Jan 22 2024

NETMANAGEIT

Intelligence Report

Security Brief: TA866 Returns with a Large Email Campaign

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Researchers have identified the return of TA866 to email threat campaign data, after a nine-month absence. Invoice-themed emails had attached PDFs with names such as “Document_[10 digits].pdf” and various subjects such as “Project achievements”. The PDFs contained OneDrive URLs that, if clicked, initiated a multi-step infection chain eventually leading to the malware payload, a variant of the WasabiSeed and Screenshotter custom toolset.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

Name
Phishing
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

Ingress Tool Transfer

ID

T1105

Description

Adversaries may transfer tools or other files from an external system into a compromised environment. Tools or files may be copied from an external adversary-controlled system to the victim network through the command and control channel or through alternate protocols such as [ftp](https://attack.mitre.org/software/S0095). Once present, adversaries may also transfer/spread tools between victim devices within a compromised environment (i.e. [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570)). On Windows, adversaries may use various utilities to download tools, such as `copy`, `finger`, [certutil](https://attack.mitre.org/software/S0160), and [PowerShell](https://attack.mitre.org/techniques/T1059/001) commands such as `IEX(New-Object Net.WebClient).downloadString()` and `Invoke-WebRequest`. On Linux and macOS systems, a variety of utilities also exist, such as `curl`, `scp`, `sftp`, `tftp`, `rsync`, `finger`, and `wget`. (Citation: t1105_lolbas) Adversaries may also abuse installers and package managers, such as `yum` or `winget`, to download tools to victim hosts. Files can also be transferred using various [Web Service](https://attack.mitre.org/techniques/T1102)s as well as native or otherwise present tools on the victim system.(Citation: PTSecurity Cobalt Dec 2016) In some cases, adversaries may be able to leverage services that sync between a web-based and an on-premises client, such as Dropbox or OneDrive, to transfer files onto victim systems. For example, by compromising a cloud account and logging into the service's web portal, an adversary may be able to trigger an automatic syncing process that transfers the file onto the victim's machine.(Citation: Dropbox Malware Sync)

Name

Screen Capture

ID

T1113

Description

Adversaries may attempt to take screen captures of the desktop to gather information over the course of an operation. Screen capturing functionality may be included as a feature of a remote access tool used in post-compromise operations. Taking a screenshot is also typically possible through native utilities or API calls, such as `CopyFromScreen`, `xwd`, or `screencapture`.(Citation: CopyFromScreen .NET)(Citation: Antiquated Mac Malware)

Indicator

Name

8277dff37fb068c3590390ca1aa6b96fd8b4f93757d5070f68ee8894e37713b1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8277dff37fb068c3590390ca1aa6b96fd8b4f93757d5070f68ee8894e37713b1']

Name

193.233.133.179

Description

ISP: AEZA INTERNATIONAL LTD **OS:** None ---------- Hostnames: - probable-lace.aeza.network - easy-bell.aeza.network - n.sni-347-default.ssl.fastly.net ---------- Domains: - aeza.network - fastly.net ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.10 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQClmdUp6vS3hJiWVDX4UFbiGiumrUH0YtFRNPIVpVwLGij y Mdw2mOzuBggtLKc5IK8MbB8Mo1sk2JDgsPkW97SURJ5OI69KyxxmhUSjy3KbR4FOyqBR8heZoFf W 8G4Gq4py6tzoYYs3Zf2E6mKVKzYGKyY2htShZckHN8dweoXR8FdDA2Q/tl0qi2xeStr2K7C3y+Cj C8bOgu66JW06GCXducEPxHjZhYHZWMRMbp5a8YgoNQyWpwU/ 8pNNfprCMA+vgFHJ6JGuJOSxg5DT

mKFFPPHfMQ1qHFdTDYYU25DxlnIZzeGZbRc3YdLUNh3kfgpDgnNmcLQf9giZZzQW9gZmsYU2M4 +w KyaBx9SL9VUHwP2r5IXgSdbdce3+H0Dapn9/TRyONEFLm8pChoU7ID96mKeny3gb+5rW/ E2ReYRV jN8ab97Wpwnvvcrg5B7C4Pz32ZyFx5eRkJLFdYCMjCxs0qtOBjEfR1xvpnRbqQTDezh1RVaJ9nfs shnancsLZrs= Fingerprint: 4e:4c:6a:2e:c7:61:c5:9f:b8:a1:50:dc:7c:e8:f2:79 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 kex-strict-s-v00@openssh.com Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ssh-rsa ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ---------- **80:** ``` HTTP/1.1 404 Not Found X-Powered-By: Express Access-Control-Allow-Origin: * Date: Sun, 14 Jan 2024 11:32:14 GMT Connection: keep-alive Keep-Alive: timeout=5 Content-Length: 0 ``` ---------- **443:** ``` HTTP/1.1 500 Domain Not Found Connection: keep-alive Content-Length: 251 Server: Varnish Retry-After: 0 content-type: text/html Cache-Control: private, no-cache X-Served-By: cache-ams21035-AMS Accept-Ranges: bytes Date: Sun, 24 Dec 2023 01:08:55 GMT Via: 1.1 varnish ``` HEARTBLEED: 2023/12/24 01:09:21 193.233.133.179:443 - SAFE ---------- **3000:** ``` HTTP/1.1 404 Not Found X-Powered-By: Express Access-Control-Allow-Origin: * Date: Tue, 16 Jan 2024 00:31:58 GMT Connection: keep-alive Keep-Alive: timeout=5 Content-Length: 0 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '193.233.133.179']

Name

19938b8918b09852ee8d27a7cc2991ba2eb110f27ce25e70fffde932a74e6a6d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '19938b8918b09852ee8d27a7cc2991ba2eb110f27ce25e70fffde932a74e6a6d']

Name

bdb0b6f52b51d989c489c3605a1534c9603ffb7a373654f62fd6f3e3599341fb

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bdb0b6f52b51d989c489c3605a1534c9603ffb7a373654f62fd6f3e3599341fb']

Name

6e53a93fc2968d90891db6059bac49e975c09546e19a54f1f93fb01a21318fdc

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6e53a93fc2968d90891db6059bac49e975c09546e19a54f1f93fb01a21318fdc']

Name

8b35b21b52780d39ea7832cb918533be7de5b6682cbeffe37797ba92a92aa368

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8b35b21b52780d39ea7832cb918533be7de5b6682cbeffe37797ba92a92aa368']

Name

c9329007524b3da130c8635a226c8cbe3a4e803b813f5b2237ed976feb9d2c8d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c9329007524b3da130c8635a226c8cbe3a4e803b813f5b2237ed976feb9d2c8d']

Name

37.1.212.198

Description

CC=US ASN=AS29802 HVC-AS

Pattern Type

stix

Pattern
[ipv4-addr:value = '37.1.212.198']
Name
aec5bf19e72ed577b0a02cffeb4f5cc713ab4478267ce348cf337b508f2fcade
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'aec5bf19e72ed577b0a02cffeb4f5cc713ab4478267ce348cf337b508f2fcade']

Intrusion-Set

Name
TA866

Region

Name
Northern America
Name
Americas
Name
Latin America and the Caribbean

Country

Name
Canada
Name
United States
Name
Mexico

Malware

Name
Rhadamanthys
Name
Screenshotter
Name
AHK Bot
Name
WasabiSeed

StixFile

Value
19938b8918b09852ee8d27a7cc2991ba2eb110f27ce25e70fffde932a74e6a6d
aec5bf19e72ed577b0a02cffeb4f5cc713ab4478267ce348cf337b508f2fcade
6e53a93fc2968d90891db6059bac49e975c09546e19a54f1f93fb01a21318fdc
8b35b21b52780d39ea7832cb918533be7de5b6682cbeffe37797ba92a92aa368
8277dff37fb068c3590390ca1aa6b96fd8b4f93757d5070f68ee8894e37713b1
c9329007524b3da130c8635a226c8cbe3a4e803b813f5b2237ed976feb9d2c8d
bdb0b6f52b51d989c489c3605a1534c9603ffb7a373654f62fd6f3e3599341fb

IPv4-Addr

Value
193.233.133.179
37.1.212.198

External References

- https://otx.alienvault.com/pulse/65a98e9c335df7bc26b4d81a
- https://www.proofpoint.com/us/blog/threat-insight/security-brief-ta866-returns-large-email-campaign