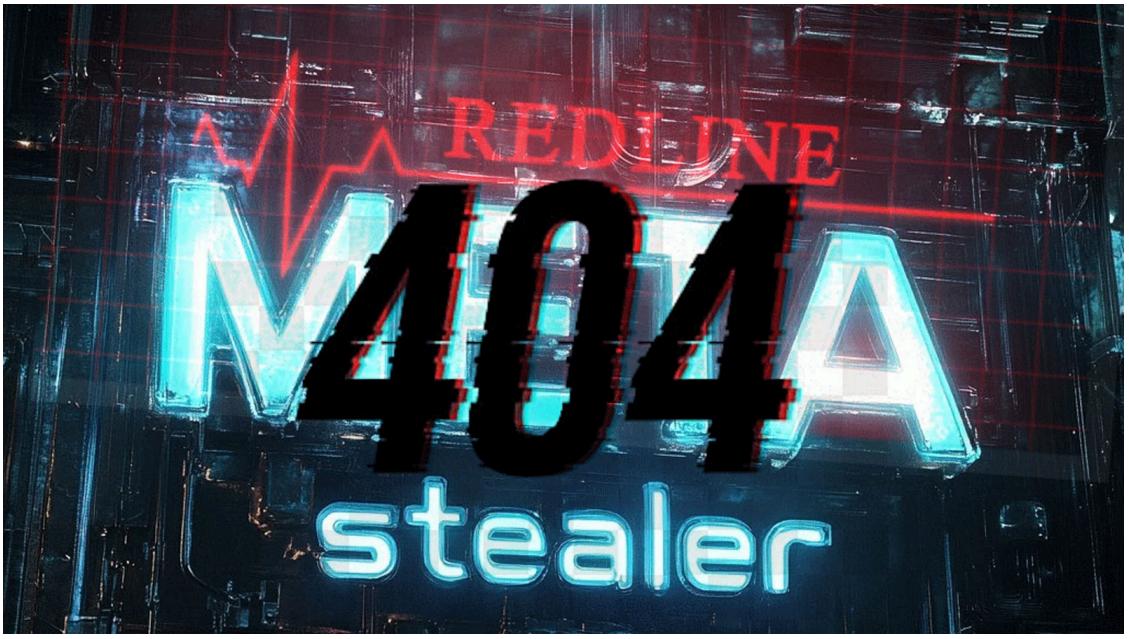
Redline, Meta infostealer malware operations seized by police

By Bill Toulas

Published: 2024-10-28 · Archived: 2026-04-05 12:56:10 UTC

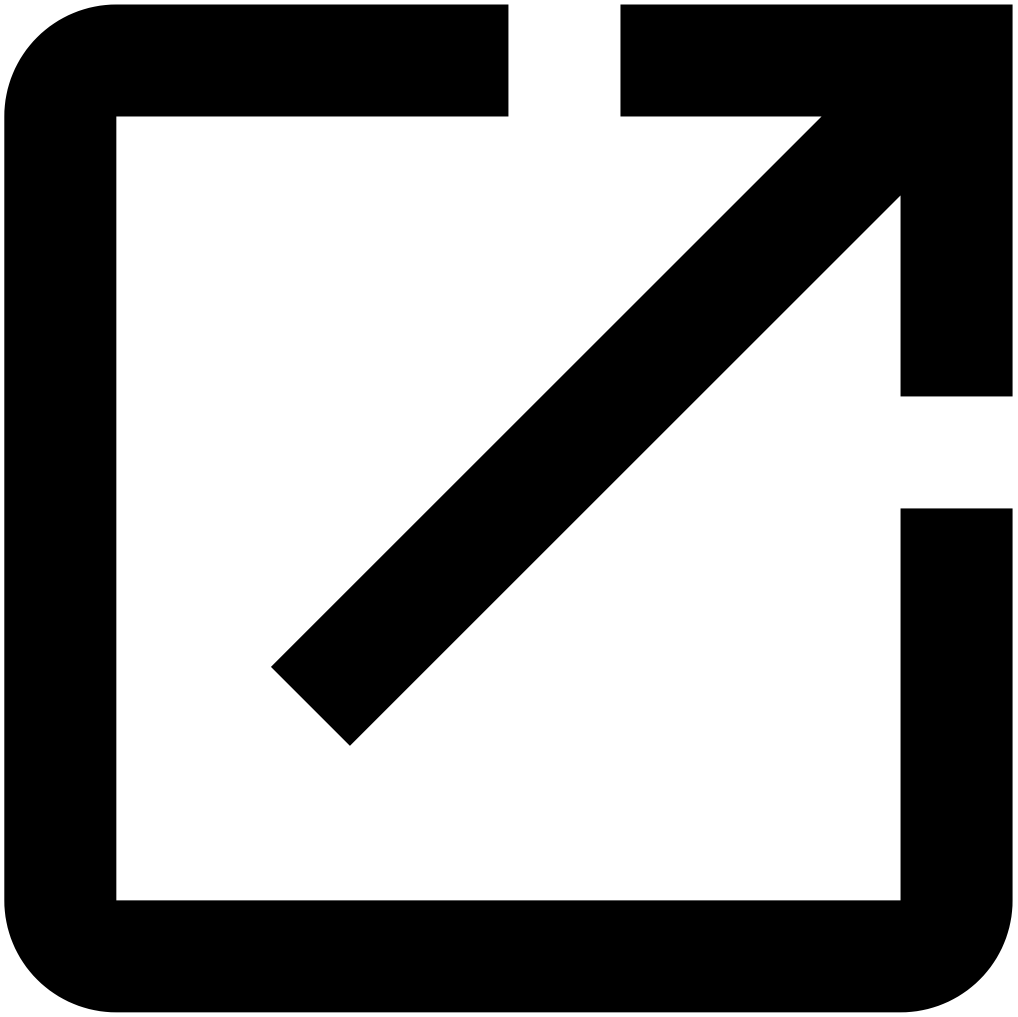


The Dutch National Police seized the network infrastructure for the Redline and Meta infostealer malware operations in "Operation Magnus," warning cybercriminals that their data is now in the hands of law enforcement.

Operation Magnus was announced on a dedicated website that disclosed the disruption of the Redline and Meta operations, stating that legal actions based on the seized data are currently underway.

"On the 28th of October 2024 the Dutch National Police, working in close cooperation with the FBI and other partners of the international law enforcement task force *Operation Magnus*, disrupted operation of the Redline and Meta infostealers," reads a short announcement on the Operation Magnus site.


DIE LINKE.
0:00



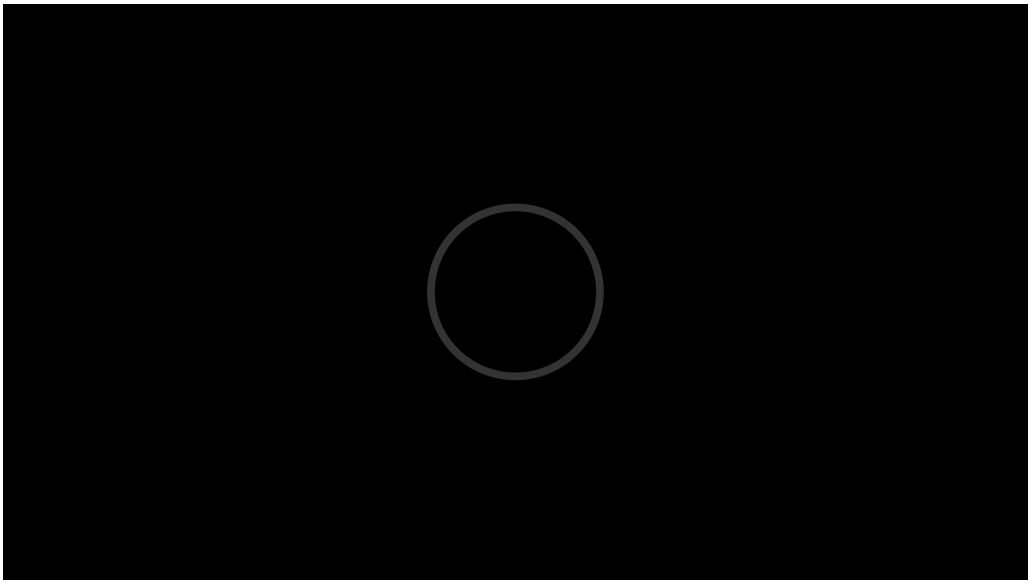
"Involved parties will be notified, and legal actions are underway."

Redline and Meta are both infostealers, a type of malware that steals stored information from browsers on an infected device, including credentials, authentication cookies, browsing history, sensitive documents, SSH keys, and cryptocurrency wallets.

This data is then sold by threat actors or used to fuel massive network breaches, leading to data theft, ransomware attacks, and cyberespionage.

Politie says they were able to disrupt the operation with the help of international law enforcement partners, including the FBI, NCIS, the U.S. Department of Justice, Eurojust, the NCA, and the police forces in Portugal and Belgium.

The agencies published the following video, announcing the "final update" for Redline and Meta users, warning that they now have their account credentials, IP addresses, activity timestamps, registration details, and more.



This makes it clear that the investigators hold evidence that can be used to track down cybercriminals who used the malware, so arrests and prosecutions are likely to be announced in the future.

Moreover, the authorities claimed they got access to the source code, including license servers, REST-API services, panels, stealer binaries, and Telegram bots, for both malware.

As they stated in the video, both Meta and Redline shared the same infrastructure, so it's likely that the same creators/operators are behind both projects.

Malware researcher g0njxa told BleepingComputer that both Redline and Meta were sold through bots on Telegram, which have now been deleted.

"These services are supported by a criminal ecosystem comprising a range of tools, infrastructure, financial services, marketplaces and forums," Deputy Director Paul Foster, head of the NCA's National Cyber Crime Unit told BleepingComputer.

"International collaboration such as this is key to identifying and taking out the various elements of this ecosystem and ultimately making it more difficult for cyber criminals to operate."

"As part of our continued support to Operation Magnus, the NCA will analyse all relevant data obtained as part of this disruption and scope out further opportunities to degrade this threat."

More information about the operation, seized infrastructure, and potential arrests is scheduled to be released tomorrow.

Police warn hackers

The Dutch police have a long history of contacting cybercriminals after conducting a law enforcement operation to warn them that they are not anonymous and are being watched.

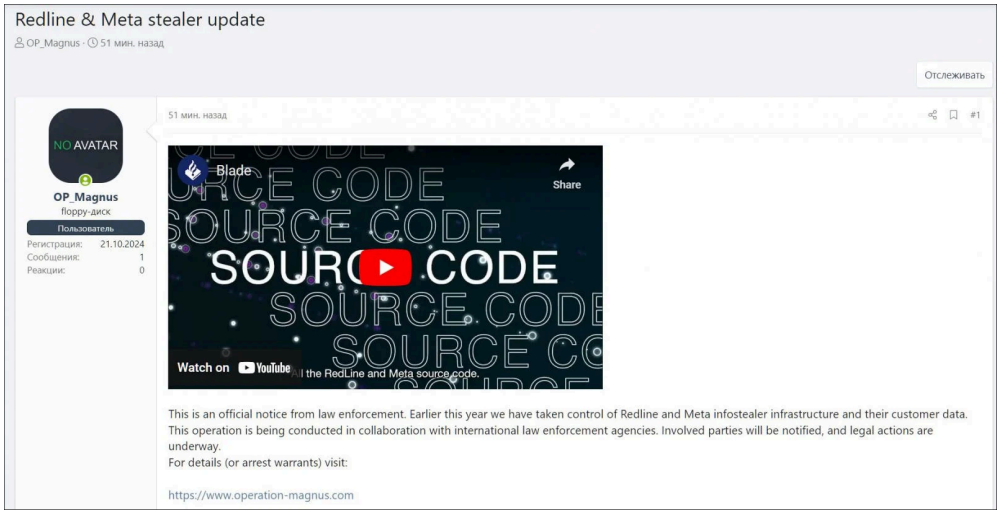
After the disruption of the Emotet botnet, the Dutch police created forum accounts on hacker forums to warn cybercriminals that they were being closely monitored.

After the RaidForums forum was seized in 2022, the Dutch Police sent emails and letters and conducted in-person "stop" calls to minors who were RaidForums members to warn them that their actions were illegal.

BleepingComputer has learned that the Dutch Police are utilizing the same tactics as part of Operation Magnus, creating forum accounts and sending direct messages that warn threat actors that they are being closely watched.

"This is an official notice from law enforcement. Earlier this year we have taken control of Redline and Meta infostealer infrastructure and their customer data." reads a post on the Russian-speaking XSS hacking forum.

This operation is being conducted in collaboration with international law enforcement agencies. Involved parties will be notified, and legal actions are underway. For details (or arrest warrants) visit: https://www.operation-magnus.com."



Operation Magnus post on the XSS hacking forum
Source: BleepingComputer

eSentire threat intelligence researcher Russian Panda also shared a screenshot of direct messages sent by the Dutch Police to cybercriminals, warning them of the action.

"Law enforcement has compromised the Redline and Meta infrastructure including the entire user database," reads the message sent to a suspected cybercriminal.

"Your client data is part of this dataset. We are reviewing this data as part of an ongoing internationally coordinated investigation."

A scourge of cybersecurity

Over the past couple of years, information-stealing malware has become a massive problem for the enterprise as the stolen credentials are commonly sold on the dark web or released for free to gain a reputation in the hacking community.

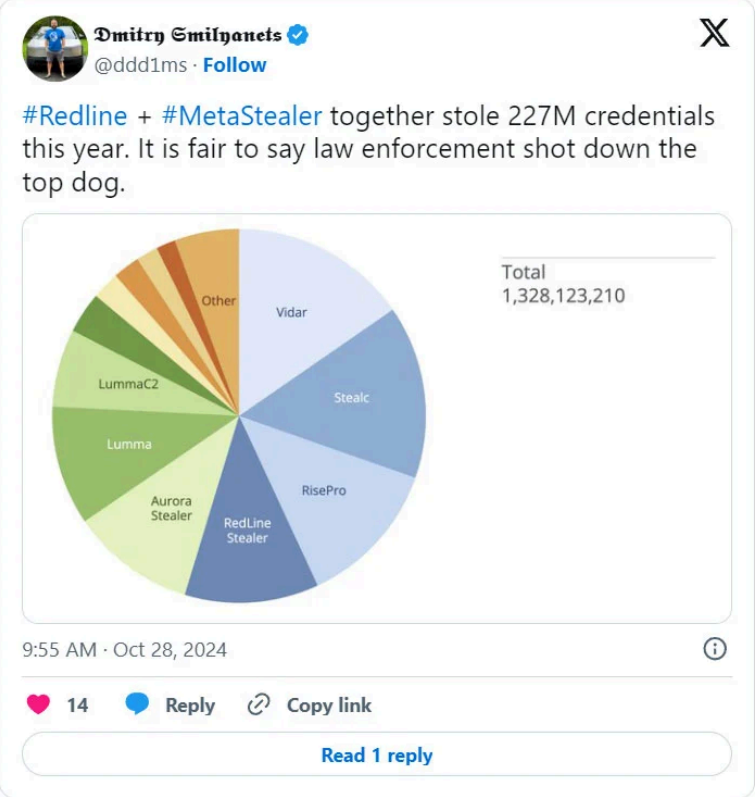
Malicious campaigns involving information-stealing malware have become abundant, with threat actors targeting victims through zero-day vulnerabilities, fake VPNs, fake fixes to GitHub issues, and even answers on StackOverflow.

One of the most common infostealers used in attacks is Redline, which launched in 2020 and has since caused widespread theft of victim's passwords, authentication cookies, cryptocurrency wallets, and other sensitive data.

Meta, aka MetaStealer, is a newer Windows infostealer malware project announced in 2022, marketed as an improved version of Redline. From Operation Magnus' announcement, we now learn that Meta was likely created by the same developers as Redline.

It should be noted that the disrupted Meta operation is different than the MetaStealer malware targeting macOS devices.

Dmitry Emilyanets, Director of Product Management at Recorded Future, shared on X that Redline and MetaStealer stole a combined total of 227 million credentials (unique email and password pair) in 2024.



Recorded Future Identity Intelligence collection metrics paints a dire picture of the entire activity, indicating that the Redline malware has stolen almost a billion credentials since it first launched.

A joint report by Specops and KrakenLabs also shared that threat actors have used Redline to steal over 170 million passwords in just six months.

These stolen credentials are then used or sold to other threat actors to breach corporate networks as part of cyberattacks.

Stolen credentials have been used to power some of the most significant breaches in recent history, including the wide-scale Snowflake data theft attacks and the Change Healthcare ransomware attack, which caused massive disruption to the U.S. healthcare system.

This is a developing story.

Source: https://www.bleepingcomputer.com/news/legal/redline-meta-infostealer-malware-operations-seized-by-police/