SORINT SEC

# THREAT HUNTING

## LAB

WEEK 10/03/2025 - 14/03/2025

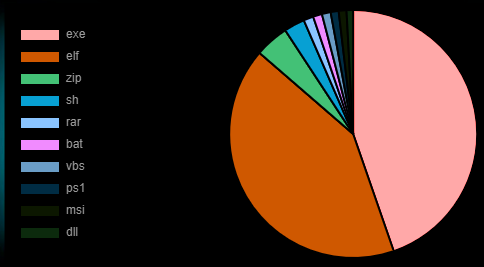
PUBLIC

# Index

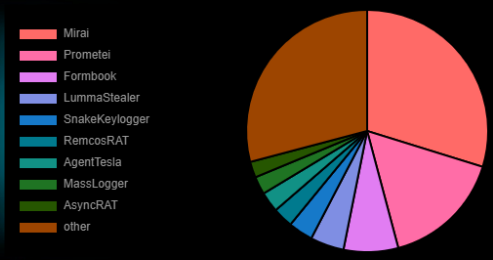
# Global Weekly Threat Overview

A widespread phishing campaign has targeted nearly 12,000 GitHub repositories with fake "Security Alert" issues, tricking developers into authorizing a malicious OAuth app that grants attackers full control over their accounts and code. "Security Alert: Unusual Access Attempt We have detected a login attempt on your GitHub account that appears to be from a new location or device," reads the GitHub phishing issue. All of the GitHub phishing issues contain the same text, warning users that their was unusual activity on their account from Reykjavik, Iceland, and the same IP address.

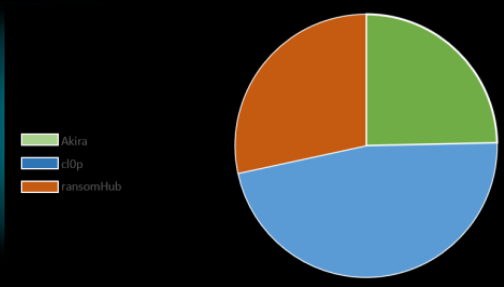
Top 10 file types




Top 10 malware family




Top 3 Ransomware Group




Six malicious packages have been identified on npm (Node package manager) linked to the notorious North Korean hacking group Lazarus. The packages, which have been downloaded 330 times, are designed to steal account credentials, deploy backdoors on compromised systems, and extract sensitive cryptocurrency information. The Socket Research Team discovered the campaign, which linked it to previously known Lazarus supply chain operations. The threat group is known for pushing malicious packages into software registries like npm, which is used by millions of JavaScript developers, and compromising systems passively.

# Global Weekly Notable One

## Trusted Developer Utilities Proxy Execution: Defense Evasion

Threat actors increasingly abuse legitimate software to bypass traditional security measures. Dark Pink group, a collective we have written about before, testing and verifying some of the techniques implemented by the group during their compromises, has been observed to exploit techniques that have been refined over time, correcting and hiding details that we need to verify and keep track of.

Dark Pink, also known as the Saaiwc Group and UNC3922, is an emerging Advanced Persistent Threat (APT) actor that has been active since mid-2021, with notable operations in the Asia-Pacific (APAC) region. The group is known for its sophisticated cyber espionage campaigns, targeting strategic organizations such as government agencies, military entities, and religious institutions across multiple countries. Dark Pink continues to update its toolset to evade detection, employing improved obfuscation routines and leveraging new platforms for persistence. The group's sophistication and stealth suggest a well-funded and organized entity.

# Global Weekly Notable One

The technique adopted involves using the MSBuild trusted developer utility to build and run a file named “darkmoon.xml” masquerading as a png file. 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.

In addition, the peculiarity of MSBuild makes sure that once the indicated solution is built, it is also executed. The MITRE ATT&CK framework provides few procedure examples to this known technique, making it noteworthy to identify them in actual in-the-wild use cases.
The rapid TTP evolution underscores a cyclical "cat and mouse" dynamic, where defenders must adopt proactive, intelligence-driven strategies to mitigate risks from increasingly agile adversaries.

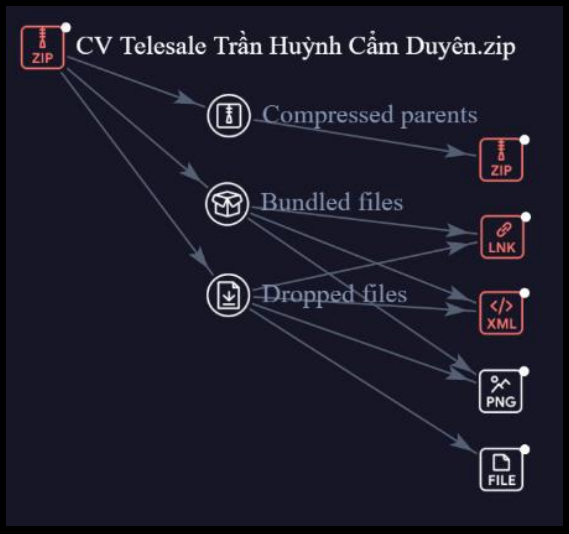
# Threat Hunting Activity

| | |
|---|---|
| **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.

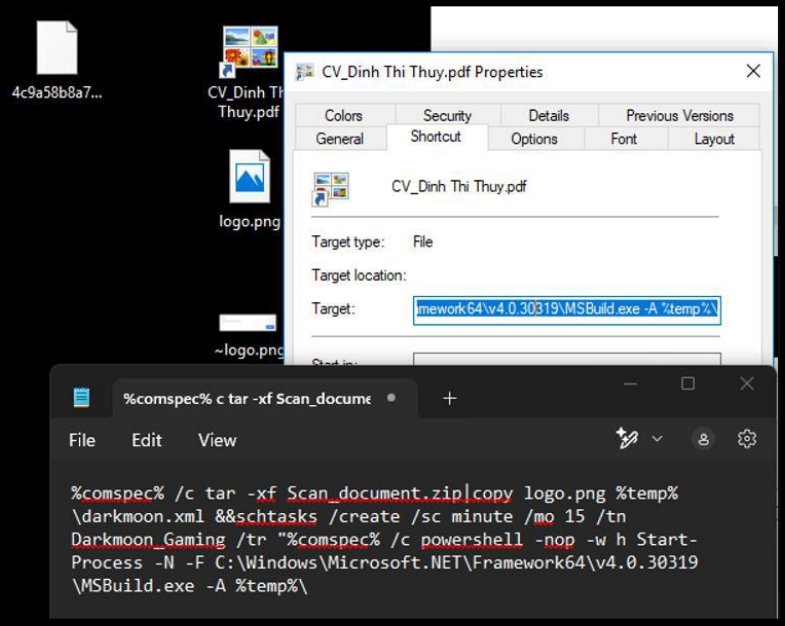
# Threat Hunting Activity

Shown next, the contents of the archive used to initiate the infection chain.
The file that looks like a .pdf actually, being a .lnk, executes a command to add persistence and proceed in executing the malicious .xml file masquerading as a .png file, using the trusted MSBuild utility.




File tree

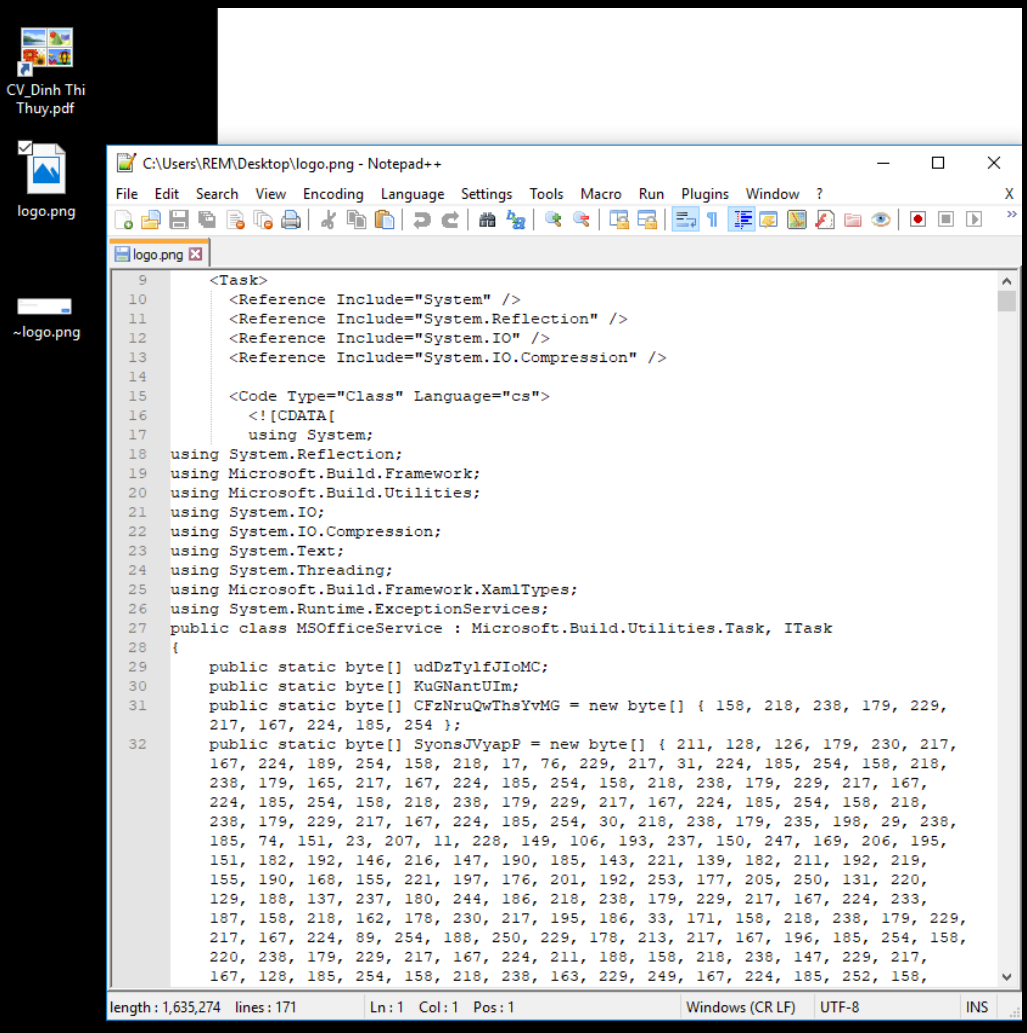
The malicious file is initially copied to a local folder , the command of build and execution is then scheduled every 15 minutes, increasing the impact by enabling adversaries to maintain long-term access, evade detection, and automate harmful activities.




.lnk content

# Threat Hunting Activity

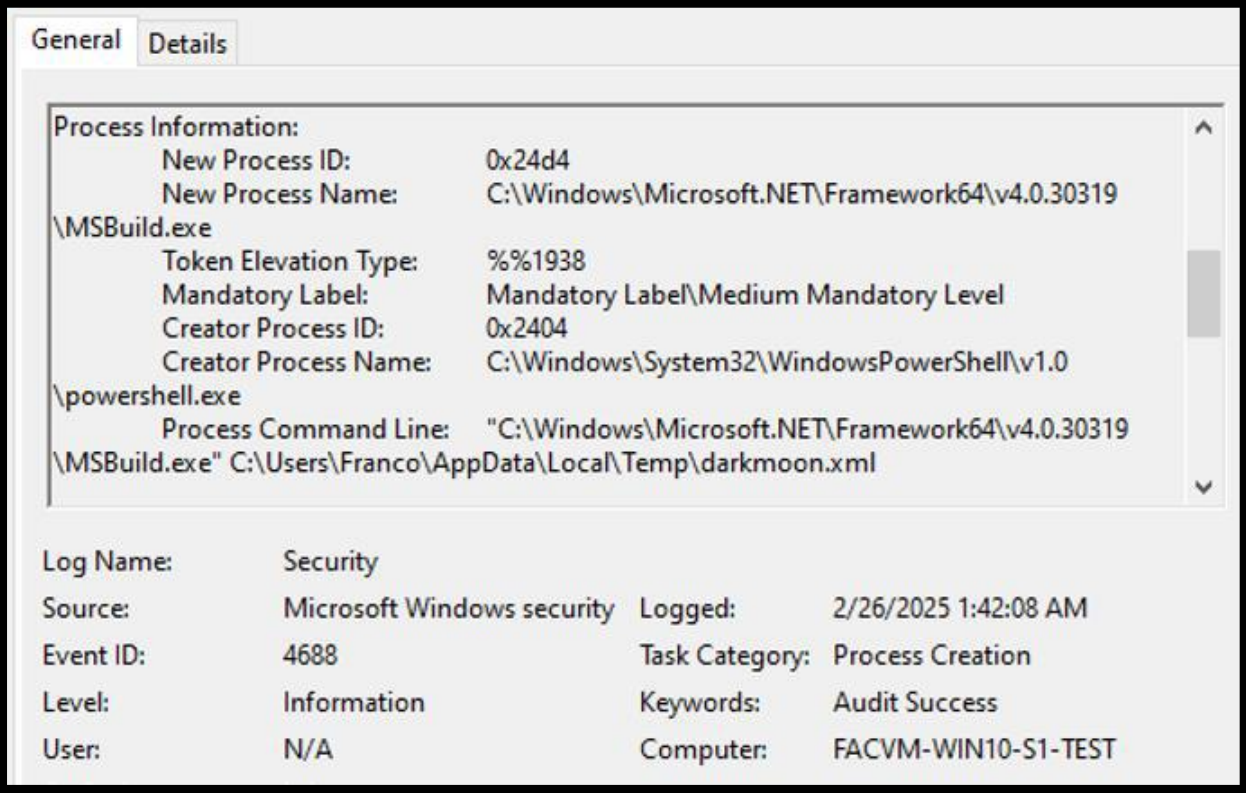
The darkmoon.xml file encapsulates malicious C# code. The malware, dubbed KamiKakaBot, will proceed in executing a stealer and opening a communication to C2 via telegram.
Our team is tracking the evolution of the techniques and malwares used by the group, observing an increase in obfuscation and encoding techniques of KamiKakaBot aimed at slowing down analysts' efforts to understand the group's capabilities and intent.




Malicious C# darkmoon.xml

# Threat Hunting Activity

EID 4688 detect this behavior intercepting .xml file loaded via MSBuild utility, help to correlating the activity with the evidences found.




EID 4688


PUBLIC