

INTRINSEC

Innovative by design



Cyber Threat Intelligence

A stalker in the box: infrastructure linking PandoraVNC and Mesh Central



[@Intrinsec](#)



[@Intrinsec](#)



[Blog](#)



[Website](#)

Table of contents

Key findings	3
Introduction.....	3
I. Strategical Intelligence	4
1. Attribution	4
1.1 Online presence.....	4
1.2 Intel gained from Vimeo.....	7
1.3 Github.....	11
2. Threat actors leveraging the tool.....	12
2.1 State-sponsored intrusion sets and hackers.....	12
2.2 Cybercrime actors.....	12
II. Tactical Intelligence	14
1. Tactics, Techniques and Procedures	14
2. Infrastructure Analysis	15
2.1 PandorahVNC C2s.....	15
2.2 Anonvnc.....	23
2.3 Mesh Agent	27
3. Technical Analysis of Mesh Agent.....	31
III. Actionable content	36
1. Indicators of compromise	36
2. Recommendations	37
Meshcentral.....	37
3. Sources	38

Key findings

In this report are presented:

- The online presence of “all_father”, the user advertising PandorahVNC.
- The capabilities of PandorahVNC and other known threat actors that were observed using it.
- An infrastructure related to PandorahVNC which is advertised as “anonvnc” and is linked with the remote tool Mesh Central.

Introduction

Hidden Virtual Network Computing (HVNC) is a sophisticated form of remote access designed for stealthy control over an infected system. Unlike traditional VNC tools, HVNC operates covertly, ensuring that the infected user's desktop environment remains unchanged and unsuspecting while the attacker manipulates a hidden desktop session.

HVNC malware is often employed in targeted attacks and is favoured for its ability to bypass traditional security measures. It enables attackers to remotely control the compromised machine, perform financial transactions, or access sensitive information without being detected by the victim. The use of HVNC has been associated with various cybercrime campaigns, particularly those targeting financial institutions and enterprises.

For this analysis, we will delve into the capabilities of PandorahVNC, exploring its infection vectors, infrastructure, and the implications of its deployment in the current threat landscape. We will also focus on an infrastructure linked with PandorahVNC that is currently being built to advertise a tool named “anonvnc”, related to MeshCentral remote session manager. By understanding the mechanisms and impact of these malware, cybersecurity professionals can better prepare defences and mitigate the risks associated with them.

On 10 March 2022, Florian Roth ([@cyb3rops on X](#)) made a tweet about PandorahVNC, exposing the content of one of its websites and asking his audience if this is “*malware or legitimate software that has the same features and functions as malware?*”. An OSINT investigation on PandorahVNC's operator was made by [SlashNext](#) on 13 December 2023, but since we did not identify a complete analysis of this operator and its tool, we decided to start an investigation on this subject.

I. Strategical Intelligence

1. Attribution

1.1 Online presence

PandorahVNC is sold and advertised by user “All_father”, “All Father” or “Allfather” on various channels. We identified the presence of this user on the cybercrime forums Exploit, XSS, Hackforum, on the messaging application Telegram, on Sellpass, GitHub, and on Vimeo. He also owns various websites where users can view the functionalities of his tool “PandorahVNC” and buy it.

“All_father” joined the forum Exploit on 13 September 2021 and created a thread named “*Pandora hVNC 2FA Bypass Hidden Desktop/ Outlook/ Foxmail/ Thunderbird Hidden Browsers/ WebGL/ Clone Profile/Chrome/ FireFox*” on 19 September 2021, to advertise its malware.

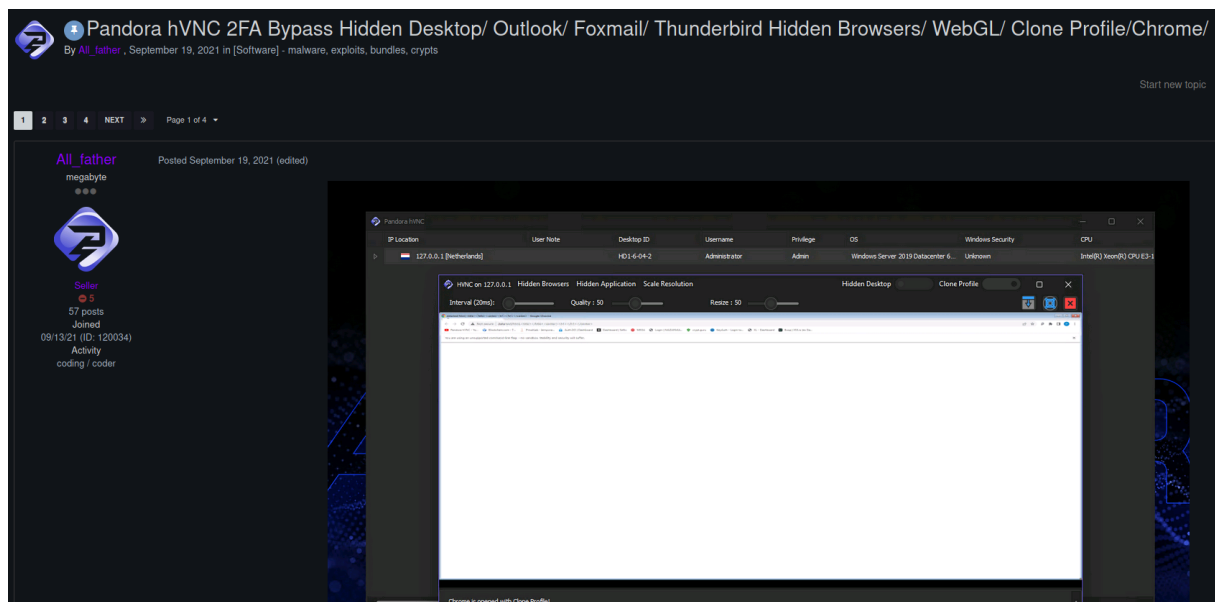


Figure 1 : « All_father » thread on Exploit.

This thread is used to showcase the capabilities of PandorahVNC, notify users of new updates and add contact information and prices for new buyers. The malware is sold for prices going from \$499 for 1 month, \$849 for 3 months, \$1199 for 6 months and \$1899 for 12 months. To contact “All_father”, users can visit his official websites “pandorahvnc.sellpass[.]io” or “hvncs[.]com”. Previously, the website “hiddenvnc[.]com” was advertised. This domain is of interest, as in the section “[AnonVNC](#)” of this analysis, it will be used to reveal links between PandorahVNC and a potential new service.

A stalker in the box: infrastructure linking PandorahVNC and Mesh Central

TLP: CLEAR

PAP: CLEAR



Figure 2: Official websites and Telegram handles advertised by “All_father”.

On the website hvncs[.]com we see that “All_father” possesses other means of contact, namely the email addresses “hiddenvnc[@]gmail[.]com”, “pandorahVNC[@]gmail[.]com” and the jabber “allfather[@]jab3r[.]org”.

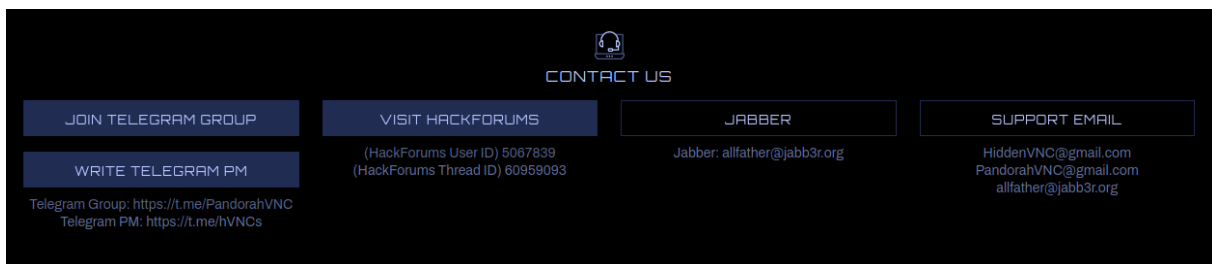


Figure 3: Contact information given by the website where users can buy PandorahVNC.

Users can also contact him privately on Telegram using the handle “@hVNCs” or go to his Telegram channel “PandorahVNC”. The channel was created on 18 August 2021, first as a group chat and was later converted into a channel. It has 969 members, and the last message was on 8 June 2024 to advertise the malware’s latest update.

A stalker in the box: infrastructure linking PandorahVNC and Mesh Central

TLP: CLEAR

PAP: CLEAR

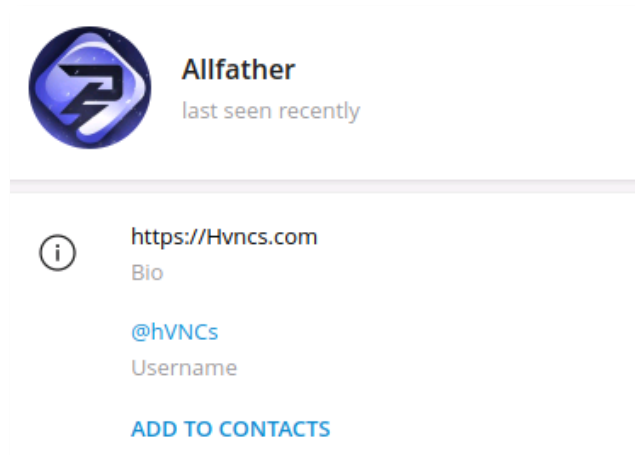


Figure 4: Telegram profile and channel of "All_father".

A stalker in the box: infrastructure linking PandorahVNC and Mesh Central

TLP: CLEAR

PAP: CLEAR

1.2 Intel gained from Vimeo

We noticed that “All Father” frequently shared Vimeo videos to showcase the capabilities of its malware. We decided to consult all his videos to see if valuable information could be gained from them. The main channel of “All Father” on Vimeo was created in August 2021 and has 9 videos. We also identified another account named “Pandora” created in June 2023. However, the only video on this channel is private.

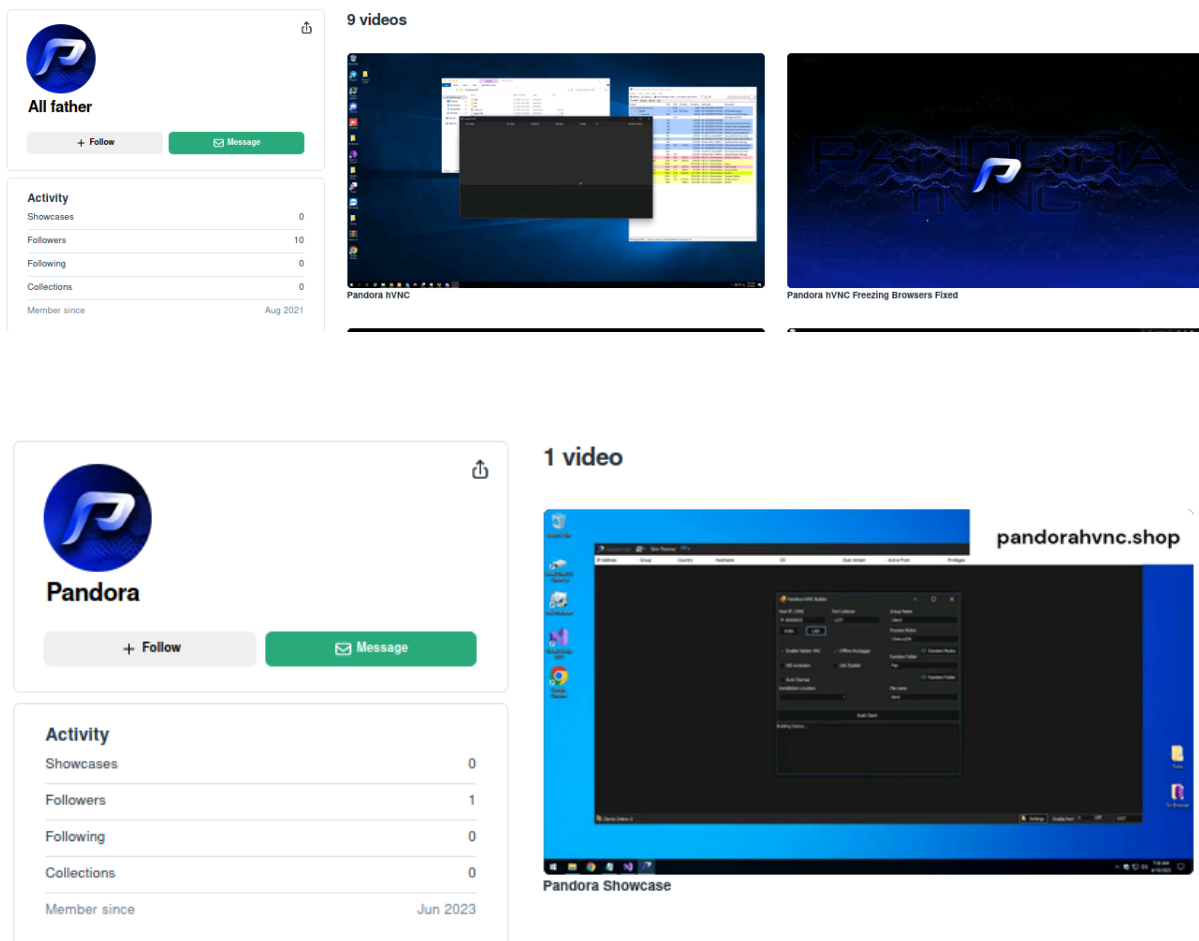


Figure 5: Vimeo channels belonging to “All_father”. Source: <https://vimeo.com/user148942049>.

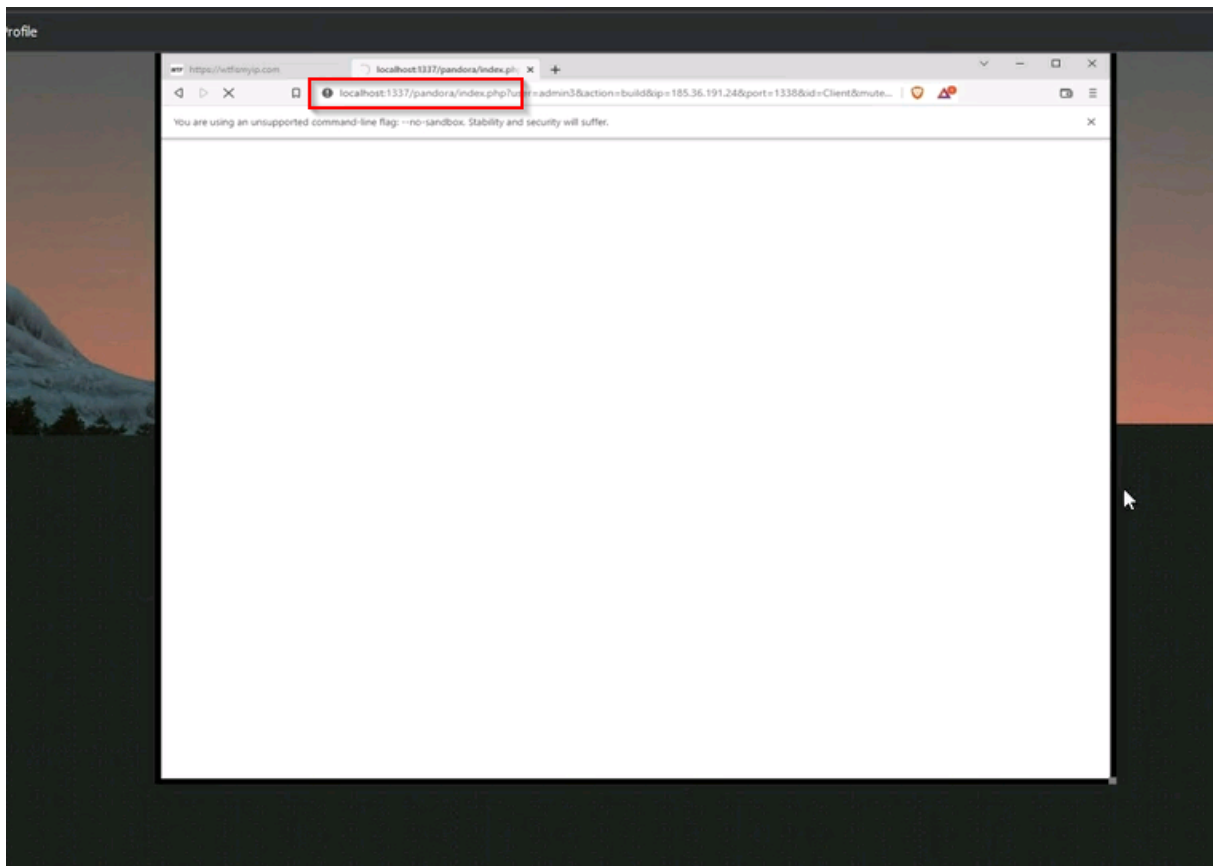
We see on one video that he visited a specific URL. The endpoint “/pandora/index.php” will be identified [later in this analysis](#) as we discovered C2 IP addresses linked with PandorahVNC:

localhost:1337/pandora/index.php?user=admin123&action=build&ip=185.36.191.24&port=1338&id=Client

A stalker in the box: infrastructure linking PandorahVNC and Mesh Central

TLP: CLEAR

PAP: CLEAR



*Figure 6: Query to the url
localhost:1337/pandora/index.php?user=admin123&action=build&ip=185.36.191.24&port=1338&id=Client seen in one of
all_father's video.*

Port 1337 was identified as the default port for listening event when a user of PandorahVNC starts a communication.

A stalker in the box: infrastructure linking PandorahVNC and Mesh Central

TLP: CLEAR

PAP: CLEAR

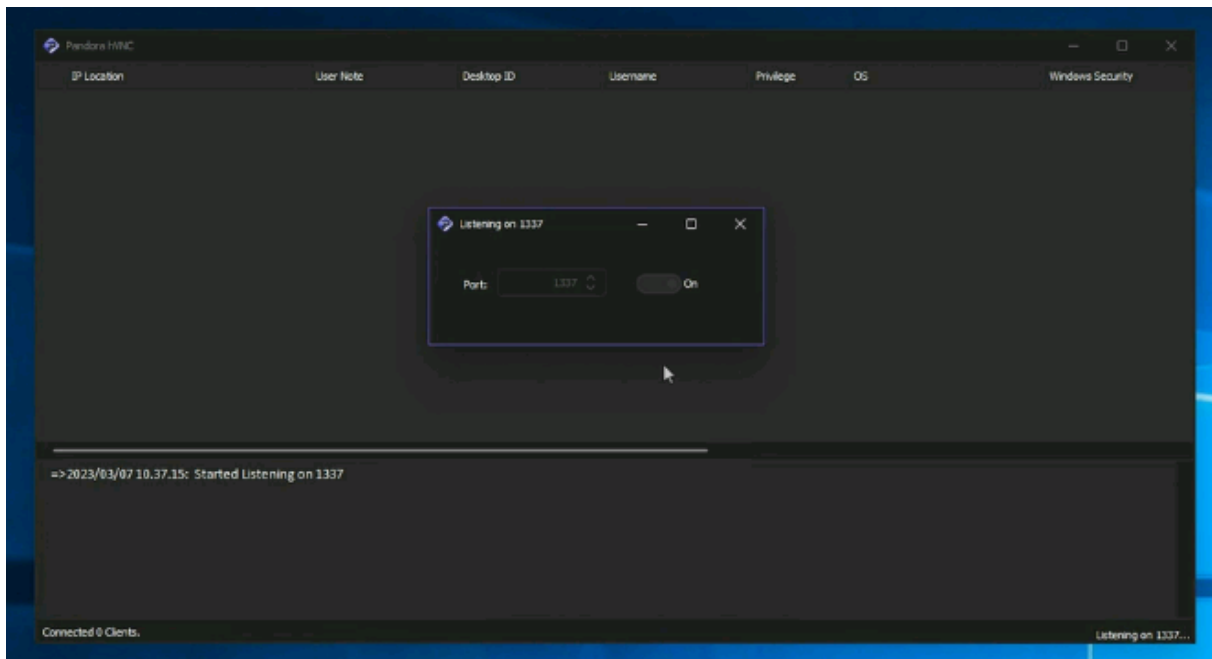


Figure 7: Default listening port is 1337, as seen in one of all_father's video.

In the same video, we can see the inbox of one of his Gmail accounts, revealing emails from WordPress, Sellix, HosterDaddy, HackForums, and potential clients of PandorahVNC.

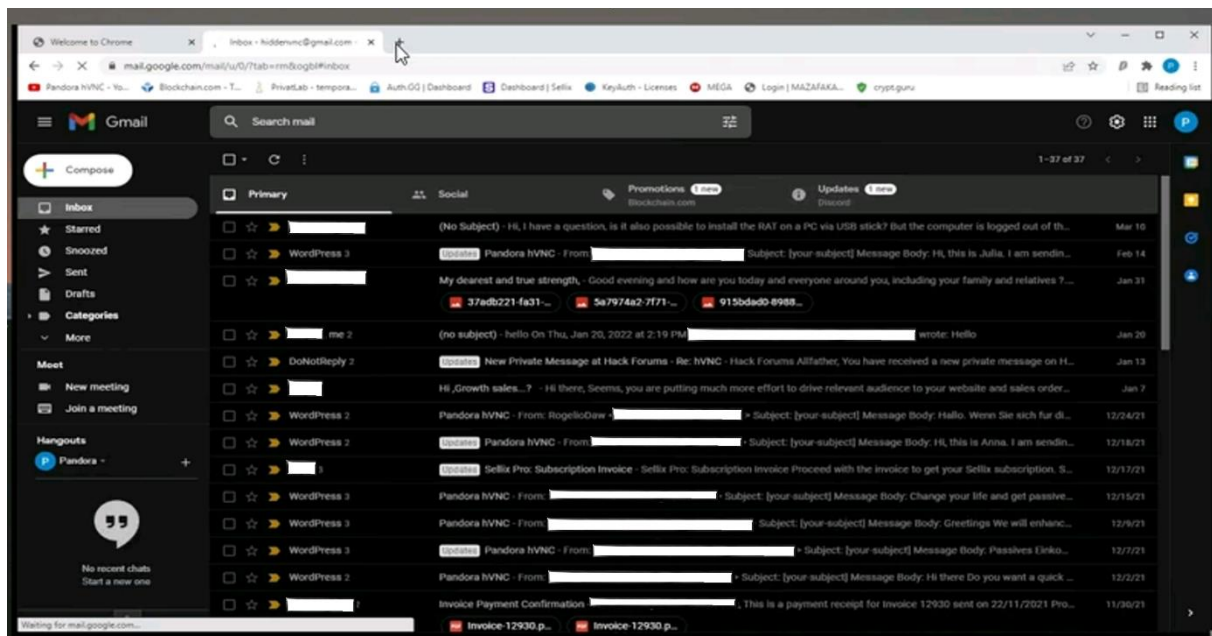


Figure 8: Gmail inbox of one of all_father's account. Source: <https://vimeo.com/687758924>.

We also see that All Father indeed has access to the two Gmail addresses advertised on his website.

A stalker in the box: infrastructure linking PandorahVNC and Mesh Central

TLP: CLEAR

PAP: CLEAR

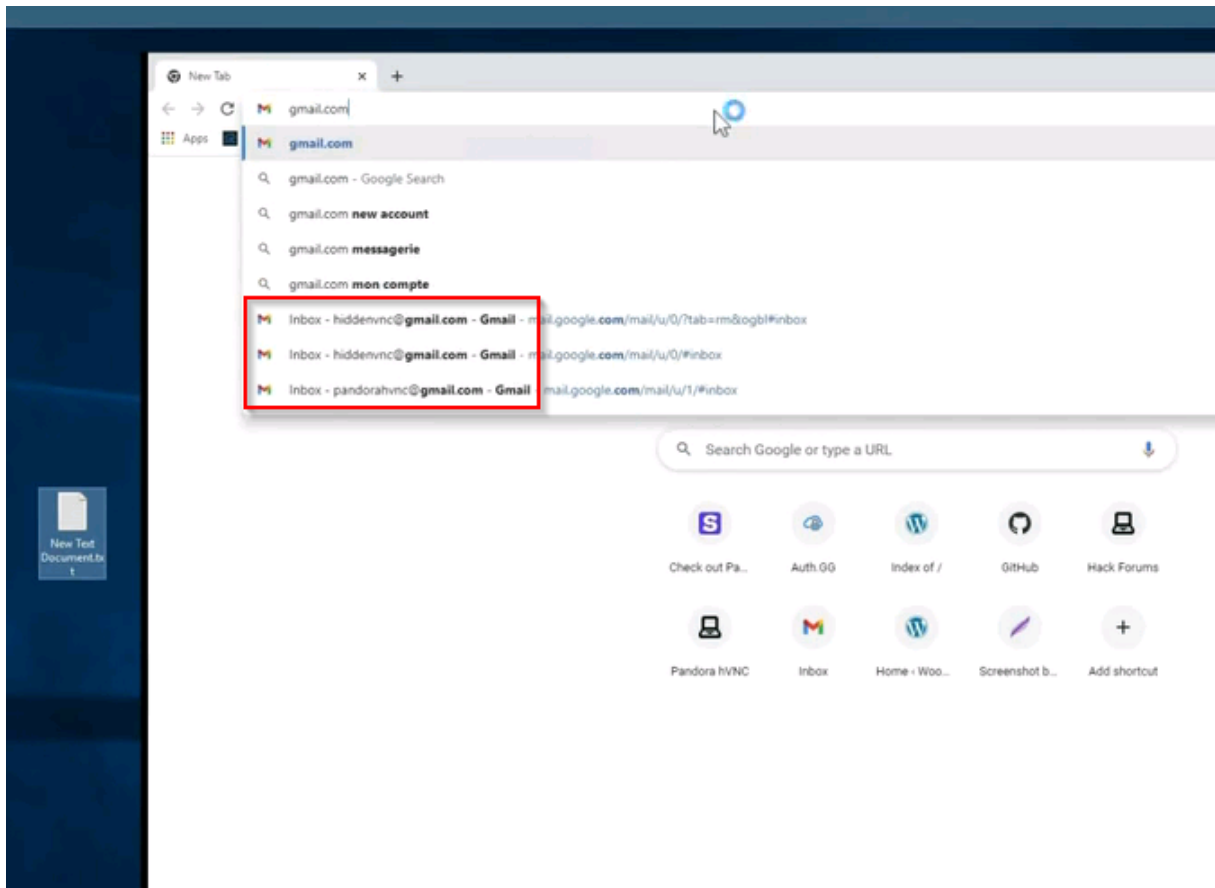


Figure 9: *hiddenvnc[.]gmail.com* and *pandorahvnc[.]gmail.com* seen in the search suggestion inside one of *all_father's* video.

A stalker in the box: infrastructure linking PandorahVNC and Mesh Central

TLP: CLEAR

PAP: CLEAR

1.3 Github

Using the email addresses exposed by AllFather on his website and videos, we were able to discover his GitHub account “PandorahVNC” with the help of Epieos.

The screenshot shows a GitHub account lookup tool interface. At the top left is the GitHub logo. To its right is a text box with the description: "This tool allows you to find a github account linked to an email address." Further right is a yellow and white checkered icon. Below this is a table of account details:

Query	hiddenvnc@gmail.com
Photo	https://avatars.githubusercontent.com/u/89485326?v=4
Login	PandorahVNC
Id	89485326
Type	User
Site Admin	false
Public Repos	1
Public Gists	0
Followers	1
Following	0
Creation Date	Tue, 24 Aug 2021 20:08:33 GMT (3 years ago)
Update Date	Fri, 08 Apr 2022 23:56:49 GMT (2 years ago)
Profile	https://github.com/PandorahVNC

A large, semi-transparent watermark "EPIEOS" is overlaid across the bottom half of the screenshot.

Figure 10: GitHub account “PandorahVNC” linked with hiddenvnc[.]gmail.com as evidenced by Epieos.

This GitHub account only has one repository that was not modified in the last 3 years, named “PhotoCollection”. It contains two .jpg files named “Pandora_by_Daniel_F.Gerhartz” and “psyche” showing work of arts related to the myth of Pandora, and a .ps1 file named “rescale.ps1”. This file will be the starting point of the section “[Infrastructure Analysis](#)”, where we discovered how PandorahVNC interacts with its central infrastructure.

A stalker in the box: infrastructure linking PandorahVNC and Mesh Central

TLP: CLEAR

PAP: CLEAR

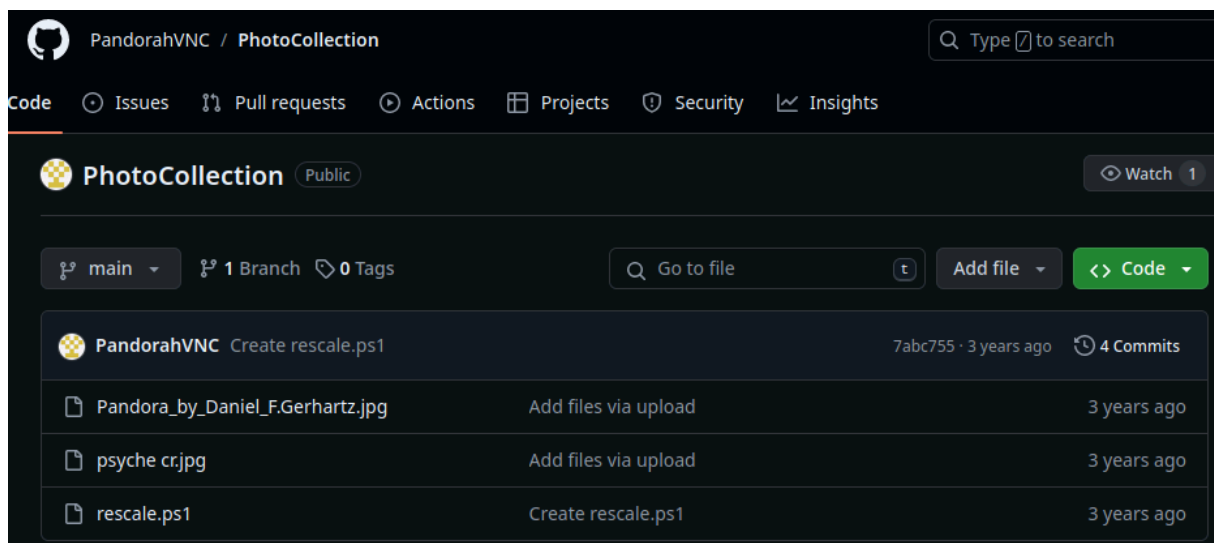


Figure 11: Content of the only repository of the GitHub account "PandorahVNC". Source: <https://github.com/PandorahVNC/PhotoCollection>.

2. Threat actors leveraging the tool

2.1 State-sponsored intrusion sets and hacktivists

Searching on public literature of other cybersecurity editors, we identified that PandorahVNC was used by various threat actors. The [Ukrainian government](#) published in 22 April 2024 an article indicating that the intrusion set tracked as UAC-0056 used PandorahVNC, combined with other tools such as GrimPlant, GraphSteel and RemoteUtilities to target Ukraine's critical IT infrastructure. UAC-0056 is identified by the Ukrainian services as being composed of "Russian hackers and cyber spies". According to [SentinelOne](#), this intrusion set is also known as UNC2589 as [tracked by Mandiant](#), and is extensively focused on targeting Ukraine and NATO members. Unfortunately, the article does not detail how PandorahVNC was used in the kill chain.

2.2 Cybercrime actors

In a phishing campaign identified by [Fortinet on May 2022](#), a threat actor delivered three different malware: PandorahVNC, AveMariaRAT and BitRAT. In this campaign, PandorahVNC was injected in RegASM.exe and contacted the domain vncgoga.duckdns[.]org as a C2 on port 1338. It is interesting that according to VirusTotal, [this domain](#) was contacted by a [file named "stub.exe"](#), that also contacted the URL "<http://51.254.27.112:1337/skra.jpg>", which is the same network communication we identified in the section "[2.1 PandorahVNC C2s](#)" of this analysis.

On Exploit, AllFather showed answers from a variety of clients on his thread, showing that they made financial gains using PandorahVNC. What is revealed by these screenshots and messages is that the tool is used to log into their victim's bank accounts and crypto wallets and empty them. One actor also showed that he is connected to an internal bank IT account and uses it to create bank accounts. This

A stalker in the box: infrastructure linking PandorahVNC and Mesh Central

TLP: CLEAR

PAP: CLEAR

highlights the risk posed by this malware that could enable various malicious actions such as espionage, financial and account theft, as well as data exfiltration.

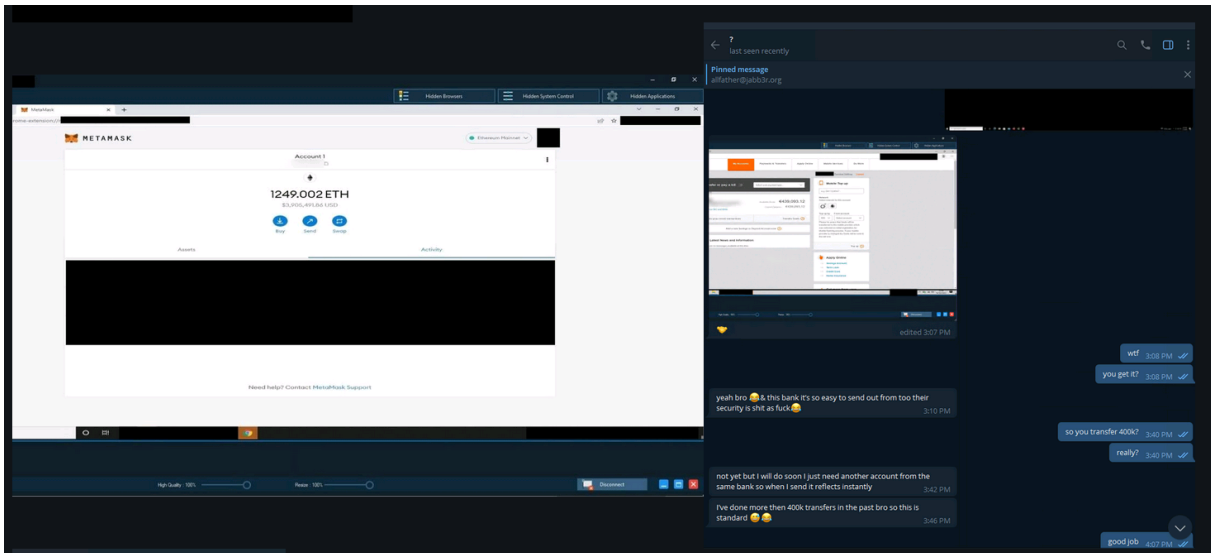


Figure 12: Messages allegedly exchanged between “all_father” and one of his client, exposing the financial gains made using PandorahVNC.

II. Tactical Intelligence

1. Tactics, Techniques and Procedures

Currently, the malware is advertised with the following capabilities on All Father's websites and forum posts:

- Hidden desktop, reverse connection, encrypted connection, browser profile cloner
- Copy/Paste (Internal) – Access to all applications/Mouse & Keyboard controls
- Access to file manager: cut/copy/paste, delete, upload, download, rename, new folder, execute, refresh
- Supports browsers and web applications: Chrome, Edge, Firefox, Brave, Comodo, Maxthon, Vivaldi, Foxmail, Thunderbird, Outlook
- Kill, restart, refresh or search process
- Launch and execute command/PowerShell
- Reflective stub injection (in memory)
- Online and offline keylogger
- Shutdown/restart victim system
- Download and execute from disk/url
- Panel to control all the features and clients.
- Password recovery (stealer module) from Firefox, Chrome, Edge: password, cookies, history, credits, autofill, bookmarks.
- Random mutex
- Obfuscated stub

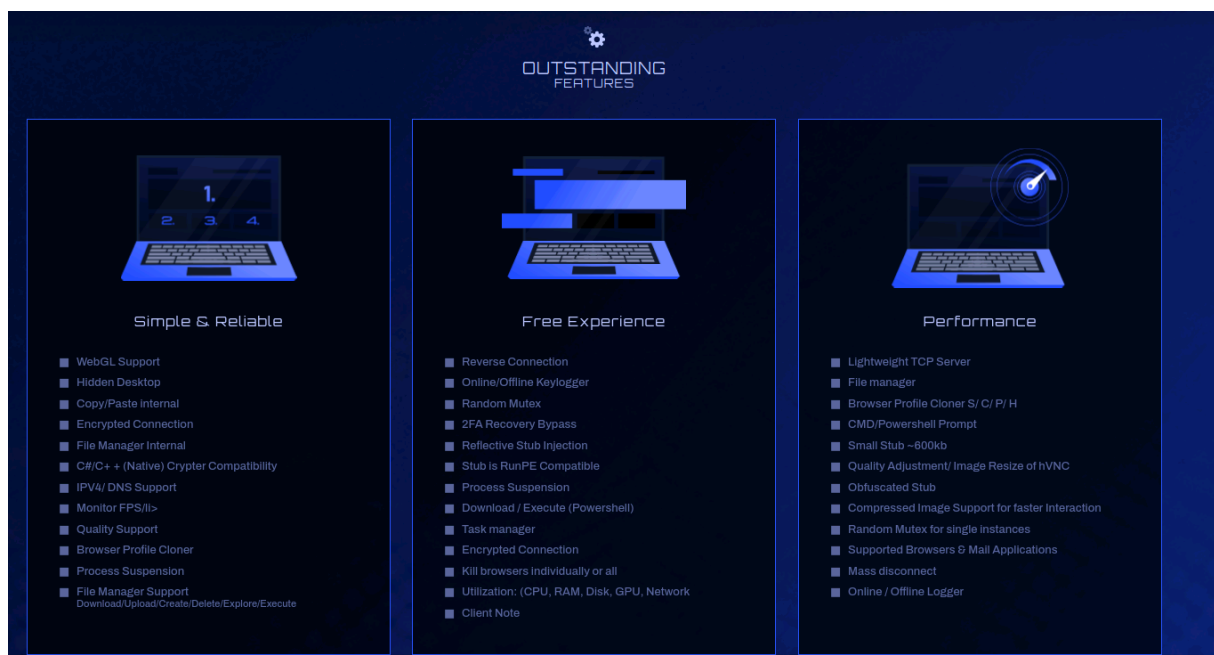


Figure 13: Features of PandorahVNC as advertised in one of all_father's websites.

A stalker in the box: infrastructure linking PandorahVNC and Mesh Central

TLP: CLEAR

PAP: CLEAR

Inside the builder of PandorahVNC, users can setup the following options: IP/DNS and port, startup folder (`%AppData%`, `%AppData%\Local`, `%AppData%\Roaming` or `%AppData%\Local\Temp`), sleep time on startup, offline keylogging. They can also modify the assembly information of the client file, namely the icon, product name, description, company, copyright, trademarks, original filename, product version, file version. This is particularly useful for threat actors looking to masquerade their malware as a legitimate file for phishing attempts.

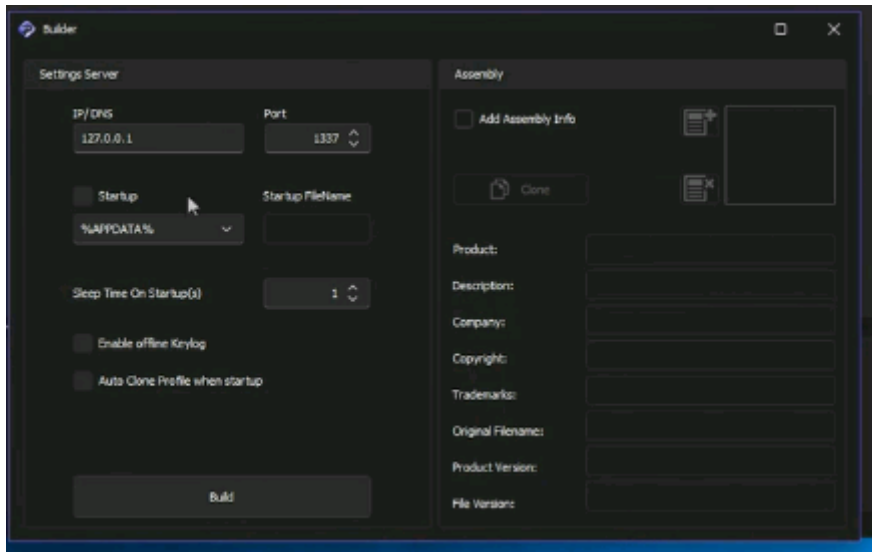


Figure 14: Builder options as seen in one of all_father's video.

2. Infrastructure Analysis

2.1 PandorahVNC C2s

We found that 155 files were referring the .ps1 file found inside PandorahVNC repository named "rescaleps1". This is highly suspicious as the content of the file is simple and the repository is not "popular" on GitHub. As indicated by its name and content, this file could be used by the "scale resolution" feature of PandorahVNC.

A stalker in the box: infrastructure linking PandorahVNC and Mesh Central

TLP: CLEAR

PAP: CLEAR

The screenshot displays the VirusTotal interface for a file named 'rescale.ps1'. At the top left, a circular progress indicator shows a score of 5 out of 90. A red banner at the top right states '5/90 security vendors flagged this URL as malicious'. Below this, the file's source is listed as 'https://raw.githubusercontent.com/PandorahVNC/PhotoCollection/main/rescale.ps1' and 'raw.githubusercontent.com'. The file type is identified as 'text/plain'. A 'Community Score' section shows a score of 5 with a green checkmark. The 'RELATIONS' tab is active, showing 'Downloaded Files (1/1)' and 'Referrer Files (10/155)'. The downloaded file name is '4b3062235faa8977836dfc8613d36c5ebd6c5584ba185d9150a47ce6a5462dc7' and the file name is 'rescale.ps1'. Several tags are associated with the file, including 'powershell', 'runtime-modules', 'direct-cpu-clock-access', and 'detect-debug-environment'.

Figure 15: 155 files seen referring the file "rescale.ps1" found inside the GitHub "PandorahVNC". Source: <https://www.virustotal.com/gui/url/7f117972eaa66dfc6b238d6a0f55f36078e3bf4bcc3698461df29614e66ca728/relations>

A stalker in the box: infrastructure linking PandorahVNC and Mesh Central

TLP: CLEAR

PAP: CLEAR

The screenshot shows a GitHub code viewer for the file 'rescale.ps1' in the 'PhotoCollection' repository of 'PandorahVNC'. The code is a PowerShell script that defines a function to call a WinAPI function for screen rescaling. The code is as follows:

```

1  # $scaling = 0 : 100% (default)
2  # $scaling = 1 : 125%
3  # $scaling = 2 : 150%
4  # $scaling = 3 : 175%
5  # screen rescale
6  param($scaling = 0)
7  $source = @"
8  [DllImport("user32.dll", EntryPoint = "SystemParametersInfo")]
9  public static extern bool SystemParametersInfo(
10         uint uiAction,
11         uint uiParam,
12         uint pvParam,
13         uint fWinIni);
14  '@
15  $apicall = Add-Type -MemberDefinition $source -Name WinAPICall -Namespace SystemParamInfo -PassThru
16  $apicall::SystemParametersInfo(0x009F, $scaling, $null, 1) | Out-Null

```

Figure 16: Content of the file "rescale.ps1". Source: <https://github.com/PandorahVNC/PhotoCollection/blob/main/rescale.ps1>

Querying one of these 155 files on VirusTotal, we see that it communicated with the IP address **51.254.27.112** to the endpoint `"/skra.jpg"`. Notice that the IP address is contacted on port 1337, as seen in the showcasing of PandorahVNC by AllFather on Vimeo (see [Intel gained from Vimeo](#)).

A stalker in the box: infrastructure linking PandorahVNC and Mesh Central

TLP: CLEAR

PAP: CLEAR

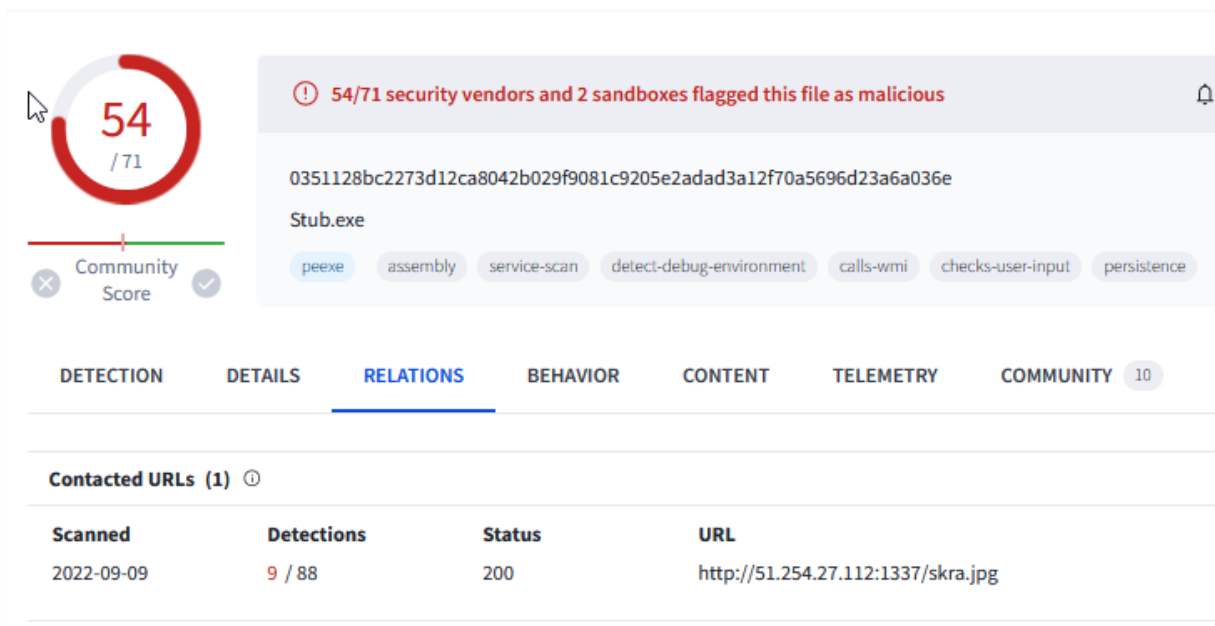


Figure 17: Stub.exe communicating with URL 51.254.27[.]112:1337/skra.jpg. Source: <https://www.virustotal.com/gui/file/0351128bc2273d12ca8042b029f9081c9205e2adad3a12f70a5696d23a6a036e/relations>

This IP address appears to be effectively linked to PandorahVNC, as evidenced by the endpoints **"/pandora/index.php"** (that was seen in one of Allfather's video) and **"/pandora/update/PandorahVNC.exe"**. As this IP address was also identified by pivoting of a threat actor's PandorahVNC C2 found by [Fortinet](#), it is possible that this is not a specific threat actor C2 but a central C2 used by the malware to update its functionalities amongst other things.

A stalker in the box: infrastructure linking PandorahVNC and Mesh Central

TLP: CLEAR

PAP: CLEAR

URLs (25) ⓘ

Scanned	Detections	Status	URL
2024-06-16	8 / 95	-	http://51.254.27.112:1337/skra.jpg=Dn
2024-06-07	7 / 95	-	https://51.254.27.112/
2024-06-12	9 / 95	-	http://51.254.27.112/
2024-06-06	6 / 95	-	http://51.254.27.112:1337/pandora/index.phpEhttp://51.254.27.112:1337/pandora
2024-06-06	6 / 95	-	http://51.254.27.112:1337/pandora/index.phpEhttp://51.254.27.112:1337/pandora/
2023-10-19	12 / 90	-	http://51.254.27.112:1337/pandora/update/
2023-10-13	5 / 90	-	https://51.254.27.112:1337/
2023-09-27	6 / 90	-	http://51.254.27.112:1337/skra.jpgP
2023-09-14	12 / 90	-	http://51.254.27.112/pandora/update/PandorahVNC.exe
2023-09-08	7 / 89	-	https://51.254.27.112:1337/bob.jpg/
2023-09-07	11 / 89	-	https://51.254.27.112/pandora/update/pandorahvnc.exe/
2023-09-06	7 / 89	404	http://51.254.27.112:1337/bob.jpg
2023-09-06	9 / 89	404	http://51.254.27.112:1337/pandora/update/PandorahVNC.exe
2023-09-05	8 / 89	-	http://51.254.27.112/pandora/update/pandorahvnc.exe
2022-10-17	9 / 89	200	http://51.254.27.112:1337/
2022-09-09	9 / 88	200	http://51.254.27.112:1337/skra.jpg
2022-06-17	12 / 95	-	http://51.254.27.112/skra.jpg
2022-02-27	10 / 93	-	https://51.254.27.112:1337/pandora/update/PandorahVNC.exe
2022-02-27	12 / 93	-	https://51.254.27.112/pandora/update/PandorahVNC.exe
2022-02-24	9 / 93	-	http://51.254.27.112/bob.jpg

Figure 18: URLs related to PandorahVNC seen in the IP address. Source: <https://www.virustotal.com/gui/ip-address/51.254.27.112/relations>

Searching the file “skra.jpg” on VirusTotal, we found two additional IP addresses that appear similar based on the endpoints identified by the platform and the files communicating with them.

A stalker in the box: infrastructure linking PandorahVNC and Mesh Central

TLP: CLEAR

PAP: CLEAR

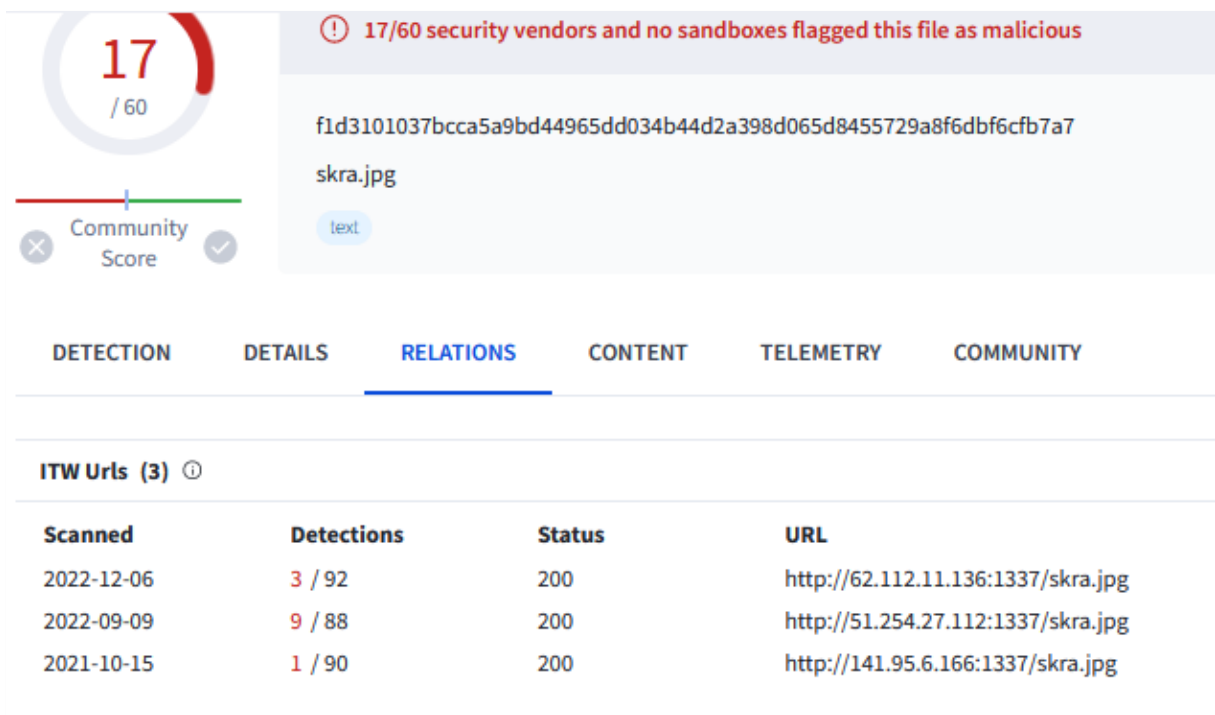


Figure 19: 3 IP addresses exposing the file skra.jpg on port 1337. Source: <https://www.virustotal.com/gui/file/f1d3101037bcc5a9bd44965dd034b44d2a398d065d8455729a8f6dbf6cfb7a7/relation>

s

A stalker in the box: infrastructure linking PandorahVNC and Mesh Central

TLP: CLEAR

PAP: CLEAR

2024-05-19	8 / 94	-	https://62.112.11.136/
2024-05-18	6 / 94	-	http://62.112.11.136:1337/pandora/index.php
2023-12-26	10 / 91	-	http://62.112.11.136/skra.jpg
2023-12-07	9 / 90	-	http://62.112.11.136:1337/pandora
2023-12-01	8 / 90	-	http://62.112.11.136:1337/pandora/
2023-11-25	6 / 90	-	http://62.112.11.136:1337/
2023-02-26	4 / 90	404	http://62.112.11.136:1337/pandora/PandoraUser/Client.exe
2022-12-06	3 / 92	200	http://62.112.11.136:1337/skra.jpg
2019-09-17	0 / 71	-	http://dovbam.com/

Downloaded Files (2) ⓘ			
Scanned	Detections	Type	Name
2024-06-10	17 / 60	Text	skra.jpg
2024-06-19	0 / 64	HTML	imgid=vLJEcAlM2jirBGG2ms9giEDeC4JX9GRovAIVFRRFi5bfTsWiZ

Communicating Files (82) ⓘ			
Scanned	Detections	Type	Name
2023-04-13	55 / 69	Win32 EXE	PandorahVNCStubInstaller.exe
2023-10-02	56 / 72	Win32 EXE	Stub.exe
2023-03-15	49 / 69	Win32 EXE	PandorahVNCStubInstaller.exe
2023-05-01	52 / 69	Win32 EXE	PandorahVNCStubInstaller.exe
2023-07-22	65 / 70	Win32 EXE	C:\Users\user\AppData\Local\Temp\3582-490\software.exe
2024-05-30	49 / 70	Win32 EXE	Stub.exe
2023-05-02	40 / 70	Win32 EXE	mangle-pandora.exe

URLs (26) ⓘ			
Scanned	Detections	Status	URL
2024-06-17	2 / 95	-	http://141.95.6.166/
2024-06-17	2 / 95	200	https://141.95.6.166/
2024-04-19	1 / 92	200	http://mail1.researcher90.com/index.php/29311313717128399581610049536
2023-09-06	5 / 89	-	https://141.95.6.166:1337/bob.jpg/
2023-09-06	6 / 89	200	http://141.95.6.166:1337/bob.jpg
2022-02-22	5 / 93	404	http://141.95.6.166/bob.jpg
2022-02-22	4 / 93	404	http://141.95.6.166/pandora/update/pandorahvnc.exe
2021-10-15	1 / 90	200	http://141.95.6.166:1337/skra.jpg
2021-10-15	1 / 90	200	http://141.95.6.166:1337/
2021-10-13	1 / 90	-	http://141.95.6.166:1337/rescale.ps1
2021-10-03	4 / 89	200	http://141.95.6.166:1337/pandora/update/pandorahvnc.exe

Figure 20: Both IP addresses appear related to PandorahVNC. Source: <https://www.virustotal.com/gui/ip-address/62.112.11.136/relations> and <https://www.virustotal.com/gui/ip-address/141.95.6.166/relations>

We indeed found the IP address **141.95.6.166** mentioned as “host IP/DNS” in one of Pandora’s videos:

A stalker in the box: infrastructure linking PandorahVNC and Mesh Central

TLP: CLEAR

PAP: CLEAR

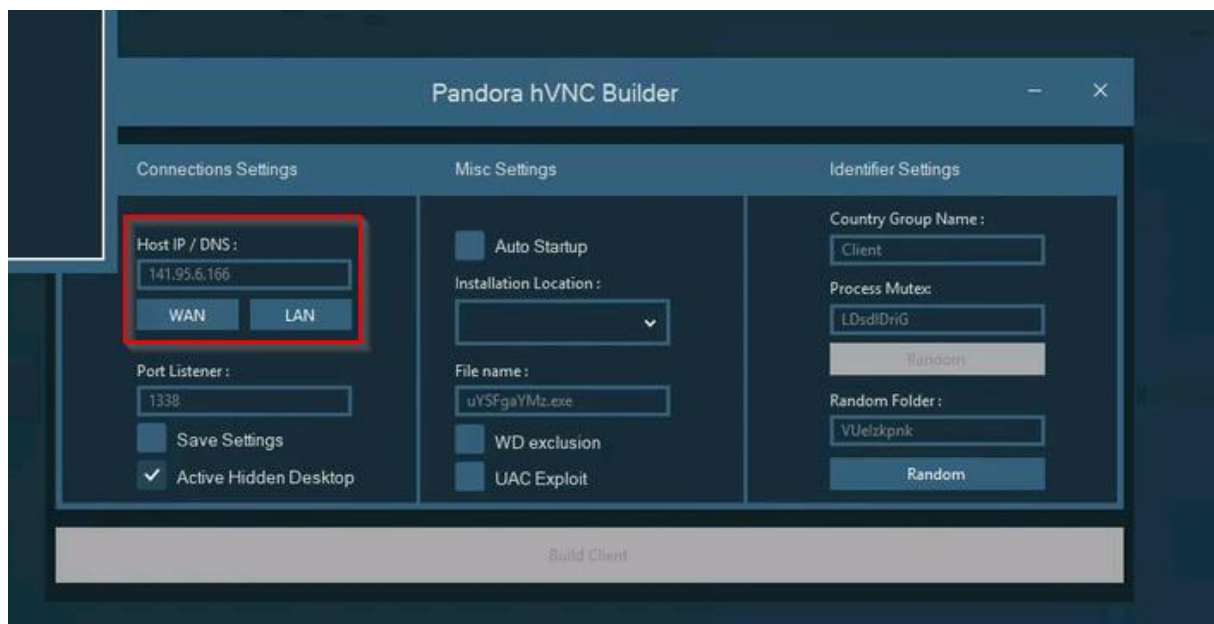


Figure 21: The IP 141.95.6.[.]166 is listed as "host ip/dns" in one of all_father's video. Source: <https://vimeo.com/595337064>

Searching for these IP addresses on Shodan, we noticed that 62.112.11[.]136 and 51.254.27[.]112 exposed on port 1337 a banner that showed a « welcome 😊 » string and an expiry date in 1980. Unfortunately, this banner does not appear to be exposed by other IP addresses.

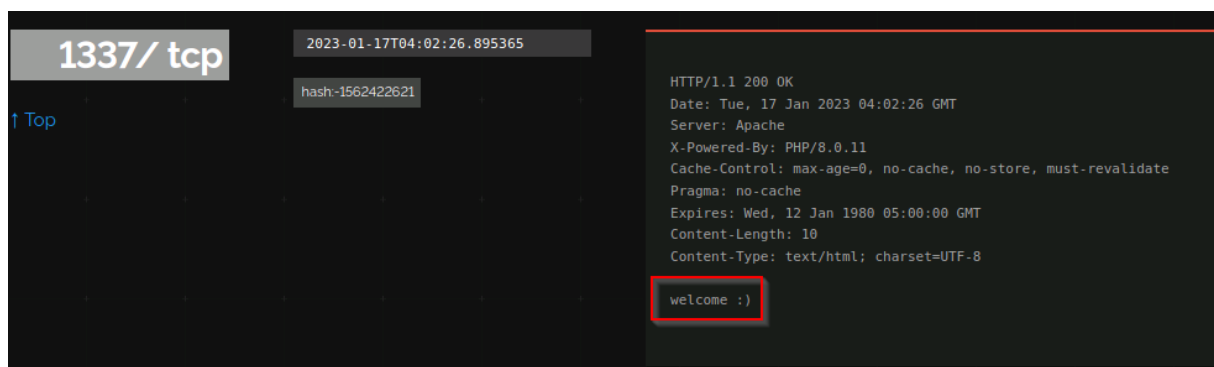


Figure 22: Content of the banner exposed by port 1337 of IP 51.254.27.112. Source: <https://www.shodan.io/host/51.254.27.112/history#1337>

A stalker in the box: infrastructure linking PandorahVNC and Mesh Central

TLP: CLEAR

PAP: CLEAR

2.2 Anonvnc

Using the IP address of the domain `hiddenvnc[.]com`, `66.94.109[.]162`, we find that it hosted two other domains related to VNC: `anonvnc[.]com` and `vncapk[.]io`:

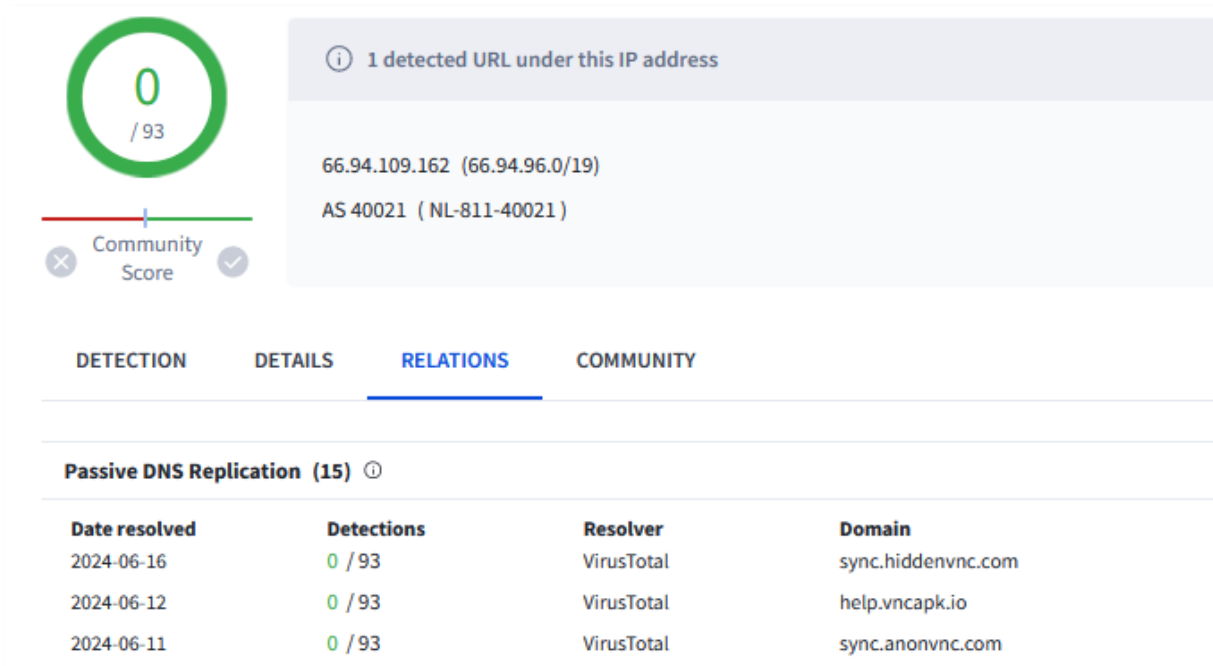


Figure 23: Domains related to vnc resolved by IP address 66.94.109[.]162. Source: <https://www.virustotal.com/gui/ip-address/66.94.109.162/relations>

The domains `sync.anonvnc.com` and `sync.hiddenvnc.com` both expose the same panel with mentions of an email address associated with PandorahVNC: “`admin[@]hiddenvnc[.]com`”.

A stalker in the box: infrastructure linking PandorahVNC and Mesh Central

TLP: CLEAR

PAP: CLEAR

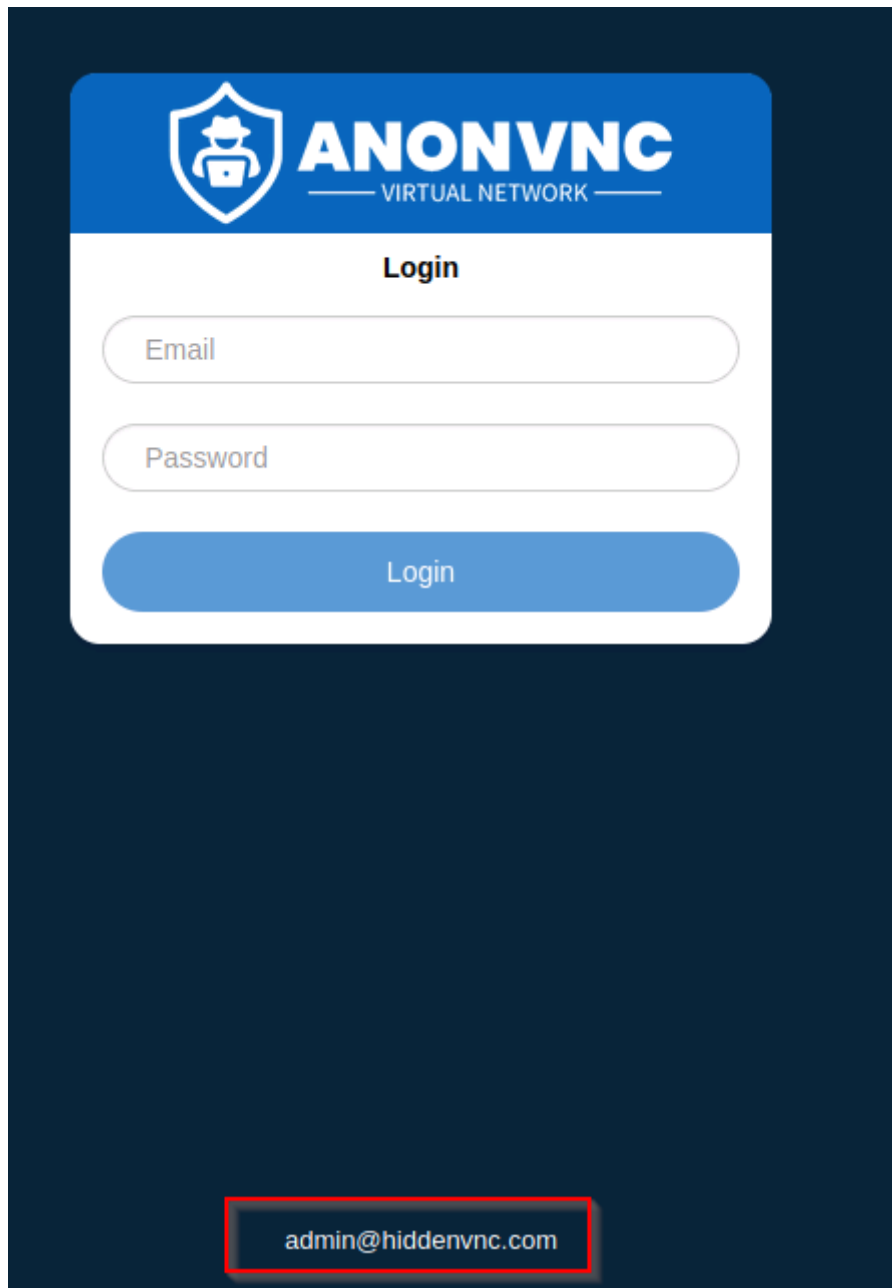


Figure 24: Login panel exposed by both domains, mentioning the mail address admin[@]hiddenvnc[.]com.

On Shodan, we see that this login panel is exposed on the IP address' port 443, with the title "AnonVNC – Login" and a specific favicon.

A stalker in the box: infrastructure linking PandorahVNC and Mesh Central

TLP: CLEAR

PAP: CLEAR

```
// 443 / TCP [external link]
-176773578 | 2024-06-19T04:17:24.790628

AnonVNC - Login

HTTP/1.1 200 OK
Referrer-Policy: no-referrer
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Security-Policy: default-src 'none'; font-src 'self'; script-src 'self' 'unsafe-inline'; connect-src 'self' wss://66.94.109.162; img-src 'self' blob: data: data:; style-src 'self' 'unsafe-inline'; frame-src 'self' blob: mcrouter; media-src 'self'; for m-action 'self'; manifest-src 'self'
Permissions-Policy: interest-cohort=()
X-Frame-Options: sameorigin
Strict-Transport-Security: max-age=63072000
Cache-Control: no-store
Content-Type: text/html; charset=utf-8
Content-Length: 74459
ETag: W/"122db-ftZYmo8RQFZMg8s9FIoEnvcjpts"
Set-Cookie: xid=e30=; path=/; samesite=lax; secure; httponly
Set-Cookie: xid.sig=sYoXnYy6Qz3HmGTrkQGsj0fY1huTnkzqfvJXa-vqQ5yqR-NYkR6Y9eGQXENnF9oe; path=/; samesite=lax; secure; httponly
Vary: Accept-Encoding
Date: Wed, 19 Jun 2024 04:17:24 GMT
Connection: keep-alive
Keep-Alive: timeout=5
```

Figure 25: Banner exposed by port 443 of IP 66.94.109[.]162. Source: <https://www.shodan.io/host/66.94.109.162>

Using Censys, we find another IP address that exposes the “AnonVNC – Login” html title on port 443: **94.131.121[.]91**. The IP address is now resolved by the domain [validatax\[.\]com](https://www.validatax[.]com) since 25 June 2024, which exposes an AnonVNC Login panel while it was previously resolved by the domain [help.vncapk\[.\]io](https://www.help.vncapk[.]io) in 30 May 2024. What is interesting is that this IP address belongs to AS44477 of **Stark Industries Solutions Ltd**. The fact that the domain name “validatax” is more phishing-ready than “vncapk” indicates that the operator may be starting to weaponize his toolset. Moreover, we found the golden image “WIN-BS656MOF35Q” on port 3389 of this IP address. This image emerged in May 2023 and is now shared across 4 335 hosts belonging to some organizations we have previously identified as renowned for being complacent with cybercrime.

A stalker in the box: infrastructure linking PandorahVNC and Mesh Central

TLP: CLEAR

PAP: CLEAR

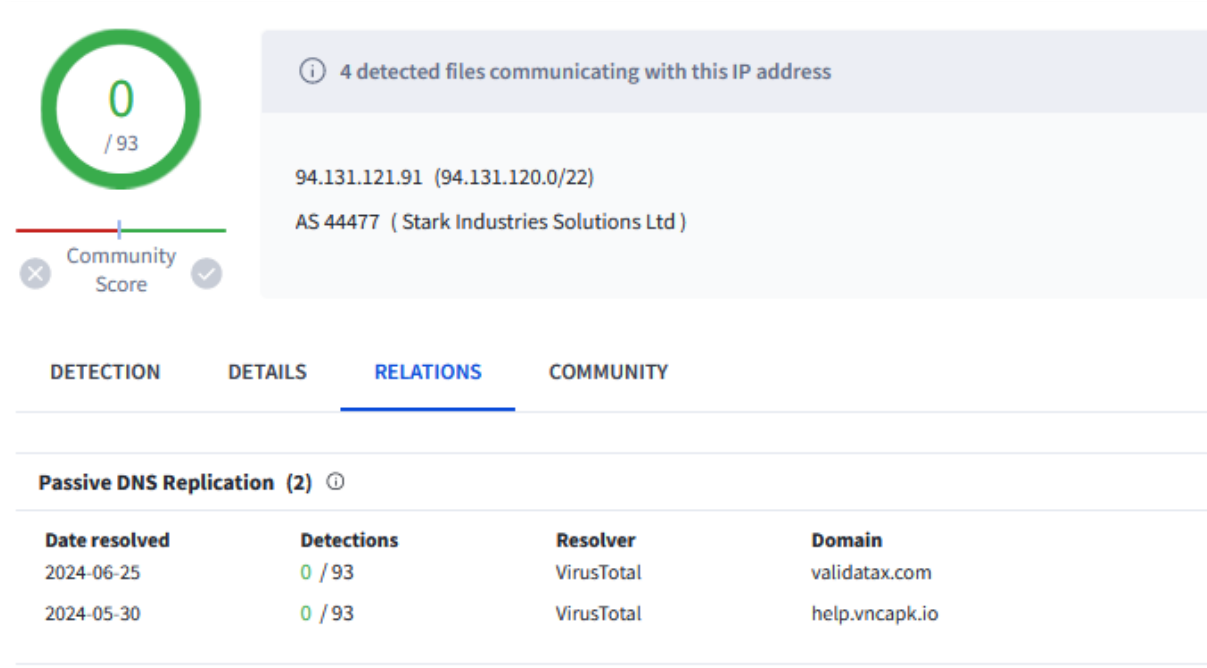


Figure 26: Stark Industries IP 94.131.121[.]91 used to host help.vncapk[.]io and now hosts validatax[.]com. Source: <https://www.virustotal.com/gui/ip-address/94.131.121.91/relations>

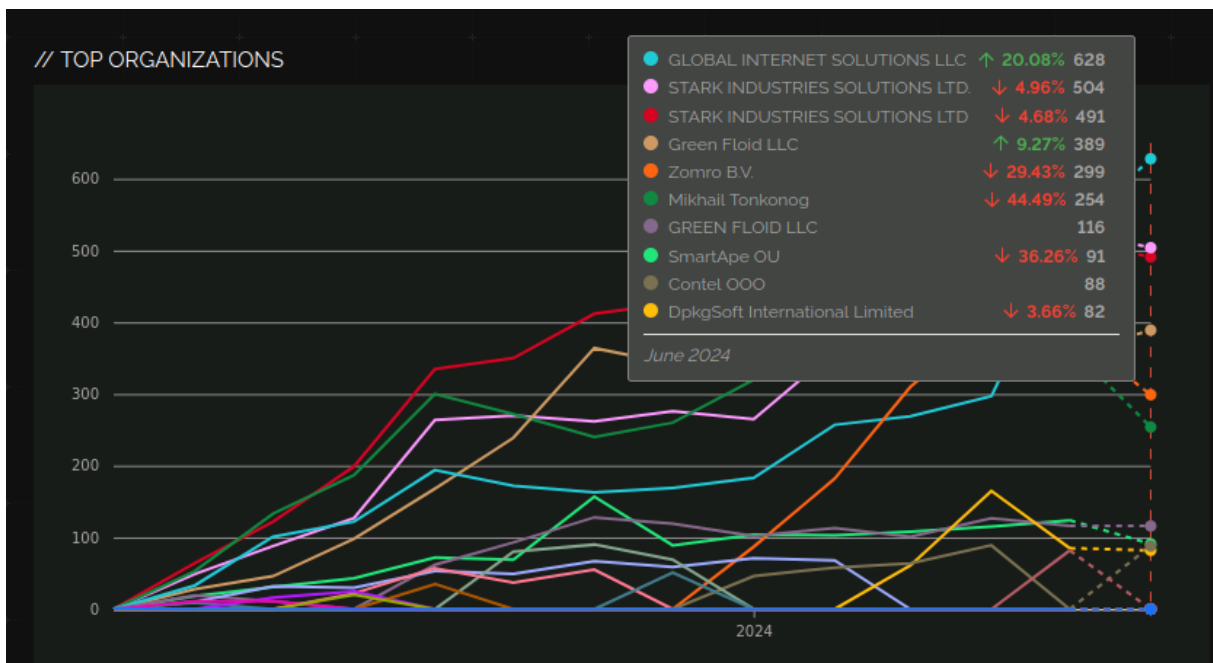


Figure 27: Top organizations for the golden image "WIN-BS656MOF35Q". Source: <https://trends.shodan.io/search?query=WIN-BS656MOF35Q&language=en#facet/org>

The domain anonvnc[.]com was created on 11 June 2024 which could indicate that this is a new service named "anonvnc" currently being created by the operator of "PandorahVNC".

A stalker in the box: infrastructure linking PandorahVNC and Mesh Central

TLP: CLEAR

PAP: CLEAR

```

Domain Name: ANONVNC.COM
Registry Domain ID: 2889762230_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.cloudflare.com
Registrar URL: https://www.cloudflare.com
Updated Date: 2024-06-11T21:09:18Z
Creation Date: 2024-06-11T21:09:14Z
Registrar Registration Expiration Date: 2025-06-11T21:09:14Z
Registrar: Cloudflare, Inc.
Registrar IANA ID: 1910
Domain Status: clienttransferprohibited https://icann.org/epp#clienttransferprohibited
Domain Status: addperiod https://icann.org/epp#addperiod
Registry Registrant ID:
Registrant Name: DATA REDACTED
Registrant Organization: DATA REDACTED
Registrant Street: DATA REDACTED
Registrant City: DATA REDACTED
Registrant State/Province: DE
Registrant Postal Code: DATA REDACTED
Registrant Country: US
    
```

Figure 28: Whois record for anonvnc[.]com showing a creation date of 11 June 2024.

2.3 Mesh Agent

On the IP hosting hiddenvnc and anonvnc (66.94.109[.]162), we found that two malicious files communicated with it.

URLs (7) ⓘ			
Scanned	Detections	Status	URL
2024-06-08	1 / 95	200	http://cloudfiles-secure-g0v.su/
2024-06-13	0 / 95	404	https://sync.anonvnc.com/w
2024-06-12	0 / 95	404	https://sync.anonvnc.com/J
2024-06-12	0 / 95	404	https://sync.anonvnc.com/n
2024-06-12	0 / 95	200	https://sync.anonvnc.com/
2024-06-12	0 / 95	-	http://sync.anonvnc.com:443/
2024-06-08	0 / 95	200	http://66.94.109.162/

Communicating Files (2) ⓘ			
Scanned	Detections	Type	Name
2024-06-12	15 / 73	Win32 EXE	C:\Program Files\Company\companyagent\companyagent.exe
2024-06-12	15 / 74	Win32 EXE	C:\Program Files\Company\companyagent\companyagent.exe

Figure 29: Two malicious files communicating with 66.94.109[.]162. Source: <https://www.virustotal.com/gui/ip-address/66.94.109.162/relations>

These files named “companyagent.exe” are detected as “mesh agent” by antivirus engines and communicated with URLs related to meshcentral and anonvnc/hiddenvnc.

A stalker in the box: infrastructure linking PandorahVNC and Mesh Central

TLP: CLEAR

PAP: CLEAR

Embedded URLs (x3) ⓘ

Scanned	Detections	Status	URL
2023-11-30	0 / 90	200	https://github.com/Ylianst/MeshAgent
2024-04-23	0 / 92	200	http://crl.usertrust.com/USERTrustRSACertificationAuthority.crl0v
2024-02-14	0 / 92	200	https://sectigo.com/CPS0
2024-04-23	0 / 92	200	http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t
2023-02-25	0 / 90	200	https://github.com/svaarala/duktape
2024-06-20	0 / 95	200	http://www.apache.org/licenses/LICENSE-2.0
2024-06-11	0 / 95	-	http://www.zlib.net/
2024-06-12	0 / 95	-	wss://sync.anonvnc.com/agent.ashx
2020-08-27	0 / 78	-	wss://meshcentral.com/agent.ashx
2023-06-21	0 / 90	-	wss://swarm.meshcentral.com/agent.ashx
2024-04-23	0 / 92	200	http://crt.usertrust.com/USERTrustRSAAddTrustCA.crt0%25
2024-05-07	0 / 92	301	http://opensource.org/licenses/MIT
2024-06-12	0 / 95	404	https://sync.anonvnc.com/0
2024-06-17	0 / 95	200	http://crl.sectigo.com/SectigoRSATimeStampingCA.crt0
2024-06-07	0 / 95	404	http://r10.i.lencr.org/0
2023-09-20	1 / 90	404	http://x1.c.lencr.org/(
2024-06-20	0 / 95	200	http://r10.i.lencr.org/
2024-06-19	0 / 95	200	http://x1.c.lencr.org/

Figure 30: Embedded URLs linked with anonvnc and meshcentral seen for the file "companyagent.exe". Source: <https://www.virustotal.com/gui/file/c20b47eddc855ce09628c26a53c81eca80b360e1a8207e67b26d040eff675f9f/relations>

Overall, many files named "MeshAgent.exe" communicated with the domains related to hiddenvnc and anonvnc.

Files Referring (11) ⓘ

Scanned	Detections	Type	Name
2024-06-20	10 / 66	Win32 EXE	meshagent
2024-06-15	36 / 73	Win32 EXE	sample_internalname
2024-06-15	31 / 74	Win32 EXE	sample_internalname
2024-06-13	1 / 74	Win32 EXE	C:\Program Files\Mesh Agent\MeshAgent.exe
2024-06-13	1 / 74	Win32 EXE	C:\Program Files\Mesh Agent\MeshAgent.exe
2024-06-12	1 / 74	Win32 EXE	3.xyz
2024-06-12	1 / 73	Win32 EXE	C:\Program Files\Mesh Agent\MeshAgent.exe
2024-06-12	1 / 74	Win32 EXE	C:\Program Files\Mesh Agent\MeshAgent.exe
2024-06-12	1 / 74	Win32 EXE	C:\Program Files\Mesh Agent\MeshAgent.exe
2024-06-12	15 / 74	Win32 EXE	C:\Program Files\Company\companyagent\companyagent.exe
2024-06-12	12 / 74	Win32 EXE	C:\Program Files\Mesh Agent\MeshAgent.exe

Figure 31: Files referring sync.anonvnc.com. Source: <https://www.virustotal.com/gui/domain/sync.anonvnc.com/relations>

This is particularly interesting as we found the logo of the website meshcentral[.]com on the website sync.hiddenvnc.com.

A stalker in the box: infrastructure linking PandorahVNC and Mesh Central

TLP: CLEAR

PAP: CLEAR

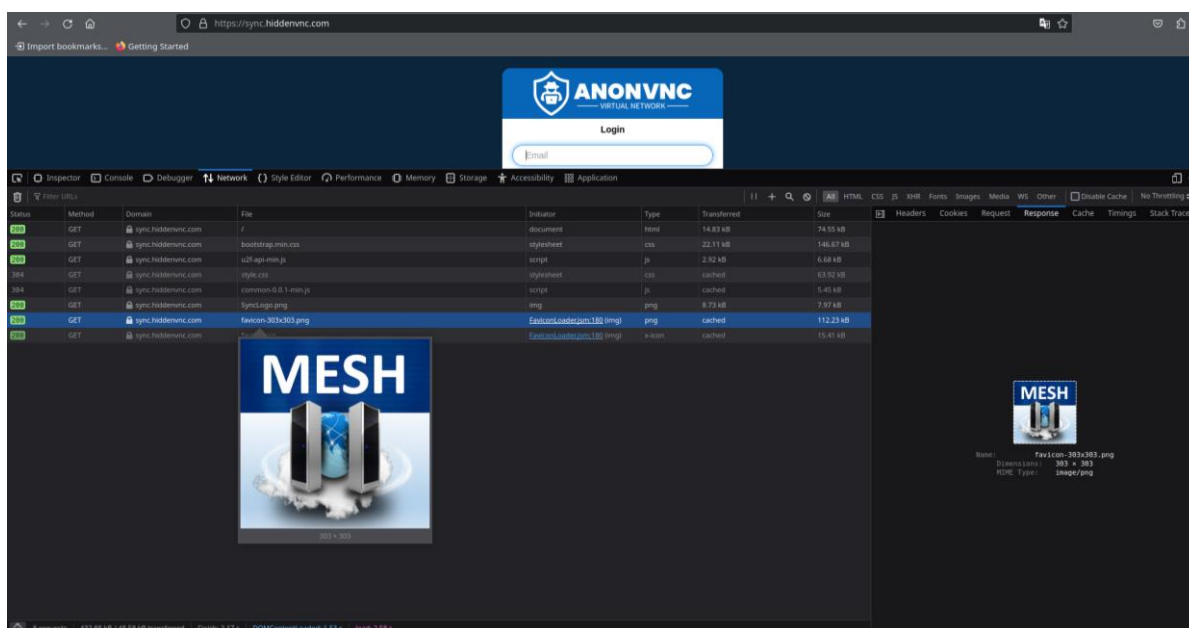


Figure 32: MeshCentral logo found inside sync.hiddenvnc.com.

MeshCentral is a legitimate open-source remote session manager that was leveraged by several intrusion sets (sometimes via [Tactical remote monitoring & management tool](#)):

- Upon an Emotet infection observed by [The DFIR Report](#) that led to Quantum ransomware
- [SparkRAT](#) and [Sliver C2](#) campaigns against Korean individuals
- a [LilacSquid campaign](#) that used Mesh Agent and QuasarRAT as primary implants to deploy customised malware after successfully compromising vulnerable application servers exposed to the internet
- an [Andariel \(Lazarus subgroup\) attack campaign](#)

In August 2022, user [@malmoeb on X](#) explained how this legitimate tool could be leveraged by malicious threat actors. [@1ZRR4H](#) also indicated in the case of Tactical RMM that it could be leveraged by the ransomware ecosystem operators as a C2.

These findings could indicate that the operator of PandorahVNC and Anonvnc could be testing MeshCentral for their toolkit.

On the IP address **66.94.109[.]162**, we also see that the domain **help.vncapk[.]io**. communicated with several files named “companyagent.exe” and a file named “MeshCentralAssistant.exe”.

A stalker in the box: infrastructure linking PandorahVNC and Mesh Central

TLP: CLEAR

PAP: CLEAR

Communicating Files (4) ⓘ

Scanned	Detections	Type	Name
2024-06-03	1 / 74	Win32 EXE	companyagent64-root (2).exe
2024-06-05	4 / 73	Win32 EXE	C:\Program Files\Company\companyagent\companyagent.exe
2024-06-03	1 / 74	Win32 EXE	C:\Program Files\Company\companyagent\companyagent.exe
2024-06-09	3 / 72	Win32 EXE	invoice#251561.exe

Files Referring (5) ⓘ

Scanned	Detections	Type	Name
2024-06-19	2 / 74	Win32 EXE	MeshCentralAssistant.exe
2024-06-09	3 / 72	Win32 EXE	invoice#251561.exe
2024-06-05	4 / 73	Win32 EXE	C:\Program Files\Company\companyagent\companyagent.exe
2024-06-03	1 / 74	Win32 EXE	companyagent64-root (2).exe
2024-06-03	1 / 74	Win32 EXE	C:\Program Files\Company\companyagent\companyagent.exe

Figure 33: Malicious files communicating with help.vncapk[.]io. Source: <https://www.virustotal.com/gui/domain/help.vncapk.io/relations>

Querying the URL sync.anoncvnc.com/0 found communicating with [this file](#) redirects us to a 404-page titled “AnonVNC – Download” exposing the logo of MeshCentral.

A stalker in the box: infrastructure linking PandorahVNC and Mesh Central

TLP: CLEAR

PAP: CLEAR

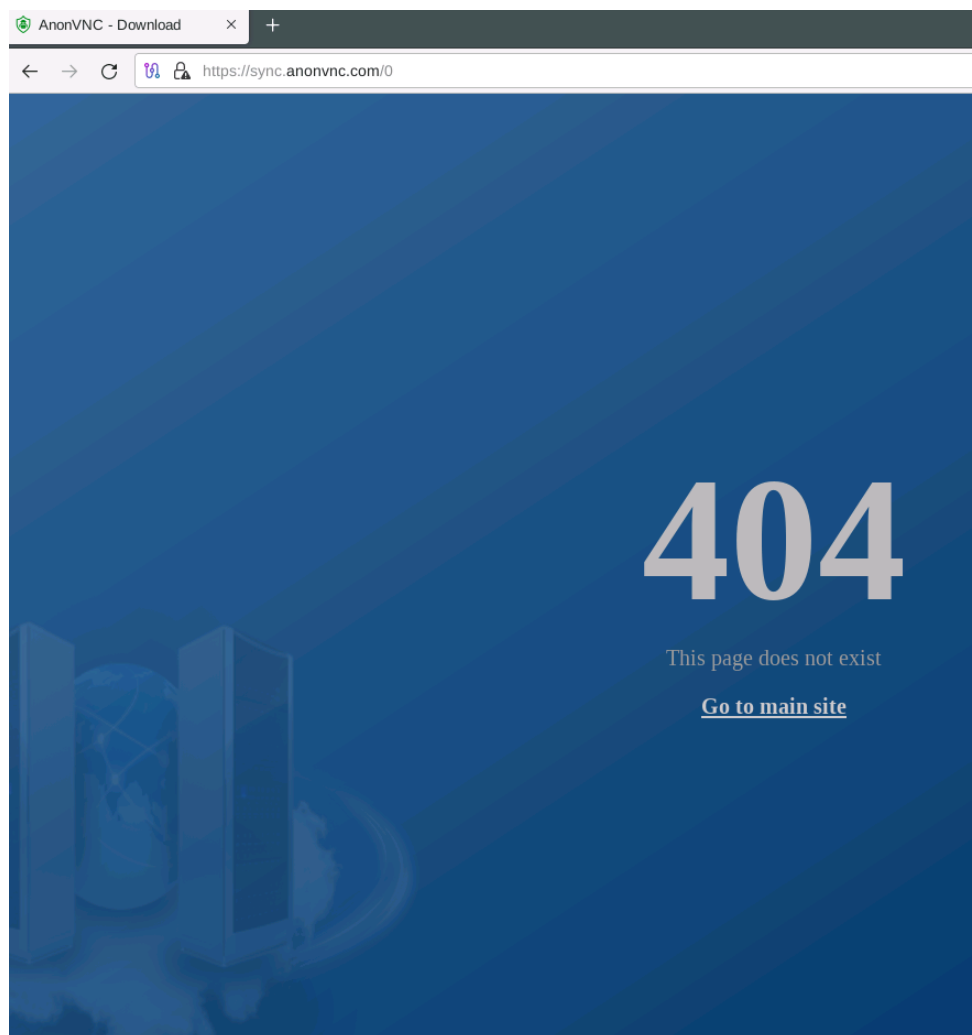


Figure 34: 404 page titled “anonvnc – download” and exposing the logo of MeshCentral.

3. Technical Analysis of Mesh Agent

We then decided to analyse one of the Mesh Agent file (named “[invoice#251561.exe](#)”) to see how it interacts with the “vnc” domains. This file appeared to be more ready to be weaponised in a campaign, as contrary to the others it had a name that could be used in a phishing attempt.

The file is a PE (Portable Executable) 64-bit with a size of 6 MB and described as “MeshCentral Background Service Agent”. In the .data section we can identify in cleartext the different switches available for Mesh Agent:

A stalker in the box: infrastructure linking PandorahVNC and Mesh Central

TLP: CLEAR

PAP: CLEAR

```

Mesh Agent available switches:\r\n
run      Start as a console agent.\r\n
start    Start the service.\r\n
restart  Restart the service.\r\n
stop     Stop the service.\r\n
state    Display the running state of the service.\r\n
-signcheck Perform self - check.\r\n
-install Install the service from this location.\r\n
-uninstall Remove the service from this location.\r\n
-nodeid  Return the current agent identifier.\r\n
-info    Return agent version information.\r\n
-resetnodeid Reset the NodeID next time the service is started.\r\n
-fulluninstall Stop agent and clean up the program files location.\r\n
-fullinstall Copy agent into program files, install and launch.\r\n
The following switches can be specified after -fullinstall:\r\n
--WebProxy="http://proxyhost:port" Specify an HTTPS proxy.\r\n
--agentName="alternate name" Specify an alternate name to be provided by the age...
    
```

Figure 35: Switches mentioned in the .data section of the Mesh Agent file.

We also identified strings related to WSS connections to the URLs **meshcentral[.]com:443/agent.ashx** and **swarm.meshcentral[.]com:443/agent.ashx**. [WSS](#) is used for WebSocket connections over TLS that enables a persistent connection between the client and server, which is especially useful in the context of a remote connection using Mesh Agent.

Address	Length	Type	String
.data:00000001...	0000002B	C	wss://swarm.meshcentral.com:443/agent.ashx
.data:00000001...	00000025	C	wss://meshcentral.com:443/agent.ashx
.data:00000001...	00000025	C	wss://meshcentral.com:443/agent.ashx
.data:00000001...	00000025	C	wss://meshcentral.com:443/agent.ashx
.data:00000001...	00000025	C	wss://meshcentral.com:443/agent.ashx

Figure 36: Strings related to wss connection to meshcentral domains.

This file is signed by “Siam Computer (MD Kamrul Hassan)”, but in [another Mesh Agent file](#) that communicated with the same domains as above using WSS, we found that it was signed by “sync.anonvnc.com-96954f” on 11 June 2024.

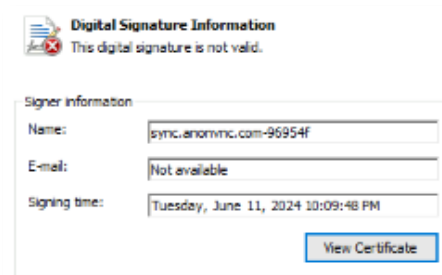


Figure 37: Certificate of the Mesh Agent file signed by sync.anonvnc.com-96954f.

A stalker in the box: infrastructure linking PandorahVNC and Mesh Central

TLP: CLEAR

PAP: CLEAR

In fact, it was issued by “**MeshCentralRoot-ad3a9c**” to “**sync.anonvnc.com-96954f**”. MeshCentralRoot is the [default issuer name used by meshcentral\[.\]com](#).

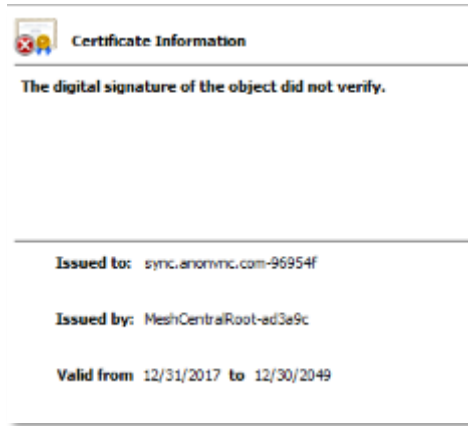


Figure 38: The certificate is issued by MeshCentralRoot-ad3a9c.

Searching for certificates signed by the subject name “sync.anonvnc[.]com” we find 12 files on VirusTotal, which correspond more or less to the files seen referring to sync.anonvnc[.]com. These files were first seen between the 12 and 13 June 2024, and last seen until 15 June 2024. They were signed by “sync.anonvnc.com-96954f” and “sync.anonvnc.com-d7add5”, issued by “MeshCentralRoot-ad3a9c” and “MeshCentralRoot-6dc5c6”.

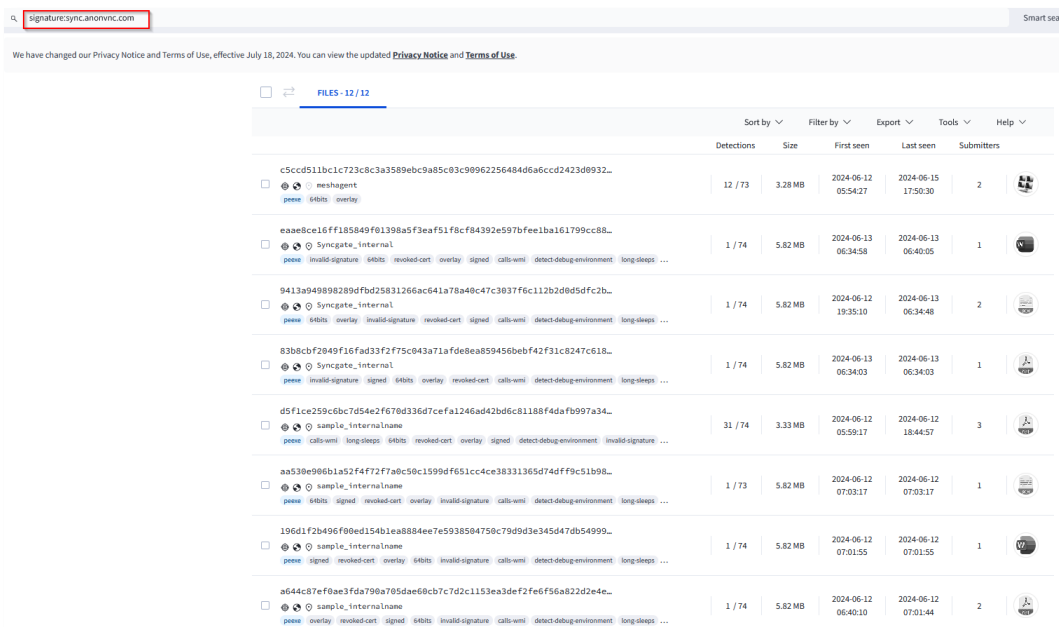



Figure 39: 12 files signed by certificates mentioning “sync.anonvnc.com”. Source: <https://www.virustotal.com/gui/search/signature%253A%5Csync.anonvnc.com/files>

Additionally, we found a discriminant certificate issued by “**MeshCentralRoot-ad7d56**” on port 4433 of the IP addresses 94.131.121[.]91 and 66.94.109[.]162 (exposing AnonVNC’s login panels):

A stalker in the box: infrastructure linking PandorahVNC and Mesh Central

TLP: CLEAR

PAP: CLEAR

```
// 4433 / TCP 

HTTP/1.1 200 OK
Host: 94.131.121.91
Connection: keep-alive
Cache-Control: no-cache
Content-Type: text/html
Content-Length: 150

SSL Certificate

Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 22301258004 (0x531423114)
    Signature Algorithm: sha384WithRSAEncryption
    Issuer: CN=MeshCentralRoot-ad7d56, O=unknown, C=unknown
    Validity
      Not Before: Jan  1 08:00:00 2018 GMT
      Not After : Dec 31 08:00:00 2049 GMT
    Subject: CN=validatax.com
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      Public-Key: (2048 bit)
```

Figure 40: Certificate issued by "MeshCentralRoot-ad7d56" on port 4433 of IP address 94.131.121.9. Source: <https://www.shodan.io/host/94.131.121.91#4433>.

A stalker in the box: infrastructure linking PandorahVNC and Mesh Central

TLP: CLEAR

PAP: CLEAR

To summarize, here are the different interactions we observed between the owner of PandorahVNC, MeshCentral's Mesh Agent, and the infrastructure linking the different files and services:

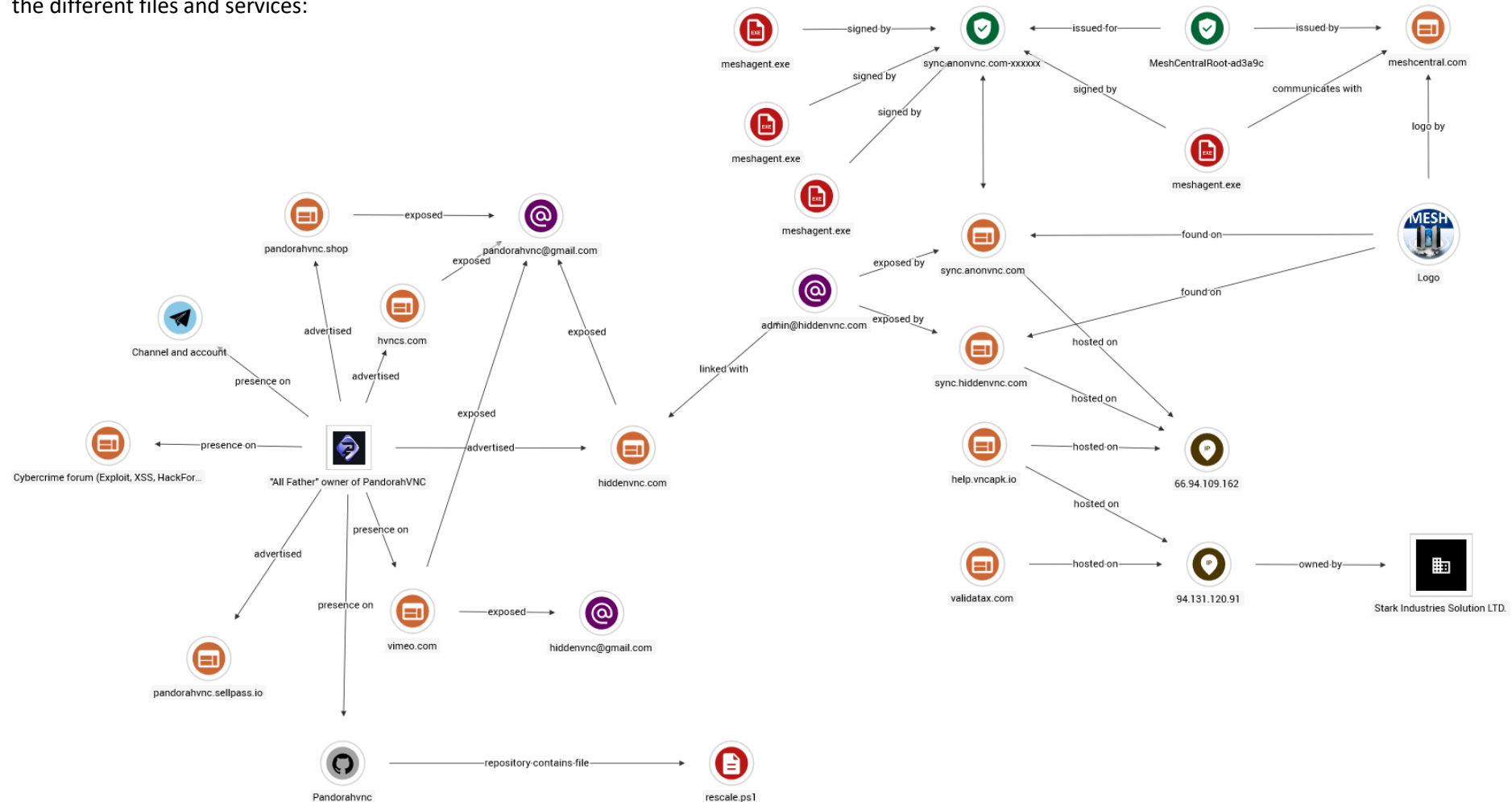


Figure 41: Summary of the interactions presented in this analysis.

A stalker in the box: infrastructure linking PandorahVNC and Mesh Central

TLP: CLEAR

PAP: CLEAR

III. Actionable content

1. Indicators of compromise

Value	Type	Description
hiddenvnc[.]com	Domain	PandorahVNC website
hvncs[.]com	Domain	PandorahVNC website
pandorahvnc[.]shop	Domain	PandorahVNC website
pandorahvnc.sellpass[.]io	Domain	PandorahVNC website
sync.hiddenvnc[.]com	Domain	Anonvnc login panel
sync.anonvnc[.]com	Domain	Anonvnc login panel
help.vncapk[.]io	Domain	Anonvnc linked domain
vncapk[.]io	Domain	Anonvnc linked domain
anonvnc[.]com	Domain	Anonvnc linked domain
admin@hiddenvnc[.]com	Email address	Email found on the login panel of anonvnc and hiddenvnc
hiddenvnc@gmai[.]com	Email address	Pandorahvnc contact
pandorahvnc@gmail[.]com	Email address	Pandorahvnc contact
allfather@jabb3r[.]org	Jabber	Pandorahvnc contact
https://raw.githubusercontent.com/PandorahVNC/PhotoCollection/main/rescale.ps1	URL	Powershell script "rescale.ps1"
51.254.27[.]112	IPv4	Old Pandorahvnc C2
141.95.6[.]166	IPv4	Old Pandorahvnc C2
62.112.11[.]136	IPv4	Old Pandorahvnc C2
f1d3101037bcc5a9bd44965dd034b44d2a398d065d8455729a8f6dbf6cfb7a7	SHA-256	Skra.jpg
66.94.109[.]162	IPv4	Sync.hiddenvnc and sync.anonvnc
94.131.121[.]91	IPv4	Help.vncapk.io and validatax.com
validatax[.]com	Domain	Anonvnc linked domain
ffe56455e38a56d76dbcb70c399137a8d0241c7ff733c9890a99f6b40707148	SHA-256	invoice#251561.exe (meshagent) communicating with help.vncapk.io
fb6cd1db1653f35b24fd9813ff0f449e4bbefdb183124dabd65e0ef1a7d19e0d	SHA-256	Companyagent64-test.exe (meshagent) communicating with sync.anonvnc.com
c20b47eddc855ce09628c26a53c81eca80b360e1a8207e67b26d040eff675f9f	SHA-256	Companyagent.exe (meshagent) communicating with sync.anonvnc.com
83684d44cf2d30951b45a3560b6387a82aebbad7242c3334996f4c55994c543b	SHA-256	Companyagent.exe (meshagent) communicating with help.vncapk.io
040cef4a919bf259e750029187dcfeff8b4b8f18e6a65cb401ee941d7999dd51	SHA-256	Stub.exe
0351128bc2273d12ca8042b029f9081c9205e2adad3a12f70a5696d23a6a036e	SHA-256	Stub.exe
eaae8ce16ff185849f01398a5f3eaf51f8cf84392e597bfee1ba161799cc8888	SHA-256	Syncgate_internal.exe (meshagent) communicating with sync.anonvnc.com

A stalker in the box: infrastructure linking PandorahVNC and Mesh Central

TLP: CLEAR

PAP: CLEAR

9413a949898289dfbd25831266ac641a78a40c47c3037f6c112b2d0d5dfc2b75	SHA-256	Syncgate_internal.exe (meshagent) communicating with sync.anonvnc.com
53fdb0af9e57a87eb52512efec8eb2a4482a70273bb8469d80c8eacea271d33	SHA-256	Companyagent64-root.exe (meshagent) communicating with help.vncapk.io
83b8cbf2049f16fad33f2f75c043a71afde8ea859456bebf42f31c8247c61876	SHA-256	Syncgate_internal.exe (meshagent) communicating with sync.anonvnc.com
vncgoga.duckdns.org	Domain	Pandorahvnc C2 (Fortinet campaign)
d74fd3b348cda03bfec1f94e675c40a6cf32b9f9b0e6cc7c628813df9f449eb9	SHA-256	Stub.exe (Fortinet campaign)
sync.anonvnc[.]com-96954f	Certificate	Certificate subject name
sync.anonvnc[.]com-d7add5	Certificate	Certificate subject name
d5f1ce259c6bc7d54e2f670d336d7cefa1246ad42bd6c81188f4dafb997a342a	SHA-256	Meshagent.exe
aa530e906b1a52f4f72f7a0c50c1599df651cc4ce38331365d74dff9c51b98fb	SHA-256	Meshagent.exe
196d1f2b496f00ed154b1ea8884ee7e5938504750c79d9d3e345d47db5499980	SHA-256	Meshagent.exe
a644c87ef0ae3fda790a705dae60cb7c7d2c1153ea3def2fe6f56a822d2e4e9e	SHA-256	Meshagent.exe
4c9aad477ebdd6bbc57a746b43db4fa1398f4f998e8ebf6e26e10ec5dccb9e68	SHA-256	Meshagent.exe
4bb2a508148f1895c0371293b6430f18a4083e753e0901dc6257b9d16114f28e	SHA-256	Meshagent.exe

2. Recommendations

- Block the indicators in the IOC section of this analysis

Meshcentral

As far as meshcentral RMM threat hunting is concerned, one could search for:

- "agent.ashx" in the proxy logs for hunting MeshCentral network connections

Windows Event ID 7045 corresponding to a new installation of a service in the system (service name: Mesh Agent). A [sigma rule](#) allows to detects a TacticalRMM service installation.

Besides, Meshcentral is sometimes embedded in [Tactical RMM](#), which uses Golang written agents and that also should be monitored closely.

We advise to pay close attention to other known [Remote Access Software](#) reported in the MITRE Attack framework.

3. Sources

- <https://slashnext.com/blog/silent-yet-powerful-pandora-hvnc-the-popular-cybercrime-tool-that-flies-under-the-radar/>
- <https://cip.gov.ua/en/news/p-yat-khakerskikh-ugrupuvan-yaki-naichastishe-atakuyut-ukrayinu>
- https://www.fortinet.com/blog/threat-research/phishing-campaign-delivering-fileless-malware-part-two?&web_view=true