

# Redline Stealer Masquerades as Photo Editing Software

By eSentire Threat Response Unit (TRU)

Archived: 2026-04-05 19:43:23 UTC

Adversaries don't work 9-5 and neither do we. At eSentire, our [24/7 SOCs](#) are staffed with Elite Threat Hunters and Cyber Analysts who hunt, investigate, contain and respond to threats within minutes.

We have discovered some of the most dangerous threats and nation state attacks in our space – including the Kaseya MSP breach and the more\_eggs malware.

Our Security Operations Centers are supported with Threat Intelligence, Tactical Threat Response and Advanced Threat Analytics driven by our Threat Response Unit – the TRU team.

In TRU Positives, eSentire's Threat Response Unit (TRU) provides a summary of a recent threat investigation. We outline how we responded to the confirmed threat and what recommendations we have going forward.

**Here's the latest from our TRU Team...**

## What did we find?

- Redline Stealer malware impacting a customer in the software industry.
  - The malware was disguised as an installer for a photo editing software and was inadvertently executed by the user.
- When executed, the fake installer communicated with the command-and-control, performed anti-analysis checks and then injected code into the legitimate Windows binary MSBuild.exe using the [process hollowing](#) technique. Using the hollowed process, the malware retrieves additional files hosted on the Discord chat service and configures a scheduled task for persistence.

## How did we find it?

- eSentire [MDR for Endpoint](#) identified the process-hollowing activity.

## What did we do?

- Our [24/7 SOC Cyber Analysts](#) investigated and confirmed the activity was malicious.
- We also provided remediation recommendations and support to the customer.

## What can you learn from this TRU positive?

- [eSentire has observed](#) an increase in Redline Stealer infections since March 2022.
- Redline Stealer is a general-purpose information stealer capable of collecting credentials and sensitive data from compromised systems.

- It was initially advertised on various hacking forums in early 2020 for \$150 and \$200 USD for a “lite” and pro version respectively (Figure 1).
- Credentials stolen by information stealing malware can be used to further infiltrate networks or monetized through sale on various underground markets.
  - It’s well-established that extortion groups such as LAPSUS\$ use stolen credentials or session cookies purchased from these markets.
  - According to [Microsoft](#), LAPSUS\$ has used Redline Stealer directly as part of their initial access phase.

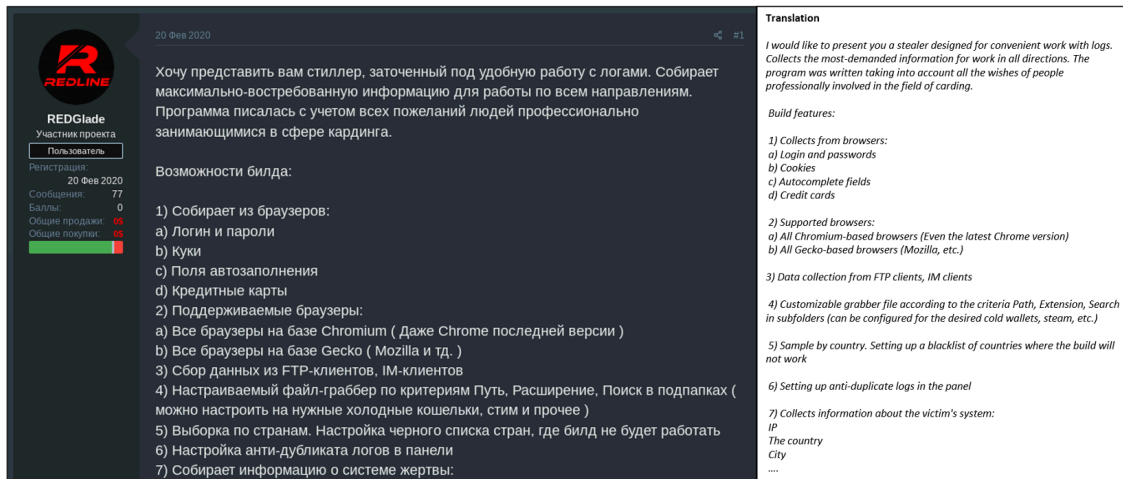


Figure 1 Early advertisement for Redline Stealer

## Recommendations from our Threat Response Unit (TRU) Team:

Protecting against information stealers requires a multi-layered defense approach to defend endpoints from malware and detect or block unauthorized login activity against applications and remote access services.

Therefore, we recommend:

- Protect all endpoints against malware.
  - Ensure antivirus signatures are up-to-date.
  - Use a Next-Gen AV (NGAV) or Endpoint Detection and Response (EDR) product to detect and contain threats.
  - In the event information stealing malware is identified, reset user credentials and terminate logon sessions.
- Restrict access to enterprise applications from personal devices outside the scope of security monitoring.
- Ensure adequate logging is in place for remote access services such as VPN and use modern authentication methods which support MFA and conditional access.

## Ask Yourself...

- Can you identify Redline Stealer in time to minimize credential compromise?
- Do you have the visibility to identify use of compromised credentials in your organization?

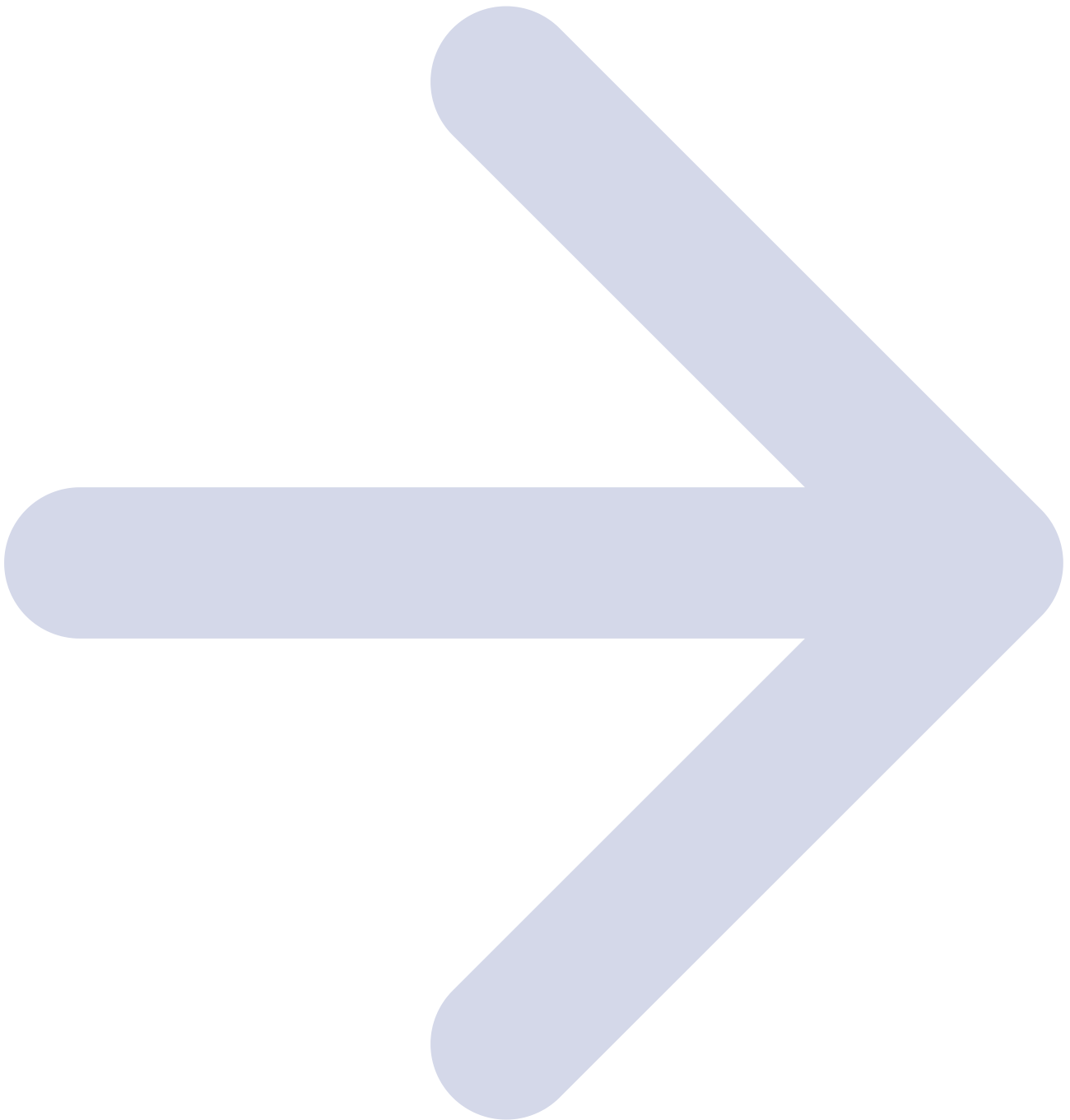
eSentire's Threat Response Unit (TRU) is a world-class team of threat researchers who develop new detections enriched by original threat intelligence and leverage new machine learning models that correlate multi-signal data and automate rapid response to advanced threats.

If you are not currently engaged with an MDR provider, eSentire MDR can help you reclaim the advantage and put your business ahead of disruption.

Learn what it means to have an elite team of Threat Hunters and Researchers that works for you. [Connect](#) with an eSentire Security Specialist.

To learn how your organization can build cyber resilience and prevent business disruption with eSentire's Next Level MDR, connect with an eSentire Security Specialist now.

[GET STARTED](#)



**ABOUT ESENTIRE’S THREAT RESPONSE UNIT (TRU)**

The eSentire Threat Response Unit (TRU) is an industry-leading threat research team committed to helping your organization become more resilient. TRU is an elite team of threat hunters and researchers that supports our 24/7 Security Operations Centers (SOCs), builds threat detection models across the eSentire XDR Cloud Platform, and works as an extension of your security team to continuously improve our Managed Detection and Response service. By providing complete visibility across your attack surface and performing global threat sweeps and proactive hypothesis-driven threat hunts augmented by original threat research, we are laser-focused on defending your organization against known and unknown threats.

[Back to blog](#)

**Take Your Cybersecurity Program to the Next Level with eSentire MDR.**

[BUILD A QUOTE](#)

**in this blog**

[What did we find?How did we find it?What did we do?What can you learn from this TRU positive? Recommendations from our Threat Response Unit \(TRU\) Team:](#)

Source: <https://www.esentire.com/blog/redline-stealer-masquerades-as-photo-editing-software>