infoblox

Threat Intel

PROLIFIC PUMA: UNDURCHSICHTIGER LINK-SHORTENER ERMÖGLICHT CYBERKRIMINALITÄT

Autoren:
Laura da Rocha
Renée Burton
Stelios Chatzistogias
Darby Wise

INHALTSVERZEICHNIS

ZUSAMMENFASSUNG 3

UNDURCHSICHTIGER LINK-SHORTENER-SERVICES 4

ERKENNUNG UND EIGENSCHAFTEN VON DOMAINNAMEN 6

MISSBRAUCH VON usTLD 8

PROLIFIC PUMA CHARAKTER 10

PROLIFIC PUMA OPERATIONS 11

EINE BEISPIELKAMPAGNE 12

FAZIT 15

AKTIVITÄTSINDIKATOREN 15

INFOBLOX THREAT INTEL 17

ZUSAMMENFASSUNG

Halloween mag die gruseligste Zeit des Jahres sein, aber Bedrohungsakteure im Internet treiben jeden Tag erschreckende Dinge. Im vergangenen Monat haben wir zwei Begriffe eingeführt: Bedrohungsakteure im Domain Name System (DNS) und RDGA (Registered Domain Generation Algorithm). Wir haben auch einen Einblick in einen Typen von DNS-Bedrohungsakteuren gegeben, den hartnäckigen Phisher, und zwar durch eine Enthüllung über Open Tangle.

Heute stellen wir den zweiten Akteur in dieser Reihe vor: **Prolific Puma**. Seit vier Jahren – vielleicht sogar länger – agiert Prolific Puma im Verborgenen, unerkannt von den Verteidigern. Wir kennen zwar ihre Entstehungsgeschichte nicht, können Prolific Puma jedoch über DNS aufspüren und über die Wahl ihrer Domainnamen-Registrierung einen Einblick in ihren Charakter gewinnen. Was steckt hinter dem Namen? Prolific kommt von der einfachen Tatsache, dass es sich um ein Netzwerk handelt, das ständig erweitert wird und in dem fast täglich neue Domains registriert werden. Was Puma betrifft, nun ... wir werden später in diesem Dokument mehr über die Inspiration berichten.

Die Cyberkriminalität ist die drittgrößte Wirtschaftsform der Welt mit einem geschätzten Wert von 8 Billionen US-Dollar im Jahr 2023, und Prolific Puma ist Teil der Lieferkette.[1] Sie erstellen Domainnamen mit einem RDGA und nutzen diese Domains, um anderen böswilligen Akteuren einen Link-Shortener zur Verfügung zu stellen, der ihnen dabei hilft, nicht entdeckt zu werden, während sie Phishing, Betrug und Malware verbreiten. Wenn wir Prolific Puma zerschlagen, zerschlagen wir ein größeres Segment der kriminellen Wirtschaft. Abbildung 1 gibt einen Überblick über die Operationen von Prolific Puma und darüber, wie sie Kriminellen helfen. Prolific Puma generiert algorithmisch große Mengen an Domains und verwendet diese Domains dann, um verkürzte Links für andere böswillige Akteure zu generieren, wodurch diese ihre wahren Aktivitäten verbergen können.

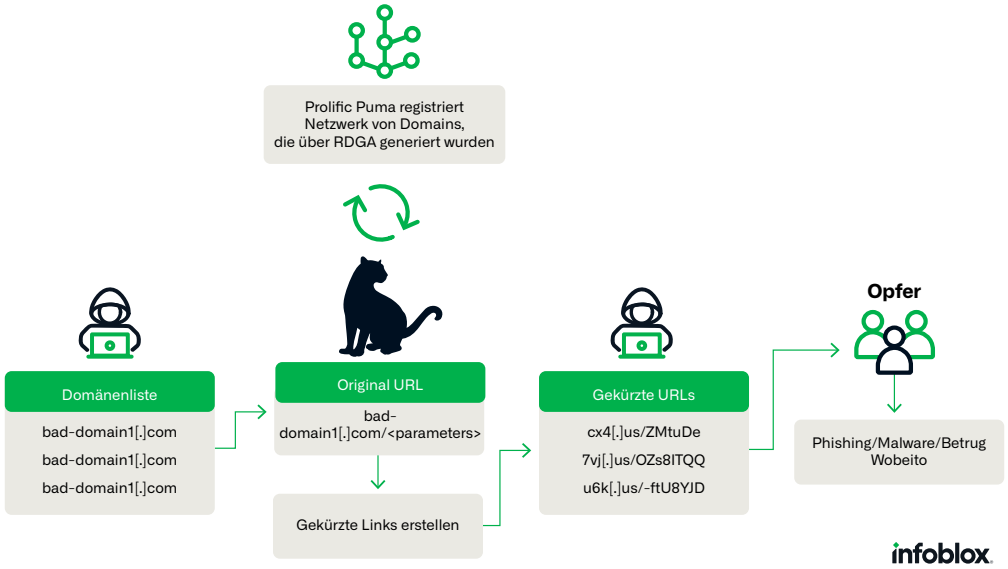


Abbildung 1. Ein Überblick über die Rolle von Prolific Puma in der Lieferkette der Cyberkriminalität.

Unseren Erkenntnissen zufolge ist dieses Dokument die erste Beschreibung eines umfangreichen verdeckten Link-Shortener-Services. Darüber hinaus wurde **der Akteur nicht über Malware oder Phishing-Websites, sondern über DNS-Analysen entdeckt**. Prolific Puma ist bemerkenswert, weil es dem Unternehmen gelungen ist, böswillige Aktivitäten über einen Zeitraum von mehr als 18 Monaten zu ermöglichen, ohne dass die Sicherheitsbranche dies bemerkt hat. Mit einer riesigen Sammlung von Domainnamen ist es dem Unternehmen möglich, böswilligen Datenverkehr zu verbreiten und einer Entdeckung zu entgehen.

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

Diese Entdeckung zeigt, wie nützlich die Verwendung von DNS- und Domainregistrierungsdaten nicht nur für die Erkennung verdächtiger Aktivitäten ist, sondern auch für die Zusammenführung dieser Informationen zu einer konsolidierten Ansicht eines DNS-Bedrohungsakteurs. Wir konnten zwar den Prolific Puma über DNS aufspüren und verfolgen, aber ihre Geschichte zeigt die Herausforderungen, mit denen Domain-Registrare und -Register bei der Missbrauchskontrolle konfrontiert sind. Wenn die Akteure weit vom eigentlichen Verbrechen entfernt sind, können Richtlinien die Fähigkeit behindern, die unterstützenden Bereiche zu identifizieren und zu beseitigen.

Wir **sind vor sechs Monaten erstmals durch einen RDGA-Detektor auf die Prolific-Puma-Domains aufmerksam geworden**. Seitdem haben wir ein besseres Verständnis für ihre Aktivitäten entwickelt, indem wir spezialisierte DNS-Detektoren einsetzen, um das Netzwerk in seiner Entwicklung zu verfolgen. In den folgenden Abschnitten werden wir den Linkverkürzungsdienst von Prolific Puma, die Art und Weise, wie sie Domains registrieren und hosten, ihren Missbrauch der US-amerikanischen Top-Level-Domain (usTLD) und die Rolle, die sie bei der Begünstigung von Kriminalität im Internet spielen, erörtern. Für diese Veröffentlichung konzentrieren wir uns absichtlich auf den Akteur und seine Nutzung von DNS und nicht auf die Kampagnen, die seine Dienste nutzen. Wir stellen ein detailliertes Beispiel für eine Kampagne vor, die mithilfe der Infrastruktur von Prolific Puma durchgeführt wurde und sowohl zum Phishing des Benutzers als auch zur Bereitstellung von browserbasierter Malware führte.

UNDURCHSICHTIGER LINK-SHORTENER-SERVICES

Prolific Puma bietet Kriminellen einen geheimen Link-Shortener-Services.[2] Beim direkten Zugriff auf eine aktive Second-Level-Domain (SLD) wird folgende Meldung angezeigt:

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

Der ursprüngliche Zweck von Link-Shortenern bestand darin, das Teilen von Website-Links zu erleichtern und die Größenbeschränkungen in den sozialen Medien zu berücksichtigen. Zum Beispiel:

- Der Link `https://tinyurl.com/c6u6myhw` ist eine verkürzte Version von
- https://blogs.infoblox.com/cyber-threat-intelligence/introducing-dns-threat-actors/, unser Dokument, in dem das Konzept der DNS-Bedrohungsakteure vorgestellt wurde.

Wenn der Benutzer auf den gekürzten Link klickt, wird er zu einer anderen URL weitergeleitet. Im Hintergrund wird eine DNS-Anfrage gestellt, um die IP-Adresse für die Domain des Kürzungsdienstes aufzulösen, z. B. `tinyurl[.]com`. Die Webanfrage wird dann an diese Adresse gesendet, die den Hash-Wert enthält, der zur Identifizierung der ursprünglichen Website verwendet wird. Im obigen Beispiel verwendet der TinyURL-Dienst den Wert „c6u6myhw”, um zu bestimmen, wohin die Verbindung umgeleitet werden soll. Es werden weitere DNS-Anfragen gestellt, um die IP-Adresse zu ermitteln, die den endgültigen Inhalt hostet, in diesem Fall für `blogs.infoblox.com`. Während legitime Benutzer einen einfachen verkürzten Link erstellen, um ihn zu teilen, kann ein böswilliger Akteur mehrere Umleitungsebenen vor der endgültigen Zielseite verwenden. Dieser Prozess ist in Abbildung 2 dargestellt.

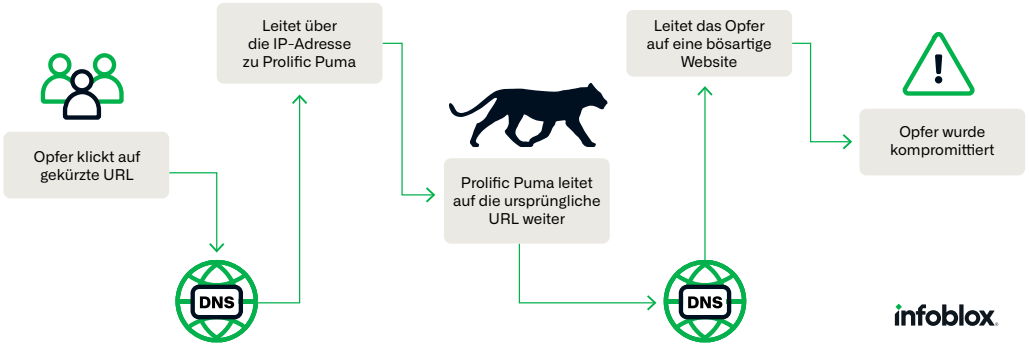


Abbildung 2: Ein fiktiver Pfad, der zeigt, wie eine gekürzte URL mit DNS und dem Link-Shortener-Service interagiert, um das Opfer auf schädliche Inhalte umzuleiten.

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

Es ist bekannt, dass böswillige Akteure Link-Shortener für Phishing-Angriffe missbrauchen.[3] In den meisten Fällen, über die berichtet wird, handelt es sich bei den Link-Shortenern jedoch um bekannte, öffentlich zugängliche Dienste wie TinyURL, BitLy und Google. Dieser Missbrauch ist so weit verbreitet, dass die Marketingfirma Rebrandly seriösen Unternehmen empfiehlt, beliebte Kurzformate in ihren E-Mails zu vermeiden.[4]

Prolific Puma wirbt nicht offen für seine Dienstleistungen. Eine Zeit lang wussten wir, dass wir einen Linkverkürzungsdienst verfolgten, aber es war unklar, was sie lieferten und für wen sie den Dienst anboten. Das Schwierige an der Untersuchung von Linkverkürzern ist, dass es ohne vollständige URL nicht möglich ist, die endgültige Zielseite zu bestimmen. Unsere Detektoren hatten eine große Gruppe miteinander verbundener Domains mit verdächtigem Verhalten und ohne öffentliche Präsenz gefunden, aber wir standen vor der Herausforderung, zu ermitteln, wie sie genutzt wurden.

Wir haben schließlich mehrere Fälle von verkürzten Links erfasst, die auf Zielseiten umgeleitet wurden, bei denen es sich um Phishing- und Betrugsseiten handelte. Interessanterweise variierte die Reihenfolge der Weiterleitungen zur letzten Seite stark. In einigen Fällen führten die gekürzten Links direkt zum Inhalt.[5] In anderen Fällen gab es mehrere Umleitungen, bevor die endgültige Zielseite angezeigt wurde.[6] Wir konnten auch gekürzte Links von Prolific Puma sehen, die zu einem anderen verkürzten Link umgeleitet wurden, der von einem anderen Dienst erstellt wurde.[7] In einigen Fällen führte der gekürzte Link zu einer CAPTCHA-Herausforderung.[8] Wir haben auch Berichte gefunden, dass bereits im Januar 2020 Links zu Prolific Puma per SMS mit gefälschten Amazon-Lieferbenachrichtigungen versendet wurden.[9] Die unterschiedliche Handhabung der Links und die Bereitstellung der Inhalte lassen darauf schließen, dass Prolific Puma höchstwahrscheinlich mehrere Akteure mit seinen Dienstleistungen versorgt. Es gibt Hinweise darauf, dass die gekürzten Links den Opfern hauptsächlich über Textnachrichten zugestellt werden, aber sie könnten auch in anderen Kontexten verwendet werden, z. B. in sozialen Medien und in der Werbung.

Prolific Puma ist nicht der einzige illegale Linkverkürzungsdienst, den wir entdeckt haben, aber es ist der größte und dynamischste. Wir haben keine legitimen Inhalte gefunden, die über ihren Link-Shortener bereitgestellt werden. Später beschreiben wir in diesem Bericht wir ein konkretes Beispiel für einen verkürzten Link, der zu Phishing für Benutzerinformationen, einer betrügerischen Zahlung und der Verbreitung von Browser-Malware führt.

Als Dienstleister innerhalb des Ökosystems der Cyberkriminalität hilft Prolific Puma anderen böswilligen Akteuren, der Entdeckung zu entgehen – eine Taktik, die im MITRE ATT&CK-Framework für Unternehmen enthalten ist.[10] Aber auch ihre indirekte Rolle bei der Verbreitung von Phishing, Betrug und Malware an Verbraucher hilft ihnen, nicht entdeckt zu werden. Sicherheitsanbieter können zwar die endgültigen Inhalte identifizieren und blockieren, aber ohne einen umfassenderen Überblick ist es schwierig, den vollen Umfang der Aktivität zu erkennen und die Domains einem einzigen DNS-Bedrohungsakteur zuzuordnen. Wie wir nachfolgend sehen werden, können wir dies mithilfe von DNS-Analysen tun.

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/

ERKENNUNG UND MERKMALE VON DOMAINNAMEN

Um originale Informationen für Infoblox-DNS-Erkennungs- und Reaktionsprodukte in der Cloud und vor Ort bereitzustellen, haben wir eine große Anzahl unabhängiger Algorithmen entwickelt, um verdächtige und bösartige Domains sowie zugehörige IP-Adressen und andere DNS-Ressourcen zu erkennen. **Durch die Aggregation von passiven DNS-Abfrageprotokollen (pDNS) und anderen Datenquellen führen wir eine Reihe von Analysen an einer Sammlung neu abgefragter, registrierter oder konfigurierter Domains durch**. Diese Analysen charakterisieren die Domains unabhängig voneinander und reichen von der Kennzeichnung einer Domain als verdächtig bis hin zur Zuordnung zu einem DNS-Bedrohungsakteur.

Die Entdeckung von Prolific Puma folgte einem Muster, das viele der DNS-Bedrohungsakteure, die wir intern benennen und verfolgen, gemeinsam haben. Bei unseren automatisierten Analysen wurden einige verwandte Domains zunächst einzeln als verdächtig eingestuft. Diese Einstufung ermöglichte es, die Domains in unseren rekursiven DNS-Resolvern zum Schutz von Kunden zu blockieren, erfasste jedoch nicht unbedingt die gesamte Bandbreite der Aktivitäten und ordnete die Domains nicht einem einzelnen Akteur zu. **Als wir im Frühjahr 2023 Algorithmen für die RDGA-Erkennung bereitstellten, wurden die Prolific Puma-Domains in Gruppen identifiziert**. Diese Gruppen wurden ebenfalls automatisch ermittelt, aber es wurden statistische Methoden verwendet, um ein hohes Maß an Sicherheit zu gewährleisten, dass die RDGA-Domains von demselben DNS-Bedrohungsakteur registriert wurden. Schließlich identifizierte ein weiterer Algorithmus Ausreißerverhalten bei IP-Auflösungen und korrelierte die einzelnen RDGA-Cluster. Die schiere Größe der Aktivität hat das Profil dieses bestimmten DNS-Bedrohungsakteurs für unsere Human-in-the-Loop-Forschung geschärft, und wir haben spezielle DNS-Fingerabdrücke entworfen, um sie zu verfolgen. Im weiteren Verlauf dieses Abschnitts werden wir Einzelheiten über die Merkmale und Eigenschaften des Domainnamens Prolific Puma mitteilen, die ihn identifizieren.

Da die Verbindung zwischen den Prolific Puma-Domains und den endgültigen Landing Pages indirekt ist, ist der Akteur in gewisser Weise vor Entdeckung geschützt. Durch die Registrierung einer großen Anzahl von Domains stärken sie jedoch auch ihre Fähigkeit, unbemerkt zu bleiben. Bösartiger Datenverkehr wird in relativ geringen Mengen auf diese Domains verteilt. Mit der Zeit können die Domains durch strategisches Altern sogar den Ruf einer „guten“ Seite erlangen. Diese Technik wird von Prolific Puma eingesetzt und wird später in diesem Dokument näher erläutert.

Prolific Puma kontrolliert eines der größten Netzwerke, die wir verfolgen. Seit April 2022 haben sie zwischen 35.000 und 75.000 einzigartige Domainnamen registriert. Abbildung 3 zeigt die Anzahl der eindeutigen Domainnamen, die pro Tag mit 3 oder 4 langen Domainbezeichnungen registriert wurden. Wie wir kürzlich berichteten, haben RDGAs zunehmend traditionelle DGAs ersetzt und stellen Verteidiger vor neue Herausforderungen. Durch den Einsatz dieser Technik können sie ihre Abläufe einfach automatisieren und skalieren. Tausende der täglich von Infoblox erkannten neuen Domains werden von einem RDGA generiert, darunter auch Prolific Puma Domains.

Prolific Puma verwendet NameSilo als Domainnamen-Registrar und neigt dazu, ihre Domains strategisch altern zu lassen, bevor sie ihren Dienst bei anonymen Anbietern hosten. Obwohl es keinen klaren Bezug zu den Vereinigten Staaten gibt, missbraucht Prolific Puma ständig die Top-Level-Domain der USA (usTLD), eine TLD, die für US-Bürger und -Unternehmen reserviert sein sollte. Prolific Puma ist dafür bekannt, sowohl neue als auch aufgegebene Domains zu registrieren. Zum Beispiel wurde 3ty[.]us im Juni 2022 von einem anderen Akteur für Phishing-Kampagnen im Facebook-Messenger verwendet und dann von Prolific Puma registriert, nachdem die Registrierung im Juli 2023 abgelaufen war.

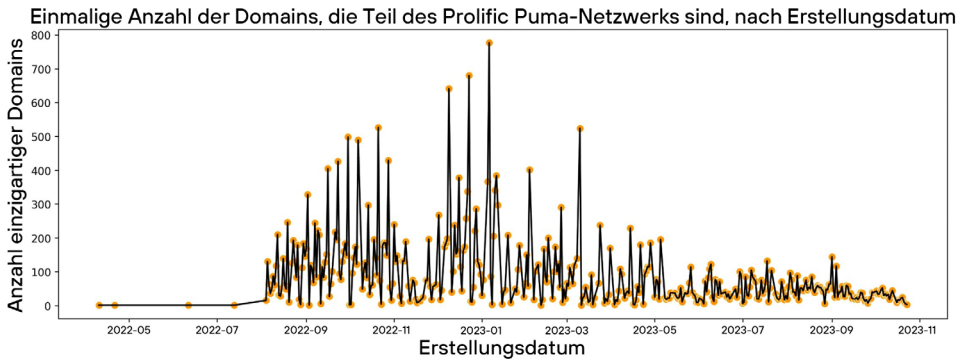


Abbildung 3: Registrierungszeitleiste für Prolific Puma-Domains mit 3 bis 4 Zeichen langen Domainnamen.

Prolific Puma-Domains sind alphanumerisch, pseudozufällig und variabler Länge, in der Regel 3 oder 4 Zeichen lang. Wir haben jedoch auch SLD-Labels mit einer Länge von bis zu 7 Zeichen beobachtet. Die Domains sind auf 13 TLDs registriert, die häufig von böswilligen Akteuren missbraucht werden, darunter: `info`, `us`, `site`, `in`, `link`, `me`, `cc`, `website`, `life`, `xyz`, `club`, `buzz` und `best`. Bis Mai 2023 machte die infoTLD den Großteil der Domains aus. Seitdem hat der Akteur die usTLD für etwa 55 % der insgesamt von ihm erstellten Domains verwendet. Seit Mai 2023 beobachten wir täglich durchschnittlich 43 neue Domains.

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

Tabelle 1: Beispiele für von Prolific Puma registrierte Domains mit 3 bis 4 Zeichen langen Domainnamen unter verschiedenen TLDs.

In den letzten 18 Monaten hat Prolific Puma NameSilo hauptsächlich für die Registrierung und die Nameserver genutzt. NameSilo, ein günstiger Anbieter für Domainnamen und Hosting, wird häufig von böswilligen Akteuren missbraucht. Abgesehen von der Erschwinglichkeit bieten sie, wie viele Registrare, eine API an, die die Massenregistrierung sowohl für legitime Benutzer als auch für Kriminelle erleichtert. Um eine Domain bei NameSilo zu registrieren, benötigen Sie lediglich eine E-Mail-Adresse und eine Zahlungsmethode. Um die Domain jedoch für die Nutzung zu konfigurieren, sind ein Name und eine physische Adresse erforderlich. Domains, die registriert, aber nicht konfiguriert sind, werden geparkt; die über DNS zurückgegebene IP-Adresse gehört der SEDO GmbH und ist Teil des Premium-SEDO-Multi-Listing-Service, der Registraren angeboten wird.

Infoblox verwendet eine Vielzahl von Reputationswerten als Merkmale in unseren Analysen. Unser Reputationsalgorithmus ist öffentlich verfügbar, gilt für alle Datentypen und ist statistisch optimal, d. h. ein anderer Algorithmus, der dieselben Daten verwendet, wäre nicht genauer. Die Werte werden an eine Normalverteilung angepasst, die über Zeit und Datentyp hinweg konsistent interpretiert werden kann. Ein Wert von 7 gilt als hohes Risiko und liegt 1,5 bis 3,5 Standardabweichungen über dem Mittelwert. Historische Analysen der Reputation von Registraren und Nameservern finden Sie in unseren vierteljährlichen Threat-Intelligence-Berichten für das 3. und 4. Quartal 2022.

NameSilo ist laut dem Infoblox-Reputationsalgorithmus ein stark missbrauchter Registrar. Wir bewerten das Risiko von bei NameSilo registrierten Domains derzeit mit 7 auf einer Skala von 0 bis 10, wobei 10 für ein extrem hohes Risiko und 5 für ein durchschnittliches Risiko steht. Zusätzlich zu TLDs können wir unseren Reputationsalgorithmus auch auf Nameserver anwenden. Prolific Puma verwendet die Standard-Nameserver für NameSilo, die sich innerhalb der Domain `dnsowl[.]com` befinden.[11] Unser Algorithmus bewertet das Risiko von `dnsowl[.]com`-Nameservern derzeit mit 6, was im Vergleich zu allen anderen bekannten Nameservern moderat, aber leicht erhöht ist.

Obwohl es nicht selten vorkommt, dass DNS-Bedrohungsakteure einen einzigen Registrar für ihre Operationen nutzen, ist dies eher ungewöhnlich. Daher ist die Nutzung eines einzigen Registrars ein Merkmal in unserer Taxonomie der DNS-Bedrohungsakteure. Die Akteure, die wir beobachten, sind in der Regel seit über einem Jahr aktiv und oft finanziell motiviert. Wir stellen fest, dass sie sich häufig für die günstigsten und unkompliziertesten Registrare und TLDs entscheiden. NameSilo ist zwar ein günstiger Registrar, aber nicht der einzige, und wird über einen längeren Zeitraum nicht den niedrigsten Preis für Domains anbieten. In der Vergangenheit hat Prolific Puma zahlreiche Domains bei anderen günstigen Anbietern registriert, insbesondere bei NameCheap. Die konsequente Nutzung von NameSilo über einen langen Zeitraum ist bemerkenswert, aber die Motivation ist unbekannt.

MISSBRAUCH VON usTLD

Prolific Puma hat seit Mai 2023 Tausende von Domains in der usTLD registriert. Dies ist bemerkenswert, da gemäß der usTLD Nexus Requirements Policy nur US-Bürger oder mit den USA verbundene Unternehmen berechtigt sind, Domains in der usTLD zu registrieren.[12] Außerdem fordert die usTLD Transparenz – es dürfen keine Domainnamen privat registriert werden. Daher sind die mit der Domain verknüpfte E-Mail-Adresse, der Name, die Adresse und die Telefonnummer öffentlich verfügbar. Dies mag zwar eine abschreckende Wirkung auf Kriminelle haben, hat sich aber nicht als wirksam erwiesen. Die usTLD ist für Missbrauch bekannt.

Wie Krebs on Security kürzlich berichtete, ist die usTLD eine der am häufigsten missbrauchten länderspezifischen TLDs (ccTLDs), und es wird nicht überprüft, ob der Registrierende in den Vereinigten Staaten ansässig ist.[13] Während Krebs GoDaddy als Registerstelle zur Verantwortung zieht, kam es zu Missbrauch der TLD, bevor diese 2020 die Verantwortung für die Registerführung übernahm. Während die TLD einst stark strukturiert und kontrolliert war, wurden 2002, nachdem Neustar den Zuschlag für die Verwaltung der TLD erhalten hatte, Registrierungen von Second-Level-Domains (SLD) möglich.[14] Infoblox bewertet die usTLD mit einem Wert von 6 als mäßig, aber leicht erhöhtes Risiko im Vergleich zu allen anderen TLDs.

Für die Registrierung einer `.us`-Domain bei NameSilo ist eine E-Mail-Adresse erforderlich, sowie die Auswahl einer der fünf Nexus-Kategorien und der Verwendungszweck, wie unten in Abbildung 4 dargestellt. Diese werden verwendet, um die Verbindung des Registranten mit den Vereinigten Staaten herzustellen. Die Akzeptanzkriterien sind jedoch sehr weit gefasst.[15] Während des Registrierung wird der Benutzer darauf hingewiesen, dass er sich für eine dieser Optionen qualifizieren und eine Auswahl treffen muss. Die Anforderung des Verwendungszwecks trennt persönliche von organisatorischen Registrierungen.

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

Abbildung 4: Registranten von Domainnamen innerhalb der usTLD müssen eine verwandte Nexus-Kategorie und einen Anwendungszweck aus den oben aufgeführten auswählen. Diese Informationen werden im WHOIS-Datensatz veröffentlicht.

Um die Domain vollständig mit NameSilo zu konfigurieren, muss der Registrierende auch einen Namen, eine physische Adresse und eine Telefonnummer angeben, aber diese werden nicht überprüft und die zugehörigen WHOIS-Einträge werden nicht automatisch aktualisiert. Ohne ein Update ist nur die mit dem Kauf verknüpfte E-Mail-Adresse öffentlich verfügbar. Der Registrierende kann Kontaktinformationen mit zuvor gekauften Domainnamen verknüpfen, dies ist jedoch eine separate Konfiguration von den Angaben des Kontoinhabers. Dieser gesamte Prozess kann mit gefälschten Daten abgeschlossen werden, und die Domain kann mit Bitcoin bezahlt werden, sodass Bedrohungsakteure den Dienst ohne große Schwierigkeiten missbrauchen können. NameSilo ist zwar in diesem speziellen Fall der Registrierende, der missbraucht wird, aber die hier hervorgehobenen Schwierigkeiten sind in der gesamten Branche verbreitet.

In der Vergangenheit haben die Inhaber von Prolific-Puma-Domains angegeben, US-Bürger (C11) zu sein, die die Domain zur gewinnorientierten Geschäftsabwicklung (P1) nutzen, obwohl sich dieses Muster in letzter Zeit geändert hat. **Ab dem 4. Oktober beobachteten wir, dass Prolific Puma-Domains innerhalb der usTLD zu einer Domain für den persönlichen Gebrauch (P3) und mit privaten Registrierungseinstellungen wechselten, sowohl bei bestehenden als auch bei neuen Registrierungen**. Diese Aktivität beseitigte jeden Zweifel daran, dass Prolific Puma ein böswilliger Akteur war. Mitte Oktober hatten fast 2000 Prolific Puma-Domains in der usTLD eine private Registrierung.

Private Registrierungen innerhalb der usTLD ist alarmierend und verstößt gegen die Bedingungen der usTLD. Der Mangel an detaillierten Informationen durch die WHOIS-Daten hat die Ermittlungen der Geheimdienste in den letzten Jahren behindert. Noch wichtiger ist allerdings, dass es nach unseren eigenen Erfahrungen mit NameSilo nicht möglich ist, private Registrierungen für Domains in der usTLD über deren Schnittstelle auszuwählen. Und doch wurde es getan. Bei näherer Betrachtung und Auswertung aller Domains, die wir zwischen dem 1. September und dem 15. Oktober bearbeitet haben, stellten wir fest, dass Prolific Puma zwar die überwiegende Mehrheit der .us-Domains unter dem Schutz von Privacy Guardian ausmachte, es aber auch andere gab. Von den über 200 Registraren, die in diesem Zeitraum usTLDs meldeten, waren nur vier Registrare mit privaten Registrierungsdaten verbunden, wie in der folgenden Tabelle dargestellt. **Über 99 % der Domains mit privaten Einträgen wurden bei NameSilo registriert**. Wir können uns dieses Verhalten derzeit nicht erklären.

Registrierender	Anzahl der Domains (1. September – 15. Oktober 2023)
NameSilo – Prolific Puma	1062
NameSilo – möglicherweise nicht Prolific Puma	411
PorkBun	5
NameCheap	4
Sav.com	1

Tabelle 2: Privat registrierte Domains in der usTLD nach Registrierendem. Diese verstoßen gegen die usTLD-Richtlinien.

Die Einschränkungen für .us-Domainnamen mögen streng erscheinen, bei näherer Betrachtung sind jedoch nur vollständig ausländische Unternehmen von der Registrierung von Domains innerhalb dieser TLD ausgeschlossen. Wenn der Registrierende verdächtigt wird, falsche WHOIS-Informationen bereitzustellen, verlangt die Internet Corporation for Assigned Names and Numbers (ICANN) vom Registrar, die Angelegenheit zu untersuchen und eine Aktualisierung der Informationen zuzulassen.[16] Gemäß der Nexus-Richtlinie müssen Registrare den Registrierenden 30 Tage Zeit geben, um unvollständige oder falsche Informationen zu aktualisieren. NameSilo und GoDaddy sind besser in der Lage, Domains aufgrund ihrer böswilligen Aktivitäten zu sperren, als aufgrund ihrer Nexus-Qualifikationen. Aber wie genau machen sie das im Fall von zwischengeschalteten Angreifern wie Prolific Puma?

Der Missbrauch der usTLD, ähnlich wie bei anderen wie .xyz und .website, ist real. Aber mit modernen Datenschutzbestimmungen und -technologien ist es nicht einfach, Missbrauch von legitimer Nutzung zu trennen, insbesondere auf der Ebene des DNS.
Der Schutz von Verbrauchern und Unternehmen vor DNS-Bedrohungsakteuren erfordert die Zusammenarbeit der Branche. Wir haben sowohl NameSilo als auch GoDaddy im September über die Aktivitäten von Prolific Puma informiert. Abgesehen von der potenziellen Verletzung der usTLD-Anforderungen ist es für einen Registrar jedoch schwierig, Domains zu regulieren, die nicht direkt für böswillige Zwecke verwendet werden. Wir haben auch eine große Sammlung aktueller Domains mit Spamhaus und anderen Anbietern geteilt.[17]

PROLIFIC PUMA CHARAKTER

Bedrohungsakteure sind im Grunde genommen Individuen. Sie haben Eigenheiten, die sich oft in ihren Taktiken, Techniken und Verfahren (TTPs) zeigen. Akteure, die Malware-Bedrohungen verbreiten, können anhand der Wahl der Variablennamen oder der Art und Weise, wie sie ihren Code kommentieren, voneinander unterschieden werden. Diese Entscheidungen könnten ihre Interessen, Gewohnheiten und ihren Sinn für Humor widerspiegeln. DNS-Bedrohungsakteure sind nicht anders. Allerdings haben wir im Allgemeinen nur wenige Informationen, mit denen wir in DNS- und Domain-Registrierungsdatensätzen arbeiten können.

Bei Infoblox konzentrieren wir uns auf verdächtige und böswillige DNS-Aktivitäten. Obwohl wir die Ressourcen für Domainnamen einem DNS-Bedrohungsakteur zuordnen, versuchen wir nur selten, seine wahre Identität oder seinen Standort zu ermitteln. Diese Art Zuordnung, bei der Analysten versuchen, Aktivitäten in der virtuellen Welt mit der physischen Welt in Verbindung zu bringen, ist ein Spezialgebiet und zeitaufwendig. Da Prolific Puma jedoch Domains in der usTLD registriert – einer Registry, die keine private Registrierung zulässt – können wir einen Einblick in die Persönlichkeit von Prolific Puma gewinnen.

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

17 https://www.spamhaus.org/

Wenn möglich, verwendet Prolific Puma private Domainregistrierungen, aber usTLD-Registrierungen müssen öffentlich sein. Für diese Domains hat der Akteur durchgehend eine E-Mail-Adresse verwendet, die einen Hinweis auf den Song „October 33" der Black Pumas enthält.[18] Die Black Pumas, eine Psychedelic-Soul-Band aus Austin, Texas, erlangten 2019 mit ihrer Single „Colors" Berühmtheit.[19] Der Song „October 33" erreichte nicht die Top-Charts und umgibt, wie auch „Prolific Puma", ein gewisses Mysterium.[20] Obwohl der Text ganz offensichtlich ein Liebesbrief ist, bezieht er sich auch auf Einsamkeit, und die Musik sollte eine eindringliche Atmosphäre schaffen.[21] Trotz ihrer Grammy-Nominierung als bester neuer Künstler im Jahr 2019 sind die Black Pumas kein Begriff für die Allgemeinheit. Trotz ihrer Grammy-Nominierung als bester neuer Künstler im Jahr 2019 sind die Black Pumas kein geläufiger Name. Der Name Leila stammt aus dem Arabischen und bedeutet „Nacht".

Obwohl wir die Identität von Prolific Puma in der realen Welt nicht kennen, gewinnen wir aus ihren Registrierungsdaten interessante Erkenntnisse über ihre Persönlichkeit. Zusätzlich zu den Hinweisen auf die Black Pumas und ihr mysteriöses Lied „October 33" verwendet Prolific Puma eine persönliche ukrainische E-Mail-Adresse. Die Adresse, die sie angeben, ist eine Grundschule in Polen. Ein unscheinbares Gebäude, das in jeder Industriestadt stehen könnte. Die Stadt Łódź, die drittgrößte Stadt Polens, hat seit der russischen Invasion im Februar 2022 ukrainische Flüchtlinge aufgenommen.[22] Eine Coverversion des Kinks-Songs „Strangers" der Black Pumas wurde in ein emotionales YouTube-Video mit dem Titel „Ukraine Strangers" umgewandelt, in dem ukrainische Flüchtlinge zu sehen sind. Obwohl dieses Video nicht mit den Aktivitäten von Prolific Puma in Zusammenhang steht, erreichte es im Herbst 2022 ein großes Publikum.[23] Wie bereits erwähnt, werden die Informationen des Registrierenden von NameSilo nicht überprüft und erscheinen gefälscht, aber ihre Auswahl gibt einige Erkenntnisse über die Person oder Personen, die Prolific Puma ausmachen.

VORGEHENSWEISE VON PROLIFIC PUMA

Nach der Registrierung einer Domain lässt Prolific Puma diese oft mehrere Wochen lang ungenutzt oder geparkt. Diese Technik wird als „**strategisches Altern" bezeichnet**.[24] Da Phishing-Angriffe traditionell mit neu registrierten Domains in Verbindung stehen, blockieren viele Sicherheitssysteme den Zugriff auf diese. Als Reaktion darauf erkannten die Bedrohungsakteure, dass sie viele Sicherheitsvorkehrungen umgehen können, indem sie mit der Nutzung von Domains in ihren Kampagnen warten oder sie „altern" lassen.

Prolific Puma wird während des Alterungsprozesses eine geringe Anzahl von DNS-Abfragen durchführen, eine Methode, die von Bedrohungsakteuren verwendet wird, um die Reputation der Domainnamen zu verbessern. Während dieser Zeit werden die Domains bei NameSilo geparkt. Prolific Puma überträgt sie dann an Anbieter von geschützten Hosting-Diensten, die mit Bitcoin bezahlt werden, auf einem Virtual Private Server (VPS) mit dedizierter IP-Adresse. Wir haben festgestellt, dass sie Domains nach einiger Zeit aufgeben und der DNS-Eintrag auf die dedizierte IP-Adresse verweist.

Aufgrund der Bandbreite der von uns beobachteten Vorgehensweisen vermuten wir, dass Prolific Puma eine Dienstleistung für andere erbringt und die endgültigen Landing Pages nicht unter ihrer Kontrolle stehen. Es ist jedoch weiterhin möglich,

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

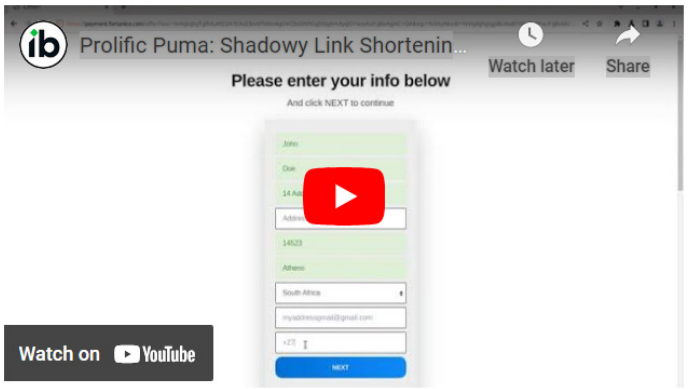
23 https://www.youtube.com/watch?v=D_Ap_7wjHIs

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

dass derselbe Bedrohungsakteur sowohl den Link-Shortening-Service als auch alle über ihn durchgeführten böswilligen Aktivitäten kontrolliert. Wir konnten nicht ermitteln, wie Prolific Puma für seine Dienste wirbt, wie seine Benutzer die gekürzte URL erhalten oder ob es legitimen Datenverkehr gibt. Im Rahmen der Kampagnen über den Prolific Puma-Dienst haben wir große Netzwerke von Domains gefunden, die von anderen DNS-Bedrohungsakteuren kontrolliert werden und oft bei billigen Registraren wie NameCheap registriert sind. Einige dieser Kampagnen-Domains werden auch von RDGAs generiert.

EINE BEISPIELKAMPAGNE

Prolific Puma betreibt einen Link-Shortener für eine Vielzahl von Phishing-, Betrugs- und Malware-Aktivitäten. Im Folgenden beschreiben wir ein Beispiel für eine der Kampagnen, die er bedient. Die Abbildungen 5.1-5.4 zeigen Screenshots dessen, was ein Opfer nach dem Klicken auf den ursprünglichen gekürzten Link, `http://bwkd[.]me/ZFjfA3`, zu sehen bekommt. Der Link führt zu einer Phishing-Seite, die wie eine E-Mail aussieht und den Benutzer auffordert, persönliche Daten anzugeben und eine Zahlung zu leisten. Anschließend wird der Benutzer mit einer Browser-Plug-in-Malware infiziert. Wir haben auch einen Screenshot des Vorgangs erstellt, der unten zu sehen ist.



Die technischen Schritte zwischen dem gekürzten Link und der Browser-Plug-in-Malware in dieser Kampagne sind wie folgt:

- Der erste gekürzte Link `http://bwkd[.]me/ZFjfA3` leitet weiter zu
- `http://ksaguna[.]com/click.php?key=<redacted>`, der wiederum weiterleitet auf
- `https://www[.]asdboloa[.]com/ZA/AB_zagopb/?uclick=<redacted>`
  - » Diese letzte Website ist eine gefälschte Gmail-Nachricht, die dem Benutzer mitteilt, dass er die Möglichkeit gewonnen hat, das neue iPhone 15 zu testen.
- Der Benutzer wird angewiesen, auf einen Link zu klicken, um sein Handy unter `https://www[.]game[.]co[.]za/2023program` anzufordern, und seine Lieferinformationen einzugeben. Die Website `www[.]game[.]co[.]za` ist ein südafrikanischer Discounter, der mit Werbeaktionen Verbraucher anlockt.
- Wenn Sie diesem Link unter den richtigen Bedingungen folgen, werden Sie aufgefordert, 18 südafrikanische Rand (ZAR) zu zahlen, um an der Studie teilzunehmen.
- Von dort aus wird dem Benutzer eine Seite angezeigt, die vorgibt, eine Sendungsverfolgung zu sein, und ihn auffordert, Benachrichtigungen von `fubsdgd[.]com` zu akzeptieren. Durch Klicken auf „Akzeptieren“ wird die Installation von Browser-Malware ausgelöst, die den OneSignal-Dienst für Push-Benachrichtigungen verwendet. Obwohl Browser-Plug-in-Malware häufig mit Werbung in Verbindung gebracht wird, wird sie unserer Erfahrung nach neben Werbung auch häufig für Betrug, Phishing und andere Malware verwendet.
- Schließlich wird das Opfer durch eine Reihe von Prompts geführt, in denen es aufgefordert wird, seine Versandpräferenzen zu bestätigen und seine persönlichen Daten einzugeben.

Wir wissen nicht, wie die ursprüngliche gekürzte URL an das Opfer übermittelt wird. Möglicherweise wird eine SMS-Textnachricht verwendet, da sie eine gefälschte Gmail-Nachricht öffnet. Die Domains, die während der Ausnutzung des Opfers verwendet werden, ändern sich und sind selbst Teil eines großen Netzwerks. Diese Kampagne verwendet eine Vielzahl von Techniken, um dem Opfer zu versichern, dass das Angebot echt ist, einschließlich eines aktiven Stroms von Erfahrungsberichten anderer „Empfänger“ bei jedem Schritt.

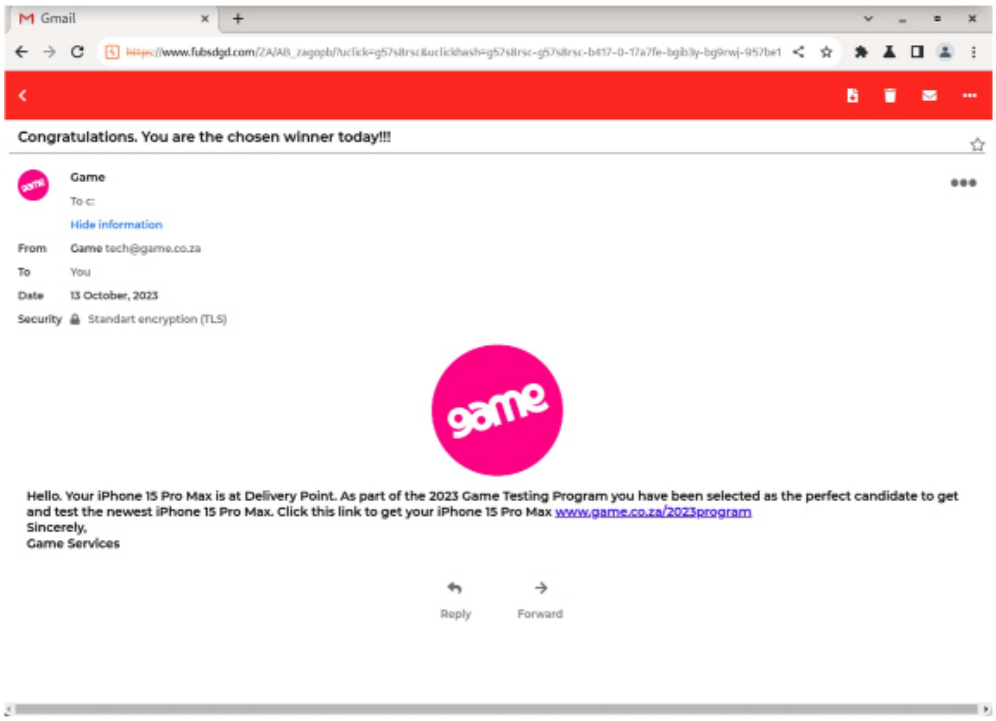


Abbildung 5.1: Ein Beispiel für den Inhalt, der von Prolific Puma Link-Shortenern bereitgestellt wird. Der ursprüngliche gekürzte Link (http://bwkd[.]me/ZFjfA3) leitete um und führte schließlich zu einer Phishing-Seite, die wie eine E-Mail von Gmail aussah.

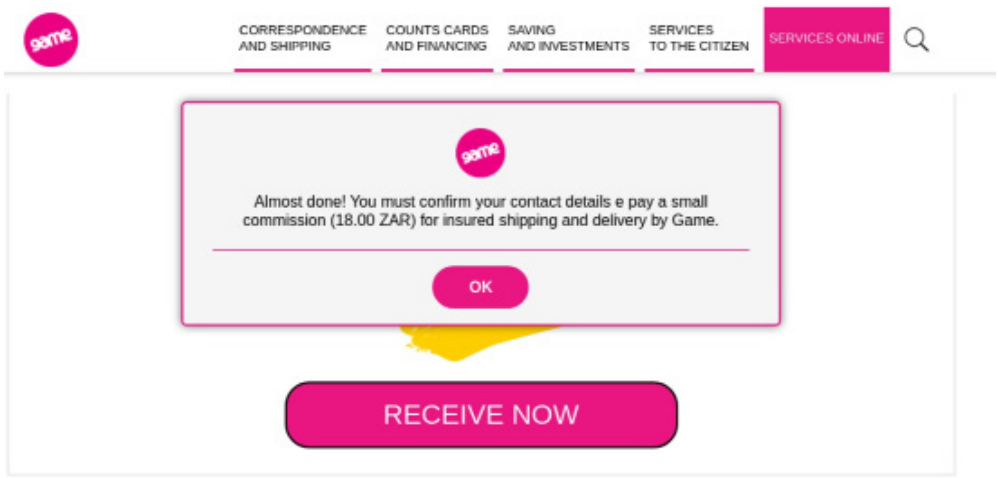


Abbildung 5.2.: Der Teil der Kampagne, der sich mit Betrug und Identitätsdiebstahl befasst. Nachdem der Benutzer sich dafür entschieden hat, das kostenlose iPhone anzunehmen (siehe Abbildung 5.1), wird er aufgefordert, eine Gebühr zu zahlen und seinen Namen und seine Adresse anzugeben.

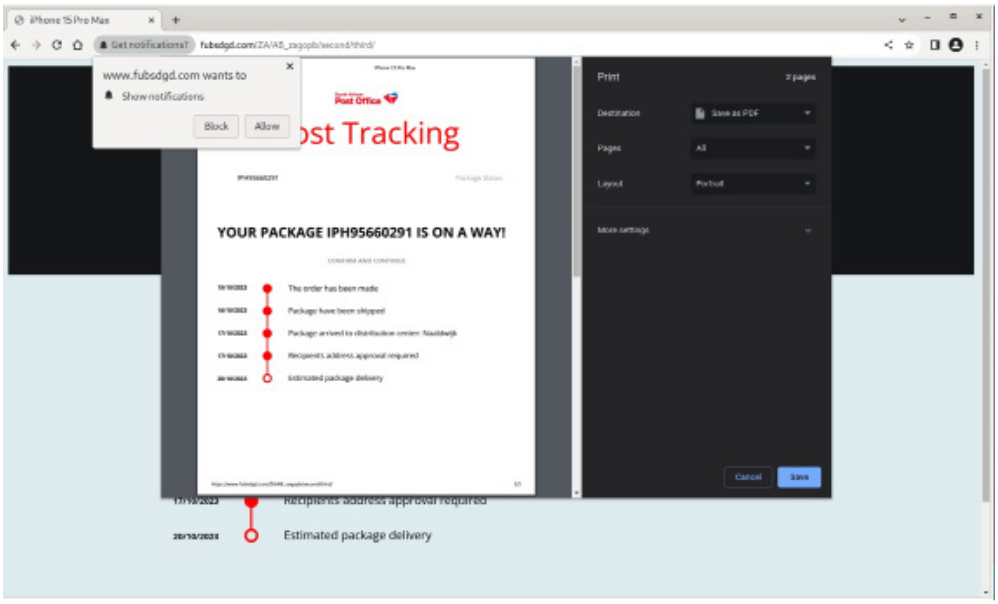


Abbildung 5.3.: Der Malware-Teil der Kampagne. Nachdem das Opfer die in Abbildung 5.2 dargestellte Gebühr bezahlt hat, erhält es eine Benachrichtigung über die Paketzustellung und wird aufgefordert, Benachrichtigungen von fubsdgd[.] com vorzuzeigen. Wenn sie Benachrichtigungen akzeptieren, wird Malware auf den Computer des Opfers übertragen.

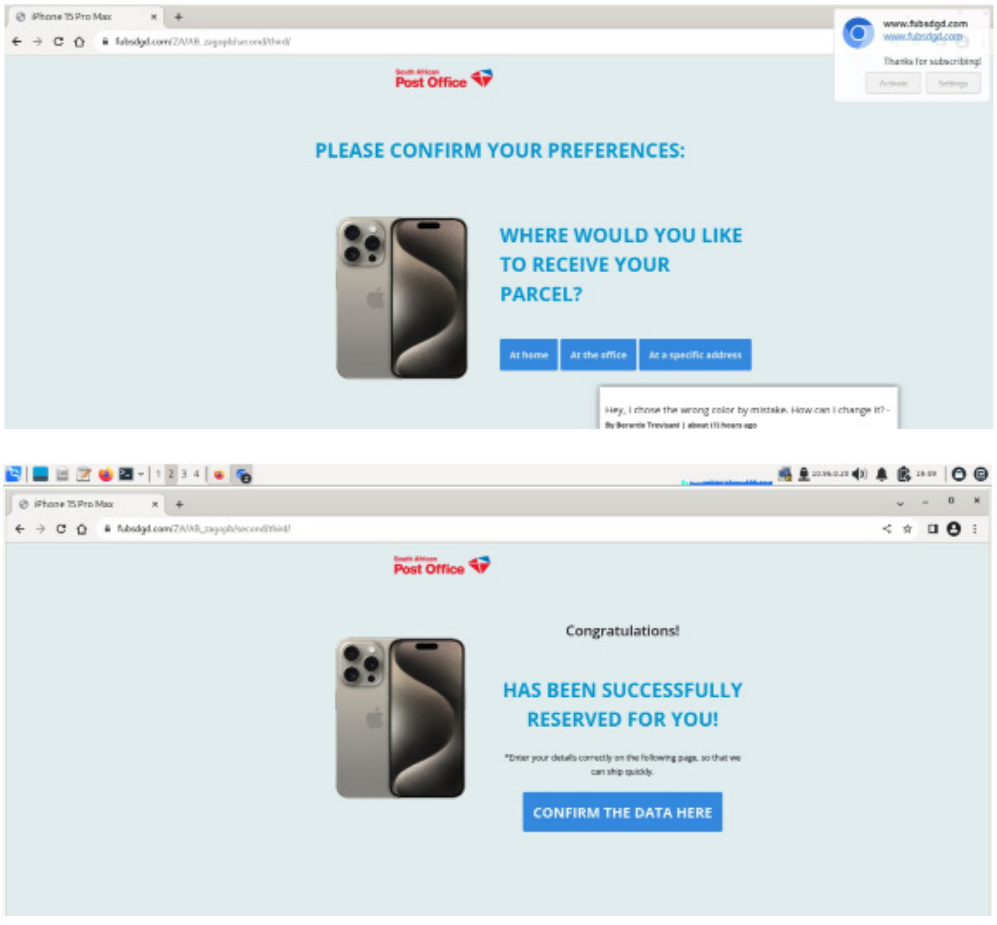


Abbildung 5.4a-b.: Nach der Annahme der in Abbildung 5.3 dargestellten Benachrichtigungen wird der Benutzer in einer Reihe von Bildschirmen zur Eingabe weiterer Details und Präferenzen aufgefordert.

ZUSAMMENFASSUNG

Prolific Puma zeigt, wie das DNS missbraucht werden kann, um kriminelle Aktivitäten zu unterstützen und jahrelang unentdeckt zu bleiben. Als Teil der Lieferkette ist dieser Akteur schwerer zu erkennen und zu bekämpfen. Herkömmliche Sicherheitssysteme schützen den Benutzer vor Schäden, die auf der letzten Zielseite eines Links basieren. DNS-Erkennungs- und Reaktionssysteme können jedoch Prolific Puma und ähnliche Dienstanbieter stören und so alle Akteure behindern, die sich auf sie verlassen, um Phishing, Betrug und Malware zu verbreiten. Durch die Verwendung eines RDGA und billiger Domain-Registrare ist Prolific Puma in der Lage, seine Aktivitäten zu skalieren und fortzusetzen. Gleichzeitig können wir jedoch die Verwendung eines RDGA über DNS und Domain-Registrierungsdatensätze erkennen.

Prolific Puma ist nur einer der von Infoblox entdeckten Link-Shortener-Betreiber, und Link-Shortener sind nur ein Typ von Dienstleistungen, die in der Schattenwirtschaft zu finden sind. **Meistens decken wir DNS-Bedrohungsakteure zuerst durch Analysen auf, die verdächtige neu registrierte, konfigurierte oder abgefragte Domains identifizieren**. Noch bevor wir Domains mit böswilligen Aktivitäten in Verbindung bringen, können wir andere Funktionen wie die TLD- und Nameserver-Reputation nutzen, um die zugehörigen Domains als verdächtig zu kennzeichnen. Später sind wir in der Lage, Domains miteinander zu verbinden und einen Bedrohungsakteur zu isolieren. Durch die Sperrung des Zugriffs auf verdächtige Domains können Unternehmen eine hochwirksame, sichere Richtlinie mit geringem Aufwand für ihr Netzwerk und ihre Benutzer implementieren.

AKTIVITÄTSINDIKATOREN

Nachfolgend finden Sie eine kleine Auswahl von Indikatoren im Zusammenhang mit Prolific Puma und den von ihnen unterstützten Kampagnen. Eine umfassendere Liste der aktuellen Indikatoren finden Sie in unserem offenen GitHub-Repository hier.

Aktivitätsindikator	Art des Indikators
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	

Aktivitätsindikator	Art des Indikators
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	

Aktivitätsindikator	Art des Indikators
ymql[.]link 7tz[.]us w6q[.]us giqj[.]me u3q[.]us ke0[.]us v1u[.]us ti7[.]uns 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

Aktivitätsindikator	Art des Indikators
bwkd[.]me ksaguna[.]com asdboloa[.]com game.co[.]za	Weiterleitung und Landingpages
fubsdgd[.]com	Browser-Plugin-Malware-Domains
blackpumaoct33@ukr[.]net	Prolific Puma Registrierungs-E-Mail-Adresse

INFOBLOX THREAT INTEL

Infoblox Threat Intel ist der führende Anbieter von Original-DNS-Bedrohungsdaten und hebt sich von der Masse der Aggregatoren ab. Was zeichnet uns aus? Zwei Dinge: verrückte DNS-Kenntnisse und beispiellose Sichtbarkeit. DNS ist bekanntermaßen schwierig zu interpretieren und zu „jagen“, aber unser tiefes Verständnis und unser einzigartiger Zugang ermöglichen es uns, Cyberbedrohungen aufzuspüren. Wir sind proaktiv, nicht nur defensiv, und nutzen unsere Erkenntnisse, um Cyberkriminalität dort zu unterbinden, wo sie entsteht. Wir glauben auch an den Wissensaustausch, um die breitere Sicherheits-Community zu unterstützen, indem wir detaillierte Forschungsergebnisse und Indikatoren auf GitHub veröffentlichen. Darüber hinaus sind unsere Informationen nahtlos in unsere Infoblox DNS Detection and Response-Lösungen integriert, sodass Kunden automatisch von den Vorteilen profitieren und von extrem niedrigen Falsch-Positiv-Raten profitieren.

Firmenhauptsitz
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054, USA

+1.408.986.4000
www.infoblox.com

Version: 20241008v1