ICT DIVISION
FUTURE IS HERE

BANGLADESH COMPUTER COUNCIL
COMPUTER FOR EVERYTHING

BGD e-GOV CIRT

TLP:CLEAR

Emerging Threat of Info Stealer Malware in Bangladesh

[THIS PAGE IS INTENTIONALLY LEFT BLANK]

Sharing Indicator Protocol

TLP definitions (FIRST - https://www.first.org/tlp/)

Community: Under TLP, a *community* is a group who share common goals, practices, and informal trust relationships. A community can be as broad as all cybersecurity practitioners in a country (or in a sector or region).

Organization: Under TLP, an *organization* is a group who share a common affiliation by formal membership and are bound by common policies set by the organization. An organization can be as broad as all members of an information sharing organization, but rarely broader.

Clients: Under TLP, clients are those people or entities that receive cybersecurity services from an *organization*. Clients are by default included in TLP:AMBER so that the recipients may share information further downstream in order for clients to take action to protect themselves. For teams with national responsibility this definition includes stakeholders and constituents.

a. TLP:RED= For the eyes and ears of *individual* recipients only, no further disclosure. Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. Recipients may therefore not share TLP:RED information with anyone else. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting.

b. TLP:AMBER = Limited disclosure, recipients can only spread this on a need-to-know basis within their *organization* and its *clients*. Note that TLP:AMBER+STRICT restricts sharing to the *organization* only. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note: if the source wants to restrict sharing to the organization **only**, they must specify TLP:AMBER+STRICT.

c. TLP:GREEN = Limited disclosure, recipients can spread this within their community. Sources may use TLP:GREEN when information is useful to increase awareness within their wider community. Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP:GREEN information may not be shared outside of the community. Note: when "community" is not defined, assume the cybersecurity/defense community.

d. TLP:CLEAR = Recipients can spread this to the *world*, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

Table of Contents

TLP: CLEAR
Distribution: Public
Type of Threat: Emerging Threat of Info Stealer Malware in Bangladesh

Date: 18 January 2024

Executive Summary

The BGD e-GOV CIRT Cyber Threat Intelligence Unit has observed a significant increase in a particular type of malware called stealer malware in the cyberspace of Bangladesh. These carefully crafted covert programs are adept in discreetly obtaining sensitive data, including login passwords, personal information, and secret data, from targeted systems. In addition to putting financial resources at risk, this breach also compromises personal and professional secrets, giving hackers the ability to plan identity theft, financial fraud, or illegal account access. The malware that has been found, namely RedLine Stealer, META Stealer, RisePro, LummaC2, and Raccoon, increases the risk of digital security on several platforms. In order to combat the growing threat of cybersecurity, this report's conclusion emphasizes the urgent necessity for proactive cybersecurity measures.

Sources of Alert: *Threat intelligence research*

Research Conducted by: *Cyber Threat Intelligence Unit, BGD e-GOV CIRT*

Threat level: *High*

Associated Malware/ Tools/ Techniques: *RedLine Stealer, META Stealer, RisePro, LummaC2, Raccoon*

Attack Surface: *Windows, Android, IOS systems, Web Browser*

Brief overview of the info stealer malware

An information stealer, also known as an info stealer, operates as a Trojan designed with the explicit purpose of extracting valuable information from a targeted system. The primary focus of these malicious entities is the gathering of login credentials, such as usernames and passwords, which are subsequently transmitted to another system over the network. Keyloggers, a common subtype of information stealers, are specifically crafted to record user keystrokes, potentially exposing sensitive information in the process.[1] The sophistication of information stealers extends to the extraction of a broad spectrum of data, including account passwords, cookies, credit card details, and cryptocurrency wallet information. These pilfered details are meticulously organized into archives, commonly referred to as 'logs,' which are then uploaded back to the threat actors. These logs serve as a repository of stolen data, fueling subsequent cyberattacks or being traded on online marketplaces, with prices ranging from $1 to $150 depending on the victim.[2] This intricate process highlights the multifaceted nature of info stealers, posing a significant threat to the security of sensitive information in the digital landscape.

Stealer Malware works with several stages which are outlined below-

Stage	Description
Infection	Stealer malware enters systems via phishing emails, malicious websites, or software vulnerabilities, staying hidden to avoid detection.
Data Collection	Stealer malware's primary function is gathering sensitive data, including login credentials, stored passwords, and information from forms and documents.
Transmission	The collected data is stealthily transmitted to a remote server controlled by the attacker to evade security software detection.
Exploitation	Cybercriminals exploit the stolen information for unauthorized account access, financial fraud, or selling data on the dark web.
Persistence	Stealer malware seeks prolonged impact by establishing persistence on the infected system through backdoors, system settings modification, or other evasion techniques.

[1] https://www.trendmicro.com/vinfo/us/security/definition/Info-stealer

[2] https://www.bleepingcomputer.com/news/security/the-new-info-stealing-malware-operations-to-watch-out-for/

Info Stealer Malware in Bangladesh

In recent times, a concerning trend has emerged, impacting a multitude of individuals within different type of organization. Notably, there has been a surge in the compromise of both official and personal credentials, presenting a substantial threat to both affected individuals and the organizations they represent. The pervasiveness of these data theft incidents raises significant alarms for Bangladesh, elevating the susceptibility to ransomware attacks. In response to this growing threat, concerted efforts have been initiated to pinpoint the most prevalent malware stealers operating in Bangladesh, aiming to address the root causes of these security breaches and fortify the nation's cybersecurity posture.

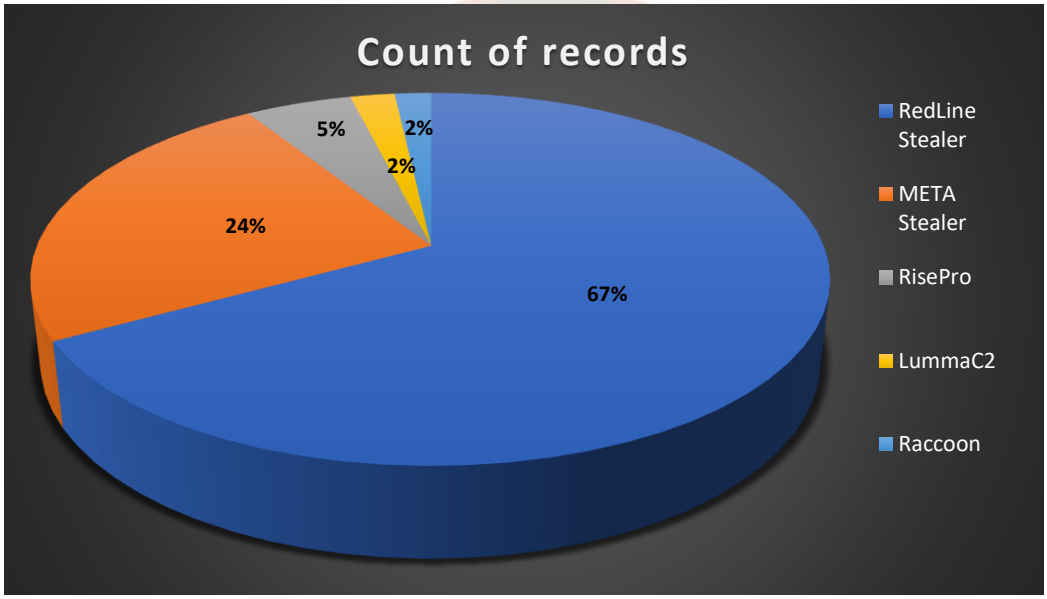


Fig: Stealer Malware records count (Percentage) in Bangladesh (recent time)

Top values malware	Count of records
RedLine Stealer	4,367
META Stealer	1,568
RisePro	333
LummaC2	139
Raccoon	114

RedLine Stealer

RedLine Stealer is a popular, cost-efficient info-stealing malware. It uses a customizable file-grabber to harvest sensitive data from various sources, enabling detailed device information collection. Operating as a remote access trojan, it facilitates ransomware attacks. Available through a malware-as-a-service model, it's easily accessible to cybercriminals. Initially surfacing in March 2020, it steals login details and sensitive data, often delivered through deceptive email campaigns posing as legitimate entities, like a fake coronavirus research company.

Signs of Infection	Description
Unauthorized Access	Indicates potential data theft through unauthorized login attempts and unrecognized account activity.
Impaired Security Software	Malware may disable or interfere with security software, exploiting anti-detection features.
Intrusive Pop-Up Ads	Increased pop-ups and online ads, even during non-browsing times, may signal attempts to trick users.
Unusual Network Activity	Suspicious connections or unexpected device activity suggest communication with command-and-control servers.
Slower Computer Performance	Infected computers may experience sluggishness due to resource consumption for malicious processes.
Unsolicited Browser Changes	Changes in browser settings, such as default search engine or homepage, may indicate malware activity.

Methods	Description
Phishing Emails	Utilizes emails with malicious attachments or links.
Compromised Websites	Exploits compromised sites through ads or typosquatting.
Legitimate-looking Applications	Disguises itself as genuine software or apps.

Targeted Data	Description
Login Credentials	Focuses on stealing sensitive data like login credentials, passwords, and credit card details.
Recent Emphasis	Recent focus on targeting crypto wallets for theft.
Browser Exploitation	Primarily attacks Chromium-based and Gecko-based browsers, exploiting browser extensions.
Various Applications	Targets applications such as email, Discord, Telegram, VPNs, and online banking for broader impact.

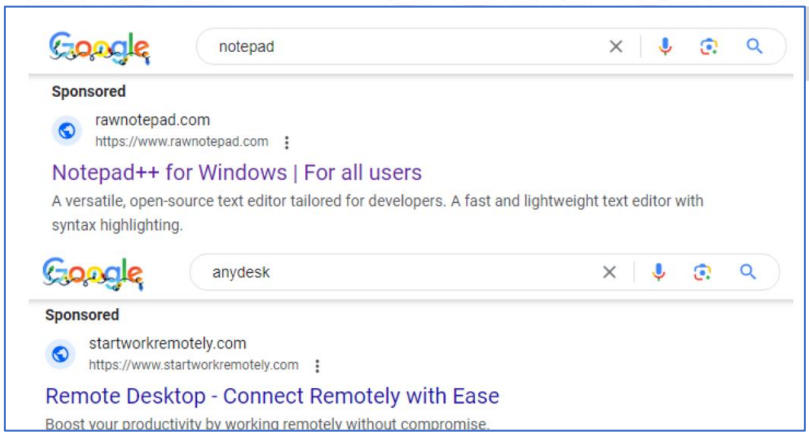
MetaStealer

MetaStealer, an information-stealing malware, has recently surfaced and garnered attention through a malspam campaign. Initially detected by KELA threat hunters, this infostealer seems to be either a variant or an advanced iteration of RedLine Stealer. The malspam campaign has raised awareness about MetaStealer, prompting scrutiny from security experts within the cyber threat landscape.

Key Points	Details
Discovery	Detected in a malspam campaign; initially identified by KELA threat hunters
Relationship	Believed to be a variant or advanced version of RedLine Stealer
Recent Observations	Malicious ads observed delivering MetaStealer payload in the past week
Author Announcement	In early December, the malware authors announced plans to release an improved version
Impact	Raised awareness and prompted scrutiny from security experts in the cyber threat landscape

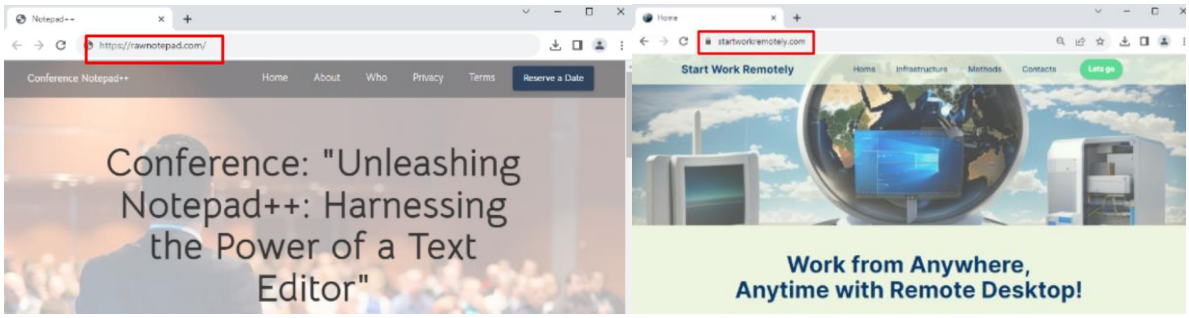
MalwareBytes.com has informed about **MetaStealer malvertising campaigns** with new payloads in November and December. [3]

In Google searches for for Notepad++ and AnyDesk they have found two different ads

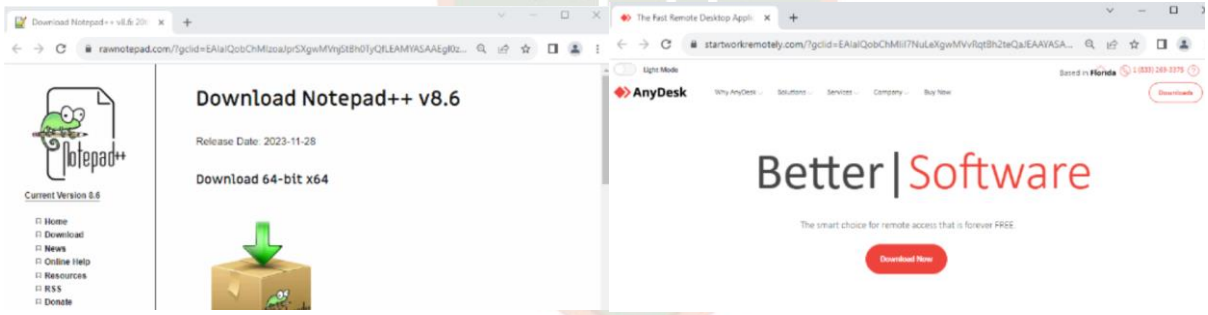


[3] https://www.malwarebytes.com/blog/threat-intelligence/2023/12/new-metastealer-malvertising-campaigns

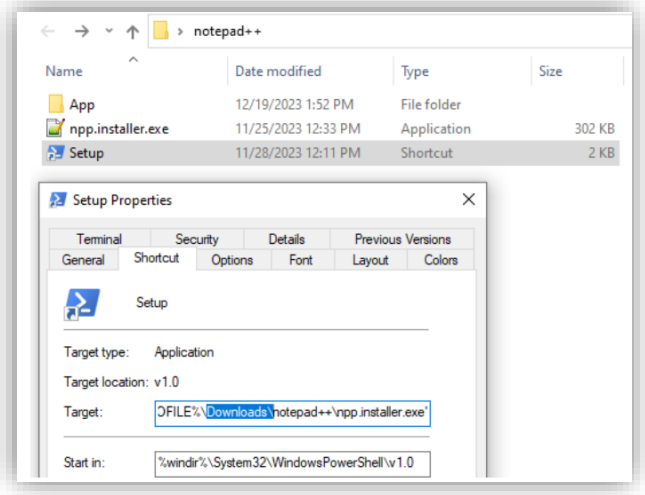
Two domains have been setup as both decoy and landing pages. If anyone browse to those sites directly, they would see content that looks like it was generated automatically.



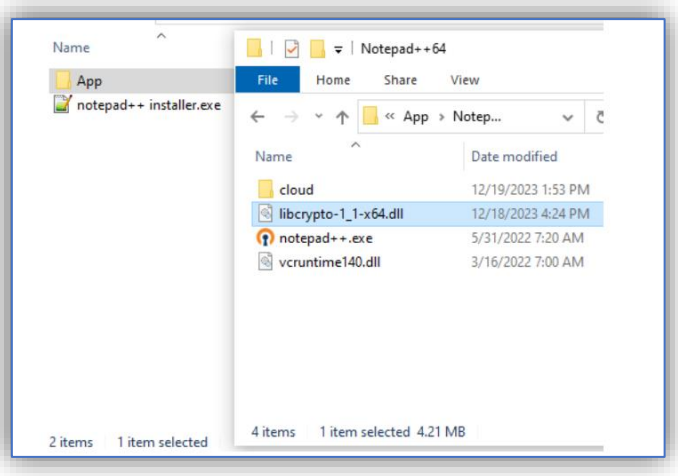
However, users that clicked on the ads and met the selection criteria will get a malicious landing page and a download link.



The November payload contained a shortcut launching PowerShell that used a hardcoded path to the Downloads folder (would fail if the file was extracted in another directory):



The December campaign got rid of the PowerShell and the malicious DLL was recompiled:



RisePro

RisePro's capabilities and potential consequences highlight the need for robust cybersecurity measures to prevent its spread and protect against the misuse of stolen information.

Characteristics	Description
Similarity with Vidar	RisePro shares similarities with Vidar, written in C++ programming language.
Distribution Method	Spread through a malware downloader called PrivateLoader.
Sales Channel	Creators are selling RisePro on Telegram.

Functionality	Description
Spreading Method	Spread through downloaders like win.privateloader.
Data Theft	Can steal credit card information, passwords, and personal data.
Additional Capabilities	Potentially extracts IP addresses, browsing history, crypto wallets, messenger messages, screenshots.

Potential Consequences	Description
Misuse of Extracted Information	Information may be used for hijacking online accounts, identity theft, fraudulent transactions, etc.
Exploitation of Stolen Accounts	Stolen accounts may be used for delivering malware, scams, and other malicious activities.

Exfiltration	Description
Data Format	Stolen data exfiltrated in the form of logs.
Market Presence	Logs uploaded to shadow markets and sold to third parties.

Lumma Stealer (LummaC2)

Lumma Stealer, a recently emerged and unfamiliar malware, is categorized as a stealer. Named LummaC2, this malicious program functions by extracting sensitive information from compromised devices and installing applications.

Aspect	Details
Characteristics	Operates by stealing sensitive information and installing applications
Discovery	Discovered by our dark web team, found being sold on underground forums
Size	Approximately 150-200 KB
Compatibility	Can affect operating systems from Windows 7 to Windows 11
Distribution	Infected email attachments, malicious online advertisements, social engineering, software 'cracks'
Symptoms	Designed to stealthily infiltrate the victim's computer; no specific symptoms are clearly visible on an infected machine
Potential Damage	Stolen passwords and banking information, identity theft, victim's computer added to a botnet
Privacy and Financial Risk	Presence of LummaC2 on devices can result in severe privacy issues, significant financial losses, and identity theft
Mitigation	Implementing robust cybersecurity measures, avoiding suspicious email attachments, being cautious with online activities, using legitimate software sources, and keeping systems updated

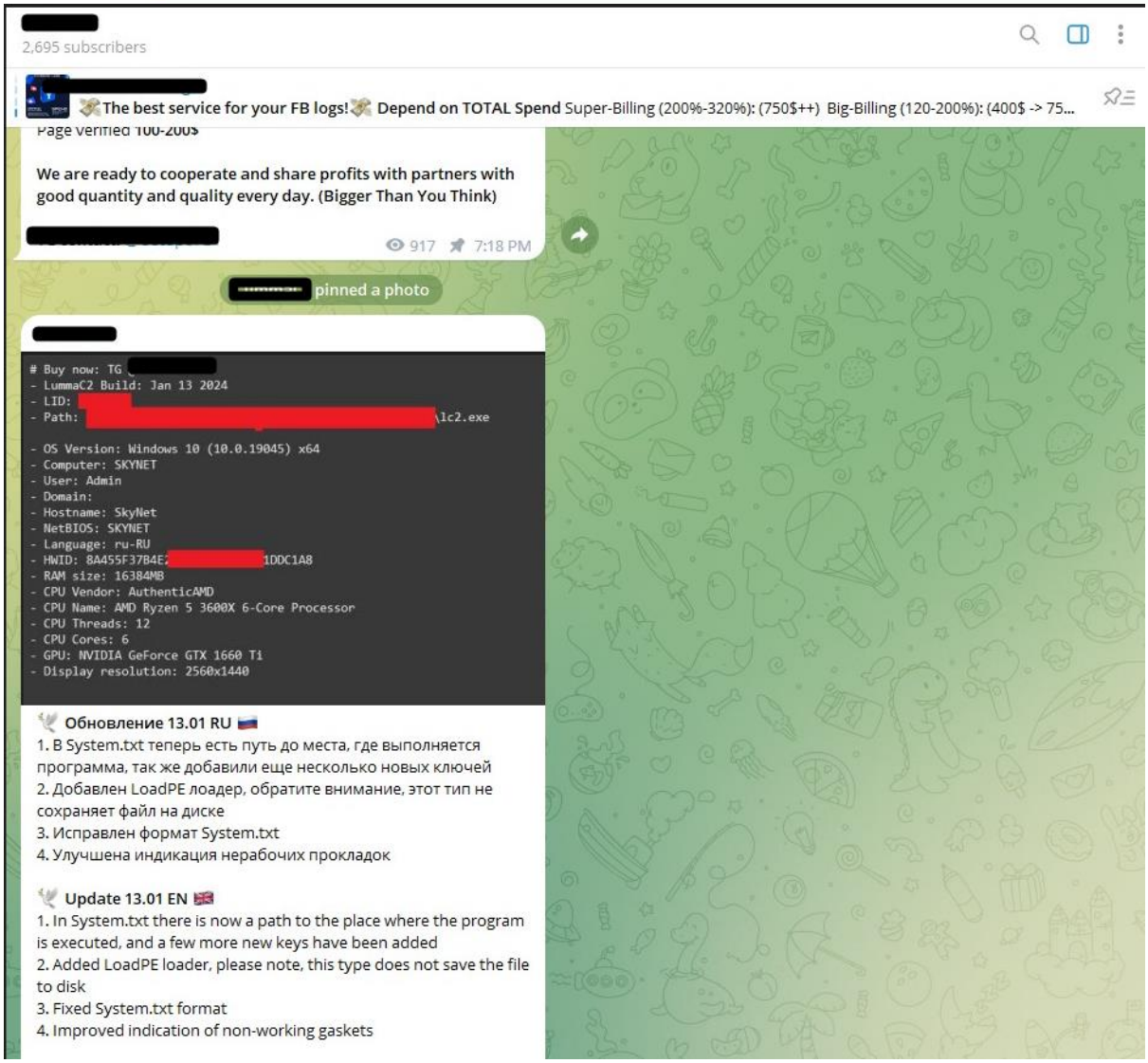


Fig: *Lumma Stealer (LummaC2) Telegram Channel*

Raccoon

Raccoon, also recognized as Mohazo and Racealer, is an information-stealing malware employed by threat actors to extract sensitive data from compromised devices. This modern malware, initially identified in 2019, operates with basic info-stealing functions similar to RedLine and lacks inherent antivirus protection. Notably, the malware's analysis is not complicated by additional features. However, Raccoon developers recommend utilizing a third-party crypter for enhanced functionality.

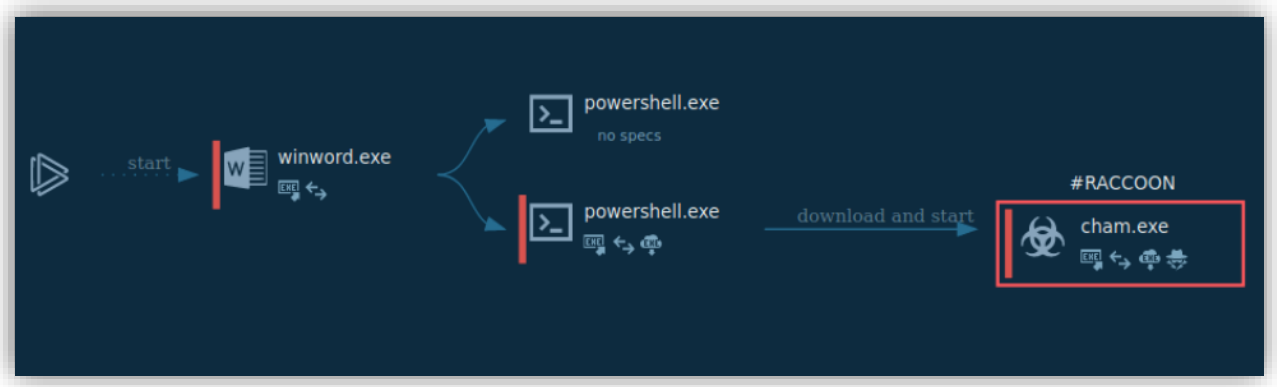


Fig: *Execution process of Raccoon (ANY.RUN)*[4]

Aspect	Details
Malware Other Name	Mohazo, Racealer
First Sighted	2019
Characteristics	Basic info stealer functions (e.g., RedLine), lacks antivirus protection, suggests the use of a third-party crypter
Execution Process	1. Enters the system, downloads additional modules (DLL dependencies)
	2. Steals information from browsers and the system
	3. Stores stolen data in an archive file
	4. Sends the file to the C2 server
	5. Some versions may delete themselves after execution
Distribution Channels	- Browsers
	- Exploit kits (mainly Fallout exploit kit)
	- Microsoft Office document attachments in mail spam campaigns
	- Dropbox account with malware stored in a .IMG file (social engineering used to trick victims into opening a malicious URL)
	- Bundled malware with legitimate software downloaded from suspicious websites
Impact	Not very technically advanced but gained attention in the underground community in 2019
	Available as a service for $200 per month
	Equipped with everything necessary for a malware attack
	Support provided by the malware team

[4] https://any.run/malware-trends/raccoon#:~:text=Raccoon%20stealer%20malware%20is%20distributed,mainly%20the%20Fallout%20exploit%20kit.

Prevention measures

1. **Security Software**: Install and regularly update reputable antivirus and anti-malware software.
2. **Regular Updates**: Keep operating systems, software, and applications up-to-date with the latest security patches.
3. **Email Awareness**: Exercise caution with email attachments and links. Use email filtering and enable two-factor authentication.
4. **Safe Browsing Practices**: Avoid clicking on suspicious links or visiting untrustworthy websites. Use secure and updated web browsers.
5. **Strong Passwords**: Use strong, unique passwords for all accounts. Consider using a password manager.
6. **Firewall Protection**: Enable firewalls on both personal devices and organizational networks.
7. **Backup Data**: Regularly back up important data to an external and secure location.
8. **Secure Wi-Fi**: Use strong passwords for Wi-Fi networks. Avoid public Wi-Fi for sensitive transactions.
9. **Application Updates**: Keep apps updated to patch security vulnerabilities.
10. **Download Wisely**: Only download software from official and reputable sources.
11. **Access Controls**: Enforce the principle of least privilege in both personal and organizational settings.
12. **Two-Factor Authentication (2FA)**: Enable 2FA wherever available for an added layer of security.
13. **Be Skeptical**: Exercise caution with unexpected requests for personal or organizational information. Verify the legitimacy of requests before responding.
14. **Social Media Privacy Settings**: Review and adjust privacy settings on personal and organizational social media accounts.
15. **Regular Scans**: Perform regular malware scans on both personal and organizational devices
16. **Employee Training (for Organizations)**: Conduct regular security awareness training for employees.
17. **Incident Response Plan (for Organizations)**: Develop and regularly update an incident response plan for organizations.
18. **Network Security (for Organizations)**: Implement robust network security measures and conduct regular audits.

By adopting these combined measures, both organizations and personal users can strengthen their defenses against info stealer malware and enhance overall cybersecurity. Regularly review and adapt security protocols to address emerging threats.

Indicators of Compromise (IoCs)

In this report, we have incorporated the most frequently occurring Indicators of Compromise (IoCs) identified recently. It's essential to note that threat actors often swiftly alter their domains, IP addresses, URIs, and other elements.

RedLine Stealer:

Some Connected Domains to RedLine Stealer:

IoC Type Domain	Content Type
nostr[.]software	"Software" + "Crack"
revosoftware[.]company	"Software" + "Crack"
reversed[.]software	"Software" + "Crack"
carbonsparksoftware[.]blog	"Software" + "Crack"
carbonsparksoftware[.]cloud	"Software" + "Crack"
crackedbedwars[.]com	"Software" + "Crack"
pccracked[.]org	"Software" + "Crack"
soft-warecrack[.]store	"Software" + "Crack"
crack-soft-ware[.]store	"Software" + "Crack"
crackedprograms[.]co.uk	"Software" + "Crack"
freesoftwaredownload[.]net	"Free" + "Ware"
freewaregadgets[.]com	"Free" + "Ware"
freesoftware[.]system[.]com	"Free" + "Ware"
freesoftwareapk[.]com	"Free" + "Ware"
designsoftwarefree[.]com	"Software" + "App"
codeapp[.]software	"Software" + "App"
applicationsoftwaredevelopment[.]com	"Software" + "App"
vpmapping[.]software	"Software" + "App"
bootstrappedsoftware[.]partners	"Software" + "App"
softwareapp[.]online	"Software" + "App"

IPv4 Addresses: (Recent)

193[.]233.20.13

176[.]113.115.17

File hashes:

3854f7f1fcb2dd48a235e69be3a7618bec6faf676c8af4fc3ad1d253dc653591

MetaStealer:

File hashes:

46f1a4c_browsing77896f38a387f785b2af535f8c29d40a105b63a259d295cb14d36a561XxX1Elf·elf
MD5: 11d211ce3fa615ce35bff30fa37e9251
SHA1: eba816d7dc084d5702ad5d222c9b6429755b25fd
SHA256: 46f1a4c77896f38a387f785b2af535f8c29d40a105b63a259d295cb14d36a561

46f1a4c_edr77896f38a387f785b2af535f8c29d40a105b63a259d295cb14d36a561XxX1Elf·elf
MD5: 11d211ce3fa615ce35bff30fa37e9251
SHA1: eba816d7dc084d5702ad5d222c9b6429755b25fd
SHA256: 46f1a4c77896f38a387f785b2af535f8c29d40a105b63a259d295cb14d36a561

http://79·124·59[·]178

Lumma Stealer (LummaC2):

IPv4 Addresses: (Lumma C2 Infrastructure)

144.76.173[.]247
45.9.74[.]78
77.73.134[.]68
82.117.255[.]127
82.117.255[.]80
82.118.23[.]50

URI

/c2sock (Lumma - C2 POST Request)

User agent

TeslaBrowser/5.5 (Lumma C2 POST Request)

URL

Walkinglate[.]com

server3.allstatsin[.]ru

dayfarrichjwclik[.]fun

politefrightenpowoa[.]pw

cakecoldsplurgrewe[.]pw

RisePro:

IPv4 Addresses:

168[.]100[.]10[.]122

5[.]42[.]79[.]238

95[.]214[.]25[.]231

45[.]15[.]159[.]248

185[.]173[.]38[.]198

194[.]169[.]175[.]128

79[.]110[.]49[.]141

38[.]47[.]220[.]202

194[.]169[.]175[.]128

Raccoon:

IPv4 Addresses: (Command and Control Server)

34.90.238[.]61

34.77.205[.]80

35.189.105[.]242

34.89.185[.]248

31.31.198[.]12

34.77.164[.]226

35.198.183[.]218