SORINTSEC

THREAT HUNTING

LAB

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

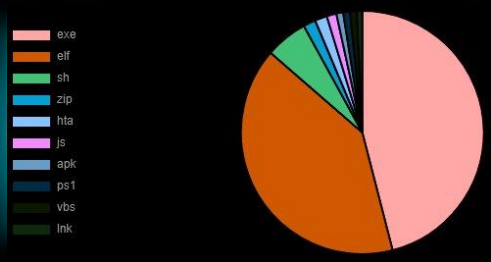
PUBLIC

Index

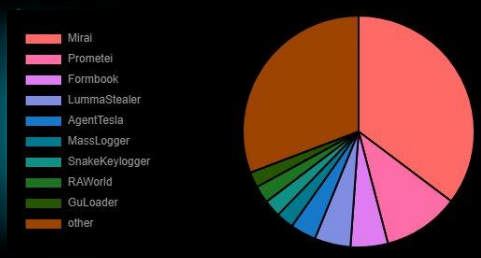
Global Weekly Threat Overview

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 inmemory 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

SORINTSEC

TACTIC

Defense Evasion

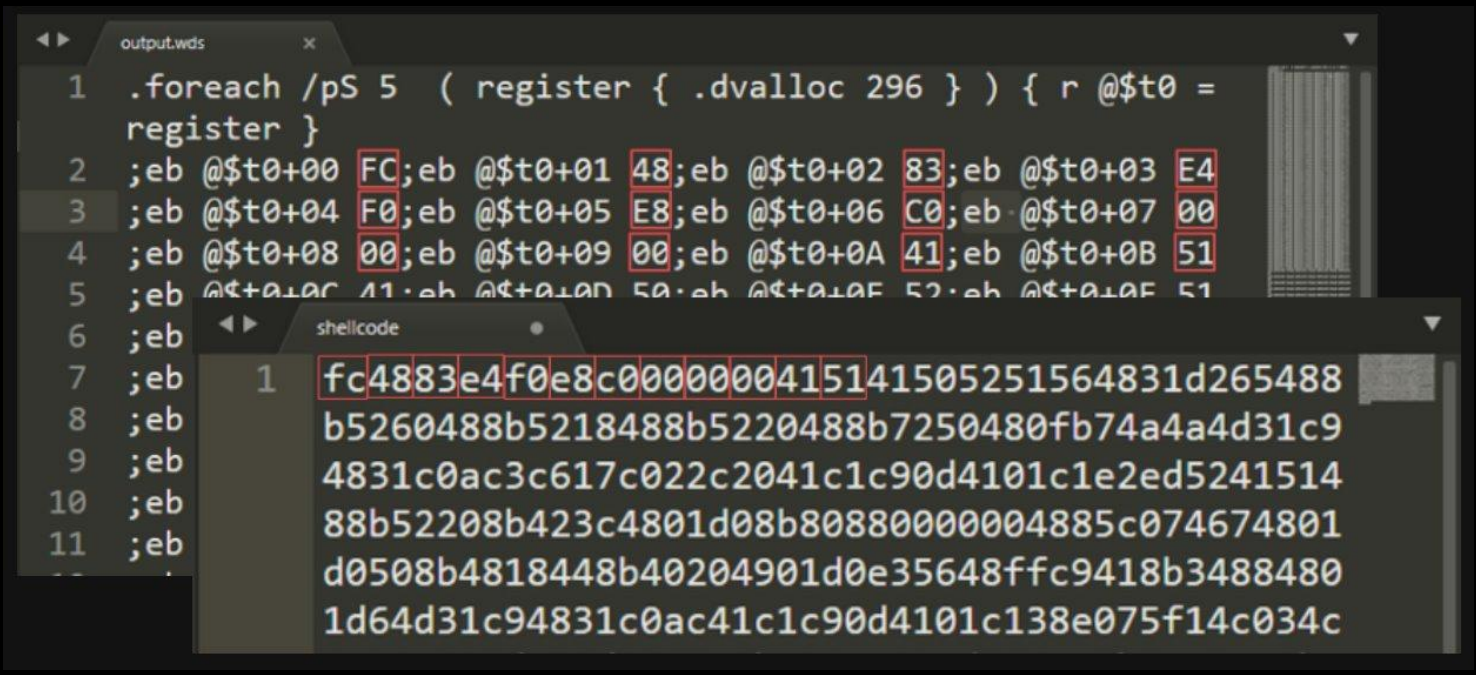
TECHNIQUES

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

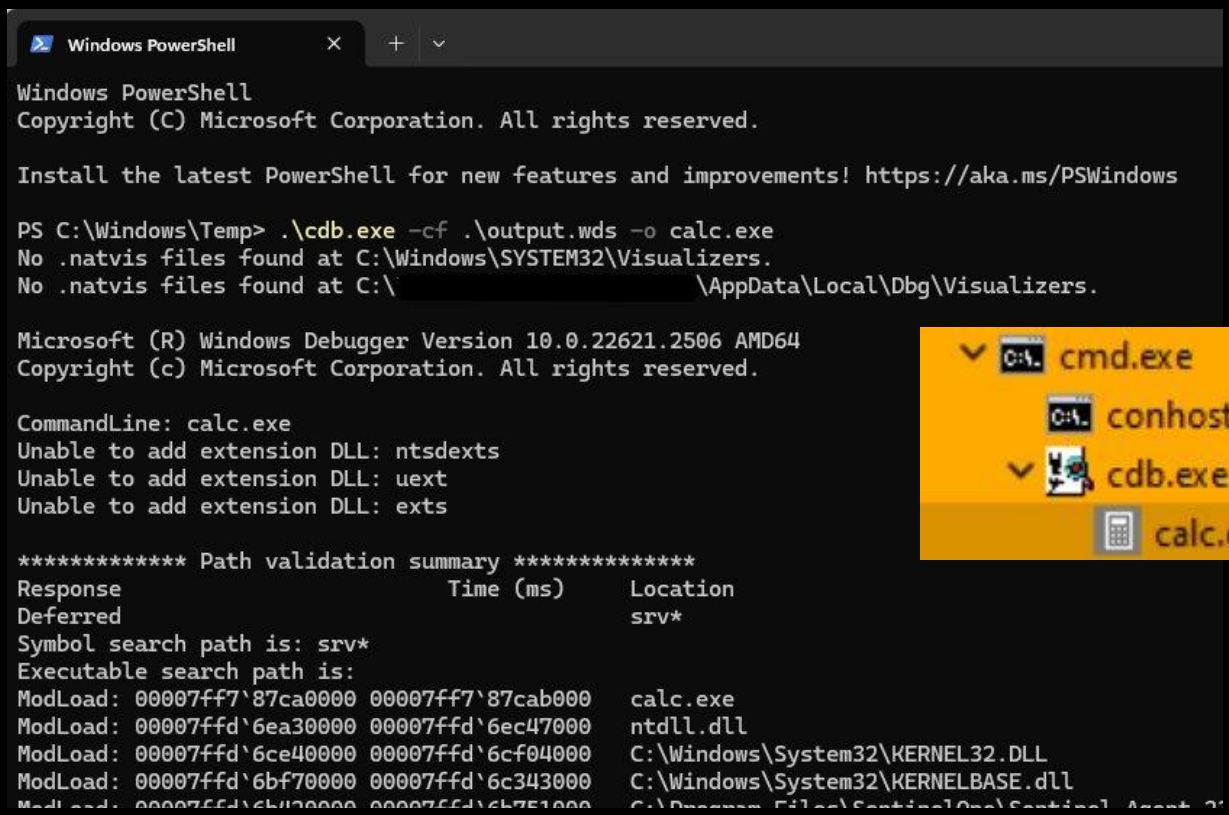
The team performed tests replicating the technique by saving the shellcode in a .wds file , as can be seen from the following image it is necessary to maintain the correct syntax in order to be processed correctly by the debugger.



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.



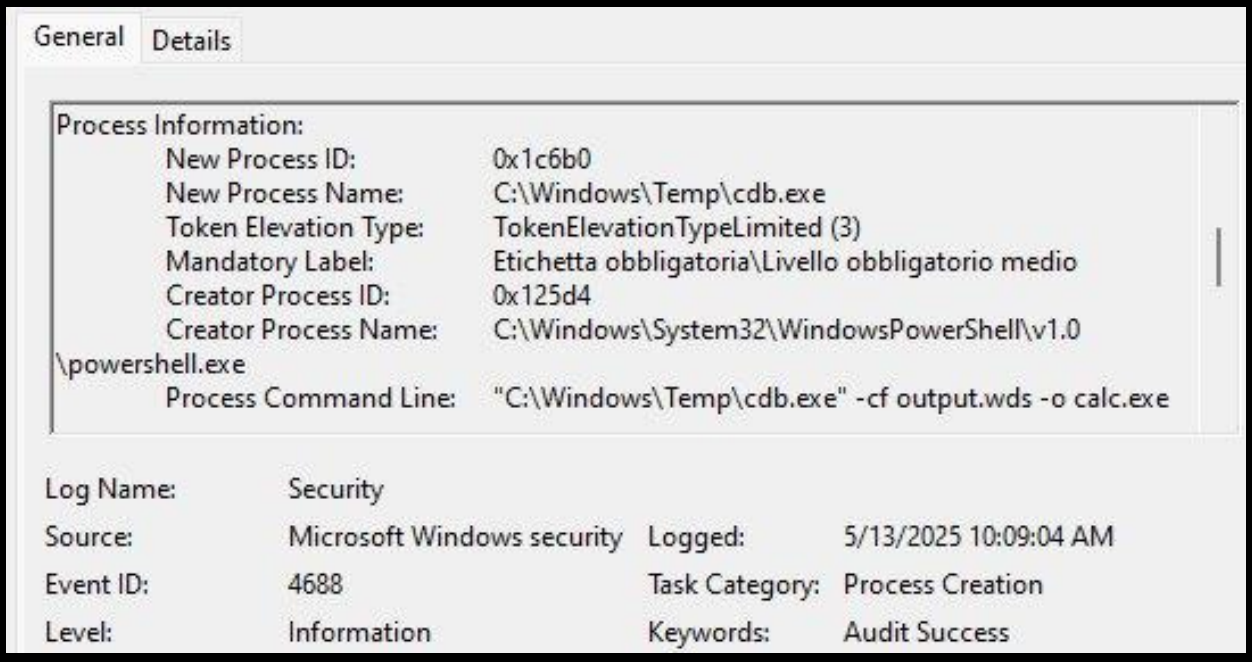
Cdb.exe execution

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

Shellcode executed and callback received

Threat Hunting Activity

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



EID 4688

THREAT HUNTING

SORINT.SEC

PUBLIC