THREAT HUNTING

LAB

WEEK 08/09/2025 - 12/09/2025

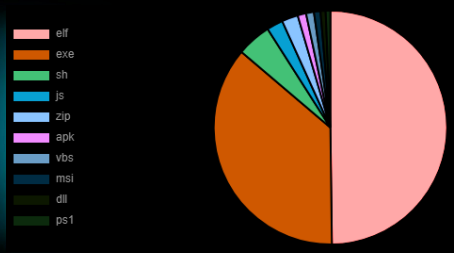
PUBLIC

Index

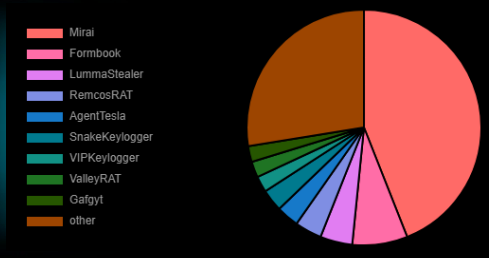
Global Weekly Threat Overview

Security researchers have identified at least 187 npm packages compromised in an ongoing supply chain attack, with a malicious self-propagating payload to infect other packages. The coordinated worm-style campaign dubbed 'Shai-Hulud' started with the compromise of the @ctrl/tinycolor npm package, which receives over 2 million weekly downloads. Since then, the campaign has expanded significantly and now includes packages published under CrowdStrike's npm namespace. These ongoing attacks demonstrate the fragility of the modern software supply chain, where a single malicious pull request or compromised maintainer account can ripple out to hundreds of projects.

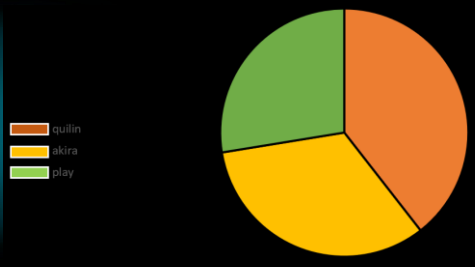
Top 10 file types



Top 10 malware family

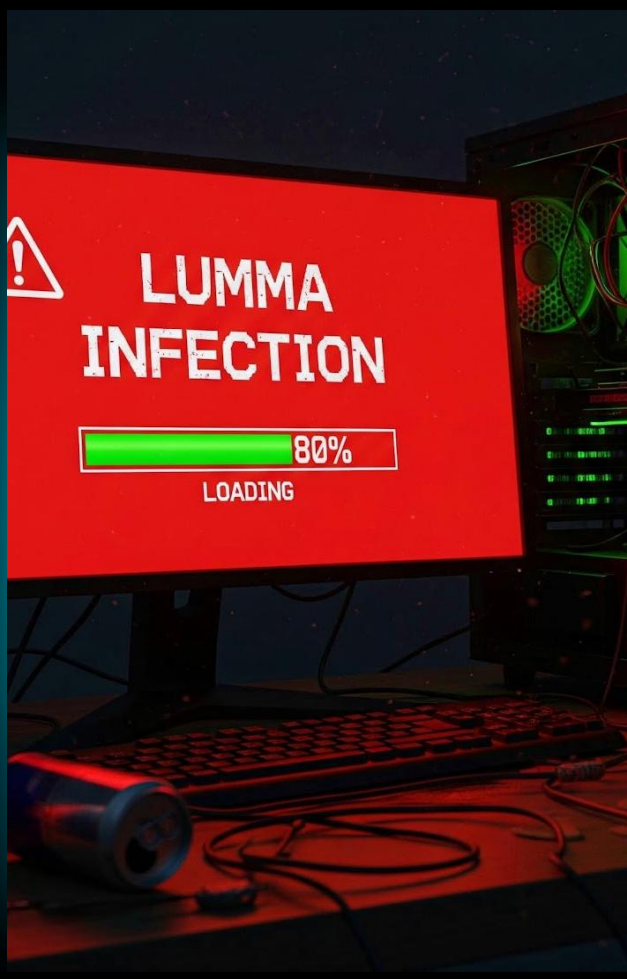


Top 3 Ransomware Group



Enterprise search and security company Elastic is rejecting reports of a zero-day vulnerability impacting its Defend endpoint detection and response (EDR) product. The company's statement follows a blog post from a company called AshES Cybersecurity claiming to have discovered a remote code execution (RCE) flaw in Elastic Defend that would allow an attacker to bypass EDR protections. According to AshES Cybersecurity's write-up, ‘elastic-endpoint-driver.sys’ could be weaponized to bypass EDR monitoring, enable remote code execution with reduced visibility, and establish persistence on the system.

Global Weekly Notable One



System Binary Proxy Execution: Defense Evasion

Lumma Stealer, a rapidly spreading infostealer malware marketed as Malware-as-a-Service (MaaS), experienced a massive surge in infections throughout 2024, fueled by its ease of use and sophisticated delivery methods. In May 2025, a coordinated global law enforcement takedown seized over 2,300 domains linked to Lumma, temporarily disrupting its infrastructure and hindering its operations. However, the malware swiftly rebounded through a stealthier resurgence, with its operators rebuilding infrastructure using less conspicuous, covert channels.

This new phase introduced advanced infection techniques, including more discreet delivery via phishing and exploitation of legitimate tools to evade detection. Despite the takedown efforts, Lumma Stealer's continued adaptability and innovative tactics have allowed it to maintain active campaigns, posing persistent risks to organizations worldwide, underscoring the critical need for proactive cybersecurity measures and continuous vigilance against evolving threats.

Threat Hunting Activity

SORINTSEC

TACTIC

Defense Evasion

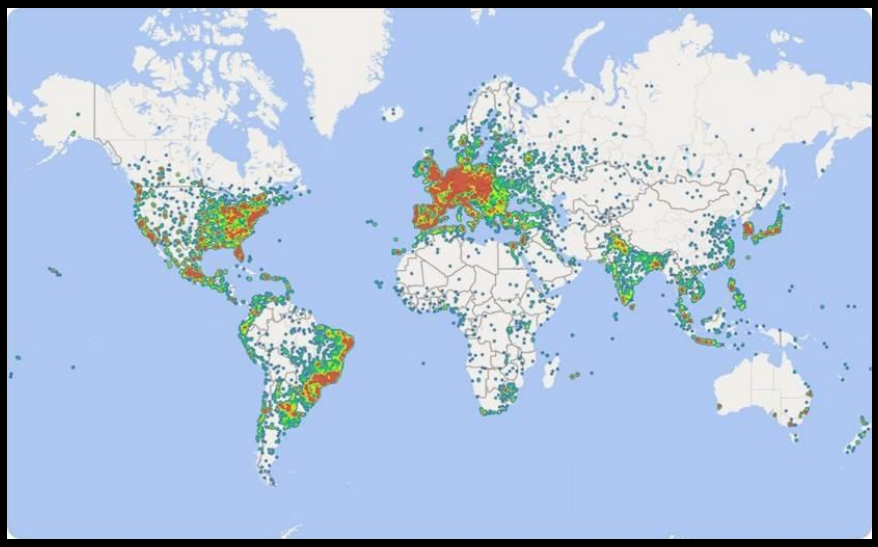
TECHNIQUES

T1218 – System Binary Proxy Execution

Adversaries leverage and abuse trusted processes to hide and masquerade their malware. Adversaries may bypass process and/or signature-based defenses by proxying execution of malicious content with signed, or otherwise trusted, binaries. Binaries used in this technique are often Microsoft-signed files, indicating that they have been either downloaded from Microsoft or are already native in the operating system.

Threat Hunting Activity

Lumma Stealer (LummaC2) is a rapidly expanding infostealer malware offered as Malware-as-a-Service (MaaS) on underground forums and Telegram, enabling even low-skilled actors to deploy it. Active since late 2022, it saw a 369% rise in detections between H1 and H2 2024. By mid-2025, infections exceeded 10 million, with Microsoft logging nearly 400,000 infections in three months, below a map detailing global spread of Lumma Stealer malware infections and encounters across Windows devices. It spreads through fake software cracks, malvertising, phishing, fake GitHub projects, and bogus CAPTCHA pages.

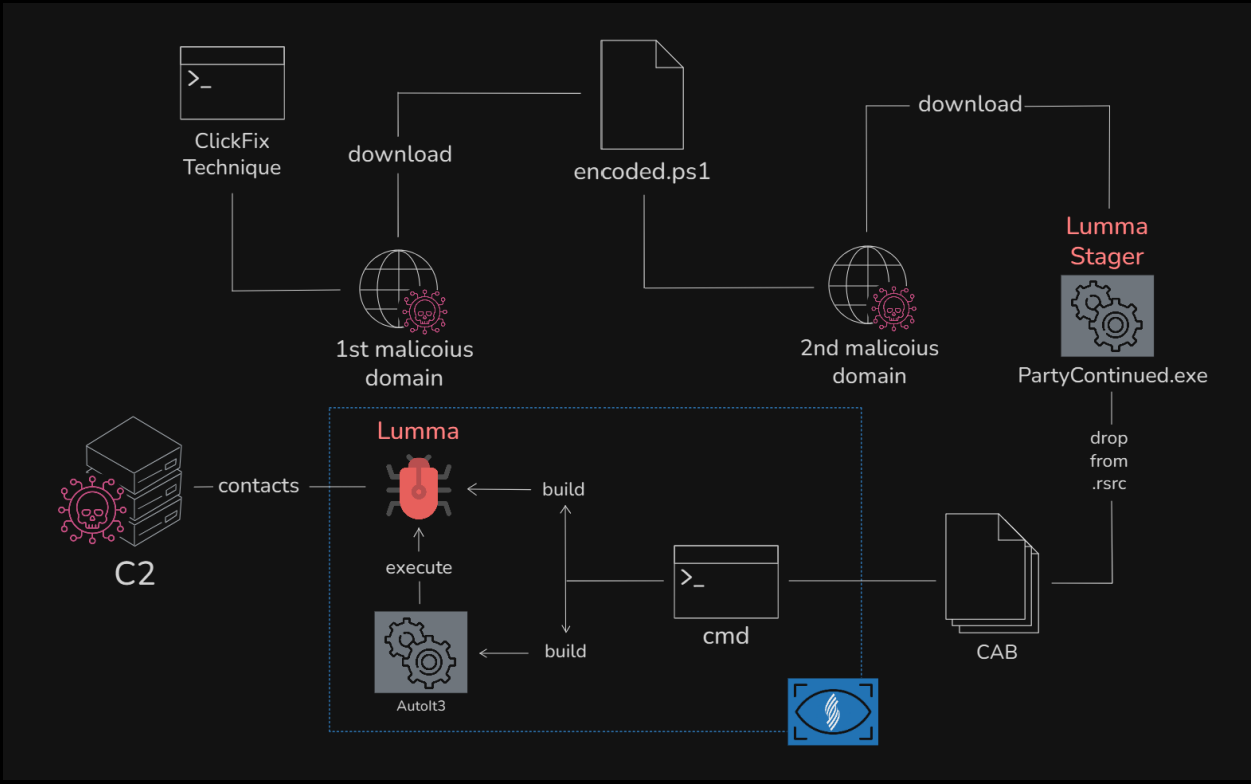


Lumma global spread

It uses advanced evasion, including process hollowing, PowerShell abuse, stolen certificates, and persistence mechanisms. A May 2025 law enforcement operation taking down 2,300 domains briefly disrupted operations, but operators quickly rebuilt infrastructure using stealthier channels.

Threat Hunting Activity

The team focuses on a loading technique that was observed as part of a new campaign employing advanced infection chains and evolved delivery tactics.

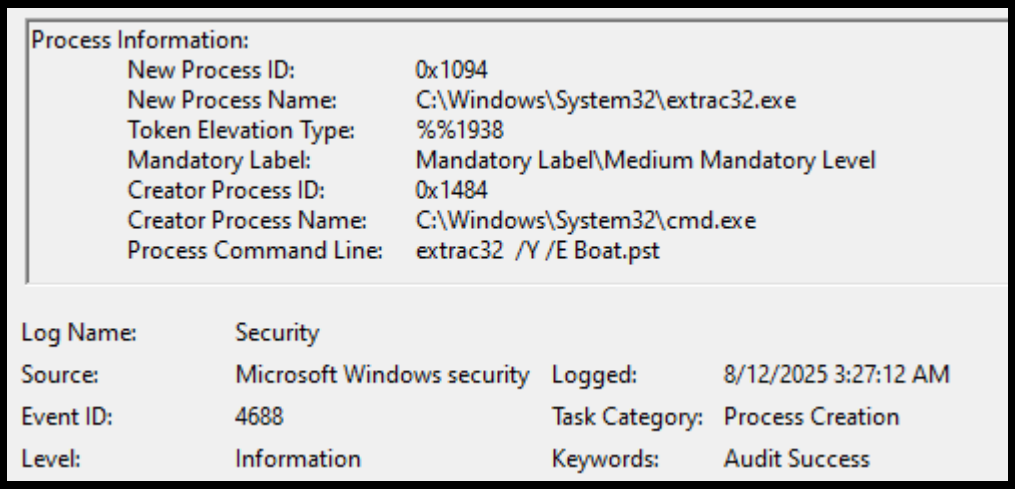


Observed Campaign Infection Chain

When the stager PartyContinued.exe runs, it initiates a new Lumma Stealer loading method that uses the scripting language Autolt. This version is similar to earlier variants but includes a Microsoft Cabinet (CAB) archive named Boat.pst, bundled inside PartyContinued.exe. The Boat.pst file is extracted with the legitimate Windows tool extrac32.exe to unpack components needed to create an Autolt3 script engine and execute an Autolt script for Lumma Stealer.

Threat Hunting Activity

Detection can be made on EID 4688 looking for uncommon extract32 parameters correlating with behavioral patterns linked to this campaign.



Process Information:

New Process ID:	0x1094
New Process Name:	C:\Windows\System32\extrac32.exe
Token Elevation Type:	%%1938
Mandatory Label:	Mandatory Label\Medium Mandatory Level
Creator Process ID:	0x1484
Creator Process Name:	C:\Windows\System32\cmd.exe
Process Command Line:	extrac32 /Y /E Boat.pst

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	8/12/2025 3:27:12 AM
Event ID:	4688	Task Category:	Process Creation
Level:	Information	Keywords:	Audit Success

EID 4688

THREAT HUNTING

SORINT SEC

PUBLIC