PROLIFIC PUMA: SHADOWY LINK SHORTENING SERVICE ENABLES CYBERCRIME

Authors:
Laura da Rocha
Renée Burton
Stelios Chatzistogias
Darby Wise

TABLE OF CONTENT

EXECUTIVE SUMMARY 3

SHADOWY LINK SHORTENING SERVICES 4

DETECTION AND DOMAIN NAME CHARACTERISTICS 6

ABUSE OF usTLD 8

PROLIFIC PUMA CHARACTER 10

PROLIFIC PUMA OPERATIONS 11

AN EXAMPLE CAMPAIGN 12

CONCLUSION 15

INDICATORS OF ACTIVITY 15

INFOBLOX THREAT INTEL 17

EXECUTIVE SUMMARY

Halloween might be the spookiest time of the year, but threat actors are doing frightening things on the internet every day. In the past month we introduced two terms: Domain Name System (DNS) threat actors and RDGA (registered domain generation algorithm). We also gave a taste of one type of DNS threat actor, the persistent phisher, through an exposé of Open Tangle.

Today, we are introducing the second actor in this series, **Prolific Puma**. For four years, maybe longer, Prolific Puma has operated in the shadows, unrecognized by defenders. While we don't know their origin story, we can detect Prolific Puma through DNS and get a glimpse into their character via their domain name registration choices. What's in the name? Prolific comes from the simple fact that this is a network that is continually expanding, with new domains registered almost daily. As for Puma, well… we'll share more about the inspiration later in this paper.

The cybercrime economy is the world's third largest, with an estimated $8 trillion value in 2023, and Prolific Puma is part of the supply chain.[1] They create domain names with an RDGA and use these domains to provide a link shortening service to other malicious actors, helping them evade detection while they distribute phishing, scams, and malware. When we disrupt Prolific Puma, we disrupt a larger segment of the criminal economy. Figure 1 is an overview of the Prolific Puma operations and how they enable criminals. Prolific Puma generates large volumes of domains algorithmically, and then they use these domains to generate shortened links for other malicious actors, allowing them to hide their true activity.

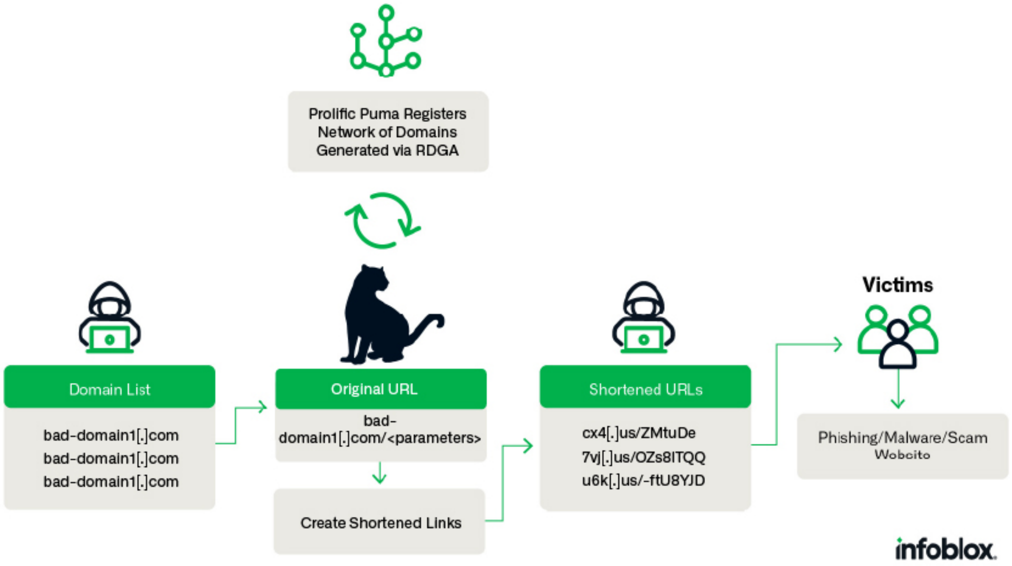


Figure 1. An overview of Prolific Puma's role in the cybercrime supply chain.

To our knowledge, this paper is the first description of a large underground link shortening service. Moreover, **the actor was discovered not from malware or phishing sites but from DNS analytics**. Prolific Puma is remarkable because they have been able to facilitate malicious activities for over 18 months and have gone unnoticed by the security industry. With a massive collection of domain names, they are able to distribute malicious traffic and evade detection.

[1] https://cybernews.com/editorial/cybercrime-world-third-economy/

This discovery demonstrates the power of using DNS and domain registration data not only to detect suspicious activity but also to bring that information together into a consolidated view of a DNS threat actor. While we were able to detect and track the Prolific Puma via DNS, their story highlights the challenges faced by domain registrars and registries to control abuse. When actors are distanced from the actual crime, policies can hinder the ability to identify and takedown the enabling domains.

We **first noticed Prolific Puma domains six months ago through an RDGA detector**. Since then, we have developed a better understanding of their activity using specialized DNS detectors to track the network as it evolves. In the sections that follow, we will discuss the Prolific Puma link shortening service, how they register and host domains, their abuse of the us top level domain (usTLD), and the role they play in facilitating crime on the internet. For the purpose of this publication, we intentionally focus on the actor and their use of DNS rather than the campaigns that use their services. We provide one detailed example of a campaign conducted using Prolific Puma infrastructure, which led to both phishing the user and delivering browser-based malware.

SHADOWY LINK SHORTENING SERVICES

Prolific Puma provides an underground link shortening service to criminals.[2] Accessing an active second level domain (SLD) directly returns the following message:

```
{“type”: “service”,”name”:”@link-shortener/handler-service”}
```

The original purpose of link shorteners was to make the sharing of website links easier, as well as follow social media size limitations. For example,

- the link `https://tinyurl.com/c6u6myhw` is a shortened version of
- https://blogs.infoblox.com/cyber-threat-intelligence/introducing-dns-threat-actors/, our paper that introduced the concept of DNS threat actors.

When the user clicks on the shortened link, they will be redirected to another URL. Behind the scenes, a DNS request is made to resolve the IP address for the shortening service domain, e.g., `tinyurl[.]com`. The web request is then sent to that address containing the hash value used to identify the original site. In the example above, the TinyURL service will use the value c6u6myhw to determine where to redirect the connection. Additional DNS requests will be made to locate the IP address that hosts the final content, in this case, for `blogs.infoblox.com`. While legitimate users will create a simple shortened link to share, a malicious actor may use multiple layers of redirection before the final landing page. This process is depicted in Figure 2.

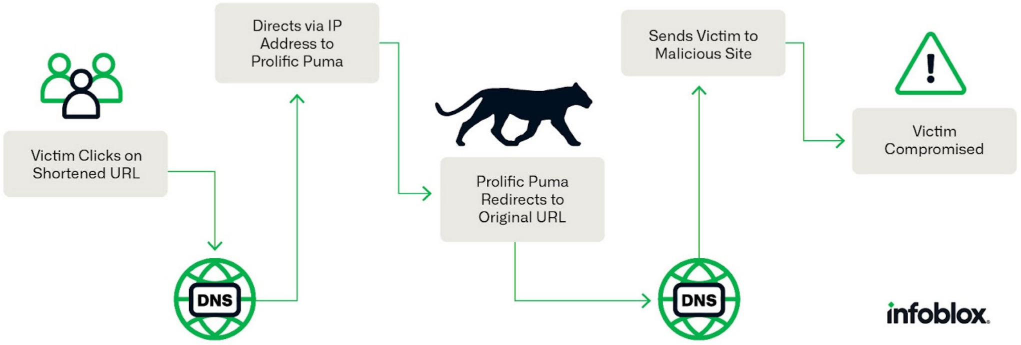

Directs via IP Address to Prolific Puma
Sends Victim to Malicious Site
Victim Clicks on Shortened URL
Victim Compromised
Prolific Puma Redirects to Original URL
DNS
DNS
infoblox

Figure 2: A notional path depicting how a shortened URL interacts with DNS and the shortening service to redirect the victim to malicious content.

[2] https://en.wikipedia.org/wiki/URL_shortening

Malicious actors are known to abuse link shorteners for phishing.[3] In the most publicized cases, however, the link shorteners are well-known, publicly available services including TinyURL, BitLy, and Google. This abuse is so rampant that marketing firm Rebrandly recommends that legitimate companies avoid using popular shorteners in their emails.[4]

Prolific Puma doesn't openly advertise their services. For some period of time, we knew we were tracking a link shortening service, but it was unclear what they were delivering and for whom they were providing the service. The tricky thing about investigating link shorteners is that without a full URL, it is not possible to determine the final landing page. Our detectors had found a large set of interconnected domains with suspicious behavior and no public presence, but we were challenged to conclude how they were being leveraged.

We eventually captured several instances of shortened links redirecting to final landing pages that were phishing and scam sites. Interestingly, the sequence of redirections to the final page varied widely. In some cases, the shortened links led directly to the content.[5] In others, multiple layers of redirection occurred before the final landing page.[6] We also saw Prolific Puma shortened links that were redirected to another shortened link created by a different service.[7] In some cases, the shortened link led to a CAPTCHA challenge.[8] We also found reports that Prolific Puma links were sent via SMS text messages with fake Amazon delivery notifications as early as January 2020.[9] The variance in how the links were handled and the content delivered, makes it most likely that Prolific Puma is providing a service to multiple actors. Evidence suggests that the shortened links are primarily delivered to victims through text messages, but they could be used in other contexts, e.g., social media and advertisements.

Prolific Puma is not the only illicit link shortening service that we have discovered, but it is the largest and the most dynamic. We have not found any legitimate content served through their shortener. Later in this report we detail a specific example of a shortened link that leads to phishing for user information, a scam payment, and the distribution of browser malware.

As a service provider within the cybercrime ecosystem, Prolific Puma helps other malicious actors evade detection, a tactic included in the enterprise MITRE ATT&CK framework.[10] But, their indirect role in the delivery of phishing, scams, and malware to consumers also helps them evade detection. While security providers may identify and block the final content, without a broader view it is difficult to see the full scope of the activity and associate the domains together under a single DNS threat actor. As we'll see next, we are able to do this through DNS analytics.

[3] https://portswigger.net/daily-swig/cybercriminals-use-reverse-tunneling-and-url-shorteners-to-launch-virtually-undetectable-phishing-campaigns

[4] https://support.rebrandly.com/hc/en-us/articles/228632488-Blacklisted-URL-Shorteners-Stop-Using-Them-in-Emails-

[5] https://urlscan.io/result/3be86d9f-e596-4a9b-9260-d331811262e5/

[6] https://urlscan.io/result/00c1d82d-0f03-44b6-96d3-63b503fff464/

[7] https://urlscan.io/result/26077ac3-1559-4329-ab48-120181555586/

[8] https://urlscan.io/result/726b6baa-d259-4f67-a4f9-aef3bd93aca3/

[9] https://turbolab.it/amazon-2444/sms-amazon-hai-messaggio-riguardante-articolo-nome-arrivato-3.-classifica-2960

[10] https://attack.mitre.org/tactics/TA0005/

DETECTION AND DOMAIN NAME CHARACTERISTICS

In order to provide original intelligence for Infoblox DNS detection and response products in the cloud and on-prem, we have designed a large corpus of independent algorithms to detect suspicious and malicious domains, as well as related IP addresses and other DNS resources. **Through aggregation of passive DNS (pDNS) query logs and other data sources, we run a series of analytics on a collection of newly queried, registered, or configured domains**. These analytics independently characterize the domains and range from flagging a domain as suspicious to assigning it to a DNS threat actor.

The discovery of Prolific Puma followed a path common to many of the DNS threat actors we internally name and track. From our automated analytics, some related domains were first labeled individually as suspicious. This adjudication allowed the domains to be blocked in our DNS recursive resolvers to protect customers, but did not necessarily capture the full breadth of activity and did not correlate the domains to a single actor. **When we deployed algorithms for RDGA discovery in Spring 2023, the Prolific Puma domains began to be identified in groups**. These groups were also automatically determined, but statistical methods were used to ensure a high degree of confidence that the RDGA domains were registered by the same DNS threat actor. Finally, another algorithm identified outlier behavior in IP resolutions and correlated the individual RDGA clusters. The sheer size of the activity raised the profile of this particular DNS threat actor for our human-in-the-loop research, and we designed specialized DNS fingerprints to track them. In the remainder of this section, we'll share details about the Prolific Puma domain name characteristics and features that identify them.

Because the connection between the Prolific Puma domains and the final landing pages is indirect, the actor has some protection against discovery. But they also fortify their ability to persist and remain unnoticed through the registration of a large number of domains. Malicious traffic gets divided across these domains at fairly low volumes. Over time, the domains may even gain a reputation as being "good" through strategic aging, a technique used by Prolific Puma that we will detail more later in this paper.

Prolific Puma controls one of the largest networks we track. Since April 2022, they have registered between 35k and 75k unique domain names. Figure 3 shows the number of unique domain names registered per day using 3 or 4 long domain labels. As we recently reported, RDGAs have increasingly replaced traditional DGAs and are offering new challenges to defenders. The use of this technique allows them to easily automate their operations for scale; Prolific Puma domains are among the thousands of new domains Infoblox detects daily that are generated by an RDGA.

Prolific Puma uses NameSilo as their domain name registrar and tends to strategically age their domains before hosting their service with anonymous providers. Despite a lack of clear relation to the United States, Prolific Puma consistently abuses the us top level domain (usTLD), a TLD intended to be reserved for U.S. citizens and organizations. Prolific Puma is known to register both new domains and dropped domains. As an example, 3ty[.]us was previously used by a different actor in June 2022 for Facebook messenger phishing campaigns and was then registered by Prolific Puma after the registration lapsed in July 2023.

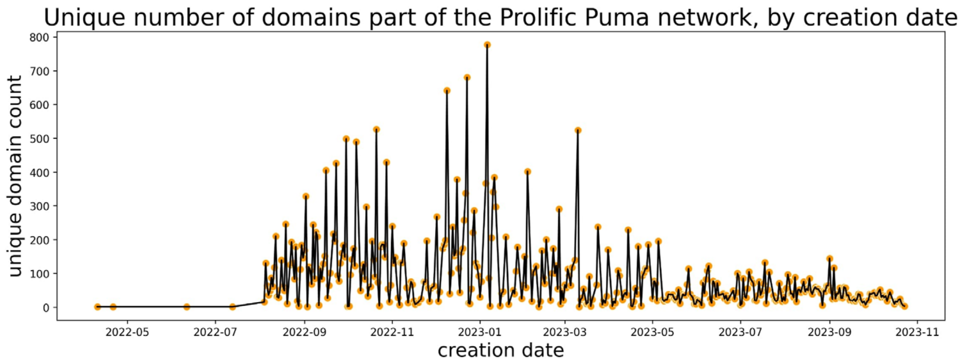


Figure 3. Registration timeline of Prolific Puma domains containing 3 to 4 characters long domain labels.

Prolific Puma domains are alphanumeric, pseudo-random, with variable length, typically 3 or 4 characters long, but we have also observed SLD labels as long as 7 characters. The domains are registered on 13 TLDs that are frequently abused by malicious actors, including: `info`, `us`, `site`, `in`, `link`, `me`, `cc`, `website`, `life`, `xyz`, `club`, `buzz`, and `best`. The `info`TLD accounted for the bulk of domains until May 2023. Since then, the actor has used the `us`TLD for approximately 55% of the total domains they created. We observe 43 new domains, on average, every day since May 2023.

TLD	us	link	info	com	cc	me
Domains	vf8[.]us	cewm[.]link	uelr[.]info	kfwpr[.]com	jlza[.]cc	scob[.]me
	2ug[.]us	wrzt[.]link	ldka[.]info	trqrh[.]com	hpko[.]cc	xnxk[.]me
	z3w[.]us	hhqm[.]link	fbvn[.]info	nhcux[.]com	ddkn[.]cc	zoru[.]me
	yw9[.]us	ezqz[.]link	baew[.]info	khrig[.]com	mpsi[.]cc	mjzo[.]me
	8tm[.]us	zyke[.]link	shpw[.]info	dvcgg[.]com	wkby[.]cc	ouzp[.]me

Table 1: Examples of domains registered by Prolific Puma on different TLDs containing 3 to 4 characters long domain labels.

Infoblox uses a wide range of reputation scores as features in our analytics. Our reputation algorithm is publicly available, applies to all data types, and is statistically optimal, meaning that another algorithm using the same data would not be more accurate. The scores are adjusted to a normal distribution that can be interpreted consistently across time and data type. A score of 7 is considered high risk and is 1.5 to 3.5 standard deviations above the mean. Historic analysis of registrar reputation and name server reputation can be found in our quarterly threat intelligence reports for Q3 and Q4 2022, respectively.

Over the last 18 months, Prolific Puma has primarily used NameSilo for registration and name servers. NameSilo, a cheap domain name and hosting provider, is frequently abused by malicious actors. Aside from affordability, they offer an API, as do many registrars, which facilitates bulk registration by both legitimate users and criminals. To register a domain with NameSilo you need only an email address and a method of payment. However, to configure the domain for use, a name and physical address are required. Domains that are registered but unconfigured are parked; the IP address returned through DNS belongs to SEDO Gmbh and is part of the premium SEDO Multi-Listing Service offered to registrars.

NameSilo is a highly abused registrar according to the Infoblox reputation algorithm. We currently rate the risk of domains registered with NameSilo as a 7 on a scale of 0 to 10, where 10 is considered extremely high risk and 5 is average. In addition to TLDs, we can also apply our reputation algorithm to name servers. Prolific Puma uses the default name servers for NameSilo, which are within the `dnsowl[.]com domain`.[11] Our algorithm currently rates the risk of `dnsowl[.]com` name servers as a 6, which is moderate but slightly elevated when compared to all other known name servers.

While it is not rare for DNS threat actors to use a single registrar for their operations, it is somewhat uncommon; as such, the use of a single registrar is a feature in our taxonomy of DNS threat actors. The actors that we track have generally persisted for over a year and are often financially motivated. We find that they frequently choose registrars and TLDs that are the least expensive and hassle-free. While NameSilo is a cheap registrar, it is not the only one, and it will not offer the lowest price on domains over a long period of time. In the past, Prolific Puma registered large numbers of domains with other cheap providers, notably NameCheap. The consistent use of NameSilo over a long period of time is notable, but the motivation is unknown.

ABUSE OF usTLD

Prolific Puma has registered thousands of domains in the usTLD since May 2023. This is remarkable because, according to the usTLD Nexus Requirements Policy, only U.S. citizens, or U.S.-affiliated businesses are eligible to register domains in it.[12] Moreover, the usTLD requires transparency; no domain names may be registered privately. As a result, the email address, name, street address, and phone number associated with the domain are publicly available. While this might seem a likely deterrent to crime, it has not been effective; the usTLD is well-known for abuse.

As Krebs on Security recently reported, the usTLD is one of the most abused country code TLDs (ccTLDs) and there is no verification made of the registrant's relationship to the United States.[13] While Krebs holds GoDaddy accountable as the registry, the TLD suffered from abuse before they took over registry responsibilities in 2020. While once a highly structured and controlled TLD, second level domain (SLD) registrations became available in 2002 after Neustar was awarded the contract to administer the TLD.[14] Infoblox rates the usTLD as a moderate but slightly elevated risk, with a score of 6, in comparison to all other TLDs.

Registration of a `.us` domain with NameSilo requires an email address, as well as selection of one of the five Nexus categories and application purposes, as shown below in Figure 4. These are used to establish the registrant's association with the United States; however, the acceptance criteria are very broad.[15] During the registration process, the user is warned that they must qualify for one of these and choose a selection. The application purpose requirement separates personal from organizational registrations.

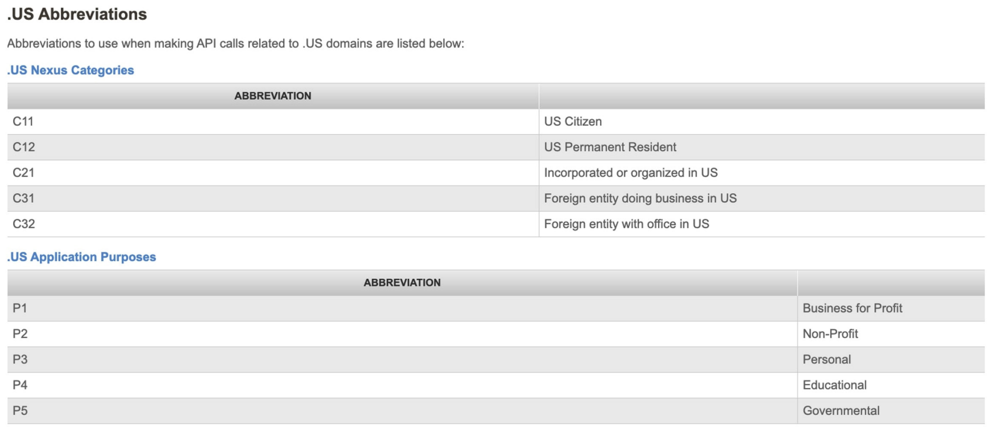
[11] https://www.namesilo.com/support/v2/articles/domain-manager/dns-troubleshooting

[12] https://www.about.us/faqs

[13] https://krebsonsecurity.com/2023/09/why-is-us-being-used-to-phish-so-many-of-us/

[14] https://en.wikipedia.org/wiki/.us

[15] https://www.namesilo.com/popups/us_abbreviations.php



.US Abbreviations

Abbreviations to use when making API calls related to .US domains are listed below:

.US Nexus Categories

ABBREVIATION	
C11	US Citizen
C12	US Permanent Resident
C21	Incorporated or organized in US
C31	Foreign entity doing business in US
C32	Foreign entity with office in US

.US Application Purposes

ABBREVIATION	
P1	Business for Profit
P2	Non-Profit
P3	Personal
P4	Educational
P5	Governmental

Figure 4. Registrants of domain names within the usTLD must choose a related Nexus category and application purpose from those listed above. This information is published in the WHOIS record.

In order to fully configure the domain with NameSilo, the registrant must also provide a name, physical address and phone number, but these are unverified, and the related WHOIS records are not updated automatically. Without an update, only the email address associated with the purchase is publicly available. The registrant can choose to associate contact information with previously purchased domain names, but this is a separate configuration from the account holder's details. This entire process can be completed with fake data, and the domain can be paid for with Bitcoin, enabling threat actors to abuse the service without much difficulty. While NameSilo is the registrar being abused in this particular case, the difficulties highlighted here are common across the industry.

Prolific Puma domain registrants have historically claimed to be a U.S. citizen (C11) using the domain to conduct business for profit (P1), although this pattern has recently changed. **Starting on October 4th, we observed Prolific Puma domains within the usTLD switch to a domain for personal use (P3) and with private registration settings, including both existing and new registrations**. This activity eliminated any doubt that Prolific Puma was a malicious actor. As of mid-October, nearly 2000 Prolific Puma domains in the usTLD now have private registration.

The presence of private registrations within the usTLD is alarming and violates the terms of the usTLD. Lack of detailed information through the WHOIS data has hindered intelligence investigations for the last several years, but more importantly, through our own experience with NameSilo, it is not possible to select private registration for domains in the usTLD through their interface. And yet, it was done. Digging a little deeper and assessing all domains we processed between September 1st and October 15th, we found that while Prolific Puma made up the vast majority of .us domains under Privacy Guardian protection, there were others. Of the over 200 registrars reporting usTLDs during this timeframe, only four registrars were associated with private registration data, as shown in the table below. **Of the total domains with private records, over 99% were registered with NameSilo**. At this time, we are not able to explain this behavior.

Registrar	Domain Count (Sept 1 – Oct 15, 2023)
NameSilo – Prolific Puma	1062
NameSilo – possibly not Prolific Puma	411
PorkBun	5
NameCheap	4
Sav.com	1

Table 2. Privately registered domains in the usTLD by registrar. These are in violation of the usTLD policies.

While the limitations of `.us` domain names may seem strict, upon closer review, only wholly foreign entities are excluded from registering domains within this TLD. If the registrant is suspected of providing false WHOIS information, the Internet Corporation for Assigned Names and Numbers (ICANN) requires the registrar to investigate and allow the information to be updated.[16] According to the Nexus requirements policy, registrars must provide registrants 30 days to update incomplete or incorrect information. NameSilo and GoDaddy are better positioned to take down domains based on their malicious activity than their Nexus qualifications. But in the case of middle-layer adversaries like Prolific Puma, exactly how do they do that?

The abuse of the usTLD, similar to that of others like `.xyz` and `.website`, is real. But with modern privacy regulations and technologies, separating abuse from legitimate use is not trivial, particularly at the scale of the DNS. Protecting consumers and organizations against DNS threat actors requires industry collaboration. For our part, we informed both NameSilo and GoDaddy of the Prolific Puma activity in September. Aside from the potential violation of usTLD requirements, however, it is difficult for a registrar to regulate domains that are not used directly for malicious purposes. We have also shared a large collection of recent domains with Spamhaus and other vendors.[17]

PROLIFIC PUMA CHARACTER

At their heart, threat actors are individuals. They have quirks that often come through in their tactics, techniques, and procedures (TTPs). Malware threat actors might be separated by their choice of variable names or how they comment their code. These choices might reflect their interests, habits, and sense of humor. DNS threat actors are no different, though we generally have little information to work with in DNS and domain registration records.

At Infoblox, we focus on suspicious and malicious DNS activity. While we attribute domain name resources to a DNS threat actor, we rarely attempt to identify their true identity or location. This type of attribution work, in which analysts attempt to tie virtual world activity to the physical world, is a specialized field and time consuming. However, because Prolific Puma registers domains in the usTLD, a registry that does not allow private registration, we can gain a glimpse into the personality of Prolific Puma.

[16] https://www.icann.org/resources/pages/inaccuracy-2013-03-22-en

[17] https://www.spamhaus.org/

Where possible, Prolific Puma uses private domain registration, but usTLD registrations must be public. For these domains, the actor has consistently used an email address containing a reference to the song October 33 by the Black Pumas.[18] An Austin, Texas-based psychedelic soul band, the Black Pumas gained fame in 2019 with their single, Colors.[19] The song October 33 did not reach the top charts, and like Prolific Puma, retains some mystery.[20] While the lyrics are overtly a love letter, they make references to loneliness and the music was intended to have a haunting feel.[21] In spite of their Grammy nomination as Best New Artist in 2019, the Black Pumas are not a household name. Prolific Puma uses the name Leila Puma, a name constructed to again refer to the Black Pumas. The name Leila originates in Arabic and means "night."

While we don't know the real world identity of Prolific Puma, we gain an interesting insight into their personality from their registration data. In addition to references to the Black Pumas and their mysterious song October 33, Prolific Puma uses a personal Ukrainian email address. The address they provide is a primary school in Poland, a nondescript building that might be found in any industrial city. The city of Łódź, the third largest city in Poland, has welcomed Ukrainian refugees since the Russian invasion in February 2022.[22] A Black Pumas cover of the Kinks song "Strangers" was made into an emotional YouTube video featuring Ukrainian refugees entitled "Ukraine Strangers." Although unrelated to Prolific Puma activities, this video reached a significant audience in Fall 2022.[23] As noted earlier, the registrant's information is unverified by NameSilo and appears fake, but their choices give some insight into the person or people who make up Prolific Puma.

PROLIFIC PUMA OPERATIONS

Following the registration of a domain, Prolific Puma often leaves it unused, or parked, for several weeks. This technique is referred to as **strategic aging**.[24] Because phishing attacks are traditionally tied to newly registered domains, many security systems will block access to them. In response, threat actors realized that by waiting to use domains in their campaigns, or "aging" them, they could bypass many security protections.

Prolific Puma will make a small number of DNS queries during the aging process, a method used by threat actors to gain reputation for the domain names. During this period, the domains are parked with NameSilo. Prolific Puma will then transfer them to bulletproof hosting providers, purchased using Bitcoin, on a virtual private server (VPS) with a dedicated IP address. We have found that they will abandon domains after some time, leaving the DNS record pointing to the dedicated IP address.

Based on the breadth of operational techniques we have seen, we suspect that Prolific Puma is providing a service for others and that the final landing pages are not in their control. It remains possible, though, that the same threat actor controls both the link shortening service and all of the malicious activity conducted through it. We have not

[18] https://www.blackpumas.com/

[19] https://en.wikipedia.org/wiki/Black_Pumas

[20] https://www.youtube.com/watch?v=an3AkQL62F8

[21] https://www.facebook.com/theblackpumas/videos/black-pumas-oct-33-song-breakdown/461719384620852/

[22] https://eurocities.eu/latest/ukrainian-refugee-integration-in-lodz-and-timisoara/#:~:text=The%20city%20of%20Lodz%20in,refugees%20since%20the%20Russian%20invasion

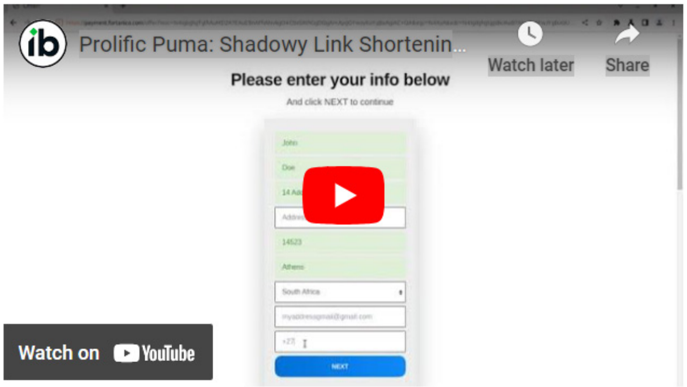
[23] https://www.youtube.com/watch?v=D_Ap_7wjHIs

[24] https://heimdalsecurity.com/blog/aged-domains-the-silent-danger-to-cybersecurity-new-report/

determined how Prolific Puma advertises its services, how its users go about receiving the shortened URL, or whether it has any legitimate traffic. Within the campaigns through the Prolific Puma service, we have found large networks of domains controlled by other DNS threat actors, often registered with cheap registrars such as NameCheap. Some of these campaign domains are also generated by RDGAs.

AN EXAMPLE CAMPAIGN

Prolific Puma operates a link shortener for a variety of phishing, scam, and malware activities. Below, we describe an example of one of the campaigns it serves. Figures 5.1-5.4 show screenshots of what a victim would encounter after clicking on the initial shortened link, `http://bwkd[.]me/ZFjfA3`. The link leads to a phishing page designed to appear like an email, prompting the user to provide personal details and make a payment, and then it infects the user with browser plug-in malware. We have also captured a screenshot recording of the process, shown below.


Prolific Puma: Shadowy Link Shortenin...

Please enter your info below

And click NEXT to continue

John

Doe

14 Ad

Addr

14523

Athens

South Africa

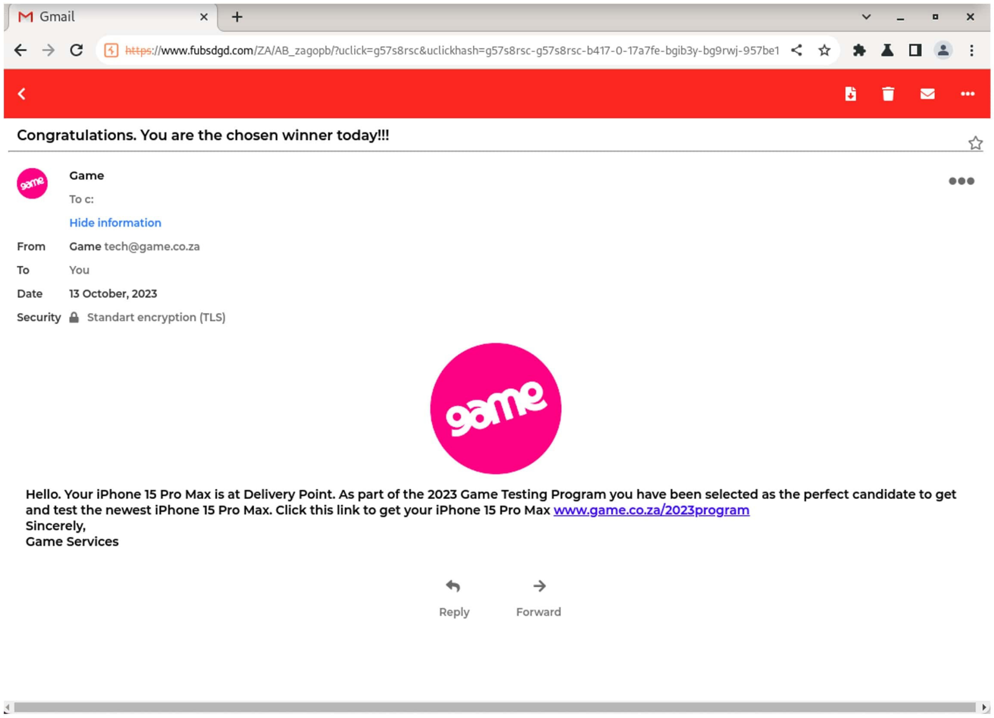
myaddressgmail@gmail.com

+27

The technical steps between the shortened link and the browser plug-in malware in this campaign are as follows:

- The first shortened link `http://bwkd[.]me/ZFjfA3` redirects to
- `http://ksaguna[.]com/click.php?key=<redacted>`, which itself redirects to
- `https://www[.]asdboloa[.]com/ZA/AB_zagopb/?uclick=<redacted>`
    - » This final website is a fake Gmail message telling the user that they have won the opportunity to test the new iPhone 15.
- The user is instructed to click on a link to claim their phone at `https://www[.]game[.]co[.]za/2023program` and enter their delivery information. The website `www[.]game[.]co[.]za` is a South African discount retailer using promotional drives to draw consumers.
- Following this link under the right conditions leads to a prompt to pay 18 South African Rand (ZAR) to participate in the trial.
- From there, the user is presented with a page claiming to be postal tracking and prompting them to accept notifications from `fubsdgd[.]com`. Clicking “accept” triggers the installation of browser malware that uses the OneSignal service to push notifications. While commonly associated with ads, in our experience, browser plug-in malware is commonly used to deliver scams, phishing, and other malware, along with ads.
- Finally, the victim is taken through a series of prompts asking them to verify shipping preferences and enter their personal information.

We do not know how the original shortened URL is delivered to the victim; it may be through an SMS text message given that it opens a fake Gmail message. The domains used during the exploitation of the victim change and are themselves part of a large network. This campaign uses a variety of techniques to assure the victim that the offer is genuine, including an active stream of testimonial reviews at each step from other "recipients."



~~https~~://www.fubsdgd.com/ZA/AB_zagopb/?uclick=g57s8rsc&uclickhash=g57s8rsc-g57s8rsc-b417-0-17a7fe-bgib3y-bg9rwj-957be1

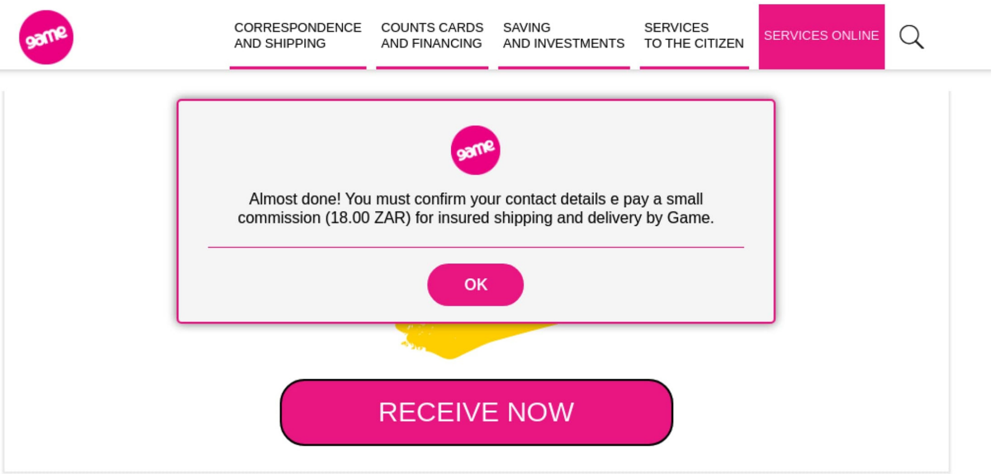
Congratulations. You are the chosen winner today!!!

Game
To c:
Hide information

From	Game tech@game.co.za
To	You
Date	13 October, 2023
Security	Standart encryption (TLS)

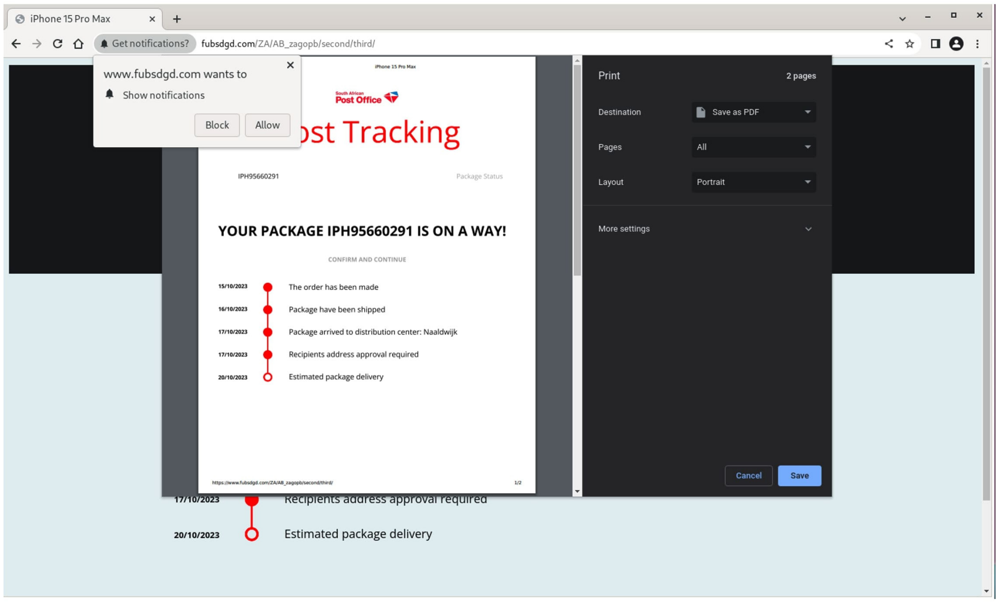
Hello. Your iPhone 15 Pro Max is at Delivery Point. As part of the 2023 Game Testing Program you have been selected as the perfect candidate to get and test the newest iPhone 15 Pro Max. Click this link to get your iPhone 15 Pro Max www.game.co.za/2023program
Sincerely,
Game Services

Figure 5.1: An example of the content delivered by Prolific Puma link shorteners. The original shortened link (http://bwkd[.]me/ZFjfA3) redirected and eventually led to a phishing page designed to look like an email served by Gmail.



Almost done! You must confirm your contact details e pay a small commission (18.00 ZAR) for insured shipping and delivery by Game.

Figure 5.2. The scam and identity theft portion of the campaign. After selecting to accept the free iPhone as shown in Figure 5.1, the user is asked to pay a fee and provide their name and address.


iPhone 15 Pro Max
Get notifications?
fubsdgd.com/ZA/AB_zagopb/second/third/
Block
Allow
South African Post Office
Print
Cancel
Save

www.fubsdgd.com wants to

Show notifications

iPhone 15 Pro Max

ost Tracking

IPH95660291 Package Status

YOUR PACKAGE IPH95660291 IS ON A WAY!

CONFIRM AND CONTINUE

15/10/2023 The order has been made
16/10/2023 Package have been shipped
17/10/2023 Package arrived to distribution center: Naaldwijk
17/10/2023 Recipients address approval required
20/10/2023 Estimated package delivery

https://www.fubsdgd.com/ZA/AB_zagopb/second/third/ 1/2

Print 2 pages

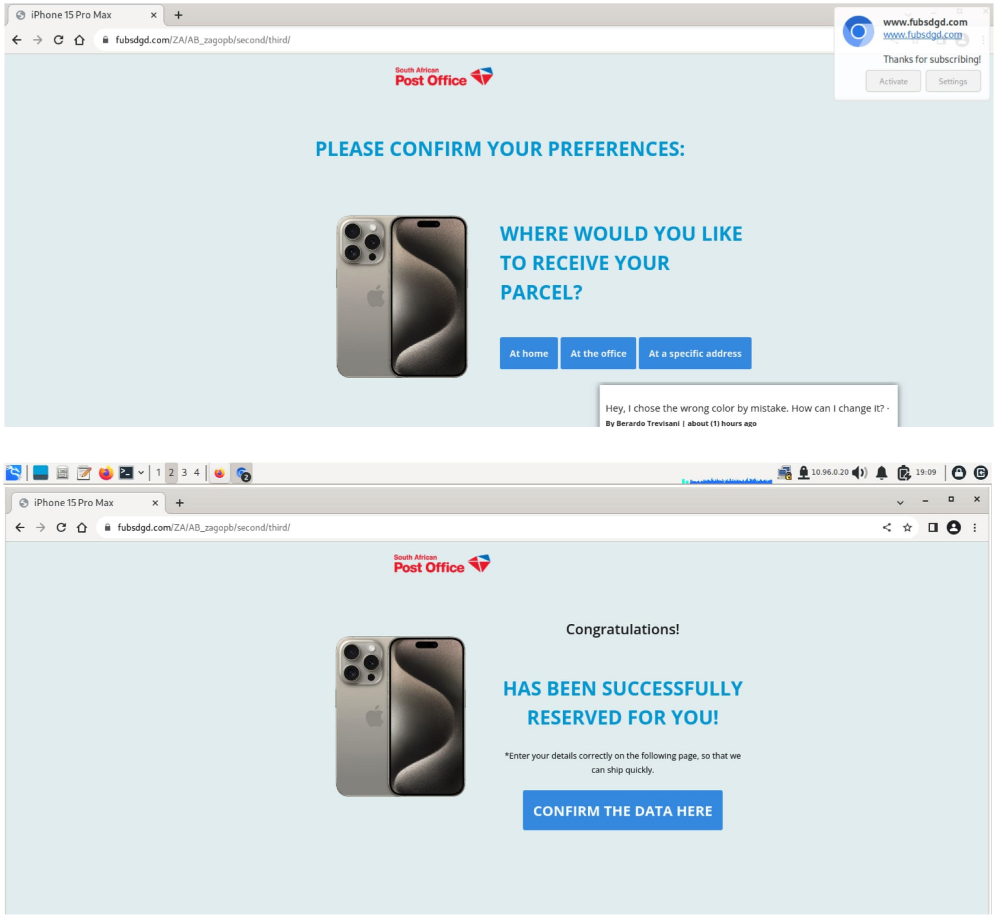
Destination: Save as PDF

Pages: All

Layout: Portrait

More settings

Figure 5.3. The malware portion of the campaign. After the victim pays the fee shown in Figure 5.2, they receive a package delivery notification and are asked to show notifications from fubsdgd[.]com. If they accept notifications, malware is delivered to the victim's machine.



www.fubsdgd.com
www.fubsdgd.com
Thanks for subscribing!

PLEASE CONFIRM YOUR PREFERENCES:

WHERE WOULD YOU LIKE TO RECEIVE YOUR PARCEL?

Hey, I chose the wrong color by mistake. How can I change it? ·
By Berardo Trevisani | about (1) hours ago

Congratulations!

HAS BEEN SUCCESSFULLY RESERVED FOR YOU!

*Enter your details correctly on the following page, so that we can ship quickly.

Figure 5.4a-b. After accepting notifications shown in Figure 5.3, the user is prompted to provide further details and preferences in a series of screens.

CONCLUSION

Prolific Puma demonstrates how the DNS can be abused to support criminal activity and remain undetected for years. As part of the supply chain, this actor is harder to detect and defeat. Traditional security systems protect the user from harm based on the final landing page of a link. DNS detection and response systems, however, can disrupt Prolific Puma and similar service providers, thereby thwarting all of the actors who rely on them to deliver phishing, scams, and malware. By using an RDGA and cheap domain registrars, Prolific Puma is able to scale and persist their operations. But at the same time, we can detect the use of an RDGA through DNS and domain registration records.

Prolific Puma is only one of the link shortener operators that Infoblox has discovered, and link shorteners are only one type of service found in the shadow economy. **Most often we uncover DNS threat actors first through analytics that identify suspicious newly registered, configured, or queried domains**. Even prior to correlating domains with malicious activity, we can use other features, such as TLD and name server reputation, to flag the related domains as suspicious. Later, we are able to connect domains together and isolate a threat actor. By blocking access to suspicious domains, organizations can implement a highly effective, low-regret, high-security policy for their network and users.\

INDICATORS OF ACTIVITY

Below is a small selection of indicators related to Prolific Puma and the campaigns they facilitate. A more comprehensive list of recent indicators is found in our open GitHub repository here.

Indicator of Activity	Type of Indicator
hygmi[.]com	Prolific Puma link shortener domain
yyds[.]is	
0cq[.]us	
4cu[.]us	
regz[.]info	
u5s[.]us	
1jb[.]us	
jrbc[.]info	
uhje[.]me	
0md[.]us	
fh3[.]us	
0qa[.]us	
9jw[.]us	
iv0[.]us	
od9[.]us	
rpzp[.]me	
8fx[.]us	
3vb[.]us	
r1u[.]us	
zost[.]link	
9ow[.]us	
sf8i[.]us	
bu9[.]us	
ce2[.]us	
wf6[.]us	
v8z[.]us	
zj4[.]us	
rjvb[.]link	
fssu[.]link	
xbsf[.]link	
wqeh[.]link	

Indicator of Activity	Type of Indicator
ymql[.]link 7tz[.]us w6q[.]us giqj[.]me u3q[.]us ke0[.]us v1u[.]us ti7[.]us 2zc[.]us gf6[.]us 6dr[.]us 6or[.]us kc0[.]us 0ty[.]us styi.info 6fe[.]us u8n[.]us d6s[.]us	
v8z[.]us zj4[.]us rjvb[.]link fssu[.]link xbsf[.]link wqeh[.]link ymql[.]link 7tz[.]us	Link shortener hosting IPs

Indicator of Activity	Type of Indicator
bwkd[.]me ksaguna[.]com asdboloa[.]com game.co[.]za	Redirection and landing pages
fubsdgd[.]com	Browser-plugin malware domains
blackpumaoct33@ukr[.]net	Prolific Puma registration email address

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 give us a high-powered scope to zero in on cyber threats. 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.

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

+1.408.986.4000
www.infoblox.com

Version: 20241008v1