

Q4 | 2022

CYBER THREAT REPORT



Powered by the
Infoblox Threat Intelligence Group

Disclaimer

Infoblox publications and research are made available solely for general information purposes. The information contained in this publication is provided on an “as is” basis. Infoblox accepts no liability for the use of this data. Any additional developments or research since the date of publication will not be reflected in this report.



Table of Contents

Executive Summary	5
Infoblox Reputation Scoring Capability	5
TLD Reputation	6
Riskiest TLDs	6
Registrar Reputation	7
Overview of Registrar Reputation	7
Recent Registrar Reputation Scores	8
In-Depth Analysis of the Stichting Registrar	9
In-Depth Analysis of Chengdu West Registrar	10
In-Depth Analysis of DNS Africa Registrar	10
Nameserver Reputation	11
Riskiest Nameservers	11
French Smishing Campaign Uses Fake Social Security Portal.....	14
Overview	14
Customer Impact.....	14
Infrastructure Analysis.....	16
Vulnerabilities and Mitigation	17
Scams Using Fake Celebrity Endorsements Target EU Countries	18
Summary	18
Background.....	18
Campaigns Analysis.....	18
Stage 1: Sponsored Facebook Ads Through SoulCircuit's Compromised Account	19
Stage 2: LinkedIn Posts.....	20
Stage 3: Landing Pages and Randomly Generated Domains.....	24
Stage 4: Personal Information Gathering	26
Stage 5: Money Theft	26
Domain Analysis	29
Prevention and Mitigation	30
Spotlight on India Cyber Threats	31
Indian Institute of Medical Services	31
Safdarjung Hospital.....	32
Central Depository Services Limited	32

Government Cyber Alerts	33
Cybersecurity and Infrastructure Security Agency Alerts: Q4 2022	33
Federal Bureau of Investigation Cyber Alerts: Q4 2022	34
National Security Agency/Central Security Service Advisories and Guidance: Q4 2022	35
The Infoblox Threat Intelligence Group	36
Infoblox Threat Intelligence	36

Executive Summary

We at Infoblox are pleased to publish this Q4 2022 edition of our Quarterly Cyber Threat Intelligence Report. We publish these reports during the first month of each calendar quarter.

This Q4 2022 report spotlights original research by the Infoblox Threat Intelligence Group (TIG) into the reputation scoring of domain registrars and nameservers and how this information can help organizations assess potential threats. This is the first time we have released and published this data externally to such a broad audience. As with the top-level domain (TLD) update provided in this report, the team expects to supply updates to this original research each quarter.

This report also includes articles on a “Meta” coin fake celebrity endorsed scam targeting the EU and on a smishing campaign targeting France and Europe. We have also added a special spotlight update on India cyber threats.

We finish the report with industry alerts, advisories, reports and original research published from October 1 to December 31, 2022, by the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI) and the NSA/CSS (National Security Agency Central Security Service).

This publication supplements our original research and insight into threats we observed leading up to and including Q4 2022. We feel that timely information on cyber threats is vital to protecting the community at large.

Infoblox Reputation Scoring Capability

In the previous Quarterly Cyber Threat Intelligence Report, we introduced Infoblox’s new reputation scoring algorithm. The algorithm enables analysts in the Threat Intelligence Group (TIG) to classify the reputation, or risk, of internet infrastructure. When we introduced the algorithm, we demonstrated its use in determining the risk associated with top-level domains (TLDs) we have observed. In this report, we expanded its use to provide an analysis of the risk associated with domain name registrars and nameservers. In future reports, we will share the results of applying our reputation scoring algorithm to data sets such as mail servers and autonomous system numbers (ASNs). For a review of the reputation scoring algorithm itself, read our [high-level overview](#) or the in-depth [white paper](#).

TLD Reputation

In the last quarterly report, we introduced our new reputation, or risk, scoring algorithm and used TLDs as an example of its application. Because the internet is ever changing, we will revisit the topic and see how the reputation of TLDs has changed each quarter.

Riskiest TLDs

As we saw last quarter, and expect to see in the future, a large number of TLDs are assigned a score of 0 with low confidence. This scoring occurs when no malicious domains are observed for a TLD, but the total number of domains for the TLD is too small for us to have high confidence in the reputation score. The high number of 0s is understandable because legitimate activity dominates the internet.

Also, similar to the preceding quarter, the number of TLDs with a risk score of 9 or 10 was minimal. Since a score of 10 indicates that all the domains observed for a TLD were malicious, such scores are rare, especially when looking at only high-confidence scores. The volumes for the rest of the scores follow the expected distribution curve, which we published previously.

Table 1 below lists the TLDs that were consistently assigned high-confidence, high-risk scores (which equates to a score of 7 or more) during Q4 2022. Most of the TLDs that matched these criteria last quarter are also present this quarter and are highlighted for reference. The new TLDs on the list barely missed making the list last time and are familiar to Infoblox researchers who hunt for malicious domains in these TLDs. As always, these TLDs represent consistent threats, and traffic to and from domains using them should be monitored.

TLD	Months at high or very high risk
autos	3 / 3
bar	3 / 3
beauty	3 / 3
buzz	3 / 3
cfc	3 / 3
click	3 / 3
cyou	3 / 3
hair	3 / 3
icu	3 / 3
live	3 / 3
lol	3 / 3

mom	3 / 3
monster	3 / 3
pics	3 / 3
quest	3 / 3
rest	3 / 3
top	3 / 3
wf	3 / 3
xyz	3 / 3

Table 1: The most consistently high-confidence, high-risk TLDs for the past quarter (October through December). Highlighted rows indicate TLDs that were also listed as consistently high-risk in the last quarterly report

Registrar Reputation

Overview of Registrar Reputation

TLDs are an excellent starting point for reputation scoring because they are chosen when domains are registered and cannot be changed. In stark contrast, reputation scores for domain registrars, the organizations that manage the purchase and management of domain names, present some challenges. While the algorithm functions the same as it does for TLD reputations, obtaining the right data to use in the algorithm for registrars is far more difficult.

The first data challenge is that the owner of a domain can change registrars whenever they want. Someone can use one registrar to purchase a domain and then transfer it to another for long-term use. As a result, a domain could be observed to be associated with multiple registrars within a given time. This transfer frequently occurs when a domain's registration expires and someone else purchases it.

The second challenge is that while many of the larger registrars follow IANA's standard for WHOIS information regarding a domain's registration details, too many registrars choose their own format. As a result, registrar names are not consistently formatted, even between domains managed by the same registrar. For example, our data shows multiple permutations for the registrar GoDaddy, including: "Godaddy . com, LLC", "GoDaddy . com, LLC" (note the lack of a space after the comma) and "Go Daddy, LLC." To address this issue, Infoblox researchers have created an algorithm that attempts to identify registrars across all these variations, but given the complexity of the problem, some variations are not caught.

Despite these challenges, we have found that registrar reputation scores are still a valuable tool for identifying potential risks before they become a problem, especially when used in combination with our TLD reputation score.

Recent Registrar Reputation Scores

Figure 1 illustrates the distribution of registrar reputation, or risk, scores for December 2022. The majority of registrars were assigned a risk score of 0, meaning no malicious domains were observed associated with them for the month. These 0 scores are primarily due to the fact that only a few domains were observed for each registrar, as is indicated by our designation of low confidence for so many of those scores.

This is an expected feature of this data set, because there is a relatively small number of registrars that are associated with many domains, and there is a very large number of registrars that are only associated with a handful of often legitimate or benign observed domains (which get a score of 0).

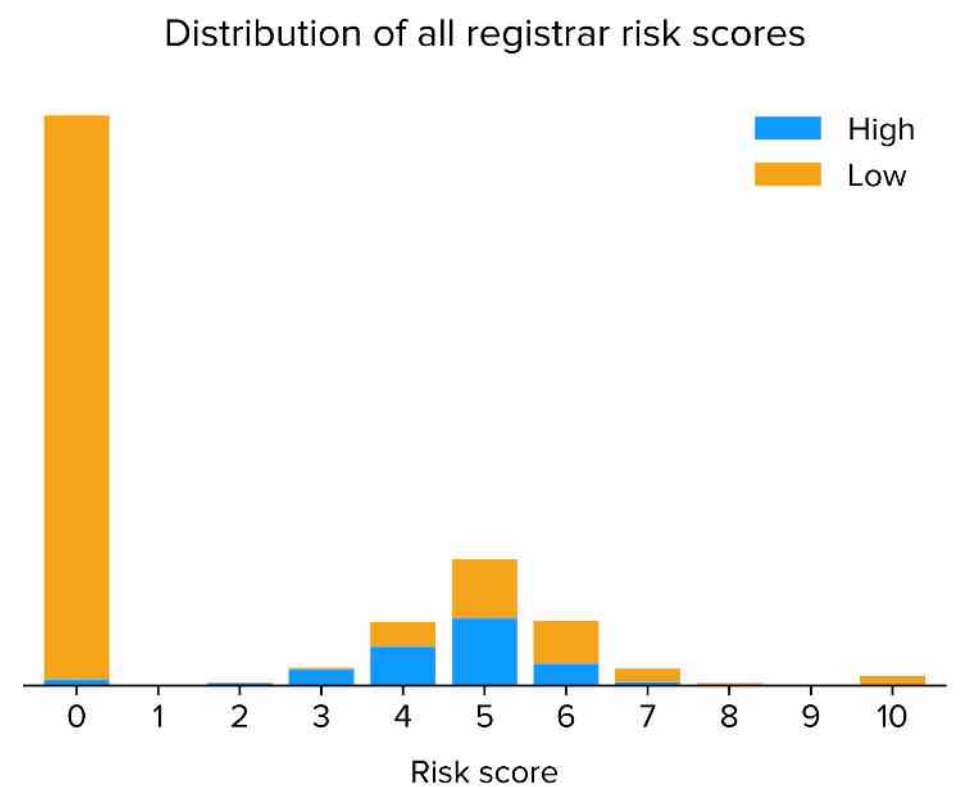


Figure 1: The distribution of risk scores for all observed registrars is shown for December. The scores are broken out by the algorithm's confidence in the calculated score

Registrar reputation risk scores change over time because of the dynamic nature of registrar usage and the Internet itself. The most consistently high-risk registrars across the past two quarters, totalling six months, appear below in Table 1. Given the highly variable nature of the internet, sensing capabilities, and threat actor infrastructure, it is not uncommon for a registrar's risk score to vary from month to month. As a result, a registrar being consistently classified as high risk indicates a long-term risk that warrants further investigation.

Registrar	Months at high or very high risk
Chengdu West Dimension Digital	6 / 6
Eranet International	6 / 6
NameSilo	6 / 6
NiceNIC International	6 / 6
Stichting	6 / 6
URL Solutions	6 / 6
Xin Net Technology Corporation	6 / 6
Bizcn.com	5 / 6
Domain International	5 / 6
MainReg	5 / 6
Sav	5 / 6
West263 International	5 / 6

Table 1: The most consistently high-confidence, high-risk registrars for the past two quarters (July to December)

In-Depth Analysis of the Stichting Registrar

Based on the data shown here, the Stichting registrar looks to be particularly risky. Of the more than 31,000 domains used for this article from August 2022 that were registered with Stichting, over 99 percent were thought to be malicious. One might think that this registrar is a wretched hive of scum and villainy, but a deeper analysis tells a more interesting story. The vast majority of the observed domains appear to be DGA domains, with names such as `bbjivsklnowk[.]bid`, `tdkiemyropqx[.]org`, `sifhfdabafmmyvqubm[.]pro` and `wxmumegfcgve[.]pw`. Many of these domains were registered within the last year and are known to act as command and control servers and serve malware, among other nefarious activities. However, there were also a significant number of domain names that were being sinkholed by security researchers. Sinkholing a domain occurs when an organization configures a DNS server to return an IP address that does not lead to malicious contents. In this case, organizations including Microsoft, Fraunhofer-Gesellschaft and SIDN Labs own these once-malicious domains and disrupt attempts to use them for malicious purposes.

“The most important part of a story is the piece of it you don't know.”

– Barbara Kingsolver, *The Lacuna*

In-Depth Analysis of Chengdu West Registrar

In the last quarterly report, we discussed the TLD `top` as a consistently high-confidence, high-risk TLD. We specifically mentioned that over 30,000 domains appear to have been created using a dictionary domain generation algorithm (DDGA). The registrar used for those DDGA domains was Chengdu West Dimension Digital, which is one of the most consistently high-confidence, high-risk registrars in our data set.

In the past two quarters, we observed over 400,000 domains registered with Chengdu West; more than 63 percent of them were classified as malicious. Table 2 breaks down these domains by threat type. Phishing domains are consistently the most common type of threat for this registrar. The most commonly observed TLD for domains registered with Chengdu West is `top`, comprising 37 percent of all the malicious domains. This amount is unsurprising given our previous analysis and demonstrates that reputation scores for different internet infrastructure components can be combined to enhance threat analysis and increase confidence in the results.

Threat Type	Percentage
Phishing	66%
Malware	25%
Spam	6%
Other	3%

Table 2: The different threat types of observed domains that were registered using Chengdu West Dimension Digital and their percentages for the past two quarters (July to December)

In-Depth Analysis of DNS Africa Registrar

While the registrar DNS Africa is not on the list of the most consistently high-confidence, high-risk registrars, it is worthy of a deeper look because of some unusual behavior. Table 3 shows the reputation information for the domains observed in the last quarter. Both the total number of observed domains and the percentage of malicious domains clearly make this registrar very risky.

Month	Total Domains	Malicious Domains	Malicious Percentage	Risk Score	Risk Label
October 2022	1,014	871	85.9%	8	High
November 2022	16,819	16,626	98.8%	10	Very High
December 2022	633	522	82.5%	8	High

Table 3: The total number of observed domains and domains found to be malicious that were registered using DNS Africa are shown for the past quarter.

A deeper look into the registrar yields some interesting insights. The median number of domains registered with them per day is only four. However, a number of days during the last quarter are clearly abnormal. For example, Table 4 lists three consecutive days during which a total of 16,115 domains were registered, with the vast majority using the `africa` TLD. Normally, only around 12 domains would be registered within that same time. Furthermore, over 89 percent of the 16,115 domains were classified as malicious. Obviously, something about this registrar makes it appealing for threat actors; and organizations should be wary of any domains registered there.

Date	Total Domains	Malicious Domains
November 14, 2022	2,075	1,857
November 15, 2022	6,397	5,404
November 16, 2022	7,643	7,643

Table 4: The total number of domains and malicious domains registered on three consecutive days using DNS Africa.

Nameserver Reputation

In this section, Infoblox will provide a baseline for a quarterly review of nameservers, using our reputation algorithm. Nameservers are far more dynamic in nature than TLDs and are not controlled by any standards authority. Domain owners can configure their own DNS resolver and use it to route traffic to their websites, all while maintaining anonymity. In fact, there are companies that promote their anonymous hosting services. When there is little or no information available related to a nameserver, our reputation score is a useful tool in evaluating it, based largely on the number of malicious and non-malicious domains we observed on that nameserver.

Riskiest Nameservers

Figure 1 illustrates the distribution of all observed nameservers for December 2022. The majority of the domains received a score of 0, with low confidence from the algorithm. This combination occurs when no malicious domains are observed for a nameserver, but the total number of domains on the nameserver is too small for us to have confidence in the score. Similarly, there are also a large number of nameservers with a low-confidence reputation or risk score of 10. This result occurs when all the observed domains associated with a nameserver are malicious, but again there are too few observed domains for us to have high confidence in the score. More specifically, 80 percent of the nameservers with a score of 0 were observed to be resolving only one or two domains. Similarly, 96 percent of the nameservers with a score of 10 have been observed to resolve to one domain only.

Distribution of all risk scores

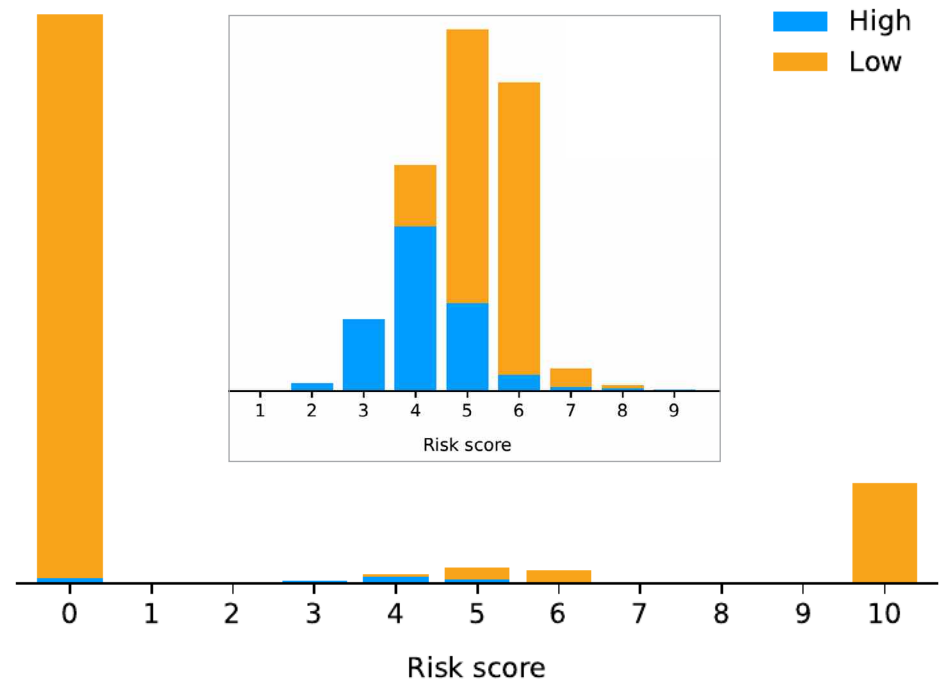


Figure 3: The distribution of TLD risk scores that were observed during September and for which the algorithm has high confidence.

Since nameservers are frequently configured to only provide name resolution for a small number of domains, a significant number of their scores are low confidence. This skews the peak of the high confidence distribution to the score of 4 rather than 5, as it was for the other data sets. The other notable feature of the distribution is that we saw a higher number of nameservers with a score of 10, because nameservers can be under the control of threat actors themselves, unlike TLDs and registrars.

Our results for this baseline produced 31 nameservers with a high score, which in general is considered to be equal to or more than 7. Out of those, the ten listed in the table below scored 9 or 10 in the last two quarters.

Nameserver
floatingpointdns[.]com
infrapu[.]sh
publicdnsservice[.]com
thinkingfastdns[.]com
honeybot[.]us

dns2us[.]com
dnshoster[.]net
dnshubpro[.]com
dnsproviders[.]info
bitcoin-dns[.]com
Table 1: The most consistently high-confidence, high-risk nameservers for the past two quarters (July to December)

These ten nameservers are associated with threats in different ways. In some cases, they are actor-controlled, such as `floatingpointdns[.]com`, while in others, they are security sinkholes, such as `honeybot[.]us`. In many cases, identifying the ownership of nameservers is extremely difficult.

- `floatingpointdns[.]com` and `thinkingfastdns[.]com` are nameserver domains used by the VexTrio actor.¹ This large malicious actor was identified by Infoblox in June of 2022 and uses compromised websites to spread advertising and malware.
- `infrapu[.]sh` is used as a nameserver domain for a variety of virtual private networking (VPN) services, phishing, and suspicious advertising activities. It is hosted in Digital Ocean and not currently tied to a specific legitimate entity.
- `publicdnsservice[.]com` is an actor-controlled nameserver used as part of a large malvertising network.
- `dns2us[.]com` is an actor-controlled nameserver domain that was picked up in November 2021 after the former registration expired. It is registered to the Bahamian Internet Domain Service BS corporation, which is well-known to be abused. This nameserver has been associated with the actor BackdoorDiplomacy.²
- `dnshoster[.]net` is a nameserver domain registered in November 2021 and associated with anonymous DNS services. It is a lookalike to the long-registered Russian domain `dnshoster[.]com`. Also, it hosts a few thousand domains, which is relatively small, and is not associated with a known company, making it likely to be actor-controlled.³
- `dnshubpro[.]com` was registered in November 2021 and is associated with the Virut DGA.⁴
- `dnsproviders[.]info` shares registration and serves the same domains as `dnshubpro[.]com`.
- `bitcoin-dns[.]com` is associated with the hack on EtherDelta.⁵
- `honeybot[.]us` is a sinkhole belonging to the vendor Security Scorecard.

1. <https://blogs.infoblox.com/cyber-threat-intelligence/executive-summary-vextrio-ddga-domains-spread-adware-spyware-and-scam-web-forms/>

2. <https://github.com/eset/malware-ioc/blob/master/backdoordiplomacy/README.adoc>

3. <https://www.domainstate.com/domain/dnshoster.net>

4. <https://mobile.twitter.com/DGAFeedAlerts/status/1537603598049230857>

5. <https://medium.com/@decktonic/following-the-trail-what-we-know-about-the-hacker-behind-the-etherdelta-attack-9ac6015fc2e1>

French Smishing Campaign Uses Fake Social Security Portal

Overview

Since late August, Infoblox has been tracking an actor sending a large number of SMS phishing (smishing) messages targeting phone numbers in France. This attack is ongoing and so widespread that it is regularly mentioned in national news. The text requests that the addressee fill out a form to receive a new Securite Sociale (Social Security) card and to keep the addressee's healthcare plan. Threat actors then charge victims' bank accounts and later make fraudulent tax claims.

14/10 3:36

ASSURANCE MALADIE :
Votre nouvelle carte vitale est
disponible.
Remplissez ce formulaire afin de
rester couvert :
<https://ameliservice.net>

Figure 1: An example of an inbound smishing message, received on October 14

Customer Impact

This campaign was first discovered in relation to Ameli: the French government's portal for Social Security and one of the single sign-on (SSO) points for other websites of government services. The campaign is focused on French speakers and French nationals who use government services and banks. However, some related domains used also include lookalikes that target British nationals, Spanish and Portuguese speakers and Belgian telco and Dutch energy companies. See Figures 2 and 3 below.

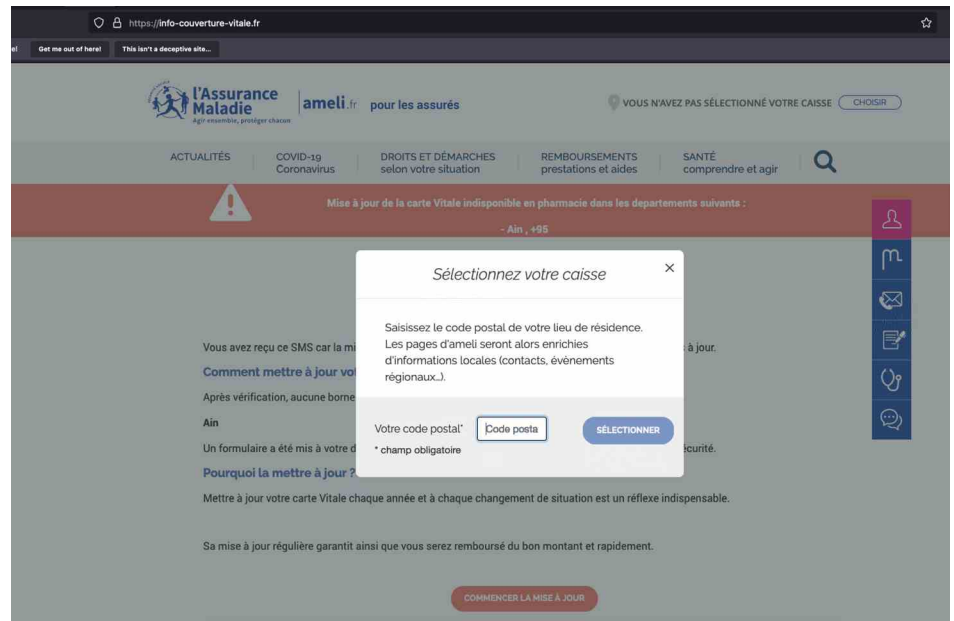


Figure 2: An example of a phishing page masquerading as the portal for the website for Securite Sociale

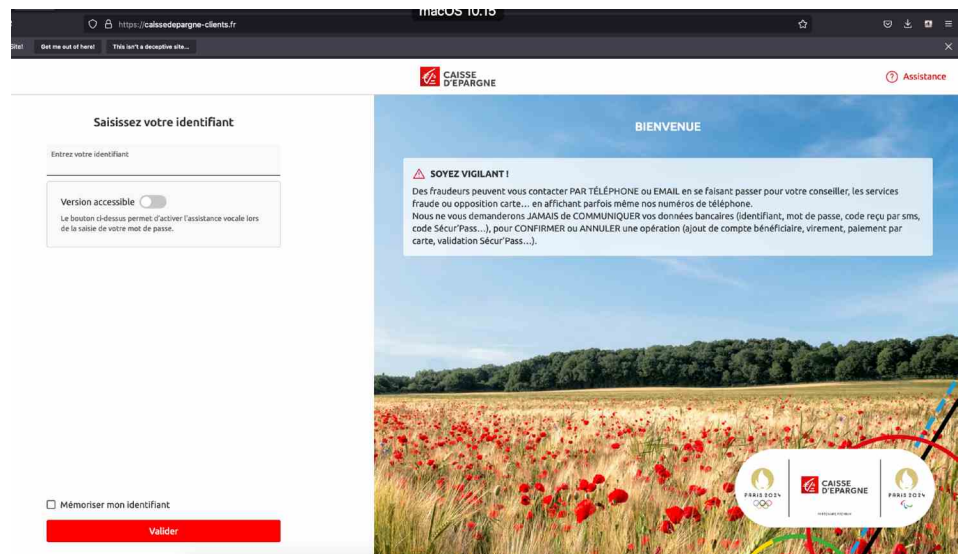


Figure 3: Example of a phishing page targeting customers of the Caisse d'Epargne bank.

Once the landing page is accessed, the victim receives a form asking for personal information, such as email addresses and passwords. The fraudulent websites also ask for financial information, purportedly to pay taxes or late fees. If the victim fills out those forms, their bank accounts will be immediately charged. Later, when tax season comes, the victim's Ameli login will be used to make fraudulent tax claims and receive tax rebates on an attacker-controlled bank account.



Figure 4: Most commonly used words in the domain names of the larger campaign targeting France

Infrastructure Analysis

Attackers used an extensive network of burner emails, phone numbers, and fake identities to cover their tracks, as well as used multiple hosts to avoid automatic takedowns. After several days, the attackers took the phishing pages offline to avoid detection by automated tools and browser safety lists. Infoblox was able to detect and identify approximately 200 IP addresses serving over 7,000 unique phishing domains, illustrated in Figure 5 below. Although the attackers have used Amazon, Google and other providers of cloud services, they also rely heavily on dedicated servers.



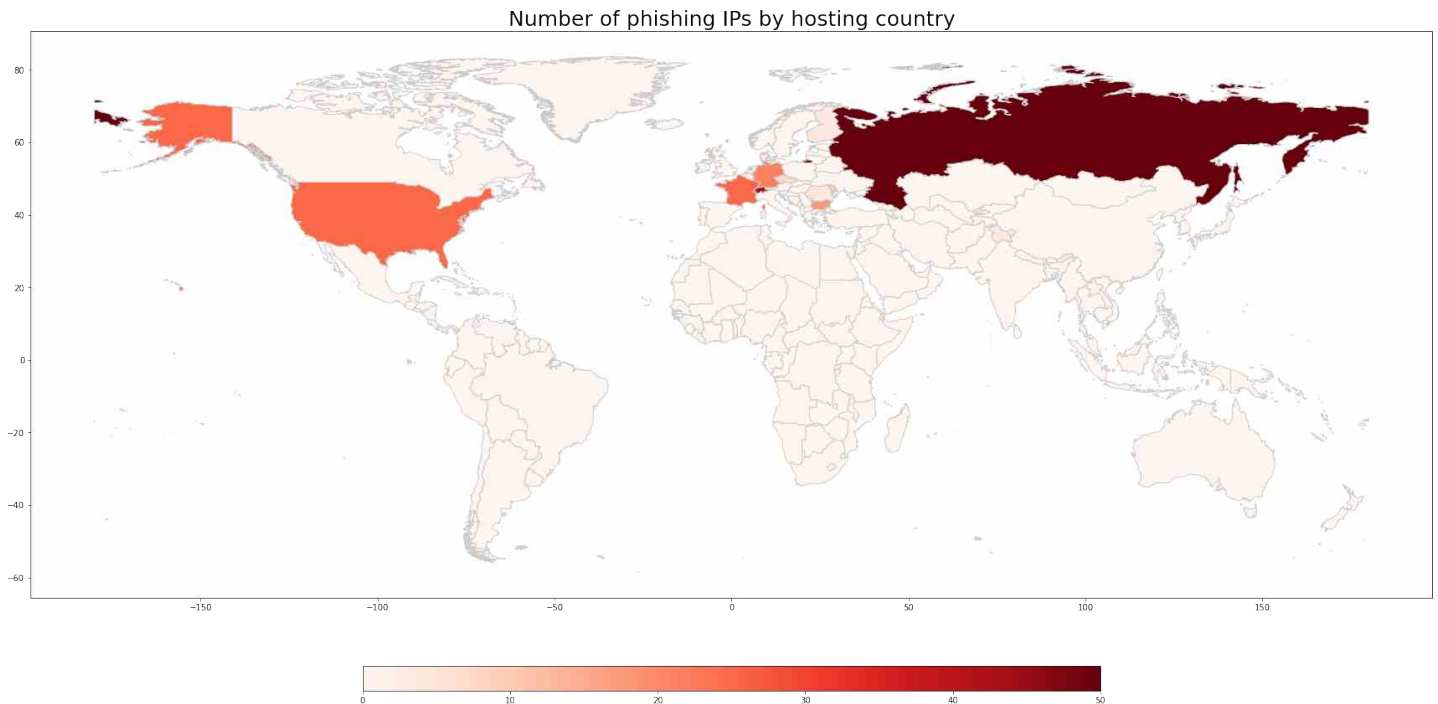


Figure 5: The number of dedicated hosting IPs used by actors, per country

The landing pages are of good quality and, to the unsuspecting eye, visually indistinguishable from the legitimate login pages. Some phishing pages ask for credit card information, purportedly to pay taxes or resolve an unsuccessful payment to a legitimate service. Using Ameli, a person can log in to a variety of government portals, including the tax office and the portal for government subsidies. This has led the government of France to temporarily cut off access to it. Nevertheless, we consider this attack as more likely to be financially motivated rather than political, because it has targeted multiple sectors—government, financial, energy and communication—in several countries.

Vulnerabilities and Mitigation

Infoblox strongly recommends that businesses consider the following security measures:

- Never click URLs in emails or texts from unknown sources.
- Be wary of links in incoming emails and texts. A link in a message from a legitimate company will usually point to the company's domain; for example, a link in a message from FedEx will point to `http://fedex[.]com`. Pause the cursor over the link to verify its true destination.
- If in doubt, do not click links in messages. Instead, navigate to the websites by typing their URLs in the web address bar of a browser.

To review the indicators of compromise (IoCs), please refer to the full report here: <https://blogs.infoblox.com/cyber-threat-intelligence/cyber-threat-advisory/french-smishing-campaign-uses-fake-social-security-portal/>

Scams Using Fake Celebrity Endorsements Target EU Countries

Summary

This section describes a series of scam campaigns that we have been tracking, in which threat actors compromise social media accounts, redirect victims, and solicit their contact information, and then attempt to convince them to deposit funds with fake trading companies. This series of campaigns uses a form of a celebrity endorsed scam, a method first seen in 2020, and uses a “Meta” coin theme. The campaigns stand out in terms of the media platforms the actors use as well as how they stage their attacks. Specifically, the campaigns use Facebook sponsored ads in combination with fake LinkedIn profiles and multiple domains with the same fake content translated into different languages.

Background

Remote working as a result of the global COVID-19 pandemic has significantly changed our daily routines. Many employees now spend more time at home or connecting virtually through devices, and the amount of digital advertising conducted through social media platforms has increased to match this trend. Online fraudsters are taking advantage of these changes. According to the Federal Trade Commission⁶ the total dollar amount reported lost to fraud from criminal actors using social media as the contact method in 2021 was \$770 million, followed by the use of websites or apps at \$554 million and phone calls at \$546 million.

Investment scams have evolved, and the actors have become more advanced in their tactics to convince victims to supply private information and credit card details. The scammers’ techniques can involve compromised social media accounts, redirects via multiple social media platforms and short-lived, randomly generated domains for landing pages, as is the case with the campaigns we will describe in this report.

Campaigns Analysis

The “Meta” coin theme used in these campaigns intentionally conflates two separate services: Facebook’s Meta and Inblock’s Metacoin cryptocurrency. Mark Zuckerberg is rebranding Facebook to Meta as part of his strategy to create Metaverse: an AI and virtual reality platform.

Separately, the founders of the Hong Kong–based company Inblock created Metacoin: a cryptocurrency that is based on hyperledger technology and that has improved security features based on IBM’s LinuxOne platform.

6. <https://techcrunch.com/2022/01/27/ftc-u-s-consumers-lost-770-million-in-social-media-scams-in-2021-up-18x-from-2017/>

Although Metacoins and the Meta services are not related, the scam campaigns in this report use the logo from Facebook's Metaverse platform and the name Metacoins from Inblock's cryptocurrency, likely to make the delivered web content appear legitimate. The fake "Meta" coin campaigns have been initialized by a compromised Facebook account under the name SoulCircuit. SoulCircuit is actually a group that consists of two DJs/musicians: Tom Moore and Dan Timcke, from the United Kingdom. Their compromised Facebook profile page has almost 600,000 followers and is being used to distribute scam-sponsored ads for the fake "Meta" coin cryptocurrency. Another interesting feature of the campaigns is that the attackers seem to be targeting people from specific countries, namely Greece, Italy, and Spain, based on the languages used in the campaigns and the use of pictures and names of actual prime ministers from those countries.

The campaigns consist of five stages. The actor uses different social media platforms to lure and then redirect the victim, eventually leading them to a short-lived domain that seems to be either fully or partially randomly generated. Once a user shows interest and supplies some initial information (name and mobile phone number), they are again redirected to fake trading websites that present requests for a deposit via a credit card or a transfer from other cryptocurrency accounts.

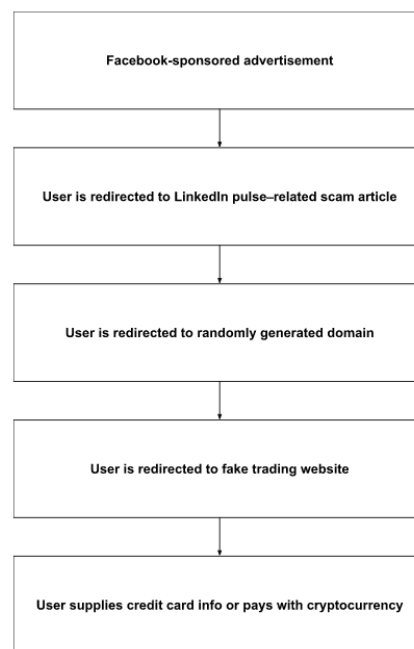


Figure 1: Stages of the Meta attack

Stage 1: Sponsored Facebook Ads Through SoulCircuit's Compromised Account

In the first stage of the attack, the actor places "Meta" coin ads on SoulCircuit's Facebook main wall. The screenshot in Figure 2 below is from a campaign targeting Greek-speaking individuals or groups. One of the obvious signs that the campaign is a scam is the fact that there is no punctuation in capital Greek letters. On the other hand, the "fact" that the account allegedly has a large number of followers (594,000)

can lead a user to believe this ad is legit. The image on the right-hand side of Figure 2 shows the caption's text translated into English. Upon clicking the Learn more button, a user is redirected to a LinkedIn page, which we consider Stage 2.



	
Original text (Greek)	Translated text (English)

Figure 2: Sponsored ad in original and English translated text

Stage 2: LinkedIn Posts

Clicking the Learn more button opens a LinkedIn page that claims that this new cryptocurrency was invented by “Meta” and presents fake reviews on it (Figures 3 through 5 below), allegedly made by the Prime Minister of Greece Konstantinos Mitsotakis and other famous Greek individuals.


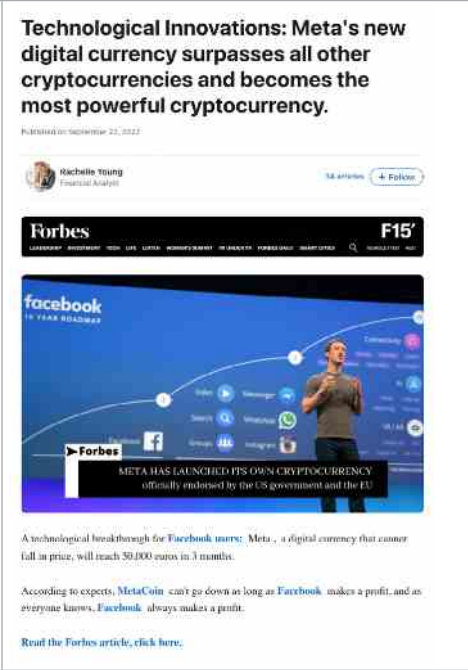
	
Original text (Greek)	Translated text (English)

Figure 3: Fake article about "Meta" coin in Greek and English





<p>Διαβάστε το άρθρο του Forbes, κάντε κλικ εδώ.</p>  <p>“Η φιλοσοφία του Facebook (Metaverse) ήταν πάντα να κάνει τη ζωή των ανθρώπων ευκολότερη και καλύτερη. Αλλά σκεφτόμουν πώς μπορούμε να ανταποκριθούμε στην πραγματική οικονομική ευημερία. Πριν δεν ξέραμε πώς να το κάνουμε, αλλά τώρα έχουμε μια λύση. Το όνειρό μας είναι ένα χρηματονظام που ταυτόχροστα μόλις έχει αρχίσει, το οποίο το καθιστά διαθέσιμο σε όλους, όπως είναι διαθέσιμος να εφοδίων μερικές εκατοντάδες ευρώ για να πάρουν 50.000 ευρώ σε 3 μήνες και 200.000 ευρώ το χρόνο, εκατομμυρια.”</p> <p>Mark Zuckerberg, Διευθύνων Σύμβουλος του Facebook</p> <p>Διαβάστε το άρθρο του Forbes, κάντε κλικ εδώ.</p>  <p>Οι καλύτεροι νομάρχων Meta Digital Coin ξεκίνησαν επίσημα τον Μάρτιο του 2022, επί του παρόντος αυτή τα νομάρχητα μερών να αγοράστούν μόνο μέσω της Meta Coin Group.</p> <p>Στην πραγματικότητα, ο Mark Zuckerberg, διευθύνων σύμβουλος της πολυεθνικής Meta, μας ενημέρωσε ότι η επίσημη τιμή εκκίνησης του νέου νομάρχητα είναι το 0.12 cent.</p> <p>Original text (Greek)</p>	<p>Read the Forbes article, click here.</p>  <p>“ Facebook’s (Metaverse) philosophy has always been to make people’s lives easier and better. But no program can match true financial wellness. Before we didn’t know how to do it, but now we found a solution. Ours is a cryptocurrency that now costs only a few cents, which makes it available to everyone who is willing to spend a few hundred euros to get 50,000 euros in 3 months and 200,000 euros a year, millions.”</p> <p>Mark Zuckerberg, CEO of Facebook</p> <p>Διαβάστε το άρθρο του Forbes, κάντε κλικ εδώ.</p>  <p>Meta Digital Coin sales officially started in March 2022, currently these coins can only be purchased through the Meta Coin Group.</p> <p>In fact, Mark Zuckerberg, CEO of the multinational Meta, informed us that the official launch price of the new coin is 0.12 cents.</p> <p>That’s right, their coin is incredibly cheap compared to other coins out there. Bitcoin, for example, is trading at \$19,336.47 and Ethereum is trading around</p> <p>Translated text (English)</p>
---	--

Figure 4: Altered photo of the Greek Prime Minister with Mark Zuckerberg



<p>Υστερ προεκλογικών έργων την οικονομία να μείνει σε στασιμότητα ο κ. Γιάννης Στουρνάρας με το νέο ψηφιακό νόμισμα της Meta, ο οποίος είναι το ερώτημα.</p> <p>Ο κ. Γιάννης Στουρνάρας επιβεβαιώνει ότι υπολόγισε:</p> <p>“Η μεγαλύτερη ευκαιρία είναι τώρα, η Meta, έλαβε την πρωτοβουλία να προωθήσει ένα νέο ψηφιακό νόμισμα.</p> <p>Αυτό θα αλλάξει την παγκόσμια αγορά, σίγουρα η τιμή του νομάρχητα θα είναι στο υψηλό μέτρο από τώρα. Υψηλότερη από όλα τα υπάρχοντα νομάρχητα.</p> <p>Τα μεγάλα και ισχυρότερα κράτη της ΕΕ και οι ΗΠΑ, ανακοίνωσαν ότι θα τα επιβεβαιώσουν επίσης.</p> <p>Όταν υπολογιστούν τα ψηφιακά νομάρχητα της Meta, πολλές άνθρωποι θα γίνουν εκατομμυριούχοι εν μία νύκτα.</p> <p>Διαβάστε το άρθρο του Forbes, κάντε κλικ εδώ.</p> <p>Γιάννης Στουρνάρας: Οι Έλληνες δεν πρέπει να χάσουν αυτή την ευκαιρία</p> <p>Start Now</p>  <p>Γιάννης Στουρνάρας: Α γρήγορη ευκαιρία</p> <p>Original text (Greek)</p>	<p>In fact, we have the opportunity to find out what Mr. Yannis Stournaras thinks about Meta’s new digital currency, who said the following:</p> <p>Mr. Yannis Stournaras confirms the following:</p> <p>The world’s largest company, Meta, has taken the initiative to promote a new digital currency.</p> <p>This will change the world market, surely the price of the currency will be very high in the near future. Higher than all other cryptocurrencies.</p> <p>The largest and most powerful EU states and the US have announced that they will officially adopt it.</p> <p>When Meta’s digital currency is released, many people will become overnight millionaires.</p> <p>Διαβάστε το άρθρο του Forbes, κάντε κλικ εδώ.</p> <p>Yannis Stournaras: The Greeks should not miss this opportunity</p> <p>Start Now</p>  <p>Yannis Stournaras: A golden opportunity</p> <p>Translated text (English)</p>
---	--

Figure 5: Unrelated photo of Yannis Stournaras: a Greek economist who has been the Governor of the Bank of Greece since June 2014

The LinkedIn profile that posted the fake article about “Meta” coin belongs to a “Rachelle Young” (Figure 6 below), who appears to be a financial analyst from the U.S. state of Colorado and whose profile has more than 500 connections. The recent activity is relevant and of interest because the profile’s owner has posted the same article translated into the same three different languages.

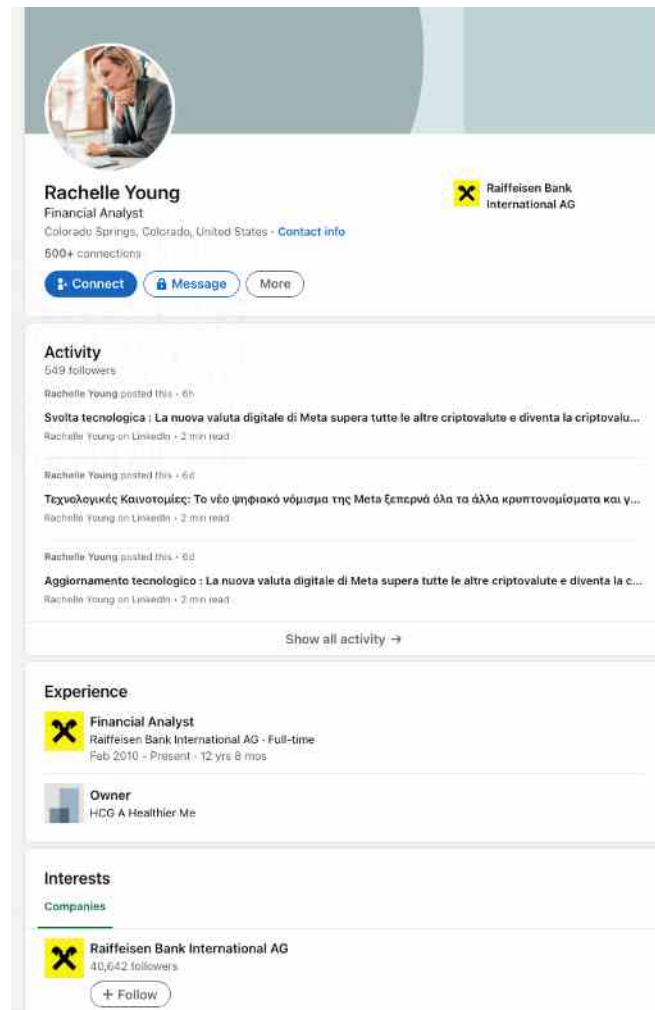


Figure 6: A fake LinkedIn profile posting the same “Meta” coin article in multiple languages

The activity tab on her profile shows that this activity has been going on for weeks.

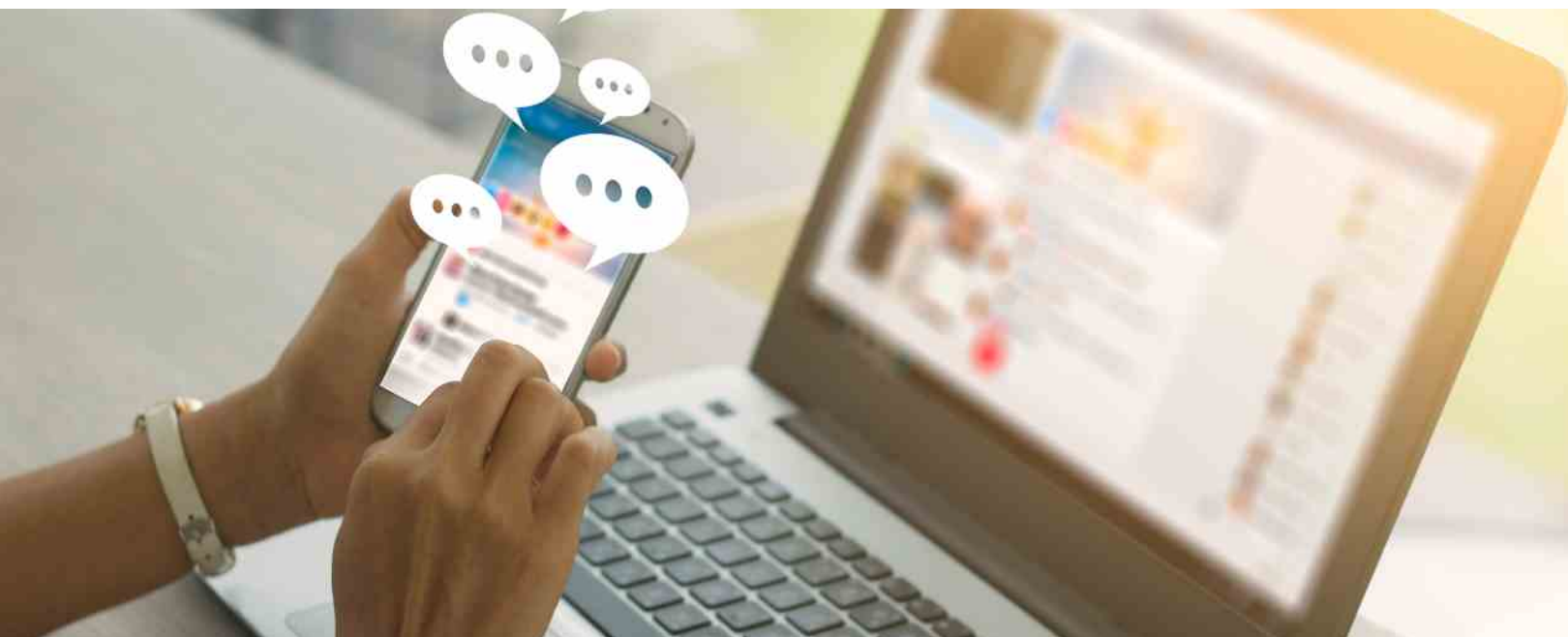




Figure 7: Continuous LinkedIn activity

The actor has posted articles in languages besides Greek and has used photos and stories tailored to those other countries. For example, the screenshots below show altered photos and narratives allegedly relating to Mario Draghi (an Italian public official) and Dietrich Mateschitz (an Austrian businessman).



Figure 8: "Meta" coin scam campaign targeting Italy

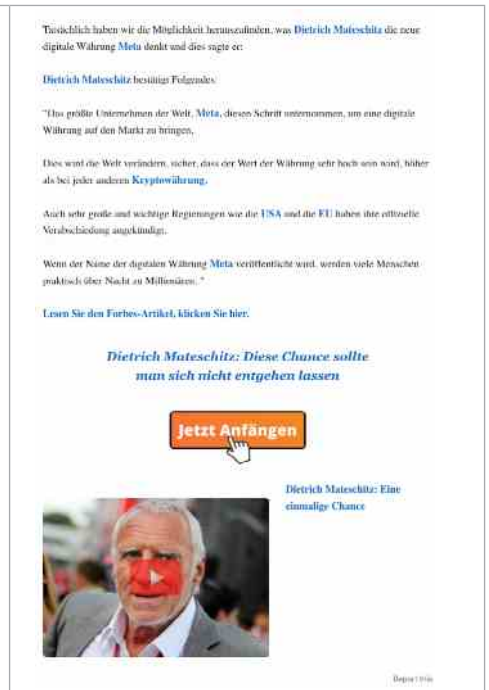


Figure 9: "Meta" coin scam campaign targeting Germany

Stage 3: Landing Pages and Randomly Generated Domains

These fake news articles contain links to two different domains that have the same content, including design and graphs, but they are in two different languages, as shown in Figures 10 and 11.



Figure 10: Altered YouTube image that points to scam website

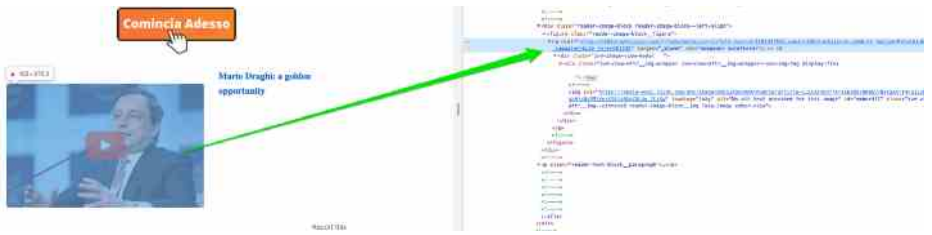


Figure 11: Altered YouTube image that points to scam website

The scam websites embedded in the code of the YouTube images above, are 365coinmode and 365graphiccoin. Both sites host the same page translated into different languages (see Figures 12 and 13). Following them, Figure 14 shows the English language version.

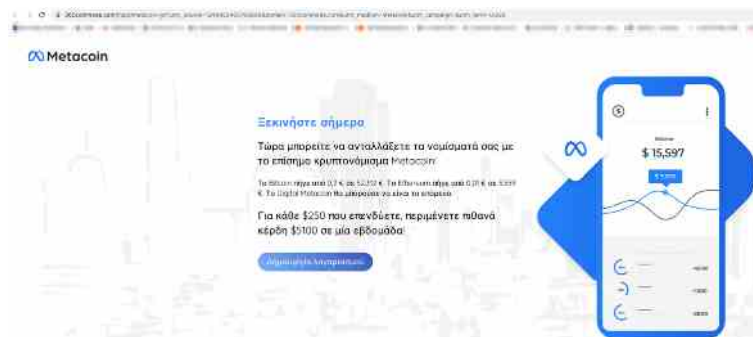


Figure 12: Landing page on 365coinmode[.com], in Greek

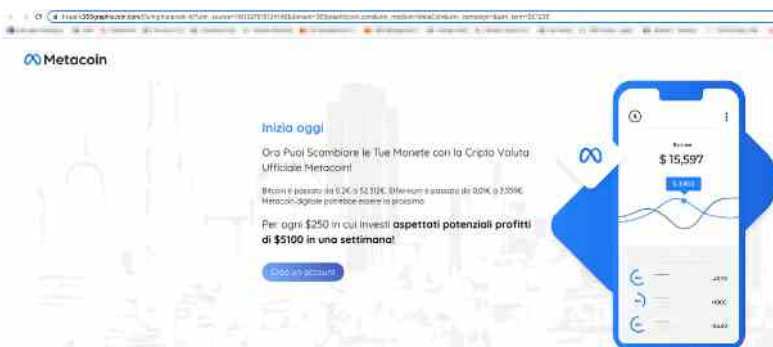


Figure 13: Landing page on 365graphiccoin[.com], in Italian

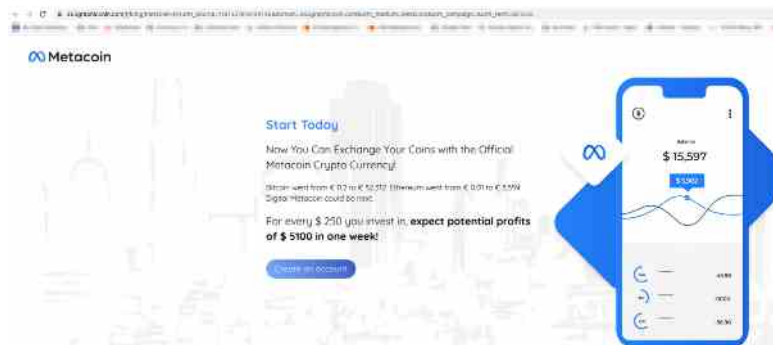


Figure 14: Landing page on 365graphiccoin[.com], in English

Stage 4: Personal Information Gathering

The goal of this particular stage of the campaigns is not to steal any credit card details but instead to have the victims complete a form with their names and phone numbers. The victims then get redirected to fake trading company websites, such as `spartan-trade[.]com` and `networkfsi[.]com`, which ask the victims to make financial deposits. Reports from Greece and the U.K. indicate that the actors use the contact information the victims provided to get in touch with them if they do not make the deposit as requested, in the next stage of the attack, described below. The scammers try to convince the victims that a legitimate investment company is conducting the campaign.

ΑΡΧΙΣΤΕ ΝΑ ΑΛΛΑΞΕΤΕ ΤΗ ΖΩΗ ΣΑΣ ΣΗΜΕΡΑ

Όνομα

Επίθετο

Email

Greece

Αριθμός τηλεφώνου

Δημιουργία λογαριασμού

© MetaCoin Team International SA. Όλα τα δικαιώματα διατηρούνται. Πολιτική Απορρήτου | Πολιτική και ευθύμιση cookies | Επικοινωνία

Original text in Greek

START CHANGING YOUR LIFE TODAY

Name

Adjective

Email

Greece

Phone number

Create Account

© MetaCoin Team International SA. All rights reserved. Privacy Policy | Cookie policy and settings | Contacts

Translated text in Greek

Figure 15: A form for creating a fake account for “Meta” coin

Stage 5: Money Theft

After providing personal details, a victim gets redirected to a fake but visually appealing website. In our tests, we were redirected to Spartan Trading, a fake trading website. It was registered on July 5, 2022, and contains the aforementioned deposit page where a victim is asked to choose an amount of money to deposit. As of this writing, the available payment options are cryptocurrencies and credit cards. The screenshots below illustrate how the cryptocurrency payment system works.

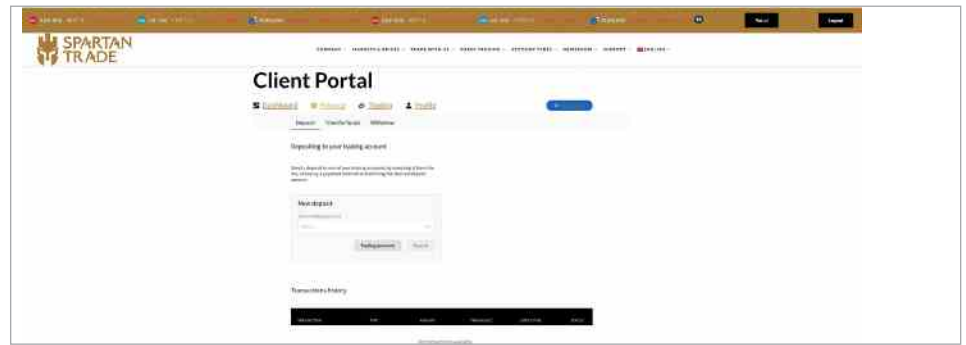


Figure 16: Fake trading website

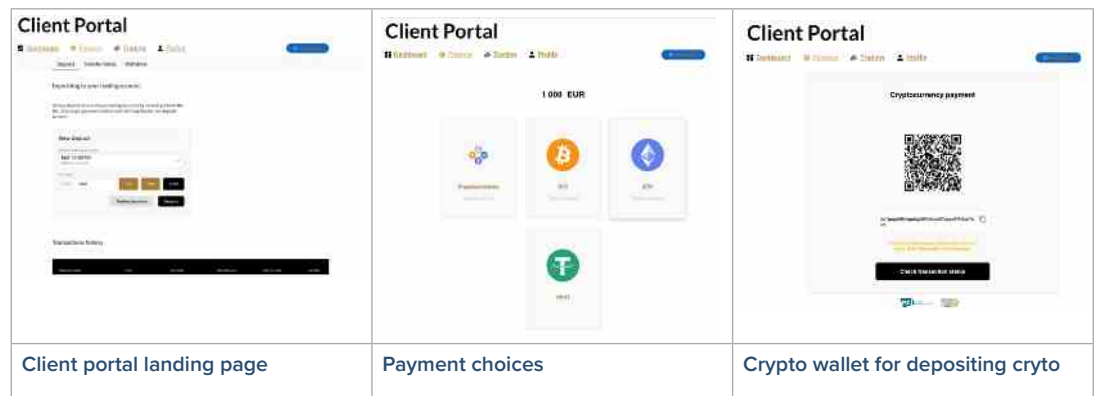


Figure 17: Deposit process for cryptocurrencies

The screenshots in Figures 18 through 21 below show the credit card payment system on the scam website.

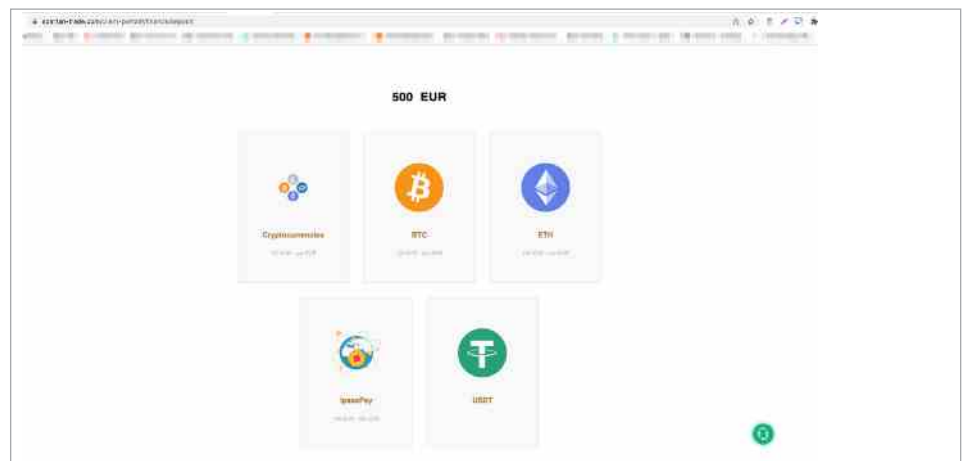


Figure 18: IpassPay option

Client Portal

[Dashboard](#)
[Finance](#)
[Trading](#)
[Profile](#)
[Withdrawal](#)

500 EUR
client deposit funds

Country

State

Submit




Figure 19: Deposit page

Client Portal

[Dashboard](#)
[Finance](#)
[Trading](#)
[Profile](#)
[Withdrawal](#)

Card Info **Billing Info**

Phone Number	Country	State/Province	City
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Address	Zip Code		
<input type="text"/>	<input type="text"/>		

[Previous](#)
[Pay 500.00 EUR](#)

- Please double check the form you submitted to confirm all mandatory fields are completed.
- All payment data is protected by an SSL Certificate and passed to us encrypted.
- Credit card data is stored, processed and transmitted in accordance with PCI data security standards.




Figure 20: Billing info

Client Portal

[Dashboard](#)
[Finance](#)
[Trading](#)
[Profile](#)
[Withdrawal](#)

Card Info **Billing Info**



Credit Card Number

Expiry Date

First Name

Last Name

[Next](#)

- Please double check the form you submitted to confirm all mandatory fields are completed.
- All payment data is protected by an SSL Certificate and passed to us encrypted.
- Credit card data is stored, processed and transmitted in accordance with PCI data security standards.












Figure 21: Billing info

Domain Analysis

All domains that serve the landing pages are registered to Namecheap and resolve to the same IP address, 45 [.] 63 [.] 119 [.] 177, which belongs to Constant Company LLC: a hosting provider that offers global automated cloud infrastructure. In turn, Constant LLC is a parent company for Vultr, which happens to offer free \$100 vouchers for using the platform. This arrangement is a springboard for attackers who have automation in place to deploy and set up scam domains and to operate them cost free. The screenshots in Figures 22 and 23 below show the landing pages belonging to Constant and Vultr that are used to advertise their automated cloud infrastructure and the \$100 promotion for new users.



Figure 22: Constant LLC's landing page

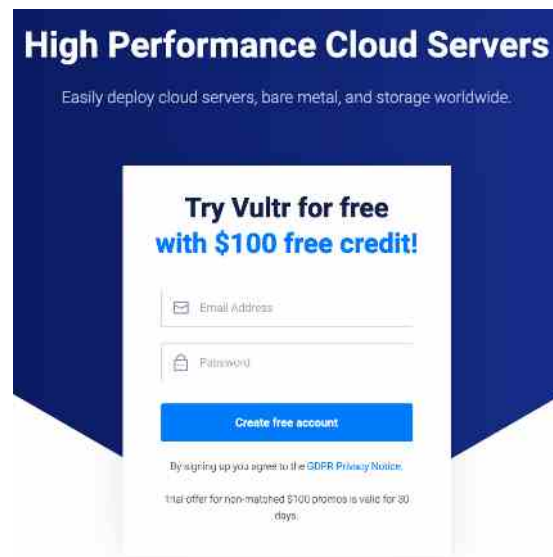


Figure 23: Vultr \$100 promotional offering

Prevention and Mitigation

These malvertising scams have the following features in common:

- The name of the domain involved in a scam is irrelevant to the scam's theme.
- The text of the initial advertisement on Facebook is automatically translated to several languages.
- Typos are easy to spot.
- The parties that own the LinkedIn profiles used in the scams claim to be financial advisors.
- None of the YouTube videos or links to popular domains redirect to any popular domains.
- The faces appearing on the websites are edited or the photos are unrelated and have been taken from other articles.
- There is no phone number or address of the company. Often, these scams are set up from abroad.

To review the indicators of compromise (IoCs), please refer to the full report here: <https://blogs.infoblox.com/cyber-threat-intelligence/cyber-threat-advisory/scams-using-fake-celebrity-endorsements-target-eu-countries/>





Spotlight on India Cyber Threats

Unfortunately, industry and government in India continue to be in the bull's-eye for threat actor activity. And 2022 saw a multitude of cyber attacks hit the Indian healthcare sector and other key industry sectors.

The securities industry also remained a significant target with the revelation that India's second largest securities depository, the Central Depository Services Limited, was the victim of an attack in Q4.

Indian Institute of Medical Services

In November 2022, the India Institute of Medical Services (AIIMS) experienced several outages following a cyber attack. Located in Delhi, AIIMS is one of the largest state-owned hospitals, with capacity for thousands of patients. The downtime associated with the cyber attack impacted hundreds of patients and clinicians who were accessing healthcare services. These services include patient billing, admission, discharge and other related administrative systems. The incident remains under investigation by law enforcement to include the Central Bureau of Investigation and the Intelligence Fusion & Strategic Operations of the Delhi Police.

The AIIMS cyber attack impacted five servers and resulted in the encryption of approximately 1.3 terabytes of data. The IP addresses of two emails linked to the files that were encrypted by the threat actors apparently originated from Hong Kong and China's Henan province. Investigations by CERT-India found that the threat actors were using two email addresses from Protonmail. These included "dog2398" and "mouse63209".

Forensic investigation found WannaCry ransomware, Mimikatz malware and a non-specific trojan. WannaCry, publicized several years ago, took advantage of a vulnerability using a malware hack allegedly developed by a U.S. government entity. WannaCry ransomware contains a worm component. It attempts to exploit vulnerabilities in the Windows SMBv1 server to remotely compromise systems, spread further to additional hosts, and encrypt files.

WannaCry leverages an exploit called EternalBlue and goes on to establish a backdoor known as DoublePulsar to allow for future access to the infected systems. WannaCry spreads by connecting to SMB services on local and internet-facing systems with the vulnerability or running the backdoor. The malware then spreads laterally by attempting connections to all systems on the local network.

During its initial infection, WannaCry checks whether an external domain (killswitch domain) is available. If the killswitch domain can be contacted, the encryption function does not run. The killswitch domains are not a command and control server for the malware and should be monitored but not blocked. If left to run normally, WannaCry will encrypt most files on a machine. The impact of WannaCry could have been reduced or eliminated if computer system software were maintained up to date with

the latest patches and updates. There is more information here on WannaCry from 2017 when its earliest presence was observed: <https://community.infoblox.com/t5/trending-kb-articles/6624-synopsis-on-WannaCry-ransomware-campaign/bap/10092>

The trojan described is a type of malware that appeared to be some form of legitimate software. Once within the network, threat actors are able to carry out most of the activities associated with a legitimate user, such as deleting files, exporting files and data, modifying data and more. Finally, Mimikatz is an open source malware program used by threat actors that can gather credentials such as passwords from endpoints running Microsoft Windows.

Note that the attack upon AIIMS was followed by additional cyber attacks to breach India's top medical research organization, the Indian Council of Medical Research.

Safdarjung Hospital

In Q4, Safdarjung Hospital, another top hospital in Delhi with over 1,500 beds, experienced a cyber attack in November that brought down one server. This attack happened within the wake of the attack upon AIIMS. This attack did not cause data loss and the server was brought back online within 24 hours. The system was restored by government resources to include the National Informatics Centre, which is the Indian government agency responsible for enabling and supporting the nation's government information technology systems.

Central Depository Services Limited

The Central Depository Services Limited (CDSL), one of India's largest security depositories, may have had the data of millions of investors breached in Q4. CDSL holds securities and processes securities transactions.

The CDSL of India reported that malware was found within some of its internal infrastructure servers. This finding was disclosed to the National Stock Exchange in November. The CDSL further reported that no confidential information or investor data was compromised in its initial investigation ("initial findings").

At this time, the nature and type of malware used, and the possible identification of the threat actors, have not been released. Sensitive data potentially exposed might have included full customer names, dates of birth, addresses, contact numbers and more. This data can be used to support phishing activities or other potentially malicious activity.

Government Cyber Alerts

Cybersecurity and Infrastructure Security Agency Alerts: Q4 2022

The [Cybersecurity and Infrastructure Security Agency \(CISA\)](#) is a U.S. government agency that leads a national effort to understand, manage and reduce risk to both cyber and physical infrastructure. CISA connects stakeholders in industry and government to resources, analysis and tools to help them design and build resilient and secure cyber, communications and physical security.

Official CISA updates help stakeholders guard against the evolving ransomware threat environment. These alerts, current activity reports, analysis reports and joint statements are geared toward system administrators and other technical staff to bolster their organization's security posture. These alerts provide timely information about current security issues, vulnerabilities and exploits. More information on CISA alerts is available here: <https://www.cisa.gov/uscert/ncas/alerts>.

These are the CISA Alerts released in Q4 2022:

- AA22-335A: [#StopRansomware: Cuba Ransomware](#)
- AA22-321A: [#StopRansomware: Hive Ransomware](#)
- AA22-320A: [Iranian Government-Sponsored APT Actors Compromise Federal Network, Deploy Crypto Miner, Credential Harvester](#)
- AA22-294A: [#StopRansomware: Daixin Team](#)
- AA22-279A: [Top CVEs Actively Exploited By People's Republic of China State Sponsored Cyber Actors](#)
- AA22-277A: [Impacket and Exfiltration Tool Used to Steal Sensitive Information from Defense Industrial Base Organization](#)



Federal Bureau of Investigation Cyber Alerts: Q4 2022

Official Federal Bureau of Investigation (FBI) updates help stakeholders guard against the ever-evolving ransomware threat environment. These Q4 2022 advisories, FBI Flashes, FBI Private Industry Notifications (PINs) and joint statements are designed to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. All organizations are encouraged to review this advisory for threat details, actor's tactics, techniques and procedures (TTPs), IoCs that can be used to detect if this activity is on your network and actions and mitigations to implement to manage the risk.

Joint Cybersecurity Advisory: Cuba Ransomware

The FBI and CISA released a joint CSA on Cuba ransomware to target a wide range of businesses and critical infrastructure sector organizations, including those in Financial Services, Government Facilities, Healthcare and Public Health (HPH), Critical Manufacturing and Information Technology.

Joint Cybersecurity Advisory: Hive Ransomware

The FBI, CISA and Health and Human Service (HHS) released a joint CSA on Hive ransomware to target a wide range of businesses and critical infrastructure sector organizations, including those in the Government Facilities, Communications, Critical Manufacturing, Information Technology and especially HPH industry sectors.

Joint Cybersecurity Advisory: Daixin Team Leverages Ransomware to Target the Healthcare and Public Health Sector

The FBI, CISA and HHS released a joint CSA on Daixin actors targeting the healthcare and public health sector with ransomware since at least June 2022.



National Security Agency/Central Security Service Advisories and Guidance: Q4 2022

The National Security Agency/Central Security Service (NSA-CSS) leverages its elite technical capability to develop advisories and mitigations on evolving cyber security threats. You can browse or search NSA-CSS repositories of advisories, info sheets, tech reports and operational risk notices listed below. [Some resources have access requirements.](#)

For a subset of cyber security products focused on telework and general network security for end users, view the [NSA Telework and Mobile Security Guidance page here.](#)

- [NSA Cybersecurity Year in Review 2022](#)
- [CSA: APT5: Citrix ADC Threat Hunting Guidance](#)
- [ESF: Potential Threats to 5G Network Slicing](#)
- [NSA CTR: DoD Microelectronics: Field Programmable Gate Array Best Practices - Threat Catalog](#)
- [NSA CTR: DoD Microelectronics: Field Programmable Gate Array Level of Assurance 1 Best Practices](#)
- [NSA CTR: DoD Microelectronics: Field Programmable Gate Array Overall Assurance Process](#)
- [NSA CTR: DoD Microelectronics: Third-Party IP Review Process for Level of Assurance 1](#)
- [ESF: Securing the Software Supply Chain: Customers Slick Sheet](#)
- [ESF: Securing the Software Supply Chain: Recommended Practices Guide for Customers](#)
- [CSI: Software Memory Safety](#)
- [ESF: Securing the Software Supply Chain: Recommended Practices Guide for Suppliers](#)
- [ESF: Securing the Software Supply Chain: Recommended Practices Guide for Suppliers Slick Sheet](#)
- [CSA: Top Common Vulnerabilities and Exposures \(CVEs\) Actively Exploited by People's Republic of China State-Sponsored Cyber Actors \(October 2022\)](#)
- [CSA: Impacket and Exfiltration Tool Used to Steal Sensitive Information from Defense Industrial Base Organization](#)

The Infoblox Threat Intelligence Group

With over 50 years of combined experience, the Infoblox Threat Intelligence Group creates, aggregates and curates information on threats to provide actionable intelligence that is high-quality, timely, and reliable. Threat information from Infoblox filters out false positives and gives you the information you need to block the newest threats and to maintain a unified security policy across the entire security infrastructure of your organization.

Infoblox Threat Intelligence

Infoblox Threat Intelligence provides content and credibility for our security products that is relevant, timely, and centered around DNS. Our priority is on conducting original research, and building out our own tradecraft and algorithm design, rather than on consuming or aggregating third party threat feeds. Our researchers are focused on customer-relevant threat hunting, specifically generating unique intelligence from our own data. This increasingly enables us to get ahead of OSINT reporting and feeds, and protect our customers as early as possible.



Powered by the
Infoblox Threat Intelligence Group

Infoblox is the leader in modern, cloud-first networking and security services. More than 12,000 customers, including over 70 percent of the Fortune 500, rely on Infoblox to scale, simplify and secure their hybrid networks to meet the modern challenges of a cloud-first world.

Corporate Headquarters | 2390 Mission College Boulevard, Ste. 501 | Santa Clara, CA | 95054

+1.408.986.4000 | info@infoblox.com | www.infoblox.com

© 2023 Infoblox, Inc. All rights reserved. Infoblox logo, and other marks appearing herein are property of Infoblox, Inc. All other marks are the property of their respective owner(s).

Infoblox 

