

Muddling Malspam: The Use of Spoofed Domains in Malicious Spam

 blogs.infoblox.com/threat-intelligence/uncovering-actor-ttp-patterns-and-the-role-of-dns-in-investment-scams

Authors: Darby Wise, Piotr Glaska, Laura da Rocha

According to the Federal Trade Commission (FTC), consumers lost more money to investment scams than any other kind in 2024. This equates to a 24 percent increase from 2023 to 2024 in the amount of money lost—a total of US\$5.7 billion¹. These threats take a variety of forms, including the so-called pig butchering scams, which generally start with generic text messages to ones advertised through social media. Sometimes human interaction is involved and sometimes it is not. We track several investment scam actors and we've previously published research on two of them, Savvy Seahorse and Horrid Hawk, who have distinctive DNS fingerprints.

This report expands on our previous publications to consider common techniques, tactics, and procedures (TTPs) of several investment scam actors who lure victims with fake platforms, including crypto exchanges. Fake websites referred to as “profit platforms” are designed to convince users they are dealing with a legitimate business. We've found that the actors often:

- Register large numbers of domains algorithmically over time, a technique we refer to as registered domain generation algorithms (RDGAs)
- Embed similar web forms to collect user data
- Hide their activity through traffic distribution systems (TDS)
- Leverage fake news often featuring spoofed government endorsements, a celebrity, or fake first-hand accounts of the investment program
- Share website structure indicative of the use of a kit

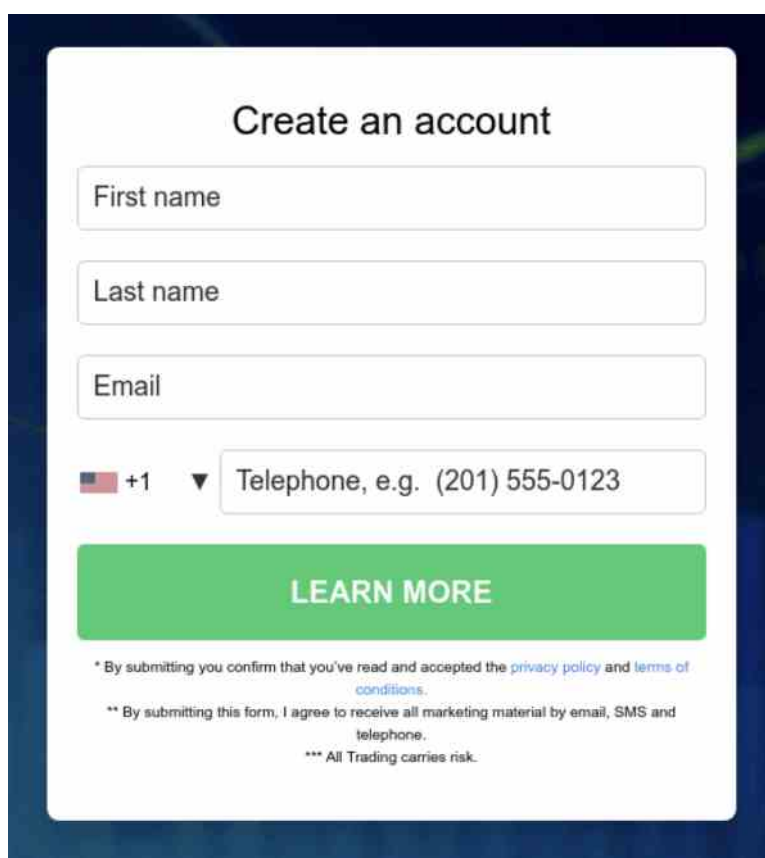
We are often able to discover and track investment scams through DNS fingerprints. Two of the actors detailed in this paper, who we call Reckless Rabbit and Ruthless Rabbit, for example, are tracked through their use of RDGAs.



Embedded Web Forms

While the actors we investigated may use different means to distribute their campaigns, we found that all of them include, at some stage, an embedded web form, which we identified as the first and most notable TTP pattern. For example, Reckless Rabbit creates ads on Facebook that lead to fake news articles featuring a celebrity endorsement for the investment platform. The article includes a link to the scam platform which contains an embedded web form persuading the user to enter their personal information to “register” for the investment opportunity.

The form typically requires the user’s first and last name, email address, and phone number, which automatically formats the country code to match the user’s IP geolocation. Some forms also require the user to create a password and offer the option to auto-generate one for them. Figure 1 below shows an example from a February 2025 scam where we accessed the landing page using a U.S.-based IP address; Figure 2 shows the auto-generated password. The actor uses this information to progress to the next step in the scam—information validation checks.



The image shows a web form titled "Create an account" on a white background with a dark blue border. The form contains four input fields: "First name", "Last name", "Email", and "Telephone, e.g. (201) 555-0123". The telephone field includes a dropdown menu showing a US flag and "+1". Below the fields is a large green button with the text "LEARN MORE" in white. At the bottom, there are three lines of small text: "* By submitting you confirm that you've read and accepted the [privacy policy](#) and [terms of conditions](#).", "** By submitting this form, I agree to receive all marketing material by email, SMS and telephone.", and "*** All Trading carries risk."

Figure 1. Example of embedded web form in a February 2025 investment scam²

EXPERIMENTA UNA SEGURIDAD MEJORADA CON XBITCOIN CLUB

Primer nombre

Apellido

Correo electrónico

YyCsCbZ7RZ

GENERAR CONTRASEÑAS

Spain (España)

+34

Teléfono

EMPODERA TU FUTURO FINANCIERO AHORA

Al registrarse y crear una cuenta, usted certifica que ha leído y aceptado nuestros [Términos y condiciones](#) y [Política de privacidad](#) y [Política de cookies](#). [Leer más](#)

Figure 2. Embedded web form with an auto-generated password field³

Validation Checks

Once the user enters their personal details, most of the campaigns conduct validation checks on the user's information and their IP address. The checks each actor performs can vary, but common ones include:

- Validity of the user's email and/or phone number
- Duplication of emails and/or phone numbers
- Multiple attempts to register using the same IP address within a specific timeframe
- Missing information (name, phone number, etc.)

The scam actors often perform HTTP GET requests to legitimate IP validation tools, such as [ipinfo\[.\]io](#), [ipgeolocation\[.\]io](#), or [ipapi\[.\]co](#). They use these validation checks to filter out traffic from specific countries, security researchers, and/or bots.

In many campaigns, if a user passes the validation, a TDS routes them either directly to the investment scam platform where they are encouraged to transfer money, or to a page that thanks them for registering and says a representative will contact them with additional information. Some campaigns use call centers to provide the victims with

instructions on how to set up an account and transfer money into the fake investment platform. For users who do not pass the validation step, many campaigns will simply display a “thank you” landing page, as shown in Figure 3.

Your order is accepted! Thank you!
We will contact you soon to clarify the details

Figure 3. Ruthless Rabbit’s “thank you” page⁴

Traffic Distribution Systems

Some of the scam actors we’ve researched leverage their own TDSs to collect information about the victim and conditionally make decisions on which web content the user will be redirected to. This is the case for an active crypto scam actor we have been tracking that utilizes a TDS to route users from different countries to different fake investment platforms. Table 1 below shows this actor’s TDS redirections based on the geolocation of the user accessing the crypto scam page [bitcoin-profit\[.\]org](https://bitcoin-profit[.]org). This threat actor routes users from the United States to the legitimate platform eToro, possibly to evade detection from security researchers.

IP Geolocation	TDS Domain(s)	Investment Platform Domain
Switzerland ⁵	mykryplogin[.]com -> murzasanny[.]com	trading[.]nexperts[.]pro
Canada ⁶	powapi[.]net	primeassets[.]uk
Australia ⁷	powapi[.]net → camersyf[.]com	trading[.]xptraders[.]com
United States ⁸	cryptoveteran[.]care	etoro[.]com (legitimate)
Table 1. TDS and redirection domains for a crypto scam campaign. Users accessing bitcoin-profit[.]org from Switzerland and Australia redirect to a secondary TDS domain.		

RDGAs and Dynamic Website Logos

In a previous blog we published in 2023, we introduced the concept of RDGAs:

Registered domain generation algorithms (RDGAs) are a programmatic mechanism that allows actors to create many domain names at once or over time to register for use in their infrastructure. These differ from traditional domain generation algorithms (DGAs) that have long been associated with malware in significant ways. In an RDGA, the algorithm is a secret kept by the actor, and they register all the domain names. In a traditional DGA, the malware contains an algorithm that can be discovered, and most of the domain names will not be registered. While DGAs are used exclusively for connection to a malware controller, malicious RDGAs are used for a wide range of malicious activity.⁹

Since then, we've observed over 3 million RDGA domains on the internet. These domains are commonly used in advertising, so seeing these investment scams intermingled with other product ads makes sense. In the actor-specific sections of this paper below, we will show the distinct RDGA patterns that Reckless and Ruthless Rabbits use to create large sets of domains for their campaigns.

Some actors use dictionary-based RDGAs to generate domain names that match dynamic website names and logos in their scam pages. Each website contains an embedded web form for the user to provide their information. As an example, Figure 4 below shows that the top left corners of the scam websites display the supposed logo of the investment platform/application, matching the domain name. The different pages displayed in Figure 4 have the same or very similar content, but the logo varies depending on the domain name. Scammers leverage the RDGAs to create large sets of domains, which they in turn use to automatically update the logo accordingly, to scale their campaigns.

vasezonix-app[.]trade
vensotixapp-platform[.]store
vasezonixapp[.]guru
vensotixapp[.]click
venzotexapp[.]cloud



aportunex-app[.]shop
aportunex-app[.]trade
aportunex-app[.]wiki
aportunexapp[.]bond
aportunexapp[.]help
aportunexapp[.]trade
aportunexapp[.]wiki



bitcoin-apex[.]guru
bitcoin-apex[.]help
bitcoin-apex[.]website
bitcoinapex-platform[.]click
bitcoinapex-platform[.]guru
bitcoinapex-platform[.]top
bitcoinapex[.]website



Figure 4: Unnamed investment scam actor using the same logo design, where the name on the logo matches the domain name. In this example, the actor creates domains in bulk with the same second-level domain (SLD) label but on several top-level domains (TLDs)^{10, 11, 12}

Other patterns we have seen threat actors use in most of the investment scam campaigns include:

- Distributing scam domains through malicious Facebook ads
- Promising high returns if a user inputs a small amount of money during registration
- Predominantly targeting users in Eastern European countries, such as Russia, Romania, Poland, etc.
- Excluding traffic from certain countries

Investment Threat Actors

As we mentioned at the beginning of the paper, two of the more notable investment scam actors that we are tracking are Reckless and Ruthless Rabbits. They follow many of the common TTPs we've described above, but they also have their own distinguishing characteristics.

Reckless Rabbit

Reckless Rabbit lures victims into fake investment scams through malicious Facebook advertisements. They intersperse them among other content, most commonly items for sale on popular marketplace stores such as Amazon (see Figure 5). This technique of

burying their investment scam ads among other, seemingly innocuous ads may be a trick they use to avoid policy enforcement from Facebook.

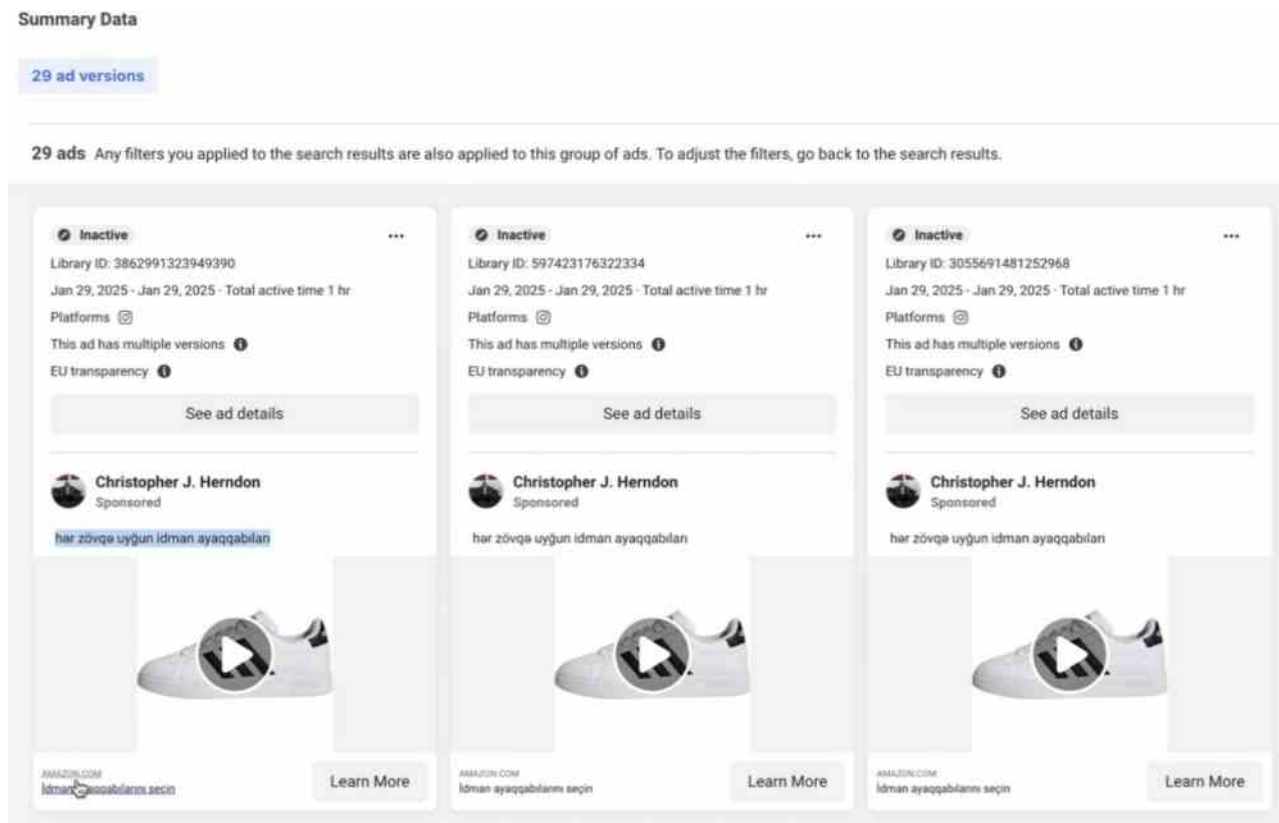


Figure 5: Reckless Rabbit's Facebook ads for products on Amazon

The main scam advertisements take the user to either:

- pages such as a full fake news story, which includes a link to the investment landing page (Figure 6), or
- the investment platform itself (Figure 7).

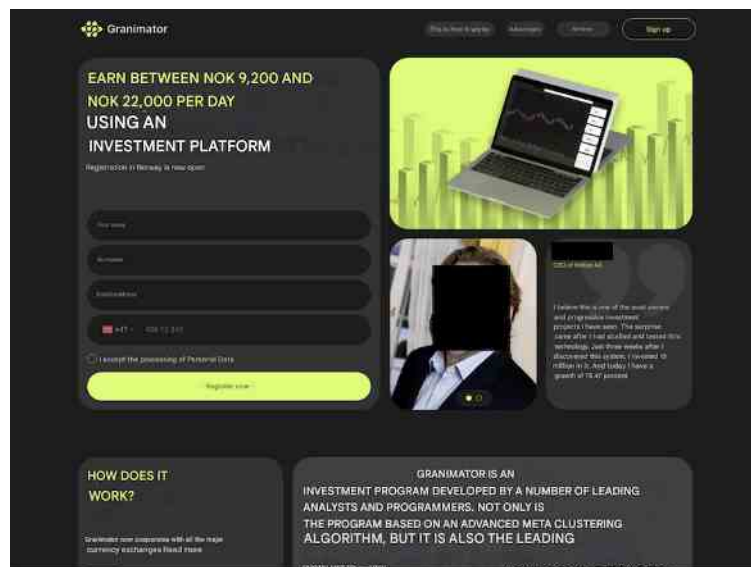


Figure 7: Reckless Rabbit’s investment scam platform in Norwegian and the translation to English. The site contains a web form similar to other investment scam actors¹³ and a fake endorsement from a Norwegian billionaire businessman.

Reckless Rabbit has been creating domains since as early as April 2024, with new domains created on a near-daily basis. Table 2 shows examples of the two RDGA patterns they use to create these domains. The first involves random characters, a three-letter month abbreviation, an English word, and is in the .info TLD. The second pattern combines two or three English words, which may or may not be separated by a dash. The domains in this group are in the .com and .info TLDs.

Domain Pattern

<1-2 random characters><3 letter month><short English word>[.]info

Examples

kcfebdrill[.]info
almarsilk[.]info
iaprwall[.]info
wmaycurr[.]info
fjunmedi[.]info
fjulswap[.]info
faugswap[.]info
ssepcoin[.]info
koctice[.]info
lnovchalk[.]info
qpdecbid[.]info

<2-3 random English words separated by dashes or not>[.]
<com, info>

well-
groomedcanvas[.]com
upkeep-vocal[.]com
extra-largewrinkles[.]info
port-rusty-time[.]com
library-novel-axe[.]com
acoustic-fund-rate[.]info
temple-well-known[.]info
roomyspeedboat[.]info
longmarble[.]info
sixcrowd[.]com
mercifulknife[.]com

Table 2: Reckless Rabbit's RDGA domain patterns and examples

When the victim accesses the fake news website, the actor collects information about the user, such as IP address and geolocation, to determine the language that will be displayed on the page. They use the metadata as input to make a call to an API endpoint they maintain (/api/v1/trigger/field/) to fetch and display the site content appropriately. Figure 8 shows a code snippet of one of the scripts called in the HTTP request chain and includes the API call.

```

<script>
  let l_settings_fullname = '{{settings.full_name_en}}';
  let l_placeholder_fullname = ' ' + '';
  // console.log(l_settings_fullname);
  // console.log(l_placeholder_fullname);

  let l_geo = '{{settings.geo}}';
  let l_language = '{{settings.language}}';

  const isPlaceholder = (value) => value.includes('{{') && value.includes('}}');

  function sleep(milliseconds) {
    const date = Date.now();
    let currentDate = null;
    do {
      currentDate = Date.now();
    } while (currentDate - date < milliseconds);
  }

  const logAndFetch = (url) => {
    // console.log('Fetching GET:', url);
    fetch(url, { method: 'GET' });
  };

  if (!isPlaceholder(l_geo) && !isPlaceholder(l_language)) {
    logAndFetch('/api/v1/trigger/field/' + aio.visit.uuid + '/?landing_geo=' + l_geo);
    logAndFetch('/api/v1/trigger/field/' + aio.visit.uuid + '/?landing_language=' + l_language);
  }
  if (!isPlaceholder(l_placeholder_fullname) && l_placeholder_fullname !== l_settings_fullname && l_placeholder_fullname !== ' ') {
    const encodedPlaceholderFullname = encodeURIComponent(l_placeholder_fullname);
    logAndFetch('/api/v1/trigger/field/' + aio.visit.uuid + '/?celebrity_1=' + encodedPlaceholderFullname);
  }
  sleep(2000);
  if (!isPlaceholder(l_settings_fullname) && l_settings_fullname !== ' ') {
    const encodedSettingsFullname = encodeURIComponent(l_settings_fullname);
    logAndFetch('/api/v1/trigger/field/' + aio.visit.uuid + '/?celebrity_1=' + encodedSettingsFullname);
  }
}
</script>

```

Figure 8. Code snippet of scripts that make an API call to get the language and the page to which the user will get redirected^{14, 15}

We've observed instances where Reckless Rabbit uses validation checks to filter out traffic from specific countries, including Afghanistan, Somalia, Liberia, Madagascar, and others. The code snippet in Figure 9 shows the full list of excluded countries.

```

var iti = window.intlTelInput(formEl.phone, {
  autoHideDialCode: true,
  separateDialCode: true,
  initialCountry: 'country',
  preferredCountries: [...new Set([country, ...possible_countries, country_default])],
  excludeCountries: ['af', 'so', 'lr', 'mg', 'mz', 'ml', 'tj', 'uz', 'by', 'kz', 'cg', 'cd', 'er', 'kg', 'ly', 'na', 'sy', 'am'],
  utilsScript: '../regv2/files/js/intlTelInput-utils.js',
});

```

Figure 9: Code snippet that shows a variable for countries to be excluded^{16, 17}

Reckless Rabbit configures wildcard DNS responses to their domains, which means that a query to any subdomain (e.g., wildcardbiddbanpdla[.]brilliantwallaby[.]info) of their domains will return a response, as shown in Figure 10. Wildcarding generates noise in DNS because it means anyone can make a query to any subdomains for that SLD, and the subdomains will return responses. This makes it difficult to determine which subdomains are actively being used by an actor, and which subdomains are random queries triggered by, for example, security researchers. In this case, security tools may not add the SLD to their feeds and instead only add the subdomains that were confirmed to contain malicious content, thereby helping the actor to use their domains longer.

```

; <<>> DiG diggui.com <<>> @8.8.8.8 wilcardbdidbanpdla.brilliantwallaby.info A
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14684
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;wilcardbdidbanpdla.brilliantwallaby.info. IN A

;; ANSWER SECTION:
wilcardbdidbanpdla.brilliantwallaby.info. 300 IN A 104.21.93.207
wilcardbdidbanpdla.brilliantwallaby.info. 300 IN A 172.67.214.119

;; Query time: 16 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Tue Mar 11 19:59:37 UTC 2025
;; MSG SIZE rcvd: 102

```


Figure 10. Wildcard response behavior to a random subdomain of an existent Reckless Rabbit domain

Reckless Rabbit uses several additional techniques to avoid detection, including:

- Interspersing ads that redirect to the investment scam between ads for items supposedly being sold on popular marketplaces, such as Amazon (Figure 11)
- Adding unrelated images to avoid detection based on image recognition (Figure 12)
- Displaying (in the ad) a decoy domain that is different from the domain that the user will be redirected to once they click on the link (Figure 13)
- Using a decoy page with non-suspicious content—such as a website for a restaurant—on the SLD, shielding the actual investment scam page hosted on the full URL (Figure 14)

Ad Details

זוגות גרביים אלסטיים באורך הקרסול Eurzom 10
גרבי כותנה אסתטיים גרביים חמודים גרביים קלי
משקל בגזרה נמוכה לנשים בנות








AMAZON.COM
זוגות גרביים Eurzom 10
לסטיים באורך הקרסול גרבי

Learn More

This ad has multiple versions ⓘ

3 of 6



Close

Figure 11. Investment scam lure mixed with items being sold in marketplaces

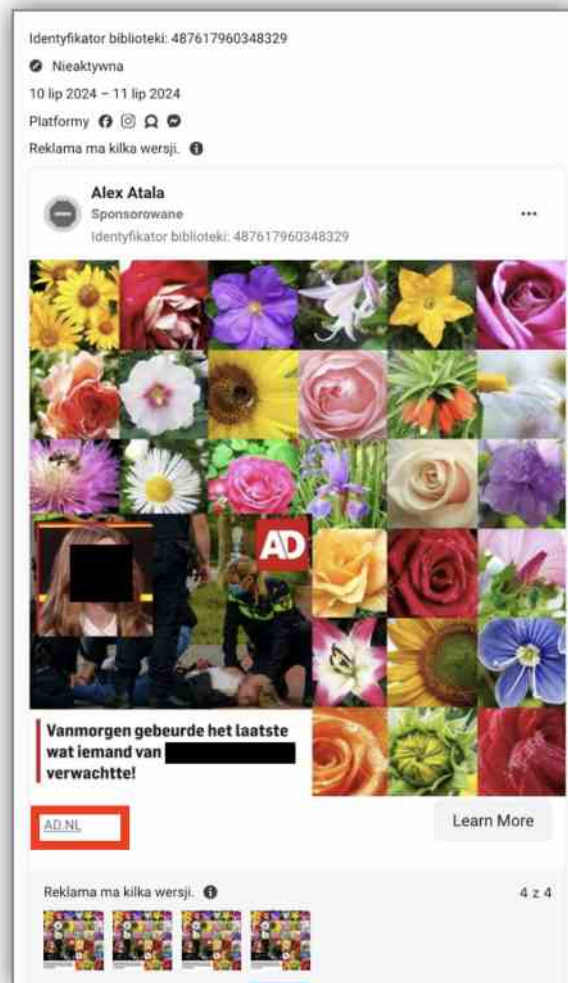


Figure 12. Technique to prevent detection by image recognition-based security technology

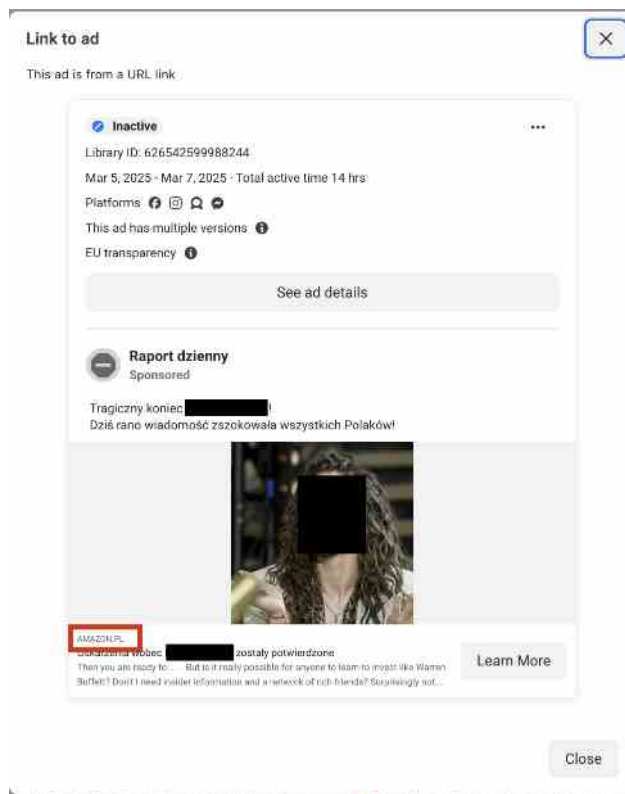


Figure 13. Example of Facebook ad caption with decoy domain, amazon[.]pl. The ad redirects to a URL under tyxarai[.]org and is associated to wjulbucks[.]info^{18, 19}



Figure 14. Decoy page with non-suspicious content on the SLD²⁰

Ruthless Rabbit

Ruthless Rabbit has been running investment scam campaigns since at least November 2022. These campaigns follow similar themes to those we have seen from Horrid Hawk and other Russian-hosted scam campaigns that primarily target users in Russia, Poland, Romania, and Kazakhstan, among other countries. Most current active campaigns are hosted on two dedicated IPs, but the actor has previously used at least eight different IPs hosted with Aeza, as well as a dedicated IP hosted with IROKO. Combined, these IPs host over 2,600 actor-owned domains. They use Namecheap for domain registration, name servers and mail servers.

In May 2024, Ruthless Rabbit began using a single RDGA pattern to create the large number of domains necessary to operate their scams (see Table 3).

Domain Pattern	Examples
<random English word or 3-7 random characters><bik, job, mot, lin, tyt, byk, bot, fat, pit, kot, etc.>[.]pro	topsmot[.]pro sitemot[.]pro viserbik[.]pro goaljob[.]pro somajob[.]pro wasakot[.]pro

Table 3. Ruthless Rabbit RDGA pattern and examples

Campaign Themes

In February 2023, Ruthless Rabbit started hosting Baltic Pipe financial scam pages, a common theme used in investment scams targeting Eastern European users. Over time, they diversified the themes of their landing pages, to include scams spoofing WhatsApp, Google Finance, and Meta. The most prevalent campaign theme since May 2024 is a news article spoofing the Russian-language news website “Channel One” that claims users who sign up for the “GazInvest” platform will earn up to 300,000 Russian rubles. This page (see Figure 15), shares the common TTP patterns we mentioned above, including lures of high returns, an embedded web form, and IP geolocation tools for conducting validation checks.

Екатерина Андреева · 10.03.2025

«ГазИнвест» запустил умную платформу для повышения благосостояния россиян! Новое **БЕСПЛАТНЫЙ СЕРВИС ПОМОГАЕТ ЗАРАБАТЫВАТЬ ОТ 300 000 РУБЛЕЙ** без специальных знаний и опыта



Новый колоссальный финансовый прорыв от «ГазИнвест» — компания выпустила сервис, доступный всем без исключения гражданам России. С помощью новой интернет-платформы крупнейшая российская корпорация планирует **многократно увеличить доходы россиян и повысить общий уровень благосостояния населения страны.**

На минувшем нефтегазовом форуме руководитель дирекции по цифровой трансформации «ГазИнвест» Яков Чернов анонсировал уникальный сервис для обогащения россиян, аналогов которому нет нигде в мире — онлайн-систему «ГазИнвест».

По его словам, сейчас главной целью цифровой трансформации компании является радикальное повышение качества жизни и благосостояния россиян. Именно поэтому компанией была разработана платформа на основе уникальных советских (!) технологических разработок, которые долгое время оставались под грифом «секретно».

Важно! Чтобы подключиться к онлайн-системе «ГазИнвест», нужно быть гражданином Российской Федерации старше 18 лет.

Figure 15. Landing page for the Russian GazInvest scam²¹

The actor hosts their scam landing pages on specific URL paths that change per campaign theme. They use a concealment technique of giving users who attempt to access the SLD alone rather than a URL—a typical move for security researchers—an HTTP 404 Not Found error. Table 4 shows examples of the URL paths for some of the most prevalent campaigns. We’ve broken out the SLDs and the URL paths because the latter are what the actor changes every couple of months.

Campaign Theme	SLD	URL Path
January 2025 – GazInvest Platform ²²	brudamot[.]pro	/4YJ3LH? MPC_3=16k3ua14tff7k
September 2024 – GazInvest Platform ²³	dropbik[.]pro	/lander/gazinvestgaz_4301/

Campaign Theme	SLD	URL Path
March 2025 – Spoofed Google Finance Page ²⁴	easyjob[.]pro	/google_finance_79/
December 2024 – Fake Russian News Site ²⁵	kinabik[.]pro	/JF5vNK? MPC_3=2pgkm0e57koso

Table 4. Examples of URL paths for different SLDs and campaigns

What’s interesting about Ruthless Rabbit is that they operate their own cloaking service to perform validation checks; the cloaking service domain (mcrafterdb[.]tech) hosts publicly available documentation for their API titled “Mcraft MediaCraft Tech API.” The documentation (Figure 16) provides insight into some of the actor’s validation checks on “leads,” or users, who enter personal information into the forms embedded in the investment scam pages. The cloaking service looks for users entering duplicate information or attempting to access the investment platform multiple times within the previous 20 minutes using the same IP address. Users who do not pass the checks will be redirected to either a 404 Not Found error page or to another page on the SLD titled **thanks.html**, which states someone will contact them for additional information. Figure 17 shows the form script the actor uses for this API call.

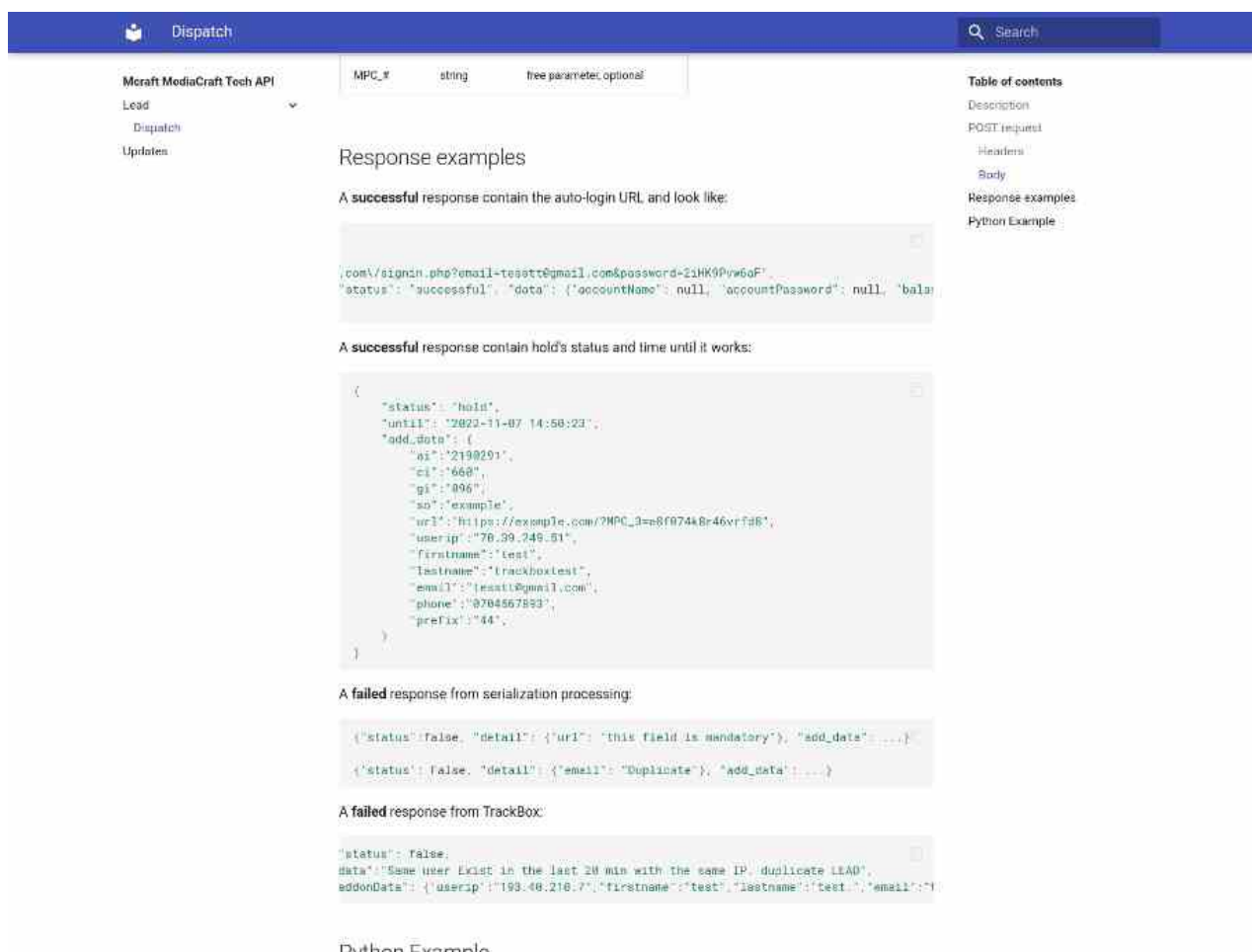


Figure 16. API documentation for the actor’s validation API²⁶

```

$('form').submit(function (event){
    $(this).submit(false);
    event.preventDefault();
    event.stopPropagation();
    event.stopImmediatePropagation();
    if($('.iti__selected-dial-code').length){
        var prefix = $('.iti__selected-dial-code').html().slice(1)
        $(this).append('<input type="hidden" name="prefix" value="'+prefix+'" /> `')
    }
    var host = `&host=${$(location).attr('hostname')}`
    var url=`&url=${$(location).attr('href')}`
    var so=`&so=Google Finance`
    var args = host + url + so
    var search = location.search.substring(1);

    $.ajax({
        type: "POST",
        url: 'https://mcrafterdb[.]tech/api/v1/submit/a6111ace-7304-4d9b-8dfe-9aafb7e9638e/' + "?" + search,
        data: $(this).serialize() + args,
        headers: $(this).headers,
        dataType: 'json',
        crossDomain: true,
        success: function (response) {
            if (response.status === true) {
                document.location.replace(response.data);
            } else {
                document.location.href = location.protocol + '//' + location.host +
location.pathname.substring(0, location.pathname.lastIndexOf('/') + 1) + 'thanks.html';
            }
        },
    })

    var btn = $(this).find(':submit')

    btn.prop('disabled', true)
    setTimeout(function () {
        btn.prop('disabled', false)

    },30000)
})

```

Figure 17. API call used by Ruthless Rabbit to perform validation checks on the user²⁷

Interestingly, none of the forms in these campaigns have a field to enter an email address, but the response examples in Figure 16 indicate an email is required. We discovered that embedded into the HTML code is a script with a function `generateRandomEmail()`, (see Figure 18), that generates a new email address in the hidden form field every time the page is refreshed. This indicates that the actor may not actually use the phone number and email address to contact the user but instead uses

them only to perform the validation checks. Most of the campaigns do, however, perform checks on the user's IP geolocation via `ipgeolocation[.]io` and `ipinfo[.]io`, two legitimate geolocation lookup tools.

```
$('#form').submit(function (event) { var phone = $(this).find("input[name=phone]"); var phone_val = phone.val(); phone_val = phone_val.replace(/[^0-9]/g, ''); if (phone_val[0] == 0) { phone_val = '7' + phone_val.substring(1) } else if (phone_val[0] != 7) { phone_val = '7' + phone_val } $("input[name=phone]").val(phone_val) var btn = $(this).find('submit') btn.prop('disabled', true) setTimeout(function () { btn.prop('disabled', false) }, 3000) return true; }) function generateRandomEmail() { var chars = 'abcdefghijklmnopqrstuvwxyz1234567890'; var domain = ['gmail.com', 'yahoo.com', 'hotmail.com', 'outlook.com']; var usernameLength = Math.floor(Math.random() * 18) + 5; var email = ''; for (var i = 0; i < usernameLength; i++) { email += chars.charAt(Math.floor(Math.random() * chars.length)); } email += '@' + domain[Math.floor(Math.random() * domain.length)]; return email; } // Set random email in hidden input var randomEmail = generateRandomEmail(); document.getElementById('email').value = randomEmail;
```

Figure 18. HTML code showing the `generateRandomEmail()` function

Users who pass the validation checks will be routed to some sort of investment platform where they will be prompted to enter their financial information to complete the registration for the investment program. After numerous tests, however, we were unable to successfully reach that final step. Despite passing the validation checks for all personal details, including the IP geolocation and phone number, we still received a failed response stating, “Cant register lead, no more fallbacks available;”. Oddly enough, there was no information on this type of response in the actor's API documentation.

The Importance of DNS

Threat actors operating these large-scale and increasingly sophisticated scams exploit DNS to help build and maintain their infrastructure. Over the years, actor abuse of DNS mechanisms, such as RDGAs and TDSs, has been underreported in the security community, despite being crucial to malicious campaigns.

Some investment scam actors capitalize on malicious TDSs to operate their campaigns. A TDS enables threat actors to strengthen their infrastructure, making it more resilient by providing the ability to hide malicious content from security researchers and bots. For example, one actor we've been tracking uses an HTTP-based TDS to shield their malicious scam landing pages. We show an instance of a redirection chain in their campaign in Figure 19. Only by tracking these TDSs through DNS are we able to detect and block the infrastructure at scale, before the redirections even occur.

```
1. https://aportunexapp.top/ Page URL
2. https://aportunexapp.top/ HTTP 302
   https://aportunexapp-r.top/v1 HTTP 301
   http://aportunexapp-r.top/v1/ HTTP 307
   https://aportunexapp-r.top/v1/ HTTP 302
   https://aportunexapp/?referrer=Unknown&key= HTTP 301
   https://globalvisitclub.com/cf/r/679f6a249b1d3500124a6d22?campaign_name=aportunex.app&lang=de_DE HTTP 302
   https://devotaverage.online/DE/var6/page.php?aff_sub3=Bit%20App&user_id=164&funnel=Aportunex%20App&aff_sub=538843fb-d2d8-4078-b0c4-247ad202f569
   Page URL
```

Figure 19. Redirection chain for an investment scam actor's TDS²⁸

Actors also take advantage of RDGAs to create large numbers of domains to use in their campaigns, which enables them to hide in plain sight and change out domains often. As we wrote last summer:

“Scammers use RDGAs for the same reasons that other threat actors use them: their domains are frequently blocked or taken down by service providers. Consequently, it’s advantageous for them to have a steady stream of new domains with which to execute their scams.”

Conclusion

There are so many RDGA domains created every day that it is impossible for human researchers to find and assess them all. Through the lens of DNS, we are able to leverage automated detection and correlate these investment scam domains at scale. Threat actors like Reckless and Ruthless Rabbits will be relentless in their attempts to trick as many users as possible. Because these types of scams have proven to be **highly profitable** for them, they will continue to grow rapidly—both in number and sophistication.

Indicators of Activity

Indicator	Note
middle.sturdypants[.]com brilliantwallaby[.]info encouragingtax[.]info tyxarai[.]org upkeep-vocal[.]com extra-largewrinkles[.]info port-rusty-time[.]com library-novel-axe[.]com acoustic-fund-rate[.]info temple-well-known[.]info roomyspeedboat[.]info longmarble[.]info sixcrowd[.]com mercifulknife[.]com wjulbucks[.]info kcfedrill[.]info almarsilk[.]info iaprwall[.]info wmaycurr[.]info bmaypost[.]info fjunmedi[.]info fjulswap[.]info faugswap[.]info ssepcoin[.]info koctice[.]info lnovchalk[.]info qpdecbid[.]info	Indicators used by Reckless Rabbit in investment scam campaigns

bortjob[.]pro topsmot[.]pro sitemot[.]pro viserbik[.]pro goaljob[.]pro somajob[.]pro wasakot[.]pro brudamot[.]pro dropbik[.]pro easyjob[.]pro kinabik[.]pro	Domains used by Ruthless Rabbit in investment scam campaigns
---	--

Indicator	Note
bitcoineverestai[.]app bitcoin-eprex[.]com echelonyieldai[.]app eco-terra[.]app everix-edge[.]org gptifexai[.]com immediatebitwave[.]app immediateluminary[.]com immediatemomentum[.]site quantumflash[.]org solidreturn[.]app	Sample of domains used by an unnamed actor for investment scams
vensotixapp- platform[.]store vasezonixapp[.]guru vensotixapp[.]click venzotexapp[.]cloud oportunex[.]app oportunex-app[.]shop oportunex-app[.]trade oportunex-app[.]wiki oportunexapp[.]top oportunexapp[.]bond oportunexapp[.]help oportunexapp[.]trade oportunexapp[.]wiki bitcoin-apex[.]guru bitcoin-apex[.]help bitcoin-apex[.]website bitcoinapex-platform[.]click bitcoinapex-platform[.]guru bitcoinapex-platform[.]top bitcoinapex[.]website	Sample of RDGA and registered DDGA domains used by an unnamed actor for investment scams

Footnotes

1. <https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024>
2. <https://urlscan.io/result/f217e772-6deb-4cbc-88fd-b6b46363494e>
3. <https://urlscan.io/result/0195f7b6-1cda-77ce-aadd-22dda511aa0e>
4. <https://urlscan.io/result/aca53e46-291b-46bd-bc67-76179d82c20a/>
5. <https://urlscan.io/result/0195d87a-5ee5-7228-b6e3-c1968ffc562b/>

6. <https://urlscan.io/result/0195ce8b-6b4e-7770-b8d5-cea621d1b835/>
7. <https://urlscan.io/result/0195ce8e-3549-700b-addc-64a4879a5ef2/>
8. <https://urlscan.io/result/0195fd9d-9679-736a-8652-99397922991a/>
9. <https://insights.infoblox.com/resources-research-report/infoblox-research-report-registered-dgas-the-prolific-new-menace-no-one-is-talking-about>
10. <https://urlscan.io/result/0ba64979-2186-44ed-858e-51f030c9651b/>
11. <https://urlscan.io/result/4859f1d7-d337-4f5e-bfb0-e3a8d677a77b/>
12. <https://urlscan.io/result/567a05cb-cae2-4937-a326-2f314c289720/>
13. <https://urlscan.io/result/924de331-a6ff-45f7-a4cc-cb13ca93f23f/>
14. <https://urlscan.io/result/3f999960-0b0f-4cfe-96ae-78cebca95290/#transactions>
15. <https://urlscan.io/responses/23fb5db0618f6a48381978574a34168554a6ecd14f7d21a1d754d27a8ca4eea8/>
16. <https://urlscan.io/result/924de331-a6ff-45f7-a4cc-cb13ca93f23f/#transactions>
17. <https://urlscan.io/responses/7402355aa0d7eb0248bf6fdb572a43e6457e5c1b26719147464ea224e5009a7/>
18. <https://urlscan.io/result/01956c44-fe9a-7113-a0c8-f025f9d4dc9e>
19. <https://urlscan.io/result/01956c44-fe9a-7113-a0c8-f025f9d4dc9e#links>
20. <https://urlscan.io/result/019585ef-23c0-7000-bdaf-babc56433b08>
21. <https://urlscan.io/result/01958f39-aa3e-7001-ab7d-fbe0e3bab026>
22. <https://urlscan.io/result/8c5fe52a-e2c3-4300-8a84-320d79e878da/>
23. <https://urlscan.io/result/5c149a21-977b-4cf7-ae02-7095bf8ac54d/>
24. <https://urlscan.io/result/fe9b35b4-910d-40a5-8edb-e0babdf75740/>
25. <https://urlscan.io/result/f90ad3c0-a347-4272-abba-d4e2357c3cb6/>
26. <https://urlscan.io/result/f1273504-36df-4db5-9a7f-2532594d0d04/>
27. <https://urlscan.io/responses/7b3001eef10d518496867654ec76e4f3c6c33550d7a67780ce0440a4c28b5b50/>
28. <https://urlscan.io/result/85e9ce2c-92f5-48ba-8dfd-ed47d63a9eca/#redirects>