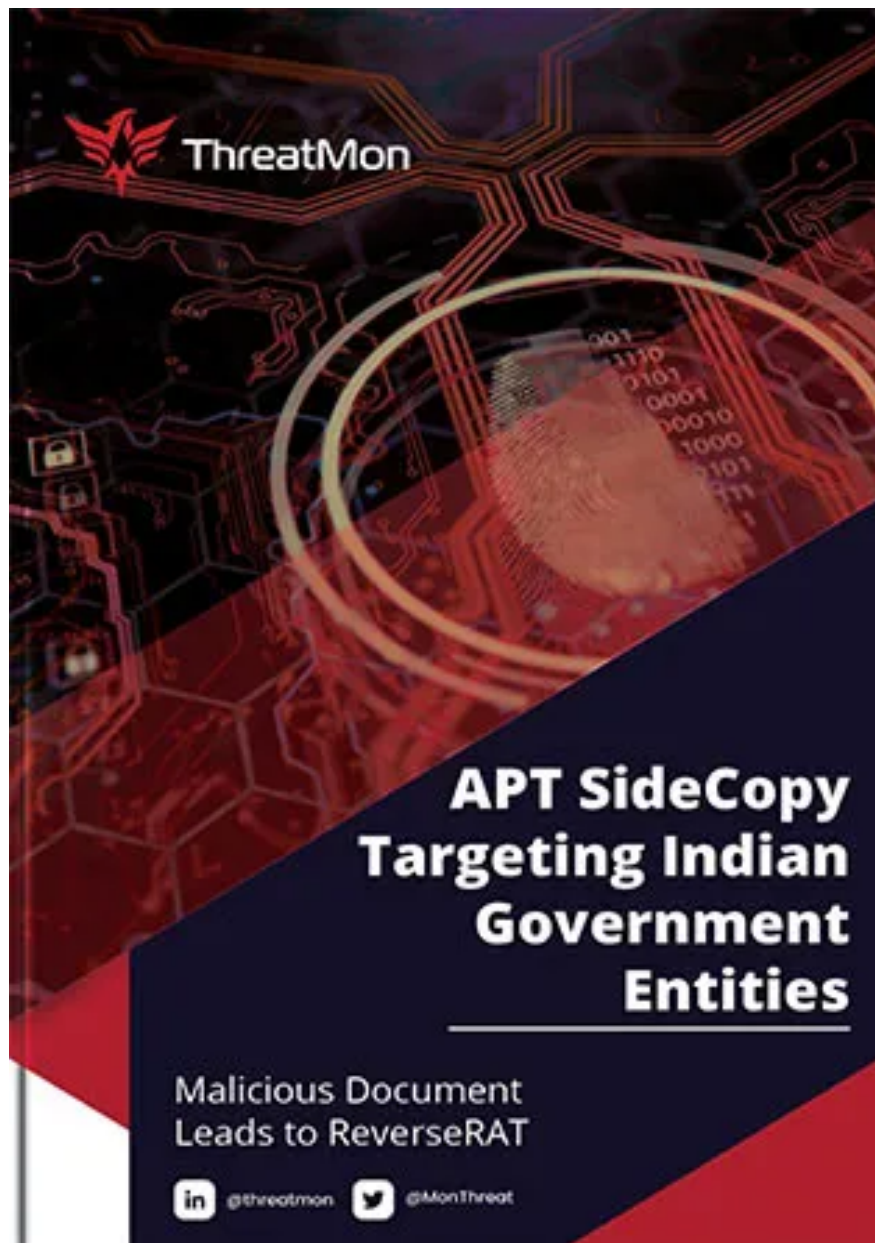


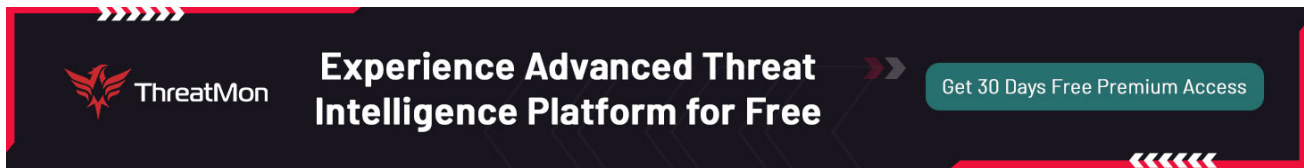
APT SideCopy Targeting Indian Government Entities

 threatmon.io/apt-sidecopy-targeting-indian-government-entities/



SideCopy, a Pakistani threat group, targeted Indian Government Entities using a spear-phishing email containing a macro-enabled Word document. If the recipient opens the document and enables macros, it triggers the execution of malicious code, allowing SideCopy to gain initial access. The malware used is a new version of ReverseRAT, which has enhanced obfuscation and sleep calls to avoid detection. Once ReverseRAT gains persistence, it enumerates the victim's device, collects data,

encrypts it using RC4, and sends it to the Command and Control (C2) server. It waits for commands to execute on the target machine, and some of its functions include taking screenshots, downloading and executing files, and uploading files to the C2 server.

A dark banner with a red border. On the left is the ThreatMon logo (a red bird-like icon) and the text "ThreatMon". In the center, the text "Experience Advanced Threat Intelligence Platform for Free" is displayed in white. On the right, there is a teal button with the text "Get 30 Days Free Premium Access".

Experience Advanced Threat Intelligence Platform for Free

Get 30 Days Free Premium Access

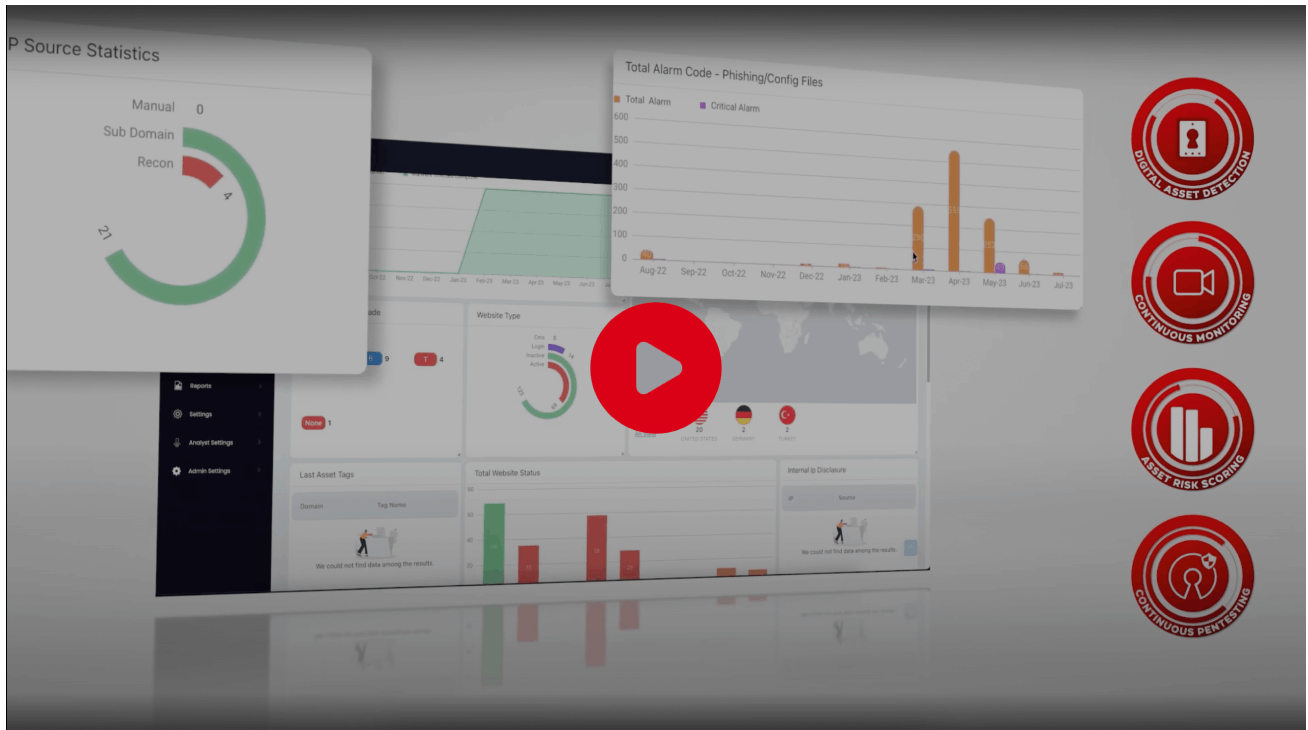


Download Here

Watch the ThreatMon's Platform Intro

ThreatMon has a team of highly Threatmon's cutting-edge solution combines Threat Intelligence, External Attack Surface Management, and Digital Risk Protection to identify vulnerabilities and provide personalized security solutions for maximum security. ThreatMon identifies the distinctive nature of each business and provides bespoke solutions that cater to its specific needs.

- Identify the external assets of your business.
- Track and manage your organization's online reputation to maintain a positive image.
- Monitor social media platforms, deep/dark web activities, and rogue applications.
- Detect and mitigate digital risks such as source code leakage and account leakage.



Latest Reports



[Kuwait Threat Landscape Report](#)

[Read the Report](#)



The Anatomy of a Sidecopy Attack: From RAR Exploits to AllaKore RAT

[Read the Report](#)



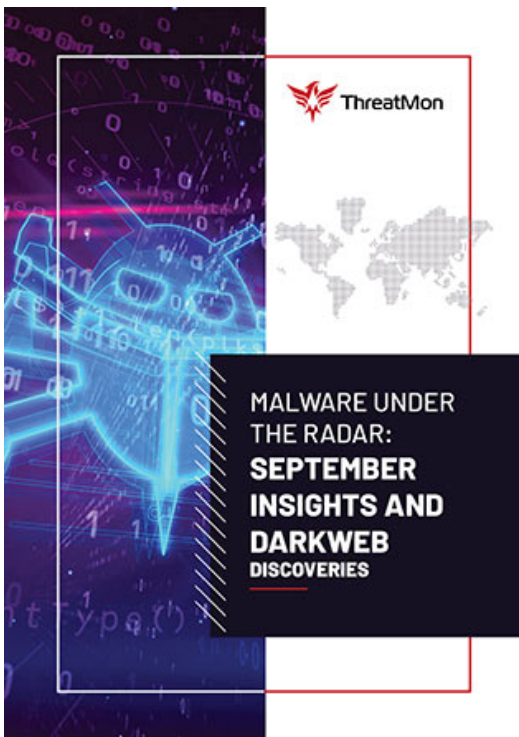
Serpent Stealer Unmasked: Threat Analysis and Countermeasures

[Read the Report](#)



Riddle Unveiled: New Evasive Stealer Malware from the Underground

[Read the Report](#)



Malware Under the Radar: September Insights and Darkweb Discoveries

[Read the Report](#)



[Navigating the Digital Frontier: Cyber Threats in the Israeli-Palestinian War](#)

[Read the Report](#)



[The Importance Of Attack Surface Management For Industries: Education](#)

[Read the Report](#)



[The Konni APT Chronicle: Tracing Their Intelligence-Driven Attack Chain](#)

[Read the Report](#)



[Unraveling the Layers: Analysis of Kimsuky's Multi-Staged Cyberattack](#)

[Read the Report](#)



The Importance Of Attack Surface Management For Industries: Health

[Read the Report](#)



Stealing in Stealth: Investigating a Python-based Evasive Malware Exela

[Read the Report](#)



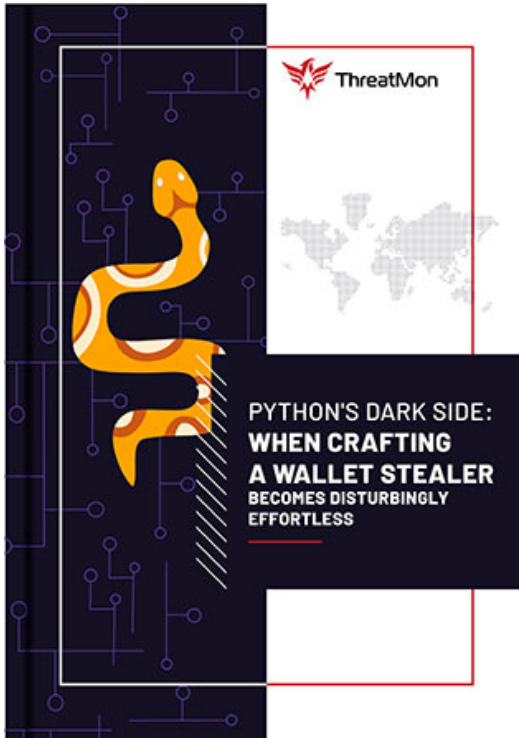
August's Cyber Underworld: Exploring Novel Malware Families on the Darkweb

[Read the Report](#)



The Importance Of Attack Surface Management For Industries: IT

[Read the Report](#)



Python's Dark Side When Crafting a Wallet Stealer Becomes Disturbingly Effortless

[Read the Report](#)



Chaos Unleashed: a Technical Analysis of a Novel Ransomware

[Read the Report](#)



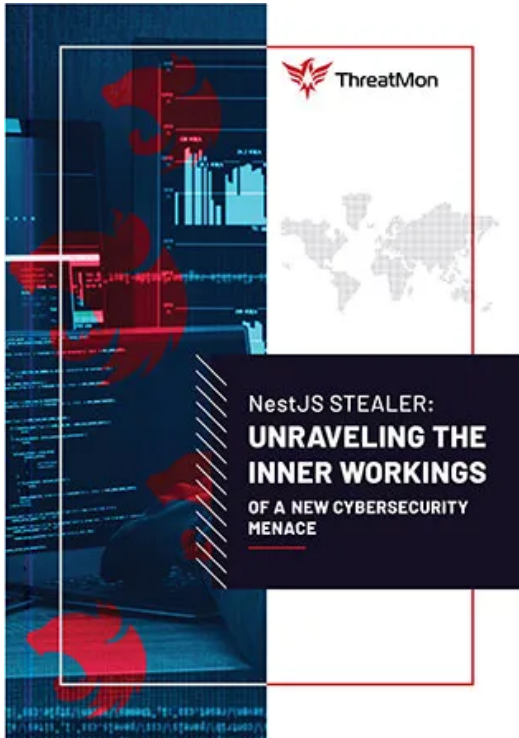
The Importance Of Attack Surface Management For Industries: Banking

[Read the Report](#)



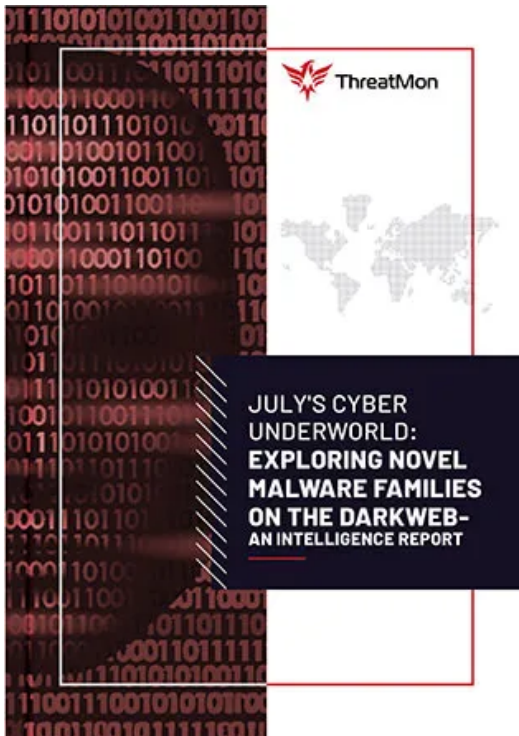
RAT Goes Phishing: Dissecting the Stealthy Techniques of REM Phishing RAT

[Read the Report](#)



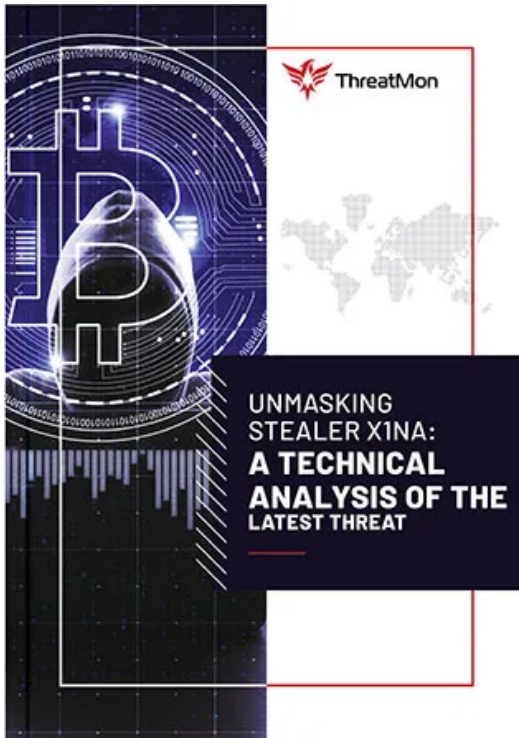
[NestJS Stealer: Unraveling the Inner Workings of a New Cybersecurity Menace](#)

[Read the Report](#)



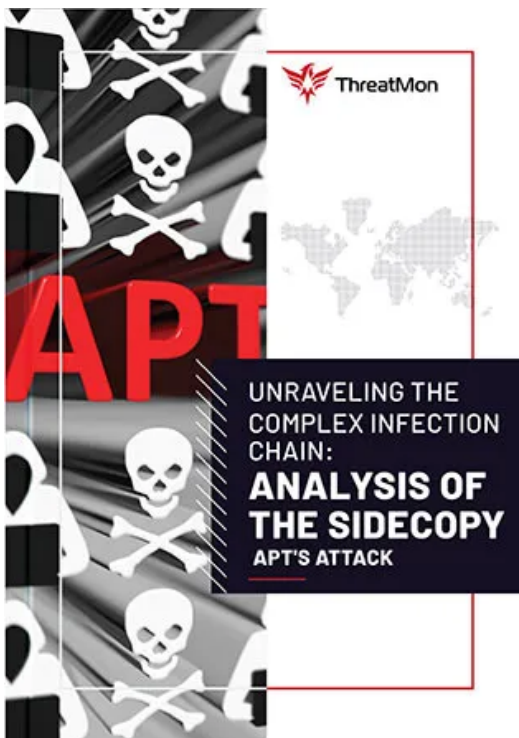
[July's Cyber Underworld: Exploring Novel Malware Families on the Darkweb- An Intelligence Report](#)

[Read the Report](#)



[Unmasking Stealer X1na: A Technical Analysis of the Latest Threat](#)

[Read the Report](#)



[Unraveling the Complex Infection Chain: Analysis of the SideCopy APT's Attack](#)

[Read the Report](#)



[Solving the Puzzle: Reversing the New Stealer Jigsaw](#)

[Read the Report](#)



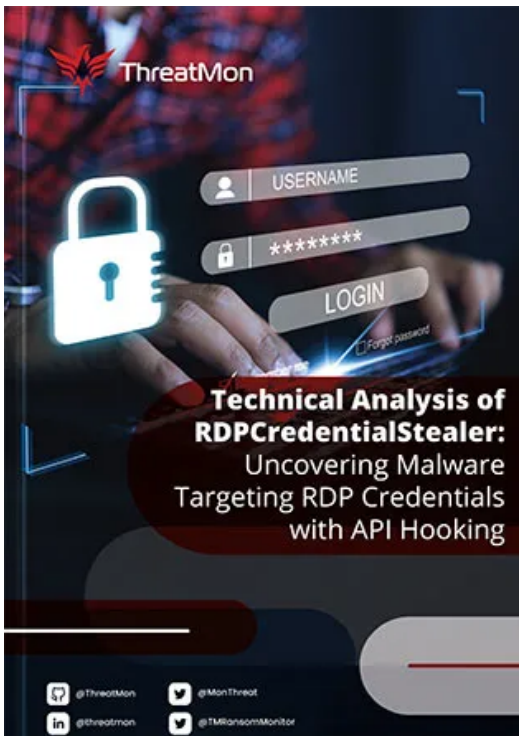
[From Slides to Threats: Transparent Tribe's New Attack on Indian Government Entities Using Malicious PPT](#)

[Read the Report](#)



[June's Cyber Battleground: Decoding Ransomware and APT Attacks in Europe](#)

[Read the Report](#)



Technical Analysis of RDP Credential Stealer: Uncovering Malware Targeting RDP Credentials with API Hooking

[Read the Report](#)



Vulnerability Report (28-04) December 2022

[Read the Report](#)



Ransomware Group Activity Report (05-18) November 2022

[Read the Report](#)



Ransomware Group Activity Report (28-04) November 2022

[Read the Report](#)



Arkei Stealer Analysis 2022

[Read the Report](#)



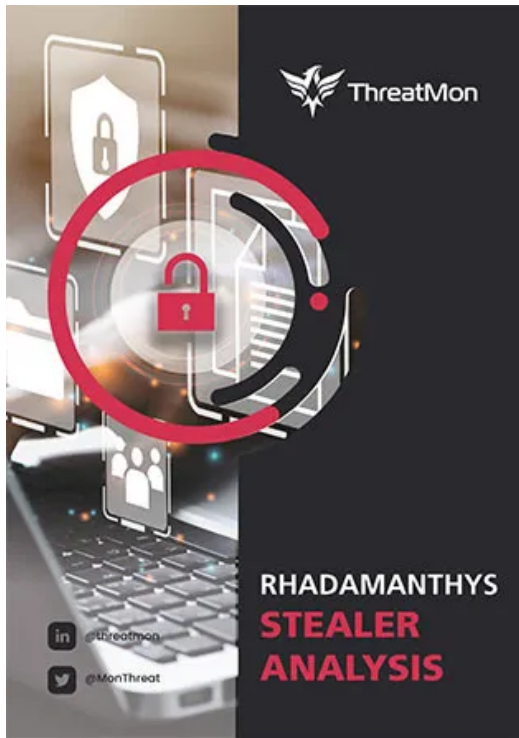
Ransomware Group Activity Report (17-28) October 2022

[Read the Report](#)



Ransomware Group Activity Report (30-16) October 2022

[Read the Report](#)



Rhadamanthys Stealer Analysis 2022

[Read the Report](#)



Ransomware Group Activity Report (17-30) September 2022

[Read the Report](#)



Ransomware Group Activity Report (03-16) September 2022

[Read the Report](#)



[Read the Report](#)

***Ransomware
Digest Report
(12-19) August
2021***

Ransomware Digest Report (12-19) August 2021

[Read the Report](#)

***Ransomware
Digest Report
(19-26) August
2021***

Ransomware Digest Report (19-26) August 2021

[Read the Report](#)

***Ransomware
Digest Report
(26-03)
August 2021***

Ransomware Digest Report (26-03) August 2021

[Read the Report](#)

***Ransomware
Digest Report
(03-09)
September 2021***

Ransomware Digest Report (03-09) September 2021

[Read the Report](#)



Phishing Intelligence Report 2021

[Read the Report](#)

Ransomware Digest Report (09-16) September 2021

Ransomware Digest Report (09-16) September 2021

[Read the Report](#)

***Ransomware
Digest Report
(17-23)
September 2021***

Ransomware Digest Report (17-23) September 2021

[Read the Report](#)

***Ransomware
Digest Report
(23-30)
September 2021***

[Read the Report](#)

***Ransomware
Digest Report
October 2021***

[Read the Report](#)

***Ransomware
Digest Report
November 2021***

[Read the Report](#)

***Log4J Remote
Code Execution
Detailed
Analysis 2021***

Log4J Remote Code Execution Detailed Analysis 2021

[Read the Report](#)

***Ransomware
Digest Report
December 2021***

Ransomware Digest Report December 2021

[Read the Report](#)

Ransomware Digest Report January 2022

Ransomware Digest Report January 2022

[Read the Report](#)

Ransomware Digest Report February 2022

Ransomware Digest Report February 2022

[Read the Report](#)

***Ransomware
Digest Report
March 2022***

Ransomware Digest Report March 2022

[Read the Report](#)

***Ransomware
Digest Report
April 2022***

Ransomware Digest Report April 2022

[Read the Report](#)



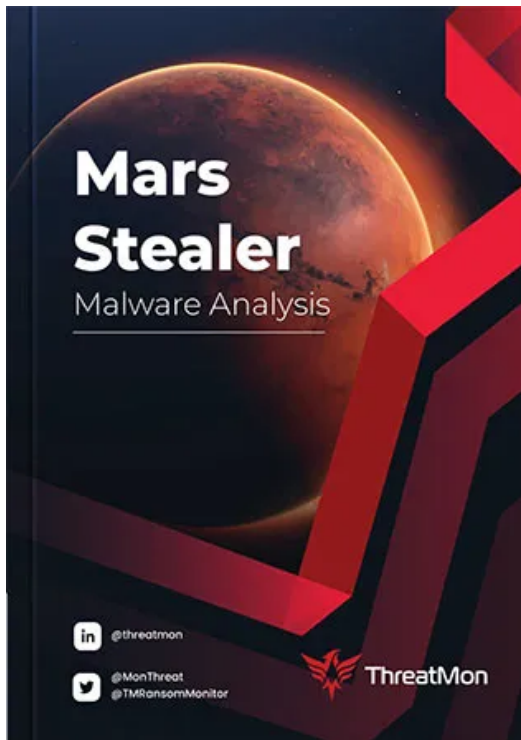
Ransomware Group Activity Report (05-18) December 2022

[Read the Report](#)

Ransomware Digest Report May 2022

Ransomware Digest Report May 2022

[Read the Report](#)



Mars Stealer Malware Analysis 2022

[Read the Report](#)



Ransomware Group Activity Report (18-01) December 2022

[Read the Report](#)

Ransomware Digest Report June 2022

Ransomware Digest Report June 2022

[Read the Report](#)



Ransomware Group Activity Report (01-13) January 2023

[Read the Report](#)

Ransomware Digest Report July 2022

Ransomware Digest Report July 2022

[Read the Report](#)



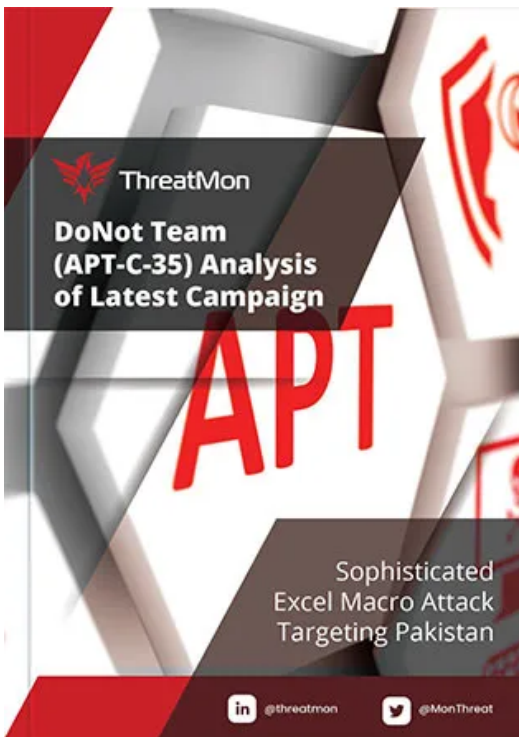
Ransomware Group Activity Report (13-27) January 2023

[Read the Report](#)



The Global Cyber Security Intelligence Risk Report 2023

[Read the Report](#)



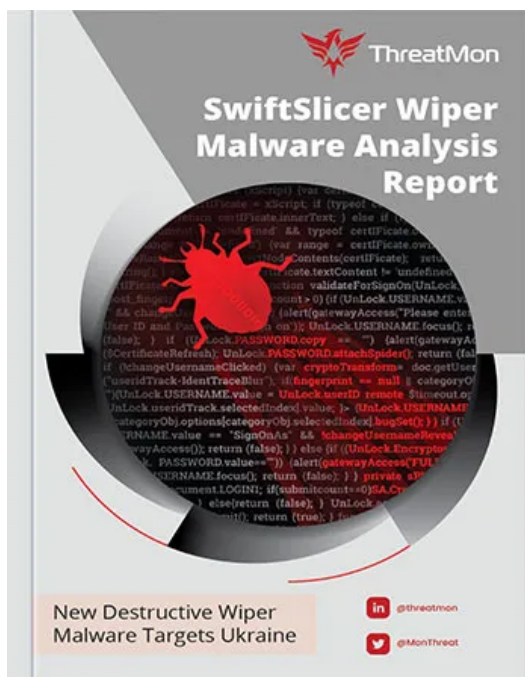
DoNot Team (APT-C-35) Analysis of Latest Campaign

[Read the Report](#)



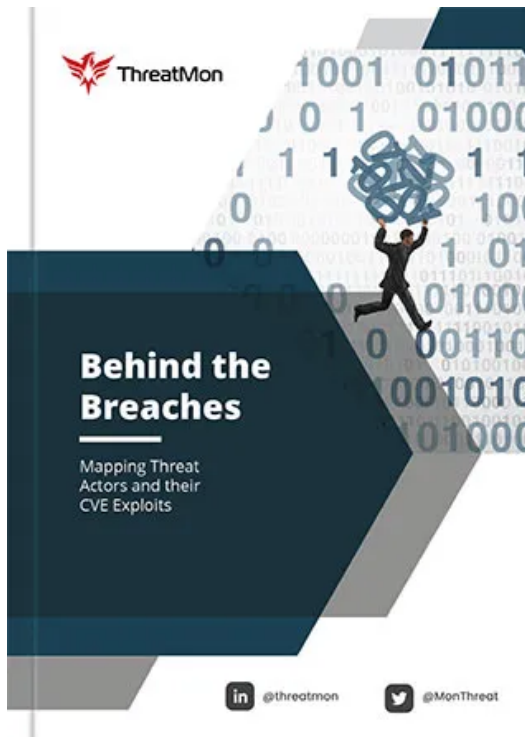
Ransomware Group Activity Report (26-02) September 2022

[Read the Report](#)



SwiftSlicer Wiper Malware Analysis Report 2023

[Read the Report](#)



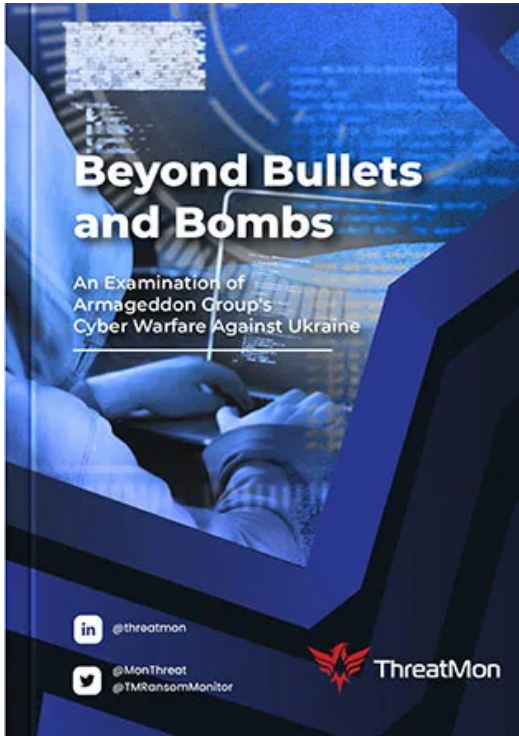
Behind the Breaches: Mapping Threat Actors and Their CVE Exploits

[Read the Report](#)



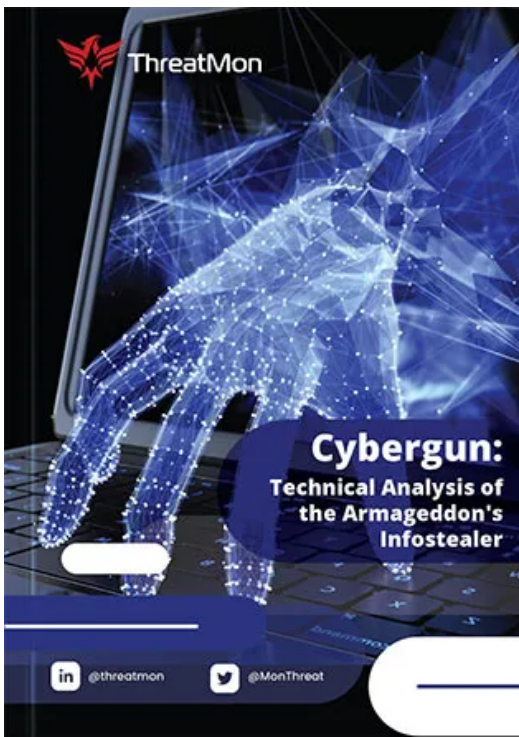
Threat Actors, Phishing Attacks and 2022 Phishing Preview

[Read the Report](#)



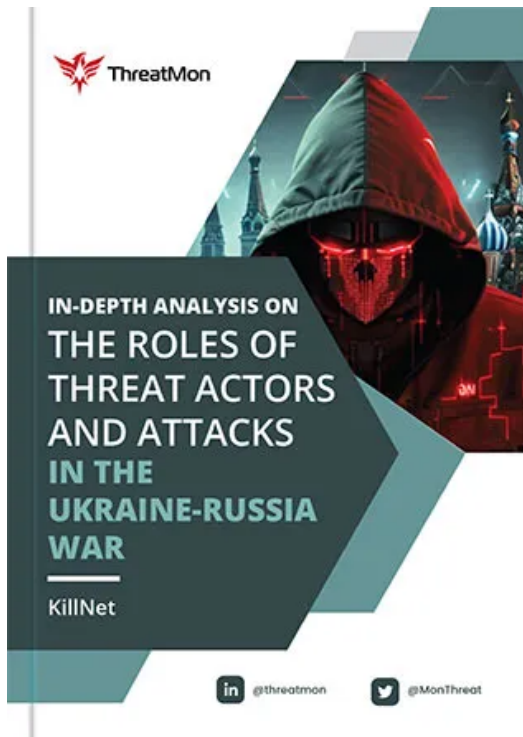
[Beyond Bullets and Bombs: An Examination of Armageddon Groups Cyber](#)

[Read the Report](#)



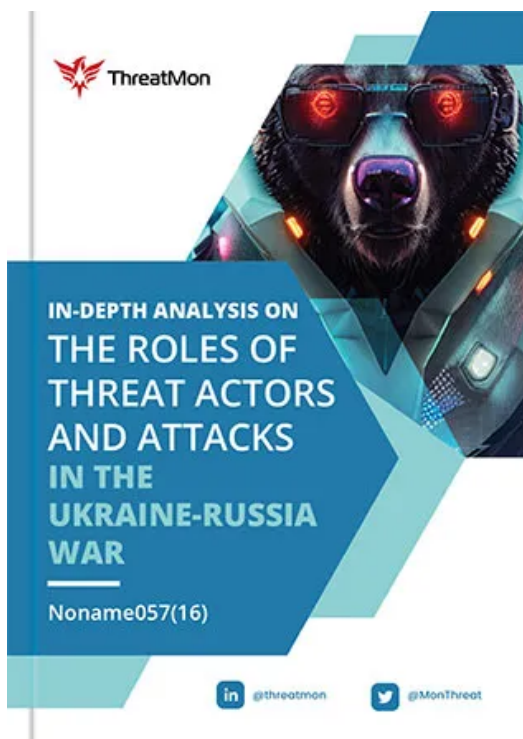
[Cybergun: Technical Analysis of the Armageddon's Infostealer](#)

[Read the Report](#)



[KillNet: In Depth Analysis on The Roles of Threat Actors and Attacks](#)

[Read the Report](#)



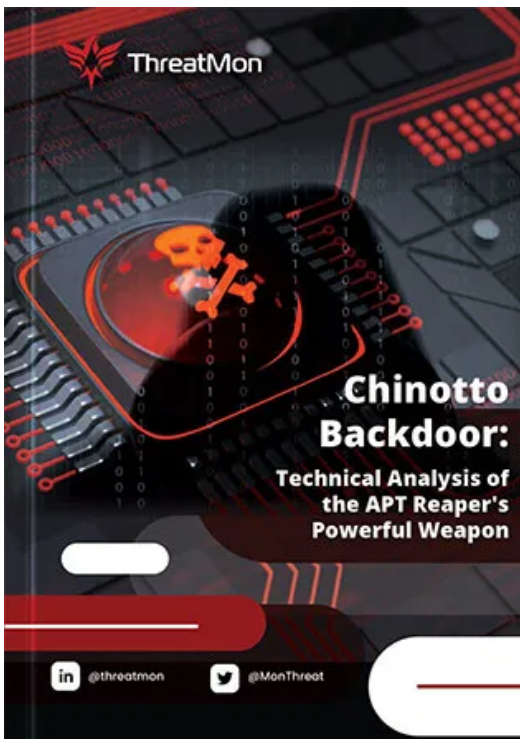
[Noname05716 In Depth Analysis on The Roles of Threat Actors and Attacks](#)

[Read the Report](#)



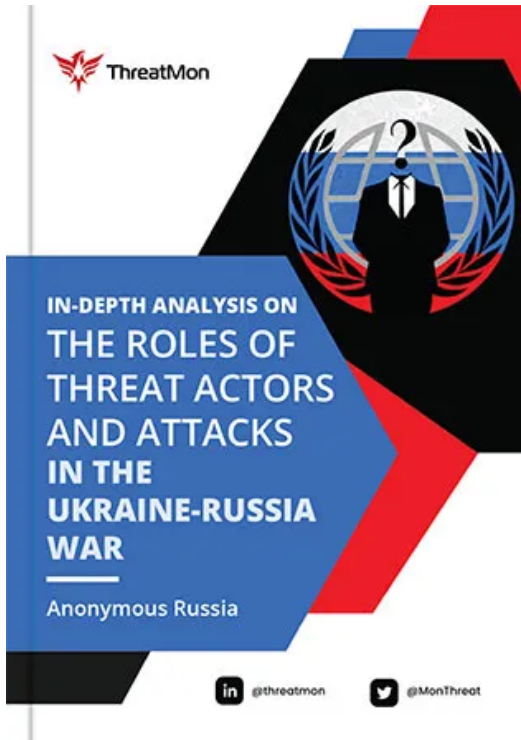
Report on Data Leaks Reported in Social Media

[Read the Report](#)



Chinotto Backdoor: Technical Analysis of the APT Reaper's Powerful Weapon

[Read the Report](#)



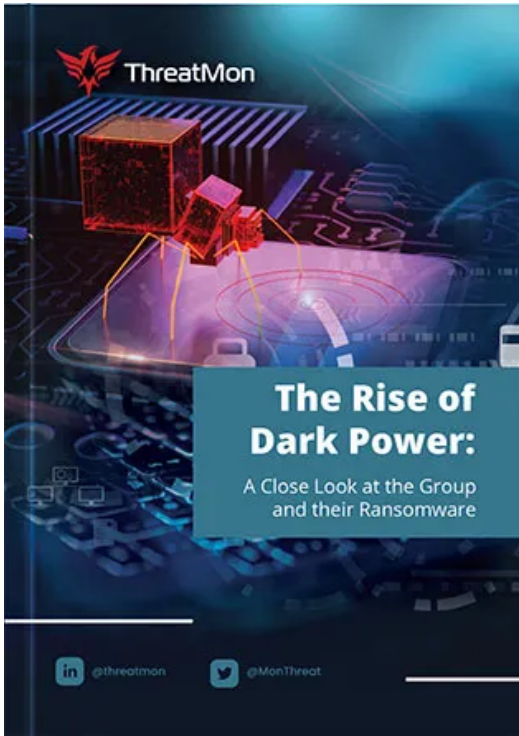
[Anonymous Russia In Depth Analysis on the Roles of Threat Actors](#)

[Read the Report](#)



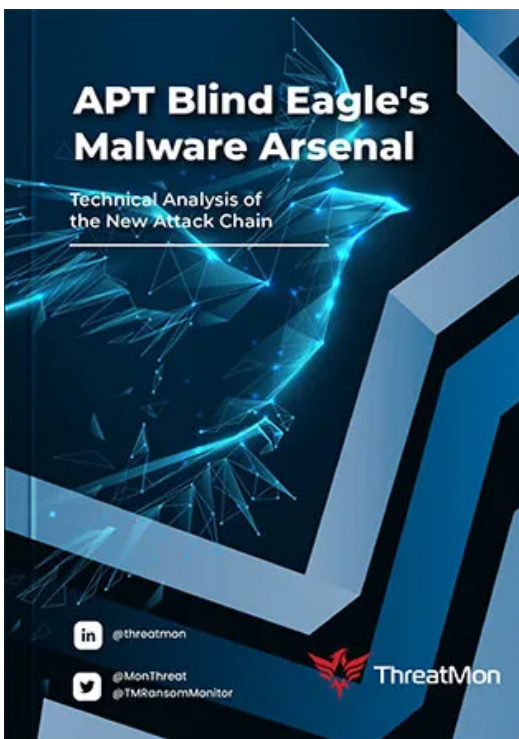
[IT Army of Ukraine: Analysis of Threat Actors In The Ukraine-Russia War](#)

[Read the Report](#)



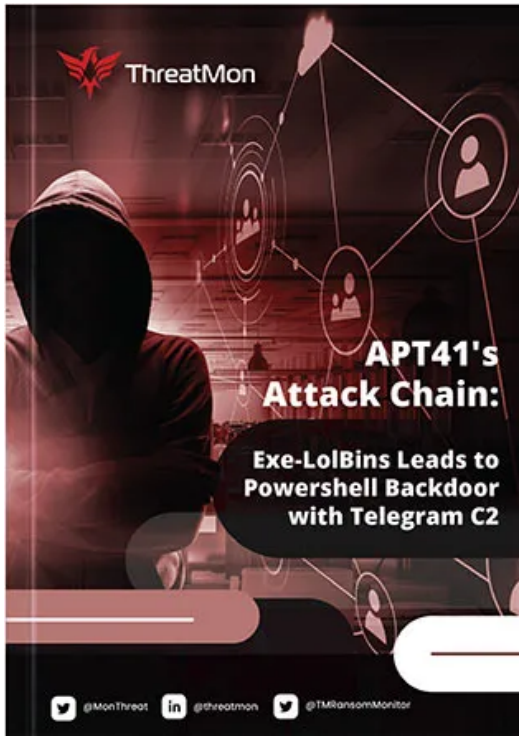
[The Rise of Dark Power: A Close Look at the Group and their Ransomware](#)

[Read the Report](#)



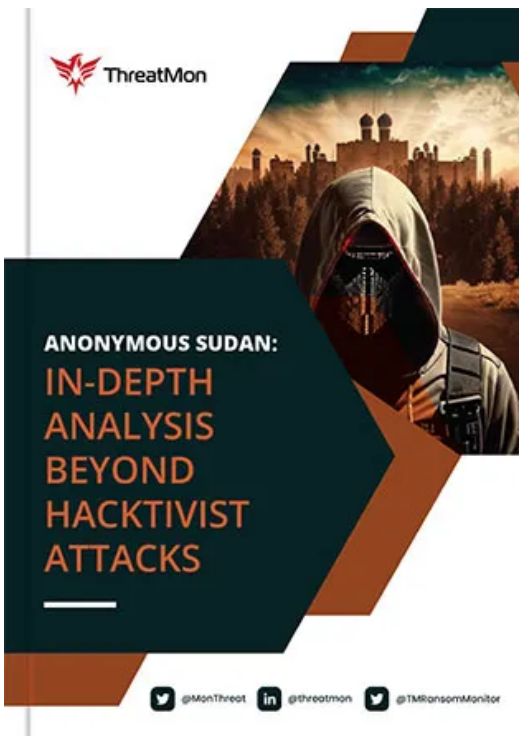
[APT Blind Eagles Malware Arsenal Technical Analysis](#)

[Read the Report](#)



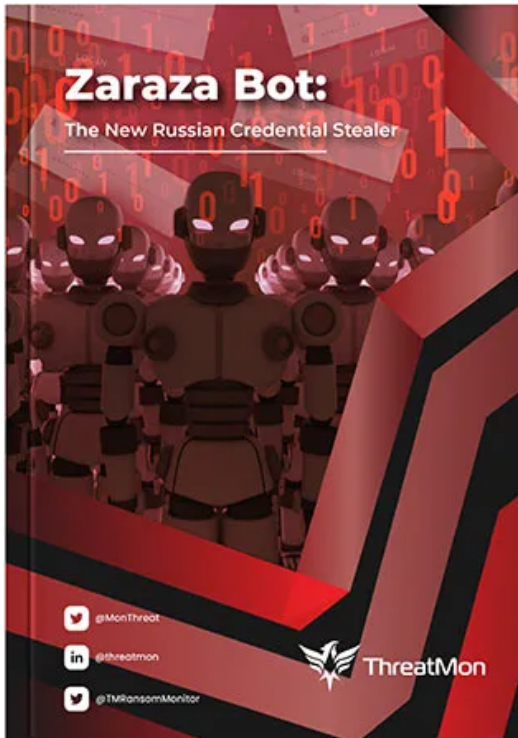
[APT41's Attack Chain: Exe-LolBins Leads to Powershell Backdoor with Telegram C2](#)

[Read the Report](#)



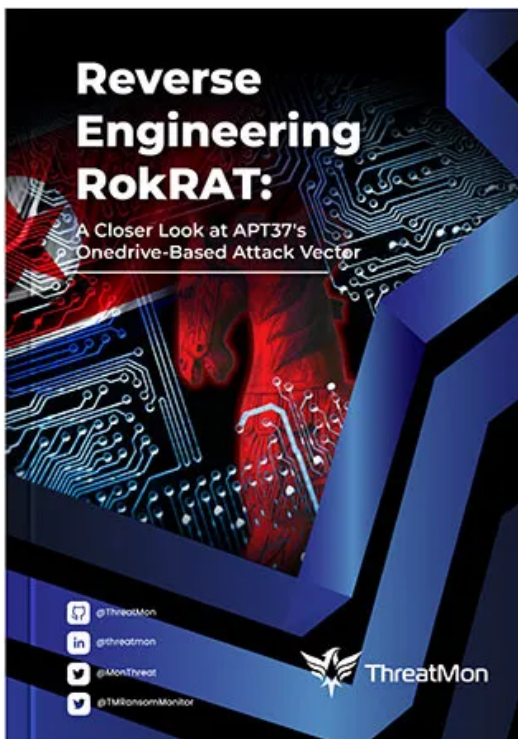
[Anonymous Sudan: In-Depth Analysis Beyond Hactivist Attacks](#)

[Read the Report](#)



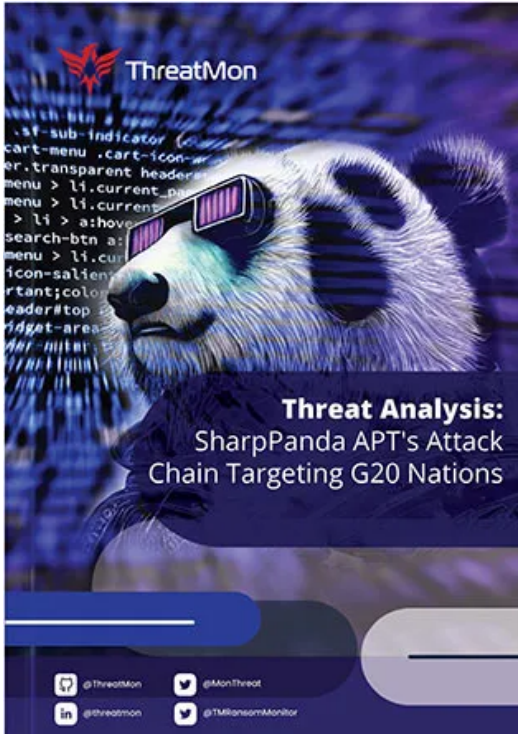
Zaraza Bot: The New Russian Credential Stealer

[Read the Report](#)



Reverse Engineering RokRAT: A Closer Look at APT37's Onedrive-Based Attack Vector

[Read the Report](#)



Threat Analysis: SharpPanda APT's Attack Chain Targeting G20 Nations

[Read the Report](#)



Cyber Threat Report: Analyzing Ransomware and Apt Attacks Targeting Türkiye May 2023

[Read the Report](#)

Start Your Free Trial Now!

The 30-day free trial of ThreatMon allows users to explore the product's security benefits. During this trial period, you can test Threat Intelligence data, detect threats to your organization and recommend security measures.

[Start Free Trial](#)