infoblox

Threat Intel

RESEARCH PAPER

REGISTERED DGAs:

THE PROLIFIC NEW MENACE NO ONE IS TALKING ABOUT

Author:
Infoblox Threat Intel

TABLE OF CONTENTS

EXECUTIVE SUMMARY

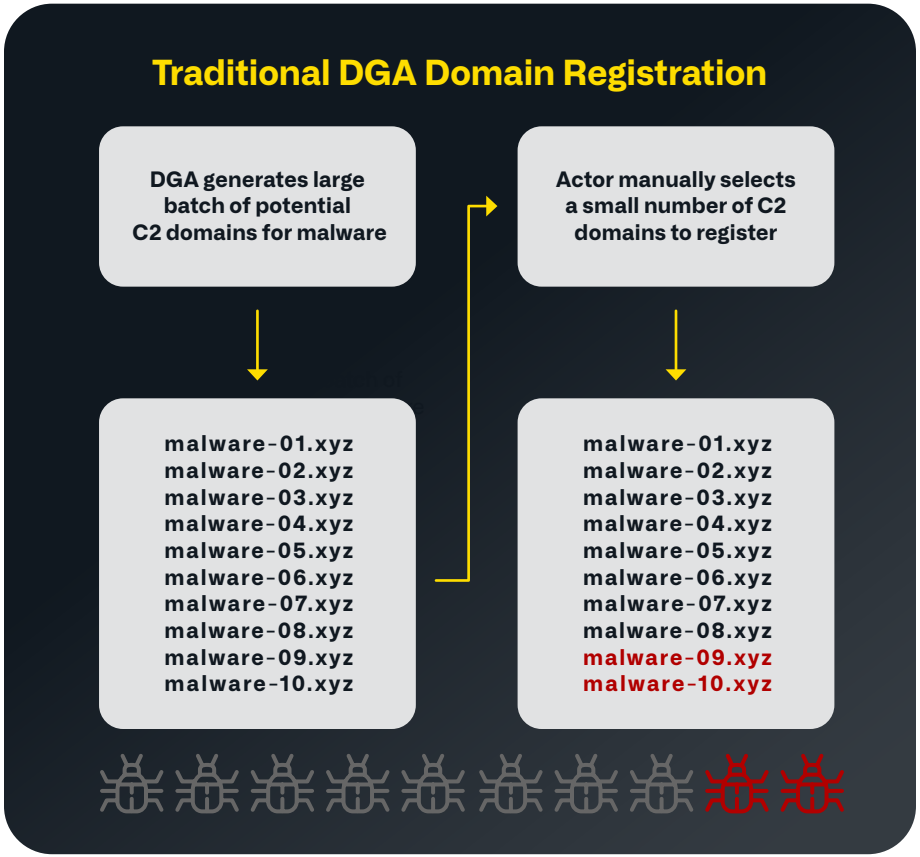
For nearly two decades, threat actors have used domain generation algorithms (DGAs) to distribute malware, adware, phishing campaigns, and other illegal content. In recent years, threat actors have been employing a technique we call registered domain generation algorithms (RDGAs), in which the actor uses an algorithm to register many domain names at one time. RDGAs are considerably harder to detect and defend against than traditional DGAs, and despite their prevalence on the internet, they have been woefully underreported by the security community. In this paper, we will share what we've learned about the quiet proliferation of RDGA threats and their massive impact in the current threat landscape.

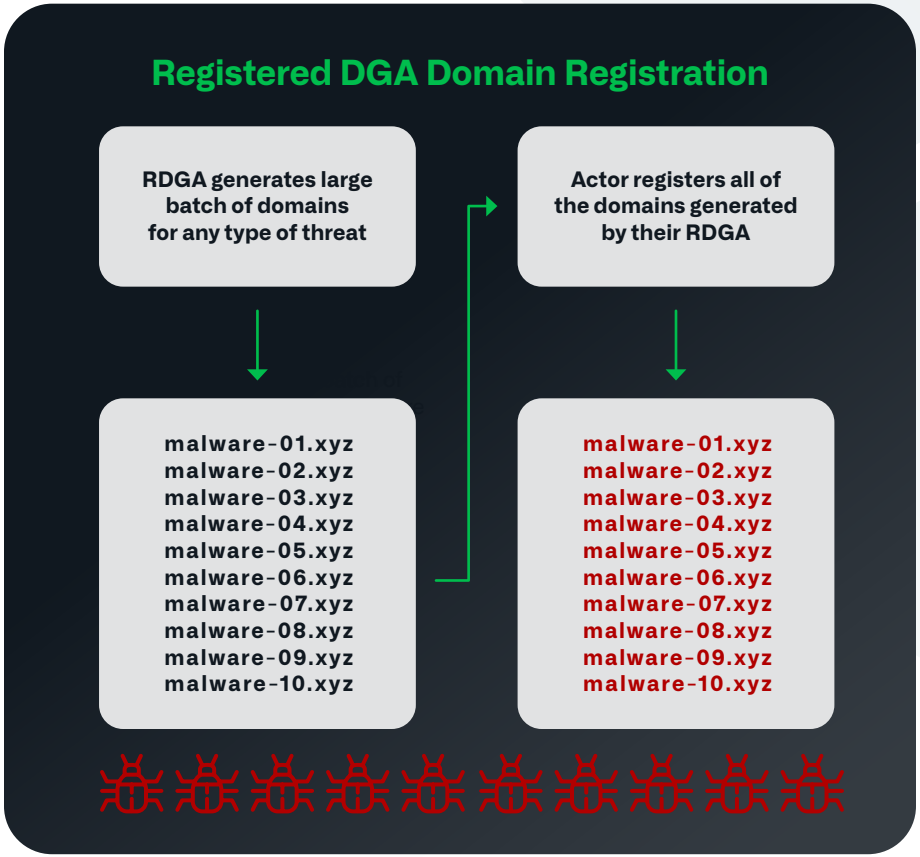
Renée Burton
VP Infoblox Threat Intelligence

WHAT EXACTLY ARE RDGAs?

Registered Domain Generation Algorithms (RDGAs)

Registered domain generation algorithms (RDGAs) are a programmatic mechanism that allows threat actors to create many domain names at once, or over time, to register for use in their criminal 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 threat 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, RDGAs are used for a wide range of malicious activity.





BACKGROUND

In short, traditional DGAs are algorithms embedded in malware to generate an arbitrary number of potential command and control (C2) domains that the malware attempts to contact, but the threat actor only registers a few of those domains.

Traditional DGAs are vulnerable to security researchers who can reverse engineer the algorithms once the malware samples become publicly available in platforms such as VirusTotal. The fact that only a few of the domains that the malware attempts to contact are actually registered leads to an unusually high number of NXDOMAIN responses that are easy to detect in DNS. By contrast, RDGAs are private algorithms that threat actors employ to generate an arbitrary number of domains that they will register and use. As such, security researchers can only infer how an RDGA's algorithm works based on large-scale analysis of registered domains, and since the domains are all registered, they don't produce the same distinctive pattern of NXDOMAIN responses as a traditional DGA.

In the same way that the concept of dictionary DGAs (DDGAs) was introduced to distinguish algorithms that generate domains using real words rather than random characters, we're using the concept of RDGAs to distinguish algorithms that threat actors use to privately register large numbers of domains from algorithms embedded in publicly-available malware to make their C2 communications more difficult to disrupt.

WHY CALL IT RDGA?

We coined this new phrase and acronym because the term "DGA" has become broadly overused in the years since the concept was introduced, effectively serving as an umbrella term for any domain that is (or appears to be) algorithmically generated.

WHAT DO RDGAs LOOK LIKE?

JUST LIKE TRADITIONAL DGAS, RDGAS COME IN ALL SHAPES AND SIZES.

Some look like prototypical DGAs with seemingly random characters and a high degree of entropy, as **Figures 1 and 2** show:

1

Prototypical DGA used by a SocGholish/TA569 affiliate

6rnd9mitqt1rz82[.]top
7r7suw52ls00i20[.]top
9w9ohb5vky5p3dz[.]top
bjbntaxmh09r09e[.]top
qcj4pirltkpqrcu[.]top

2

RDGA for a weight loss pill scam

h87e1mbm0u5f85[.]xyz
n8j1nau3os4otr[.]xyz
xnnxr1jquyupjc[.]xyz
xqajkr8fbrdryp0[.]xyz
xryqcgcb2upb28k[.]xyz

Figure 3 shows that other RDGAs use nonsensical combinations of dictionary words like a traditional DDGA:

3

VexTrio RDGA

arriveplanetsnow[.]buzz
coatthinkverb[.]buzz
debtgenepub[.]live
poemtrainsurprise[.]top
quarterneighbourforward[.]xyz

RDGAs COME IN A VARIETY OF FORMS

h87e1mbm0u5f85[.]xyz
n8j1nau3os4otr[.]xyz
arriveplanetsnow[.]buzz
coatthinkverb[.]buzz
debtgenepub[.]live
lasalleparishjail[.]org
areas-diplom24[.]com
areas-diplomy24[.]com

WHEN BATTLING RDGAs, DNS MATTERS

Detecting and blocking RDGAs requires access to large-scale DNS data and enough DNS expertise to properly analyze it.

Some RDGAs use a limited set of dictionary words in a more structured format in order to fit a theme, like this set of domains in **Figure 4**, whose names correspond to various regional jails:

4 **RDGA with a regional jail theme**

castrocountyjail[.]org
killeencityjail[.]org
lasalleparishjail[.]org
miamidadecountyjail[.]org
northcentralregionaljail[.]org

Still other RDGAs generate variations of a single domain name by inserting, shifting or deleting characters from the base domain name (**see Figure 5**). More often than not, the character changes in these variant domain names follow some sort of structure so that the generated domains are still somewhat intelligible and similar to the base domain, like the following set of RDGA domains for a Russian diploma mill:

5 **RDGA for a Russian diploma mill**

arenadiploma[.]com
area-diploman24[.]com
area-diplomans24[.]com
area-diploms24[.]com
area-diplomy24[.]com
areas-diplom[.]com
areas-diplom24[.]com
areas-diplomy24[.]com
arena-diplomsy24[.]com
arena-diplomy24[.]com

Clearly, RDGAs come in a variety of forms and their domains may not be immediately recognizable when viewed in isolation. This is why researching and identifying RDGAs requires access to large-scale DNS data and enough DNS expertise to properly analyze it.

HOW ARE RDGAs USED IN THE WILD?

THREAT ACTORS, CRIMINAL ENTERPRISES AND LEGITIMATE BUSINESSES ALL USE RDGAs.

Registrars like Namecheap even offer tools to generate variants of a chosen domain name, and these tools can be leveraged by anyone — legitimate customers or threat actors. In this section we'll show examples of RDGAs we've observed in the wild to give a sense of the different ways they can be used.

examplerdga ✕ Clear (1)

Enter up to 5,000 domains or keywords to get started

Price Range

$ 0 to $ 500,000

Transform

- Use Domain Hacks
- Drop Last Vowel
- Pluralize Nouns

Options

- Show Premiums
- Hide Unavailable

Append Prefix/Suffix

Prefix: try ✕ use ✕ get ✕ the ✕ meet ✕ open ✕

Type a prefix ...

Suffix: ly ✕ app ✕ labs ✕ hub ✕ hq ✕

Type a suffix ...

Search 1187 TLDs ... Clear (30)

Popular (30) Clear

ac ai app art biz bot cc club co com cx dev game health info io is live lol net one org pro sh so today us vip wiki xyz

International (10)

Academic & Education (3)

Finance

Professional (3)

Businesses (4)

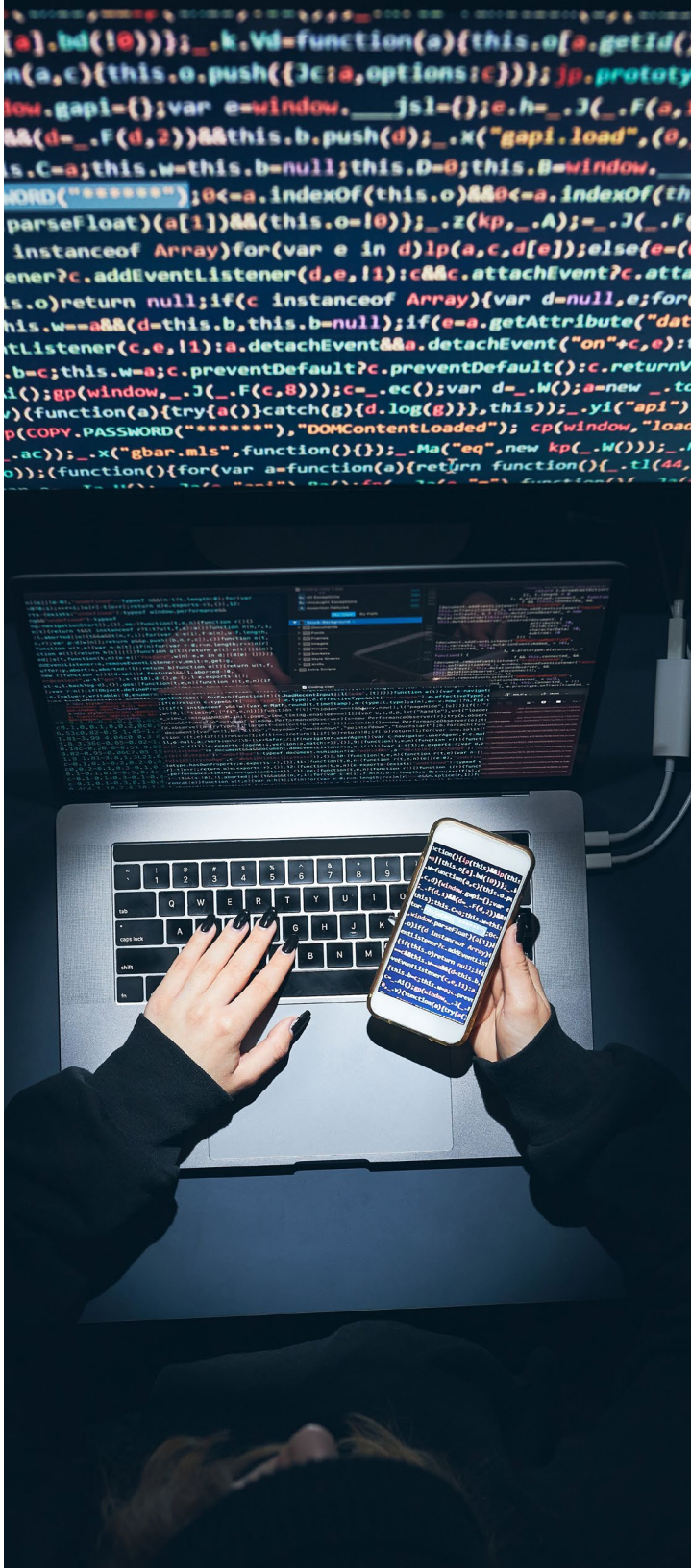
Audio & Video (1)

Arts & Culture (1)

Adult

Generate

6 Namecheap's "Beast Mode" is a fully-featured graphical RDGA builder available to all customers



WHY THE RISE IN RDGAs?

While traditional DGAs are still the most popular choice for malware authors, some threat actors have opted to use RDGAs for their malware instead. RDGA domains are often used to host malicious payloads or drive-by exploits rather than acting as C2s for the malware, although there are cases of threat actors embedding hardcoded RDGA domains into their payloads.

THEY'RE USED FOR MALWARE

It may seem surprising that threat actors would use hardcoded RDGA domains in their malware, given that traditional DGAs were invented to overcome the limitations of using hardcoded C2 domains. However, there's actually a logical explanation for why some actors prefer RDGAs:

- Hardcoded RDGA domains can be obfuscated through some type of encoding process, so they aren't vulnerable to basic string dumps in the same way as the hardcoded C2s of older malware.
- Since the algorithm used to generate the domains isn't included in the malware sample, it's significantly harder for security researchers to reverse engineer the algorithm and predict the domains the threat actor will use before their malware campaigns become active.

Each campaign will likely infect at least some percentage of its targets before security researchers capture a sample and extract its hardcoded C2s.

For those reasons, hardcoded RDGA domains are an attractive choice for threat actors who use spam as a delivery method. Essentially, they can deliver new payloads with different hardcoded C2 values on a daily or even hourly basis. This is especially true when the payload is a loader for other types of malware because the loader will likely have done its job by the time the campaign is discovered and its C2s are blocked.

HANCITOR

If you're reading this paper, there's a good chance you've heard of Hancitor malware.

Although it hasn't been active recently, it was an incredibly popular malware loader with prolific malspam campaigns that regularly delivered booby-trapped documents to unsuspecting victims for the better part of a decade. What most people don't realize about Hancitor is that they were using an RDGA to generate all of their C2 domains, which meant they could be detected in DNS and blocked before their campaigns even became active.

Looking at the C2 domains embedded in a single sample of Hancitor (Figure 7), the pattern isn't obvious.

7 **Hancitor C2 domains from one sample**

choppprousite[.]ru
thougolograrly[.]ru
patiennerrhe[.]com

The C2s are nonsensical and look like DGA domains, but they don't contain numbers or lots of high-entropy strings like a randomized traditional DGA. Some of them appear to contain English words like a DDGA, but they're not exclusively made of intelligible words like a standard DDGA. While all of these observations are true, and they may even help identify Hancitor domains during manual threat hunting, they aren't enough to fully characterize the algorithm and build an automated detector for it.

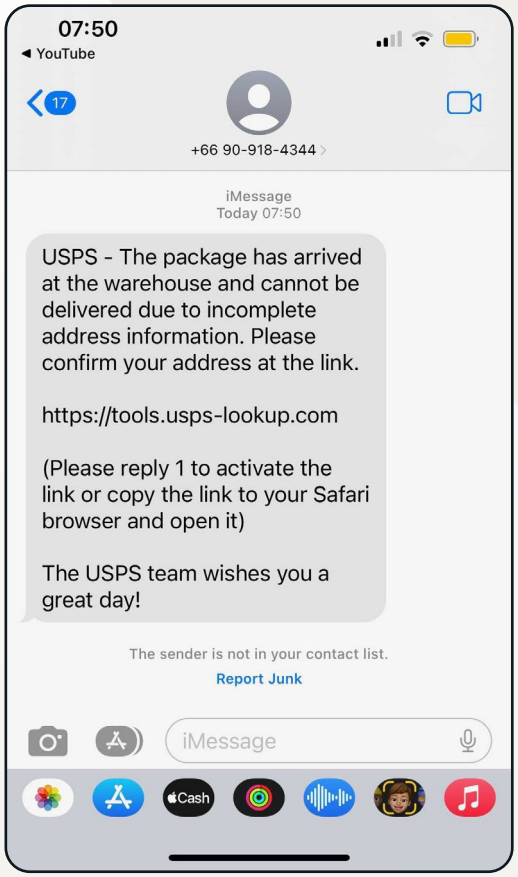
If we look at a larger list of Hancitor C2 domains taken from multiple samples, however, the underlying patterns of its RDGA become more apparent (**Figure 8**):

8 **Selected Hancitor C2 domains taken from various samples**

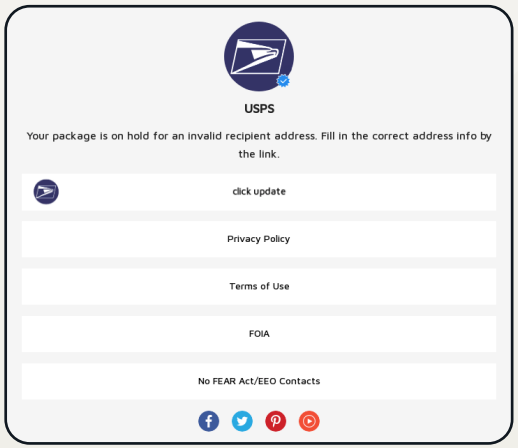
dintretonid[.]com
dintretrewor[.]com
dintrolletone[.]com
dintromparsup[.]com
direnrolpar[.]ru
hadhecrecled[.]com
hadrecrolof[.]ru
hadsparmirat[.]com
hanparolhar[.]com
rofromandfor[.]ru
rowrorofrat[.]com

From this set of domains, we can see that Hancitor's RDGA has a tendency to repeat specific sequences of characters, such as "di" and "ha." We could infer that the reason its domains appear random while having fairly low entropy is that the character sequences it uses are common in English words.

Infoblox recognized these peculiarities of the Hancitor RDGA in 2018 and created a statistical model to identify domains that follow Hancitor's RDGA pattern. By combining this with our knowledge of Hancitor's registration patterns and DNS signatures, we created a predictive analytic to identify and block Hancitor C2 domains before they were used in active campaigns.



9 USPS smishing SMS received on iPhone



10 USPS phishing page

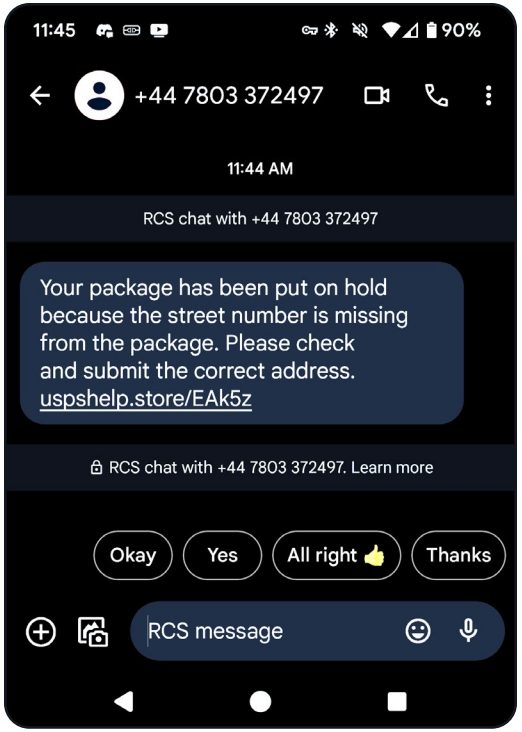
THEY'RE USED FOR PHISHING

Phishing, including spear-phishing, Business Email Compromises (BECs) and similar variations, is one of the most commonly-known and reported cyberthreats, so malicious actors need a constant stream of new domains to bypass security measures and keep their phishing operations effective.

As such, RDGAs are an incredibly popular choice for phishing actors. Some phishing actors use randomized high-entropy RDGAs that appear similar to traditional DGAs, while others use RDGAs to create a high volume of lookalike domains to conduct more targeted phishing campaigns.

USPS Phishing

Multiple threat actors have been using RDGAs and lookalike domains to conduct SMS-based phishing attacks (smishing) that incorporate United States Postal Service (USPS) lures. These actors also target other shipping and postal organizations, but a significant surge in USPS-themed attacks began in August 2023. Most of these attacks use the same phishing kit and are run by Chinese threat actors. Resecurity reported one of these actors under the name "Smishing Triad,"[1] and Brian Krebs reported a different actor with the Telegram username @chenlun.[2] Infoblox has detected RDGA activity associated with both of these threat actors as well as others. See **Figures 9-11** for screenshots of USPS smishing messages from several device types.



11 USPS smishing SMS received on Android

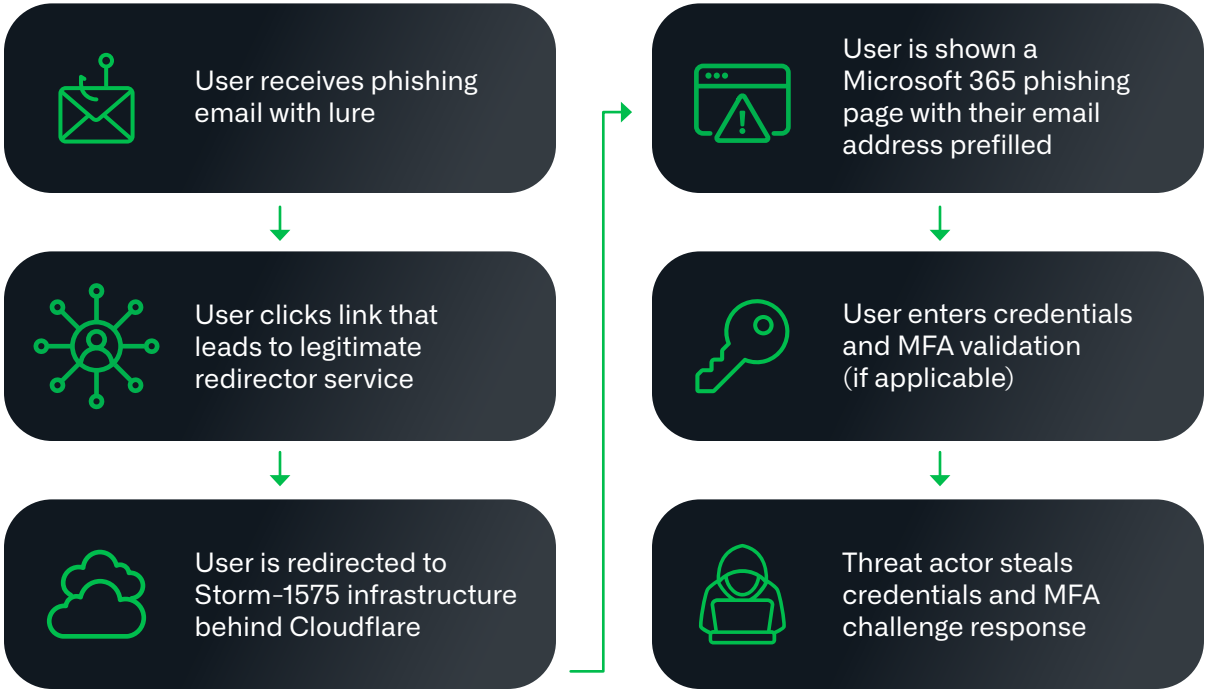
[1] https://www.resecurity.com/blog/article/smishing-triad-targeted-usps-and-us-citizens-for-data-theft
[2] https://krebsonsecurity.com/2023/10/phishers-spoof-usps-12-other-natl-postal-services/

STORM-1575

Storm-1575, a threat actor tracked by Microsoft, is responsible for the development, support and sale of the Dadsec Phishing-as-a-Service (PhaaS) platform.[3]

The Dadsec platform allows cybercriminals to launch phishing campaigns without developing the phishing websites themselves, enabling even unskilled actors to run campaigns with minimal financial investment. Dadsec phishing websites are designed to look like legitimate web portals and harvest user credentials and authentication tokens. Bridewell has observed specific phishing campaigns on the Dadsec platform that used an RDGA as part of the attack.[4]

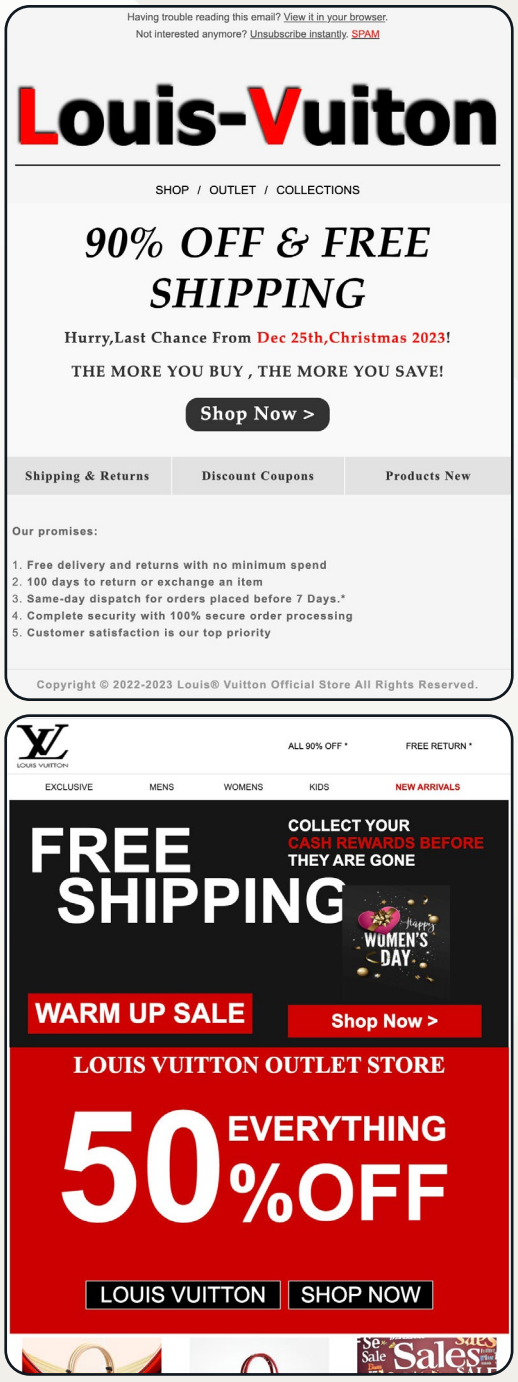
Example: Storm-1575 Attack Chain



ATTACKER IN THE MIDDLE (AiTM)

AiTM attacks are a variant of classic Man-in-the-Middle (MitM) attacks that can intercept Multi-Factor Authentication (MFA) exchanges, allowing Storm-1575 to bypass one of the most commonly-recommended security measures.

[3] https://twitter.com/MsftSecIntel/status/1712936244987019704
[4] https://www.bridewell.com/insights/blogs/detail/analysing-widespread-microsoft365-credential-harvesting-campaign



12 Evolution of Louis Vuitton-themed spam campaigns

THEY'RE USED FOR SPAM

Spam domains inherently generate high volumes of activity, making them prone to detection and blocking by email providers and anti-spam solutions.

Using an RDGA to register large quantities of new domains can help spammers evade domain-based blocking and ensure that their messages reach as many recipients as possible.

President-Themed Spam

This threat actor uses an RDGA to register domains on the .top and .xyz top-level domain (TLD) to send spam. Their domains have large numbers of subdomains whose names follow several different themes including U.S. presidents (e.g. "biden," "obama," "trump") and shopping (e.g. "coupon," "discount," "sales"). The actor uses these subdomains to create a variety of mail exchange records (MX records) for each domain, and each of those MX records points to one of many different IP addresses within the same IPv4 /24 subnet range. This configuration allows the actor to operate multiple MX servers using only a single domain. This behavior may be an attempt to circumvent spam blocking mechanisms that rely on sender IPs or hostnames, as the actor has a pool of different IPs and hostnames from which to send their spam. The behavior may also indicate that the actor is offering spam as a service to other threat actors, with each customer receiving their own infrastructure so that their campaigns don't interfere with each other.

While we have yet to fully uncover the extent of this actor's activity, we have observed at least two unique varieties of spam campaigns from them so far. The first type was in English and imitated the Louis Vuitton brand, directing recipients to websites selling counterfeit merchandise. Early iterations of this campaign had a plain appearance with a generic text logo that misspelled the brand's name as "Louis *Vuiton*," but later versions appeared more like real advertisements and used the official Louis Vuitton logo (**see Figure 12**).

AND MORE SPAM

The second type of spam campaign was in Chinese and themed as a corporate communication regarding China's Spring Festival, also known as Chinese New Year (**Figure 13**). The email subject line and body text both used generic references to "the company." It enticed recipients to open an attached Microsoft Word document by claiming it was an application for a state-sponsored tax subsidy for employees who were returning home during the Spring Festival. This document purported to be a tax refund application from the State Taxation Bureau of the People's Republic of China, and its contents instruct recipients to use the popular Chinese communication app WeChat to scan an included QR code to visit the tax bureau's application website. In reality, this QR code led visitors to an attacker-controlled RDGA domain. The content of this domain was already offline by the time of our investigation, but given the overall theme of the campaign, we consider it likely that the domain was used for some type of scam, such as identity theft or banking fraud.

国家税务总局文件

中华人民共和国税务局政策编号：（2024-01-05）

个人所得税退税申办通知

为切实维护纳税人合法权益，进一步落实好专项附加扣除政策，根据个人所得税法及其实施条例和税收管理法及其实施细则有关规定，现就办理 2023 年个人综合所得税退税申办工作，有关事项通知如下：

一、 申请条件：工作满一年以上且正常缴纳个人所得税的中国公民。

二、 申请通过后，将返还 2023 年个人所得税缴纳金额的百分之七十。

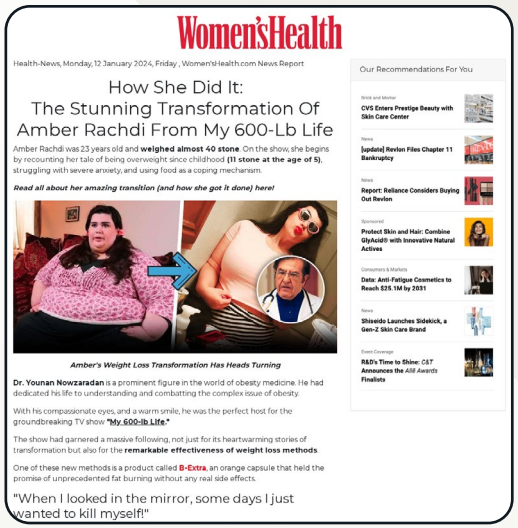
三、 截止日期 2024 年 1 月 31 日，过期视为主动放弃，请尽快办理。

四、 使用微信扫码进入国家税务局官方小程序在线办理。

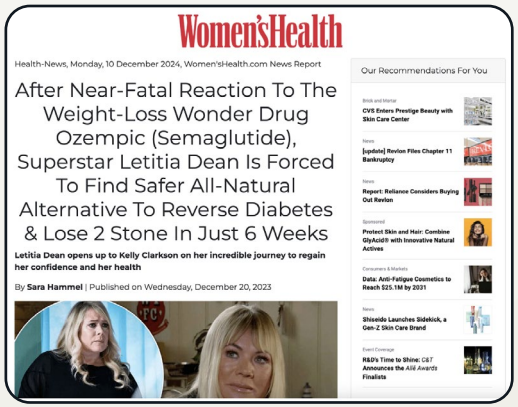
2024 年 1 月 5 日

主办单位：中华人民共和国税务总局

13 Fake Chinese tax document attached to Spring Festival-themed spam



14 RDGA domain faking an article from Women's Health to sell weight loss pills



15 Another fake Women's Health article that appeared on the same RDGA domain at a later date; note how the date at the top of the page reads "10 December 2024" (a date that hasn't occurred yet) while the article's supposed publishing date is "December 20, 2023"

THEY'RE USED FOR SCAMS

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.

Weight Loss Pill Scam

This actor used an RDGA to create domains imitating articles from *Women's Health* magazine, claiming to reveal weight loss secrets used by famous people. In reality, the stories on these sites are entirely fabricated and only serve as advertisements for weight loss supplements (**Figures 14 and 15**).

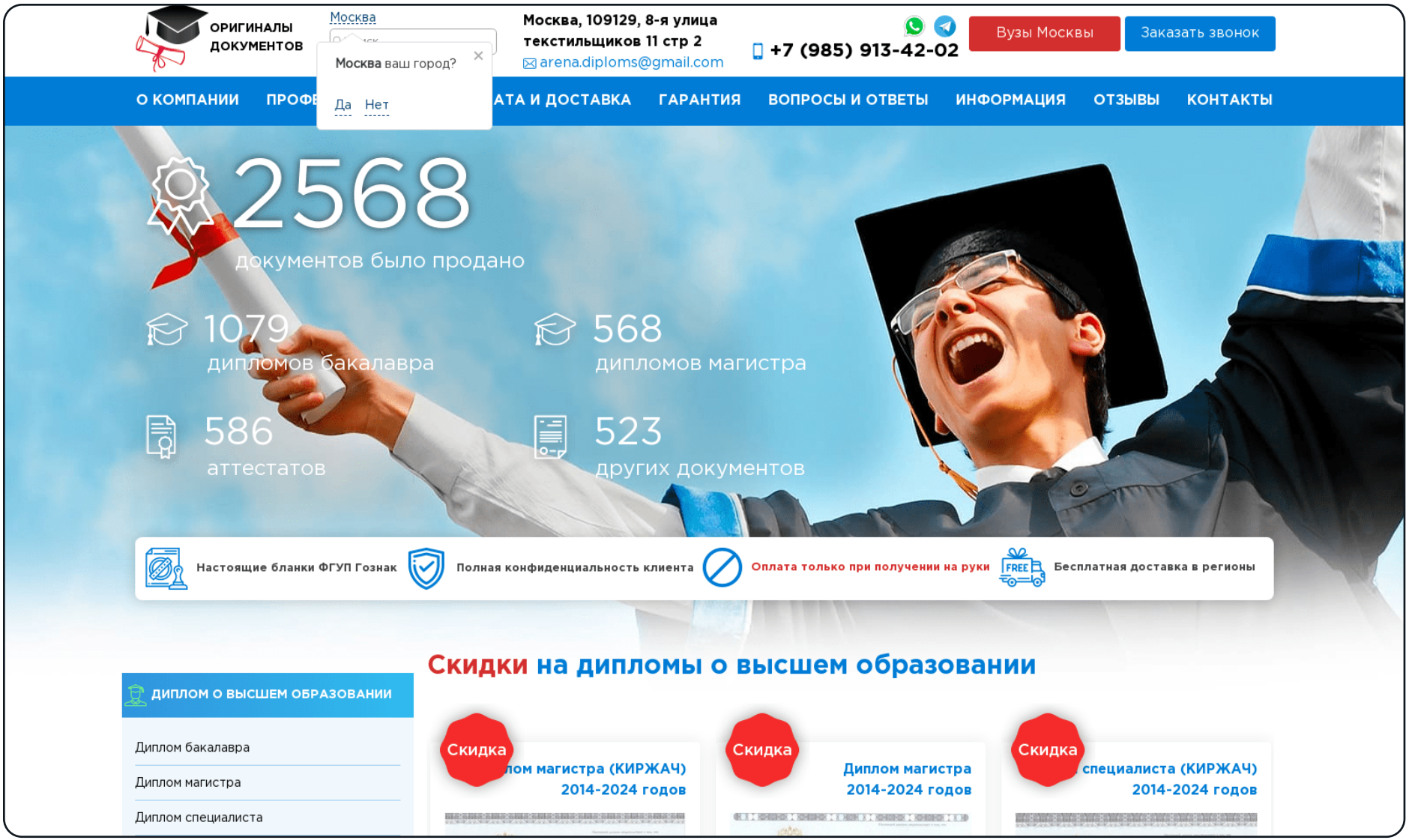
When a visitor clicks the links provided in these fake articles, they're redirected to one of several sites offering weight loss capsules under varying names. One such site for "Shape Capsules" claims that a customer can expect to go from 113kg (250 lbs) to 68kg (150 lbs) in a matter of 94 days, meaning they'd lose slightly over one pound per day on average. This claim is completely unrealistic for any weight loss supplement to make, and TrustPilot reviews for Shape Capsules indicate that the supplement fails to live up to its marketing claims (**Figure 16**).[5]

16 Projected weight loss timeline provided by the Shape Capsules site

[5] https://www.trustpilot.com/review/shapecapsule.wowdealcollection.com

Russian Diploma Mill

This actor used an RDGA to create domains for their Russian diploma mill (**Figure 17**). These domains offer customizable college degrees for low prices, such as a master's degree for 19,999 rubles (roughly US$216).



17 Russian diploma mill RDGA domain

GAMBLING AS A CYBER THREAT?

It may seem strange to see an activity like gambling listed in this paper alongside clearly malicious threats like malware and phishing, but the reality is that it is illegal in many parts of the world.

THEY'RE USED FOR GAMBLING

Actors running gambling operations have as much reason to use RDGAs as any other cybercriminals.

In our research, RDGA domains with gambling content tailored towards Chinese audiences are particularly prevalent, likely due to the Chinese government's Golden Shield Project (commonly referred to as the "Great Firewall of China"), which blocks access to known gambling websites. Operators of gambling websites, therefore, use RDGAs to create large numbers of new domains that mirror their content to make it accessible to users in China without the use of a virtual private network (VPN).[6]

XC Sports

XC Sports (a.k.a. Xingcai Sports, Sincai Sports) is a Chinese sports betting website that's notable for its brand partnership with famous Brazilian soccer player Ronaldinho Gaúcho.[7,8] What makes XC Sports notable from a security perspective is the way they obfuscate their activities. The company's official website listed in their promotional materials is sc[.]sc, but this domain isn't part of the company's online gambling platform. Rather, it functions as an advertisement of the company's services and invites interested visitors to contact the company through one of several messaging platforms, including Telegram and Letstalk. XC Sports likely uses these messaging platforms for some sort of user verification process to protect their infrastructure from investigation and blocking by Chinese authorities, only supplying the addresses of their actual gambling domains to users who pass their verification.

Despite the company's attempts to obfuscate their infrastructure, XC Sports uses an RDGA to generate domains for its actual gambling platform, which made their domains readily identifiable to our RDGA detectors. These domains use short strings of letters (most commonly "xc") combined with numbers, such as xc0078[.]vip, and we've observed these domains across a number of different TLDs.

[6] https://www.businessinsider.com/inside-the-world-of-illegal-online-gambling-in-china-2022-9
[7] https://twitter.com/10Ronaldinho/status/1629093248307195904
[8] https://www.youtube.com/watch?v=hJL_bASsfAg

When these domains are visited from IP addresses outside of China, they display a message that roughly translates to “Due to your country and region restrictions, we are unable to provide services to you.” But when visited from a Chinese IP address, the domains show what appears to be a fully-functioning gambling site. When visited on a mobile device, the site even includes a banner inviting users to download a native XC Sports mobile app (**Figure 18**).

18 Comparison of XC Sports RDGA domain content when visited from IPs outside China (left) and IPs in China (right)

THEY'RE USED FOR TRAFFIC DISTRIBUTION SYSTEMS

Traffic distribution systems (TDSs) are used for routing incoming web traffic based on user characteristics such as IP geolocation, browser capabilities, HTTP request headers and more.

Legitimate organizations most commonly use a TDS for marketing and SEO purposes, as it offers sophisticated capabilities for performing targeted advertising and tracking the success of advertising campaigns. Cybercriminals leverage TDSs in a very similar way: using their capabilities to perform targeted attacks and tracking the success of their phishing and malware campaigns.

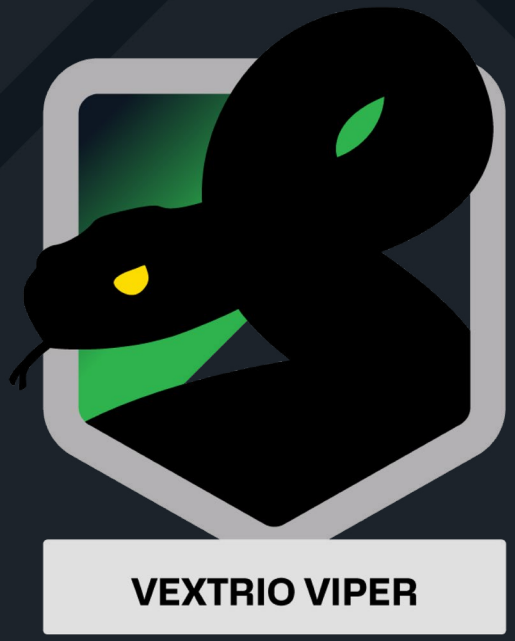
Traffic distribution systems first became popular with threat actors in the late 2000s and early 2010s as critical components of exploit kits such as Angler and Neutrino. These exploit kits used TDSs to check if potential victims were using a vulnerable web browser or plugin and direct them to a page with appropriate exploits for their specific vulnerabilities. As gradual security improvements in web browsers made traditional exploit kits increasingly ineffective, some exploit kit operators decided to start offering the TDS portion of their kits as a standalone service to other cybercriminals.[9] Since then, TDS-as-a-Service operators have remained a staple of the threat landscape, with two of the largest DNS threat actors we've discovered and reported so far being associated with TDS activity.

THE MAGNITUDE EXPLOIT KIT

Magnitude was a notorious exploit kit that used a TDS to redirect advertisements to malicious landing pages. Infoblox identified Magnitude's dictionary-based RDGA and created an analytic to detect it in 2017. Here are some examples of their domains:

- fellfelt[.]gdn
- plugfour[.]vip
- plugtin[.]live
- tinfelt[.]life

[9] https://www.bleepingcomputer.com/news/security/tds-systems-are-the-next-big-money-makers-in-the-land-of-cybercrime/



VEXTRIO VIPER

VexTrio Viper is a massive criminal TDS operation with at least 60 affiliate partners including ClearFake and SocGholish, making them the single largest malicious traffic broker described in security literature thus far.

VexTrio Viper uses a dictionary-based RDGA to generate and register high volumes of domains that can serve as either a TDS or as a host for malicious content. This aspect of their operation is a major contributor to their success as a cybercriminal affiliate network, as their constantly expanding list of domains makes it difficult for internet providers to bring their infrastructure down.

Infoblox first identified VexTrio Viper two years ago because their methods of operation leave a substantial footprint in our network logs. As a result, we've been able to extensively study their activities, create automated detectors to proactively identify and block their domains based on their unique DNS signatures and publish detailed analyses of their operations.[10,11] VexTrio Viper is easily one of the best examples of why RDGAs matter and why organizations need security solutions based on large-scale DNS analysis. This actor has been running malicious TDS services since at least 2017 and has registered more than 70,000 domains to date, but their operations went undetected and unreported by the security industry for years. Even now that Infoblox has reported on VexTrio Viper and their methods several times, the only way to truly prevent them from affecting a network is to conduct the type of large-scale DNS analysis and anomaly detection that we perform.

We've adopted a new animal-based threat actor naming system since we first discovered and reported on VexTrio, so we've updated their name to "VexTrio Viper." To learn more about our actor classification system, check out our new Infoblox Threat Intel page.

[10] https://blogs.infoblox.com/cyber-threat-intelligence/cybercrime-central-vextrio-operates-massive-criminal-affiliate-program/
[11] https://blogs.infoblox.com/cyber-threat-intelligence/cyber-threat-advisory/vextrio-ddga-domains-spread-adware-spyware-and-scam-web-forms/

PROLIFIC PUMA

Prolific Puma is a threat actor that provides illicit link shortening services to other malicious actors to help them evade detection while they distribute phishing, scams and malware.

Prolific Puma uses an RDGA to generate domain names for their services, and as their name suggests, their output is rather voluminous, with between 35k and 75k unique domain names registered since April 2022.

Infoblox first detected Prolific Puma in April 2023 through one of our generic RDGA detectors. Since then we have developed a better understanding of their activity, built more specialized DNS signature detectors to track the evolution of their network and published a paper on their operations.[12] Prolific Puma is another excellent example of how important DNS analytics and RDGA detection are to an organization's overall security.

[12] https://blogs.infoblox.com/cyber-threat-intelligence/prolific-puma-shadowy-link-shortening-service-enables-cybercrime/

THEY'RE USED FOR VPNs

Since VPNs can anonymize traffic and allow users to access websites that might otherwise be blocked on the user's network, network administrators and security solutions may place blocks on known VPN infrastructure to prevent people from using them to bypass network security.

Meanwhile, companies that offer VPN services want their infrastructure to remain accessible on as many networks as possible since their business depends on it. As a result, some VPN companies use RDGAs to evade blocking mechanisms in the same way as threat actors do.

SetupVPN

SetupVPN is a free VPN application and browser extension whose infrastructure is dependent on large quantities of RDGA domains. It uses these domains for a variety of purposes, including managing user connections, communicating infrastructure changes to the client and even displaying onboarding guides for new users. The SetupVPN browser extension includes a bundled JSON file (**Figure 19**) that contains an initial set of server hostnames, as well as links to the latest versions of the file on public code repositories, including GitHub,[13] BitBucket[14] and Launchpad.[15] These repository links presumably serve as a fallback to allow the extension to update its server list, in the event that none of the included servers are reachable, and a new version of the server file is pushed to the repositories on an hourly basis.

When the user initiates a new connection with SetupVPN, it communicates with one or more of the hostnames in its servers file, and these servers respond with encrypted traffic that appears to tell the VPN what domain to use for the actual connection. We can infer this due to the fact that after the initial polling of hostnames from the bundled server file, SetupVPN starts communicating with a unique hostname on a single domain, and the domains it communicates with in this way aren't listed in the server file or any other part of SetupVPN's public repositories. This is presumably intended to obfuscate the domains SetupVPN uses for its actual communications to make them more difficult to enumerate and block.


```
{
    "retcode": 200,
    "data": {
        "version": 4,
        "update_interval_hours": 6,
        "settings": {
            "tierbase_search_timeout": 15000,
            "mainbase_search_timeout": 20000,
            "tierbase_api_timeout": 35000,
            "mainbase_api_timeout": 30000,
            "proxy_search_timeout": 30000,
            "mirror_timeout": 30000
        },
        "mainbase": [
            "https://icax.slight.pics",
            "https://xcxx.locally.pics",
            "https://uaia.valley.pics",
            "https://1.foreground.work",
            "https://1.awakened.work",
            "https://1.6912044.cc",
            "https://1.chairs-notify.top",
            "https://1.discs-bound.top",
            "https://1.absolute-refined.top"
        ],
        "tierbase": [
            "https://api.keepthisdomain.com",
            "https://1.amino-vertical.top",
            "https://1.ranks-learning.top",
            "https://1.brass-gardens.top",
            "https://1.rather-times.top",
            "https://1.actually-rewards.top",
            "https://1.treasure-equipped.top",
            "https://1.bidder-sessions.top",
            "https://1.luther-episodes.top",
            "https://1.advise-stomach.top",
            "https://1.glossary-titled.top",
            "https://1.reward-reserved.top",
            "https://1.online-device.top",
            "https://1.makeup-melissa.top",
            "https://1.shine-styles.top",
            "https://1.wireless-bailey.top",
            "https://1.depth-crafts.top",
            "https://1.bright-motion.top",
            "https://1.generic-partial.top",
            "https://1.property-reward.top",
            "https://1.manner-obesity.top",
            "https://1.people-borough.top",
            "https://1.trainers-wooden.top",
            "https://1.summit-integral.top",
            "https://1.framed-watch.top",
            "https://1.fitted-bruce.top",
            "https://1.hampton-warned.top",
            "https://1.reality-clearing.top",
            "https://1.static-firms.top",
            "https://1.instant-drama.top",
            "https://1.expand-herein.top",
            "https://1.coated-textiles.top",
            "https://1.wesley-reviewed.top",
            "https://1.familiar-malaysia.top",
            "https://1.heretowe.win",
            "https://topluok.uk",
            "https://listitnow.org",
            "https://baseserver.uk",
            "https://datacntech.com",
            "https://1.default2024.uk",
            "https://1.sahi.uk",
            "https://1.area9.uk",
            "https://1.allnine.uk",
            "https://ksho.uk",
            "https://3245.uk"
        ],
        "t": 1713214920253,
        "mirrors": [
            "https://bitbucket.org/the7c/update/raw/
                master/edge/pub/data.json",
            "https://raw.githubusercontent.com/the7c/
                update/master/master/ui/data.json",
            "https://git.launchpad.net/returner/plain
                /gui/data.json"
        ]
    }
}
```


19 SetupVPN's data.json file containing its initial server list and repository links

[13] https://github.com/the7c/update/blob/master/master/ui/data.json
[14] https://bitbucket.org/the7c/update/raw/master/edge/pub/data.json
[15] https://bitbucket.org/the7c/update/raw/master/edge/pub/data.json

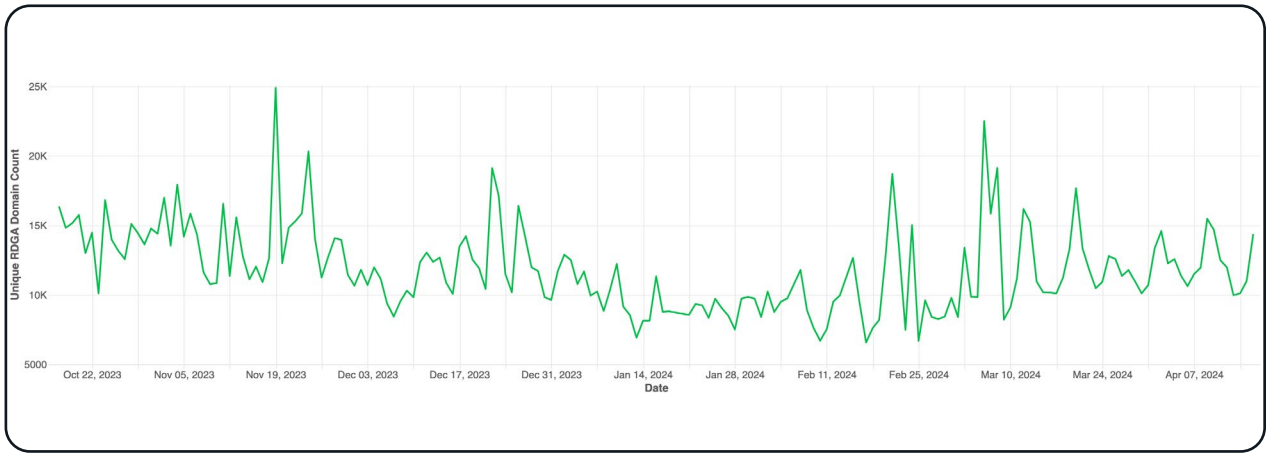
RDGAs ARE ON THE RISE

In the six month period from October 17, 2023 to April 17, 2024, our RDGA detectors identified over 2M unique RDGA domains, or an average of over 11k new RDGA domains per day (**see Figure 20**).

THEY'RE USED FOR UNKNOWN ACTIVITY

As our examples have shown, RDGAs can take many forms and serve myriad purposes. But more importantly, the RDGA threats we know about are just the tip of the iceberg.

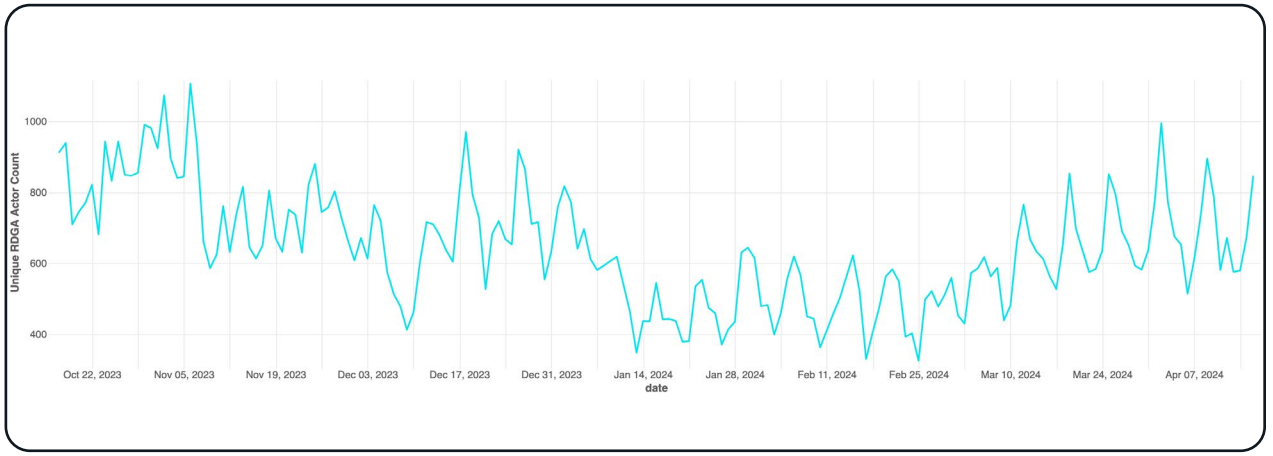
For every RDGA like VexTrio Viper that we've extensively researched and published on, we've detected thousands of other RDGAs whose purposes remain largely unknown. Given the wide array of malicious activity we've observed from the RDGAs we know, the sheer quantity of unknown RDGAs is a matter of significant interest and concern. The patterns and DNS signatures that tie RDGA domains together can only be identified by large-scale analysis, so unknown RDGA domains are able to function largely unimpeded on networks that aren't protected by advanced DNS analytics like ours.



20 Daily RDGA domain detection counts from October 17, 2023 to April 17, 2024

> **It only takes a day for RDGA actors to register tens of thousands of new domains for researchers to investigate.**

Our detectors initially clustered these domains into roughly 117k unique actor groups, which we later reduced to roughly 52k actor groups using a combination of automated refinements and manual analysis (**see Figure 21**).



21 Daily RDGA actor cluster counts from October 17, 2023 to April 17, 2024

The key takeaway from these statistics is that there are so many RDGA domains being registered that the security industry will never be able to research them all. It can take months for human researchers to understand a threat to the point that they can publish on it, but it only takes a day for RDGA actors to register tens of thousands of new domains for researchers to investigate. This is why automated detection is the only viable defense against RDGA threats.

MEET REVOLVER RABBIT

Prolific and malicious

REVOLVER RABBIT

One of the most prolific RDGA actors we've found, which we've named Revolver Rabbit, has registered over 500k domains on the .bond TLD alone, at an estimated cost of over $1M.

Their RDGA pattern is unique but also highly variable, which makes some of their domains difficult to identify without additional DNS context.

The most common RDGA pattern this actor uses is a series of one or more dictionary words followed by a five-digit number, with each word or number separated by a dash (**see Figure 22**). When multiple dictionary words are used, they usually form coherent phrases rather than appearing completely random.

22 **Examples of most common RDGA pattern for unknown .bond actor**

assisted-living-11607[.]bond
online-jobs-42681[.]bond
perfumes-76753[.]bond
security-surveillance-cameras-42345[.]bond
yoga-classes-35904[.]bond

Sometimes the actor uses ISO 3166-1 country codes, full country names or numbers corresponding to years instead of dictionary words (**see Figures 23A and 23B**). They tend to use these elements as prefixes or suffixes, and the domains that use them generally omit the standard five-digit numerical suffix regardless of whether the element is being used as a prefix or suffix.

23A

Domains using the basic pattern

ai-courses-12139[.]bond
ai-courses-13069[.]bond
ai-courses-14729[.]bond
ai-courses-16651[.]bond
ai-courses-17621[.]bond
app-software-development-training-52686[.]bond
app-software-development-training-54449[.]bond
app-software-development-training-55554[.]bond
app-software-development-training-57549[.]bond

23B

Domains using country codes, country names, and year numbers

ai-courses-2024-pe[.]bond
ai-courses-2024-pk[.]bond
ai-courses-2024sa[.]bond
ai-courses2023-in[.]bond
ai-courses2023in[.]bond
ai-courses2024in[.]bond
app-software-development-italy[.]bond
app-software-development-training-usa[.]bond

Figures 24A and 24B show how the actor occasionally replaces their standard five-digit suffix with one or two digits followed by a single character.

24A

Domains using the basic pattern

online-degrees-16099[.]bond
portable-air-conditioner-12322[.]bond
river-cruises-13890[.]bond
roofing-services-10175[.]bond
travel-insurance-43494[.]bond

24B

Domains using 1-2 digits and a single letter

usa-online-degree-29o[.]bond
bra-portable-air-conditioner-9o[.]bond
uk-river-cruises-8n[.]bond
rsa-roofing-services-8n[.]bond
col-travel-insurance-3n[.]bond

Figures 25A and 25B show that in some cases the actor uses two dashes in a row rather than the single dash they normally use.

25A

Domains using the basic pattern

welding-machines-10120[.]bond
welding-machines-35450[.]bond
welding-machines-56397[.]bond
welding-machines-76813[.]bond
welding-machines-99146[.]bond

25B

Domains using two dashes instead of one

welding-machines--11015[.]bond
welding-machines--31109[.]bond
welding-machines--56717[.]bond
welding-machines--75378[.]bond
welding-machines--97422[.]bond

REVOLVER RABBIT

The amount of variation in this actor's RDGA highlights the need for advanced DNS expertise and visibility when implementing automated RDGA detection.

While many of their domains follow a basic pattern that could be detected with regular expressions or other string-based matching, they also have a number of domains that use different patterns. The similarities between this actor's patterns may be obvious to a human observer, but for an automated detector to accurately group these somewhat disparate domains together, additional DNS context is required.

We initially planned to publish Revolver Rabbit as an example of an interesting but unclassified RDGA actor, but during our research we found their domains being used as both active C2s and decoy domains in XLoader (a.k.a. Formbook) malware samples.[16,17] This discovery further underscores the importance of RDGA detection and analysis, as without it actors like Revolver Rabbit can operate undetected despite their massive network footprints.

[16] https://www.joesandbox.com/analysis/1466892/0/html
[17] https://www.virustotal.com/gui/file/7738ec817c97182e16e409767c55c87460d83d37b0442eb337bc2507763d4486/relations

IOCs

The complete list for this paper can be found on GitHub at https://github.com/infobloxopen/threat-intelligence

CONCLUSION

RDGA domains are associated with a panoply of dubious activities that most organizations don't want on their networks.

But despite being used to register millions of new domains, RDGAs have gone almost entirely unrecognized by the security industry. This lack of reporting is likely due to the fact that RDGA detection requires both significant DNS expertise and access to large volumes of DNS data. Organizations should be aware of the threat that RDGAs pose to their networks, and should implement security solutions that include automated RDGA detection.

INFOBLOX SOLUTIONS

Infoblox BloxOne® Threat Defense (B1TD) Advanced offers a uniquely broad and comprehensive solution against known and unknown RDGA threats. Leveraging large-scale DNS, Infoblox is able to apply a series of analytics to hundreds of thousands of new second-level domains every day. These capabilities include multiple patent-pending algorithms for RDGA detection.

Our new Zero Day DNS feature can also detect and block RDGA domains within minutes of the first DNS query, ensuring rapid coverage against unknown RDGA threats.

The Infoblox suite of RDGA threat detection solutions are just a few of the many services offered by BloxOne Threat Defense, enabling the product to see threats that other solutions do not, and to stop attacks earlier in the threat lifecycle. Through pervasive automation and ecosystem integration, BloxOne Threat Defense can drive greater efficiencies in SecOps, uplift the effectiveness of the existing security stack, secure digital and work-from-anywhere efforts and lower the total cost for cybersecurity.

FOR MORE INFORMATION

Visit infoblox.com

Follow-us on LinkedIn

Follow-us on X

INFOBLOX THREAT INTEL

Infoblox Threat Intel is the leading creator of original DNS threat intelligence, distinguishing itself in a sea of aggregators. What sets us apart? Two things: mad DNS skills and unparalleled visibility. DNS is notoriously tricky to interpret and hunt from, but our deep understanding and unique access to the internet's inner workings allows us to track down threat actors that others can't see. We're proactive, not just defensive, using our insights to disrupt cybercrime where it begins. We also believe in sharing knowledge to support the broader security community by publishing detailed research and releasing indicators on GitHub. In addition, our intel is seamlessly integrated into our Infoblox DNS Detection and Response solutions, so customers automatically get its benefits, along with ridiculously low false positive rates.

infoblox.

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

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

+1.408.986.4000
www.infoblox.com