Mar 24 2024

NETMANAGEIT

Intelligence Report

Large-Scale StrelaStealer Campaign in Early 2024

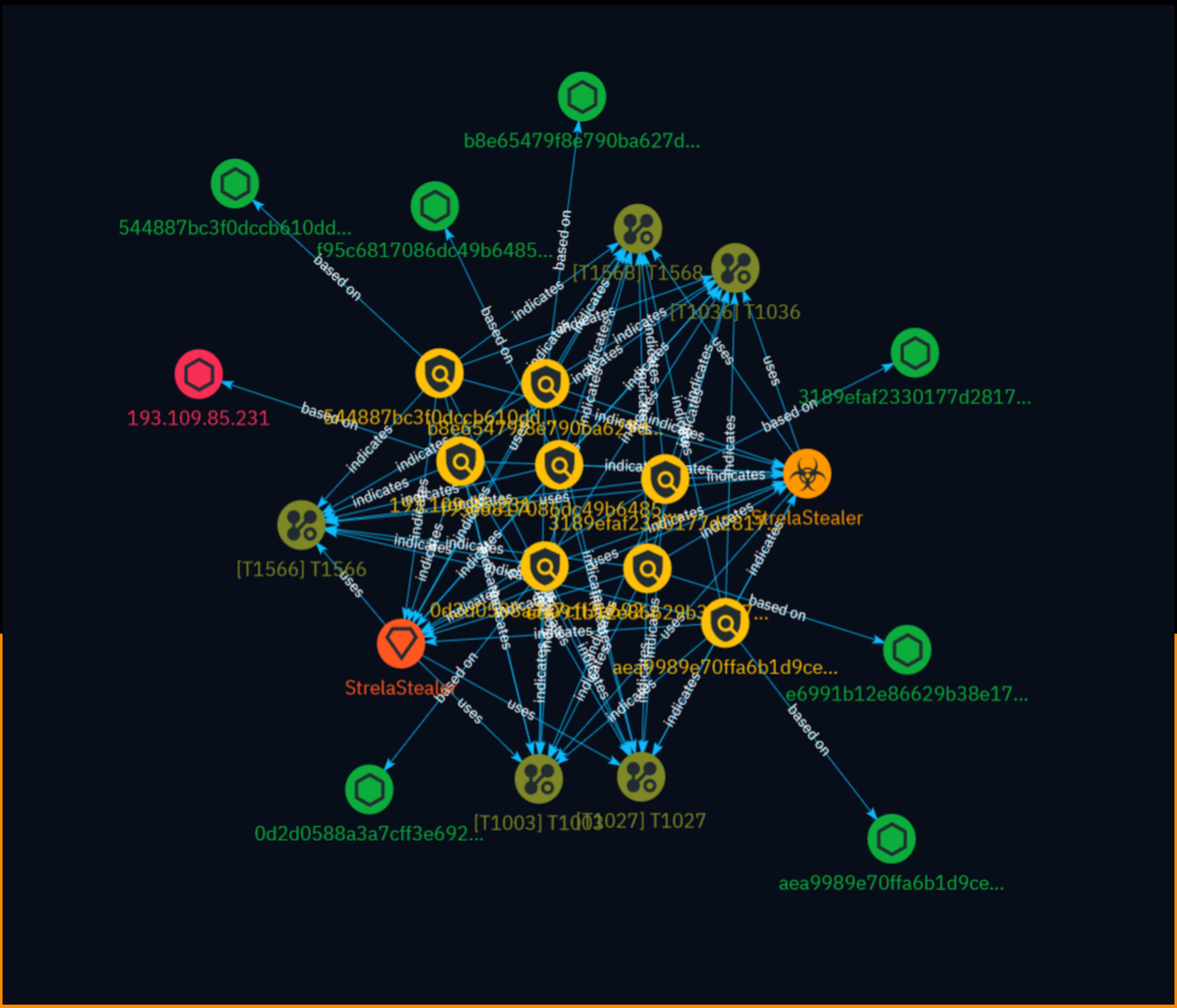

Table of contents

Overview

- Description 4
- Confidence 4
- Content 5

Entities

- Indicator 6
- Malware 10
- Intrusion-Set 11
- Attack-Pattern 12

Observables

- StixFile 16
- IPv4-Addr 17

External References

- External References 18

Overview

Description

A recent wave of large-scale StrelaStealer email campaigns was observed targeting over 100 organizations across the EU and U.S. The campaigns distribute spam emails with attachments that launch the malware's DLL payload. The malware steals email login credentials and sends them to the attacker's command and control server. The malware author frequently updates the malware to evade detection. Technical analysis revealed the malware is now delivered via a zipped JScript employing updated obfuscation in the DLL payload.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

100 / 100

Content

N/A

Indicator

Name
f95c6817086dc49b6485093bfd370c5e3fc3056a5378d519fd1f5619b30f3a2e
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'f95c6817086dc49b6485093bfd370c5e3fc3056a5378d519fd1f5619b30f3a2e']
Name
e6991b12e86629b38e178fef129dfda1d454391ffbb236703f8c026d6d55b9a1
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'e6991b12e86629b38e178fef129dfda1d454391ffbb236703f8c026d6d55b9a1']
Name

b8e65479f8e790ba627d0deb29a3631d1b043160281fe362f111b0e080558680

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b8e65479f8e790ba627d0deb29a3631d1b043160281fe362f111b0e080558680']

Name

aea9989e70ffa6b1d9ce50dd3af5b7a6a57b97b7401e9eb2404435a8777be054

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'aea9989e70ffa6b1d9ce50dd3af5b7a6a57b97b7401e9eb2404435a8777be054']

Name

544887bc3f0dccb610dd7ba35b498a03ea32fca047e133a0639d5bca61cc6f45

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '544887bc3f0dccb610dd7ba35b498a03ea32fca047e133a0639d5bca61cc6f45']

Name

3189efaf2330177d2817cfb69a8bfa3b846c24ec534aa3e6b66c8a28f3b18d4b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3189efaf2330177d2817cfb69a8bfa3b846c24ec534aa3e6b66c8a28f3b18d4b']

Name

0d2d0588a3a7cff3e69206be3d75401de6c69bcff30aa1db59d34ce58d5f799a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0d2d0588a3a7cff3e69206be3d75401de6c69bcff30aa1db59d34ce58d5f799a']

Name

193.109.85.231

Description

- **Zip Code:** N/A - **ISP:** Dzardanov Artur Kazbekovich - **ASN:** 206243 - **Organization:** Dzardanov Artur Kazbekovich - **Is Crawler:** False - **Timezone:** Europe/Moscow - **Mobile:** False - **Host:** 193.109.85.231 - **Proxy:** True - **VPN:** False - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** True - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** RU - **Region:** Kabardino-Balkarskaya Respublika - **City:** Nal'chik - **Latitude:** 43.49805832 - **Longitude:** 43.61888885

Pattern Type

stix

Pattern

[ipv4-addr:value = '193.109.85.231']

Malware

Name
StrelaStealer

Intrusion-Set

Name
StrelaStealer

Attack-Pattern

Name
T1568
ID
T1568
Description
Adversaries may dynamically establish connections to command and control infrastructure to evade common detections and remediations. This may be achieved by using malware that shares a common algorithm with the infrastructure the adversary uses to receive the malware's communications. These calculations can be used to dynamically adjust parameters such as the domain name, IP address, or port number the malware uses for command and control. Adversaries may use dynamic resolution for the purpose of [Fallback Channels](https://attack.mitre.org/techniques/T1008). When contact is lost with the primary command and control server malware may employ dynamic resolution as a means to reestablishing command and control.(Citation: Talos CCleanup 2017)(Citation: FireEye POSHSPY April 2017)(Citation: ESET Sednit 2017 Activity)
Name
T1027
ID
T1027

Description

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses. Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140) for [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016) Adversaries may also use compressed or archived scripts, such as JavaScript. Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. (Citation: Linux/Cdorked.A We Live Security Analysis) Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled. (Citation: Carbon Black Obfuscation Sept 2016) Adversaries may also abuse [Command Obfuscation](https://attack.mitre.org/techniques/T1027/010) to obscure commands executed from payloads or directly via [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Revoke-Obfuscation July 2017)(Citation: PaloAlto EncodedCommand March 2017)

Name

T1566

ID

T1566

Description

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name

T1036

ID

T1036

Description

Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. Masquerading occurs when the name or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names. Renaming abusable system utilities to evade security monitoring is also a form of [Masquerading](https://attack.mitre.org/techniques/T1036).(Citation: LOLBAS Main Site) Masquerading may also include the use of [Proxy](https://attack.mitre.org/techniques/T1090) or VPNs to disguise IP addresses, which can allow adversaries to blend in with normal network traffic and bypass conditional access policies or anti-abuse protections.

Name

T1003

ID
T1003

Description
Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform [Lateral Movement](https://attack.mitre.org/tactics/TA0008) and access restricted information. Several of the tools mentioned in associated sub-techniques may be used by both adversaries and professional security testers. Additional custom tools likely exist as well.

StixFile

Value
f95c6817086dc49b6485093bfd370c5e3fc3056a5378d519fd1f5619b30f3a2e
e6991b12e86629b38e178fef129dfda1d454391ffbb236703f8c026d6d55b9a1
b8e65479f8e790ba627d0deb29a3631d1b043160281fe362f111b0e080558680
aea9989e70ffa6b1d9ce50dd3af5b7a6a57b97b7401e9eb2404435a8777be054
544887bc3f0dccb610dd7ba35b498a03ea32fca047e133a0639d5bca61cc6f45
3189efaf2330177d2817cfb69a8bfa3b846c24ec534aa3e6b66c8a28f3b18d4b
0d2d0588a3a7cff3e69206be3d75401de6c69bcff30aa1db59d34ce58d5f799a

IPv4-Addr

Value
193.109.85.231

External References

- https://unit42.paloaltonetworks.com/strelastealer-campaign/#post-133130-_vl741f7mzldf
- https://otx.alienvault.com/pulse/65fd5f1d8f2927d1bbe4a415