SORINT SEC

THREAT HUNTING

LAB

WEEK 02/06/2025 - 06/06/2025

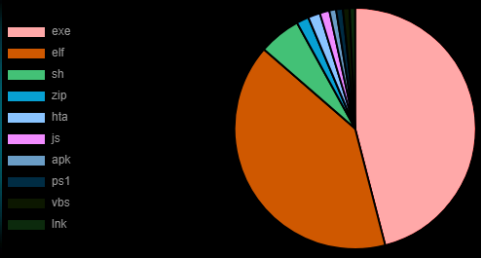
PUBLIC

Index

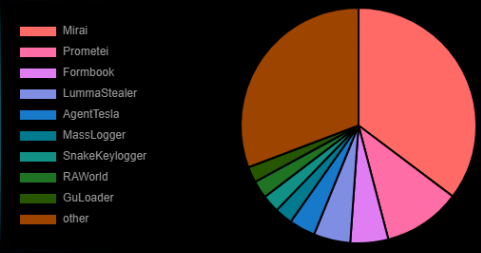
Global Weekly Threat Overview

A vulnerability in the DanaBot malware operation introduced in June 2022 update led to the identification, indictment, and dismantling of their operations in a recent law enforcement action. Zscaler's ThreatLabz researchers who discovered the vulnerability, dubbed 'DanaBleed,' explain that a memory leak allowed them to gain a deep peak into the malware's internal operations and the people behind it. Leveraging the flaw to collect valuable intelligence on the cybercriminals enabled an international law enforcement action named 'Operation Endgame' to take DanaBot infrastructure offline and indict 16 members of the threat group.

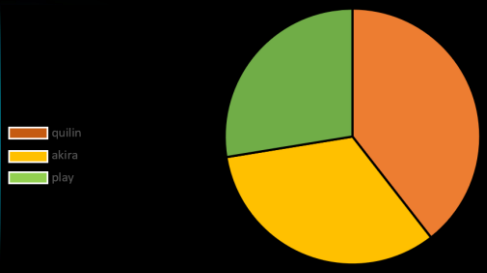
Top 10 file types



Top 10 malware family



Top 3 Ransomware Group



In a twist on typical hiring-related social engineering attacks, the FIN6 hacking group impersonates job seekers to target recruiters, using convincing resumes and phishing sites to deliver malware. FIN6 (aka "Skeleton Spider") is a hacking group that was initially known for conducting financial fraud, including compromising point-of-sale (PoS) systems to steal credit cards. However, in 2019, the threat actors expanded into ransomware attacks, joining existing operations like Ryuk and Lockergoga. The group has recently used social engineering campaigns to deliver 'More Eggs,' a JavaScript backdoor used for credential theft, system access, and ransomware deployment.

Global Weekly Notable One

Masquerading: Defense evasion

In recent weeks, our SOC shared a report on a malware campaign targeting the Italian territory. What makes this email campaign particularly sophisticated is its combination of multiple tactics designed to evade detection and exploit trusted platforms. Its multi-layered strategy ends with what we are focusing on: the chain ends with java executing a jar file disguised as a png file.

The team focused on that crucial point with which the attacker, in order to evade defenses, performs the final stage to infect the victim's host via java by providing a png file as an input file. This technique helps attackers evade detection because many antivirus solutions, email gateways, and endpoint protections perform quick checks based on file extensions or simple header analysis.

Threat Hunting Activity

TACTIC

Defense Evasion

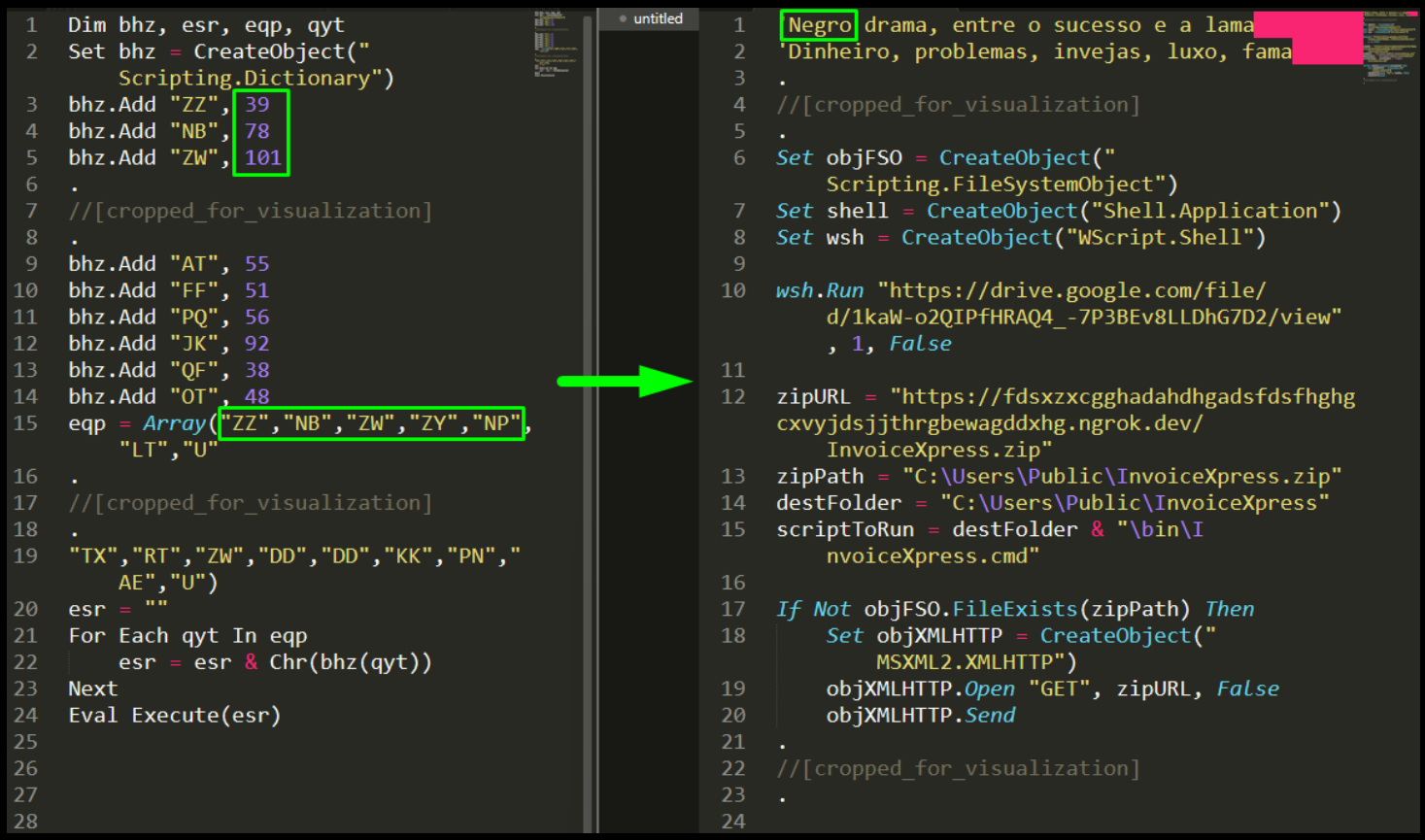
TECHNIQUES

T1036 – Masquerading

Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. Masquerading occurs when the name or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names.

Threat Hunting Activity

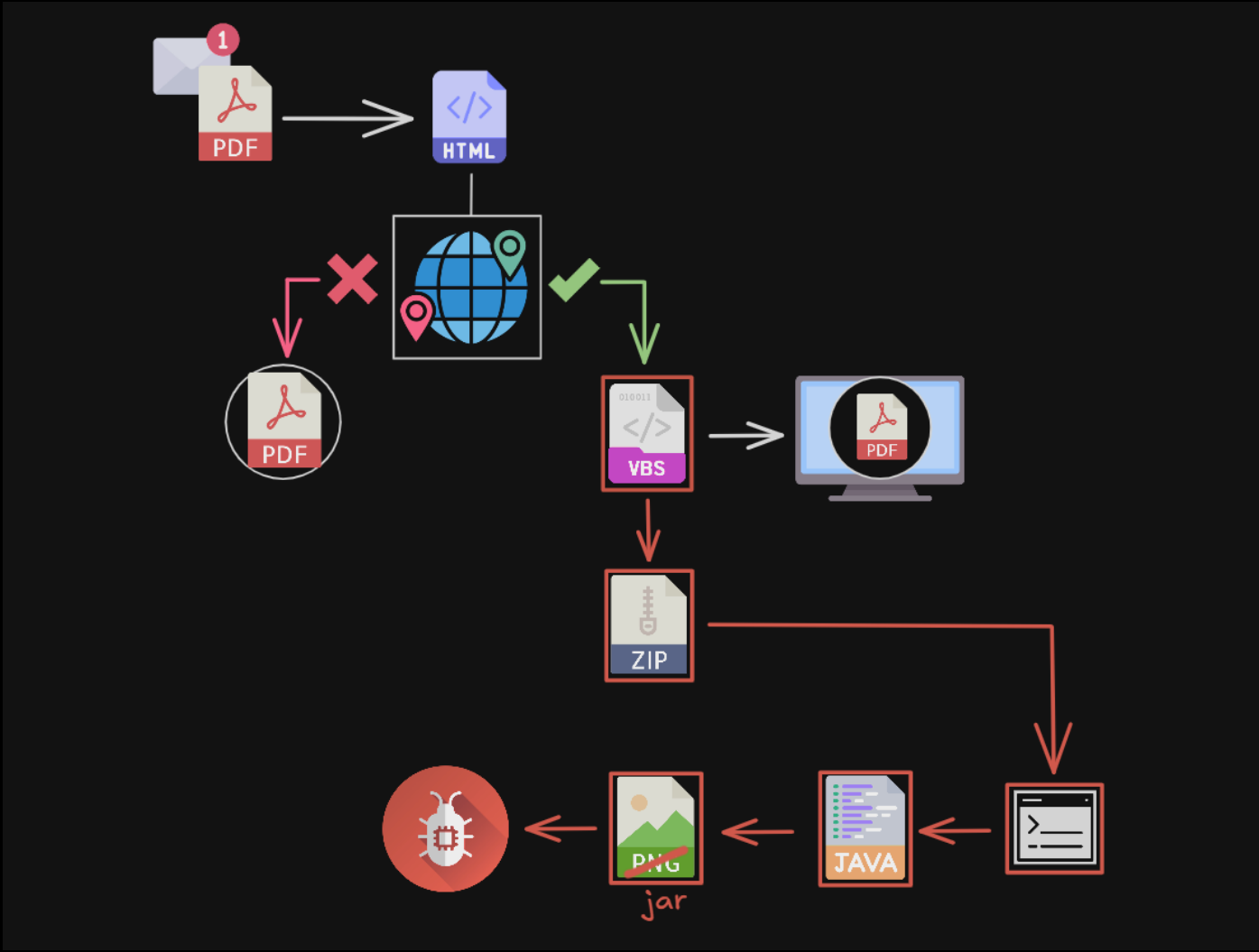
The first file of the chain is an obfuscated VBS with a custom dictionary that is recompiled during runtime. Part of the deobfuscated code is a song lyric, we assume it is used as padding, and/or to evade not-so-skilled analysts who at the evidence of something not initially malicious do not investigate further. At the end of the translated array we have the script with which it does the pdf and zipped archive retrieve, the next stager.



Deobfuscation of the second stager

Threat Hunting Activity

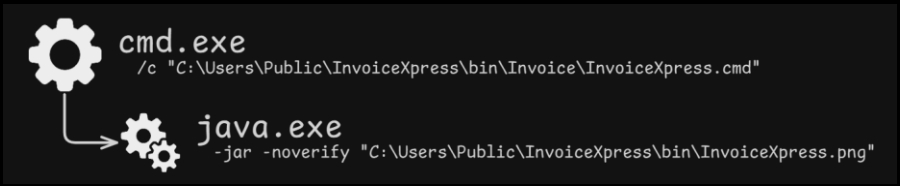
This sophisticated campaign uses social engineering, legitimate-looking senders, domain research, file-sharing platforms, geolocation, and Ngrok tunnels to evade detection and deliver malware effectively. Focusing on the last steps, by crafting a file that have a valid PNG extension but contains a ZIP/JAR archive embedded inside, attackers masquerade malware initializer file. Most security tools and filters often rely on file extensions or the first few bytes of a file to determine its type, so they might classify it as a safe image and allow it through without further inspection.



Infection Chain

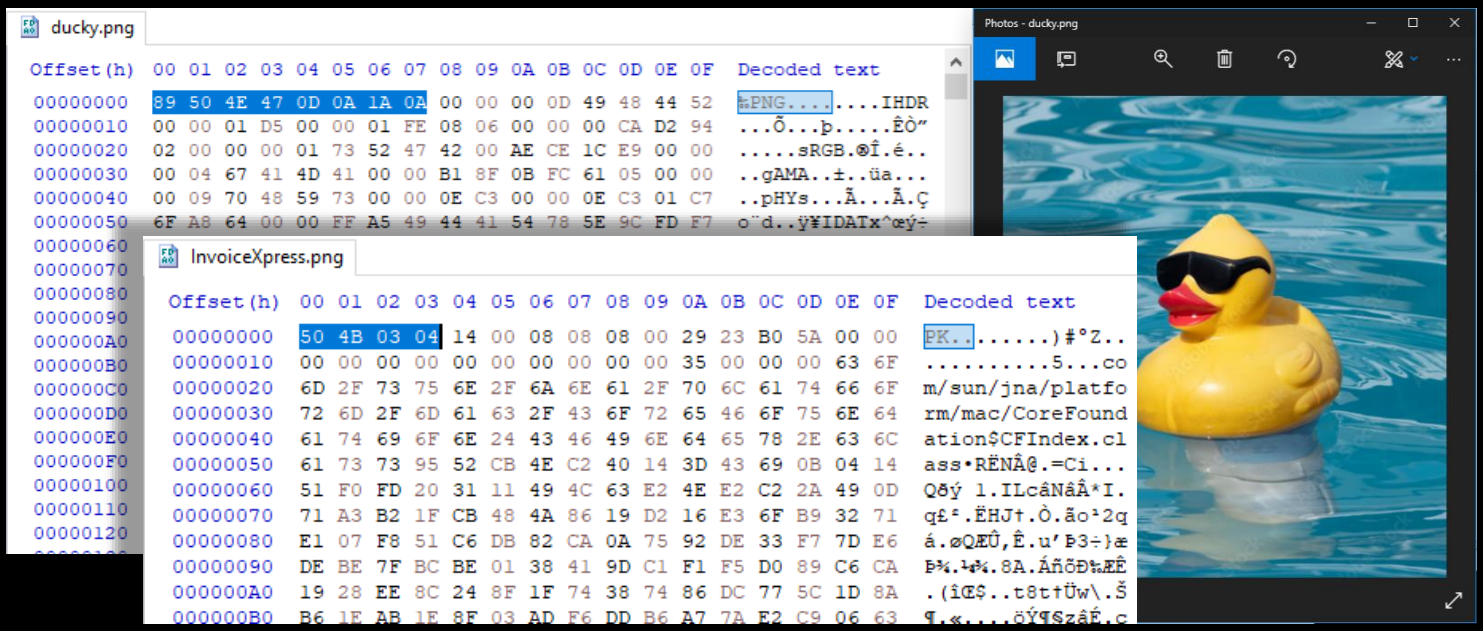
Threat Hunting Activity

When this file is passed to Java with the -jar option, Java ignores the PNG extension and instead validates the internal ZIP structure.



Observed Process Tree

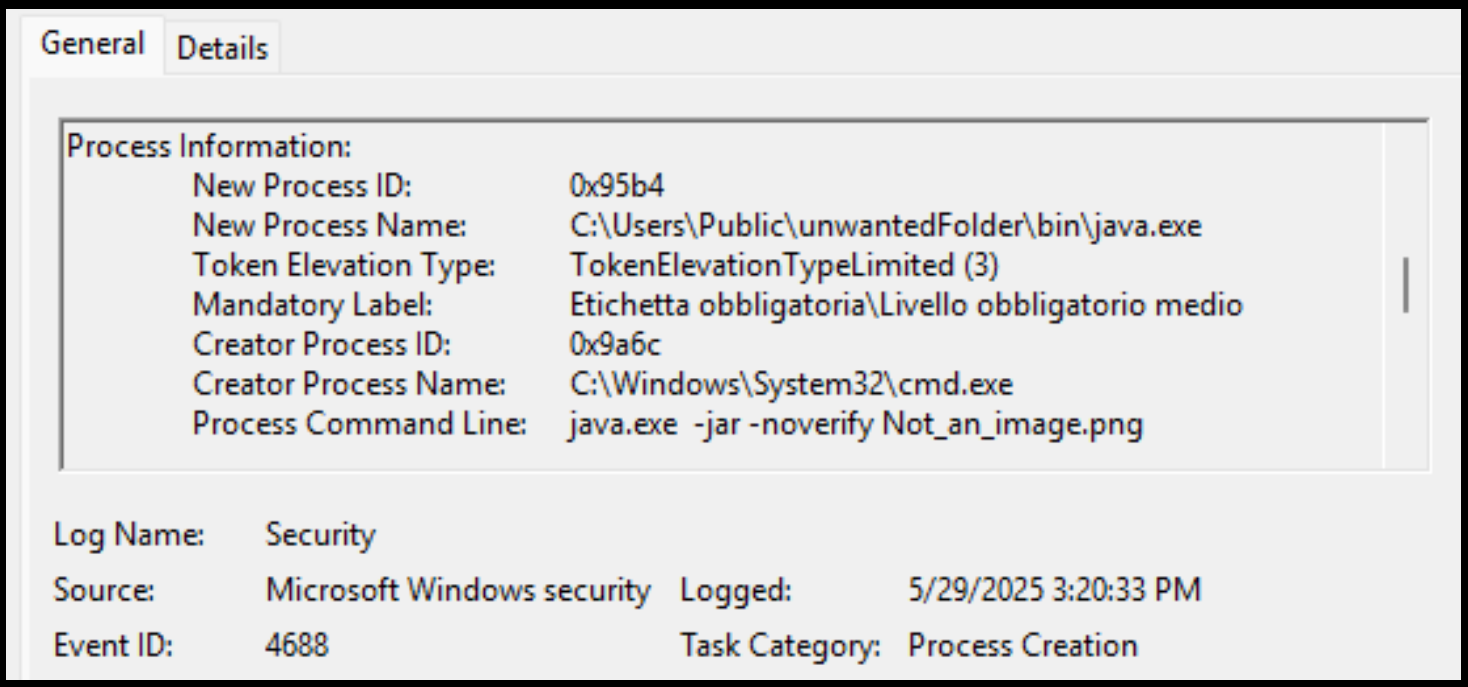
Since the embedded JAR archive is intact, Java successfully loads and executes the malicious code inside, effectively bypassing defenses that expect JAR files to have a .jar extension or a specific MIME type. EDRs and security solutions might not scan the entire file to detect the embedded JAR payload hidden behind the PNG facade. Additionally, dynamic analysis environments or sandboxes might treat the file as an image and not trigger the Java execution path, allowing the malware to slip through automated defenses. Disguising initialize a RAT with a PNG file takes advantage of gaps in how security tools validate files and how Java processes them.



Headers differences

Threat Hunting Activity

Detection can be made on EID 4688 looking suspicious process execution pattern, like what was observed during this campaign, that tricks defenses into trusting the file based on its outward appearance while still enabling the attacker to execute malicious code. This highlights the importance of continuous research rely on deeper content inspection and behavior-based detection to catch such sophisticated evasion techniques.



EID 4688

PUBLIC