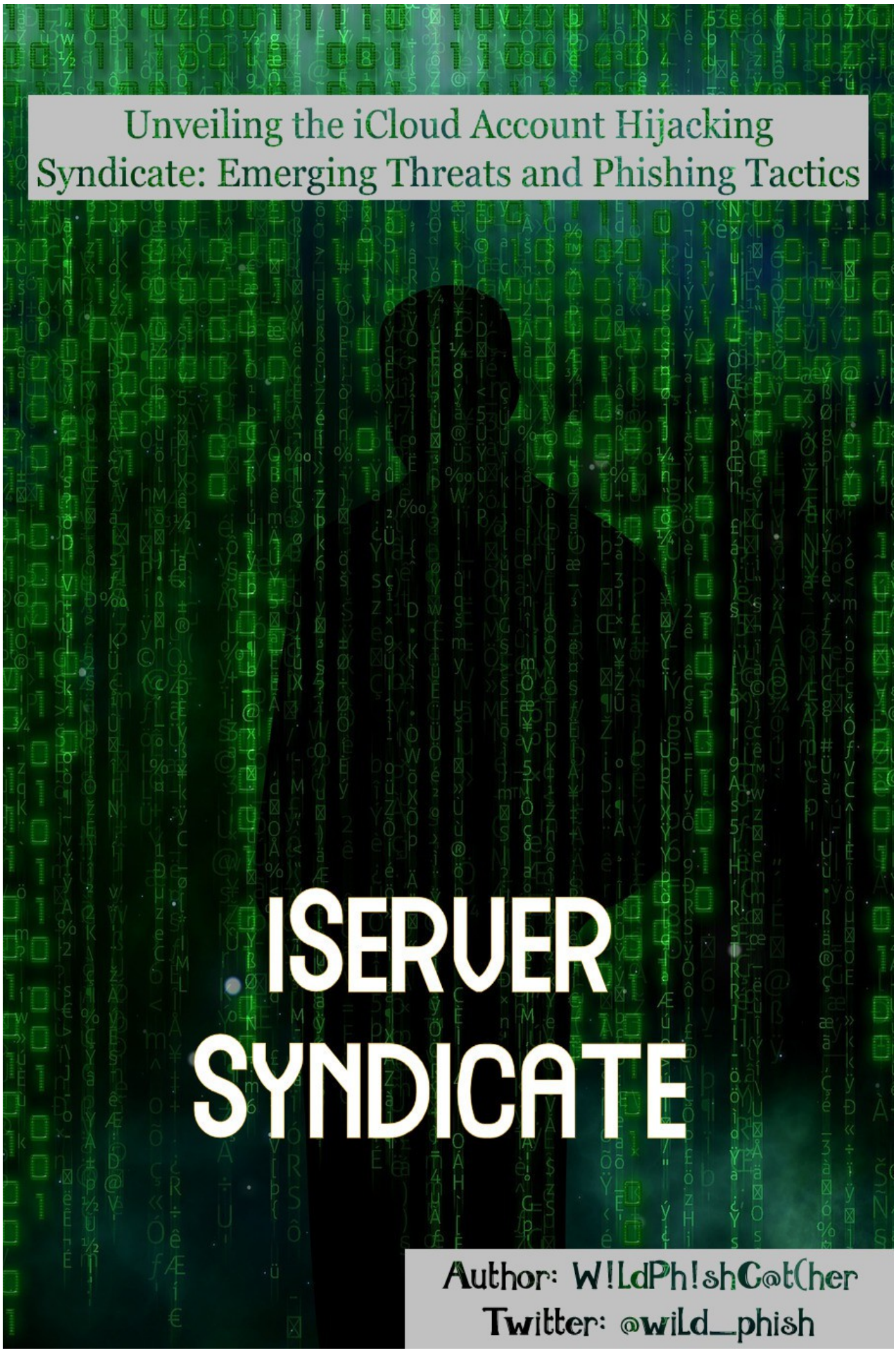

Unveiling the iCloud Account Hijacking Syndicate: Emerging Threats and Phishing Tactics
ISERVER SYNDICATE
Author: W!LdPh!shC@tCher
Twitter: @wiLd_phish

Executive Summery

This threat report sheds light on a significant increase in domain registrations related to Apple and iCloud phishing activities observed since the beginning of 2022. Our investigation aimed to identify the individuals or groups behind this surge and uncover their intentions. During our research, we uncovered the existence of a well-established syndicate that has been actively involved in these malicious activities since 2022. Moreover, we have gathered substantial evidence indicating that the syndicate has expanded its operations to include the hijacking of iCloud accounts. This report provides crucial insights into the tactics employed by this threat syndicate and the potential risks posed to individuals and organizations relying on iCloud services.

During our investigation, a notable observation emerged regarding the consistent usage of the term "iServer" in various aspects of the syndicate's activities. This recurring pattern led us to designate this threat group as the "iServer Syndicate." The syndicate strategically employs the term "iServer" in its promotional materials, as well as in the nomenclature of its command and control (C2) servers. This naming convention not only serves as an identifier but also provides insight into the syndicate's self-perception and branding strategy. By referring to the threat group as the "iServer Syndicate," we aim to capture the distinctive essence of their operations and emphasize their focus on leveraging the concept of an interconnected server infrastructure to facilitate their malicious activities.

The iServer syndicate operates based on an Infrastructure-as-a-Service (IaaS) model, which offers a convenient and all-inclusive solution for various phishing-related activities. Their infrastructure provides threat actors with a comprehensive platform, allowing them to focus solely on their phishing campaigns, while iServer takes care of the operational aspects.

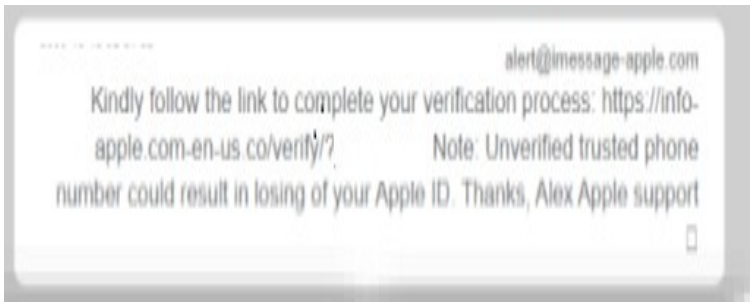
The iServer panel offers a range of services and features that cater to the needs of threat actors engaged in phishing campaigns. This includes the provision of new domains specifically for phishing purposes, eliminating the need for threat actors to independently acquire domains through traditional channels. Additionally, the iServer platform facilitates the distribution of phishing campaigns through multiple channels, such as email and SMS, enabling threat actors to reach a broader target audience.

One of the notable advantages of the iServer platform is its comprehensive support system. The syndicate's support team ensures that threat actors receive assistance and guidance throughout their phishing campaigns, alleviating any concerns or technical challenges they may encounter. By providing a one-stop solution and offering robust support, iServer streamlines the phishing process, making it more accessible and efficient for threat actors.

Introduction

The genesis of this investigation can be traced back to a significant event that occurred when a direct message (DM) landed in my inbox, containing compelling evidence that piqued my interest as a dedicated security researcher. The DM, purportedly from Apple Support, caught my attention due to its urgent tone and the clear indication that a threat actor was masquerading as a representative from a reputable entity.

Recognizing the potential severity of this incident, I embarked on a meticulous investigation to uncover the true nature of the threat and identify the individuals or group responsible for this deceptive scheme. It was evident from the evidence presented in the DM that the threat actor had intentions aligned with compromising the security of iCloud accounts, raising concerns about the vulnerability of unsuspecting users.



Modus Operandi

During our investigation, a striking pattern emerged in the infrastructure utilized by the syndicate. It was observed that the syndicate consistently relied on a limited number of IP addresses to support their operations for a specific duration, typically spanning several months. This practice allowed them to maintain a level of continuity while minimizing their footprint. Additionally, the syndicate adopted the use of Content Delivery Network (CDN) technology, leveraging shared services and occasionally acquiring dedicated virtual private servers (VPS) to further obfuscate their IP addresses and ensure operational security.

Furthermore, our findings revealed that the syndicate employed an extensive network of domains to serve their nefarious purposes. The sheer volume of domains utilized by the syndicate was unprecedented, indicating a deliberate effort to establish a robust infrastructure for their illicit activities.

The purpose of this report is to provide a comprehensive analysis that transcends individual domain incidents, allowing us to discern the patterns, tactics, and strategies employed by the syndicate. By examining the syndicate's operations holistically, we can gain a deeper understanding of their overall impact and the potential risks they pose to individuals and organizations.

Individual reports of phishing domains being marked as such may be seen as isolated events, this report aims to connect the dots and reveal the interconnected nature of the syndicate's activities. By presenting the bigger picture of this emerging threat, we can provide valuable insights into their operations, methodologies, and geographic targeting. This broader perspective enables stakeholders to grasp the magnitude and severity of the syndicate's activities and take appropriate measures to mitigate the risks associated with their malicious campaigns.

By consolidating the knowledge gained from various reported incidents and combining it with our own investigative findings, this report strives to shed light on the larger implications of the syndicate's activities. It is through this comprehensive approach that we can effectively counter the evolving threat landscape and safeguard against the pervasive nature of this emerging threat.

Our investigation also uncovered the presence of various malware hosted within the syndicate's infrastructure, for the sake of simplicity and focus, we have chosen to

present only the evidence related to phishing activities. Phishing remains the syndicate's primary modus operandi, demonstrating their heavy reliance on deceptive techniques to exploit unsuspecting individuals.

By concentrating on the phishing-related evidence, this investigation aims to provide a clear and concise overview of the syndicate's activities and shed light on their elaborate phishing operations.

In 2017, an insightful report published by KrebsOnSecurity shed light on a particular aspect of the syndicate we are currently investigating. The report, while significant in its own right, primarily focused on a relatively small-scale operation within the larger syndicate's activities.

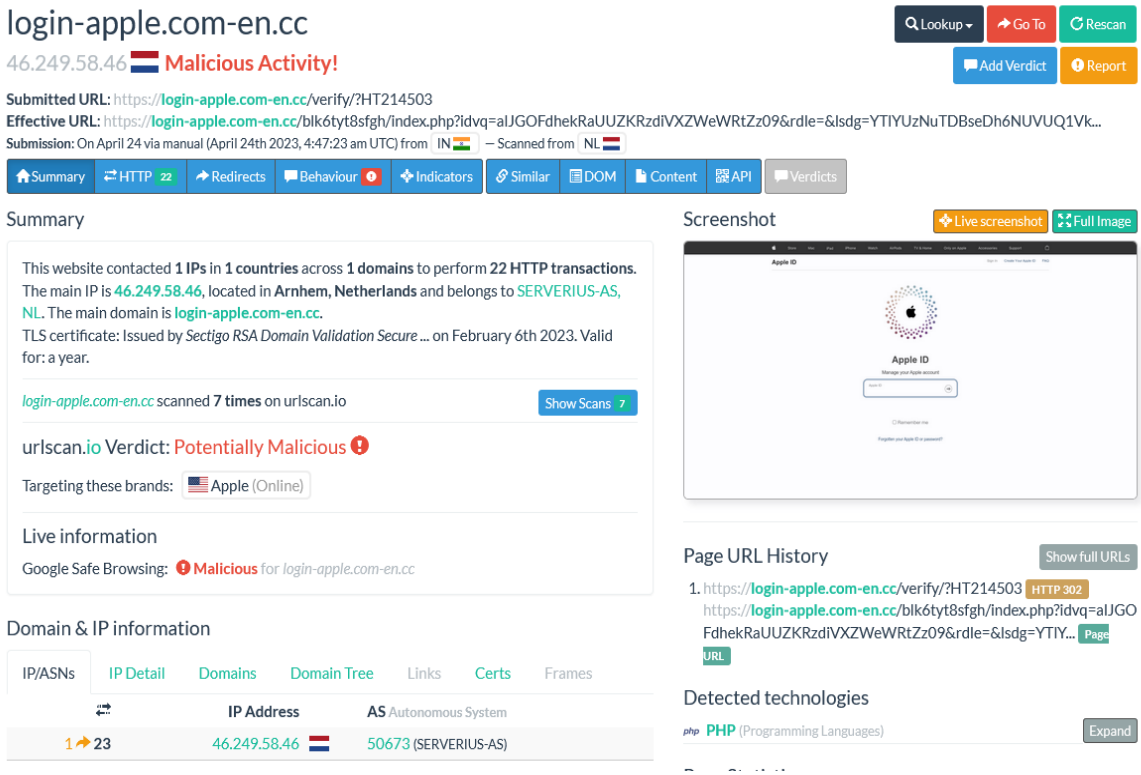
While the KrebsOnSecurity report provided valuable insights into the syndicate's operations during that specific period, it is important to recognize that the threat landscape is constantly evolving. Since 2017, the syndicate has expanded its operations, refined its tactics, and potentially adopted more sophisticated techniques.

This current investigation seeks to build upon the foundational knowledge shared in the KrebsOnSecurity report, delving deeper into the syndicate's activities, modus operandi, and infrastructure. By examining the larger scope of their operations, we can develop a more comprehensive understanding of the syndicate's growth, impact, and the potential risks it poses.

https://krebsonsecurity.com/2017/03/if-your-iphone-is-stolen-these-guys-may-try-to-iphish-you/

Key Finding's

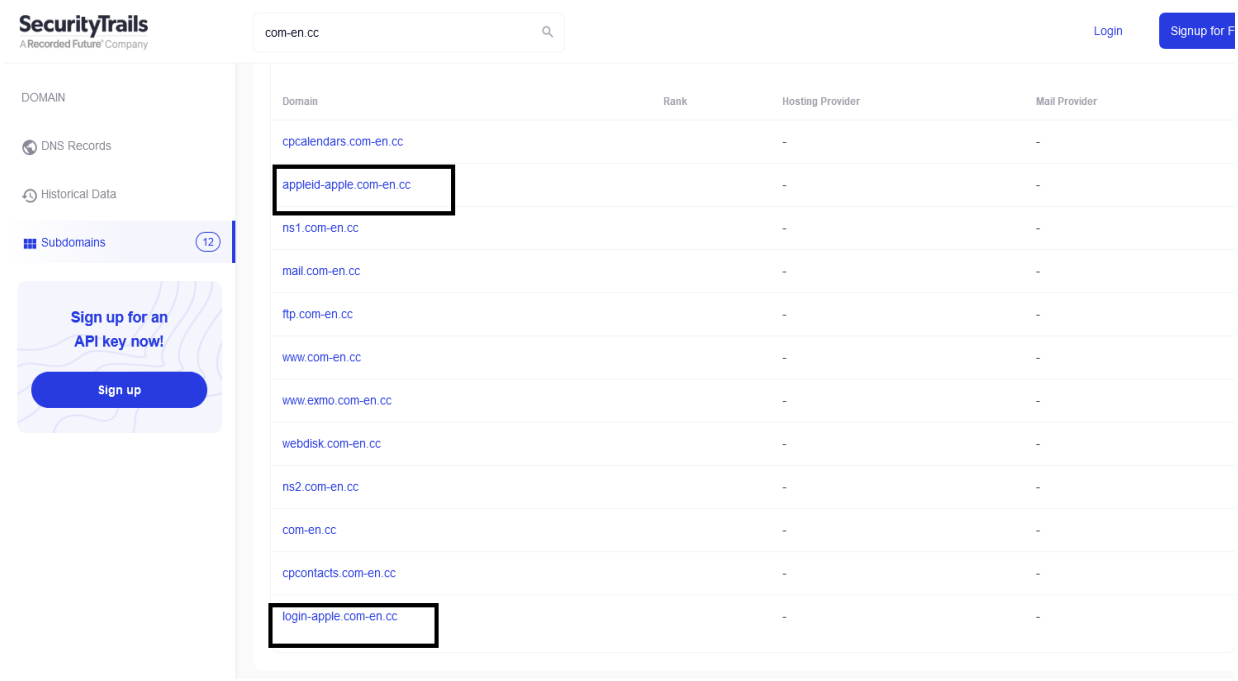
While investigating the link redirect to icloud phishing page with the url **https://login-apple.com-en.cc/blk6tyt8sfgh/index.php?idvq=alJGOFdhekRaUUZKRzdiVXZWeWRtZz09&rdle=&lsdg=YTlYUzNuTDBseDh6NUVUQ1VkZ0dJQT09&adsw=&ctr=QzBXOVJ1TGdmTWFNTURKOTNkK2pSQT09**

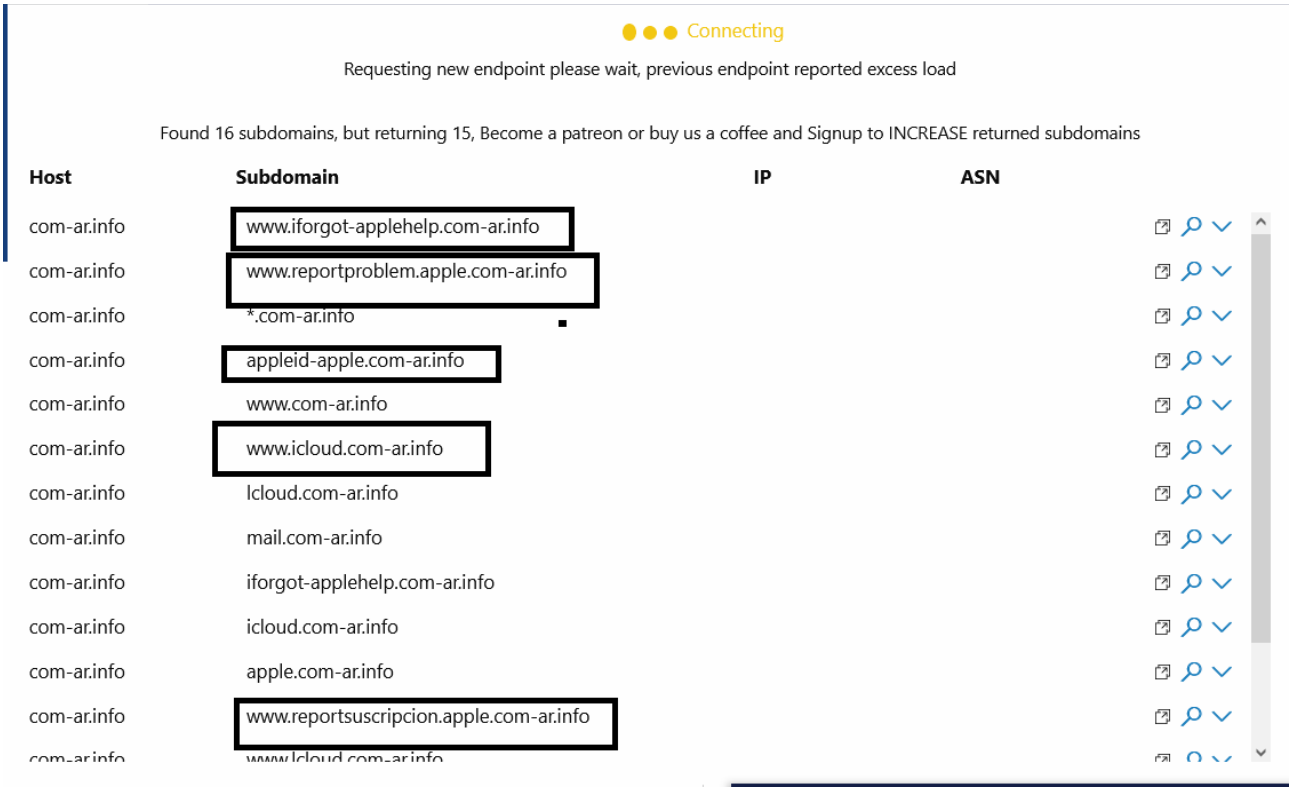


After further investigation we found multiple Phishing pages on same domain

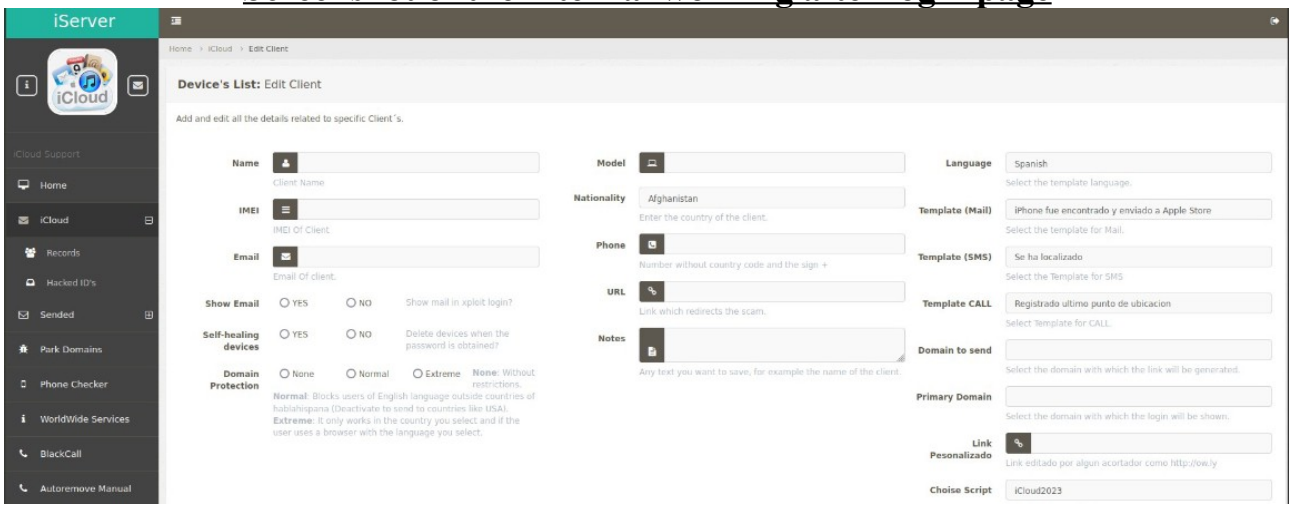
ShortURL	FullURL
http://appleid-apple.com-en.cc/verify/?HT203541	https://appleid-apple.com-en.cc/blk678sfgh/index.php?idvq=Qm5lc1NQckZTbTJvUzZVekpBQkYxZz09&rdle=&lsdg=UEkxMDBGdU1Xb2hXZC84ZjA0YW5ZUT09&adsw=&ctr=OU5sN0lOcm9lcXB3OEFRVGxBeWltdz09
https://login-apple.com-en.cc/verify/?HT214503	https://login-apple.com-en.cc/blk6tyt8sfgh/index.php?idvq=alJGOFdhekRaUUZKRzdiVXZWeWRtZz09&rdle=&lsdg=YTlYUzNuTDBseDh6NUVUQ1VkZ0dJQT09&adsw=&ctr=QzBXOVJ1TGdmTWFNTURKOTNkK2pSQT09
https://login-apple.com-en.cc/verify/?HT245130	https://login-apple.com-en.cc/blk6tyt8sfgh/index.php?idvq=NC9vVFl0aVBvOFpSbmFOc3FzaURHQT09&rdle=&lsdg=czJybS8xVWFZMndPT3VzQVNCclNMUT09&adsw=&ctr=QzBXOVJ1TGdmTWFNTURKOTNkK2pSQT09
https://login-apple.com-en.cc/verify/?HT321504	https://login-apple.com-en.cc/blk6tyt8sfgh/index.php?idvq=VEhtRVRhcTlqelJhaG84TnptV0RPUT09&rdle=&lsdg=&adsw=&ctr=d1BhSlNQQzI0V0gzMkxYL1NPUWJSWU5BK2k1RnBDNDBKbDFMTDhIb0o1TT0=
https://login-apple.com-en.cc/verify/?HT342510	https://login-apple.com-en.cc/blk6tyt8sfgh/index.php?idvq=ZGovSDJWc2J6UVpyRjU2RVRkdFdHUT09&rdle=&lsdg=UmU5QW9RS0hJRXdoNnRHVWVFQmRqUT09&adsw=&ctr=OU5sN0lOcm9lcXB3OEFRVGxBeWltdz09
https://login-apple.com-en.cc/verify/?HT504321	https://login-apple.com-en.cc/wid86764fgh/index.php?idvq=Rm1jRzBRamJVaG14YUdsaE54cEF4bzZnTFIvMWIzM2w0RjNrdUVWN1cvND0=&rdle=&lsdg=NWY3TUd3cmtoQVVLb2NTU0FuemxXQT09&adsw=&ctr=d1BhSlNQQzI0V0gzMkxYL1NPUWJSWU5BK2k1RnBDNDBKbDFMTDhIb0o1TT0=
https://login-apple.com-en.cc/verify/?HT534201	https://login-apple.com-en.cc/blk6tyt8sfgh/index.php?idvq=bDU0aDdnS1RtSHhJWnNmbDArQkVQUT09&rdle=&lsdg=YTlYUzNuTDBseDh6NUVUQ1VkZ0dJQT09&adsw=&ctr=d1BhSlNQQzI0V0gzMkxYL1NPUWJSWU5BK2k1RnBDNDBKbDFMTDhIb0o1TT0=

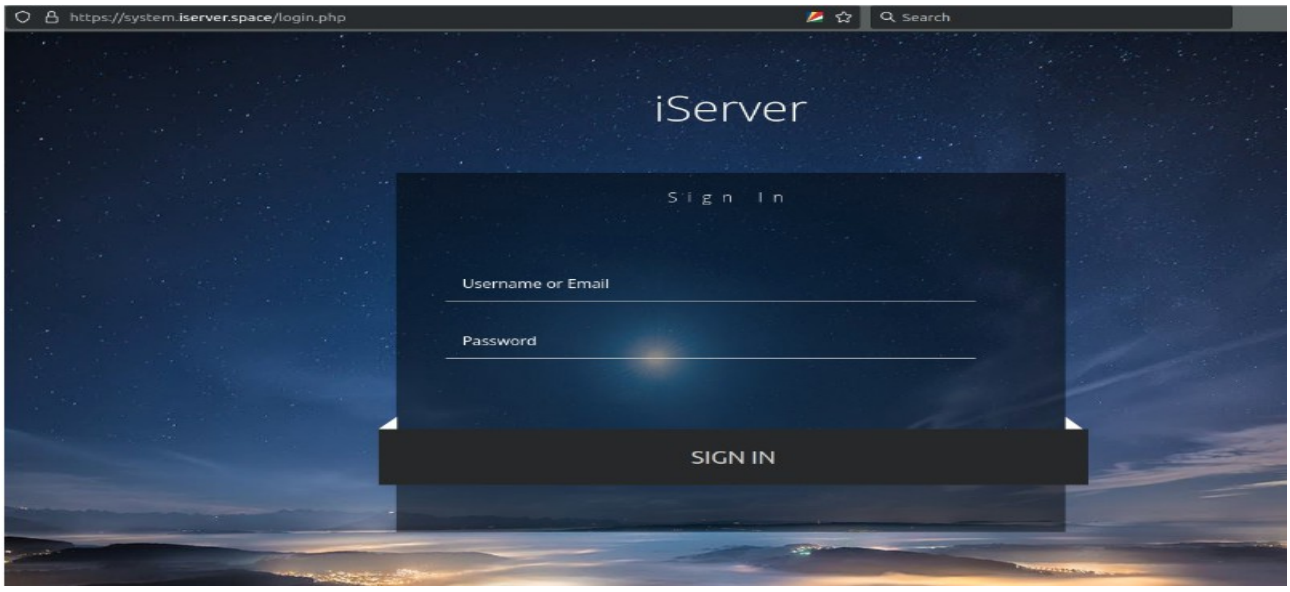
ShortURL	FullURL
https://appleid-apple.com-ar.info/verify/?HT015432	https://appleid-apple.com-ar.info/blk932hdb882/index?idvq=dStQNkdaSG9GdmYvb1VLb25xSnhVdz09&rdle=&lsdg=dDlRNmlpVUZxekphQUFFSlBnOUtqdz09&adsw=&ctr=SXhhT2xiZU5LZEN6ZWZ2blZSQXE5Zz09

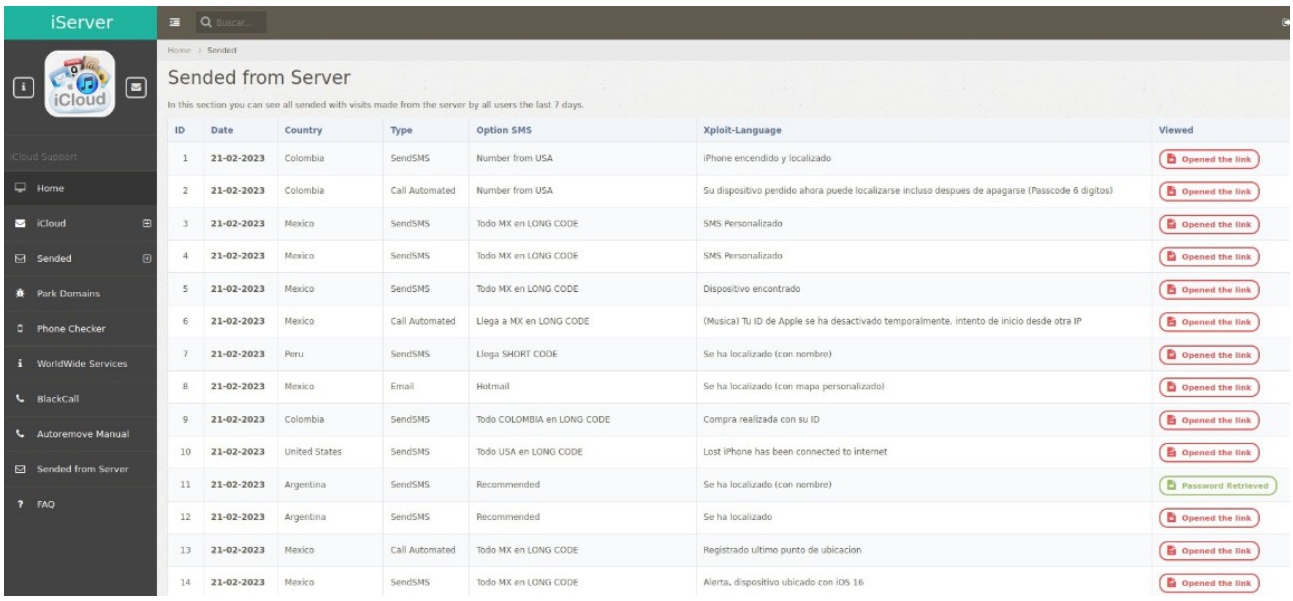




Screenshot of the internal working after login page







https://system.iserver.space/test.php

Search

TinyURL was created!

The following URL:

https://id-icloudapple.com/?c9lfh

has a length of 33 characters and resulted in the following TinyURL which has a length of 28 characters:

https://tinyurl.com/y93afa93
[Open in new window] [Copy to clipboard]

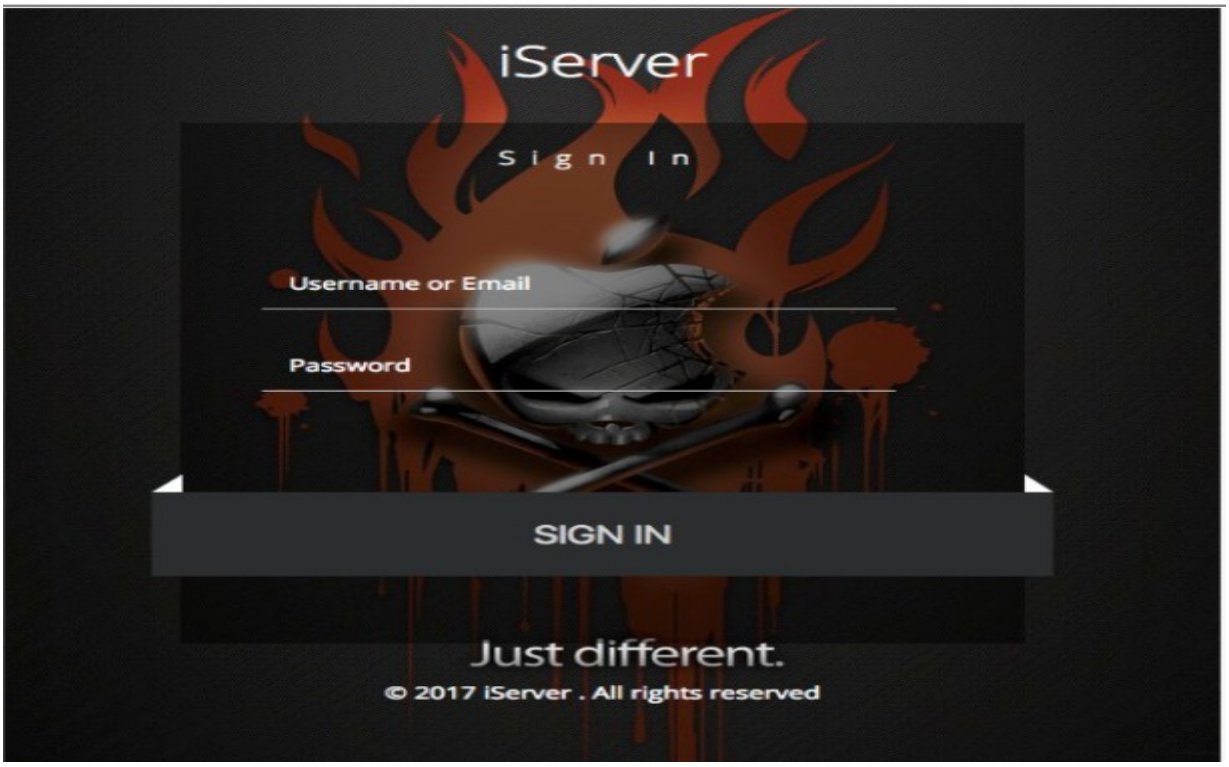
Or, give your recipients confidence with a preview TinyURL:

https://preview.tinyurl.com/y93afa93
[Open in new window]

How to copy and paste the TinyURL: *To copy the TinyURL to your clipboard, right click the link under the TinyURL and select the copy link location option. To paste the TinyURL into a document, press Ctrl and V on your keyboard, or select "paste" from the edit menu of the program you are using.*

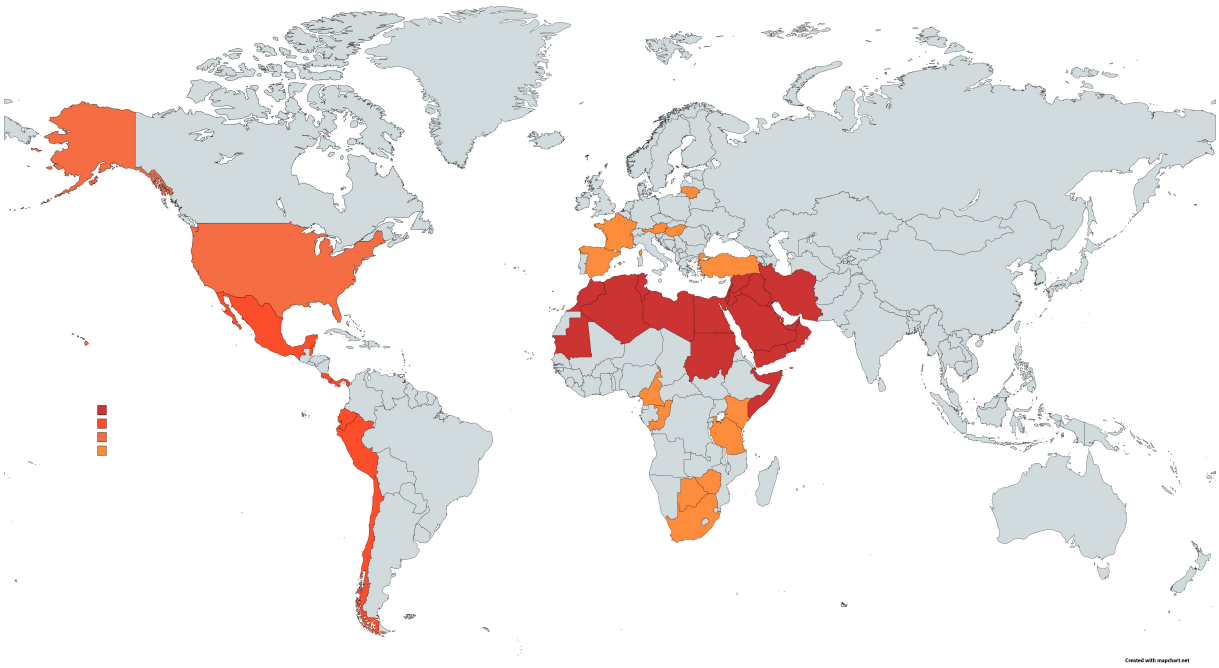
Enter a long URL to make tiny:
Make TinyURL!

Custom alias (optional):
https://tinyurl.com/
May contain letters, numbers, and dashes.



After conducting an extensive analysis of the linked IP addresses and domains, we quickly realized that the scale of this investigation exceeded our initial expectations. The findings revealed a staggering number of over 10000 domains associated with the same infrastructure, along with the identification of more than 40 IP addresses dedicated to facilitating the syndicate's illicit activities. For a comprehensive understanding of the infrastructure employed by the syndicate, we encourage readers to refer to the dedicated section on infrastructure within this report.

Target Countries



Target Geolocation: The iCloud account hijacking syndicate operates on a global scale, targeting individuals and organizations worldwide. However, our investigations have revealed specific regions where their activities are particularly prominent. The syndicate shows significant activity in the following geolocations:

a) **Middle East**: The syndicate has a notable presence in the Middle East, with a focus on countries such as Saudi Arabia, United Arab Emirates, Qatar, and Kuwait. The region's economic prosperity and high smartphone penetration make it an attractive target for iCloud-related scams.

b) **Africa**: The syndicate has extended its operations to various countries across Africa, including Nigeria, South Africa, Kenya, and Egypt. This expansion can be attributed to the increasing adoption of Apple products and the growing digital landscape in these regions.

c) **South America**: The syndicate has been actively targeting countries in South America, with a particular emphasis on Brazil, Argentina, Colombia, and Chile. The region's large population, rapid internet penetration, and thriving online commerce create ample opportunities for the syndicate to exploit unsuspecting iCloud users.

d) **Europe**: While the syndicate's operations in Europe are more limited compared to other regions, there have been reports of their activities in select countries, such as the United Kingdom, Germany, Spain, and Italy. The affluent user base and widespread use of Apple devices in these countries make them attractive targets.

It is important to note that while these regions have experienced higher levels of syndicate activity, iCloud users worldwide should remain vigilant as the syndicate may expand its reach to other geolocations over time.

Our investigation into the iCloud account hijacking syndicate has uncovered compelling evidence suggesting that their infrastructure setup is specifically designed to target iCloud accounts of individuals and organizations in Middle Eastern countries. The syndicate's operations in this region exhibit a higher level of sophistication and customization, indicating a deep understanding of the targeted audience and their online behaviors.

Generic iCloud Password Reset Tactics:

The syndicate employs various generic tactics to initiate iCloud password reset attempts, with the intention of gaining unauthorized access to accounts. These tactics typically involve creating scenarios that trigger suspicion or urgency in the target's mind, compelling them to take immediate action. Two common tactics employed by the syndicate include:

a) **Suspicious Login Detected**: The syndicate sends phishing emails or SMS messages to potential victims, claiming that suspicious login activity has been detected on their iCloud account. The message urges the recipient to click on a provided link to verify their account information or change their password to secure their account. In reality, this link leads to a fraudulent website designed to capture the victim's login credentials.

b) **Verify Your Trusted Number or Apple ID Phone Number**: Another tactic used by the syndicate involves sending messages that request users to verify their trusted phone number or Apple ID phone number. The message typically warns that failure to verify the phone number may result in the suspension or termination of the iCloud account. Victims are directed to a counterfeit verification page where they unwittingly provide their personal information, including their iCloud login credentials.

These tactics exploit users' concern for the security of their accounts and their desire to protect their personal information. The syndicate capitalizes on the sense of urgency and trust associated with official Apple notifications, creating an illusion of legitimacy to deceive unsuspecting victims.

Multiple Communication Channels Exploited:

The syndicate employs a multi-channel approach, utilizing various communication platforms to conduct their iCloud password reset phishing

campaigns. In addition to email and SMS, they have expanded their tactics to target users through iMessage and instant messaging (IM) applications. By diversifying their channels, the syndicate increases their chances of reaching potential victims and amplifying their success rate. The following are examples of how they exploit these communication channels:

a) **iMessage**: The syndicate leverages iMessage, Apple's proprietary instant messaging service, to send phishing messages directly to iCloud users' Apple devices. These messages mimic official notifications from Apple, informing users of a detected security breach or suspicious activity on their iCloud account. The messages prompt users to click on a link or reply with their login credentials to verify their account, ultimately providing the syndicate with unauthorized access.

b) **Instant Messaging (IM)**: Recognizing the widespread use of instant messaging applications, the syndicate utilizes popular platforms such as WhatsApp, Telegram, or Facebook Messenger to distribute phishing messages. These messages often employ social engineering techniques, creating a sense of urgency or offering enticing rewards to entice users to click on malicious links or provide their iCloud account information.

By exploiting these additional communication channels, the syndicate maximizes their reach and increases the likelihood of successful phishing attempts. Users must exercise caution when interacting with messages received through iMessage or IM applications, ensuring they verify the legitimacy of any requests before sharing sensitive information or clicking on suspicious links.

Fake Apple Websites and Domains:

To establish a sense of authenticity and credibility, the syndicate has created a network of fake Apple websites and domains that closely mimic legitimate Apple platforms. These malicious websites often use SSL certificates and employ tactics to make them appear trustworthy. Unsuspecting victims are lured to these sites through carefully crafted phishing emails, advertisements, or malicious links, where they are prompted to enter their iCloud login information. The syndicate's infrastructure ensures a seamless user experience while covertly capturing sensitive login credentials.

Command and Control (C2) Infrastructure:

The syndicate operates a sophisticated command and control infrastructure to manage their malicious activities and exfiltrate stolen iCloud account data. This infrastructure comprises a network of shared hosting and dedicated vps across

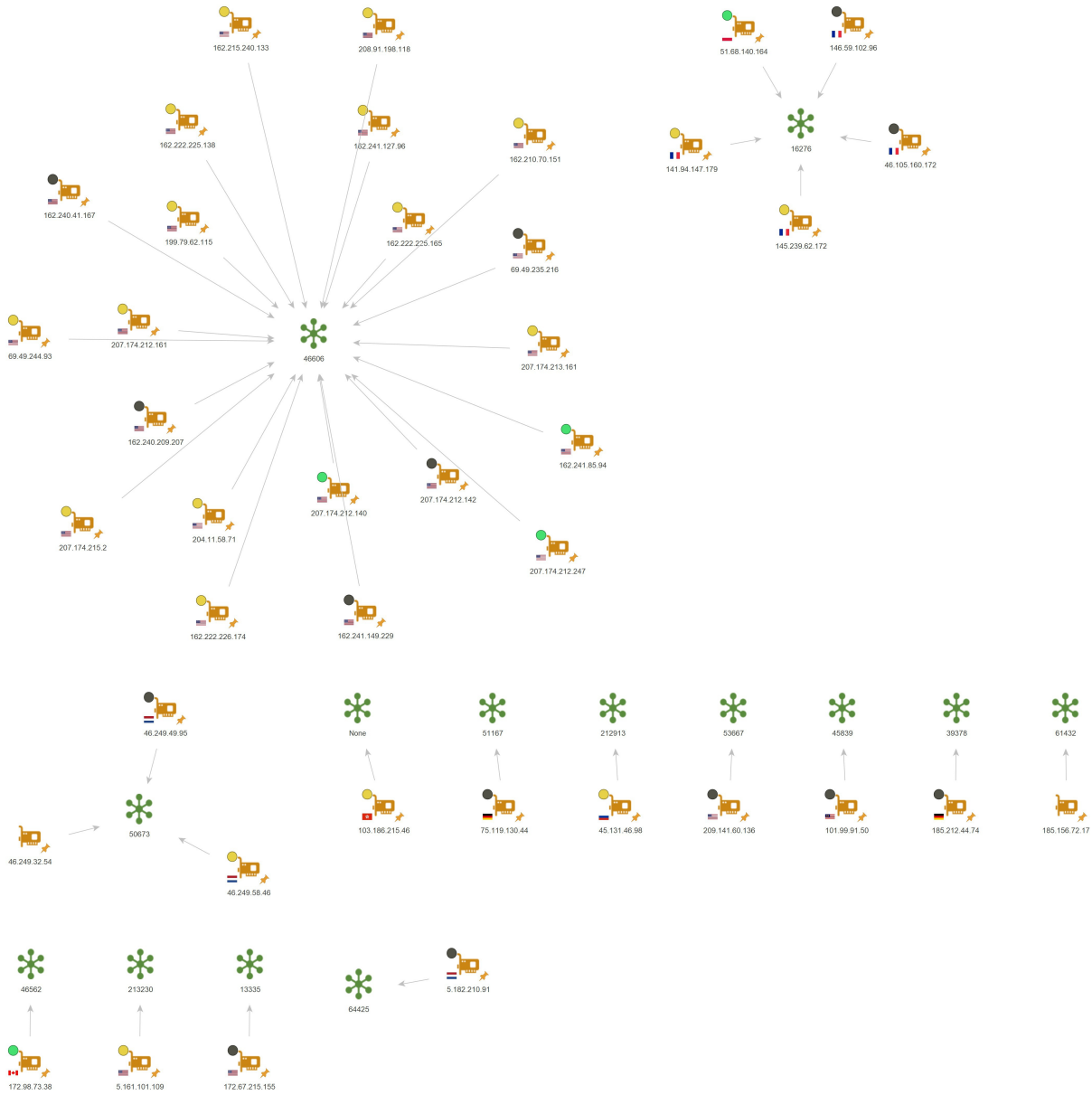
different countries, making it challenging to trace back to the syndicate's operations. These compromised servers act as intermediaries for command dissemination, data exfiltration, and communication with the syndicate's operators.

Proxy and VPN Services:

To further obfuscate their activities and evade detection, the syndicate employs proxy and virtual private network (VPN) services. These services allow them to hide their true geographic location, making it difficult for law enforcement agencies and cybersecurity researchers to pinpoint their exact origins. By routing their traffic through multiple proxy servers and VPN nodes, the syndicate ensures anonymity and increased operational security.

The syndicate's infrastructure setup, tailored phishing campaigns, and usage of proxy and VPN services highlight their strategic approach in targeting iCloud accounts of Middle Eastern countries. It is crucial for users and organizations in the region to be aware of these tactics and employ proactive security measures, such as multi-factor authentication and user awareness training, to mitigate the risk of falling victim to these targeted attacks.

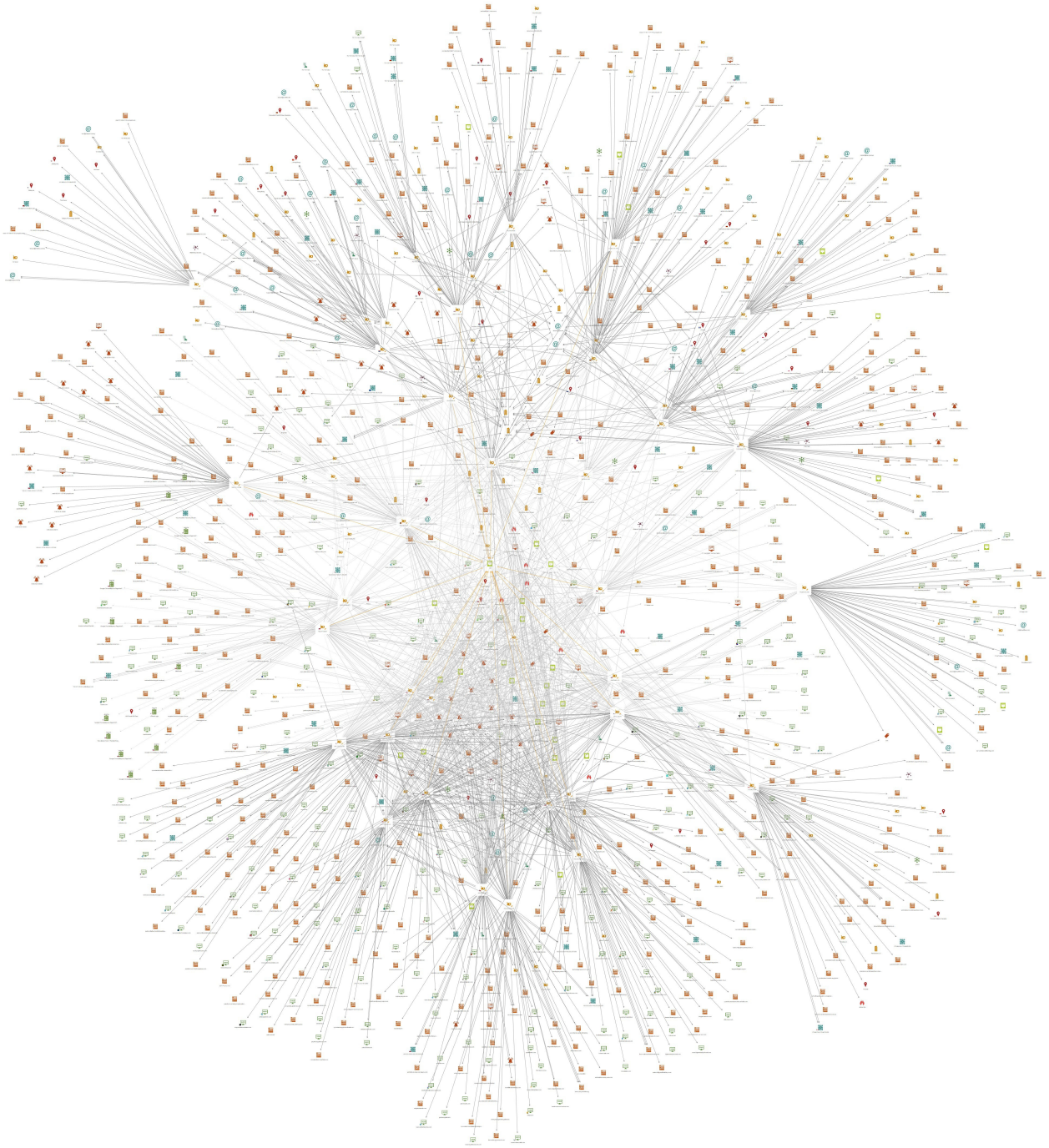
Infrastructure

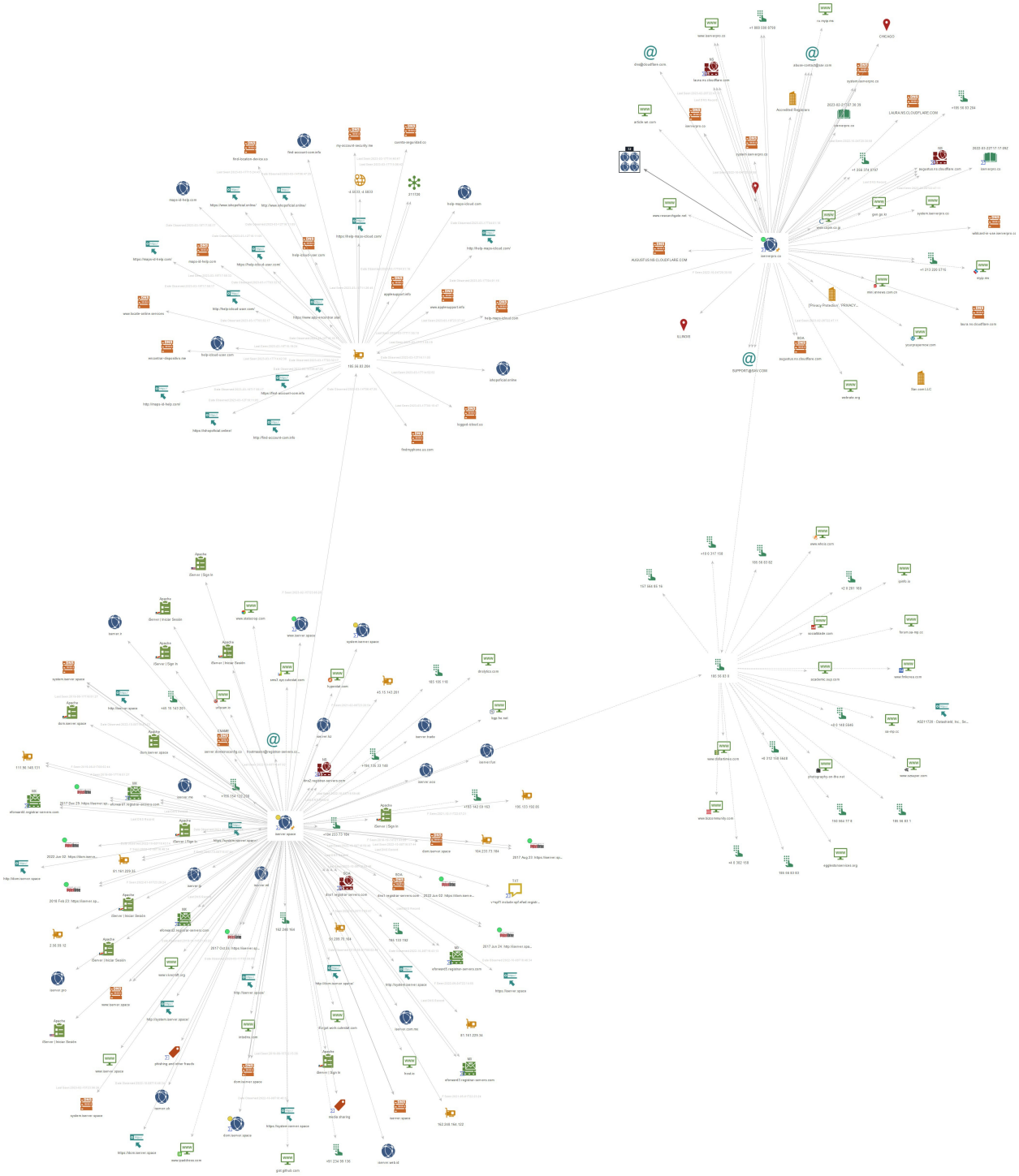


Infrastructure used by this syndicate

The high volume of registered domains and their continued operation, despite detection and reporting, can be attributed to the sophisticated architecture and methodology employed by the iServer syndicate. One notable aspect of their operations is the utilization of Telegram for notifications. When any suspicious activity or unauthorized access is detected, which deviates from their intended targets, users within the syndicate are promptly alerted. This immediate notification allows them to swiftly react and close any exposed subdomains or links that may compromise their activities.

This Telegram-based notification system exemplifies the advanced techniques employed by the syndicate. It showcases their ability to adapt and respond rapidly to potential threats, ensuring the longevity and resilience of their infrastructure. While this is just one technique among many employed by the syndicate, it highlights their sophistication and underscores the need for proactive countermeasures.





Few Panels which are discoved hosted on the same IOCs

gatox-unlock.com

45.113.122.95

Lookup | Go To | Rescan | Add Verdict | Report

URL: http://gatox-unlock.com/
Submission: On May 17 via manual (May 17th 2023, 10:18:57 am UTC) from PL — Scanned from PL

Summary | HTTP 21 | Redirects | Behaviour | Indicators | Similar 315 | DOM | Content | API | Verdicts

Summary

This website contacted **3 IPs** in **2 countries** across **3 domains** to perform **21 HTTP transactions**. The main IP is **45.113.122.95**, located in **Central, Hong Kong** and belongs to PUBLIC-DOMAIN-REGISTRY, US. The main domain is **gatox-unlock.com**.

gatox-unlock.com scanned **8 times** on urlscan.io — Show Scans 8

315 similar pages on different IPs, domains and ASNs found — Show Scans 315

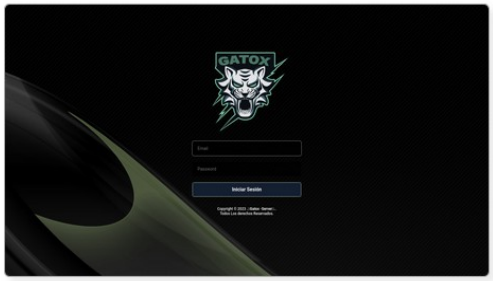
urlscan.io Verdict: No classification

Live information

Google Safe Browsing: No classification for *gatox-unlock.com*
Current DNS A record: 45.113.122.95 (AS394695 - PUBLIC-DOMAIN-REGISTRY, US)
Domain created: September 22nd 2021, 03:34:17 (UTC)
Domain registrar: PDR Ltd. d/b/a PublicDomainRegistry.com

Screenshot

Live screenshot | Full Image



Detected technologies

Bootstrap (Web Frameworks) — Expand

zeus-server.info

162.222.225.165

Lookup | Go To | Rescan | Add Verdict | Report

URL: https://zeus-server.info/
Submission: On May 17 via manual (May 17th 2023, 10:17:47 am UTC) from PL — Scanned from PL

Summary | HTTP 23 | Redirects | Behaviour | Indicators | Similar 316 | DOM | Content | API | Verdicts

Summary

This website contacted **3 IPs** in **1 countries** across **3 domains** to perform **23 HTTP transactions**. The main IP is **162.222.225.165**, located in **United States** and belongs to UNIFIEDLAYER-AS-1, US. The main domain is **zeus-server.info**.
TLS certificate: Issued by *R3* on May 4th 2023. Valid for: 3 months.

This is the only time *zeus-server.info* was scanned on urlscan.io!

316 similar pages on different IPs, domains and ASNs found — Show Scans 316

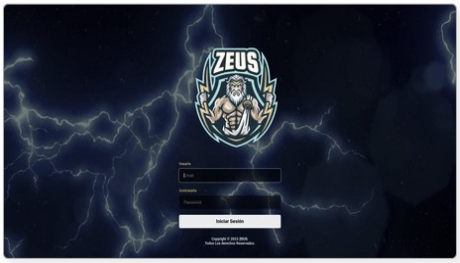
urlscan.io Verdict: No classification

Live information

Google Safe Browsing: No classification for *zeus-server.info*
Current DNS A record: 162.222.225.165 (AS46606 - UNIFIEDLAYER-AS-1, US)

Screenshot

Live screenshot | Full Image



Detected technologies

manzanitaserver.net

162.215.240.133

Lookup | Go To | Rescan | Add Verdict | Report

URL: https://manzanitaserver.net/
Submission: On May 17 via manual (May 17th 2023, 10:16:41 am UTC) from PL — Scanned from PL

Summary | HTTP 21 | Redirects | Behaviour | Indicators | Similar 316 | DOM | Content | API | Verdicts

Summary

This website contacted **3 IPs** in **1 countries** across **3 domains** to perform **21 HTTP transactions**. The main IP is **162.215.240.133**, located in **United States** and belongs to UNIFIEDLAYER-AS-1, US. The main domain is **manzanitaserver.net**.
TLS certificate: Issued by *R3* on May 13th 2023. Valid for: 3 months.

This is the only time *manzanitaserver.net* was scanned on urlscan.io!

316 similar pages on different IPs, domains and ASNs found — Show Scans 316

urlscan.io Verdict: No classification

Live information

Google Safe Browsing: Malicious for *manzanitaserver.net*
Current DNS A record: 162.215.240.133 (AS46606 - UNIFIEDLAYER-AS-1, US)

Screenshot

Live screenshot | Full Image

Detected technologies

Bootstrap (Web Frameworks) — Expand

genius-server.cc

199.79.62.115

Lookup | Go To | Rescan | Add Verdict | Report

URL: https://genius-server.cc/
Submission: On May 17 via manual (May 17th 2023, 10:13:56 am UTC) from PL — Scanned from PL

Summary | HTTP 32 | Redirects | Links 2 | Behaviour | Indicators | Similar 36 | DOM | Content | API | Verdicts

Summary

This website contacted **5 IPs** in **2 countries** across **5 domains** to perform **32 HTTP transactions**.
The main IP is **199.79.62.115**, located in **United States** and belongs to UNIFIEDLAYER-AS-1, US. The main domain is **genius-server.cc**.
TLS certificate: Issued by *R3* on May 2nd 2023. Valid for: 3 months.

This is the only time *genius-server.cc* was scanned on urlscan.io!

36 similar pages on different IPs, domains and ASNs found — Show Scans 36

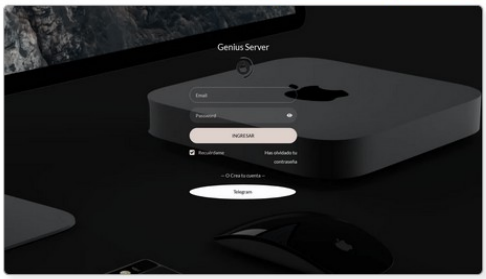
urlscan.io Verdict: No classification

Live information

Google Safe Browsing: No classification for *genius-server.cc*
Current DNS A record: 199.79.62.115 (AS46606 - UNIFIEDLAYER-AS-1, US)
Domain created: April 19th 2023, 12:30:00 (UTC)
Domain registrar: NameSilo, LLC

Screenshot

Live screenshot | Full Image



Detected technologies

Bootstrap (Web Frameworks) — Expand
animate.css (Web Frameworks) — Expand
Font Awesome (Font Scripts) — Expand

www.unlock-server.net

193.233.15.15

Lookup | Go To | Rescan | Add Verdict | Report

Submitted URL: http://unlock-server.net/main
Effective URL: https://www.unlock-server.net/main
Submission: On May 06 via manual (May 6th 2023, 10:20:08 am UTC) from FR — Scanned from FR

Summary | HTTP 38 | Redirects | Links 3 | Behaviour | Indicators | Similar 391 | DOM | Content | API | Verdicts

Summary

This website contacted **6 IPs** in **4 countries** across **5 domains** to perform **38 HTTP transactions**.
The main IP is **193.233.15.15**, located in **Russian Federation** and belongs to SAFEVALUE-AS, SC. The main domain is **www.unlock-server.net**.
TLS certificate: Issued by *R3* on May 5th 2023. Valid for: 3 months.

unlock-server.net scanned **5 times** on urlscan.io — Show Scans 5

www.unlock-server.net scanned **5 times** on urlscan.io — Show Scans 5

391 similar pages on different IPs, domains and ASNs found — Show Scans 391

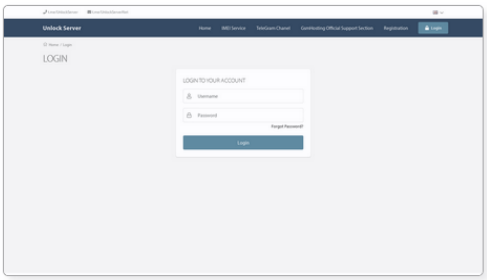
urlscan.io Verdict: No classification

Live information

Google Safe Browsing: No classification for *www.unlock-server.net*
Current DNS A record: 193.233.15.15 (AS42745 - SAFEVALUE-AS, SC)
Domain created: May 5th 2015, 17:43:09 (UTC)
Domain registrar: NAMECHEAP INC

Screenshot

Live screenshot | Full Image



Page URL History

Show full URLs

1. http://unlock-server.net/main HTTP 301
   http://www.unlock-server.net/main HTTP 302
   https://www.unlock-server.net/main Page URL

Detected technologies

Summary

This website contacted **5 IPs** in **2 countries** across **4 domains** to perform **18 HTTP transactions**.
The main IP is **204.11.58.71**, located in **United States** and belongs to UNIFIEDLAYER-AS-1, US.
The main domain is **ecuacellunlocker.com**.

This is the only time *ecuacellunlocker.com* was scanned on urlscan.io!

3 similar pages on different IPs, domains and ASNs found — Show Scans 3

urlscan.io Verdict: No classification

Live information

Google Safe Browsing: No classification for *ecuacellunlocker.com*
Current DNS A record: 204.11.58.71 (AS46606 - UNIFIEDLAYER-AS-1, US)
Domain created: April 11th 2023, 23:44:57 (UTC)
Domain registrar: Atak Domain

Screenshot

Live screenshot | Full Image

Detected technologies

Statcounter (Analytics) — Expand

Page Statistics

theanonymouss.us

Lookup | Go To | Rescan | Add Verdict | Report

162.210.70.199

URL: https://**theanonymouss.us**/login

Submission: On May 06 via manual (May 6th 2023, 10:16:09 am UTC) from FR — Scanned from US

Summary | HTTP 7 | Redirects | Links 1 | Behaviour | Indicators | Similar | DOM | Content | API | Verdicts

Summary

This website contacted **1 IPs** in **1 countries** across **1 domains** to perform **7 HTTP transactions**. The main IP is **162.210.70.199**, located in **United States** and belongs to UNIFIEDLAYER-AS-1, US. The main domain is **theanonymouss.us**.
TLS certificate: Issued by *GoGetSSL RSA DV CA* on May 5th 2023. Valid for: a month.

theanonymouss.us scanned **7 times** on urlscan.io — Show Scans 7

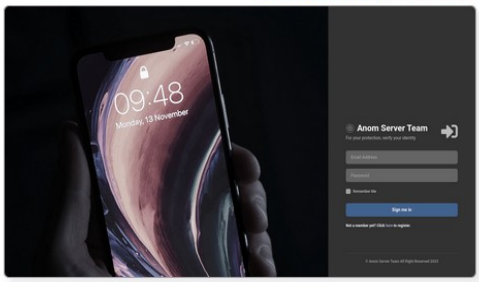
urlscan.io Verdict: No classification

Live information

Google Safe Browsing: No classification for *theanonymouss.us*
Current DNS A record: 162.210.70.199 (AS46606 - UNIFIEDLAYER-AS-1, US)
Domain created: June 28th 2021, 07:21:57 (UTC)
Domain registrar: NAMECHEAP INC

Screenshot

Live screenshot | Full Image



Page Statistics

7	100 %	0 %	1	1

aliunlockers.com

Lookup | Go To | Rescan | Add Verdict | Report

2a02:4780:b:1060:0:2c32:e001:7

URL: https://**aliunlockers.com**/

Submission: On May 06 via manual (May 6th 2023, 10:14:12 am UTC) from FR — Scanned from FR

Summary | HTTP 50 | Redirects | Links 7 | Behaviour | Indicators | Similar 1 | DOM | Content | API | Verdicts

Summary

This website contacted **5 IPs** in **2 countries** across **4 domains** to perform **50 HTTP transactions**. The main IP is **2a02:4780:b:1060:0:2c32:e001:7**, located in **Phoenix, United States** and belongs to AS-HOSTINGER, CY. The main domain is **aliunlockers.com**.
TLS certificate: Issued by *R3* on April 12th 2023. Valid for: 3 months.

This is the only time *aliunlockers.com* was scanned on urlscan.io!

1 similar pages on different IPs, domains and ASNs found — Show Scans 1

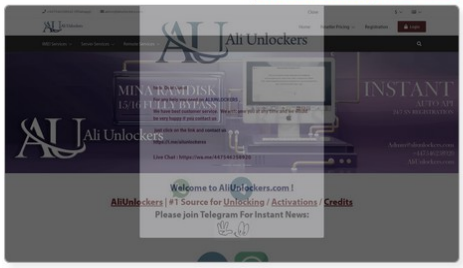
urlscan.io Verdict: No classification

Live information

Google Safe Browsing: No classification for *aliunlockers.com*
Current DNS A record: 86.38.202.246 (AS47583 - AS-HOSTINGER, CY)
Domain created: November 27th 2021, 14:52:29 (UTC)
Domain registrar: NAMECHEAP INC

Screenshot

Live screenshot | Full Image



Detected technologies

Cart Functionality (Ecommerce) — Expand
Chart.js (JavaScript Graphics) — Expand

provip-server.com

Lookup | Go To | Rescan | Add Verdict | Report

69.49.235.216

URL: http://**provip-server.com**/

Submission: On May 06 via manual (May 6th 2023, 10:12:30 am UTC) from FR — Scanned from FR

Summary | HTTP 13 | Redirects | Links 1 | Behaviour | Indicators | Similar 10 | DOM | Content | API | Verdicts

Summary

This website contacted **3 IPs** in **2 countries** across **3 domains** to perform **13 HTTP transactions**. The main IP is **69.49.235.216**, located in **United States** and belongs to NETWORK-SOLUTIONS-HOSTING, US. The main domain is **provip-server.com**.

This is the only time *provip-server.com* was scanned on urlscan.io!

10 similar pages on different IPs, domains and ASNs found — Show Scans 10

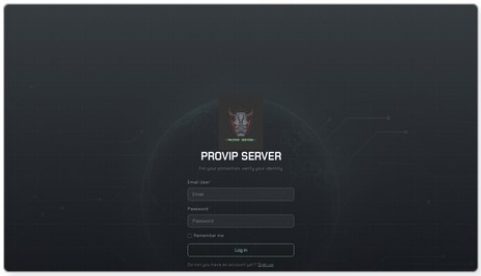
urlscan.io Verdict: No classification

Live information

Google Safe Browsing: No classification for *provip-server.com*
Current DNS A record: 69.49.235.216 (AS19871 - NETWORK-SOLUTIONS-HOSTING, US)
Domain created: March 18th 2023, 20:58:42 (UTC)
Domain registrar: PDR Ltd. d/b/a PublicDomainRegistry.com

Screenshot

Live screenshot | Full Image



Page Statistics

13	23 %	67 %	3	3
Requests	HTTPS	IPv6	Domains	Subdomains

45.131.46.98

45.131.46.98

Lookup | Go To | Rescan | Add Verdict | Report

URL: https://45.131.46.98/
Submission: On May 05 via manual (May 5th 2023, 9:31:25 am UTC) from FR — Scanned from FR

Summary | HTTP 13 | Redirects | Links 1 | Behaviour | Indicators | Similar 29 | DOM | Content | API | Verdicts

Summary

This website contacted **3 IPs** in **2 countries** across **2 domains** to perform **13 HTTP transactions**.
The main IP is **45.131.46.98**, located in **Russian Federation** and belongs to TIMEHOST-AS, UA.
The main domain is **45.131.46.98**.
TLS certificate: Issued by *R3* on May 1st 2023. Valid for: 3 months.

This is the only time *45.131.46.98* was scanned on urlscan.io!

29 similar pages on different IPs, domains and ASNs found — Show Scans 29

urlscan.io Verdict: No classification

Live information

Google Safe Browsing: No classification for *45.131.46.98*
(AS212913 - TIMEHOST-AS, UA)

Screenshot

Live screenshot | Full Image

Page Statistics

13	23 %	67 %	2	2

server-unlocker.com

162.210.70.199

Lookup | Go To | Rescan | Add Verdict | Report

URL: https://server-unlocker.com/
Submission: On May 05 via manual (May 5th 2023, 7:30:48 am UTC) from NL — Scanned from NL

Summary | HTTP 29 | Redirects | Links 4 | Behaviour | Indicators | Similar 4 | DOM | Content | API | Verdicts

Summary

This website contacted **5 IPs** in **3 countries** across **5 domains** to perform **29 HTTP transactions**.
The main IP is **162.210.70.199**, located in **United States** and belongs to UNIFIEDLAYER-AS-1, US. The main domain is **server-unlocker.com**.
TLS certificate: Issued by *R3* on April 29th 2023. Valid for: 3 months.

server-unlocker.com scanned **3 times** on urlscan.io — Show Scans 3

4 similar pages on different IPs, domains and ASNs found — Show Scans 4

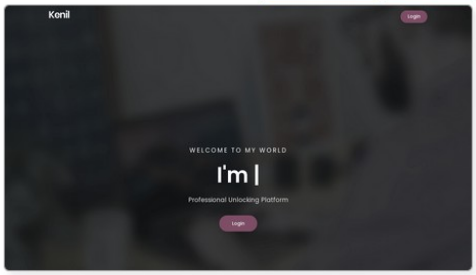
urlscan.io Verdict: No classification

Live information

Google Safe Browsing: No classification for *server-unlocker.com*
Current DNS A record: 162.210.70.199 (AS46606 - UNIFIEDLAYER-AS-1, US)
Domain created: January 4th 2023, 12:17:19 (UTC)
Domain registrar: PDR Ltd. d/b/a PublicDomainRegistry.com

Screenshot

Live screenshot | Full Image



Detected technologies

Bootstrap (Web Frameworks) — Expand
animate.css (Web Frameworks) — Expand
Font Awesome (Font Scripts) — Expand

jjunlocks-kit-server.us

172.98.73.38

Lookup | Go To | Rescan | Add Verdict | Report

URL: https://**jjunlocks-kit-server.us**/
Submission: On May 05 via manual (May 5th 2023, 7:29:42 am UTC) from NL — Scanned from US

Summary | HTTP 31 | Redirects | Links 1 | Behaviour | Indicators | Similar 44 | DOM | Content | API | Verdicts

Summary

This website contacted **5 IPs** in **2 countries** across **5 domains** to perform **31 HTTP transactions**. The main IP is **172.98.73.38**, located in **Toronto, Canada** and belongs to PERFORMIVE, US. The main domain is **jjunlocks-kit-server.us**.
TLS certificate: Issued by *cPanel, Inc. Certification Authority* on April 13th 2023. Valid for: 3 months.

jjunlocks-kit-server.us scanned **5 times** on urlscan.io — Show Scans 5

44 similar pages on different IPs, domains and ASNs found — Show Scans 44

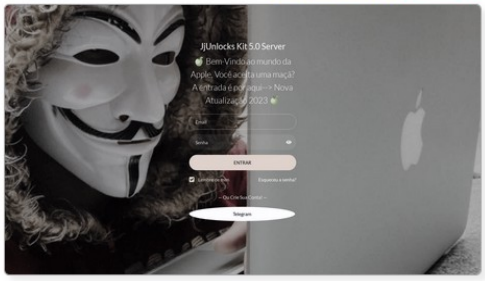
urlscan.io Verdict: No classification

Live information

Google Safe Browsing: No classification for *jjunlocks-kit-server.us*
Current DNS A record: 172.98.73.38 (AS46562 - PERFORMIVE, US)

Screenshot

Live screenshot | Full Image



Detected technologies

Bootstrap (Web Frameworks) — Expand
animate.css (Web Frameworks) — Expand

unlockcdserver.com

69.49.235.216

Lookup | Go To | Rescan | Add Verdict | Report

URL: http://**unlockcdserver.com**/
Submission: On May 05 via manual (May 5th 2023, 7:28:14 am UTC) from NL — Scanned from NL

Summary | HTTP 13 | Redirects | Links 1 | Behaviour | Indicators | Similar 27 | DOM | Content | API | Verdicts

Summary

This website contacted **3 IPs** in **2 countries** across **3 domains** to perform **13 HTTP transactions**. The main IP is **69.49.235.216**, located in **United States** and belongs to NETWORK-SOLUTIONS-HOSTING, US. The main domain is **unlockcdserver.com**.

unlockcdserver.com scanned **5 times** on urlscan.io — Show Scans 5

27 similar pages on different IPs, domains and ASNs found — Show Scans 27

urlscan.io Verdict: No classification

Live information

Google Safe Browsing: No classification for *unlockcdserver.com*
Current DNS A record: 69.49.235.216 (AS19871 - NETWORK-SOLUTIONS-HOSTING, US)

Screenshot

Live screenshot | Full Image

Page Statistics

13 | 23 or | 67 or | 3 | 3

www.iunlockersmx.com
hitserver.in

Lookup | Go To | Rescan

Lookup | Go To | Rescan

iserverkit.info

91.209.70.161

Lookup | Go To | Rescan | Add Verdict | Report

URL: http://**iserverkit.info**/
Submission: On May 19 via manual (May 19th 2023, 7:11:53 am UTC) from FR — Scanned from FR

ultimate-kit.live

2a06:98c1:3120::3

Lookup | Go To | Rescan | Add Verdict | Report

URL: https://**ultimate-kit.live**/
Submission: On May 19 via manual (May 19th 2023, 7:18:03 am UTC) from FR — Scanned from NL

Summary | HTTP 10 | Redirects | Links 1 | Behaviour | Indicators | Similar | DOM | Content | API | Verdicts

Summary

This website contacted **3 IPs** in **2 countries** across **3 domains** to perform **10 HTTP transactions**. The main IP is **2a06:98c1:3120::3**, located in **United States** and belongs to CLOUDFLARENET, US. The main domain is **ultimate-kit.live**.
TLS certificate: Issued by *Cloudflare Inc ECC CA-3* on July 12th 2022. Valid for: a year.

This is the only time *ultimate-kit.live* was scanned on urlscan.io!

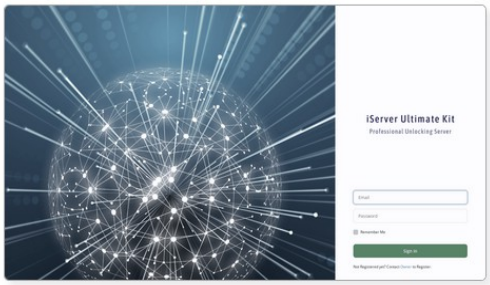
urlscan.io Verdict: No classification

Live information

Google Safe Browsing: No classification for *ultimate-kit.live*
Current DNS A record: 188.114.96.3 (AS13335 - CLOUDFLARENET, US)
Domain created: July 12th 2022, 17:04:04 (UTC)
Domain registrar: SAV.COM, LLC

Screenshot

Live screenshot | Full Image



Detected technologies

Google Font API (Font Scripts) — Expand

Indicators (IOCs)

We have compiled a comprehensive list of Indicators of Compromise (IOCs) resulting from our investigation. Due to the extensive number of IOCs, we have published a separate report specifically dedicated to this information. This report provides detailed insights into the various IOCs discovered during the investigation, including domains, IP addresses, email addresses, and other relevant data.

To ensure widespread access and dissemination of this vital information, we have made the IOC report available through multiple channels. You can access the IOC report through the following resources:

1. Link 1: This link directs you to our dedicated blog post, where we have published the IOC report in a comprehensive and easily accessible format.
2. Link 2: We have also shared the IOC report on our GitHub repository. This allows for collaborative contributions and facilitates integration into existing security tools and platforms.
3. Link 3: Our IOC report is available on the Open Threat Exchange (OTX), a community-driven threat intelligence platform. This platform enables users to access, contribute to, and collaborate on threat intelligence data.

By making the IOC report accessible through these various channels, we aim to empower security professionals, researchers, and organizations in their efforts to detect, prevent, and mitigate the threats posed by the iServer syndicate.