Sep 11 2023

NETMANAGEIT

Intelligence Report

“MrTonyScam” — Botnet of Facebook Users Launch High-Intent Messenger Phishing Attack on Business Accounts

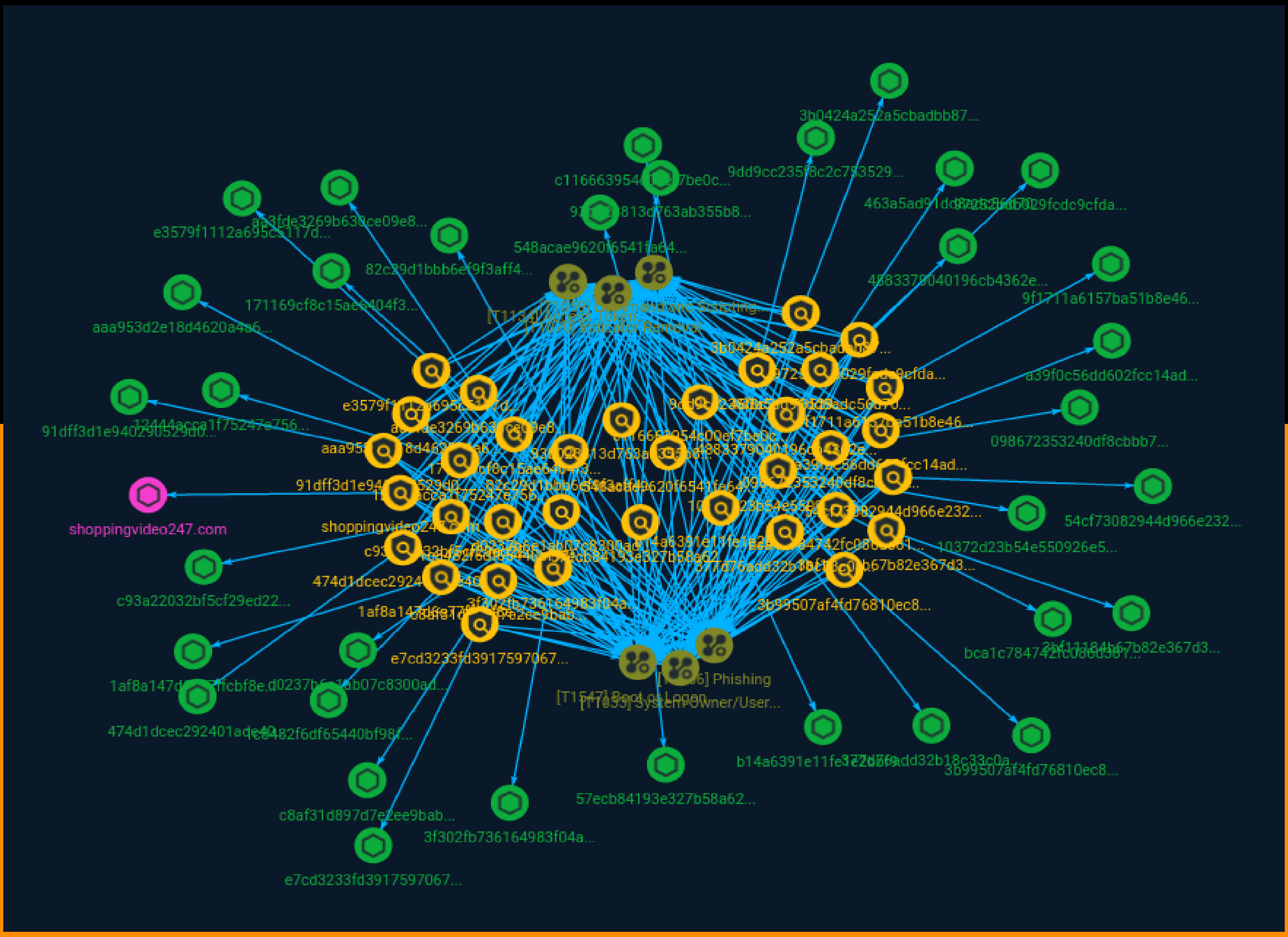

Table of contents

Overview

- Description 3
- Confidence 3

Entities

- Indicator 4
- Attack-Pattern 18

Observables

- Domain-Name 23
- StixFile 24

External References

- External References 27

Overview

Description

A new phishing campaign targeting Facebook business accounts has been uncovered by security researchers at the University of California, San Francisco, and is being exploited by a group of Vietnamese-based threat actors, writes Oleg Zaytsev from Guardio Labs.

Confidence

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

15 / 100

Indicator

Name

3f302fb736164983f04a9ebb8e2ab5604bb92380e8ccac8b160698fb02ccaebd

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3f302fb736164983f04a9ebb8e2ab5604bb92380e8ccac8b160698fb02ccaebd']

Name

c93a22032bf5cf29ed22065ce572caca41152281852f8b81e034e1e64f4057f4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c93a22032bf5cf29ed22065ce572caca41152281852f8b81e034e1e64f4057f4']

Name

171169cf8c15ae6404f3849274fdbbe0cabc4f3ec0b65a3441228b1dbe31a0d6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'171169cf8c15ae6404f3849274fdbbe0cabc4f3ec0b65a3441228b1dbe31a0d6']

Name

a39f0c56dd602fcc14adcdeaa31c21d389af8ea8abcb89862fac19e2807c799d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'a39f0c56dd602fcc14adcdeaa31c21d389af8ea8abcb89862fac19e2807c799d']

Name

d0237b6e1ab07c8300ad282ed3aa1f6e0e90220d893bbeee26786e886cedb9ad

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'd0237b6e1ab07c8300ad282ed3aa1f6e0e90220d893bbeee26786e886cedb9ad']

Name

82c29d1bbb6ef9f3aff4d3ca91f3ec6dfc17018ec0e6da32d080658a19502db6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'82c29d1bbb6ef9f3aff4d3ca91f3ec6dfc17018ec0e6da32d080658a19502db6']

Name

10372d23b54e550926e59ec359aadf5180e9839cf20086473422d55b444353d6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'10372d23b54e550926e59ec359aadf5180e9839cf20086473422d55b444353d6']

Name

c116663954c00ef7be0ce7d391bed95fe0c1f775b97652906c49ec3fcd814719

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c116663954c00ef7be0ce7d391bed95fe0c1f775b97652906c49ec3fcd814719']

Name

bca1c784742fc086d381f4e1e4495941626d1b829147d0d5f6d3f47af78364dd

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bca1c784742fc086d381f4e1e4495941626d1b829147d0d5f6d3f47af78364dd']

Name

aa3fde3269b630ce09e882ed0224b2271ebda197f5e5e4beb69994e9fc8ddc44

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'aa3fde3269b630ce09e882ed0224b2271ebda197f5e5e4beb69994e9fc8ddc44']

Name

098672353240df8cbbb7487ad1e3df3e25ceae3ad1dc84e451f03b803183e86a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'098672353240df8cbbb7487ad1e3df3e25ceae3ad1dc84e451f03b803183e86a']

Name

57ecb84193e327b58a62663d5e34d96503bbd81c461f91780b4f6bdb9fc4aabf

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'57ecb84193e327b58a62663d5e34d96503bbd81c461f91780b4f6bdb9fc4aabf']

Name

aaa953d2e18d4620a4a6e60c42f67a6e07cab05eec50e6e8f16f19cfa7c1d13b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'aaa953d2e18d4620a4a6e60c42f67a6e07cab05eec50e6e8f16f19cfa7c1d13b']

Name

9f1711a6157ba51b8e464ff4659c3a1db036e2e93721263e0091ed6fe53bf503

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9f1711a6157ba51b8e464ff4659c3a1db036e2e93721263e0091ed6fe53bf503']

Name

12444acca1f75247e756516a5d3ca2a33d67641f0664c00c3220f141b3dd8ce1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '12444acca1f75247e756516a5d3ca2a33d67641f0664c00c3220f141b3dd8ce1']

Name

9dd9cc235f8c2c753529955a351805e01229cc5052932561b0b96344537ce46c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9dd9cc235f8c2c753529955a351805e01229cc5052932561b0b96344537ce46c']

Name

b14a6391e11fe1e2bbf9972e5fefb7579bfcb4177acf60bcf1fc39fdacd1ddfa

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b14a6391e11fe1e2bbf9972e5fefb7579bfcb4177acf60bcf1fc39fdacd1ddfa']

Name

474d1dcec292401ade40bd90a95b872e5ab2c8fb68737b786e4308444d3ad33a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '474d1dcec292401ade40bd90a95b872e5ab2c8fb68737b786e4308444d3ad33a']

Name

97252bdb029fcdc9cfda86688a6327f76ea780761a3c1736db6a368ea30ffa14

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'97252bdb029fcdc9cfda86688a6327f76ea780761a3c1736db6a368ea30ffa14']

Name

c8af31d897d7e2ee9babb6a60dec5b65fc4b018e4ce8da6a5d8008ce5926bd54

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'c8af31d897d7e2ee9babb6a60dec5b65fc4b018e4ce8da6a5d8008ce5926bd54']

Name

1c8482f6df65440bf98fdceddac178e841bc801f591de6b060c45b50136dff1f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1c8482f6df65440bf98fdceddac178e841bc801f591de6b060c45b50136dff1f']

Name

3bf11184b67b82e367d36cb9ed3380a43814b000d84aef0bb89d4e08e4fcd581

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3bf11184b67b82e367d36cb9ed3380a43814b000d84aef0bb89d4e08e4fcd581']

Name

1af8a147d6e77ffcbf8e5dda14b32c715c4149b5e1c933fa69e451600ecfbf8e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1af8a147d6e77ffcbf8e5dda14b32c715c4149b5e1c933fa69e451600ecfbf8e']

Name

4883379040196cb4362ed4dfe4c011512febbfac7217e029f107b62c9acce6df

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4883379040196cb4362ed4dfe4c011512febbfac7217e029f107b62c9acce6df']

Name

548acae9620f6541fa647dcbfe7ed2f3d9637f228b24bfcb0c7d17f34e83b8e5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '548acae9620f6541fa647dcbfe7ed2f3d9637f228b24bfcb0c7d17f34e83b8e5']

Name

91dff3d1e940290529d064a0b13e190e6231679ea067df399de559d5bd071d81

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '91dff3d1e940290529d064a0b13e190e6231679ea067df399de559d5bd071d81']

Name

463a5ad91dd8adc56d700c059770de8ee01b3ba5bc276d17db872cc69d6768bf

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '463a5ad91dd8adc56d700c059770de8ee01b3ba5bc276d17db872cc69d6768bf']

Name

shoppingvideo247.com

Pattern Type

stix

Pattern

[domain-name:value = 'shoppingvideo247.com']

Name

93b023813d763ab355b82a3ce7693dbd668d80c3f0034fedbe16a5c44509f250

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '93b023813d763ab355b82a3ce7693dbd668d80c3f0034fedbe16a5c44509f250']

Name
3b99507af4fd76810ec8224122bc3701f7f2ef2cfa9677d012854df3abd44f5c
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '3b99507af4fd76810ec8224122bc3701f7f2ef2cfa9677d012854df3abd44f5c']
Name
e7cd3233fd39175970675135dac2c582382747b328b3786f8a833ae2ab8f4239
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'e7cd3233fd39175970675135dac2c582382747b328b3786f8a833ae2ab8f4239']
Name
3b0424a252a5cbadbb870907ed3c118cafc01ae86382f1775de5b9bc6cc3bce3
Pattern Type
stix
Pattern

[file:hashes.'SHA-256' = '3b0424a252a5cbadbb870907ed3c118cafc01ae86382f1775de5b9bc6cc3bce3']

Name

377d76add32b18c33c0ade90cb355a1e9f0ead3b9a7060f56557fb1fe1b39434

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '377d76add32b18c33c0ade90cb355a1e9f0ead3b9a7060f56557fb1fe1b39434']

Name

e3579f1112a695c5117dff5830ef64bf47703943e7ee7dbd32086c7865fcf126

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e3579f1112a695c5117dff5830ef64bf47703943e7ee7dbd32086c7865fcf126']

Name

54cf73082944d966e232d74c33f0cd4e05411846d57fab35171369910be84eb1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'54cf73082944d966e232d74c33f0cd4e05411846d57fab35171369910be84eb1']

Attack-Pattern

Name

Boot or Logon Autostart Execution

ID

T1547

Description

Adversaries may configure system settings to automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges on compromised systems. Operating systems may have mechanisms for automatically running a program on system boot or account logon.(Citation: Microsoft Run Key)(Citation: MSDN Authentication Packages)(Citation: Microsoft TimeProvider)(Citation: Cylance Reg Persistence Sept 2013)(Citation: Linux Kernel Programming) These mechanisms may include automatically executing programs that are placed in specially designated directories or are referenced by repositories that store configuration information, such as the Windows Registry. An adversary may achieve the same goal by modifying or extending features of the kernel. Since some boot or logon autostart programs run with higher privileges, an adversary may leverage these to elevate privileges.

Name

Indicator Removal

ID

T1070

Description

Adversaries may delete or modify artifacts generated within systems to remove evidence of their presence or hinder defenses. Various artifacts may be created by an adversary or something that can be attributed to an adversary’s actions. Typically these artifacts are used as defensive indicators related to monitored events, such as strings from downloaded files, logs that are generated from user actions, and other data analyzed by defenders. Location, format, and type of artifact (such as command or login history) are often specific to each platform. Removal of these indicators may interfere with event collection, reporting, or other processes used to detect intrusion activity. This may compromise the integrity of security solutions by causing notable events to go unreported. This activity may also impede forensic analysis and incident response, due to lack of sufficient data to determine what occurred.

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

Access Token Manipulation

ID

T1134

Description

Adversaries may modify access tokens to operate under a different user or system security context to perform actions and bypass access controls. Windows uses access tokens to determine the ownership of a running process. A user can manipulate access tokens to make a running process appear as though it is the child of a different process or belongs to someone other than the user that started the process. When this occurs, the process also takes on the security context associated with the new token. An adversary can use built-in Windows API functions to copy access tokens from existing processes; this is known as token stealing. These token can then be applied to an existing process (i.e. [Token Impersonation/Theft](https://attack.mitre.org/techniques/T1134/001)) or used to spawn a new process (i.e. [Create Process with Token](https://attack.mitre.org/techniques/T1134/002)). An adversary must already be in a privileged user context (i.e. administrator) to steal a token. However, adversaries commonly use token stealing to elevate their security context from the administrator level to the SYSTEM level. An adversary can then use a token to authenticate to a remote system as the account for that token if the account has appropriate permissions on the remote system.(Citation: Pentestlab Token Manipulation) Any standard user can use the `runas` command, and the Windows API functions, to create impersonation tokens; it does not require access to an administrator account. There are also other mechanisms, such as Active Directory fields, that can be used to modify access tokens.

Name

Command and Scripting Interpreter

ID

T1059

Description

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](https://attack.mitre.org/techniques/T1059/004) while Windows installations include the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) and [PowerShell](https://attack.mitre.org/techniques/T1059/001). There are also cross-platform interpreters such as [Python](https://attack.mitre.org/techniques/T1059/006), as well as those commonly associated with client applications such as [JavaScript](https://attack.mitre.org/techniques/T1059/007) and [Visual Basic](https://attack.mitre.org/techniques/T1059/005). Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](https://attack.mitre.org/tactics/TA0001) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](https://attack.mitre.org/techniques/T1021) in order to achieve remote Execution. (Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

Name

System Owner/User Discovery

ID

T1033

Description

Adversaries may attempt to identify the primary user, currently logged in user, set of users that commonly uses a system, or whether a user is actively using the system. They may do this, for example, by retrieving account usernames or by using [OS Credential Dumping] (https://attack.mitre.org/techniques/T1003). The information may be collected in a number of different ways using other Discovery techniques, because user and username details are prevalent throughout a system and include running process ownership, file/directory ownership, session information, and system logs. Adversaries may use the information from [System Owner/User Discovery](https://attack.mitre.org/techniques/T1033) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Various utilities and commands may acquire this information, including `whoami`. In macOS and Linux, the currently logged in user can be identified with `w` and `who`. On macOS the `dscl . list /Users | grep -v '_'` command can also be used to enumerate user accounts. Environment variables, such as `%USERNAME%` and `$USER`, may also be used to access this information. On network devices, [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands such as `show users` and `show ssh` can be used to display users currently logged into the device.(Citation: show_ssh_users_cmd_cisco)(Citation: US-CERT TA18-106A Network Infrastructure Devices 2018)

Domain-Name

Value
shoppingvideo247.com

StixFile

Value
54cf73082944d966e232d74c33f0cd4e05411846d57fab35171369910be84eb1
9dd9cc235f8c2c753529955a351805e01229cc5052932561b0b96344537ce46c
57ecb84193e327b58a62663d5e34d96503bbd81c461f91780b4f6bdb9fc4aabf
82c29d1bbb6ef9f3aff4d3ca91f3ec6dfc17018ec0e6da32d080658a19502db6
a39f0c56dd602fcc14adcdeaa31c21d389af8ea8abcb89862fac19e2807c799d
1c8482f6df65440bf98fdceddac178e841bc801f591de6b060c45b50136dff1f
548acae9620f6541fa647dcbfe7ed2f3d9637f228b24bfcb0c7d17f34e83b8e5
93b023813d763ab355b82a3ce7693dbd668d80c3f0034fedbe16a5c44509f250
1af8a147d6e77ffcbf8e5dda14b32c715c4149b5e1c933fa69e451600ecfbf8e
9f1711a6157ba51b8e464ff4659c3a1db036e2e93721263e0091ed6fe53bf503
3bf11184b67b82e367d36cb9ed3380a43814b000d84aef0bb89d4e08e4fcd581
3b0424a252a5cbadbb870907ed3c118cafc01ae86382f1775de5b9bc6cc3bce3
377d76add32b18c33c0ade90cb355a1e9f0ead3b9a7060f56557fb1fe1b39434

b14a6391e11fe1e2bbf9972e5fefb7579bfcb4177acf60bcf1fc39fdacd1ddfa

171169cf8c15ae6404f3849274fdbbe0cabc4f3ec0b65a3441228b1dbe31a0d6

bca1c784742fc086d381f4e1e4495941626d1b829147d0d5f6d3f47af78364dd

c93a22032bf5cf29ed22065ce572caca41152281852f8b81e034e1e64f4057f4

e3579f1112a695c5117dff5830ef64bf47703943e7ee7dbd32086c7865fcf126

3f302fb736164983f04a9ebb8e2ab5604bb92380e8ccac8b160698fb02ccaebd

12444acca1f75247e756516a5d3ca2a33d67641f0664c00c3220f141b3dd8ce1

c116663954c00ef7be0ce7d391bed95fe0c1f775b97652906c49ec3fcd814719

91dff3d1e940290529d064a0b13e190e6231679ea067df399de559d5bd071d81

97252bdb029fcdc9cfda86688a6327f76ea780761a3c1736db6a368ea30ffa14

e7cd3233fd39175970675135dac2c582382747b328b3786f8a833ae2ab8f4239

c8af31d897d7e2ee9babb6a60dec5b65fc4b018e4ce8da6a5d8008ce5926bd54

4883379040196cb4362ed4dfe4c011512febbfac7217e029f107b62c9acce6df

474d1dcec292401ade40bd90a95b872e5ab2c8fb68737b786e4308444d3ad33a

463a5ad91dd8adc56d700c059770de8ee01b3ba5bc276d17db872cc69d6768bf

098672353240df8cbbb7487ad1e3df3e25ceae3ad1dc84e451f03b803183e86a

d0237b6e1ab07c8300ad282ed3aa1f6e0e90220d893bbeee26786e886cedb9ad

aa3fde3269b630ce09e882ed0224b2271ebda197f5e5e4beb69994e9fc8ddc44

3b99507af4fd76810ec8224122bc3701f7f2ef2cfa9677d012854df3abd44f5c
aaa953d2e18d4620a4a6e60c42f67a6e07cab05eec50e6e8f16f19cfa7c1d13b
10372d23b54e550926e59ec359aadf5180e9839cf20086473422d55b444353d6

External References

- https://otx.alienvault.com/pulse/64ff3139607f4acc122a7ccf
- https://labs.guard.io/mrtonyscam-botnet-of-facebook-users-launch-high-intent-messenger-phishing-attack-on-business-3182cfb12f4d