Jul 03 2023

NETMANAGEIT

Intelligence Report

Email Spam with Attachment Modiloader

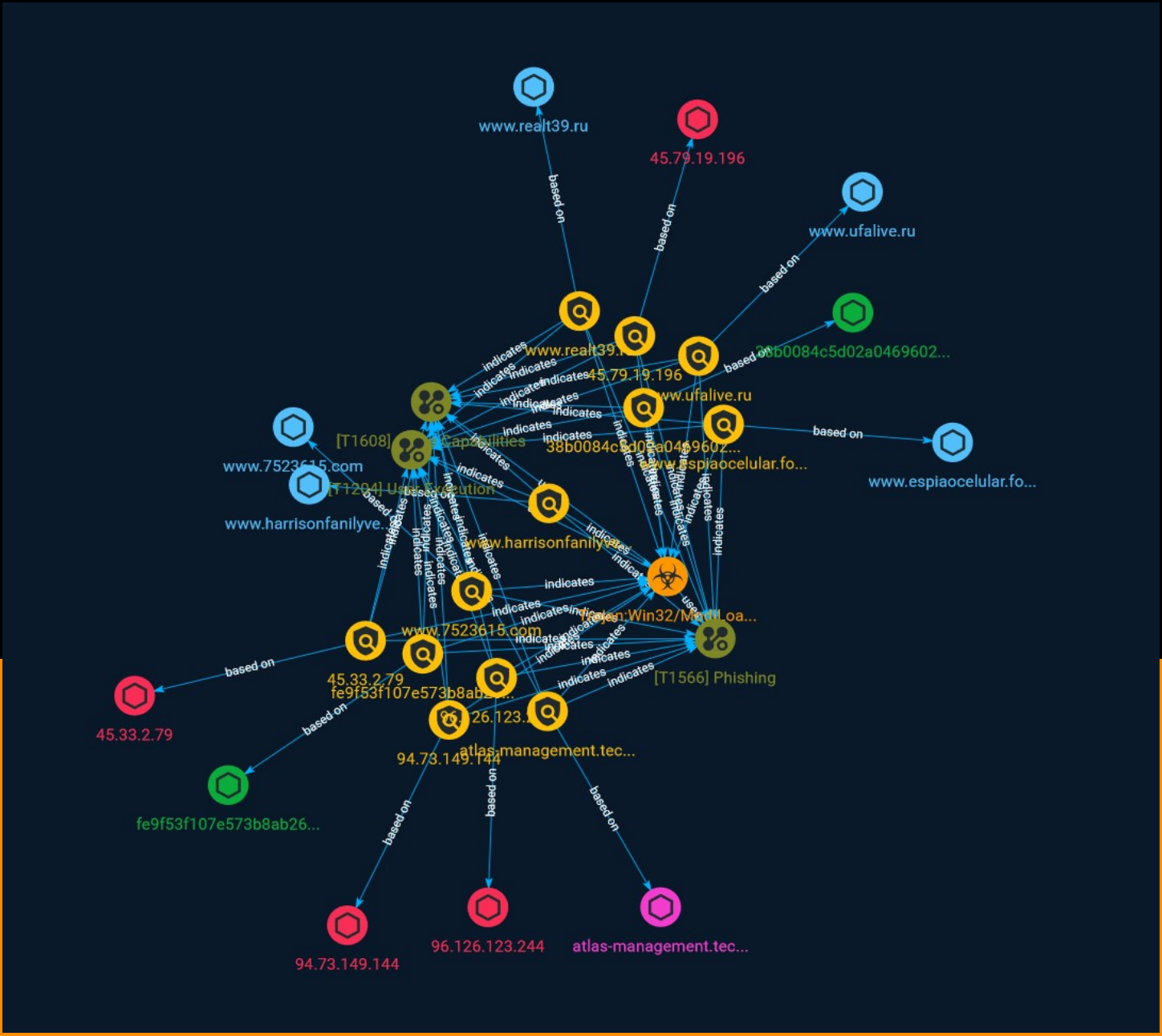

Table of contents

Overview

Entities

Observables

External References

Overview

Description

This week (2023-06-21) I found 2 emails attachment in quarantine that had different text with the same attachment. The first one had an Office 365 indicating the admin had setup a custom rule to block the message and could not be delivered to the recipients and what to do to fix it.

Confidence

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

15 / 100

Indicator

Name
fe9f53f107e573b8ab26e52e4f894d5f157b57e81a828ff4e530c3741c0006d5
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'fe9f53f107e573b8ab26e52e4f894d5f157b57e81a828ff4e530c3741c0006d5']
Name
www.harrisonfanilyvets.co.uk
Pattern Type
stix
Pattern
[hostname:value = 'www.harrisonfanilyvets.co.uk']
Name

94.73.149.144

Description

CC=TR ASN=AS34619 Cizgi Telekomunikasyon Anonim Sirketi

Pattern Type

stix

Pattern

[ipv4-addr:value = '94.73.149.144']

Name

www.7523615.com

Pattern Type

stix

Pattern

[hostname:value = 'www.7523615.com']

Name

www.realt39.ru

Pattern Type

stix

Pattern

[hostname:value = 'www.realt39.ru']

Name

45.33.2.79

Description

ISP: Akamai Connected Cloud **OS:** None ---------- Hostnames: - careambassadors.org - li956-79.members.linode.com ---------- Domains: - linode.com - careambassadors.org ---------- Services: **80:** ``` HTTP/1.1 200 OK server: openresty/1.13.6.1 date: Mon, 03 Jul 2023 12:40:28 GMT content-type: text/html transfer-encoding: chunked connection: close ``` ---------- **443:** ``` HTTP/1.1 302 Found content-length: 0 location: http://careambassadors.org/ cache-control: no-cache set-cookie: mtmssl=1; path=/; ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.33.2.79']

Name

45.79.19.196

Description

ISP: Akamai Connected Cloud **OS:** None ---------- Hostnames: - li1118-196.members.linode.com - hutchmanufacturing.com ---------- Domains: - linode.com - hutchmanufacturing.com ---------- Services: **80:** ``` HTTP/1.1 200 OK server: openresty/1.13.6.1 date: Mon, 03 Jul 2023 12:40:12 GMT content-type: text/html transfer-encoding: chunked connection: close ``` ---------- **443:** ``` HTTP/1.1 302 Found content-length: 0 location: http://hutchmanufacturing.com/ cache-

control: no-cache set-cookie: mtmssl=1; path=/; ``` HEARTBLEED: 2023/07/03 12:39:34 45.79.19.196:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.79.19.196']

Name

www.espiaocelular.foundation

Pattern Type

stix

Pattern

[hostname:value = 'www.espiaocelular.foundation']

Name

96.126.123.244

Description

ISP: Akamai Connected Cloud **OS:** None ---------- Hostnames: - com.com - li372-244.members.linode.com ---------- Domains: - com.com - linode.com ---------- Services: **80:** ``` HTTP/1.1 200 OK server: openresty/1.13.6.1 date: Mon, 03 Jul 2023 07:57:18 GMT content-type: text/html transfer-encoding: chunked connection: close ``` ---------- **443:** ``` HTTP/1.1 302 Found content-length: 0 location: http://q-uiz.com.com/ cache-control: no-cache set-cookie: mtmssl=1; path=/; ``` HEARTBLEED: 2023/07/03 07:57:19 96.126.123.244:443 - SAFE ----------

Pattern Type
stix
Pattern
[ipv4-addr:value = '96.126.123.244']
Name
www.ufalive.ru
Pattern Type
stix
Pattern
[hostname:value = 'www.ufalive.ru']
Name
atlas-management.tech
Pattern Type
stix
Pattern
[domain-name:value = 'atlas-management.tech']
Name
38b0084c5d02a04696027b5f58eaf6f528af5ba303f67f8cdf2d193a267beda8

Pattern Type
stix

Pattern
[file:hashes.'SHA-256' = '38b0084c5d02a04696027b5f58eaf6f528af5ba303f67f8cdf2d193a267beda8']

Malware

Name
Trojan:Win32/ModiLoader

Attack-Pattern

Name

Stage Capabilities

ID

T1608

Description

Adversaries may upload, install, or otherwise set up capabilities that can be used during targeting. To support their operations, an adversary may need to take capabilities they developed ([Develop Capabilities](https://attack.mitre.org/techniques/T1587)) or obtained ([Obtain Capabilities](https://attack.mitre.org/techniques/T1588)) and stage them on infrastructure under their control. These capabilities may be staged on infrastructure that was previously purchased/rented by the adversary ([Acquire Infrastructure](https://attack.mitre.org/techniques/T1583)) or was otherwise compromised by them ([Compromise Infrastructure](https://attack.mitre.org/techniques/T1584)). Capabilities may also be staged on web services, such as GitHub or Pastebin, or on Platform-as-a-Service (PaaS) offerings that enable users to easily provision applications.(Citation: Volexity Ocean Lotus November 2020)(Citation: Dragos Heroku Watering Hole)(Citation: Malwarebytes Heroku Skimmers)(Citation: Netskope GCP Redirection)(Citation: Netskope Cloud Phishing) Staging of capabilities can aid the adversary in a number of initial access and post-compromise behaviors, including (but not limited to): * Staging web resources necessary to conduct [Drive-by Compromise](https://attack.mitre.org/techniques/T1189) when a user browses to a site.(Citation: FireEye CFR Watering Hole 2012)(Citation: Gallagher 2015)(Citation: ATT ScanBox) * Staging web resources for a link target to be used with spearphishing.(Citation: Malwarebytes Silent Librarian October 2020)(Citation: Proofpoint TA407 September 2019) * Uploading malware or tools to a location accessible to a victim network to enable [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105).(Citation: Volexity Ocean Lotus November 2020) * Installing a previously acquired SSL/TLS certificate to use to encrypt

command and control traffic (ex: [Asymmetric Cryptography](https://attack.mitre.org/techniques/T1573/002) with [Web Protocols](https://attack.mitre.org/techniques/T1071/001)).(Citation: DigiCert Install SSL Cert)

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

User Execution

ID

T1204

Description

An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behavior from forms of [Phishing](https://attack.mitre.org/techniques/T1566). While [User Execution](https://attack.mitre.org/techniques/T1204) frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after [Internal Spearphishing](https://attack.mitre.org/techniques/T1534). Adversaries may also deceive users into performing actions such as enabling [Remote Access Software](https://attack.mitre.org/techniques/T1219), allowing direct control of the system to the adversary, or downloading and executing malware for [User Execution](https://attack.mitre.org/techniques/T1204). For example, tech support scams can be facilitated through [Phishing](https://attack.mitre.org/techniques/T1566), vishing, or various forms of user interaction. Adversaries can use a combination of these methods, such as spoofing and promoting toll-free numbers or call centers that are used to direct victims to malicious websites, to deliver and execute payloads containing malware or [Remote Access Software](https://attack.mitre.org/techniques/T1219).(Citation: Telephone Attack Delivery)

Domain-Name

Value
atlas-management.tech

StixFile

Value
38b0084c5d02a04696027b5f58eaf6f528af5ba303f67f8cdf2d193a267beda8
fe9f53f107e573b8ab26e52e4f894d5f157b57e81a828ff4e530c3741c0006d5

Hostname

Value
www.espiaocelular.foundation
www.realt39.ru
www.ufalive.ru
www.harrisonfanilyvets.co.uk
www.7523615.com

IPv4-Addr

Value
96.126.123.244
45.33.2.79
45.79.19.196
94.73.149.144

External References

- https://otx.alienvault.com/pulse/64a2e1b31615d5a3975beaf5
- https://isc.sans.edu/diary/rss/29978