2025 BERLIN

24 - 26 September, 2025 / Berlin, Germany

TA PHONE HOME: EDR EVASION TESTING REVEALS EXTORTION ACTOR'S TOOLKIT

Navin Thomas, Renzon Cruz & Cuong Dinh

Palo Alto Networks, USA

nthomas@paloaltonetworks.com
rcruz@paloaltonetworks.com
cdinh@paloaltonetworks.com

ABSTRACT

In a recent investigation involving an extortion attempt, we discovered a threat actor had purchased access to the client network via *Atera* Remote Monitoring and Management (RMM) from an initial access broker. We discovered the threat actor used rogue systems to install the old version of *Cortex XDR* agent onto a virtual system. They did this to test a new anti-virus/endpoint detection and response (AV/EDR) bypass tool, leveraging the bring-your-own-vulnerable-driver (BYOVD) technique [1].

Connectivity between the threat actor's rogue systems and the client's EDR platform inadvertently gave *Unit 42* investigators a certain level of access to the rogue systems. This provided visibility into various tools and files held by the threat actor. While the threat actor intended to find a way to bypass *Cortex*, in actuality this activity helped *Unit 42* protect other organizations by providing unique visibility into the threat actor's tooling, targeting and persona.

In this report, we provide an overview of the attack that occurred, details about the AV/EDR bypass tool, and its sale on cybercrime forums. Most importantly, we present a walkthrough of how *Unit 42* researchers managed to unmask one of the threat actors involved. We'll give a peek into all the discoveries related to the identification of the threat actor.

OVERVIEW

Unit 42 was called to assist with an extortion incident. Through the investigation process, we encountered two endpoints involved in the attack that were unknown to the client environment.

As a means to test an AV/EDR bypass tool, threat actors installed older versions of *Cortex XDR* agents on these endpoints. Unbeknownst to the threat actor, we were able to access these rogue endpoints.

We also discovered a series of toolkits and other files belonging to the threat actor on the system, which included a bypass tool. We successfully traced and identified posts related to the sale of this specific tool on cybercrime forums like XSS and Exploit.

Using files obtained from the rogue endpoints and subsequent investigation, we discovered the true identity of one of the threat actors involved in the incident. We also found additional information about the individual's personal and professional background.

Figure 1 presents a high-level chain of events in the attack investigated by *Unit 42*.

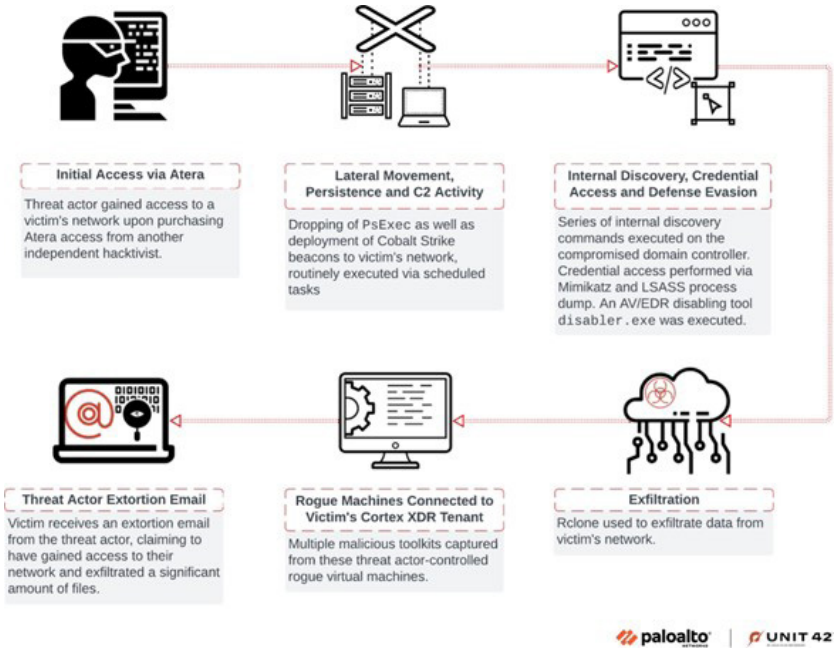

Figure 1: High-level chain of events for this attack.

AV/EDR BYPASS TOOL

The bypass tool, named `disabler.exe`, appears to use the publicly available source code from EDRSandBlast [2] with small modifications and removal of the CLI features. As shown in Figures 2 and 3, clear similarities can be seen between strings from the EDRSandBlast source code files and strings in `disabler.exe`.

The tool's primary function is to target and remove EDR hooks in user-mode libraries and kernel-mode callbacks. It includes a companion file, `wnbios.sys` or `WN_64.sys`, which is a vulnerable driver that the tool attempts to load and gain access to.

Figure 2: Snippet of some of the strings printed by EDRSandBlast.

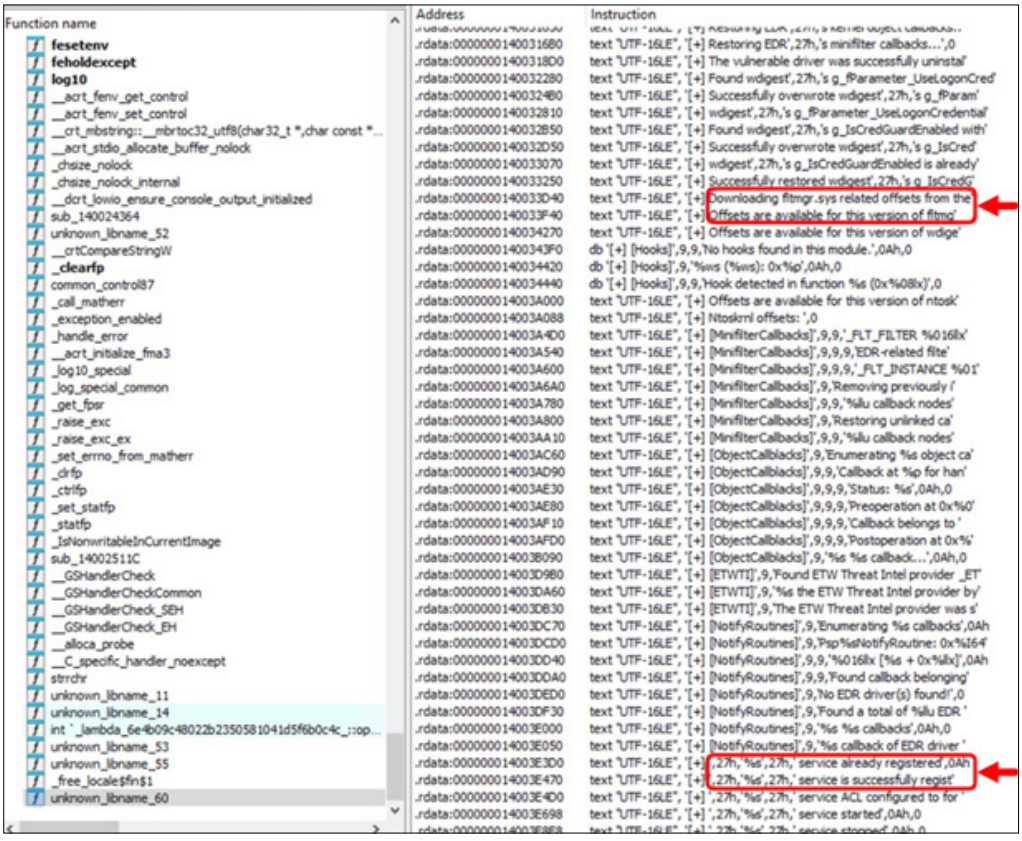

Figure 3: The same strings seen in the disabler.exe static library.

Based on certain files and folders found on one of the rogue endpoints, we searched cybercrime forums such as XSS and Exploit to identify the likely seller of this bypass tool.

Identifying the seller of the bypass tool

The rogue system had a hostname of `DESKTOP-J8AOTJS` and contained several directories with interesting names – shown below in Figure 4 – under the file path `Z:\freelance`. This led us to the hypothesis that these were names or monikers of various other affiliates.

Figure 4: List of folders in Z:\freelance on the rogue system.

With that in mind, we searched cybercrime forums for usernames matching any of the directory names under `Z:\freelance`. While some of them were either too noisy or didn't return any result at all, others did return some interesting hits. The matching names are consistently posted either in Russian, or in Russian-based cybercrime forums, the most common being XSS and Exploit.

The username that piqued our interest the most was Marti71. This username posted in multiple places looking for tools to bypass AV/EDR. Figure 5 shows one such example, with the post translated to English as follows:

```
Greetings, everyone!

Does anyone have an out-of-the-box solution to kill antivirus software? I'm ready to
purchase several solutions with regular support/subscription.
```

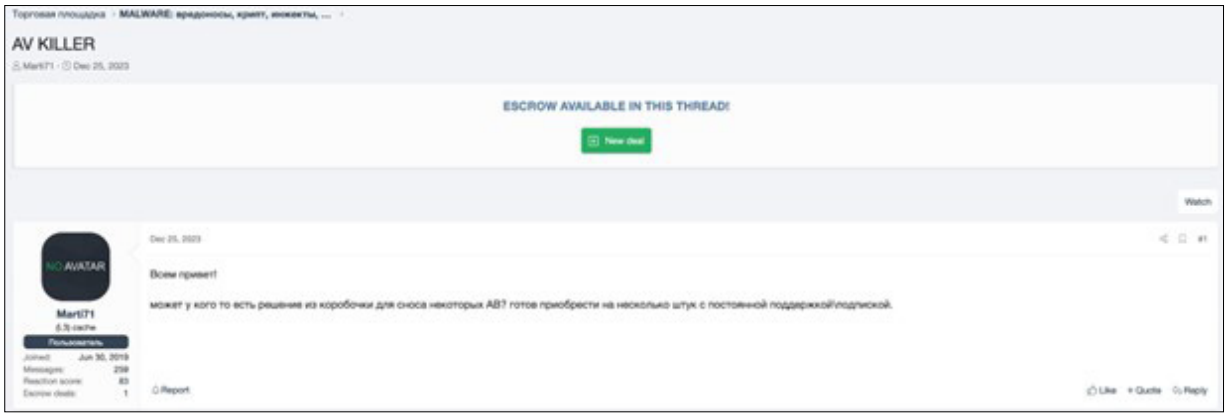

Figure 5: Marti71 enquiring about anti-virus-killing software.

The final post on this thread was from a user account named KernelMode, who suggested an AV/EDR bypass tool.

Figure 6: User KernelMode suggesting an AV/EDR bypass tool.

Pivoting to the link in KernelMode's post in Figure 6, we found a thread that KernelMode had initiated in order to sell subscriptions to an AV/EDR bypass tool, as shown in Figure 7. However, the post contains nothing that would confirm that the person or people behind KernelMode are the developers of this bypass tool.

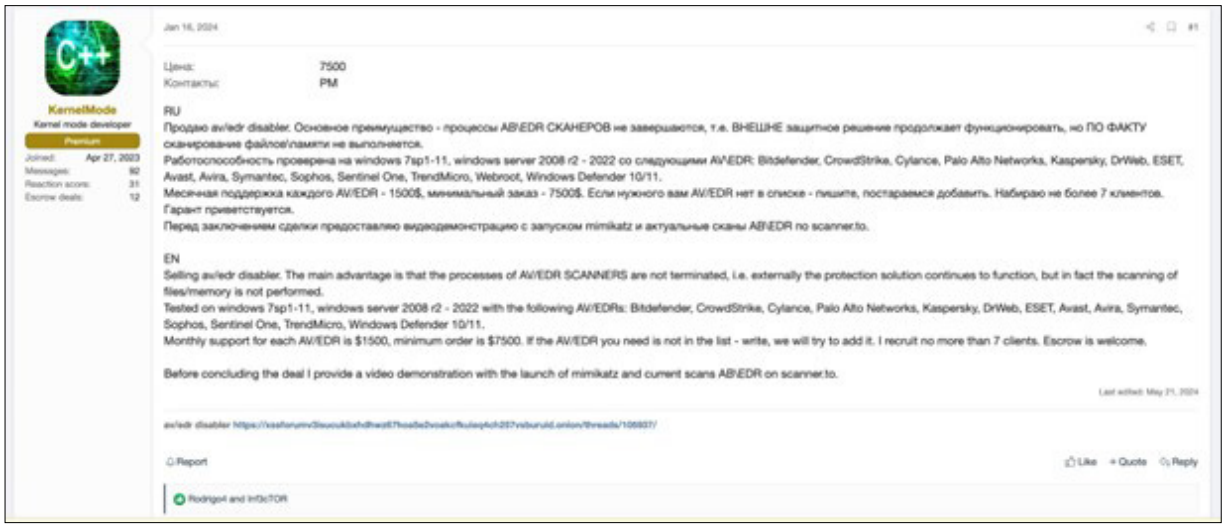

Figure 7: KernelMode posting about the sale of an AV/EDR bypass tool.

Marti71 also posted on this thread, as shown in Figure 8, seeming to indicate a positive experience with the tool.

Marti71s Russian language post translates to "`In general, it will go, finishing some moments, trying to speed up. Bitdef/sentic fly off quickly.`".

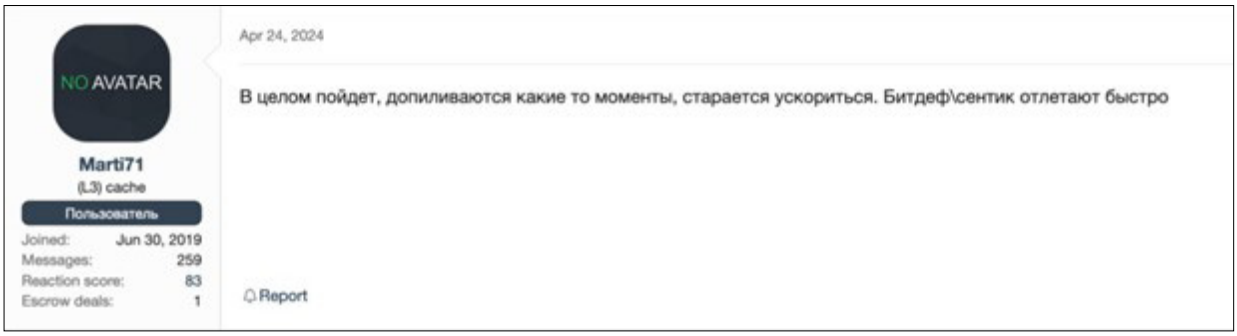

Figure 8: Marti71's comment on the bypass tool.

Returning to KernelMode's post, the actor mentions at the end of the post that they will provide a video demonstration. We were able to procure an archive of multiple recordings demonstrating the tool. Each recording shows a particular AV/EDR agent installed during the recording that included the actor executing the bypass tool and successfully executing Mimikatz. The intent of the demonstration is to illustrate that the AV/EDR agent has been bypassed to some extent.

We found files for such tool demonstration recordings on the rogue system as well. Comparing the recordings on the rogue system with recordings from KernelMode revealed they were the same. Figure 9 shows a screenshot from one of the recordings.

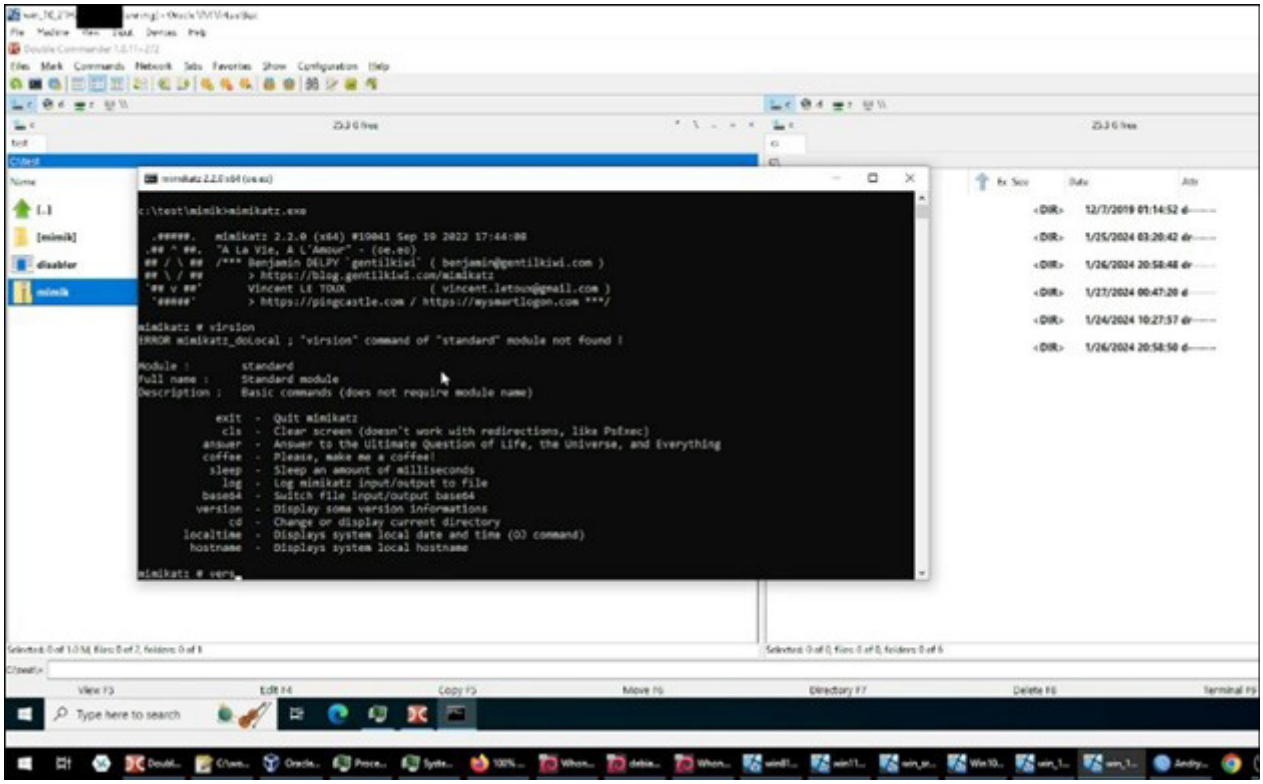

Figure 9: Snippet of the AV/EDR bypass tool demonstration video from KernelMode, also on the rogue system.

PEEK INTO THE ROGUE SYSTEM

Overview of tools and files

We retrieved a portion of files from the shared `Z:\` drive of the rogue system `DESKTOP-J8AOTJS`. Figure 10 shows some of the files we captured.

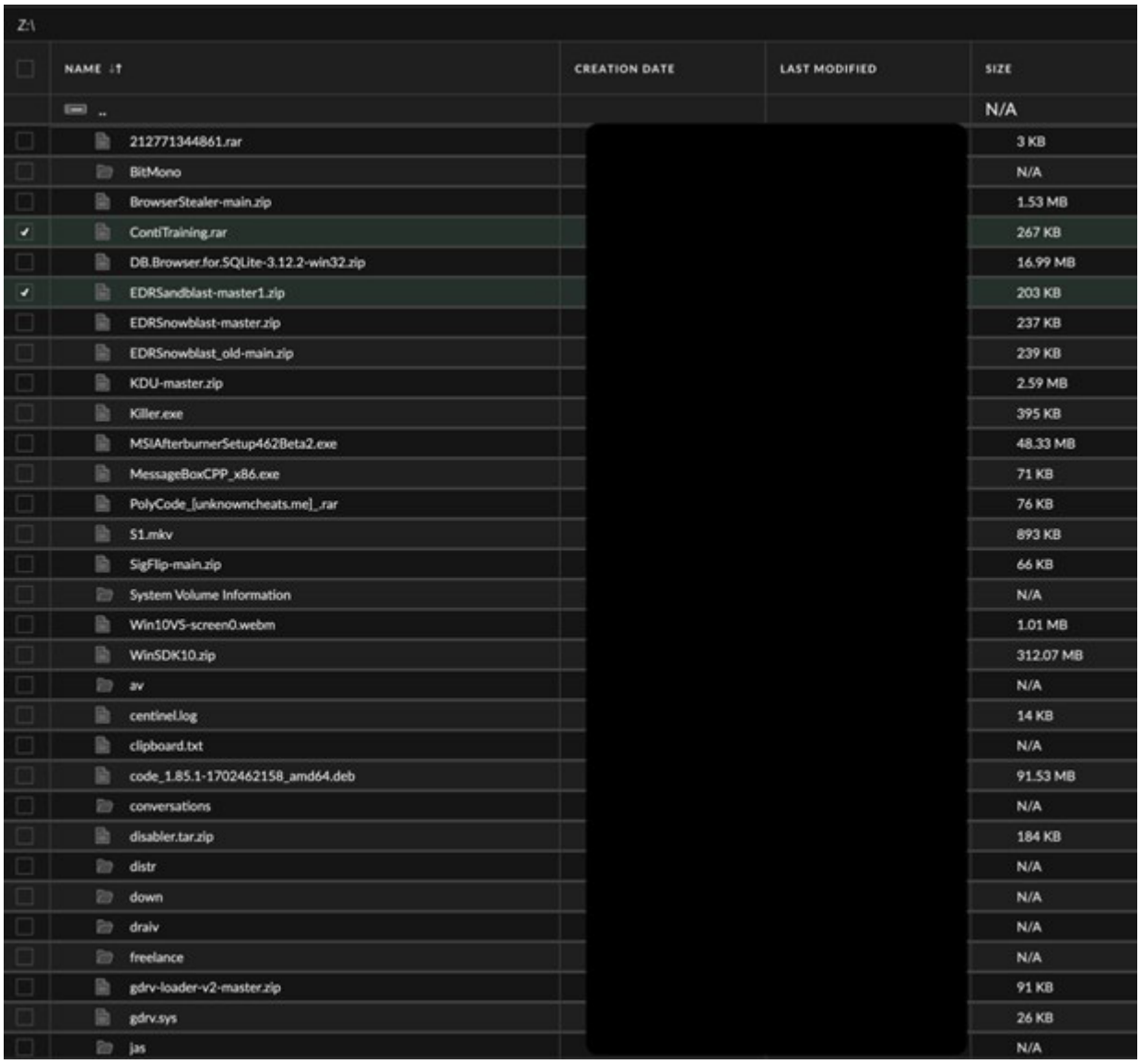

Figure 10: Files and folders on the root path.

Highlights of the captured material include:

- An encrypted archive file, `ContiTraining.rar`, was present in the system.
- The extracted archive contained a torrent file named `ContiTraining.torrent` that was created on 14 August 2021.
- This torrent file would reach out to the following servers to download the Conti playbook that was publicly leaked [3] in 2021:
  - `udp[://]tracker.coppersurfer[.]tk:6969`
  - `udp[://]9.rarbg[.]to:2920`
  - `udp[://]tracker.opentrackr[.]org:1337`
  - `udp[://]tracker.leechers-paradise[.]org:6969`
  - `udp[://]exodus.desync[.]com:6969`
- Files specified by `ContiTraining.torrent` to download:
  - `Кряк 2019.rar`
  - `Метасплоит US.rar`

  - Метасплоит RU.zip
  - Network Pentesting.rar
  - Cobalt Strike.rar
  - Powershell for Pentesters+.rar
  - Windows Red Team Lab+.rar
  - WMI Attacks and Defense +.rar
  - Abusing SQL Server Trusts in a Windows Domain+.rar
  - Attacking and Defending Active Directory+.rar
  - GCB.zip
  - GeekBrayns Реверс-инжиниринг.rar
- A folder with files containing personally identifiable information (PII) and other confidential information on one individual, such as:
  - Their name
  - Device details
  - Phone number
  - An account number
  - A two-factor authentication-based key
- Multiple copies of the AV/EDR bypass tool along with video demonstrations, as explained above.
- Various builds of the Mimikatz tool, probably for the purposes of testing out the AV/EDR bypass tool.
- Various tools that were sourced either from *GitHub* or from underground forums, with functionalities such as:
  - Generating and executing shellcode
  - Kernel driver utilities
  - Obfuscating code
  - Bypassing protection
  - Bypassing anti-cheat
- A presentation deck by a researcher from a Russian institute on compiler obfuscation.
- An installer and multiple other files pertaining to an EDR product, also likely used for testing the AV/EDR bypass tool.
- A text file with escrow payment details (shown in Figure 11)

Figure 11: Text file with payment information.

- Another text file containing a long list of host IP addresses along with their credentials.
  - A portion of those credentials likely corresponds to various compromised hosts.

One file from the rogue system that caught our attention was `P-1 (акт выполненных работ) № <redacted> от <redacted>.xls`, which translates to 'act of completed work'. The spreadsheet contains a 'P-1 form' for a transaction between two limited liability companies based in Kazakhstan, as shown in Figure 12.

According to a post on the government procurement site for the Republic of Kazakhstan [4], the P-1 form is used to document completed work, services rendered, invoices (as in this case), and other related items. The name of one of the companies, along with its business identifier number (BIN), exposed in this document reveals a piece of information that is vital when it comes to threat actor profiling. This specific form shows the organization submitting an expense for renting 30 *Mercedes* cars.

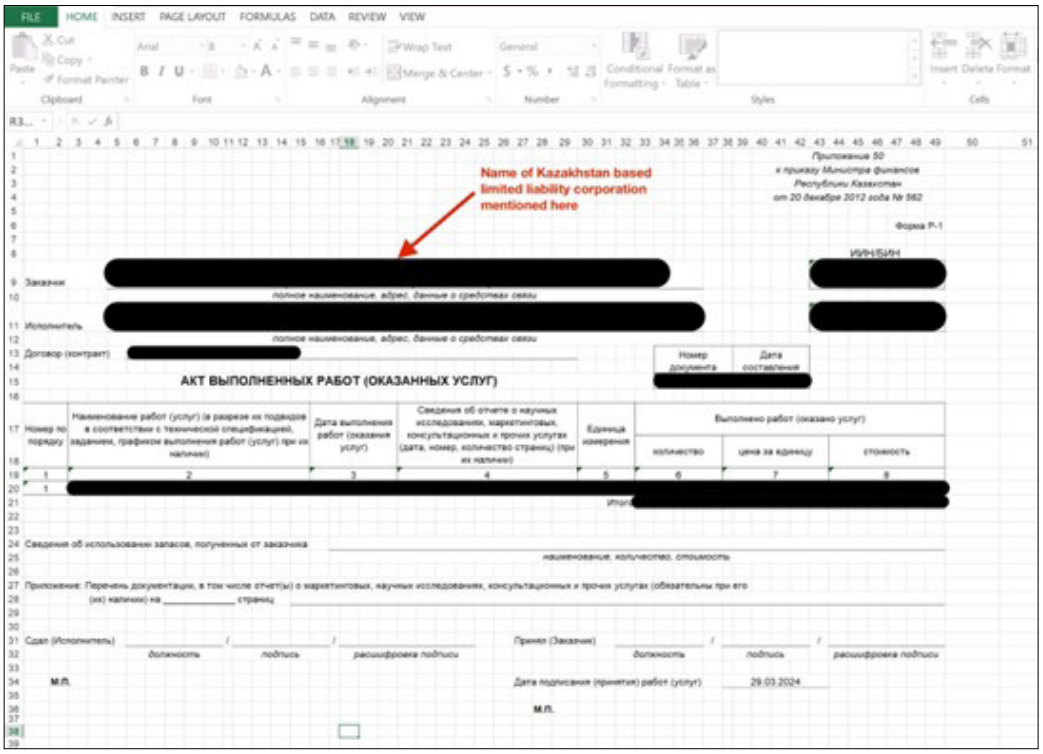

Figure 12: P-1 form recovered from the rogue system.

Artifacts from AV/EDR bypass tool recording

We previously mentioned the presence of multiple video files demonstrating the AV/EDR bypass tool against various endpoint protection products. These files are identical to the ones provided by the user account named KernelMode on various cybercrime forums.

We found the video recording shown in Figure 13 and noted a few relevant details on an AV/EDR agent panel and the taskbar of the host machine.

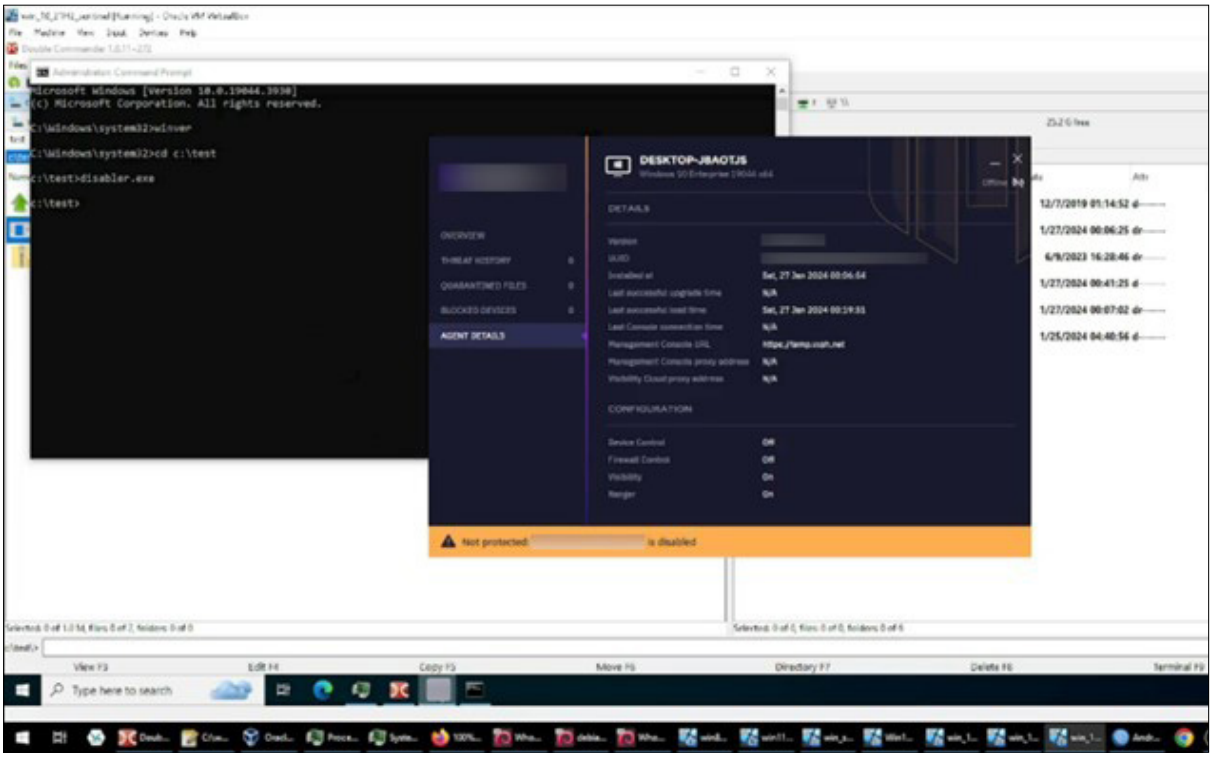

Figure 13: Screenshot of an AV/EDR bypass tool video demonstration.

Our observations based on the video noted in Figure 13 include:

- The AV/EDR bypass tool is being tested in a virtual machine and is accessible via *Oracle VM VirtualBox*. Looking at the taskbar of the host machine (as shown at the bottom of Figure 13), it appears that the individual recording the demonstration video is accessing multiple instances of virtual machines.
- The virtual machine hostname displayed on the AV/EDR agent panel is `DESKTOP-J8AOTJS`. This also happens to be the hostname of the rogue system behind the attack that we managed to capture. With this piece of information, we can confirm that the rogue system is a virtual machine.
- The management console URL on the agent panel seems rather unconventional: `https[://]temp.vxsh[.]net`. A quick search on this domain reveals a *Telegram* channel where a user shared a fake token to install the AV/EDR agent. Base64-decoding of the fake token unveils that exact URL. We cannot confirm if the agent can still be installed via this particular fake token.
- Looking at the titles of open applications in the *Windows* taskbar in the host machine, the first one from the right (next to the *Google Chrome* icon) is incomplete but appears to show a name beginning with 'Andr'.
- While going through the remaining videos, we identified the same application in the taskbar. But this time, the first word, 'Andry', is visible in the title 'Andry-ad…', as shown in Figure 14. The icon indicates this application is likely *WinBox* [5], a utility used to remotely log into and administer *Mikrotik* routers. We believe that 'Andry' is part of the username logged into a *Mikrotik* router.

Figure 14: Snippet of a Windows taskbar from one of the demonstration videos.

- As shown above in Figure 14, another application visible in the taskbar is *OBS Studio* [6], a free and open-source tool for video recording and live streaming. Threat actors often abuse, take advantage of or subvert legitimate products for malicious purposes. This does not imply that the legitimate product is flawed or malicious.

Browser history

Through *Cortex XDR* we got a peek into *Edge* browser activity on `DESKTOP-J8AOTJS`, as shown in Figure 15. We observed that the adversary's operations included visiting the following websites to search for and download certain tools such as *Process Hacker* [7] and *Double Commander* [8].

- `ya[.]ru`: *Yandex* (Russian-based search engine)
- `sourceforge[.]net`

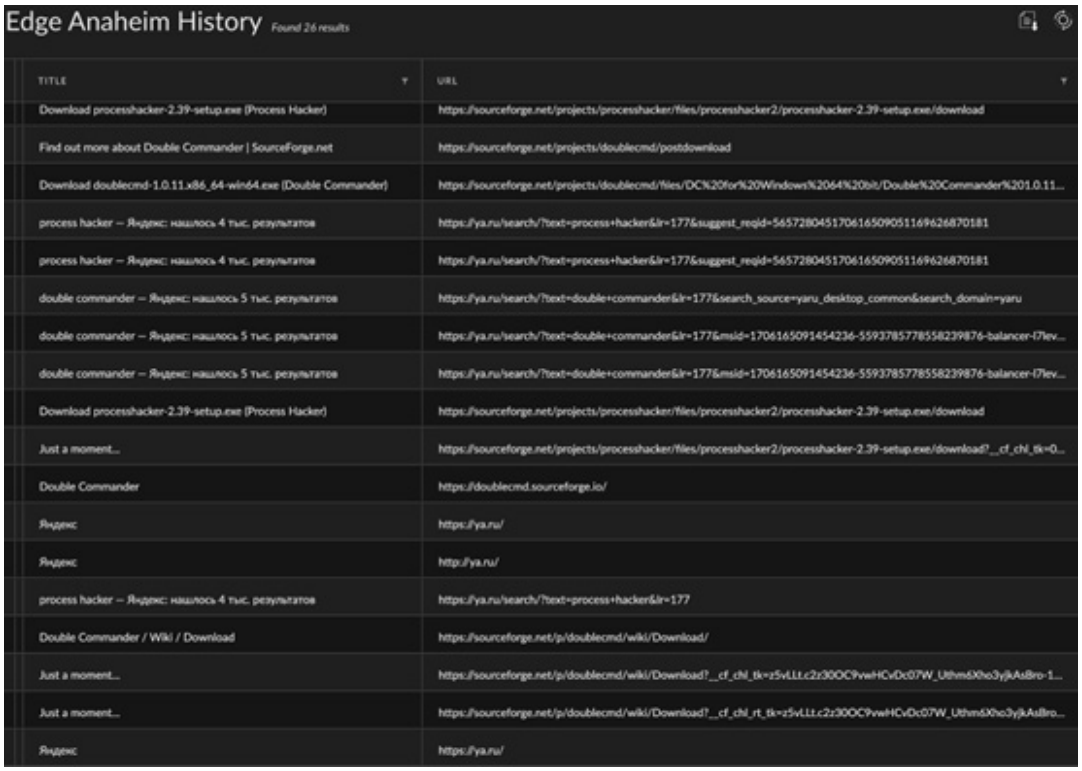

Figure 15: Portion of the adversary's browser history.

ADDITIONAL FINDINGS

TTP overlaps with Conti playbook

As noted in the previous section, the rogue system contained `ContiTraining.rar`, but we found no indication that the attackers downloaded material from the Conti playbook on the rogue system. However, we observed some overlaps between the Conti playbook and tactics, techniques and procedures (TTPs) captured during this incident attack chain, such as:

- Using *Atera* agent to access the client network and maintain persistence
- Cobalt Strike beaconing activity
- Using PsExec for lateral movement
- Exfiltrating data using the Rclone utility.

Findings from Cobalt Strike watermark

We extracted configuration data from Cobalt Strike beacons used during the attack, and the watermark ID across all the extracted configuration data was `1357776117`. *Threatfox* [9] has so far identified around 160 unique IPv4 and domain names associated with this particular Cobalt Strike watermark ID.

Cobalt Strike activity has frequently been noted in ransomware attacks, and a small portion of the identified Cobalt Strike IPv4 and domain names have also been associated with the Dark Scorpius (a.k.a. Black Basta) ransomware. Despite the association of Cobalt Strike with ransomware, we did not observe any attempts to deploy ransomware during our investigation. We speculate this might be because the threat actor lost access to the network before attempting further actions.

THREAT ACTOR PROFILING

Files on the rogue system, like the AV/EDR bypass tool demonstration videos and the P-1 form, constitute an operational security (OpSec) failure by the threat actor that exposed information we believe helps us identify them.

We identified the *LinkedIn* profile of the individual whose name ('Andry') we captured from the video. The individual is employed at the company based in Kazakhstan listed in the P-1 form. Furthermore, we found a matching profile on the Russian social networking platform *VKontakte*, which reveals more details about the individual.

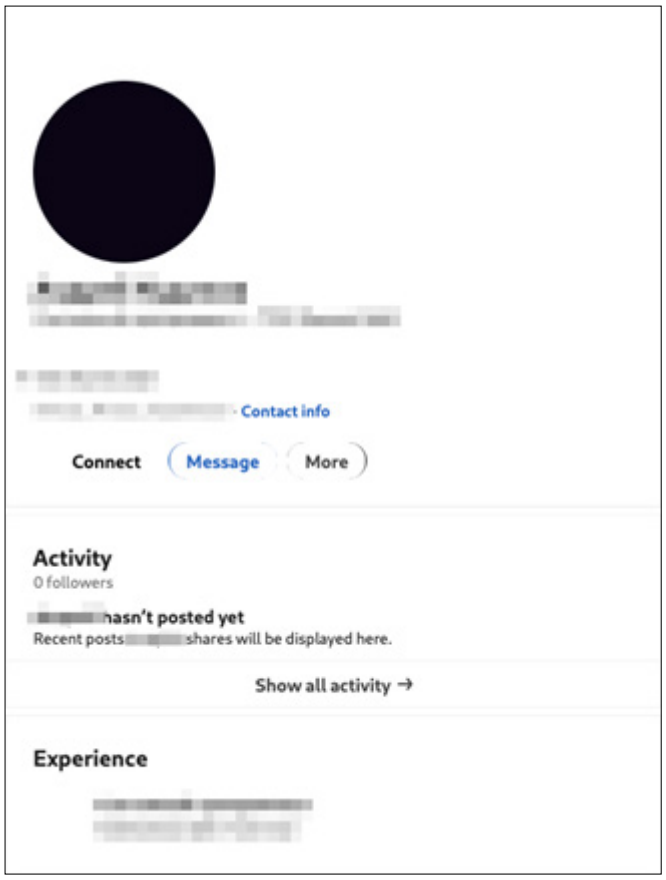

Figure 16: LinkedIn profile of the rogue individual.

We also gathered additional details on the organization employing this individual, including its website, legal address and registration details. While we cannot disclose exact details about the organization where this individual reportedly worked, we can share some relevant key details.

The company was first registered with the Kazakhstan government in early January 2023, listing fewer than five employees and 'software development' as its line of business. The company's website states its location as an address in Almaty, Kazakhstan. However, several other sources indicate that its legal address is in Saran, Karaganda region. Furthermore, an official Kazakhstan government document shows that it conducted business in the Karaganda region during the first quarter of 2023. Notably, Saran lies over 1,000 km north of Almaty.

The company website also offers detailed profiles of its employees, outlining their professional backgrounds. According to the site, one individual brings managerial experience, while the others are programmers. Most of these programmers, if not all, possess a background in low-level operating systems.

Figure 17: Images of five employees at the organization.

Of the five employees, one matched our individual of interest. Their image on the company website was identical to the one on their *LinkedIn* profile. We also located their *VKontakte* (*VK*) profile, which lists their hometown as Saran – the same town as noted in several official addresses for the organization employing this individual.

One *VK* post contained images similar to those on the individual's *LinkedIn* profile and the company website. This post included the caption 'Набережная Павлодар', which translates to 'Naberezhnaya Embankment'. This area is located in Pavlodar, Kazakhstan, which is a town northeast of Karaganda.

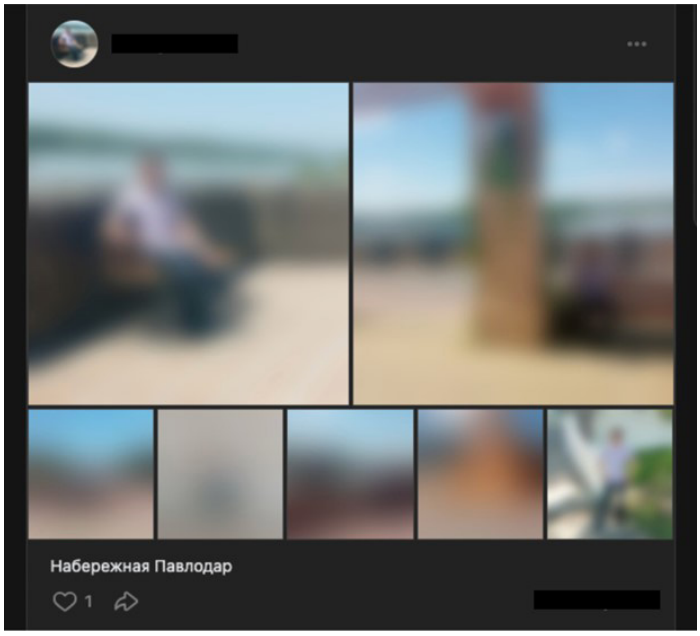

Figure 18: VK post by threat actor.

KernelMode connection

Revisiting some of the points we covered so far:

- The rogue system `DESKTOP-J8AOTJS` contained multiple recordings of an AV/EDR bypass tool being demonstrated against various EDR products.
- Those exact videos were also distributed by an actor that uses the moniker KernelMode on different cybercrime forums.
- The *Windows* taskbar exposed the name of the host machine in those recordings.
- Additionally, a P-1 expense form was present on the rogue system, revealing the name of the company employing the individual.
- We pivoted on this information to discover what we believe to be the true identity of the individual, along with personal and professional details.

With these points in mind, we assess with moderate confidence that the individual in question is one of the people, if not the only person, behind KernelMode. Moreover, based on the individual's background and relevant information we gathered, this individual is likely one of the developers, if not the sole developer, of the AV/EDR bypass tool.

However, we cannot ascertain if this particular individual is the owner of the rogue virtual machine `DESKTOP-J8AOTJS`, and by extension, the person behind this whole attack. This is primarily for the following reasons:

- The rogue individual is definitely one of the active users of `DESKTOP-J8AOTJS`, but access to this virtual machine could have been shared across multiple individuals. There isn't concrete evidence to suggest otherwise.
- There is no indication of `DESKTOP-J8AOTJS` being involved in the attack, except for the purposes of AV/EDR bypass.

CONCLUSION

Recently, there has been a growing trend in the use of AV/EDR bypass tools, extending beyond the incident discussed here. These tools will likely continue to evolve in their attempts to exploit various security platforms.

Ongoing monitoring of underground forums provides valuable insights into the latest developments and techniques of these tools. Threat actors and developers monetize such platforms on a subscription basis, regularly releasing updates as part of their affiliate payment plans.

This incident allowed us to expose a rogue system and, by extension, the toolkit and files owned by the threat actor. Using all the information gathered, *Unit 42* unveiled what we believe to be the true identity of one of the threat actors and assessed their involvement in this incident.

REFERENCES

[1] Behling, D. Bring Your Own Backdoor: How Vulnerable Drivers Let Hackers In. VMware. 19 April 2023. https://blogs.vmware.com/security/2023/04/bring-your-own-backdoor-how-vulnerable-drivers-let-hackers-in.html.

[2] wavestone-cdt / EDRSandblast. https://github.com/wavestone-cdt/EDRSandblast.

[3] Abrams, L. Angry Conti ransomware affiliate leaks gang's attack playbook. Bleeping Computer. 5 August 2021. https://www.bleepingcomputer.com/news/security/angry-conti-ransomware-affiliate-leaks-gangs-attack-playbook/.

[4] Government procurement of the the Republic of Kazakhstan. УВАЖАЕМЫЕ ПОЛЬЗОВАТЕЛИ ВЕБ-ПОРТАЛА ГОСУДАРСТВЕННЫХ ЗАКУПОК! (DEAR USERS OF THE STATE PROCUREMENT WEB PORTAL!) 13 November 2017. https://goszakup.gov.kz/ru/news/view/146.

[5] Wiki/Manual:Winbox. https://wiki.mikrotik.com/Wiki/Manual:Winbox.

[6] OBS Studio. https://obsproject.com/.

[7] System Informer. https://processhacker.sourceforge.io/.

[8] Double Commander. https://doublecmd.sourceforge.io/.

[9] ThreatFox Database. https://threatfox-api.abuse.ch/browse/tag/cs-watermark-1357776117/.