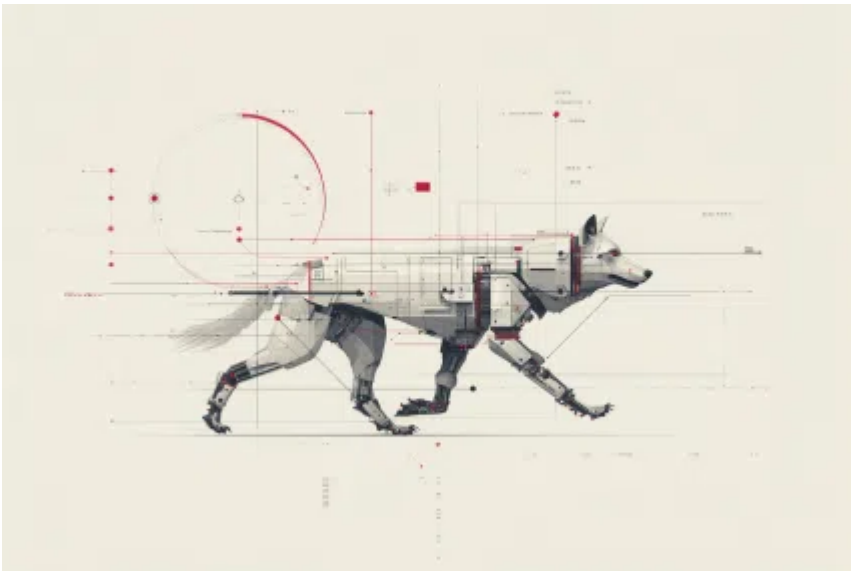
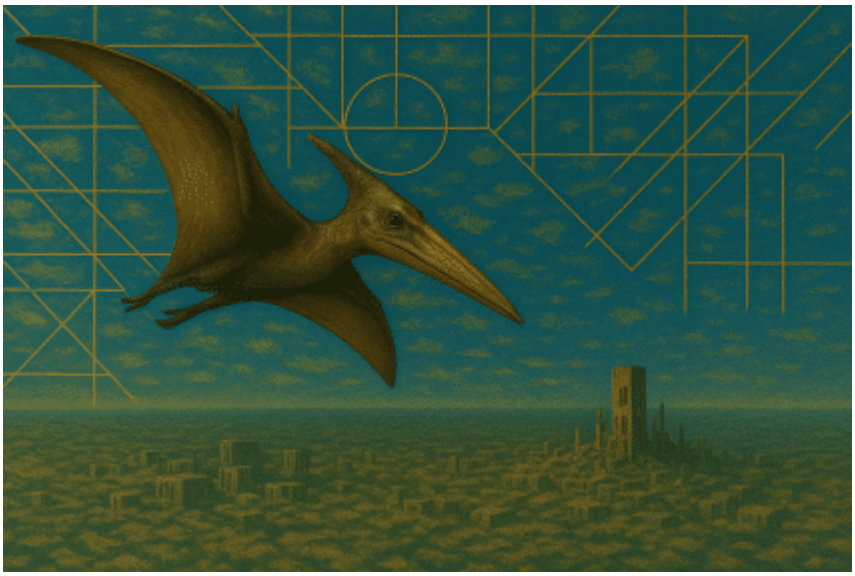
Inside The Lab - HarfangLab

Archived: 2026-04-05 22:49:27 UTC



Identifier: TRR250601. Summary This report examines recent activities we attribute to the XDSpy threat actor, focusing on an ongoing campaign targeting Eastern European and Russian governmental entities using the XDigo malware, dating back to March 2025. Our investigation stemmed from…



Identifier: TRR250401. Proactively hunting for Russian-nexus threats, we identified samples from the Pterodo malware family, commonly associated with Gamaredon, uploaded to a public malware analysis platform between late 2024 and mid-March 2025. Notably, related Gamaredon Dead Drop Resolvers (DDR) are…

Identifier: TRR250201. Summary Between October 2024 and late January 2025, public reports described the exploitation of Ivanti CSA vulnerabilities which started Q4 2024. We share analysis results confirming a worldwide exploitation, that lead to Webshells deployments in September and October…

Looking ahead to 2025, we acknowledge that predicting the future is never an exact science. However, by analyzing emerging trends and patterns, we aim to anticipate the risks that could shape the cybersecurity landscape in the year to come, with…

Summary Since mid-September 2024, our telemetry has revealed a significant increase in “Lumma Stealer”1 malware deployments via the “HijackLoader”2 malicious loader. On October 2, 2024, HarfangLab EDR detected and blocked yet another HijackLoader deployment attempt – except this time, the…

Summary In early July 2024, the Sentinel Labs researchers released an extensive article1 about “FIN7 reboot” tooling, notably introducing “AvNeutralizer”, an anti-EDR tool. This tool has been found in the wild as a packed payload. In this article, we offer…

Identifier: TRR240801. Summary This report introduces Cyclops, a newly discovered and previously undocumented malware platform written in Go which dates back to December 2023, and that we believe has been deployed against targets in the Middle-East in 2024. Cyclops allows…

Identifier: TRR240701. Summary This report delves into Doppelgänger information operations conducted by Russian actors, focusing on their activities from early June to late-July 2024. Our investigation was motivated by the unexpected snap general election in France, prompting a closer look…

Identifier: TRR240601. Summary Hunting for malicious infrastructure possibly targeting the Israeli government, we identified a previously unreported, long-standing and suspicious domain. The latter is still active at the time of this report, and is leveraged as a command and control…

Identifier: TRR240501. Summary Earlier in May, our security product spotted a malicious payload, which was tentatively delivered to a computer in Brazil, via an intricate infection chain involving Python scripts and a Delphi-developed loader. The final malicious payload, that we…

Identifier: TRR240402. Summary We have been closely monitoring the activities of the Iranian state-sponsored threat actor MuddyWater since the beginning of 2024. Our investigations reveal an active campaign that has been ramping up since October 2023, aligning with the Hamas…
