Jul 11 2024

NETMANAGEIT

Intelligence Report

FIN7: Silent Push unearths 4000+ phishing and shell domains

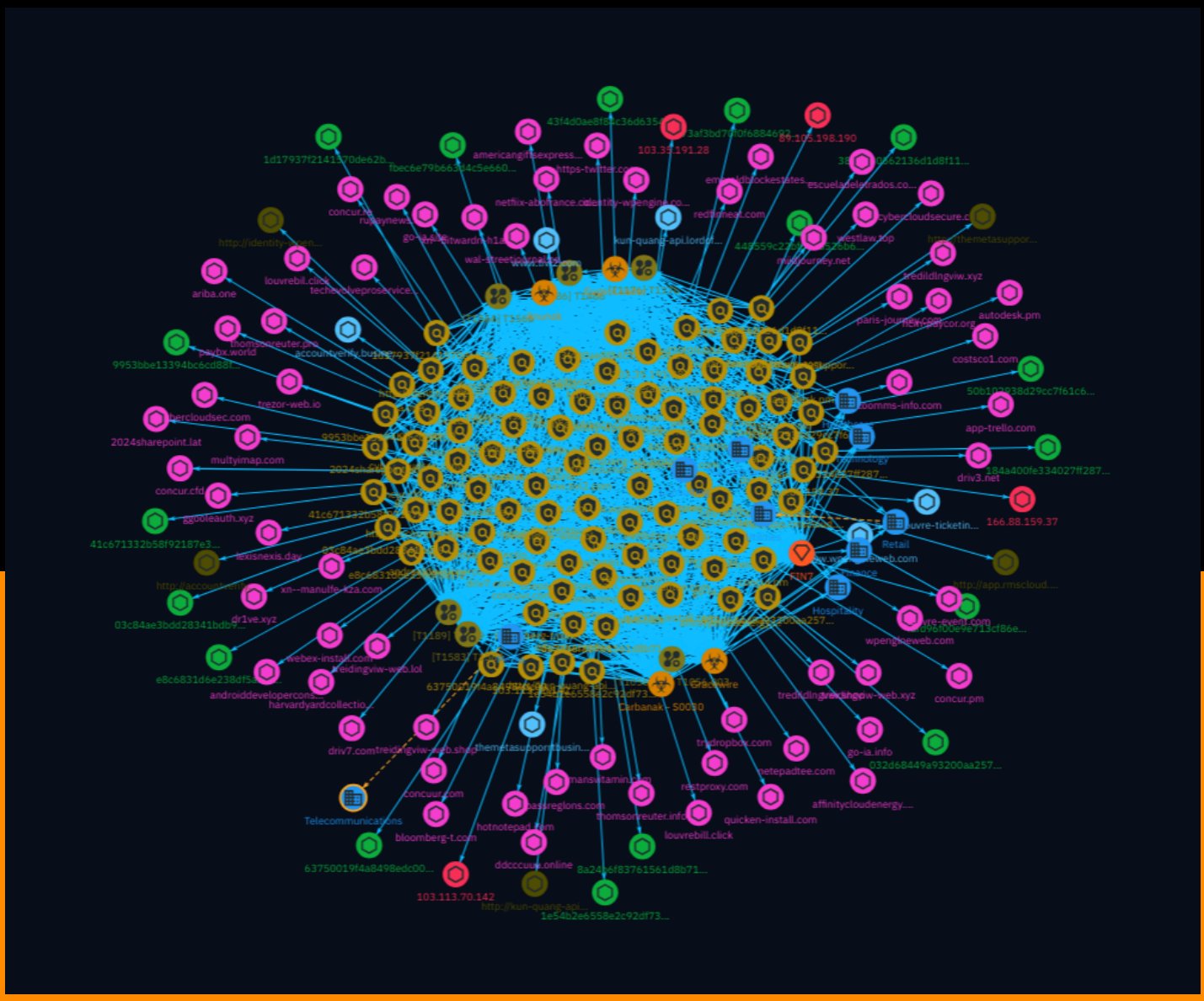

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Silent Push threat analysts have uncovered an extensive series of campaigns linked to the FIN7 cybercrime group, including several hundred active phishing, spoofing, shell and malware delivery domains and IPs targeting various organizations. The campaigns utilize over 4000 domains and subdomains, with nearly half active in the past week. Prominent global brands like Louvre Museum, Meta, Reuters, Microsoft, and others have been targeted. The group employs tactics like spearphishing, malware distribution, and renting infrastructure from bulletproof hosting providers.

Confidence

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

100 / 100

Content

N/A

Attack-Pattern

Name
T1566
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

T1486

ID

T1486

Description

Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources. They can attempt to render stored data inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted.(Citation: US-CERT Ransomware 2016)(Citation: FireEye WannaCry 2017)(Citation: US-CERT NotPetya 2017)(Citation: US-CERT SamSam 2018) In the case of ransomware, it is typical that common user files like Office documents, PDFs, images, videos, audio, text, and source code files will be encrypted (and often renamed and/or tagged with specific file markers). Adversaries may need to first employ other behaviors, such as [File and Directory Permissions Modification](https://attack.mitre.org/techniques/T1222) or [System Shutdown/Reboot](https://attack.mitre.org/techniques/T1529), in order to unlock and/or gain access to manipulate these files.(Citation: CarbonBlack Conti July 2020) In some cases, adversaries may encrypt critical system files, disk partitions, and the MBR.(Citation: US-CERT NotPetya 2017) To maximize impact on the target organization, malware designed for encrypting data may have worm-like features to propagate across a network by leveraging other attack techniques like [Valid Accounts](https://attack.mitre.org/techniques/T1078), [OS Credential Dumping](https://attack.mitre.org/techniques/T1003), and [SMB/Windows Admin Shares](https://attack.mitre.org/techniques/T1021/002).(Citation: FireEye WannaCry 2017)(Citation: US-CERT NotPetya 2017) Encryption malware may also leverage [Internal Defacement](https://attack.mitre.org/techniques/T1491/001), such as changing victim wallpapers, or otherwise intimidate victims by sending ransom notes or other messages to connected printers (known as "print bombing").(Citation: NHS Digital Egregor Nov 2020) In cloud environments, storage objects within compromised accounts may also be encrypted.(Citation: Rhino S3 Ransomware Part 1)

Name

T1176

ID

T1176

Description

Adversaries may abuse Internet browser extensions to establish persistent access to victim systems. Browser extensions or plugins are small programs that can add functionality and customize aspects of Internet browsers. They can be installed directly or through a browser's app store and generally have access and permissions to everything that the browser can access.(Citation: Wikipedia Browser Extension)(Citation: Chrome Extensions Definition) Malicious extensions can be installed into a browser through malicious app store downloads masquerading as legitimate extensions, through social engineering, or by an adversary that has already compromised a system. Security can be limited on browser app stores so it may not be difficult for malicious extensions to defeat automated scanners.(Citation: Malicious Chrome Extension Numbers) Depending on the browser, adversaries may also manipulate an extension's update url to install updates from an adversary controlled server or manipulate the mobile configuration file to silently install additional extensions. Previous to macOS 11, adversaries could silently install browser extensions via the command line using the `profiles` tool to install malicious `.mobileconfig` files. In macOS 11+, the use of the `profiles` tool can no longer install configuration profiles, however `.mobileconfig` files can be planted and installed with user interaction.(Citation: xorrior chrome extensions macOS) Once the extension is installed, it can browse to websites in the background, steal all information that a user enters into a browser (including credentials), and be used as an installer for a RAT for persistence. (Citation: Chrome Extension Crypto Miner)(Citation: ICEBRG Chrome Extensions)(Citation: Banker Google Chrome Extension Steals Creds)(Citation: Catch All Chrome Extension) There have also been instances of botnets using a persistent backdoor through malicious Chrome extensions for [Command and Control](https://attack.mitre.org/tactics/TA0011). (Citation: Stantinko Botnet)(Citation: Chrome Extension C2 Malware) Adversaries may also use browser extensions to modify browser permissions and components, privacy settings, and other security controls for [Defense Evasion](https://attack.mitre.org/tactics/TA0005). (Citation: Browers FriarFox)(Citation: Browser Adrozek)

Name

T1583

ID

T1583

Description

Adversaries may buy, lease, rent, or obtain 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) Some infrastructure providers offer free trial periods, enabling infrastructure acquisition at limited to no cost.(Citation: Free Trial PurpleUrchin) 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), including from residential proxy services.(Citation: amnesty_nso_pegasus)(Citation: FBI Proxies Credential Stuffing)(Citation: Mandiant APT29 Microsoft 365 2022) 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.

Name

T1189

ID

T1189

Description

Adversaries may gain access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is typically targeted for exploitation, but adversaries may also use compromised websites for non-exploitation behavior such as acquiring [Application Access Token](https://attack.mitre.org/techniques/T1550/001). Multiple ways of delivering exploit code to a browser exist (i.e., [Drive-by Target](https://attack.mitre.org/techniques/T1608/004)), including: * A legitimate website is compromised where adversaries have injected some form of malicious code such as JavaScript, iFrames, and cross-site scripting * Script files served to a legitimate

website from a publicly writeable cloud storage bucket are modified by an adversary * Malicious ads are paid for and served through legitimate ad providers (i.e., [Malvertising](https://attack.mitre.org/techniques/T1583/008)) * Built-in web application interfaces are leveraged for the insertion of any other kind of object that can be used to display web content or contain a script that executes on the visiting client (e.g. forum posts, comments, and other user controllable web content). Often the website used by an adversary is one visited by a specific community, such as government, a particular industry, or region, where the goal is to compromise a specific user or set of users based on a shared interest. This kind of targeted campaign is often referred to a strategic web compromise or watering hole attack. There are several known examples of this occurring.(Citation: Shadowserver Strategic Web Compromise) Typical drive-by compromise process: 1. A user visits a website that is used to host the adversary controlled content. 2. Scripts automatically execute, typically searching versions of the browser and plugins for a potentially vulnerable version. * The user may be required to assist in this process by enabling scripting or active website components and ignoring warning dialog boxes. 3. Upon finding a vulnerable version, exploit code is delivered to the browser. 4. If exploitation is successful, then it will give the adversary code execution on the user's system unless other protections are in place. * In some cases a second visit to the website after the initial scan is required before exploit code is delivered. Unlike [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190), the focus of this technique is to exploit software on a client endpoint upon visiting a website. This will commonly give an adversary access to systems on the internal network instead of external systems that may be in a DMZ. Adversaries may also use compromised websites to deliver a user to a malicious application designed to [Steal Application Access Token](https://attack.mitre.org/techniques/T1528)s, like OAuth tokens, to gain access to protected applications and information. These malicious applications have been delivered through popups on legitimate websites.(Citation: Volexity OceanLotus Nov 2017)

Name

T1056.003

ID

T1056.003

Description

Adversaries may install code on externally facing portals, such as a VPN login page, to capture and transmit credentials of users who attempt to log into the service. For example, a compromised login page may log provided user credentials before logging the user in to

the service. This variation on input capture may be conducted post-compromise using legitimate administrative access as a backup measure to maintain network access through [External Remote Services](https://attack.mitre.org/techniques/T1133) and [Valid Accounts](https://attack.mitre.org/techniques/T1078) or as part of the initial compromise by exploitation of the externally facing web service.(Citation: Volexity Virtual Private Keylogging)

Sector

Name
Utilities
Description
Private entities transforming and selling goods, products and equipment which are not included in other activity sectors.
Name
Finance
Description
Public and private entities involved in the allocation of assets and liabilities over space and time.
Name
Telecommunications
Description
Private and public entities involved in the production, transport and dissemination of information and communication signals.

Name
Hospitality
Description
Private entities offering to customers' leisure activities and experiences.
Name
Retail
Description
Distribution and sale of goods directly to the consumer.
Name
Technology
Description
Private entities related to the research, development, manufacturing and distribution of electronics, softwares, computers and products related to information technologies.
Name
Media
Description
Communication outlets used to deliver information by print, broadcast or Internet and people working in these outlets.
Name

Consulting

Name
Healthcare
Description
Public and private entities involved in research, services and manufacturing activities related to public health.

Domain-Name

Value
thomsonreuter.info
americangiftsexpress.com
multyimap.com
tredildlngviw.xyz
xn--bitwardn-h1a.com
driv7.com
miidjourney.net
concur.re
louvrebil.click
netepadtee.com
quicken-install.com
trydropbox.com
cybercloudsecure.com

wpenglneweb.com

hcm-paycor.org

lexisnexis.day

concuur.com

netfiix-abofrance.com

louvrebill.click

womansvitamin.com

bloomberg-t.com

restproxy.com

webex-install.com

hotnotepad.com

concur.cfd

identity-wpengine.com

affinitycloudenergy.com

ariba.one

costsco1.com

trezor-web.io

go-ia.site

techevolveproservice.com

onepassreglons.com

app-trello.com

escueladeletrados.com

wal-streetjournal.com

cybercloudsec.com

xn--manulfe-kza.com

driv3.net

go-ia.info

zoomms-info.com

paybx.world

ddcccuuu.online

treidingviw-web.lol

androiddeveloperconsole.com

emeraldblockestates.com

https-twitter.com

rupaynews.com

treidingviw-web.shop

concur.pm

paris-journey.com

westlaw.top

thomsonreuter.pro

autodesk.pm

louvre-event.com

treidingviw-web.xyz

harvardyardcollection.com

redfinneat.com

tredildlngviw.shop

2024sharepoint.lat

dr1ve.xyz

ggooleauth.xyz

StixFile

Value
03c84ae3bdd28341bdb9ef24918c3cad6c9ed27c768d351f23e6d37bf048f7a4
fdfd96f00e9e713cf86e2d32fb0c653b66fccc0e4969eac9f26d5cdcca98ff7d
3869340562136d1d8f11c304f207120f9b497e0a430ca1a04c0964eb5b70f277
50b102938d29cc7f61c67da6981545c69f70c7178d009ec1999ee0ddfe81ebba
9953bbe13394bc6cd88fd0d13ceff771553e3a63ff84dc20960b67b4b9c9e48e
1e54b2e6558e2c92df73da65cd90b462dcafa1e6dcc311336b1543c68d3e82bc
8a24b6f83761561d8b71429f586248f264139aee2d8349f375ccbba702e4ecb2
43f4d0ae8f84c36d635423719562cdb0f5d9647b79a758a33fdf4aa7540f5622
e8c6831d6e238df5a1f20fc00867b333474a659734ac46a9902fbbadaaf0b51e
1d17937f2141570de62b437ff6bf09b1b58cfdb13ff02ed6592e077e2d368252
d73af3bd70f0f68846920d61fab8836cf8906a2876489801f6e130f4d92aa50d
41c671332b58f92187e32771ed1ba86c1ed256e36f036f74c91cf1aa7db07bc2
032d68449a93200aa257943b7e22e619e5ab383f61c7466f7872eeba5ea5b838

448559c22bf09e6526b67defddcace275d7a0c580a38b0961165bc1efdb3367e

fbec6e79b663d4c5e660a7aff23e392a4f1311382923669548945e8346edbffb

63750019f4a8498edc008a343be90aac8fbb3307ba7eb519fc5df16258dff19c

184a400fe334027ff287ad0cf83c165fdf4605507c83ec054fb2b544f877163c

Hostname

Value
www.wpenglneweb.com
accountverify.business-helpcase718372649.click
www.tivi2.com
kun-quang-api.lordofscan.pro
book.louvre-ticketing.com
themetasupporrtbusiness.nexuslink.click

External References

- https://www.silentpush.com/blog/fin7/
- https://otx.alienvault.com/pulse/668fc73a5d94ad96c0882bb8