



# L00k alike Domains

## Eine unsichtbare Bedrohung

Steffen Eid  
Solution Architect Manager Central Europe



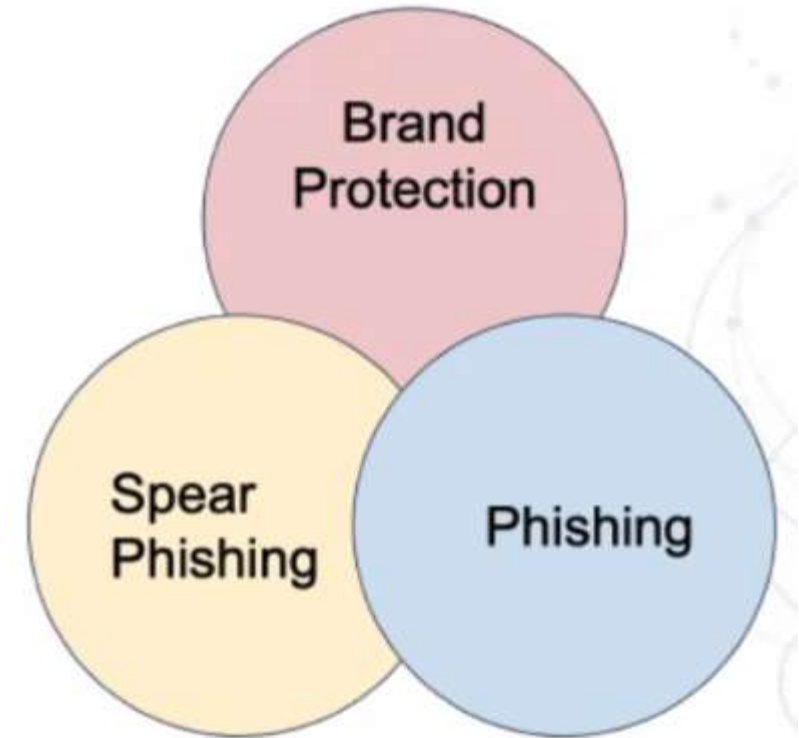
# Why care about Lookalike Domains?

---

About risks, about reputation loss, about serious trouble...

# Use Cases: Brand Reputation, Phishing / Spear Phishing

- **Brand Protection:** Protecting customer's own domain from harm via impersonation (Example: using infoblocks.com to harm our customers). Alerts on creation or discovery of domain.
- **Spear Phishing:** User visiting lookalike of company's own domain (Example: user visits Infobloxbenefits[.]com) Alerts when domain is visited.
- **Phishing:** Local users visiting global lookalikes (Example: user going to g00gle.com) Alerts when domain is visited.



# The Story of PayPal.com

- No, not PAYPAL, PAYPAI
- Uses fonts to disguise
- Uppercase i ↔ l

Notification - Account Review

**PayPal**

*This email will be brief. We would appreciate your prompt attention to this matter.*

PayPal is constantly working to ensure security by regularly screening the accounts in our system. We recently reviewed your account and made adjustments resulting in the following changes.

Unfortunately, access to your account has been limited.

Use the following link to restore your account access:

[https://www.paypal.co.uk/cgi-bin/restore\\_account\\_access](https://www.paypal.co.uk/cgi-bin/restore_account_access)

**(Your case ID for this reason is PP-218-581-792.)**

Should access to your account remain limited for an extended period of time, it may result in further limitations on the use of your account or may result in eventual account closure.

Sincerely,  
PayPaI Account Review Team

# Charakterisierung von lookalike Domains

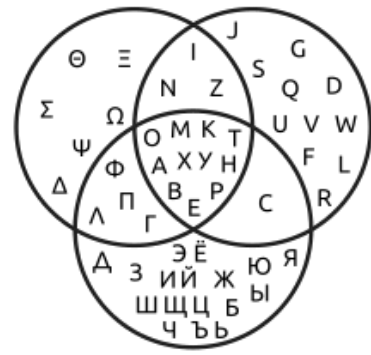
Type	Description	Example
<b>Lexical / Combo</b>	Changing domain to appear like target. <b>Low sophistication</b> . Used to confuse users to believe they are interacting with target.	amazon-accountspayable[.]com
<b>Homograph / Homoglyph</b>	Swapping characters to impersonate target. <b>More sophisticated</b> . Designed to completely impersonate target. Frequently used for targeted attack or Phishing.	Aliexpress[.]com
<b>Typo-Squat</b>	Select common misspellings of words to take advantage of mistakes. <b>More sophisticated</b> , but often used for “drive by” attacks. Generalized attacks, <b>collects “low hanging fruit”</b> .	Hoogle[.]com
<b>Prefix</b>	Target domain is added as a prefix hostname in another domain. There are many legitimate uses for this, but some malicious actors can still use this technique	facebook.baddomain[.]com

# Charakterisierung von lookalike Domains

Type	Description	Example
Combo Squat Sounds Squat TLD-Squat	Form of lookalike that combines popular brand or company names with other keywords. Terms like support, help, security, and mail are common.	wordpress- <b>security</b> [.] cloud infoblox <b>grid</b> [.]com
Combo Squat Sounds Squat TLD-Squat	Soundsquat domains leverage the use of homophones, words that sound the same but have a different spelling. Soundsquatting has gained more attention from researchers recently due to the proliferation of smart speakers á la <b>Alexa, Siri, and Google Voice</b>	youtube.com: <b>yew</b> tube.com, <b>ewetube</b> .com, <b>utube</b> .com worldfreeforu.com: worldfree <b>4u</b> .com
TLD-Squat	Select common misspellings of words to take advantage of mistakes. <b>More sophisticated</b> , but often used for “drive by” attacks. Generalized attacks, <b>collects</b> “low hanging fruit”.	calendar: calender accommodate: acommodate, accomodate homonyms: (‘piece’ vs. ‘peace’) (America’s ‘color’ vs. Britain’s ‘colour’)



# Lookalike Domain Detection



- Internationalized Domain Name (IDN) - homograph attack  
Arabic, Chinese, Cyrillic, Devanagari, Greek, Hebrew or the Latin alphabet-based characters. German äöü
- Cyrillic letters **a, c, e, o, p, x** and **y** have optical counterparts in the basic Latin alphabet and look close or identical to a, c, e, o, p, x and y.
- Alphabet change, used in homograph attacks like Beta Bot Trojan:  
adobe[.]com                      [http://xn--adoe-x34a\[.\]com/](http://xn--adoe-x34a[.]com/)

medium.com	mediurn.com	m - rn
walmart.com	wa1mart.com	l - 1
apple.com	apple.com	Cyrillic
ikea.com	iķea.com	Cyrillic
AEZ.DE	ÆEZ.DE	Greek

# Lookalike Domain Detection

---

paypal.com

paypał.com

paypal.com

Text

xn--pypl-53dc.com

xn--pypl-btac.com

paypal.com

Punycode

google.com

google.com

google.com

Text

google.com

xn--ggle-0nda.com

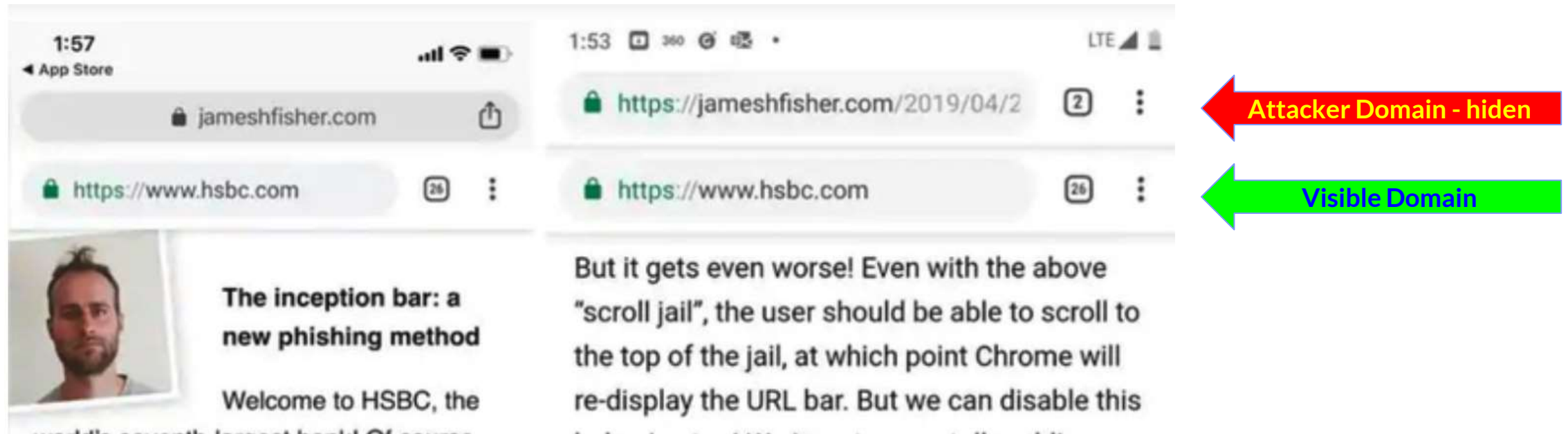
xn--ggle-55da.com

Punycode



# Hide the Name: Inception Bar

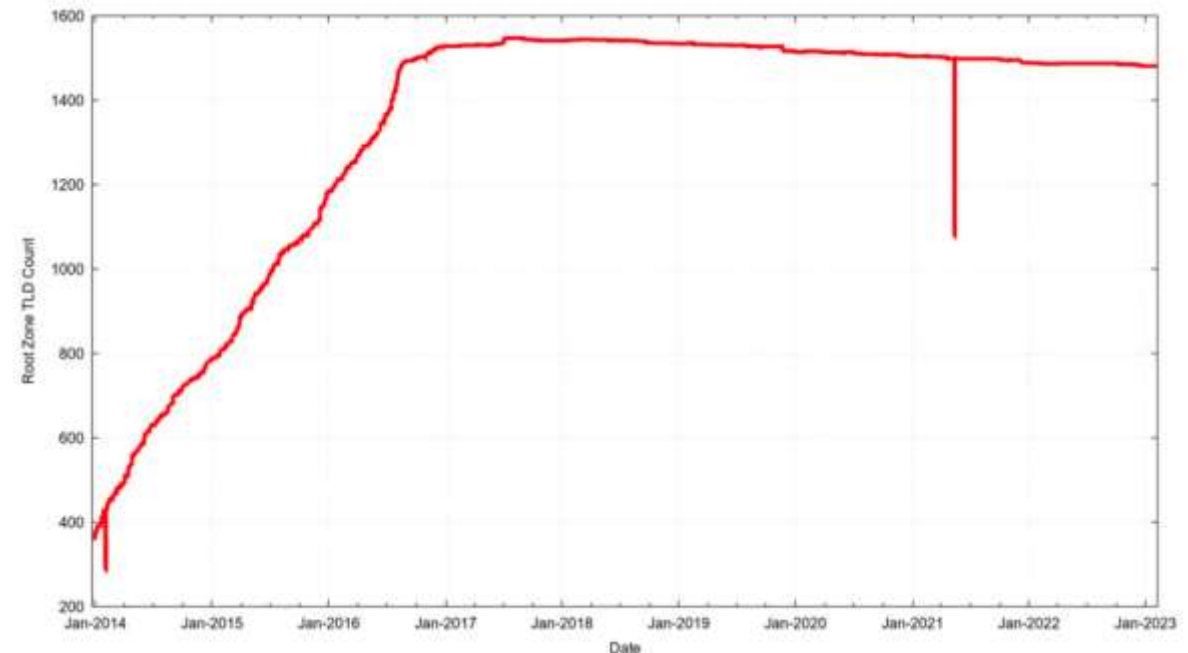
- Attacker takes screenshot of legitimate domain
- Use screenshot near the top of the web page
- Use web browser flaw to hide real URL bar
- Even if users scrolled up, they cannot see the real URL



# Wieviele lookalike Domains kann es geben?

- 136.000 verfügbare Unicode Buchstaben (IDN = International Domain Names)
- 829+ Millionen Optionen für „Infoblox“
- 1.591 TLDs in der DNS Root Zone (Juni 23)
- ?? Möglichkeiten für Typo-Squad, Lexical und Prefix

**Registrieren aller möglichen Domains ist keine Option**



Anzahl der Top Level Domains:  
<https://blog.apnic.net/2023/02/08/the-root-of-the-dns-revisited/>

# Lookalike Domain Detection

infoblox

Dashboard

Manage

Policies

Reports

DHCP Reports

DNS Reports

DNS Activity

Security Activity

Summary Reports

Application Disco...

Web Content Dis...

Lookalike Domains

Scheduled Events

Research

Administration

Activity

Custom Watched Domains

Common Watched Domains

Muted Lookalikes

Lookalike Domains

Lookalike domains are domains that appear to be using aspects of other trusted domains for the purpose of associating themselves with those domains. Frequently, this association is used in attacks to make users believe they are interacting with a trusted source. Not all lookalikes are malicious, but once a lookalike is discovered it is investigated to determine if there are any suspicious or malicious behaviors associated with them.

Last 7 days

15K

22.3%

Total Lookalikes

3.9K

33.3%

Total Lookalikes from Custom Watched Domains

17

88.9%

Threats from Custom Watched Domains

Export

Select All

Unselect All

Sort by Watched Domain

Type Show All

Show Last 30 days

Search

Threat Classes

70,000

60,000

50,000

40,000

30,000

20,000

10,000

0

Suspicious

Phishing

Malware C2

Others

\*One lookalike can be in multiple Threat Classes

accuweather.com

Common Watched Domain

Lookalikes: 37

Threat lookalikes: 3 (Phishing, Suspicious)

Content Category: International News, Weather

Registration Date: Oct 27 1995

adobe.com

Common Watched Domain

Lookalikes: 1073

Threat lookalikes: 90 (Phishing, Suspicious)

Content Category: Graphics Software

Registration Date: N/A

Custom Watched Domains

You can add up to 10 custom watched domains.

Create

Import

Edit

Remove

DOMAIN

almond.eu

durex.com

Common Watched Domains

Infoblox is tracking over 100 of the common domains used.

Enable

Disable

DOMAIN

accuweather.com

active.aero

adobe.com

WATCHED

On

Off

On

# Searching for IDN homographs in Infoblox

[https://csp.infoblox.com/tide/api/data/threats/host/daily?target=starbucks.com&data\\_format=tsv&field=detected,host&rlimit=20&property=Policy\\_LookalikeDomains](https://csp.infoblox.com/tide/api/data/threats/host/daily?target=starbucks.com&data_format=tsv&field=detected,host&rlimit=20&property=Policy_LookalikeDomains)

2022-06-26T07:28:33.398Z	starbuckscoffee.homeserver.com
2022-06-26T07:28:41.884Z	starbucks-nz.demo-application.net
2022-06-26T07:28:53.602Z	starbucksthirdplace.com
2022-06-26T07:28:38.330Z	starbucksplaces.com
2022-06-26T07:28:47.485Z	starbucksdelivery.com
2022-06-26T07:28:33.398Z	customstarbucks.com



# Suspicious\_Lookalike

infoblox

Dashboard

Manage

Policies

Reports

Research

Dossier

Active Indicators

Resources

Threat Lab

Administration

Infoblox SE EM...

Stephan Fritsche

User Agreee...

Help

Recycle Bin

Host

IP

URL

Threat Class/Property

Select all

APT

(23,777,749)

Bot

(139,410)

CompromisedDomain

(227,940)

CompromisedHost

Cryptocurrency

DNSTunnel

(8,622)

ExploitKit

(5)

ICS

(2)

IllegalContent

(1,271)

InternetInfrastructure

(2,011)

MaliciousNameserver

(3)

MalwareC2

(983)

MalwareC2DGA

(1)

MalwareDownload

(122)

Parked

(65,361)

Phishing

(6,239,541)

Policy

(5,089)

Proxy

(274)

Scanner

(681)

Sinkhole

(712,179)

Suspicious

(6,102,609)

Suspicious\_Behavior

(2,352)

Suspicious\_DGA

(25,915)

Suspicious\_EmergentDomain

(5,039,758)

Suspicious\_Generic

(494,693)

Suspicious\_Lookalike

(140,663)

Clear

(4)

Apply Filter

Export

Generate API Request

Search...

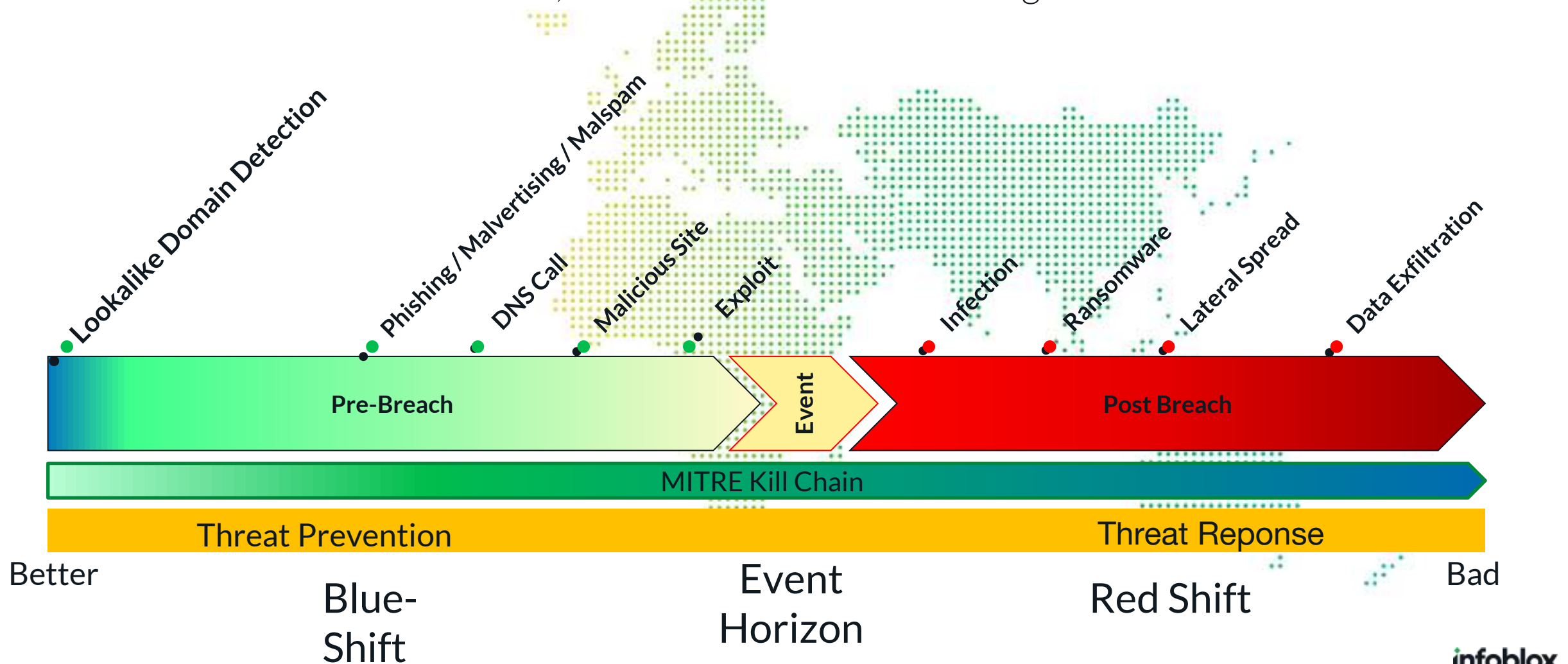
INDICATOR	DATA TYPE	THREAT CLASS	THREAT PROPERTY	DETECTED	DATA PROVIDER	THREAT
winserverupdates.com	HOST	UncategorizedThreat	UncategorizedThreat_Generic	2023-05-15T20:39:30.000Z	AISCOMM	80
compromiseddomain.eicar.network	HOST	CompromisedDomain	CompromisedDomain_Generic	2017-07-24T17:24:54.704Z	AISCOMM	75
sinkhole.eicar.network	HOST	Sinkhole	Sinkhole_Generic	2017-07-24T17:27:39.423Z	AISCOMM	100
windowsservicecenter.com	HOST	UncategorizedThreat	UncategorizedThreat_Generic	2023-05-15T20:39:30.000Z	AISCOMM	80
upd488.windowsservicecenter.com	HOST	UncategorizedThreat	UncategorizedThreat_Generic	2023-05-15T20:39:30.000Z	AISCOMM	80
malwarec2.eicar.network	HOST	MalwareC2	MalwareC2_Generic	2017-07-24T17:22:09.348Z	AISCOMM	100
apt.eicar.network	HOST	APT	APT_Generic	2017-07-24T17:24:26.654Z	AISCOMM	100
maliciousnameserver.eicar.network	HOST	MaliciousNameserver	MaliciousNameserver_Generic	2017-07-24T17:27:11.225Z	AISCOMM	100
ber6vjyb.com	HOST	UncategorizedThreat	UncategorizedThreat_Generic	2023-05-15T20:39:30.000Z	AISCOMM	80
windowcsupdates.com	HOST	UncategorizedThreat	UncategorizedThreat_Generic	2023-05-15T20:39:30.000Z	AISCOMM	80

Page: 1 2 ... 81

infoblox

# Methodology: What part of the kill chain is detected?

The earlier a threat is discovered, the better the chance to mitigate it!





# Use Infoblox Suspicious Domain Feed to protect against MFA Lookalike Domains

Since January 2022: over 1600 domains were registered as lookalikes to MFA domains

Since early November 2022, Infoblox has detected 75% of the MFA lookalike domains registered with these characteristics as suspicious



## You are protected against MFA Lookalike with Infoblox Suspicious Domain feeds in blocking mode

<https://blogs.infoblox.com/security/recent-sms-phishing-attacks-reveal-the-dangers-of-mfa-lookalike-domains/#:~:text=Infoblox%20identifies%20attacks%20related%20to%20MFA%20lookalike%20domains&text=In%20total%2C%20since%20January%202022,possibly%20related%20to%20phishing%20attacks.>



# Recent SMS Phishing Attacks Reveal the Dangers of MFA Lookalike Domains

- From January 2022 to February 2023, **over 1600 domains** were registered as **lookalikes to MFA** (Multi-factor authentication) domains.
- The team detected MFA lookalikes for major services such as Dropbox, Paypal, Microsoft, Okta, Netflix, Amazon, Tripadvisor, and YouTube, in addition to those reported in the media.
- Since November 2022, Infoblox has detected 75% of the MFA lookalike domains registered with these characteristics as suspicious.
- July 2023 116,520 Suspicious\_Lookalike domains in blocklist



Report:  
[https://blogs.infoblox.com/security/recent-sms-phishing-attacks-reveal-the-dangers-of-mfa-lookalike-](https://blogs.infoblox.com/security/recent-sms-phishing-attacks-reveal-the-dangers-of-mfa-lookalike-domains/#:~:text=Infoblox%20identifies%20Attacks%20Related%20to%20MFA%20Lookalike%20Domains&text=In%20total%2C%20si)

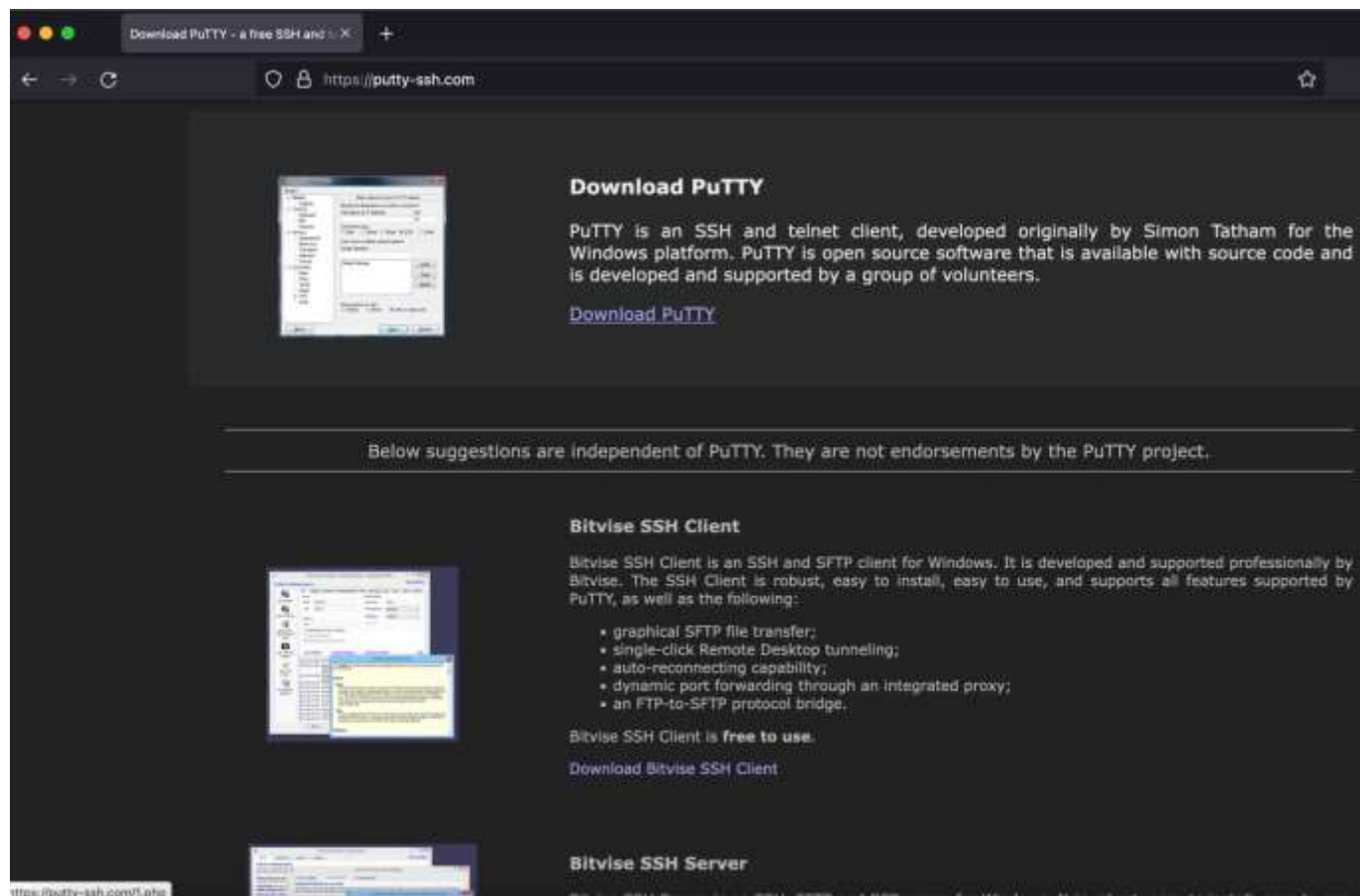
[domains/#:~:text=Infoblox%20identifies%20Attacks%20Related%20to%20MFA%20Lookalike%20Domains&text=In%20total%2C%20si](https://blogs.infoblox.com/security/recent-sms-phishing-attacks-reveal-the-dangers-of-mfa-lookalike-domains/#:~:text=Infoblox%20identifies%20Attacks%20Related%20to%20MFA%20Lookalike%20Domains&text=In%20total%2C%20si)  
[nce%20January%202022,possibly%20related%20to%20phishing%20attacks.](https://blogs.infoblox.com/security/recent-sms-phishing-attacks-reveal-the-dangers-of-mfa-lookalike-domains/#:~:text=Infoblox%20identifies%20Attacks%20Related%20to%20MFA%20Lookalike%20Domains&text=In%20total%2C%20si)

# Still using Putty?

---

A recent Malware example

# Putty SSH Client



## Download PuTTY: latest release (0.79)

[Home](#) | [FAQ](#) | [Feedback](#) | [Licence](#) | [Updates](#) | [Mirrors](#) | [Keys](#) | [Links](#) | [Team](#)

Download: [Stable](#) - [Snapshot](#) | [Docs](#) | [Changes](#) | [Wishlist](#)

This page contains download links for the latest released version of PuTTY. Currently this is 0.79, released on 2023-08-26.

When new releases come out, this page will update to contain the latest, so this is a good page to bookmark or link to. Alternatively, here is a [permanent link to the 0.79 release](#).

Release versions of PuTTY are versions we think are reasonably likely to work well. However, they are often not the most up-to-date version of the code available. If you have a problem with this release, then it might be worth trying out the [development snapshots](#), to see if the problem has already been fixed in those versions.

## Package files

You probably want one of these. They include versions of all the PuTTY utilities (except the new and slightly experimental Windows pterm).

(Not sure whether you want the 32-bit or the 64-bit version? Read the [FAQ entry](#).)

We also publish the latest PuTTY installers for all Windows architectures as a free-of-charge download at the [Microsoft Store](#); they usually take a few days to appear there after we release them.

### MSI ('Windows Installer')

64-bit x86:	<a href="#">putty-64bit-0.79-installer.msi</a>	<a href="#">(signature)</a>
64-bit Arm:	<a href="#">putty-arm64-0.79-installer.msi</a>	<a href="#">(signature)</a>
32-bit x86:	<a href="#">putty-0.79-installer.msi</a>	<a href="#">(signature)</a>

IOCs:

putty-ssh[.]com (#malware download)

puttysshhub[.]club (redirector)

sshwithputty[.]info (redirector)

puttyseuressh[.]cloud (redirector)

puttysshtools[.]xyz (redirector)

# Infoblox Dossier info

Dossier™ Threat Research Port...

Enter a domain, IP Address, Hostname, Email, URL, or Hash value...

Search

Resources

putty-ssh.com

Like Active Threat Domains (MIT) 1/2023 (Active)

Add to Custom List

Generate API Request

Feedback on Results

Export

Summary

More Details

Impacted Devices

Current DNS

Related Domains

Related URLs

Related IPs

Related File Samples

Related Contacts

Metadata

Timeline


Threat Actor

MITRE ATT&CK™

WHOIS Record

Raw Whois

Domain Screen Image



Full Image

8

DNS Record Count

2

Domain/Subdomain Count

1

URL Count

25

IP Count

Categorizations

Infoblox Threat Property	MalwareDownload_Generic
Infoblox Threat Property	Policy_LookalikeDomains
Infoblox Web Category	Image Search/Search Engines
Infoblox Nameserver Repu...	Moderate Risk (5)
Infoblox TLD Score	Moderate Risk (6)
Forcepoint ThreatSeeker	information technology

Lookalike Detection

⚠️

This domain putty-ssh.com may be trying to impersonate putty.org based on a detected host of putty-ssh.com.  
[View your Lookalike Report](#)

Infoblox Threat Level

Threat Level is designed to help users understand how dangerous an indicator can be, since not all malware behave the same way. The information can be used in combination with other scores from Infoblox.

3.5

/10

Low

Infoblox Risk Level

The Risk score represents the likelihood that a user will be exposed to a threat or compromised by interacting with the indicator.

4.9

/10

Medium

Infoblox Confidence Level

The Confidence Score provides additional insight into the indicator class and property. It represents our level of trust in the classification and threat of the indicator.

High

Infoblox Threat Intelligence Group Research Notes

◆

Domain is a lookalike to putty.org. The creation date is 2023-08-23.

Active Threat Feeds and Status

Info	Low	Medium	High
Infoblox Anti(Malware			●
2000512.bstafford-custom-feed.ft			●
2000512.sofia.ft			●



# Domain Takedown Service

---

Brand protection and much more....

# What we do

---

## VALIDATION

Comprehensive in-depth analysis of suspected fraud submitted by our clients. We will review and report our observations, if necessary, requesting additional information.

## MITIGATION

Expedient trust-based remediation of internet fraud by leveraging years of experience in abuse desk best practices.

## REPORTING

Communicate patterns to improve awareness and increase understanding of threat landscape.

## MONITORING

Constant monitoring of all reported content for specific periods of time. Any reactivations of the original content will be deactivated by us for free. All non-threat content will be monitored to determine if it will evolve into a threat.

# Mitigation progress

## CASE TIMELINE (EFFORT / TIME)



If we detect a reactivation within 30 days, we will immediately pursue the reactivation at no additional cost.



