SORINT SEC

THREAT HUNTING

LAB

WEEK 20/10/2025 – 24/10/2025

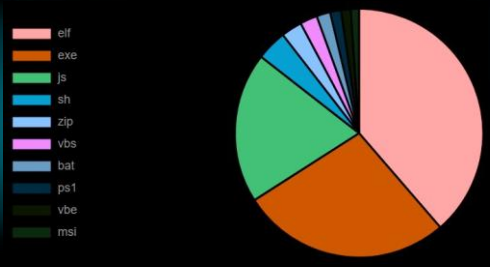
PUBLIC

Index

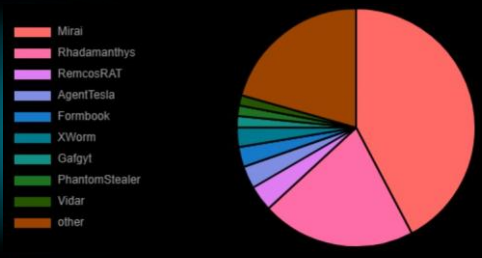
Global Weekly Threat Overview

Microsoft says that the File Explorer (formerly Windows Explorer) now automatically blocks previews for files downloaded from the Internet to block credential theft attacks via malicious documents. The change is already live for users who have installed this month's Patch Tuesday security updates on Windows 11 and Windows Server systems. The preview functionality will be disabled by default only for files viewed on an Internet Zone file share and those marked with the Mark of the Web (MotW), which shows that they've been downloaded using a web browser, received as email attachments, and obtained from other internet sources.

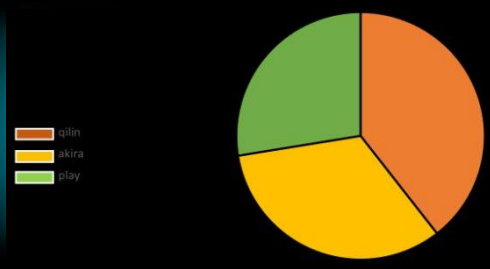
Top 10 file types



Top 10 malware family



Top 3 Ransomware Group



State-sponsored Iranian hacker group MuddyWater has targeted more than 100 government entities in attacks that deployed version 4 of the Phoenix backdoor. The threat actor is also known as Static Kitten, Mercury, and Seedworm, and it typically targets government and private organizations in the Middle East region. Starting August 19, the hackers launched a phishing campaign from a compromised account that they accessed through the NordVPN service. The emails were sent to numerous government and international organizations in the Middle East and NorthAfrica.

Global Weekly Notable One

Ingress Tool Transfer:
Command and Control

We are witnessing a significant evolution in adversary tactics: threat actors are actively leveraging legitimate, open-source incident response tools like Velociraptor for malicious purposes, effectively adopting a "misuse pattern“ instead of relying solely on custom malware.

In one major incident reported in August 2025, the suspected China-based threat actor Storm-2603 was identified as having deployed DFIR Tool Velociraptor in a ransomware campaign. Storm-2603, known for deploying multiple variants like LockBit, Warlock, and Babuk, used an outdated version of the DFIR tool to establish stealthy persistent access within the victim environment.

Global Weekly Notable One

Ingress Tool Transfer: **Command and Control**

Velociraptor is a powerful open-source digital forensics and incident response (DFIR) tool. Maintained by Rapid7, it is widely used by defenders for legitimate forensic and response workflows, enabling security teams to conduct endpoint monitoring and deliver forensic detail across various systems. Threat actors have evolved their tactics by leveraging legitimate tools like Velociraptor, minimizes the need to deploy custom malware and helps adversaries gain a foothold. Adversaries deploy the Velociraptor binary, configuring it to connect to an attacker-specified C2 server, granting stealthy persistent access.

Once C2 communication is established, the access is leveraged to download and execute such as Visual Studio Code, with the tunnel option enabled. This creates a tunnel to the C2 server, enabling both remote access and remote code execution. Threat actors also repurpose Velociraptor's native collection capabilities to conduct reconnaissance and data exfiltration, the same way DFIR teams gather evidence.

Threat Hunting Activity

TACTIC

Command and Control

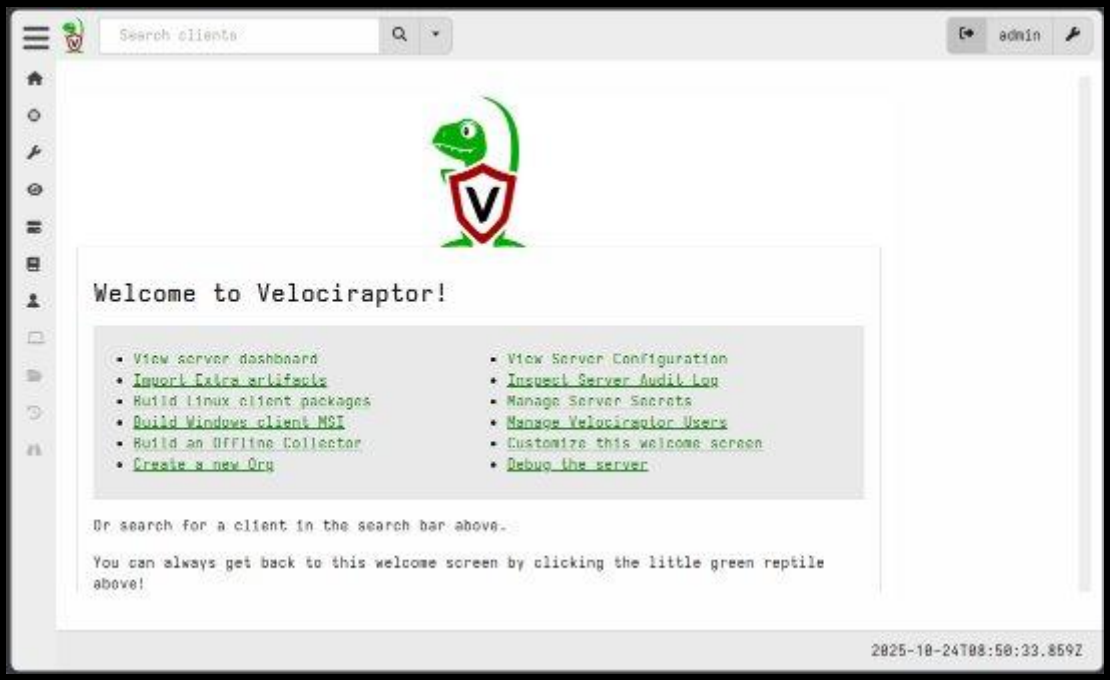
TECHNIQUES

T1105 – Ingress Tool Transfer

The adversary is trying to communicate with compromised systems to control them. Command and Control consists of techniques that adversaries may use to communicate with systems under their control within a victim network. Adversaries may transfer tools or other files from an external system into a compromised environment. Tools or files may be copied from an external adversary-controlled system to the victim network through the command and control channel or through alternate protocols such as ftp.

Threat Hunting Activity

Velociraptor is an advanced open-source digital forensic and incident response (DFIR) tool designed for endpoint monitoring and investigation.



Velociraptor GUI

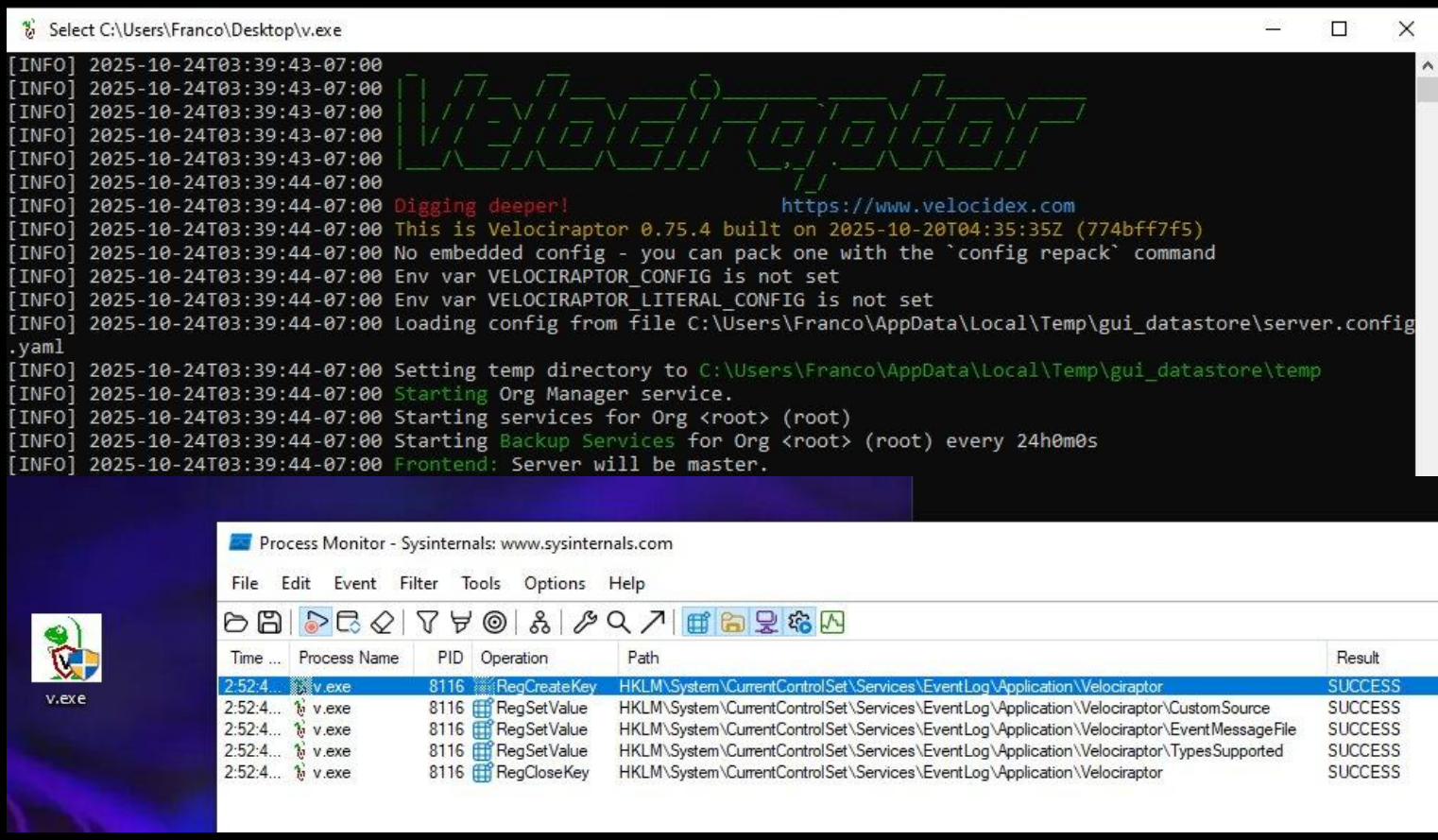
It enables administrators to run commands through CMD or PowerShell on deployed servers or clients to collect forensic data, hunt threats, and respond to incidents. Its powerful Velociraptor Query Language (VQL) allows creation of custom artifacts for targeted endpoint analysis at scale.

Velociraptor GUI

However, because it provides remote command execution capabilities, Velociraptor can be exploited by attackers as a legitimate tool for different nefarious purposes such as unauthorized access, remote code execution, and malware deployment in compromised environments. This dual-use nature makes it powerful but also risky if misused.

Threat Hunting Activity

Once the tool is executed or installed on a system, regardless the name of the binary, it registers a new event log source with the name Velociraptor

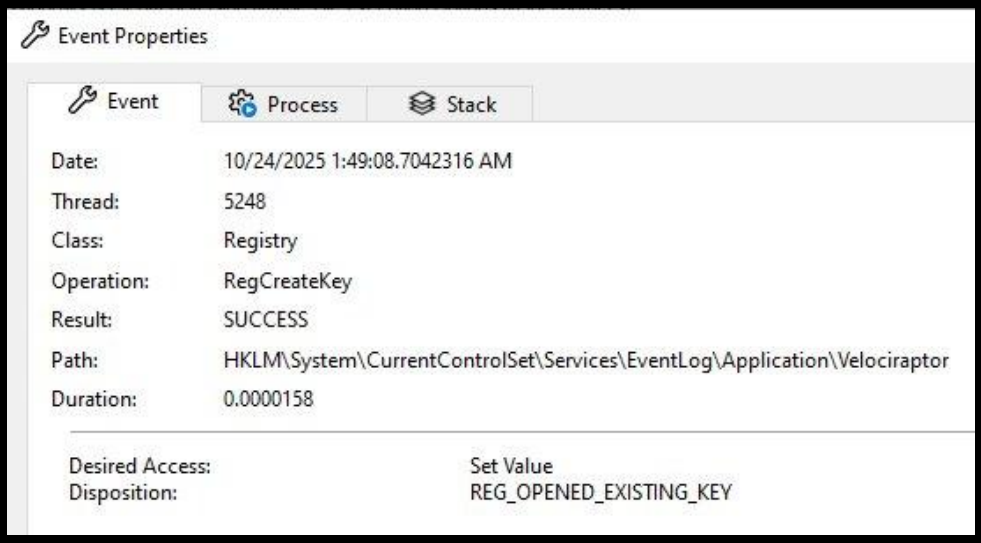


Velociraptor registry key events

This will create a new key at a precise location. The creation or last modification timestamp of this registry key generally serves as a reliable marker for when the Velociraptor binary was initially executed on the system. Looking for activities against registry key path HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Application\Velociraptor we can intercept (mis)usage of the DFIR tool.

Threat Hunting Activity

Another useful indicator that we observed while testing the instant fully functional and self-contained version “Instant Velociraptor,” is the creation of a process with an unusual and specific command line. Detection can be made intercepting this indicators.



Registry Key quered during DFIR tool initialization

EID 4688

Because Velociraptor is open source, attackers can modify the binary to remove these indicators; however, the altered binary will lack Rapid7’s digital signature, resulting in an unsigned binary. Conversely, the official Rapid7-signed binary consistently leaves detectable traces upon execution.

PUBLIC