Jun 14 2023

NETMANAGEIT

Intelligence Report

Brand Impersonation Campaign Targeting Big Brands

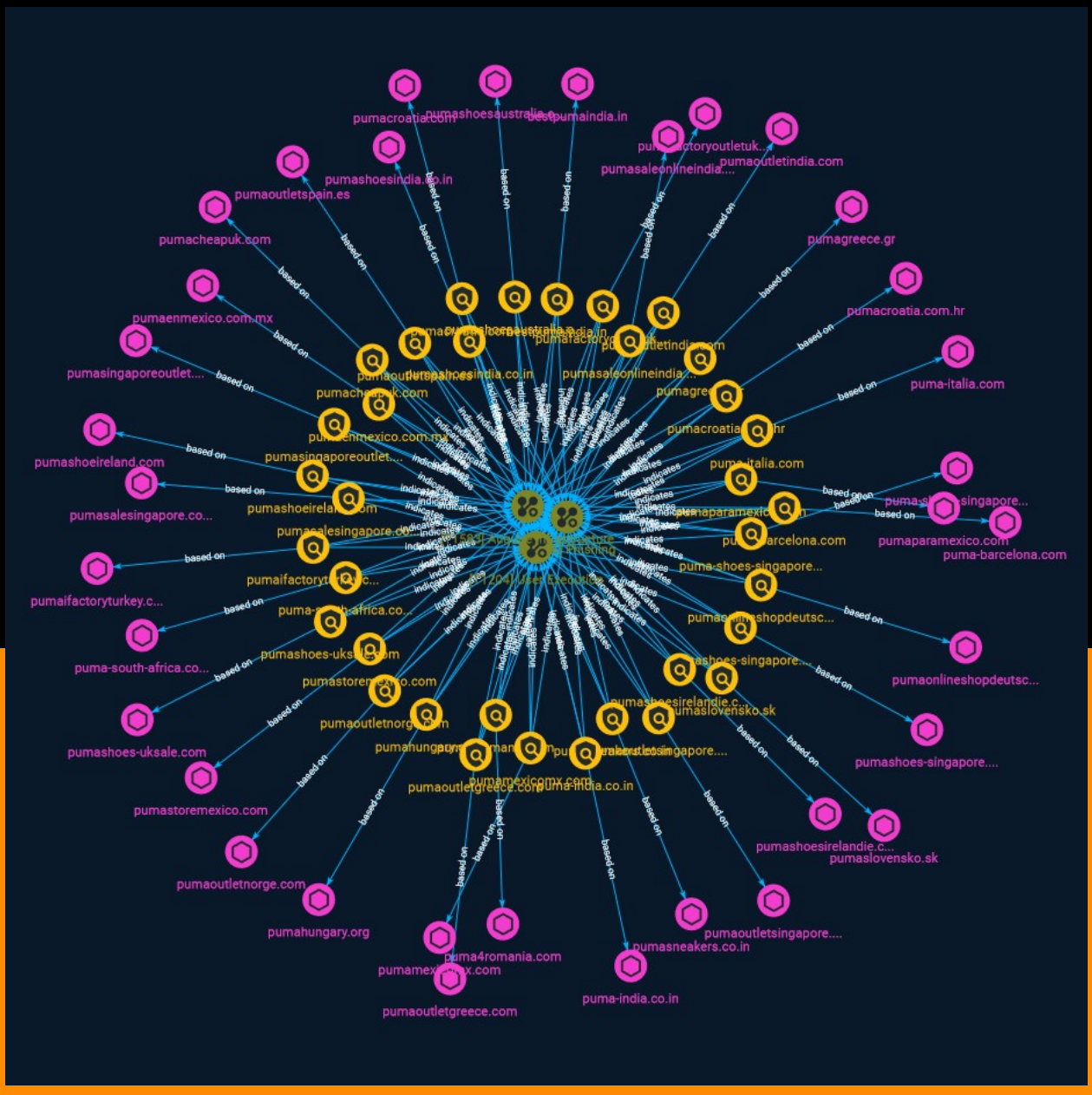

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Bolster has uncovered a widespread scam campaign targeting 100+ popular clothing, footwear and apparel brands, with over 3,000 sites identified as being part of an extensive network of brand impersonation websites.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

15 / 100

Attack-Pattern

Name
Phishing
ID
T1566
Description
Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name

User Execution

ID

T1204

Description

An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behavior from forms of [Phishing](https://attack.mitre.org/techniques/T1566). While [User Execution](https://attack.mitre.org/techniques/T1204) frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after [Internal Spearphishing](https://attack.mitre.org/techniques/T1534). Adversaries may also deceive users into performing actions such as enabling [Remote Access Software](https://attack.mitre.org/techniques/T1219), allowing direct control of the system to the adversary, or downloading and executing malware for [User Execution](https://attack.mitre.org/techniques/T1204). For example, tech support scams can be facilitated through [Phishing](https://attack.mitre.org/techniques/T1566), vishing, or various forms of user interaction. Adversaries can use a combination of these methods, such as spoofing and promoting toll-free numbers or call centers that are used to direct victims to malicious websites, to deliver and execute payloads containing malware or [Remote Access Software](https://attack.mitre.org/techniques/T1219).(Citation: Telephone Attack Delivery)

Name

Acquire Infrastructure

ID

T1583

Description

Adversaries may buy, lease, or rent infrastructure that can be used during targeting. A wide variety of infrastructure exists for hosting and orchestrating adversary operations. Infrastructure solutions include physical or cloud servers, domains, and third-party web services.(Citation: TrendmicroHideoutsLease) Additionally, botnets are available for rent or purchase. Use of these infrastructure solutions allows adversaries to stage, launch, and execute operations. Solutions may help adversary operations blend in with traffic that is seen as normal, such as contacting third-party web services or acquiring infrastructure to support [Proxy](https://attack.mitre.org/techniques/T1090).(Citation: amnesty_nso_pegasus) Depending on the implementation, adversaries may use infrastructure that makes it difficult to physically tie back to them as well as utilize infrastructure that can be rapidly provisioned, modified, and shut down.

Indicator

Name
pumashoes-singapore.com
Pattern Type
stix
Pattern
[domain-name:value = 'pumashoes-singapore.com']
Name
pumashoeireland.com
Pattern Type
stix
Pattern
[domain-name:value = 'pumashoeireland.com']
Name
pumagreece.gr

Pattern Type
stix
Pattern
[domain-name:value = 'pumagreece.gr']
Name
puma4romania.com
Pattern Type
stix
Pattern
[domain-name:value = 'puma4romania.com']
Name
pumaenmexico.com.mx
Pattern Type
stix
Pattern
[domain-name:value = 'pumaenmexico.com.mx']
Name
pumaparamexico.com

Pattern Type
stix
Pattern
[domain-name:value = 'pumaparamexico.com']
Name
pumahungary.org
Pattern Type
stix
Pattern
[domain-name:value = 'pumahungary.org']
Name
pumashoesindia.co.in
Pattern Type
stix
Pattern
[domain-name:value = 'pumashoesindia.co.in']
Name
pumamexicomx.com

Pattern Type
stix
Pattern
[domain-name:value = 'pumamexicomx.com']
Name
pumaoutletspain.es
Pattern Type
stix
Pattern
[domain-name:value = 'pumaoutletspain.es']
Name
puma-barcelona.com
Pattern Type
stix
Pattern
[domain-name:value = 'puma-barcelona.com']
Name
pumaoutletgreece.com

Pattern Type
stix
Pattern
[domain-name:value = 'pumaoutletgreece.com']
Name
pumashoesaustralia.org
Pattern Type
stix
Pattern
[domain-name:value = 'pumashoesaustralia.org']
Name
pumaoutletsingapore.com
Pattern Type
stix
Pattern
[domain-name:value = 'pumaoutletsingapore.com']
Name
puma-south-africa.co.za

Pattern Type
stix
Pattern
[domain-name:value = 'puma-south-africa.co.za']
Name
pumaoutletindia.com
Pattern Type
stix
Pattern
[domain-name:value = 'pumaoutletindia.com']
Name
pumasneakers.co.in
Pattern Type
stix
Pattern
[domain-name:value = 'pumasneakers.co.in']
Name
pumacheapuk.com

Pattern Type
stix
Pattern
[domain-name:value = 'pumacheapuk.com']
Name
pumaonlineshopdeutschland.com
Pattern Type
stix
Pattern
[domain-name:value = 'pumaonlineshopdeutschland.com']
Name
pumaifactoryturkey.com
Pattern Type
stix
Pattern
[domain-name:value = 'pumaifactoryturkey.com']
Name
pumafactoryoutletuk.com

Pattern Type
stix
Pattern
[domain-name:value = 'pumafactoryoutletuk.com']
Name
pumashoesirelandie.com
Pattern Type
stix
Pattern
[domain-name:value = 'pumashoesirelandie.com']
Name
pumasingaporeoutlet.com
Pattern Type
stix
Pattern
[domain-name:value = 'pumasingaporeoutlet.com']
Name
pumacroatia.com.hr

Pattern Type
stix
Pattern
[domain-name:value = 'pumacroatia.com.hr']
Name
pumaoutletnorge.com
Pattern Type
stix
Pattern
[domain-name:value = 'pumaoutletnorge.com']
Name
pumacroatia.com
Pattern Type
stix
Pattern
[domain-name:value = 'pumacroatia.com']
Name
pumaslovensko.sk

Pattern Type
stix
Pattern
[domain-name:value = 'pumaslovensko.sk']
Name
pumastoremexico.com
Pattern Type
stix
Pattern
[domain-name:value = 'pumastoremexico.com']
Name
pumasaleonlineindia.in
Pattern Type
stix
Pattern
[domain-name:value = 'pumasaleonlineindia.in']
Name
puma-india.co.in

Pattern Type
stix
Pattern
[domain-name:value = 'puma-india.co.in']
Name
pumasalesingapore.com
Pattern Type
stix
Pattern
[domain-name:value = 'pumasalesingapore.com']
Name
puma-italia.com
Pattern Type
stix
Pattern
[domain-name:value = 'puma-italia.com']
Name
pumashoes-uksale.com

Pattern Type
stix
Pattern
[domain-name:value = 'pumashoes-uksale.com']
Name
bestpumaindia.in
Pattern Type
stix
Pattern
[domain-name:value = 'bestpumaindia.in']
Name
puma-shoes-singapore.com
Pattern Type
stix
Pattern
[domain-name:value = 'puma-shoes-singapore.com']

Domain-Name

Value
pumashoeireland.com
puma4romania.com
puma-barcelona.com
bestpumaindia.in
pumafactoryoutletuk.com
puma-italia.com
pumashoesaustralia.org
pumaonlineshopdeutschland.com
pumasingaporeoutlet.com
pumashoes-singapore.com
pumaenmexico.com.mx
pumacroatia.com.hr
pumastoremexico.com

pumacheapuk.com

puma-shoes-singapore.com

puma-south-africa.co.za

pumashoes-uksale.com

pumaoutletgreece.com

pumasaleonlineindia.in

pumashoesirelandie.com

pumasalesingapore.com

pumaparamexico.com

pumaoutletspain.es

pumamexicomx.com

pumaoutletindia.com

pumahungary.org

pumaoutletnorge.com

pumasneakers.co.in

pumaoutletsingapore.com

pumaifactoryturkey.com

pumacroatia.com

pumashoesindia.co.in
pumagreece.gr
puma-india.co.in
pumaslovensko.sk

External References

- https://bolster.ai/blog/brand-impersonation-scam
- https://otx.alienvault.com/pulse/648a0adc070803c396efc642