Hive Pro

Threat Level

Red

HiveForce Labs

# THREAT ADVISORY

## ATTACK REPORT

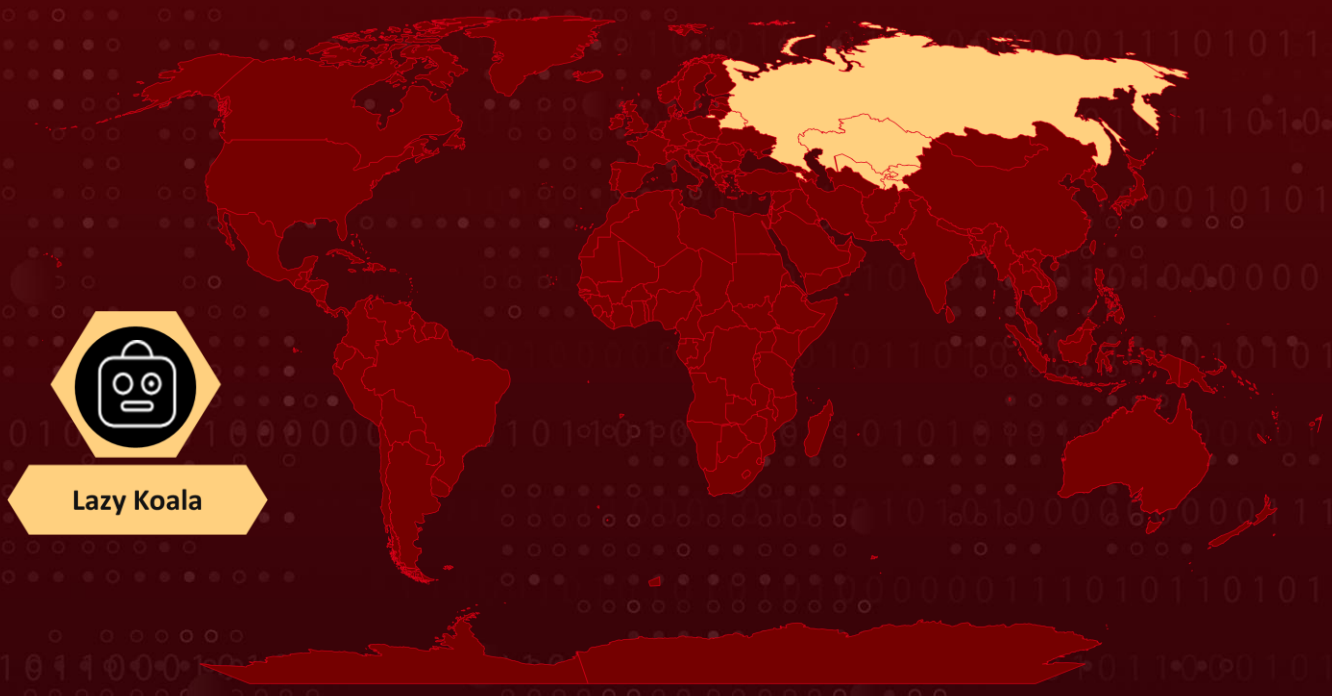
# LazyStealer the Unconventional Approach to Cyber Espionage


| Date of Publication | Admiralty Code | TA Number |
| --- | --- | --- |
| April 12, 2024 | A1 | TA2024142 |

# Summary

**Attack Commenced:** January 2024
**Malware:** LazyStealer
**Threat Actor:** Lazy Koala
**Attack Region:** Russia, Belarus, Kazakhstan, Uzbekistan, Kyrgyzstan, Tajikistan, and Armenia
**Targeted Industries:** Government, Financial, Medical, and Educational Institutions
**Attack**: A cybercriminal group known as Lazy Koala orchestrated a string of successful attacks, primarily targeting government entities across multiple countries in Eastern Europe and Central Asia. Despite the simplicity of their methods, the malware they deployed, named LazyStealer, demonstrated remarkable effectiveness.

## Attack Regions



# Attack Details

**#1** During the first quarter of 2024, a cybercriminal syndicate known as "Lazy Koala" successfully infiltrated primarily governmental organizations across Russia, Belarus, Kazakhstan, Uzbekistan, Kyrgyzstan, Tajikistan, and Armenia.

**#2** Their main objective was the illicit acquisition of credentials for various services used by public officials. Despite its basic design, the malware driving these attacks, named LazyStealer, achieved significant results.

**#3** Lazy Koala employed simple methods, likely utilizing phishing emails to lure unsuspecting victims into downloading and activating malicious attachments. LazyStealer employs several evasion tactics, initially bundled with PyInstaller and further concealed through Pyarmor.

**#4** Its core functions, built with Cython, greatly complicate reverse engineering efforts. Notably, LazyStealer intercepts Google Chrome login credentials and sends them to a Telegram bot for the attackers to retrieve. The targeted regions and the tools used suggest Lazy Koala's association with the YoroTrooper faction, known for employing similar methods and technologies.

**#5** The stolen data is either sold or repurposed for subsequent attacks, often aimed at corporate internal systems. The Lazy Koala incident highlights that successful breaches do not necessarily require sophisticated weaponry, strategies, or methodologies.

# Recommendations

**Enhance Email Security Measures:** It's crucial to bolster email security protocols. Implementing advanced email filtering and scanning technologies can help detect and block suspicious emails containing malware payloads.

**Network Segmentation:** Implement network segmentation to minimize the lateral movement of attackers within the network, limiting their ability to access critical systems and data.

**Zero Trust Architecture:** Adopt a Zero Trust security architecture, where trust is never assumed and continuous authentication and authorization mechanisms are implemented, reducing the risk of unauthorized access.

**Monitoring and Logging:** Implement robust monitoring and logging mechanisms to detect suspicious activity or unauthorized access to your accounts. Regularly review access logs and audit trails for unusual patterns or login locations.

**Heighten Employee Awareness:** Educate employees on cybersecurity best practices, emphasizing the importance of vigilance against phishing attempts. Encourage reporting of any suspicious emails or activities.

## Potential MITRE ATT&CK TTPs

| | | | |
|---|---|---|---|
| TA0001 Initial Access | TA0002 Execution | TA0003 Persistence | TA0005 Defense Evasion |
| TA0006 Credential Access | TA0007 Discovery | TA0011 Command and Control | TA0010 Exfiltration |
| T1204.002 Malicious File | T1204 User Execution | T1140 Deobfuscate/Decode Files or Information | T1555.003 Credentials from Web Browsers |
| T1555 Credentials from Password Stores | T1567 Exfiltration Over Web Service | T1566 Phishing | T1059 Command and Scripting Interpreter |
| T1059.006 Python | T1055 Process Injection | T1211 Exploitation for Defense Evasion | T1027 Obfuscated Files or Information |
| T1212 Exploitation for Credential Access | | | |

# Indicators of Compromise (IOCs)

| TYPE | VALUE |
|---|---|
| Filename | 33ms.exe,<br>Recommendation.exe,<br>05-1254_Minzrav.exe,<br>test.pyc,<br>test.pyc,<br>1.pyc,<br>test.pyc,<br>hello.cp39-win_amd64.pyd,<br>hello.cp39-win_amd64.pyd,<br>hello.cp39-win_amd64.pyd,<br>pdfbyte.cp39-win_amd64.pyd,<br>pdfbyte.cp39-win_amd64.pyd,<br>pdfbyte.cp39-win_amd64.pyd,<br>docpdf.cp39-win_amd64.pyd |
| MD5 | 4f060c5c6813e269f01e6cba1d3ac4cd,<br>641932b66490630005dde2aef405e5e9,<br>882d63c5ff749f232a3ce70a36c95b83,<br>fe245cf57be8b3daf8cdb3882de99f35,<br>8e233b0250d85ae63076af45ee829c55,<br>032a586d08e7f31e2aedbec61d5d0f62,<br>8cb819b48958540fac07244188508156,<br>2d51a6620c976e1d736448082338e0b1,<br>763eb39787756744b4062336eb945750,<br>5b84b516760773c538647bc6e4d26d37,<br>1dedf5772ea1126b79b5e22ca10cefd3,<br>0f5727bada96b3b62573bba51538e9e3,<br>c3242bce783d5fa0ab0ce645f1283c64,<br>1cff5f65c85d8cf614beedf8fd5112d7,<br>98914403f428abeea89c94e0b7edaaa9 |
| SHA1 | 4f0a1831d4d8c09f46e8f5fbe8b17b024daa6eee,<br>9bad63eab92144b8a365428aa68531c80fc2da0f,<br>cd1f89f3d56df6a775d8694c1cbf588961dc7f06,<br>40789ef406772e52a0dfc86509cc7617fa8b54a3,<br>ec14cf28fe8764d4f285b95ee7001af49ff0af68,<br>51ad91409698d8f4017defbd0a382cce9e69ed6f,<br>1f204cfb02df849f935c296a5e4b2f120bfa563b,<br>755ade0ddaceaabe9577d22a240e0430375f502f,<br>7685dd23d64fa94bb8d2d54dd2e104fbe5379ec5,<br>3e497222f9bc13d43d6a3e5fbdcae3474b3d2d22,<br>140968b7004aca9785a0a1f0a6712322db22fd6c,<br>6f54d068423cee9b2cf5ef50b4348025f983e220, |

| TYPE | VALUE |
| --- | --- |
| SHA1 | 845be44fb0d663636e500187d7d394714e562e08, c10637e35dfe326bd2c9a92f432d483f2f7591bd, 9866dfedbd311ed2f838ec56947cdf4ccabe8634 |
| SHA256 | 9fd197b7402285ed2a75dac9a5ce3ef499a58342fd0dcefe1c40443a12bc6832, e419a8158c6fe326dc7ab16dbd5f3b2723dffe8c9561fe835bb16f62a8fa61f5, a6e68f3066424daae4a54b2e0b01a4474a9a381469ae69daae6fef9a1626fa6d, 1db3d0ac68515b5c9876634605ba8492ba558f7df435bff2b20a74239107f3ec, 5ecdf5efe2a74db93450f2b35e942b91ee6dd1b0f545c04810d2794b748b1dea, 9fc75a6a17238ec3833dce0605b334c03fd84363f56313a5bf58d57ff286a9f9, 7d3733513e0645e66009e3d677af76653baa75c8ddf0d126aa0f270b56183272, 216f4e858f84269bee999fdc29dafbd79ec2270575e19a8626e25d5fe72a8f25, 8246e66ff043374477c06a612602f6e8a2cb487a33d8b046357a6c4870648ed1, ef6fb63259eac9f7642e468726a042f5a29576bf9f846b96fa6ded8bf145b64c, f2a8088f1a634e62a2d0e5b2d6427d67fae640bf03dd04c8571006e1f31d7992, bfa3718f6492dd337c127ccdbd8033b503ca089699ddbff3ac5c45f5f95f01e8, 1549114ea6d86198d29f79a009218ca991aa17d215a84b90e3c91ef3268180e4, 864a38b028d5b9e41fa0d4eee7cfa3a284d0ab9874b42cc4d50f1e2b2e26e1e5, 18e00bb5dee23815a89067258b11ef13d6327bcb3555d70596c906d4875ed8c2 |

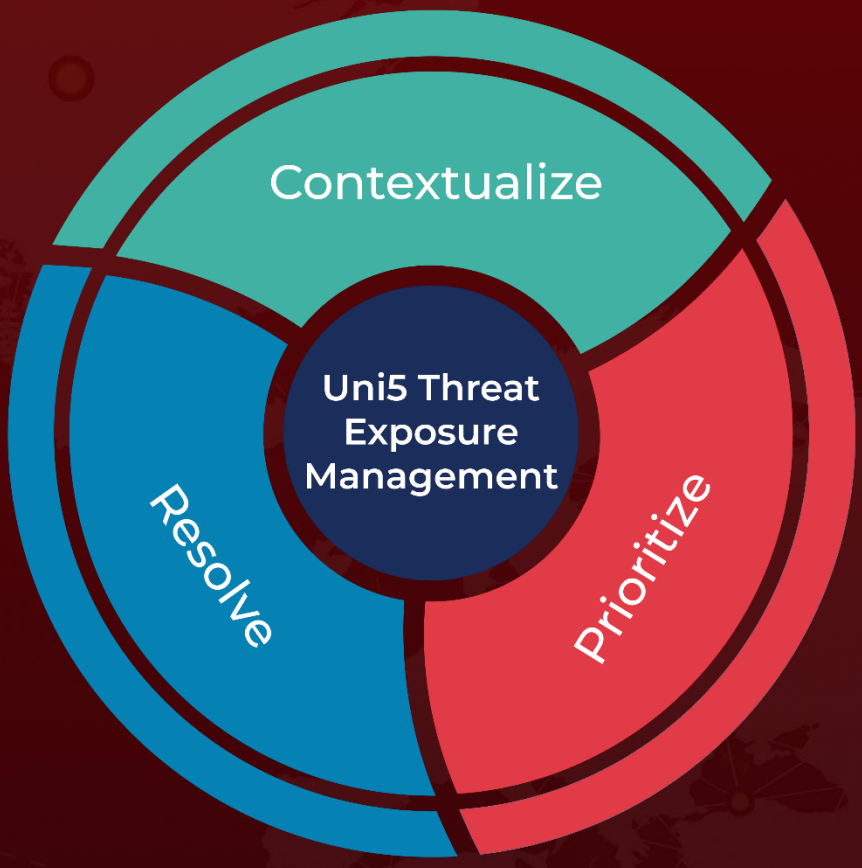
## References


https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/lazystealer-sophisticated-does-not-mean-better/

# What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.




REPORT GENERATED ON

**April 12, 2024 • 2:30 AM**



More at www.hivepro.com