1.reportservicefuture.website	185.193.38.60	57878:”Prager Connect GmbH”	France	Sat, 09 May 2020 11:04:41 -0700	Sun, 02 May 2021 08:04:13 -0700

ns2.reportservicefuture.website	185.193.38.60	57878:”Prager Connect GmbH”	France	Sat, 09 May 2020 11:04:41 -0700	Sun, 02 May 2021 08:04:13 -0700
ns1.wiki-text.xyz	193.239.84.205	9009:”M247 Ltd”	United Kingdom	Thu, 03 Sep 2020 15:58:08 -0700	Wed, 23 Jun 2021 08:18:42 -0700
ns2.wiki-text.xyz	193.239.84.205	9009:”M247 Ltd”	United Kingdom	Thu, 03 Sep 2020 15:58:08 -0700	Wed, 23 Jun 2021 08:18:42 -0700
ns1.visual-translator.xyz	193.239.85.55	9009:”M247 Ltd”	Romania	Thu, 03 Sep 2020 14:35:02 -0700	Wed, 23 Jun 2021 08:18:41 -0700
ns2.visual-translator.xyz	193.239.85.55	9009:”M247 Ltd”	Romania	Thu, 03 Sep 2020 14:35:02 -0700	Wed, 23 Jun 2021 08:18:41 -0700
ns1.sbvjhs.xyz	194.187.249.102	9009:”M247 Ltd”	France	Sat, 01 Aug 2020 21:29:06 -0700	Wed, 23 Jun 2021 07:08:08 -0700
ns2.sbvjhs.xyz	194.187.249.102	9009:”M247 Ltd”	France	Sat, 01 Aug 2020 21:29:06 -0700	Wed, 23 Jun 2021 07:08:08 -0700
ns1.statistics-update.xyz	194.5.249.18	64398:”Nxtservers Srl”	Romania	Fri, 31 Jul 2020 09:23:54 -0700	Wed, 23 Jun 2021 06:56:20 -0700
ns2.statistics-update.xyz	194.5.249.18	64398:”Nxtservers Srl”	Romania	Fri, 31 Jul 2020 09:23:54 -0700	Wed, 23 Jun 2021 06:56:20 -0700
ns1.accounting-consult.xyz	194.5.249.180	64398:”Nxtservers Srl”	Romania	Sun, 02 Aug 2020 06:27:13 -0700	Wed, 23 Jun 2021 07:37:33 -0700
ns2.accounting-consult.xyz	194.5.249.180	64398:”Nxtservers Srl”	Romania	Sun, 02 Aug 2020 06:27:13 -0700	Wed, 23 Jun 2021 07:37:33 -0700

ns1.ntservicepack.com	194.5.250.216	64398:”Nxtservers Srl”	Romania	Wed, 29 Apr 2020 10:19:42 -0700	Tue, 24 Nov 2020 00:58:02 -0800
ns2.ntservicepack.com	194.5.250.216	64398:”Nxtservers Srl”	Romania	Wed, 29 Apr 2020 10:19:42 -0700	Tue, 24 Nov 2020 00:58:02 -0800
ns1.starhouse.xyz	198.252.100.37	20068:”HAWKHOST”	United States	Thu, 26 Nov 2020 21:55:56 -0800	Thu, 24 Jun 2021 14:24:10 -0700
ns2.starhouse.xyz	198.252.100.37	20068:”HAWKHOST”	United States	Thu, 26 Nov 2020 21:55:56 -0800	Thu, 24 Jun 2021 14:24:10 -0700
ns1.ccenter.tech	23.83.133.136	19148:”LEASEWEB-USA-PHX-11”	United States	Wed, 24 Mar 2021 12:30:02 -0700	Tue, 31 Aug 2021 04:10:51 -0700
ns2.ccenter.tech	23.83.133.136	19148:”LEASEWEB-USA-PHX-11”	United States	Wed, 24 Mar 2021 12:30:02 -0700	Tue, 31 Aug 2021 04:10:51 -0700
ns1.transnet.wiki	45.147.228.49	30823:”combahton GmbH”	Germany	Wed, 24 Mar 2021 12:30:03 -0700	Wed, 23 Jun 2021 08:13:07 -0700
ns2.transnet.wiki	45.147.228.49	30823:”combahton GmbH”	Germany	Wed, 24 Mar 2021 12:30:03 -0700	Wed, 23 Jun 2021 08:13:07 -0700
ns1.productoccup.tech	45.147.229.29	30823:”combahton GmbH”	Germany	Tue, 23 Mar 2021 03:17:32 -0700	Thu, 24 Jun 2021 07:16:58 -0700
ns2.productoccup.tech	45.147.229.29	30823:”combahton GmbH”	Germany	Tue, 23 Mar 2021 03:17:32 -0700	Thu, 24 Jun 2021 07:16:58 -0700
ns2.spm.best	72.52.178.23	32244:”LIQUIDWEB”	United States	Fri, 23 Jul 2021 04:32:25 -0700	Tue, 31 Aug 2021 06:03:43 -0700

ns1.sbvjhs.club	89.38.225.208	9009:"M247 Ltd"	Singapore	Sun, 02 Aug 2020 05:45:47 -0700	Wed, 23 Jun 2021 11:33:13 -0700
ns2.sbvjhs.club	89.38.225.208	9009:"M247 Ltd"	Singapore	Sun, 02 Aug 2020 05:45:47 -0700	Wed, 23 Jun 2021 11:33:13 -0700
ns1.serchtext.xyz	89.41.26.173	9009:"M247 Ltd"	United States	Mon, 02 Nov 2020 13:30:18 -0800	Thu, 24 Jun 2021 06:26:39 -0700
ns2.serchtext.xyz	89.41.26.173	9009:"M247 Ltd"	United States	Mon, 02 Nov 2020 13:30:18 -0800	Thu, 24 Jun 2021 06:26:39 -0700

Conclusion

Many actors target multiple architectures to increase their footprint, so this may be the motive here and could represent an evolution in PYSA operations. It is currently unclear if the Linux variant was used in operations, however it was observed prior to the associated infrastructure going offline. The observed debug output however may indicate the specimen is still in the testing phase.

Ransomware is hugely lucrative and actors are continuously looking for any edge that will increase their profits. While ransomware activity involving Linux Servers and cloud infrastructure remains rare, it still poses a real threat to business operations and customer data. Indicators for this activity are available on the Lacework Labs's Github. If you found this blog useful then please share and follow us on LinkedIn and Twitter!