New Play Ransomware Linux Variant Targets ESXi Shows Ties With Prolific Puma

By Cj Arsley Mateo, Darrel Tristan Virtusio, Sarah Pearl Camiling, Andrei Alimboyao, Nathaniel Morales, Jacob Santos, Earl John Bareng (words)

Published: 2024-07-19 · Archived: 2026-04-06 01:50:35 UTC

Ransomware

Trend Micro threat hunters discovered that the Play ransomware group has been deploying a new Linux variant that targets ESXi environments. Read our blog entry to know more.

By: Cj Arsley Mateo, Darrel Tristan Virtusio, Sarah Pearl Camiling, Andrei Alimboyao, Nathaniel Morales, Jacob Santos, Earl John Bareng Jul 19, 2024 Read time: 8 min (2104 words)

Summary:

- The Playnews article ransomware group, known for its double-extortion tactic, now has a Linux variant targeting ESXi environments.
- Most attacks this year have been concentrated in the US.
- This ransomware verifies if it is running on an ESXi environment before executing. It has successfully evaded security measures, as indicated by VirusTotal.
- The Play ransomware group appears to be using the services and infrastructure peddled by the Prolific Puma group.

Our Threat Hunting team uncovered a Linux variant of the Play ransomware that only encrypts files when running in a VMWare ESXi environment. First detected in June 2022, the Play ransomware group became notable for its double-extortion tactic, evasion techniques, custom-built tools, and substantial impact on various organizations in Latin America.

This is the first time that we've observed Play ransomware targeting ESXi environments. This development suggests that the group could be broadening its attacks across the Linux platform, leading to an expanded victim pool and more successful ransom negotiations.

VMWare ESXi environments are commonly used by businesses to run multiple virtual machines (VMs). They often host critical applications and data, and normally include integrated backup solutions. Compromising them can significantly disrupt business operations and even encrypt backups, which further reduces the victim's capability to recover data.

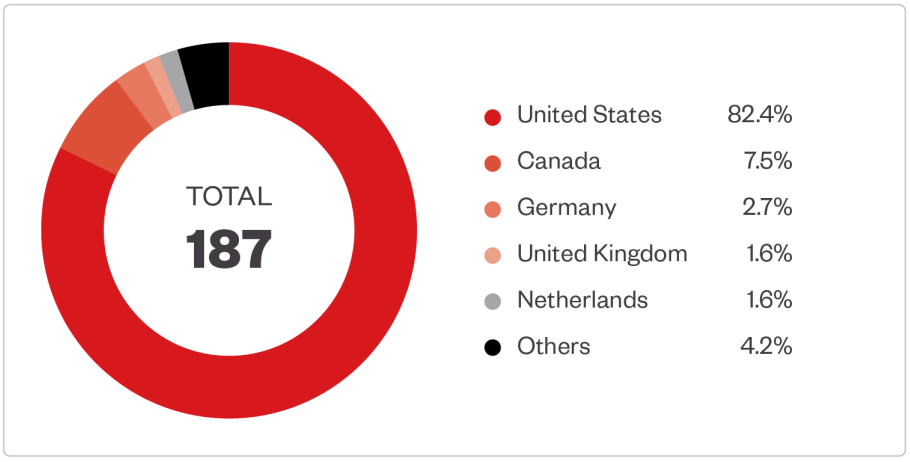

Figure 1. Based on ransomware.live, the US is the top country with the most victim counts by the Play ransomware group from January to July 2024

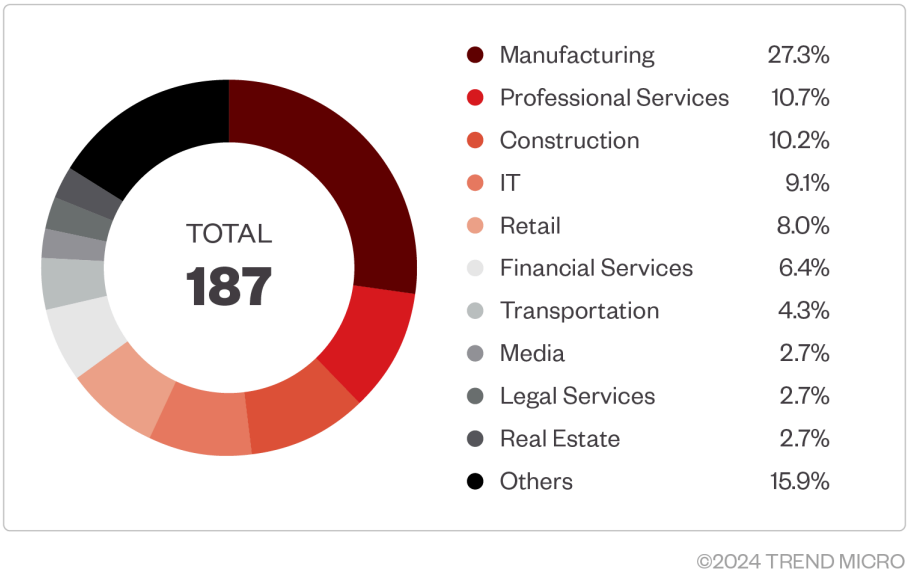

Figure 2. Manufacturing and professional services are the top industries affected by the Play ransomware group from January to July 2024

The submitted sample in VirusTotal indicates that it has managed to evade security detections. In our analysis, we found that the Linux variant is compressed in a RAR file with its Windows variant and is hosted in the URL, *hxxp://108.[BLOCKED].190/FX300.rar*.

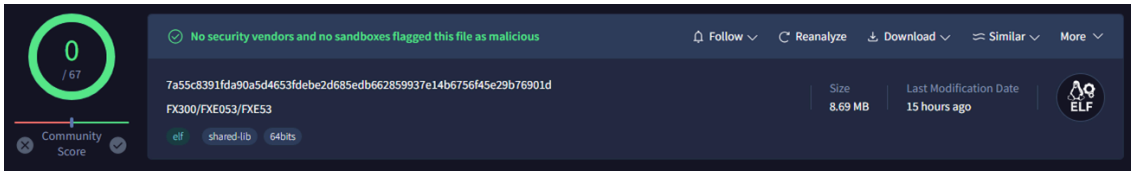

Figure 3. The Linux variant of Play ransomware showed 0 detections in VirusTotal.

This IP address contains tools that were used by Play ransomware in their previous attacks — including PsExec, NetScan, WinSCP, WinRAR, and the Coroxy backdoor.

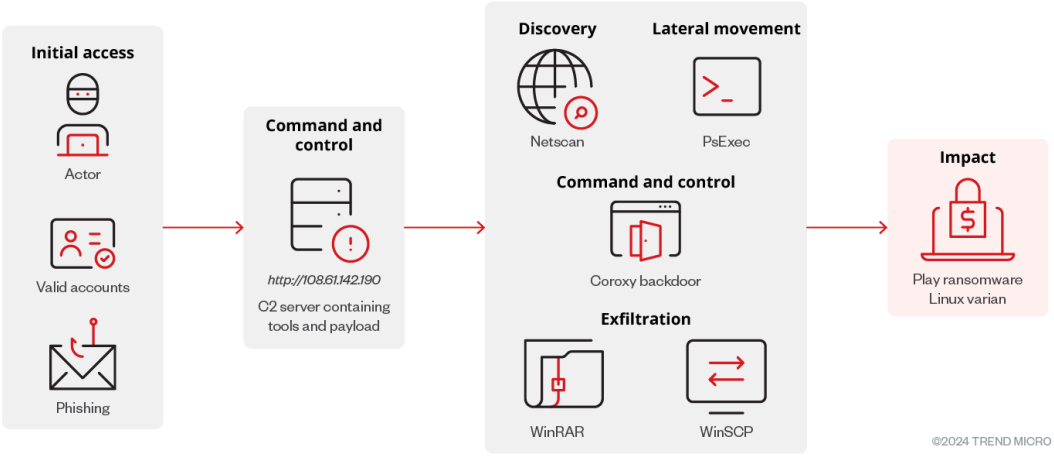

Figure 4. The infection chain of the Linux variant of Play ransomware includes the use of several tools.

Figure 4 shows the infection chain of this ransomware variant. Though no actual infection has been observed, the command-and-control (C&C) server hosts the common tools that Play ransomware currently uses in its attacks. This could denote that the Linux variant might employ similar tactics, techniques, and procedures (TTPs).

Infection Routine of the Linux Variant of Play Ransomware

Like its Windows variant, the sample accepts command-line arguments, but their behaviors are still unknown.

Play Ransomware Windows Variant	**Description**	**Play Ransomware Linux Variant**	**Description**
-mc	Execute normal functionality; same as no command-line argument	-p	N/A
-d <drive path>	Encrypt a specific drive	-f	N/A

-ip <shared resource path> <username> <password>	Encrypt network shared resource	-s	N/A
-p <path>	Encrypt a specific folder/file	-e	N/A

Table 1. The command-line arguments of the Windows and Linux variants of Play ransomware include commands for encrypting drives, files, and network shared resources.

The sample runs ESXi-related commands to check that it is running in an ESXi environment before performing its malicious routines. Otherwise, it will terminate and delete itself.

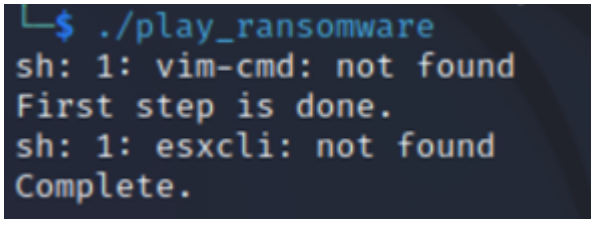

Figure 5. Error logs indicate that the vim-cmd and esxcli commands are missing. These commands are specific to the ESXi environment.

We also found a series of shell script commands that the sample executes once it is running in an ESXi environment. The command below is responsible for scanning and powering off all VMs found in the environment:

/bin/sh -c “for vmid in $(vim-cmd vmsvc/getallvms | grep -v Vmid | awk '{print $1}'); do vim-cmd vmsvc/power.off $vmid; done"

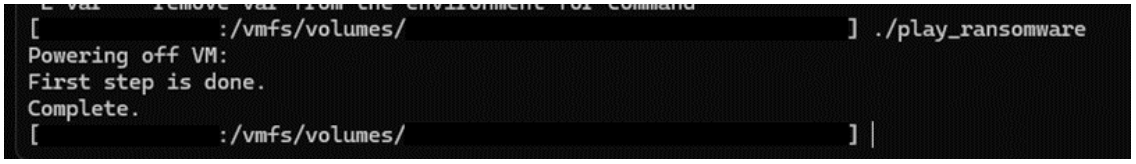

Figure 6: Once the ransomware runs successfully, it turns off any running VMs using the command, esxcli.

This command is responsible for setting a custom welcome message on the ESXi host:

/bin/sh -c “esxcli system welcomemsg set -m=\"

Once the ransomware executes the series of ESXi-related commands, it proceeds to encrypt VM files, including VM disk, configuration, and metadata files. The VM disk file, for example, contains critical data, including applications and user data.

```
aVmdk           db '.vmdk',0
aVmem           db '.vmem',0
aVmsd           db '.vmsd',0
aVmsn           db '.vmsn',0
aVmx            db '.vmx',0
aVmxf           db '.vmxf',0
aVswp           db '.vswp',0
aVmss           db '.vmss',0
aNvram          db '.nvram',0
aVmtx           db '.vmtx',0
aLog            db '.log',0
```

Figure 7. List of extensions to be encrypted

After completing the process, most of the encrypted files inside the guest OS “ubuntu” (as an example) are appended with the extension “.PLAY”.

```
[              :/vmfs/volumes/                                  /ubuntu] ls
ubuntu-000001-delta.vmdk.PLAY  ubuntu-flat.vmdk.PLAY
ubuntu-000001.vmdk.PLAY        ubuntu.nvram.PLAY
ubuntu-000002-delta.vmdk.PLAY  ubuntu.scoreboard
ubuntu-000002.vmdk.PLAY        ubuntu.vmdk.PLAY
ubuntu-1.scoreboard            ubuntu.vmsd.PLAY
ubuntu-2.scoreboard            ubuntu.vmx.PLAY
ubuntu-3.scoreboard            vmware-1.log.PLAY
ubuntu-Snapshot4.vmsn.PLAY     vmware-2.log.PLAY
ubuntu-Snapshot5.vmsn.PLAY     vmware-3.log.PLAY
ubuntu-aux.xml                 vmware.log.PLAY
[              :/vmfs/volumes/                                  /ubuntu]
```

Figure 8. Most of the VM files encrypted by the ransomware will have the .PLAY extension.

It will also drop a ransom note in the root directory, which is also displayed in the login portal of the ESXi client.

```
[              :~] cat PLAY_Readme.txt
PLAY
news portal, tor network links:
                                                                .onion
                                                                .onion
              @gmx.de[              :~]
```

Figure 9. The ransom note named PLAY_Readme.txt contains links to the Tor network.

Figure 10. The login portal of the affected ESXi server also displays the ransom note.

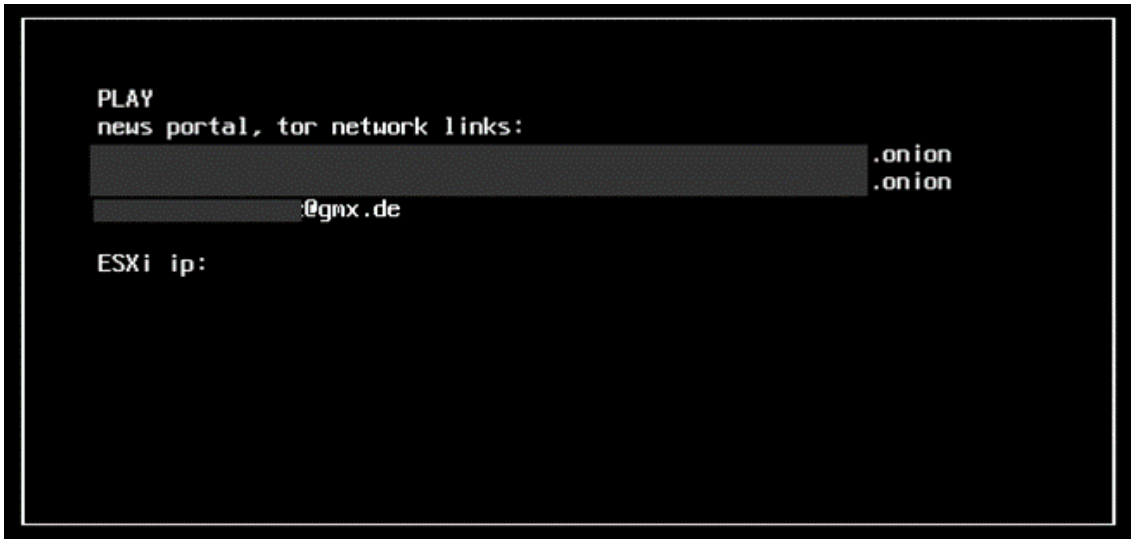

Figure 11. Once the ESXi system is rebooted, the ransom note will also appear in the console.

Exploring the Connection Between Prolific Puma and Play Ransomware

Monitoring the external activities of the suspicious IP address, we saw that the URL used to host the ransomware payload and its tools is related to another threat actor, which is named Prolific Puma**.**

Prolific Puma is known to generate domain names using a random destination generator algorithm (RDGA) and utilizes them to offer a link-shortening service to fellow cybercriminals, who then use it to avoid detection while disseminating phishing schemes, scams, and malware.

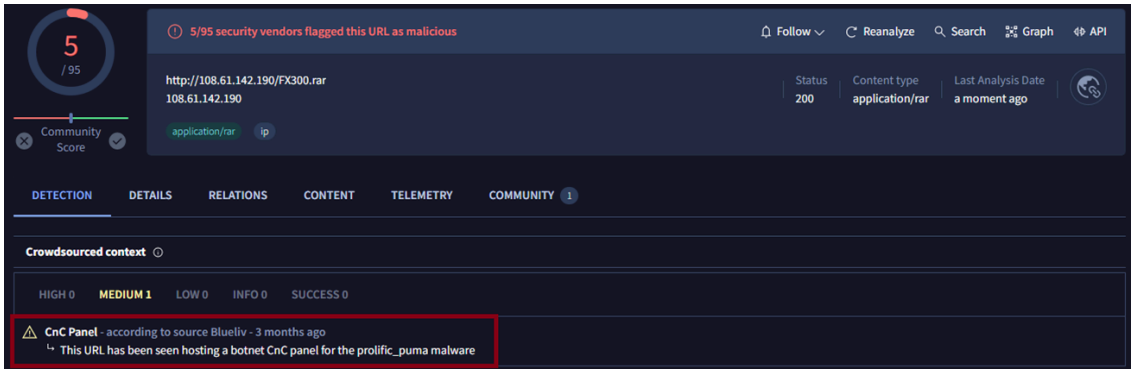

Figure 12. The VirusTotal result of the URL mentions Prolific Puma.

SUBJECT	SUBJECT-TYPE	INDICATOR	DETECTION	DESCRIPTION
108] [.]61[.]142[.]190	IP address	hxxp://108 [.]61[.]142[.]190/ FX300.rar	95 - Ransomware	Hosting URL for Play Ransomware binary
108 [.]61[.]142[.]190	IP address	hxxp://108 [.]61[.]142[.]190/ 1.dll.sa	79 -Disease Vector	Hosting URL for Coroxy backdoor
108 [.]61[.]142[.]190	IP address	hxxp://108 [.]61[.]142[.]190/ 64.zip	79 – Disease Vector	Hosting URL for NetScan
108 [.]61[.]142[.]190	IP address	hxxp://108 [.]61[.]142[.]190/ winrar-x64-611.exe	Untested	Hosting URL for WinRAR
108 [.]61[.]142[.]190	IP address	hxxp://108 [.]61[.]142[.]190/ PsExec.exe	Untested	Hosting URL for PsExec

108 [.]61[.]142[.]190	IP address	hxxp://108 [.]61[.]142[.]190/ host1.sa	78 - Malware Accomplice	Hosting URL for Coroxy backdoor

Table 2. The different tools of Play ransomware resolve to several IP addresses.

SUBJECT	SUBJECT-TYPE	INDICATOR	INDICATOR-TYPE	REGISTRAR
108 [.]61[.]142[.]190	IP address	ztqs[.]info	Domain (RDGA)	Porkbun, LLC
108 [.]61[.]142[.]190	IP address	zfrb[.]info	Domain (RDGA)	Porkbun, LLC
108 [.]61[.]142[.]190	IP address	xzdw[.]info	Domain (RDGA)	Porkbun, LLC
108 [.]61[.]142[.]190	IP address	iing[.]info	Domain (RDGA)	Porkbun, LLC
108 [.]61[.]142[.]190	IP address	mcmb[.]info	Domain (RDGA)	NameCheap, Inc
108 [.]61[.]142[.]190	IP address	lcmr[.]info	Domain (RDGA)	NameCheap, Inc
108 [.]61[.]142[.]190	IP address	thfq[.]info	Domain (RDGA)	NameCheap, Inc
108 [.]61[.]142[.]190	IP address	hibh[.]info	Domain (RDGA)	NameCheap, Inc

108 [.]61[.]142[.]190	IP address	iwqe[.]info	Domain (RDGA)	NameCheap, Inc
108 [.]61[.]142[.]190	IP address	ukwc[.]info	Domain (RDGA)	NameCheap, Inc
108 [.]61[.]142[.]190	IP address	apkh[.]info	Domain (RDGA)	NameCheap, Inc
108 [.]61[.]142[.]190	IP address	vqbl[.]info	Domain (RDGA)	NameSilo, LLC
108 [.]61[.]142[.]190	IP address	vgkb[.]info	Domain (RDGA)	NameSilo, LLC
108 [.]61[.]142[.]190	IP address	znuc[.]info	Domain (RDGA)	NameSilo, LLC

Table 3. The IP addresses hosting the Play ransomware resolves to different domains.

TLD	us	link	info	com	cc	me
Domains	vf8[.]us 2ug[.]us z3w[.]us yw9[.]us 8tm[.]us	cewm[.]link wrzt[.]link hhqm[.]link ezqz[.]link zyke[.]link	uelr[.]info ldka[.]info fbvn[.]info baew[.]info shpw[.]info	kfwpr[.]com trqrh[.]com nhcux[.]com khrig[.]com dvcgg[.]com	jlza[.]cc hpko[.]cc ddkn[.]cc mpsi[.]cc wkby[.]cc	scob[.]me xnxk[.]me zoru[.]me mjzo[.]me ouzp[.]me

Figure 13. Prolific Puma uses numerous registered domains.

Figure 14. A shortened link created by Prolific Puma correlates with the observed IP address associated with Play ransomware

Tables 2 and 3 display the domains, particularly DGAs, that resolve to the IP address alongside the Play ransomware toolkit. These domains are registered under different registrar names. Our research indicates that Prolific Puma typically uses three to four random characters on their registered domain. The sample registered domains by Prolific Puma in the tables match the domains that resolve to the IP address associated with Play ransomware.

Additionally, the message showed when accessing one of the domains matches the one mentioned by other [security researchersopen on a new tab](#).

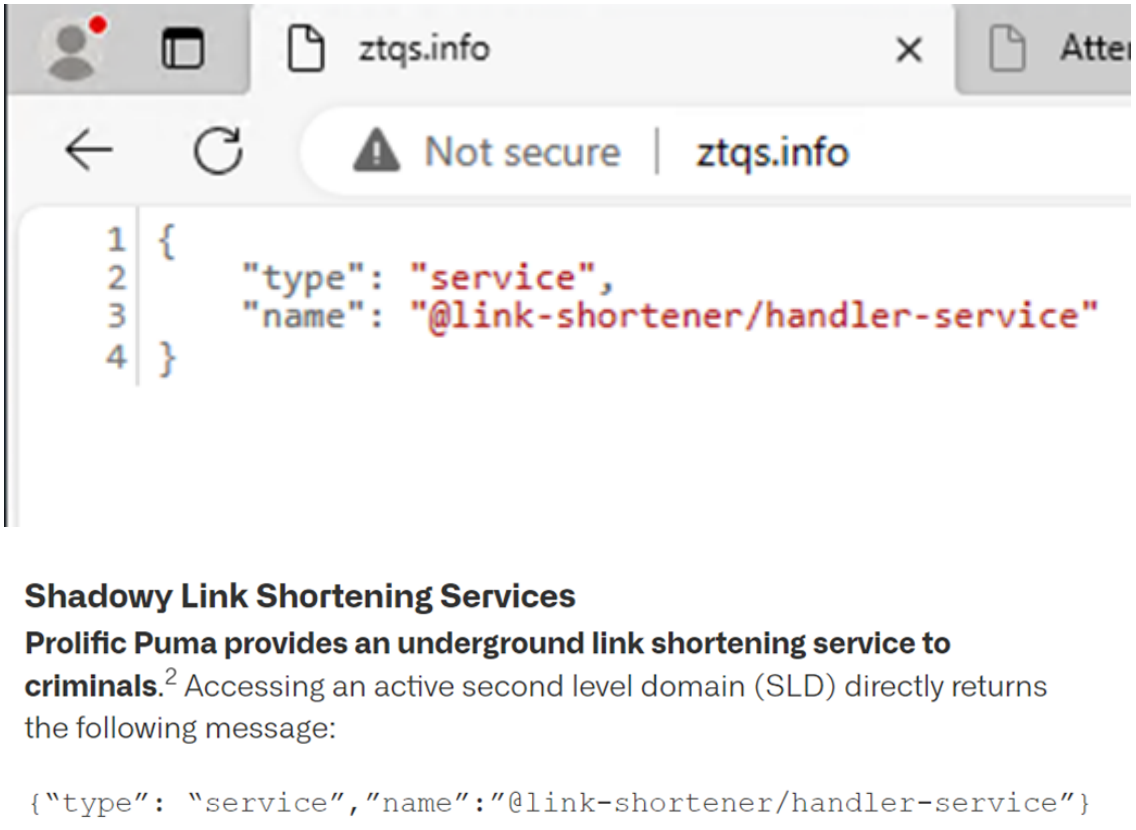

Figure 15. Accessing different domains shows the same message about link-shortening services.

To further verify the connection between the two groups, the team also tested the Coroxy backdoor hosted in the same IP address. Black-box analysis shows that the Coroxy backdoor was observed connecting to 45[.]76[.]165[.]129. This IP address also resolves to various domains associated with Prolific Puma.

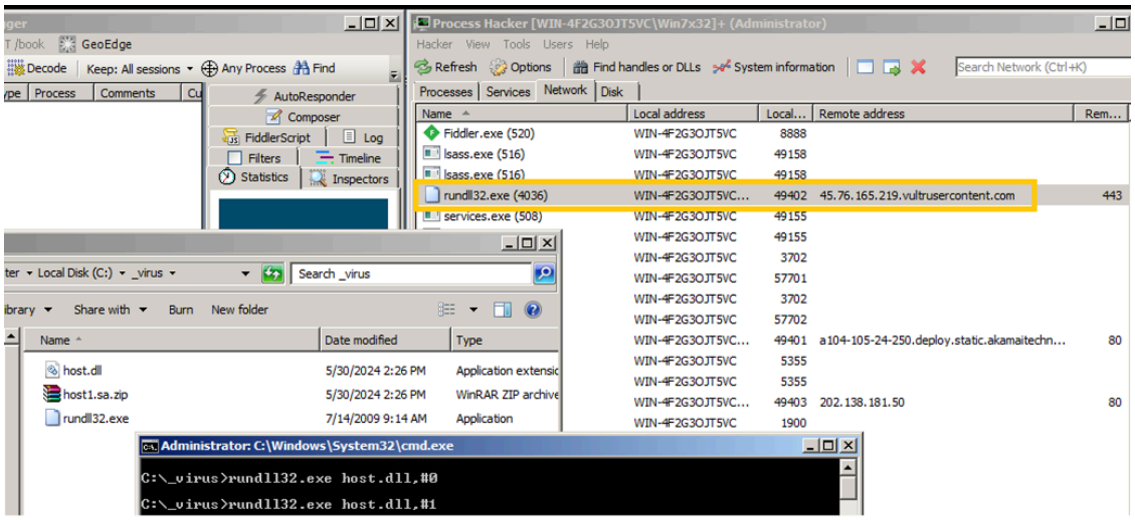

Figure 16. The Coroxy backdoor used by Play ransomware has been detected establishing a connection to the specified IP address.

SUBJECT	SUBJECT-TYPE	INDICATOR	INDICATOR-TYPE	REGISTRAR
45[.]76[.]165[.]129	IP address	jhrd[.]me	Domain (RDGA)	NameSilo, LLC
45 [.]76[.]165[.] 129	IP address	pkil[.]me	Domain (RDGA)	NameSilo, LLC
45 [.]76[.]165[.] 129	IP address	kwfw[.]me	Domain (RDGA)	NameSilo, LLC
45 [.]76[.]165[.] 129	IP address	whry[.]me	Domain (RDGA)	NameSilo, LLC
45 [.]76[.]165[.] 129	IP address	pxkt[.]me	Domain (RDGA)	NameSilo, LLC
45 [.]76[.]165[.] 129	IP address	ylvq[.]me	Domain (RDGA)	NameSilo, LLC
45 [.]76[.]165[.]129	IP address	flbe[.]link	Domain (RDGA)	NameSilo, LLC

45 [.]76[.]165[.]129	IP address	mmhp[.]link	Domain (RDGA)	NameSilo, LLC
45 [.]76[.]165[.] 129	IP address	gunq[.]link	Domain (RDGA)	NameSilo, LLC
45 [.]76[.]165[.] 129	IP address	ojry[.]link	Domain (RDGA)	NameSilo, LLC
45 [.]76[.]165[.] 129	IP address	bltr[.]me	Domain (RDGA)	NameSilo, LLC

Table 4. Different domains resolve to the IP address of the Coroxy backdoor connection.

The IP address that the Coroxy backdoor connects to also resolves to different domains that matches the registered domains of Prolific Puma. By further examining the IP address, “vultrusercontent.com” is appended and matches the original IP, as shown in Figure 17.

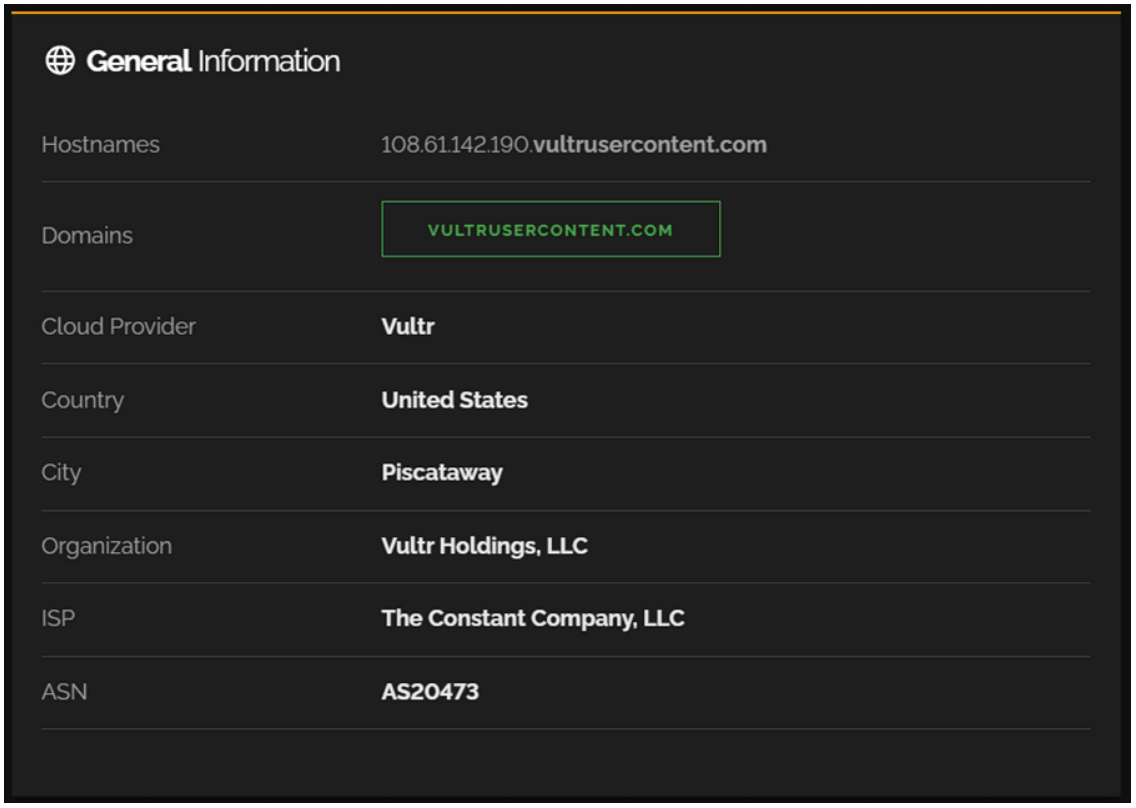

Figure 17. A Shodan query of the IP address hosting Play ransomware reveals some details on its associated infrastructure.

Comparison of the IP address that hosted Play ransomware and its tools with another IP address related to Prolific Puma shows that both IP addresses have the same autonomous system number (ASN). This means that they belong in the same network and are being managed by the same network provider.

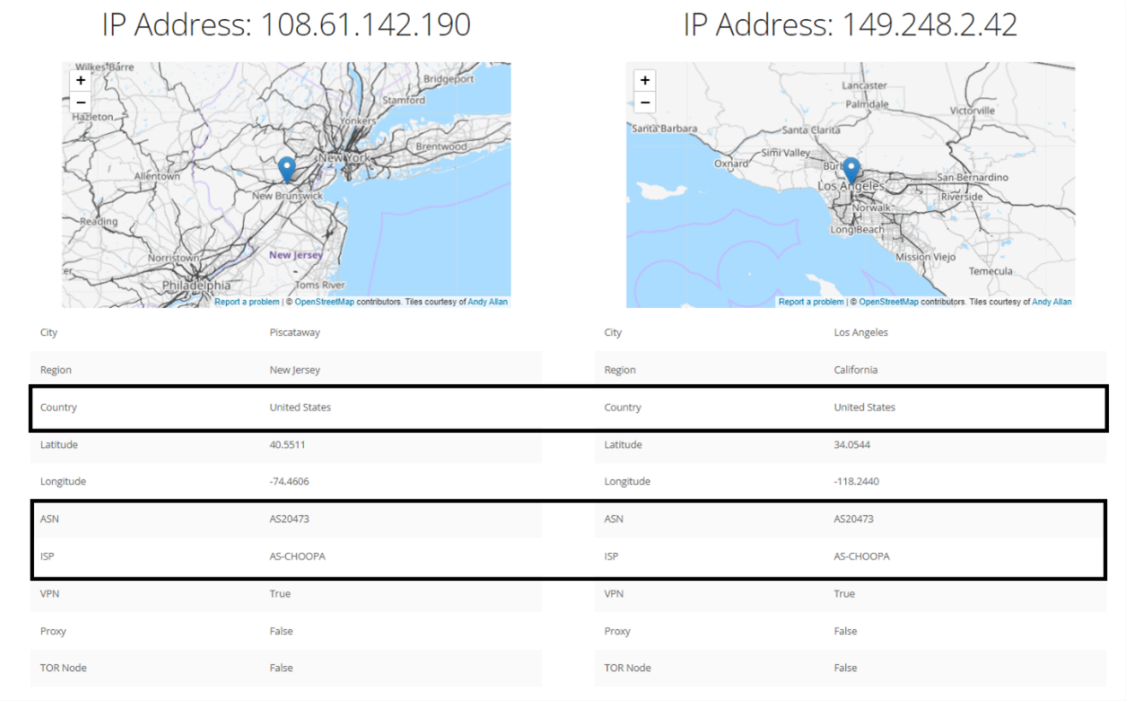

Figure 18. The IP address hosting the ransomware (left) and the IP address related to Prolific Puma from (right) have similarities.

Prolific Puma is discerning in its client selection process, preferring to engage with individuals or groups deemed deserving of its services. Given the established reputation of the threat actors behind Play ransomware, they might be considered a suitable candidate to access Prolific Puma's offerings. These findings suggest a potential collaboration between these cybercriminal entities. The Play ransomware group, too, might be seeking to enhance its capabilities in circumventing defensive security protocols through Prolific Puma's services.

Mitigating ransomware attacks on ESXi environments

ESXi environments are high-value targets for ransomware attacks due to their critical role in business operations. The efficiency of encrypting numerous VMs simultaneously and the valuable data they hold further elevate their lucrativeness for cybercriminals. To mitigate risks and exposure to these attacks, organizations should implement several best practices:

- Regular patching and updates: Keep the ESXi environment and associated management software up to date to protect against known vulnerabilities.
- Virtual patching: Many organizations may not patch or update their ESXi environments as frequently as they should due to complexity, downtime concerns, resource constraints, operational priorities, or compatibility issues. Virtual patching helps by applying security measures at the network level to protect vulnerable systems, mitigating risks without needing to alter the underlying software immediately.
- Addressing inherent misconfigurations: Regularly audit and correct misconfigurations within ESXi environments, as these can create vulnerabilities that ransomware can exploit. Implementing strong configuration management practices can help ensure that settings adhere to security best practices and reduce the risk of exploitation.

- Strong access controls: Implement robust authentication and authorization mechanisms, such as multifactor authentication (MFA), and restrict administrative access.
- Network segmentation: Segregate critical systems and networks to limit the spread of ransomware.
- Minimized attack surface: Disable unnecessary and unused services and protocols, restrict access to critical management interfaces, and implement strict firewall rules to limit network exposure. VMWare provides various guidelines and best practicesopen on a new tab on how to secure ESXi environments.
- Regular offline backups: Maintain frequent and secure backups of all critical data. Ensure that backups are stored offline and tested regularly to verify their integrity.
- Security monitoring and incident response: Deploy solutions and develop an incident response plan to promptly and proactively address suspicious activities.

Trend Micro Vision One Hunting Query

The following text lists potentially useful queries for threat hunting within Vision One:

- malName:*Linux.PLAYDE* AND eventName:MALWARE_DETECTION

Indicators of Compromise (IoC)

IOC	Detection	Description
2a5e003764180eb3531443946d2f3c80ffcb2c30	Ransom.Linux.PLAYDE.YXEE3T	ELF Binary
hxxp://108.61.142[.]190/FX300.rar	95 - Ransomware	Hosting URL for Play Ransomware Binary
108.61.142[.]190	Untested	Observed IP address
hxxp://108.61.142[.]190/1.dll.sa	79 - Disease Vector	Hosting URL for Coroxy Backdoor
hxxp://108.61.142[.]190/64.zip	79 - Disease Vector	Hosting URL for NetScan

hxxp://108.61.142[.]190/winrar-x64-611.exe	Untested	Hosting URL for WinRAR
hxxp://108.61.142[.]190/PsExec.exe	Untested	Hosting URL for PsExec
hxxp://108.61.142[.]190/host1.sa	78 - Malware Accomplice	Hosting URL for Coroxy Backdoor

MITRE ATT&CK Tactics and Techniques:

Tactic	Tactic	ID
Defense Evasion	File Deletion	T1070.004
Discovery	Network Service Discovery	T1046
	File and Directory Discovery	T1083
Execution	Command and Scripting Interpreter: Unix Shell	T1059.004
Lateral Movement	Lateral Tool Transfer	T1570
Command and Control	Dynamic Resolution: Domain Generation Algorithms	T1568.002
	Ingress Tool Transfer	T1105
Exfiltration	Exfiltration over C&C Channel	T1041
Impact	Data Encrypted for Impact	T1486

	Defacement: Internal Defacement	T1491.001
	Service Stop	T1489

Tags
