



The Malware Chronicles: Urelas, Sality, LockBit and StealC Examined

Published by [David Brunsdon](#) on Sep 04, 2024

Threat Intelligence Report

Date: September 4, 2024

Prepared by: David Brunsdon, Threat Intelligence - Security Engineer, HYAS

- Malware, short for malicious software, refers to any software designed to harm, exploit or otherwise

ransomware, spyware and adware, each with distinct characteristics and effects that pose significant risks to individuals and organizations.

- HYAS Insight tracks four malware “families”: Urelas, Sality, LockBit and StealC. Here’s a look at how each variety works and how they all pose unique threats.

The critically acclaimed film “The Hurt Locker” follows an elite U.S. Army task force as they dispose of explosives in the Iraq War. Bomb defusing makes for the most suspenseful moments, but several other scenes depict strategically controlled detonations.

When safely disarming a threat is too risky or impractical, bomb squads all over the world practice controlled detonation. There’s a significant advantage to this tactic: bomb technicians can analyze the device’s remnants to gather forensic evidence, understand its construction and maybe even identify its origin.

Although civilian cybersecurity experts don’t usually work with live explosives, they do detonate malware (malicious software such as viruses, ransomware and spyware). How? They execute a suspicious file or program on purpose. Like a bomb squad, they do this in a controlled and isolated environment, both for security and to observe and understand how it works.

Inside the Detonation: Tracking and Monitoring

systems. We do this by isolating and monitoring the file(s) as they execute, typically on a virtual machine (VM), but sometimes on a bare metal server with no connection to existing network infrastructure (aka an “air-gapped” machine).

Usually, the HYAS team spins up a new VM for each malware sample and tracks all telemetry, including log data and network communication, such as connections to command-and-control (C2) servers. We monitor the malware’s actions, like file creation and process initiation. That information is **mapped to the MITRE ATT&CK framework**, and with the rest of the detonation data, is added to our dynamic data lake. This data powers the platform’s applications and provides the latest intelligence on domains, IP addresses and other details about the threat.

We also share the intelligence with industry peers through our free daily malware feed.

HYAS’ main challenge is sandbox evasion. This is the phenomenon in which malware tries to detect if it’s being analyzed and alters its behavior accordingly. It’s an ongoing battle between detection and evasion.

Recently, we used **HYAS Insight, our leading advanced threat intelligence and investigation platform**, to track four major malware “families.” Here’s a breakdown of the key characteristics of each.

Urelas

operating systems and is characterized by its advanced evasion techniques, making it difficult to detect and analyze.

Urelas malware infiltrates systems through phishing emails containing malicious attachments or links and deploys a range of tactics, including taking screenshots of users' screens and monitoring their keystrokes. Once a hacker has gained access to a system with Urelas, it's capable of downloading additional malware — which is where the big threats come in.

Salinity

Salinity is a sophisticated and persistent family of malware known primarily for its file-infecting capabilities. Originating in the early 2000s, Salinity targets Windows operating systems and spreads rapidly by infecting executable files by attaching its malicious code to them, enabling it to execute whenever these files are run. This self-replication allows the malware to propagate across networks, removable drives, and shared folders.

The result: Salinity effectively turns every infected file into a new vector for spreading malware. Peer-to-peer technology like BitTorrent functions in a similar manner but without harmful results.

One of Salinity's key features is its polymorphic engine, which alters its code with each malware sample, making it excellent at avoiding signature-based detection. Salinity malware can also disable security software, modify system settings, and block access to security-related websites, further entrenching itself within the network it targets.

StealC is a sophisticated malware primarily designed for data theft and credential harvesting. It infiltrates systems through phishing attacks or malicious downloads. Once inside, it stealthily collects sensitive information, such as login credentials, financial data and personal details, often targeting browsers and email clients.

StealC employs advanced evasion techniques to avoid detection by antivirus software, including encryption and anti-analysis methods. The stolen data is then transmitted to a remote server controlled by the attackers. Due to its effectiveness and stealth, StealC poses a significant threat to individuals and organizations alike.

LockBit

LockBit is a notorious ransomware strain that targets organizations by encrypting their data and demanding a ransom for decryption. Known for its rapid encryption speed and advanced evasion techniques, LockBit spreads through phishing emails, exploiting vulnerabilities and remote desktop protocol (RDP) attacks. It employs a double extortion tactic, threatening to publish stolen data if the ransom is not paid.

LockBit's operators offer a **Ransomware-as-a-Service (RaaS) model**, allowing affiliates to use the malware for a share of the profits. Its effectiveness and aggressive tactics make LockBit a major threat in the cybersecurity landscape.

Real Threat Intelligence for Real Life

and response capabilities.

Our **HYAS Insight threat intelligence platform** stands out as uniquely suited to targeting these threats due to its comprehensive approach. By leveraging advanced threat intelligence and real-time tracking, HYAS enables proactive identification and mitigation of malware attacks. Its integration with the MITRE ATT&CK framework facilitates precise mapping of malware behaviors, empowering organizations to strengthen their defenses and stay one step ahead in the ongoing battle against cyber threats.

Want more threat intel on a weekly basis?

Follow HYAS on LinkedIn

Follow HYAS on X

Read recent HYAS threat reports:

HYAS Investigates Threat Actors Hidden In Gaming Services

Caught in the Act: StealC, the Cyber Thief in C

HYAS Protects Against Polyfill.io Supply Chain Attack with DNS Safeguards

StealC & Vidar Malware Campaign Identified

Sign up for the (free!) HYAS Insight Intel Feed

Disclaimer: This Threat Intelligence Report is provided “as is” and for informational purposes only. HYAS disclaims all warranties, express or implied, regarding the report’s completeness, accuracy, or reliability. You are solely

available information based on our independent research using the HYAS Insight platform. The Report's inclusion of any companies, organizations, or ASNs does not imply any wrongdoing on their part; it is simply an indication of where digital threat activities have been observed. HYAS reserves the right to update the Report as additional information is made known to us.

Learn More About HYAS Insight

An efficient and expedient investigation is the best way to protect your enterprise. **HYAS Insight** provides threat and fraud response teams with unparalleled visibility into everything you need to know about the attack. This includes the origin, current infrastructure being used and any infrastructure.

Read how the HYAS Threat Intelligence team **uncovered and mitigated a Russian-based cyber attack** targeting financial organizations worldwide.

More from HYAS Labs

**Polymorphic Malware Is No Longer Theoretical:
BlackMamba PoC.**

**Polymorphic, Intelligent and Fully Autonomous Malware:
EyeSpy PoC.**