THE UNITED REPUBLIC OF TANZANIA
TANZANIA COMMUNICATIONS REGULATORY AUTHORITY
ISO9001:2015 CERTIFIED

SECURITY ADVISORY

THE RISE OF INFORMATION STEALER MALWARE CAMPAIGNS

1.0. INTRODUCTION

Tanzania Computer Emergency Response Team (TZ-CERT) has observed a significant rise in malware campaigns leveraging information stealer malware such as ***LummaC2***, ***Nexus Stealc***, ***Vidar***, etc. These malware families have the capability to harvest information including user credentials, session cookies, browser history, crypto wallets, user files etc. from compromised device and transmit them to a remote threat actor, thereby posing a growing threat to organizations and individuals.

Information stealer malware is increasingly being used in initial access campaigns and as part of cybercriminal supply chains. The stolen user credentials particularly those granting access to internet-facing services or privileged accounts are exploited to gain initial footholds within corporate systems and data. This access can lead to further compromises and attacks such as business email compromise (BEC), ransomware deployment, social engineering (SE), financial fraud and many other suspicious activities.

Pursuant to section 6(i) and 6(s) of the **Electronic and Postal Communications (Computer Emergency Response Team) Regulations 2018**, TZ-CERT issues this advisory to notify institutions and the general public of the threat and

This document is marked as TLP: CLEAR. Recipients can spread this to the world; there is no limit on disclosure. For more information, visit the Traffic Light Protocol (TLP) definition

recommend appropriate security measures to facilitate safeguard of data and systems.

2.0. IMPACTS

The possible impacts of these malware infections include:

2.1. **Theft of user credentials**, including usernames and passwords, authentication tokens, cryptocurrency wallets, and associated keys which results in unauthorized access to sensitive personal and/or corporate systems such as online banking platforms, email accounts, cloud services, and social media profiles.

2.2. **Identity theft and Impersonation**, where attackers use stolen credentials and other personal information to pose as the victim. This allows them to commit fraud, access systems and/or carry out malicious activities under the victim's identity.

2.3. **Data breach**, the successful deployment of information stealer malware may lead to unauthorized acquisition and widespread exposure of data/information.

2.4. **Reputation damage**, the exfiltrated data is often sold on underground or dark web marketplaces significantly increasing the risk of reputational damage to both individuals and organizations, but also can erode trust to stakeholders.

2.5. **Facilitation of more sophisticated attacks against people, systems and networks**, stolen credentials are often exploited to facilitate follow-on attacks such as ransomware deployment, social engineering (SE) and lateral movement across networks. Threat actors may also employ Living off the Land (LoL) techniques leveraging legitimate system tools and processes to evade detection, maintain persistence and deepen their infiltration without raising alerts. These tactics significantly amplify the impact of the initial compromise.

This document is marked as TLP: CLEAR. Recipients can spread this to the world; there is no limit on disclosure. For more information, visit the Traffic Light Protocol (TLP) definition

3.0. TECHNICAL OVERVIEW

3.1. Information stealer malware

(i) Overview

Information stealer malware, also known as **info stealers**, are a type of malware designed to collect information from a victim's device. This can include usernames and passwords, credit card details, cryptocurrency wallets, local files, and browser data, including cookies, user history and autofill form details.

(ii) Information Stealer Ecosystem

Stage 1: Acquire the malware

Info stealers are mostly offered on cybercriminal marketplaces as Malware as a Service (MaaS) or Stealer-as-a-Service or sold as source code. MaaS refers to a business model under which cybercriminals provide access to malicious software and related infrastructure for a fee. MaaS is a malicious variation of the Software-as-a-Service (SaaS) model, and also forms part of the Cybercrime-as-a-Service (CaaS) model. This model allows individuals without extensive technical skills to distribute malware and collect stolen information for use in cyberattacks.

The subscription to MaaS allows cybercriminals access to the dashboard that facilitates the creation of info stealer malware, organizes stolen data, and tracks the number of compromised systems. MaaS may also feature tools and technical support to evade detection by antivirus software, which attracts and retains subscribers. Many info stealers can delete themselves from the victim's device after performing data exfiltration.

Stage 2: Distribution

This document is marked as TLP: CLEAR. Recipients can spread this to the world; there is no limit on disclosure. For more information, visit the Traffic Light Protocol (TLP) definition

Traffic distributors, or traffers, are cybercriminals specialized in the distribution of information stealers and the collection of data from infected devices. Traffers facilitate the dissemination of information stealers as part of broad campaigns by directing victims to malicious links.

Traffers can deploy info stealers to victim devices using a wide range of techniques, including:

(i) **Botnets**: Networks of compromised computer systems controlled by cybercriminals to perform malicious activities such as distribution of phishing messages or malware.

(ii) **Phishing:** attempts to gain sensitive information by deception, including via emails or direct messages on social media, forums and messaging apps, which are common distribution methods that have lowered the barrier to entry for cybercriminals.

(iii) **Malicious search results:** Cybercriminals use Search Engine Optimization (SEO) poisoning techniques that direct targets to malicious websites that serving malware disguised as legitimate software or other popular content. Unsuspecting users who click on these links may unknowingly download info stealers and other form of malwares.

(iv) **Malvertising:** A technique where harmful code injected into legitimate online advertisements, to distribute malware. When users interact with or simply view these ads, the code may redirect them to malicious sites or silently initiate malware download including info stealer. Social media posts are another way to lure users into downloading malware.

This document is marked as TLP: CLEAR. Recipients can spread this to the world; there is no limit on disclosure. For more information, visit the Traffic Light Protocol (TLP) definition

(v) **Malicious software updates:** Disguise malware as legitimate updates for popular software or operating systems to trick users into installing them.

(vi) **Cracked or pirated software:** Cracked software refers to illegally modified applications that bypass licensing or activation requirements. Cybercriminals often bundle these pirated versions with malicious payloads, such as info stealer malware and they are normally downloaded from untrustworthy sites. Victims lured by the promise of free access to premium software unknowingly allowing the malware to infect their systems. This method is particular effective since it targets users who are less likely to report infections due to the illegal nature of the software they are using.

Stage 3: Data harvesting

Once an info stealer executes on the victim's device, it commences collecting data from the compromised device. In cases where info stealers are part of a botnet, cybercriminals remotely control the compromised device by sending configuration commands to activate additional capabilities or deliver other forms of malware. Apart from stealing user credentials (*username & password, authentication tokens, PINs, etc.*), in general info stealers are capable of collecting many other information to include chat logs from messaging apps, system information, user documents and files, web history and autofill forms, credit card details.

Stage 4: Data aggregation and monetisation

Info stealers are configured to exfiltrate victim information, common referred to as 'logs' to malicious Command-and-Control (C2) servers. In general, info stealers leverage popular messaging apps, such as Telegram and Discord, to share a feed of logs with cybercriminals. Specialized

This document is marked as TLP: CLEAR. Recipients can spread this to the world; there is no limit on disclosure. For more information, visit the Traffic Light Protocol (TLP) definition

marketplaces exist on Telegram and across the dark web for the sale and trade of logs. Cybercriminals monetize the logs in various ways, including:

(i) Selling logs on criminal marketplaces, including to initial access brokers;
(ii) Exploiting the victim directly, via identity theft and extortion;
(iii) Leveraging the information for initial access into corporate networks for ransomware activity.

3.2. Top Variant observed

3.2.1. LummaC2

LummaC2 (also known as Lumma Stealer) is a commercially distributed Stealer-as-a-Service that targets browsers, email clients, VPN credentials, cryptocurrency wallets, and even Two Factor Authentication (2FA) plugins.

It utilizes a complex infection chain, primarily leveraging techniques such as Dynamic Link Library (DLL) side loading, malicious payload injection into legitimate software overlays to stealthily execute harmful codes. Social Engineering (SE) tactics through fake CAPTCHA verifications to lure users into executing the malware via PowerShell and Microsoft HTML Application (MSHTA) commands. It supports exfiltration via multiple protocols and utilizes dynamic command-and-control (C2) domains to evade detection and maintain resilient communication with attacker.

3.2.2. RisePro Stealer

RisePro is a sophisticated information-stealing malware first observed in late 2022, primarily distributed via a pay-per-install (**PPI**) service called **PrivateLoader**. It targets credentials and sensitive information from infected systems and has been linked to extensive

This document is marked as TLP: CLEAR. Recipients can spread this to the world; there is no limit on disclosure. For more information, visit the Traffic Light Protocol (TLP) definition

campaigns utilizing various distribution methods, including phishing pages posing as legitimate software updates.

The malware employs advanced obfuscation techniques and communicates with command-and-control (C2) servers using custom TCP protocols, making it challenging to detect and analyze.

3.2.3. Stealc

Stealc is a sophisticated information-stealing malware that has recently evolved, with its second version, StealC v2, released in early **April 2025**.

This malware, primarily targeting web browser credentials, files, and cryptocurrency wallets, it is known for its robust capabilities such as server-side decryption for Google Chrome credentials and enhanced evasion tactics. It gains initial access through exploitation of vulnerabilities like **CVE-2025-26633** in **Microsoft Management Console (MMC)**, using malicious provisioning packages disguised as legitimate installer files.

3.2.4. Vidar

Vidar is a sophisticated info stealer malware observed extensively from late 2023 to early 2025, primarily targeting browser-stored credentials and cryptocurrency wallet data. It connects to known command-and-control (C2) domains like *ikores[.]sbs* and utilizes various techniques for initial access, including social engineering tactics such as fake reCAPTCHA prompts or malicious software distribution through platforms like GitHub and Steam.

4.0. INDICATORS OF COMPROMISE

The following are possible indicators of compromise (IOC) associated with the top four (4) info stealer malware.

This document is marked as TLP: CLEAR. Recipients can spread this to the world; there is no limit on disclosure. For more information, visit the Traffic Light Protocol (TLP) definition

4.1. Lumma Stealer (LummaC2)

Hashes (SHA256)

(i) a1b3164e0327a2ee19171debc62d31c5665f81923589e6424cea08a801d1df48
(ii) 614125ef1289a65554422ef38cdc8d899e7c439396f86aa1f9d7b0ac46ed20ae
(iii) 0e5a768a611a4d0ed7cb984b2ee790ad419c6ce0be68c341a2d4f64c531d8122
(iv) 748924e97a23601ddd8ea505b5601bbc8c7687528b921a8a6d22b5d4f9f4b41f
(v) 8aecd82f1657ec863032e6b326d0c91a7599200a0ef9ba4bfe88a9da5256de8c

Command and Control (C2)

(i) hxxps[:]//mediaflowq[.]run/aeui
(ii) hxxps[:]//brandihx[.]run/lowp
(iii) hxxps[:]//techguidet[.]digital/apdo
(iv) hxxps[:]//btcgeared[.]live/lbak
(v) hxxps[:]//datamanipy[.]run/bent
(vi) hxxps[:]//techsyncq[.]run/riid

4.2. RisePro Stealer

Hashes (SHA256)

(i) e711519f57201d4a464f9af8109131173dd9f1ba9cad7fe94a6a1711037ba23f
(ii) 6e485e3592c5da768b22325c418370524d8933e8204346427b77095aa13560d4
(iii) 8c318c16c714156084fdcfc074c61b4be3b8b6386bfb2bf4399d6da551d2d0c1
(iv) f5a3ab895da82773a180cadb6ac0f8e0dfc832c855c1cd533082fa37ab8d49b1
(v) 1edd479d188e5dde25addd4864aa922ee81f95a397e0e586eafdd8cb694237da

Command and Control (C2)

(i) 92.119.114.169:50505
(ii) 77.105.164.24:50505

This document is marked as TLP: CLEAR. Recipients can spread this to the world; there is no limit on disclosure. For more information, visit the Traffic Light Protocol (TLP) definition

(iii) 77.105.132.27:8081

(iv) 77.91.77.180:50500

(v) 77.91.77.180:8081

(vi) 147.45.47.176:8081

(vii) 3.36.173.8:50500

4.3. Stealc

Hashes (SHA256)

(i) d5355c5bddacdf20377d6cc75766ccb25199724c382be1b9b29d4adb0ee97972

(ii) 629d83659df3e1aaa04b6c296a3cf8e2248033e9d1ff422e350453d77cb2a5f0

(iii) 9efb3b655d41be4ed8b3fba0b7f34f90cc7861da036cd3e3eff59f4fba0ff805

(iv) 315672212df531419373584a2825abf74212faa2e9c5cacb9063dce0d6d0ef45

(v) a26095cf5fff9a7ec04c3fd3fb60372f38f3dc300addf4983e0ce4f7490ef7b2

Command and Control (C2)

(i) 193.24.123[.]86:443

(ii) serholders.pro

(iii) statisticapp.asia

(iv) miauwonderland[.]help

(v) wallsekker[.]store

(vi) hdkxbax[.]click

4.4. Vidar

Hashes (SHA256)

(i) f9585c2d9b0b20fa6ca2e33d9d2c6fe21a0effa36ca818e061e2bdf570ae06bc

(ii) 1607f4c2da90691381b6304286e6c95e300495ff3cc2ca22c02dc7a3bc128999

(iii) 23076d148144e0ca92d69bf92edd6cd8b4cc99749c3d50f3af0ab05c58a2efe7

(iv) 33a1cd793d9966e4f9bd7e5d5a3416725ffd05849ede6e30e415f5c099f4382e

This document is marked as TLP: CLEAR. Recipients can spread this to the world; there is no limit on disclosure. For more information, visit the Traffic Light Protocol (TLP) definition

(v) 26790a672c3c832a6b0365fd01cc81b2f91d6112891a7d30077ada26f1625173

Command and Control (C2)

(i) 5.75.210[.]140:443
(ii) 32.aa.4t[.]com
(iii) hxxps://32.aa.4t[.]com/
(iv) hxxps://5.75.210.140/
(v) hxxps://72.aa.4t[.]com/
(vi) 78.46.233.21:443
(vii) 5.75.211.124:443
(viii) 157.180.94.222[:]443
(ix) s.p.formaxprime[.]co.uk
(x) hokagehuyaki[.]space

A complete list of detailed IOCs is available on our website and can be downloaded from the following link:

✓ https://www.tzcert.go.tz/publication/TZCERT-DET-25-0012-info-stealer-malware-additional-iocs

5.0. DETECTION RULES

To support network defenders and threat analysts in identifying infections and related activity, detection rules specific to the aforementioned stealer malware variants are available for download. These rules are curated from trusted sources and cover the following formats:

- **Snort Rules –** for network intrusion detection**.**
- **YARA Rules –** for malware sample detection and memory scanning.
- **Sigma Rules –** for event log analysis and SIEM systems**.**

You can download these detection rules at the following link:

This document is marked as TLP: CLEAR. Recipients can spread this to the world; there is no limit on disclosure. For more information, visit the Traffic Light Protocol (TLP) definition

Malware Variant	Snort Rules	Yara Rules	Sigma Rules
Lumma Stealer	https://www.tzcert.go.tz/report/TZCERT-DET-25-0001/download	https://www.tzcert.go.tz/report/TZCERT-DET-25-0002/download	https://www.tzcert.go.tz/report/TZCERT-DET-25-0003/download
Rise Pro Stealer	-	https://www.tzcert.go.tz/report/TZCERT-DET-25-0004/download	https://www.tzcert.go.tz/report/TZCERT-DET-25-0005/download
Stealc	https://www.tzcert.go.tz/report/TZCERT-DET-25-0006/download	https://www.tzcert.go.tz/report/TZCERT-DET-25-0008/download	https://www.tzcert.go.tz/report/TZCERT-DET-25-0007/download
Vidar	https://www.tzcert.go.tz/report/TZCERT-DET-25-0010/download	https://www.tzcert.go.tz/report/TZCERT-DET-25-0009/download	https://www.tzcert.go.tz/report/TZCERT-DET-25-0011/download

***Table No.1**: Detection rule formats for identifying information stealer malware activities.*

Note: *Always review and test detection rules in a staging environment before deployment in production***.**

6.0. MITIGATION MEASURES

To protect computer systems against information stealer malware, organizations should implement the following mitigation strategies based on their operational context:

6.1. Recommendations for all organizations

This document is marked as TLP: CLEAR. Recipients can spread this to the world; there is no limit on disclosure. For more information, visit the Traffic Light Protocol (TLP) definition

TZ-CERT recommends that organizations prioritize the implementation of security measures aimed mitigating the risk of information stealers targeting malware. These mitigations include:

6.1.1. **Conduct cybersecurity awareness training to staff regularly** Organization should regular conduct cybersecurity awareness training to its staff educating on means and techniques in recognizing and avoiding common dissemination methods of Information Stealer malware e.g. Social Engineering and Phishing, deceptive online advertisement and unsafe downloads. Raising awareness about these vectors helps reduce the risk of credential compromise and strengthen overall security posture.

6.1.2. **Ensure Operating System and all installed application are regularly updated with latest security patches.** Timely patching address known vulnerabilities that cybercriminals often exploit to gain unauthorized access preventing malware infection and reducing the risk of being exploited.

6.1.3. **Make use of Endpoint Detection and Response (EDR) or Extended Detection and Response (XDR) solutions** as a modern alternative to traditional antivirus tools. XDR provides integrated threat detection, analysis and automated response capabilities across endpoints, networks and cloud environment enabling faster and more effective containment of malicious activity.

6.1.4. **Incorporate Indicator of Compromises (IOCs) and detection rules identified into Intrusion Detection Systems (IDS) and Security Information and Event Management (SIEM) platforms**. This integration enables active detection, blocking and reporting of malicious activity within the network environment.

This document is marked as TLP: CLEAR. Recipients can spread this to the world; there is no limit on disclosure. For more information, visit the Traffic Light Protocol (TLP) definition

6.1.5. **Enforce the principle of least-privilege**, ensuring that users, application and systems are granted only the minimum level of access to perform their tasks. This approach reduces the attack surface, limiting lateral movements and minimizes the potential impact of a security attack.

6.1.6. If your organization permits the use personal devices for work, **consider implementing a Bring Your Own Device (BYOD) policy**. Corporately managed devices typically offer stronger security controls, and formal BYOD policy helps mitigate risks by establishing clear guidance for secure access, data protection and device management.

6.1.7. **Disable all user accounts that are no longer active or in use**. Dormant accounts are often overlooked during routine security updates such as password changes, leaving them with the outdated credentials that attackers may exploit over time. Proactive removing unnecessary access reduce the risk of unauthorized entry and strengthens overall access control hygiene.

6.1.8. **Enforce multifactor authentication (MFA) for all sensitive systems and services**, particularly webmail, VPNs, and privileged user accounts that access critical systems. MFA adds an extra layer of security by requiring additional verification factor beyond the standard username and password of which reduce the risk of unauthorized access.

6.1.9. **Develop and enforce comprehensive security policies aimed at reducing the attack surface of the cooperate infrastructure**. Well defined policies guide user behavior, system configuration and access management thereby minimizing potential entry points for threat actors and enhancing overall cybersecurity posture.

This document is marked as TLP: CLEAR. Recipients can spread this to the world; there is no limit on disclosure. For more information, visit the Traffic Light Protocol (TLP) definition

6.1.10. **Develop a cybersecurity incident plan and supporting playbooks for handling various types of incidents** including Information Stealer compromises. Well defined plans and procedures help streamline response efforts, reduce decision making time under pressure and improve overall coordination during an incident. Also **ensure all employees are familiar with response steps** especially reporting and know whom to contact if they suspect malicious events.

6.2. Recommendations for end users

To help mitigate the threat, the following recommendations are provided to guide individuals in protecting their personal data, digital identity and devices against these evolving malware variants: -

6.2.1. Develop good cyber hygiene; avoid clicking on suspicious links or attachments, refrain downloading files or software from untrusted sources or unofficial source, and never install cracked or pirated software. This habit significantly reduces the risk of malware infection and unauthorized access to your personal data.

6.2.2. Use Multi-Factor Authentication (MFA) for personal accounts wherever possible. MFA add an extra layer of security beyond just a password. This significantly reduce the risk of unauthorized access even if login credential is compromised, by requiring a second form of verification such as one-time code or biometrics confirmation.

6.2.3. Avoid storing credentials in browsers or plain text files. Storing credentials such as passwords directly in web browser or unencrypted plain text files exposes them to theft if your device is compromised. Work related credentials should not be stored in a personal password manager, including web browser based manager.

This document is marked as TLP: CLEAR. Recipients can spread this to the world; there is no limit on disclosure. For more information, visit the Traffic Light Protocol (TLP) definition

6.2.4. **Keep operating systems and software up to date with the latest patches.** Regularly update your operating systems and software's to ensure that all known vulnerabilities are fixed promptly. This reduces the risk of exploitation by malwares including Information Stealer which often target outdated and unpatched systems to gain unauthorized access.

6.2.5. **Make sure endpoint security software (Antivirus) is enabled and up to date.** Activate and regularly update built-in antivirus or endpoint security software to provide continuous protection against malware threats. If you are using third-party antivirus solution, choose reputable vendor and maintain timely update to ensure detection and removal of emerging threats.

6.2.6. **Sign out from all online services and clear web browser cookies after completing a browsing session.** This reduces residual data exposure that Information Stealer could exploit, thereby enhancing the protection of your personal and other sensitive information from unauthorized access.

7.0. IMPORTANT NOTICE

TZ-CERT urges all constituents and the general public to remain highly vigilant and promptly report any incidents of cyberattacks for immediate technical assistance. Timely reporting is essential as it allows containment of threat at early stage, preventing damage and further spread by sharing actionable intelligence with sectors. This collaborative approach enhances national cyber resilience and helps combating ongoing malicious campaign more effectively. All incidents can be submitted to TZ-CERT through contact details as stipulated in section 9 of this advisory.

This document is marked as TLP: CLEAR. Recipients can spread this to the world; there is no limit on disclosure. For more information, visit the Traffic Light Protocol (TLP) definition

8.0. REFERENCES

i. https://www.malwarebytes.com/blog/threats/info-stealers
ii. https://redcanary.com/threat-detection-report/trends/info-stealers/
iii. https://www.ndit.nd.gov/news/information-stealers
iv. https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-malware/infostealers/
v. https://blog.sekoia.io/traffers-a-deep-dive-into-the-information-stealer-ecosystem/
vi. https://www.cyber.gov.au/sites/default/files/2024-09/Information-Stealer-Malware-Advisory.pdf
vii. https://flare.io/wp-content/uploads/stealer-malware-ecosystems-report-Oct-12.pdf
viii. https://www.bitsight.com/blog/what-is-stealer-malware
ix. https://www.cyfirma.com/research/vidar-stealer-an-in-depth-analysis-of-an-information-stealing-malware/

9.0. CONTACTS:

Tanzania Computer Emergency Response Team (TZ-CERT)
Mawasiliano Towers, 20 Sam Nujoma Road
P.O. Box 474
14414 DAR ES SALAAM
Phone: +255 22 2199760-9
Fax: +255 22 2412009 / +255 22 2412010
Email: info@tzcert.go.tz / incidents@tzcert.go.tz
PGP Key id: EED630F6
PGP Fingerprint: 0A1C CF48 D623 9BE7 676B 4C03 EF91 6FCA EED6 30F6

This document is marked as TLP: CLEAR. Recipients can spread this to the world; there is no limit on disclosure. For more information, visit the Traffic Light Protocol (TLP) definition