Dec 06 2023

NETMANAGEIT

Intelligence Report

Beware of predatory fin(tech): Loan sharks use Android apps to reach new depths

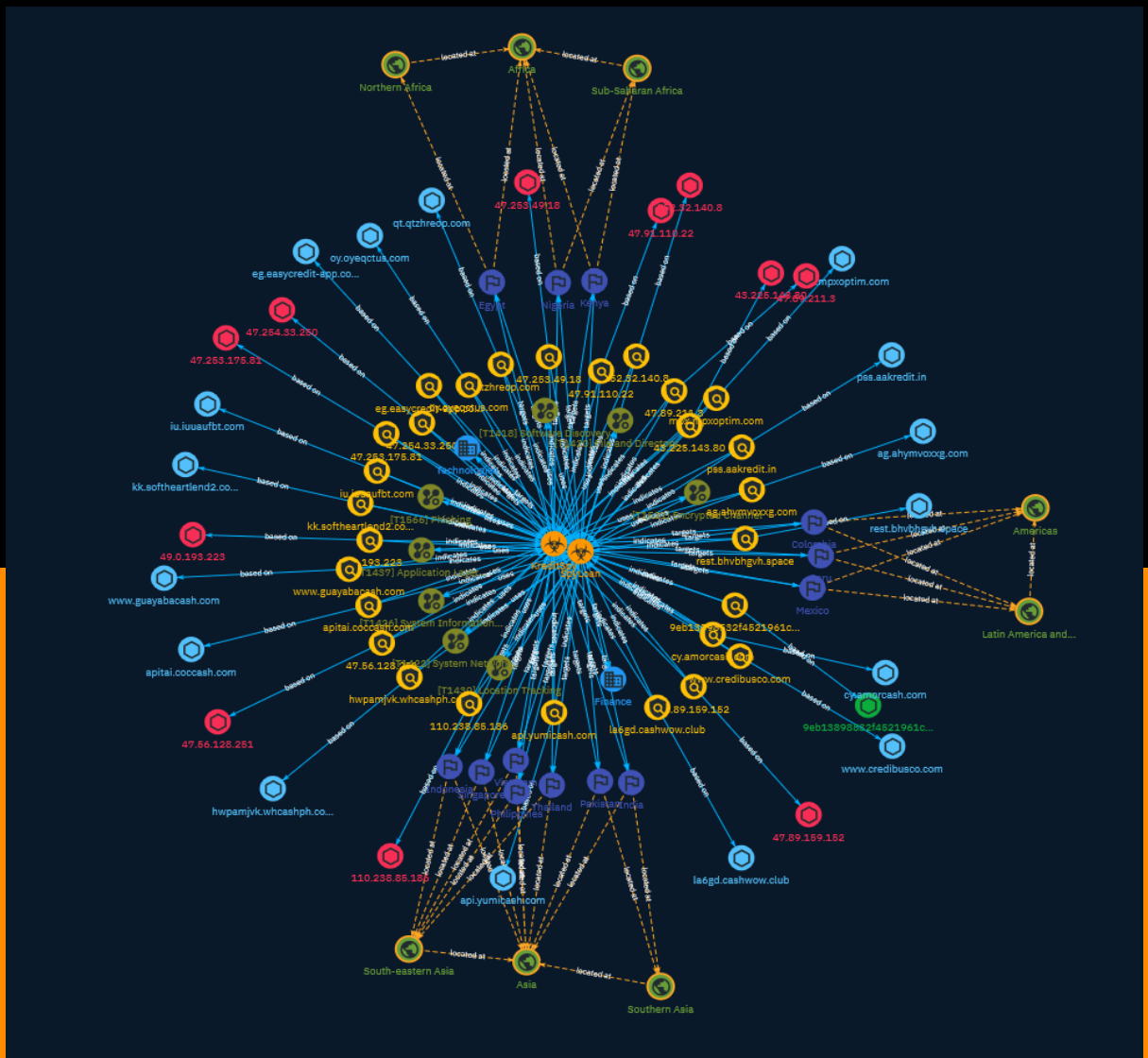

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Researchers have identified and identified a growing number of malicious Android loan apps that are being used to blackmail and defraud users, and are available to download from third-party app stores and websites.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

Name
Software Discovery
ID
T1418
Description
Adversaries may attempt to get a listing of applications that are installed on a device. Adversaries may use the information from [Software Discovery](https://attack.mitre.org/techniques/T1418) during automated discovery to shape follow-on behaviors, including whether or not to fully infect the target and/or attempts specific actions. Adversaries may attempt to enumerate applications for a variety of reasons, such as figuring out what security measures are present or to identify the presence of target applications.
Name
Location Tracking
ID
T1430
Description
Adversaries may track a device's physical location through use of standard operating system APIs via malicious or exploited applications on the compromised device. On

Android, applications holding the `ACCESS_COAURSE_LOCATION` or `ACCESS_FINE_LOCATION` permissions provide access to the device's physical location. On Android 10 and up, declaration of the `ACCESS_BACKGROUND_LOCATION` permission in an application's manifest will allow applications to request location access even when the application is running in the background.(Citation: Android Request Location Permissions) Some adversaries have utilized integration of Baidu map services to retrieve geographical location once the location access permissions had been obtained.(Citation: PaloAlto-SpyDealer)(Citation: Palo Alto HenBox) On iOS, applications must include the `NSLocationWhenInUseUsageDescription`, `NSLocationAlwaysAndWhenInUseUsageDescription`, and/or `NSLocationAlwaysUsageDescription` keys in their `Info.plist` file depending on the extent of requested access to location information.(Citation: Apple Requesting Authorization for Location Services) On iOS 8.0 and up, applications call `requestWhenInUseAuthorization()` to request access to location information when the application is in use or `requestAlwaysAuthorization()` to request access to location information regardless of whether the application is in use. With elevated privileges, an adversary may be able to access location data without explicit user consent with the `com.apple.locationd.preauthorized` entitlement key.(Citation: Google Project Zero Insomnia)

Name

File and Directory Discovery

ID

T1420

Description

Adversaries may enumerate files and directories or search in specific device locations for desired information within a filesystem. Adversaries may use the information from [File and Directory Discovery](https://attack.mitre.org/techniques/T1420) during automated discovery to shape follow-on behaviors, including deciding if the adversary should fully infect the target and/or attempt specific actions. On Android, Linux file permissions and SELinux policies typically stringently restrict what can be accessed by apps without taking advantage of a privilege escalation exploit. The contents of the external storage directory are generally visible, which could present concerns if sensitive data is inappropriately stored there. iOS's security architecture generally restricts the ability to perform any type

of [File and Directory Discovery](https://attack.mitre.org/techniques/T1420) without use of escalated privileges.

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

Application Layer Protocol

ID

T1437

Description

Adversaries may communicate using application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the mobile device, and often the results of those commands, will be embedded within the protocol traffic between the mobile device and server. Adversaries may utilize many different protocols, including those used for web browsing, transferring files, electronic mail, or DNS.

Name

Encrypted Channel

ID

T1521

Description

Adversaries may explicitly employ a known encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol. Despite the use of a secure algorithm, these implementations may be vulnerable to reverse engineering if necessary secret keys are encoded and/or generated within malware samples/configuration files.

Name

System Information Discovery

ID

T1426

Description

Adversaries may attempt to get detailed information about a device's operating system and hardware, including versions, patches, and architecture. Adversaries may use the information from [System Information Discovery](https://attack.mitre.org/techniques/T1426) during automated discovery to shape follow-on behaviors, including whether or not to fully infects the target and/or attempts specific actions. On Android, much of this information is programmatically accessible to applications through the `android.os.Build` class. (Citation: Android-Build) iOS is much more restrictive with what information is visible to applications. Typically, applications will only be able to query the device model and which version of iOS it is running.

Name

System Network Configuration Discovery

ID

T1422

Description

Adversaries may look for details about the network configuration and settings, such as IP and/or MAC addresses, of operating systems they access or through information discovery of remote systems. On Android, details of onboard network interfaces are accessible to apps through the `java.net.NetworkInterface` class.(Citation: NetworkInterface) Previously, the Android `TelephonyManager` class could be used to gather telephony-related device identifiers, information such as the IMSI, IMEI, and phone number. However, starting with Android 10, only preloaded, carrier, the default SMS, or device and profile owner applications can access the telephony-related device identifiers.(Citation: TelephonyManager) On iOS, gathering network configuration information is not possible without root access. Adversaries may use the information from [System Network Configuration Discovery](https://attack.mitre.org/techniques/T1422) during automated discovery to shape follow-on behaviors, including determining certain access within the target network and what actions to do next.

Sector

Name
Finance
Description
Public and private entities involved in the allocation of assets and liabilities over space and time.
Name
Technologies
Description
Private entities related to the research, development, manufacturing and distribution of electronics, softwares, computers and products related to information technologies.

Indicator

Name

api.yumicash.com

Pattern Type

stix

Pattern

[hostname:value = 'api.yumicash.com']

Name

152.32.140.8

Description

ISP: UCLOUD INFORMATION TECHNOLOGY (HK) LIMITED **OS:** None ---------- Hostnames: - truenaira.co ---------- Domains: - truenaira.co ---------- Services: **443:** ``` HTTP/1.1 403 Forbidden Date: Sun, 26 Nov 2023 02:49:09 GMT Content-Type: text/html Content-Length: 548 Connection: keep-alive Server: nginx ``` HEARTBLEED: 2023/11/26 02:49:36 152.32.140.8:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '152.32.140.8']

Name

rest.bhvbhgvh.space

Pattern Type

stix

Pattern

[hostname:value = 'rest.bhvbhgvh.space']

Name

apitai.coccash.com

Pattern Type

stix

Pattern

[hostname:value = 'apitai.coccash.com']

Name

47.89.159.152

Description

ISP: Alibaba (US) Technology Co., Ltd. **OS:** None ---------- Hostnames: - goloannw.com - qtzhreop.com ---------- Domains: - goloannw.com - qtzhreop.com ---------- Services: **80:** ``` HTTP/1.1 200 OK Server: nginx Date: Tue, 05 Dec 2023 23:21:58 GMT Content-Type: text/html Content-Length: 1326 Last-Modified: Wed, 26 Apr 2017 08:03:47 GMT Connection: keep-alive Vary: Accept-Encoding ETag: "59005463-52e" Accept-Ranges: bytes ``` ---------- **443:** ``` HTTP/1.1 401 Unauthorized Server: nginx Date: Tue, 05 Dec 2023 05:31:22 GMT Content-Type: application/json;charset=utf-8 Content-Length: 109 Connection: keep-alive X-Content-Type-Options: nosniff Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET, POST, OPTIONS Access-Control-Allow-Headers: DNT,X-Mx-ReqToken,Keep-Alive,User-Agent,X-Requested-With,If-Modified-Since,Cache-Control,Content-Type,Authorization,X-DF-API-ID,X-DF-API-SECRET ``` HEARTBLEED: 2023/12/05 05:31:27 47.89.159.152:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '47.89.159.152']

Name

kk.softheartlend2.com

Pattern Type

stix

Pattern

[hostname:value = 'kk.softheartlend2.com']

Name

47.89.211.3

Description

ISP: Alibaba (US) Technology Co., Ltd. **OS:** Ubuntu ---------- Hostnames: - privacy.felizcartera.ltd - rest.bhvbhgvh.space - privacy.bhvbhgvh.space - bhvbhgvh.space.bhvbhgvh.space - rest.felizcartera.ltd ---------- Domains: - felizcartera.ltd - bhvbhgvh.space ---------- Services: **80:** ``` HTTP/1.1 200 OK Server: nginx/1.10.3 (Ubuntu) Date: Tue, 05 Dec 2023 17:17:06 GMT Content-Type: text/html Content-Length: 612 Last-Modified: Wed, 27 Oct 2021 03:15:58 GMT Connection: keep-alive ETag: "6178c46e-264" Accept-Ranges: bytes ``` ---------- **443:** ``` HTTP/1.1 404 Not Found Server: nginx/1.10.3 (Ubuntu) Date: Mon, 04 Dec 2023 17:36:47 GMT Content-Type: text/html Content-Length: 580 Connection: keep-alive ``` HEARTBLEED: 2023/12/04 17:36:56 47.89.211.3:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '47.89.211.3']

Name

43.225.143.80

Description

ISP: HUAWEI CLOUDS **OS:** None ---------- Hostnames: - ecs-43-225-143-80.compute.hwclouds-dns.com ---------- Domains: - hwclouds-dns.com ---------- Services: **80:** ``` HTTP/1.1 200 OK Server: nginx Date: Tue, 05 Dec 2023 12:18:51 GMT Content-Type: text/html Content-Length: 1326 Last-Modified: Wed, 26 Apr 2017 08:03:47 GMT Connection: keep-alive Vary: Accept-Encoding ETag: "59005463-52e" Accept-Ranges: bytes ``` ---------- **443:** ``` HTTP/1.1 302 Moved Temporarily Server: nginx Date: Fri, 01 Dec 2023 08:54:54 GMT Content-Type: text/html Content-Length: 138 Connection: close Location: https://43.225.143.80/ Strict-Transport-Security: max-age=31536000 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '43.225.143.80']

Name

hwpamjvk.whcashph.com

Pattern Type

stix

Pattern

[hostname:value = 'hwpamjvk.whcashph.com']

Name

mpx.mpxoptim.com

Pattern Type

stix

Pattern

[hostname:value = 'mpx.mpxoptim.com']

Name

47.56.128.251

Description

ISP: Alibaba (US) Technology Co., Ltd. **OS:** Ubuntu ---------- Hostnames: ---------- Domains: ---------- Services: **443:** ``` HTTP/1.1 400 Bad Request Server: nginx/1.10.3 (Ubuntu) Date: Thu, 30 Nov 2023 13:30:32 GMT Content-Type: text/html Content-Length: 682 Connection: close ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '47.56.128.251']

Name

eg.easycredit-app.com

Pattern Type

stix

Pattern

[hostname:value = 'eg.easycredit-app.com']

Name

www.credibusco.com

Pattern Type

stix

Pattern

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

Name

iu.iuuaufbt.com

Pattern Type

stix

Pattern

[hostname:value = 'iu.iuuaufbt.com']

Name

qt.qtzhreop.com

Pattern Type

stix

Pattern

[hostname:value = 'qt.qtzhreop.com']

Name

pss.aakredit.in

Pattern Type

stix

Pattern

[hostname:value = 'pss.aakredit.in']

Name

47.254.33.250

Description

ISP: Alibaba (US) Technology Co., Ltd. **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **80:** ``` HTTP/1.1 200 OK Server: nginx Date: Tue, 21 Nov 2023 07:24:31 GMT Content-Type: text/html Content-Length: 1326 Last-Modified: Wed, 26 Apr 2017 08:03:47 GMT Connection: keep-alive Vary: Accept-Encoding ETag: "59005463-52e" Accept-Ranges: bytes ``` ---------- **443:** ``` HTTP/1.1 302 Moved Temporarily Server: nginx Date: Thu, 30 Nov 2023 15:43:26 GMT Content-Type: text/html Content-Length: 138 Connection: close Location: https://47.254.33.250/ Strict-Transport-Security: max-age=31536000 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '47.254.33.250']

Name

ag.ahymvoxxg.com

Pattern Type

stix

Pattern

[hostname:value = 'ag.ahymvoxxg.com']

Name

110.238.85.186

Description

ISP: HUAWEI CLOUDS **OS:** None ---------- Hostnames: - ecs-110-238-85-186.compute.hwclouds-dns.com ---------- Domains: - hwclouds-dns.com ---------- Services: **80:** ``` HTTP/1.1 404 Not Found Date: Wed, 06 Dec 2023 12:22:23 GMT Content-Type: text/plain; charset=utf-8 Content-Length: 21 Connection: keep-alive ``` ---------- **443:** ``` HTTP/1.1 400 Bad Request Date: Thu, 30 Nov 2023 21:18:18 GMT Content-Type: text/html Content-Length: 650 Connection: close ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '110.238.85.186']

Name

47.91.110.22

Description

CC=AE ASN=AS45102 Alibaba US Technology Co., Ltd.

Pattern Type

stix

Pattern

[ipv4-addr:value = '47.91.110.22']

Name

cy.amorcash.com

Pattern Type

stix

Pattern

[hostname:value = 'cy.amorcash.com']

Name

47.253.175.81

Description

ISP: Alibaba (US) Technology Co., Ltd. **OS:** None ---------- Hostnames: - rapidomo.com - oyeqctus.com ---------- Domains: - rapidomo.com - oyeqctus.com ---------- Services: **80:** ``` HTTP/1.1 200 OK Server: nginx Date: Mon, 04 Dec 2023 01:20:31 GMT Content-Type: text/html Content-Length: 1326 Last-Modified: Wed, 26 Apr 2017 08:03:47 GMT Connection: keep-alive Vary: Accept-Encoding ETag: "59005463-52e" Accept-Ranges: bytes ``` ---------- **443:** ``` HTTP/1.1 401 Unauthorized Server: nginx Date: Sat, 02 Dec 2023 17:54:15 GMT Content-Type: application/json;charset=utf-8 Content-Length: 109 Connection: keep-alive X-Content-Type-Options: nosniff Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET, POST, OPTIONS Access-Control-Allow-Headers: DNT,X-Mx-ReqToken,Keep-Alive,User-Agent,X-Requested-With,If-Modified-Since,Cache-Control,Content-Type,Authorization,X-DF-API-ID,X-DF-API-SECRET ``` HEARTBLEED: 2023/12/02 17:54:21 47.253.175.81:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '47.253.175.81']

Name

47.253.49.18

Description

ISP: Alibaba (US) Technology Co., Ltd. **OS:** None ---------- Hostnames: - optimaca.com - mpxoptim.com ---------- Domains: - optimaca.com - mpxoptim.com ---------- Services: **80:** ``` HTTP/1.1 200 OK Server: nginx Date: Mon, 04 Dec 2023 01:06:54 GMT Content-Type: text/html Content-Length: 1326 Last-Modified: Wed, 26 Apr 2017 08:03:47 GMT Connection: keep-alive Vary: Accept-Encoding ETag: "59005463-52e" Accept-Ranges: bytes ``` ---------- **443:** ``` HTTP/1.1 404 Not Found Server: nginx Date: Sat, 02 Dec 2023 20:29:34 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 1561 Connection: keep-alive Vary: Accept-Encoding X-XSS-Protection: 0 X-Frame-Options: SAMEORIGIN X-Content-Type-Options: nosniff Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '47.253.49.18']

Name

la6gd.cashwow.club

Pattern Type

stix

Pattern

[hostname:value = 'la6gd.cashwow.club']

Name

49.0.193.223

Description

ISP: HUAWEI CLOUDS **OS:** None ------------------------- Hostnames: - borrowconfidencemm.com - ecs-49-0-193-223.compute.hwclouds-dns.com ------------------------- Domains: - hwclouds-dns.com - borrowconfidencemm.com ------------------------- Services: **80:** ``` HTTP/1.1 200 OK Server: nginx Date: Fri, 01 Dec 2023 16:51:07 GMT Content-Type: text/html Content-Length: 1326 Last-Modified: Wed, 26 Apr 2017 08:03:47 GMT Connection: keep-alive Vary: Accept-Encoding ETag: "59005463-52e" Accept-Ranges: bytes ``` ----------------- **443:** ``` HTTP/1.1 200 OK Server: nginx Date: Mon, 04 Dec 2023 04:46:48 GMT Content-Type: text/html Content-Length: 91332 Last-Modified: Tue, 19 Sep 2023 07:13:42 GMT Connection: keep-alive Vary: Accept-Encoding ETag: "65094a26-164c4" Strict-Transport-Security: max-age=31536000 Accept-Ranges: bytes ``` HEARTBLEED: 2023/12/04 04:47:16 49.0.193.223:443 - SAFE -----------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '49.0.193.223']

Name

9eb13898532f4521961c5a5a1382cd0b96dfe40196371628b1792678b900b6db

Description

SHA256 of 0951252e7052ab86208b4f42eb61fc40ca8a6e29

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9eb13898532f4521961c5a5a1382cd0b96dfe40196371628b1792678b900b6db']

Name

www.guayabacash.com

Pattern Type

stix

Pattern

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

Name

oy.oyeqctus.com

Pattern Type

stix

Pattern

[hostname:value = 'oy.oyeqctus.com']

Country

Name
India
Name
Egypt
Name
Nigeria
Name
Peru
Name
Colombia
Name
Philippines
Name
Viet Nam

Name
Kenya
Name
Pakistan
Name
Singapore
Name
Mexico
Name
Indonesia
Name
Thailand

Region

Name
Asia
Name
Sub-Saharan Africa
Name
Northern Africa
Name
Africa
Name
Southern Asia
Name
Americas
Name
Latin America and the Caribbean

Name
South-eastern Asia

Malware

Name
SpyLoan

Name
KreditSpy

StixFile

Value
9eb13898532f4521961c5a5a1382cd0b96dfe40196371628b1792678b900b6db

Hostname

Value
la6gd.cashwow.club
oy.oyeqctus.com
pss.aakredit.in
api.yumicash.com
kk.softheartlend2.com
cy.amorcash.com
apitai.coccash.com
iu.iuuaufbt.com
hwpamjvk.whcashph.com
eg.easycredit-app.com
rest.bhvbhgvh.space
ag.ahymvoxxg.com
www.guayabacash.com

www.credibusco.com

qt.qtzhreop.com

mpx.mpxoptim.com

IPv4-Addr

Value
47.91.110.22
47.56.128.251
152.32.140.8
110.238.85.186
47.253.49.18
47.254.33.250
47.89.159.152
43.225.143.80
47.89.211.3
49.0.193.223
47.253.175.81

External References

- https://otx.alienvault.com/pulse/657085f982e8bd03f9491513
- https://www.welivesecurity.com/en/eset-research/beware-predatory-fintech-loan-sharks-use-android-apps-reach-new-depths/