

# Remcos RAT

By eSentire Threat Response Unit (TRU)

Archived: 2026-04-05 19:45:53 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?

- [Remcos](#) (Remote Control & Surveillance Software) was identified in a customer environment in the legal services industry.
- Remcos is a malicious remote access tool (RAT) marketed as a legitimate remote administration tool which can be purchased for between €58-399.
  - The tool can be used to control the system, capture keystrokes, webcam images, screen captures, and passwords (among other capabilities).
  - Version 3.3.2 Pro was identified in this incident.
- The infection vector for Remcos was a password-protected, macro-enabled Excel file named "[remittance advice.xlsm](#)".
  - Once opened, PowerShell is executed to retrieve a remote script ([edi.vbs/firewall.vbs](#)) from **hxxp://lbl[.]support**.
  - The script fetches additional components, enables persistence via registry run key and ultimately executes Remcos within a legitimate Windows process.



Figure 1 Online purchasing form for Remcos

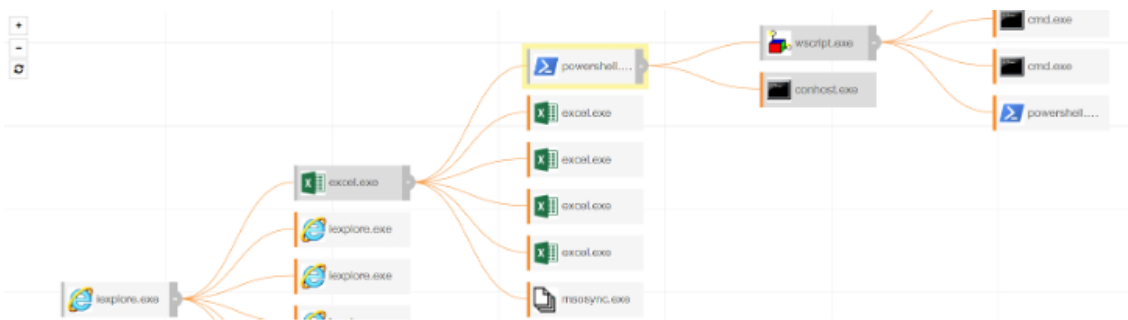


Figure 2 Process tree showing execution stages

## How did we find it?

- BlueSteel, our machine-learning powered PowerShell classifier, identified PowerShell commands executed by Remcos RAT
- MDR for Endpoint identified secondary execution phases.

## What did we do?

- Our team of [24/7 SOC Cyber Analysts](#) isolated the host and worked with the customer to remediate.

## What can you learn from this TRU positive?

- Remcos provides an attacker with nearly full control of the compromised system, so rapid identification and removal is critical.
- Remcos stores captured information in the following files and folders:
  - %APPDATA%\rem\logs.dat (captured keystrokes)
  - %APPDATA%\Screenshots

- %APPDATA%\MicRecords
- Unfortunately, antivirus detection for the macro-enabled Excel document is minimal since password-protected documents can be used to evade link and attachment inspection.
  - As of January 18th, 2022 only two vendors have [identified it](#) on VirusTotal.

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

- Employ email filtering and protection measures.
  - Block or quarantine email attachments such as EXEs, Password-Protected ZIPs, Javascript, and VisualBasic scripts.
  - Implement anti-spoofing measures such as DMARC and SPF.
  - Employ an MFA solution to reduce impact of compromised credentials.
  - Train users to identify and report suspicious emails.
- Protect 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.
  - Limit or disable macros across the organization. See UK's [National Cyber Centre](#) guidance on Macro Security.

## Ask Yourself...

- Can my team prevent emails containing encrypted malicious documents from reaching users?
- Does my team have endpoint monitoring in place to identify malicious documents which bypass email controls?

## Indicators of Compromise

Type	Value	Note
File (SHA256)	50f2ff7d96392fcfe6ed57a1ff71ae9c87a1346ff3694173a255b67e9ff8a208	firewall.vbs
File (SHA256)	abf8ada022fce92c24e0aead4f1b1ae8991002130bbbc4335f3381972683b400	Remittance Advice.xlsm
Domain	eter101[.]dvrlists[.]com	Remcos C2
Domain	eter103[.]dvrlists[.]com	Remcos C2
Domain	lb[.]support	Hosts firewall.vbs and other components

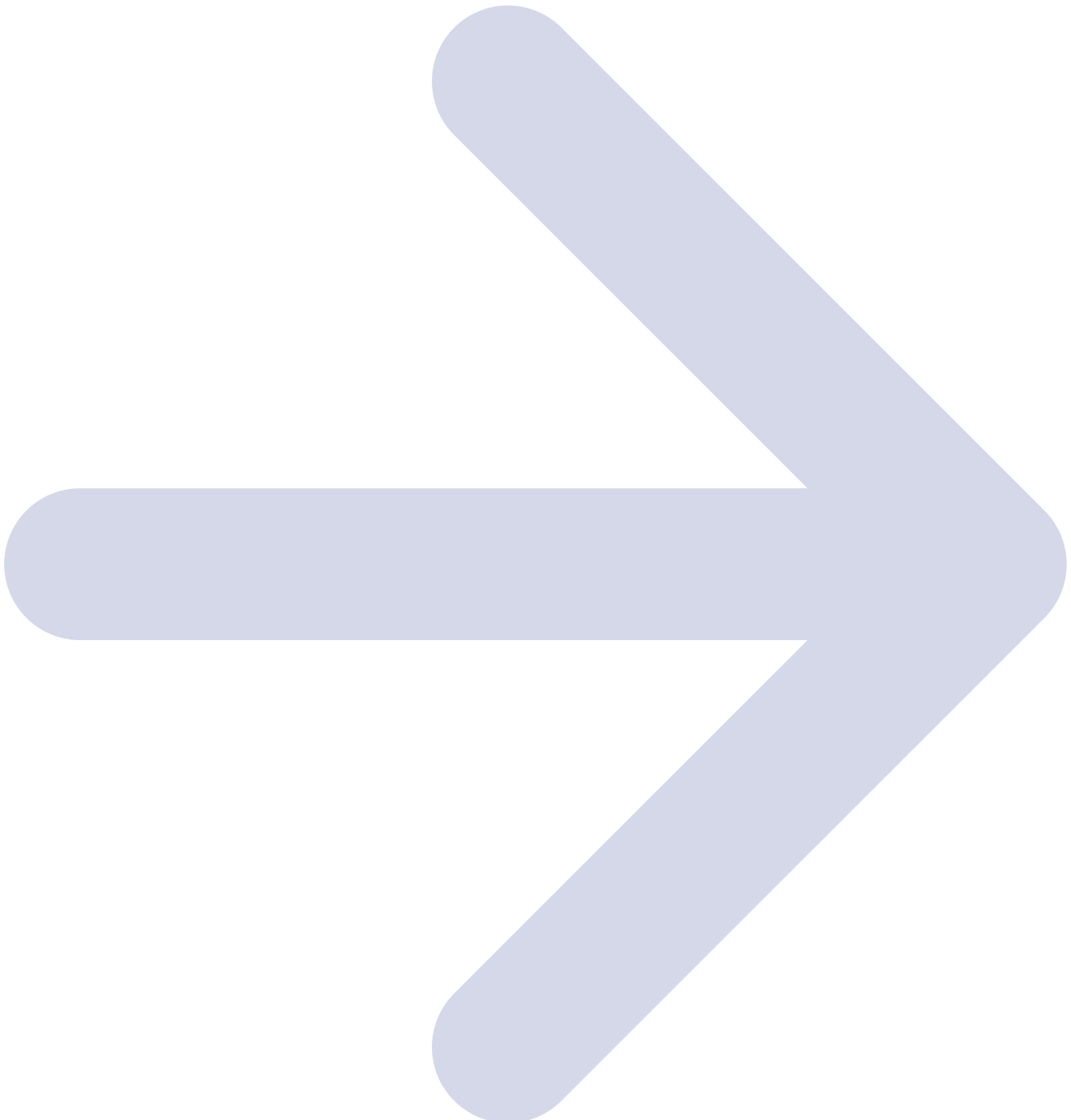
		used during execution
--	--	--------------------------

If you're not currently engaged with a Managed Detection and Response provider, we highly recommend you partner with us for security services in order to disrupt threats before they impact your business.

Want to learn more? [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/remcos-rat>