SORINTSEC

THREAT HUNTING

LAB

WEEK 24/03/2025 - 28/03/2025

PUBLIC

Index

Global Weekly Threat Overview

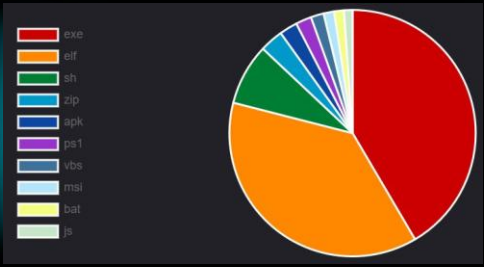
Global Weekly Notable One

Threat Hunting Activity

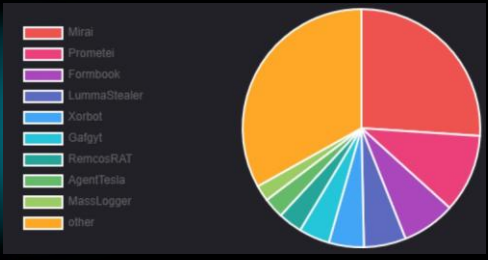
Global Weekly Threat Overview

The threat actor known as EncryptHub exploited a recently-patched security vulnerability in Microsoft Windows as a zero-day to deliver a wide range of malware families, including backdoors and information stealers such as Rhadamanthys and StealC. In this attack, the threat actor manipulates .msc files and the Multilingual User Interface Path (MUIPath) to download and execute malicious payload, maintain persistence and steal sensitive data from infected systems. Trend Micro has given the exploit the moniker MSC EvilTwin, tracking the suspected Russian activity cluster under the name Water Gamayun. The threat actor, recently the subject of analyses by PRODAFT and Outpost24, is also called LARVA-208.

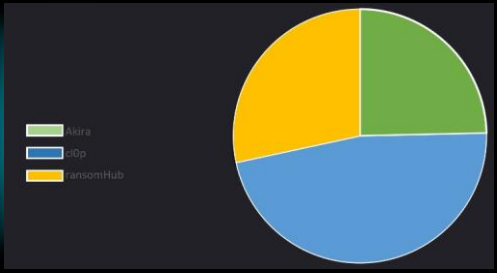
Top 10 file types



Top 10 malware family



Top 3 Ransomware Group



A new analysis has uncovered connections between affiliates of RansomHub and other ransomware groups like Medusa, BianLian, and Play. The connection stems from the use of a custom tool that's designed to disable endpoint detection and response software on compromised hosts, according to ESET. The EDR killing tool, dubbed EDRKillShifter, was first documented as used by RansomHub actors in August 2024. EDRKillShifter accomplishes its goals by means of a known tactic called Bring Your Own Vulnerable Driver that involves using a legitimate but vulnerable driver to terminate security solutions protecting the endpoints.

Global Weekly Notable One

Hijack Execution Flow: Defense Evasion

Stately Taurus, also known as Mustang Panda, Earth Preta, and several other aliases, is a Chinese advanced persistent threat (APT) group that has been active since at least 2012.

This group is primarily engaged in cyberespionage campaigns targeting government entities, NGOs, religious organizations, and critical infrastructure across Southeast Asia, Europe, and North America. Their operations align closely with the geopolitical interests of the Chinese government, particularly in regions of strategic importance such as Southeast Asia, where they have conducted numerous high-profile campaigns.

Among their arsenal, the group leverages KeyScramble, a keyboard encryption tool, to enhance their operational stealth and data exfiltration capabilities.

Global Weekly Notable One

KeyScramble, designed to protect keystrokes from keyloggers by encrypting input at the driver level, has been repurposed by Stately Taurus to evade detection during espionage campaigns.

The tool suffer from DLL side-loading and it is integrated into their malware ecosystem to obscure sensitive data exfiltration processes. DLL sideloading is an attack technique exploiting Windows' Dynamic Link Library (DLL) loading mechanism. When an application attempts to load a DLL without specifying its absolute path, Windows searches directories in a predefined order. Attackers place a malicious DLL with the same name as a legitimate one in a higher-priority directory. During execution, the application loads the malicious DLL, allowing attackers to execute arbitrary code, escalate privileges, or maintain persistence.

Threat Hunting Activity

TACTIC

Defense Evasion

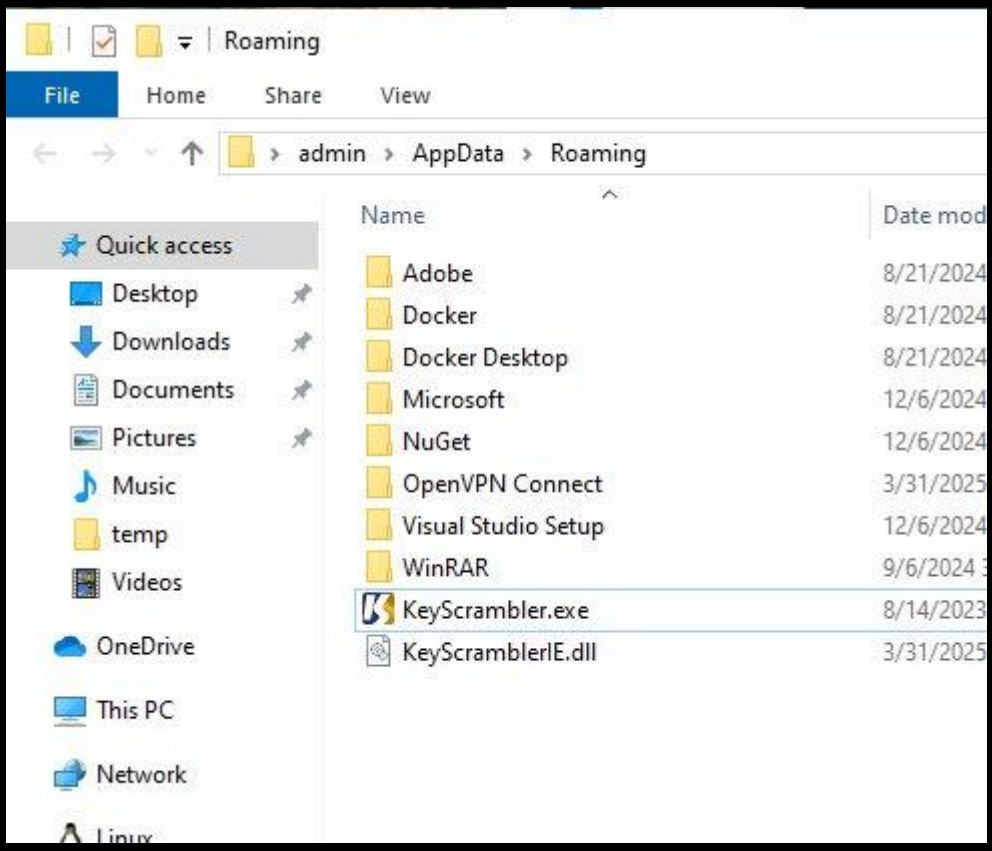
TECHNIQUES

T1574 – Hijack Execution Flow

Adversaries may execute their own malicious payloads by side-loading DLLs. Similar to DLL Search Order Hijacking, side-loading involves hijacking which DLL a program loads. But rather than just planting the DLL within the search order of a program then waiting for the victim application to be invoked, adversaries may directly side-load their payloads by planting then invoking a legitimate application that executes their payload(s).

Threat Hunting Activity

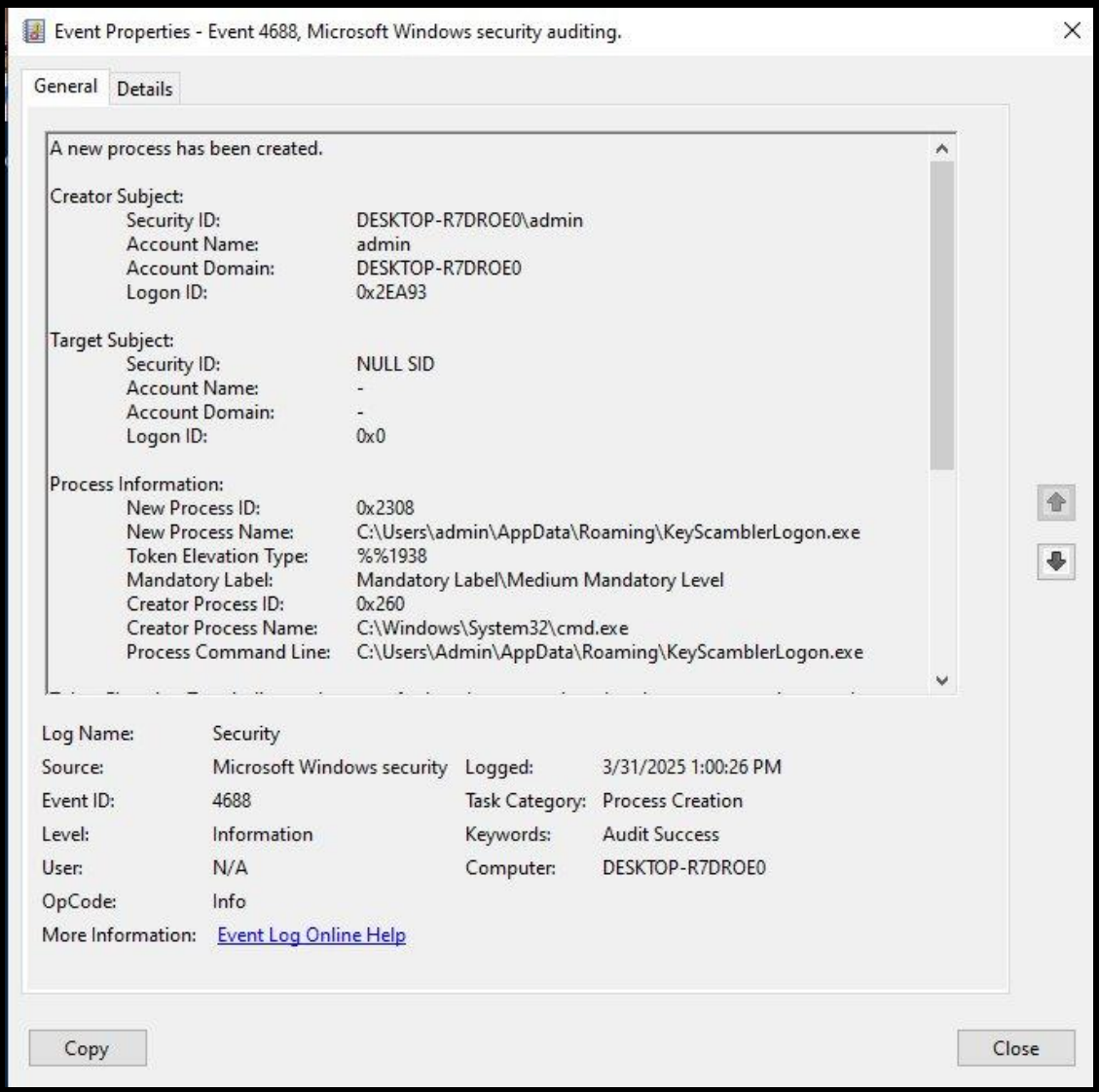
Keyscrambler DLL sideloading is exploited by copying its legitimate executable to a writable directory and placing a malicious DLL with the same name. When executed, the application loads the malicious DLL, enabling unauthorized code execution and bypassing security defenses.



.lnk content

Threat Hunting Activity

Detection can be made on EID 4688 looking for anomalous path of execution of KeyScambler.



PUBLIC