Attacker Identity Revealed: Insights from Rogue VMs & BYOVD in EDR Evasion

Virus Bulletin 2025

Renzon Cruz | Technical Director, Incident Response
Navin Thomas | Threat Researcher

Renzon Cruz

Technical Director,
Incident Response
Unit 42
Palo Alto Networks

https://www.linkedin.com/in/renzoncruz/
https://x.com/r3nzsec

paloalto NETWORKS | UNIT 42

- Technical Director, Incident Response @ Unit 42 Palo Alto Networks
- Ex-Senior Consultant @ NCSA QA
- 8 years in DFIR - Digital Forensics & Incident Response
- DFIR Analyst/Contributor @ TheDFIRReport
- CFP Board/APT Labs Contributor @ Xintra APT Labs
- Co-Founder @ GuideM

Navin Thomas

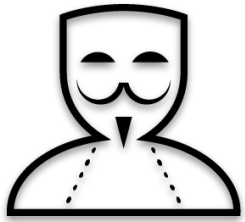
Threat Researcher
Unit 42
Palo Alto Networks

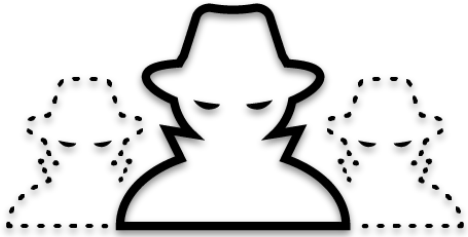
linkedin.com/in/navin-thomas-093a7b182

- Reactive Services - Intel Response Unit
- 8+ years in cybersecurity
- Previously at FireEye
- Master's in Information Security at Carnegie Mellon University

paloalto NETWORKS | UNIT 42

Initial Access



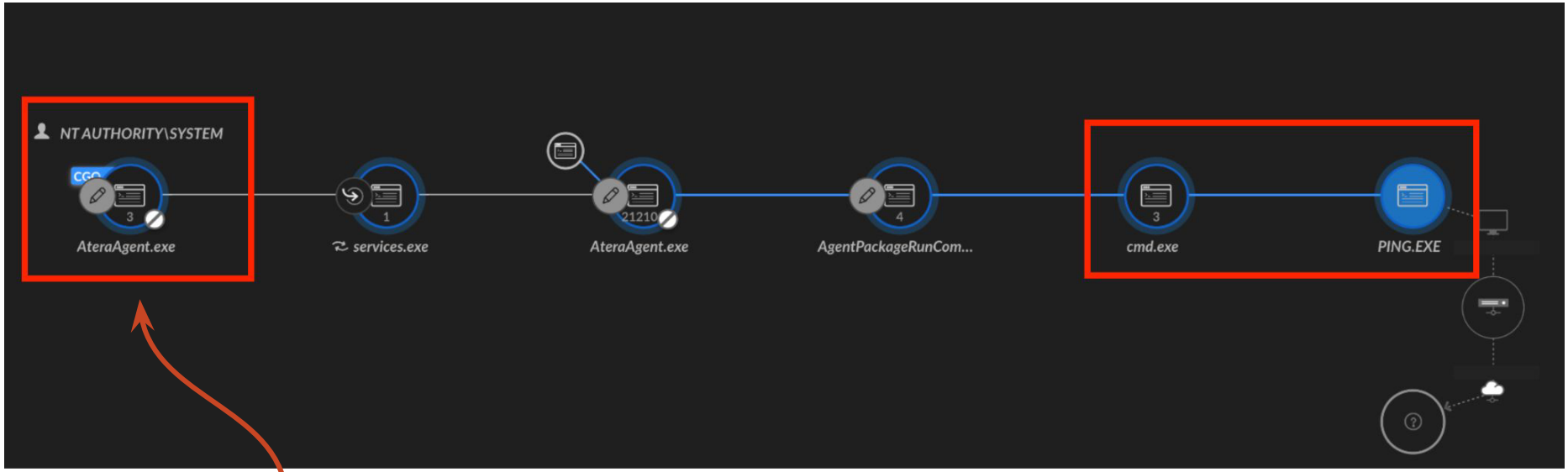


TA looks into buying valid credentials via the dark web

IAB provides stolen helpdesk credentials

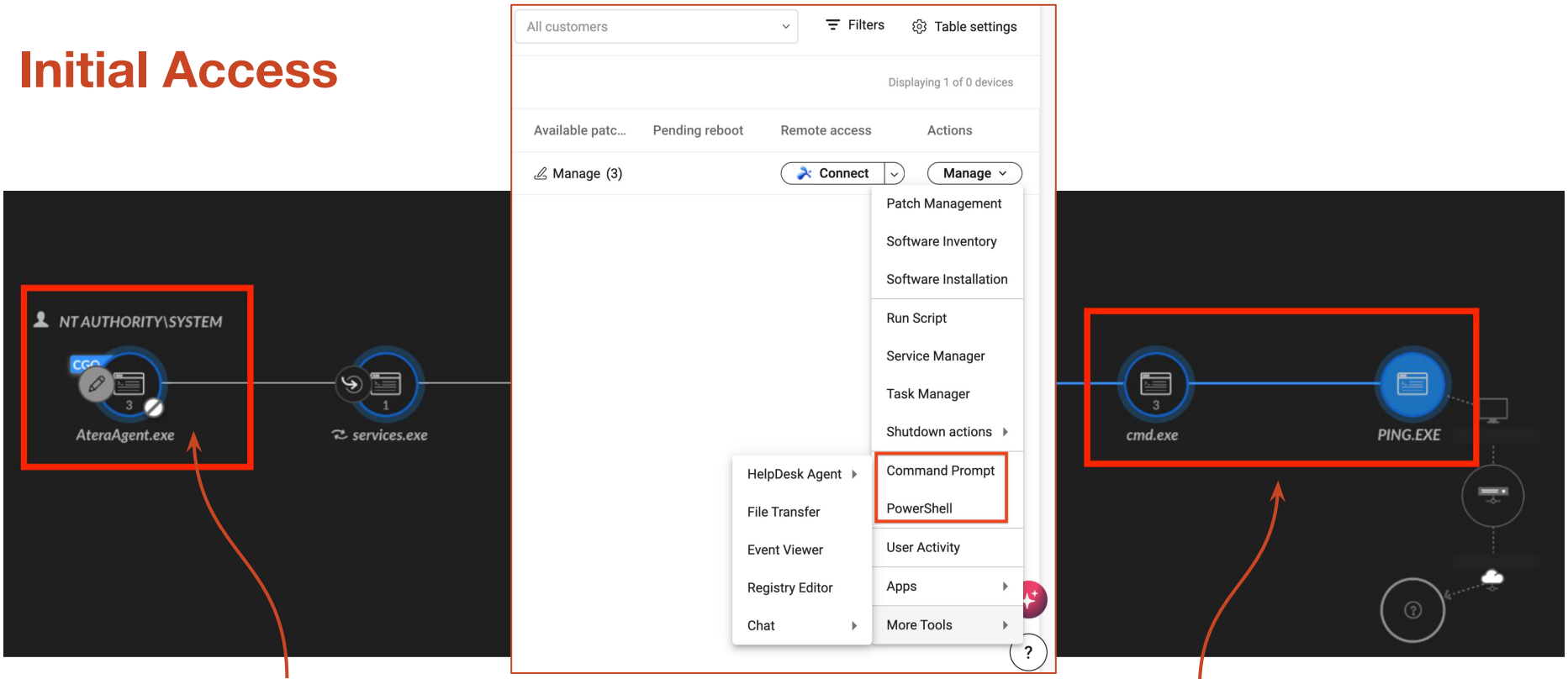
TA successfully acquires helpdesk credentials with access to Atera

Initial Access



TA purchased a valid credential (helpdesk) on the dark web

Initial Access



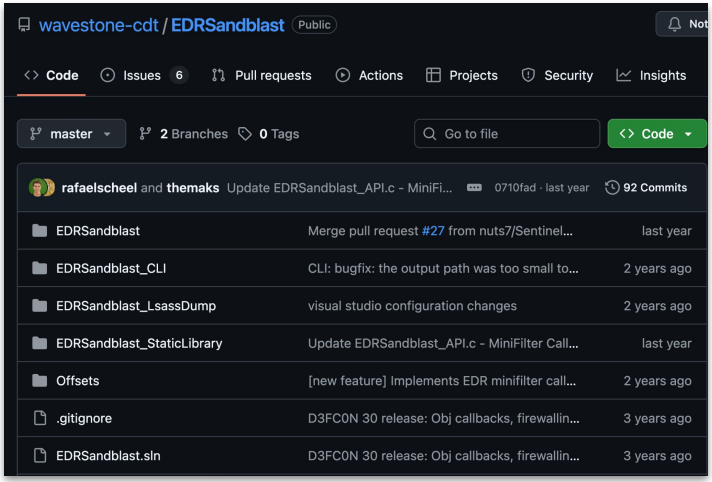
TA purchased a valid credential (helpdesk) on the dark web

TA performed “ping” command via Atera terminal feature

Defense Evasion

PDBFileName:

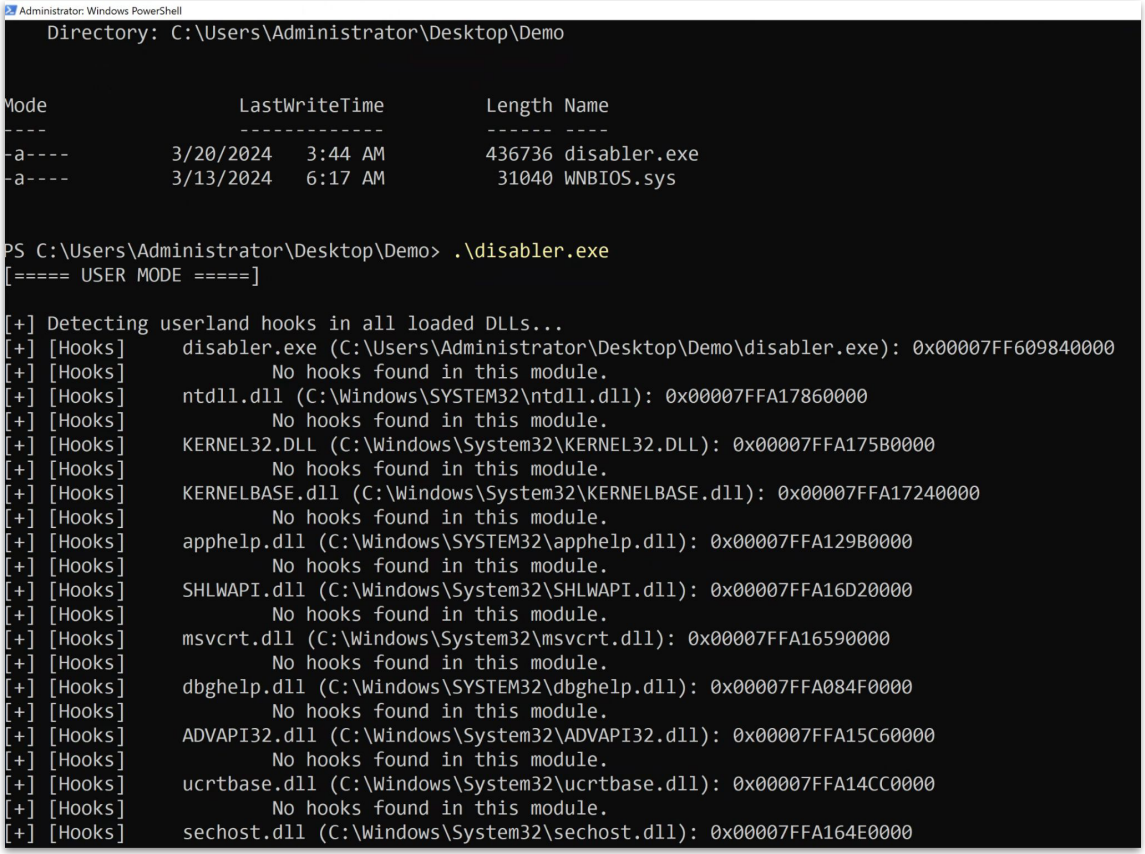
D:\EDR**EDRSandblast-master**\x64\Release\disabler.pdb



https://github.com/wavestone-cdt/EDRSandblast

```
PE ▾  Linear ▾  Pseudo C ▾

0x14004bf64 .rdata {0x14002c000-0x14004fd20} Read-only data

14004bf64  uint32_t debugInfoType = 'RSDS'
14004bf68  uint8_t PDBGuid[0x10] =
14004bf68  {
14004bf68      [0x0] =  0x3b
14004bf69      [0x1] =  0x10
14004bf6a      [0x2] =  0x08
14004bf6b      [0x3] =  0x8e
14004bf6c      [0x4] =  0xf0
14004bf6d      [0x5] =  0x8a
14004bf6e      [0x6] =  0x9b
14004bf6f      [0x7] =  0x4d
14004bf70      [0x8] =  0x8d
14004bf71      [0x9] =  0xa7
14004bf72      [0xa] =  0x44
14004bf73      [0xb] =  0xd4
14004bf74      [0xc] =  0x1a
14004bf75      [0xd] =  0x33
14004bf76      [0xe] =  0x3e
14004bf77      [0xf] =  0x9e
14004bf78  }
14004bf78  uint32_t PDBAge = 0x3
14004bf7c  char PDBFileName[0x34] = "D:\\EDR\\EDRSandblast-master\\x64\\Release\\disabler.pdb", 0
14004bfb0  uint8_t debug_type_vc_feature[0x14] =
14004bfb0  {
14004bfb0      [0x00] =  0x00
14004bfb1      [0x01] =  0x00
14004bfb2      [0x02] =  0x00
14004bfb3      [0x03] =  0x00
14004bfb4      [0x04] =  0x2a
14004bfb5      [0x05] =  0x01
14004bfb6      [0x06] =  0x00
14004bfb7      [0x07] =  0x00
14004bfb8      [0x08] =  0x2a
14004bfb9      [0x09] =  0x01
```

Defense Evasion



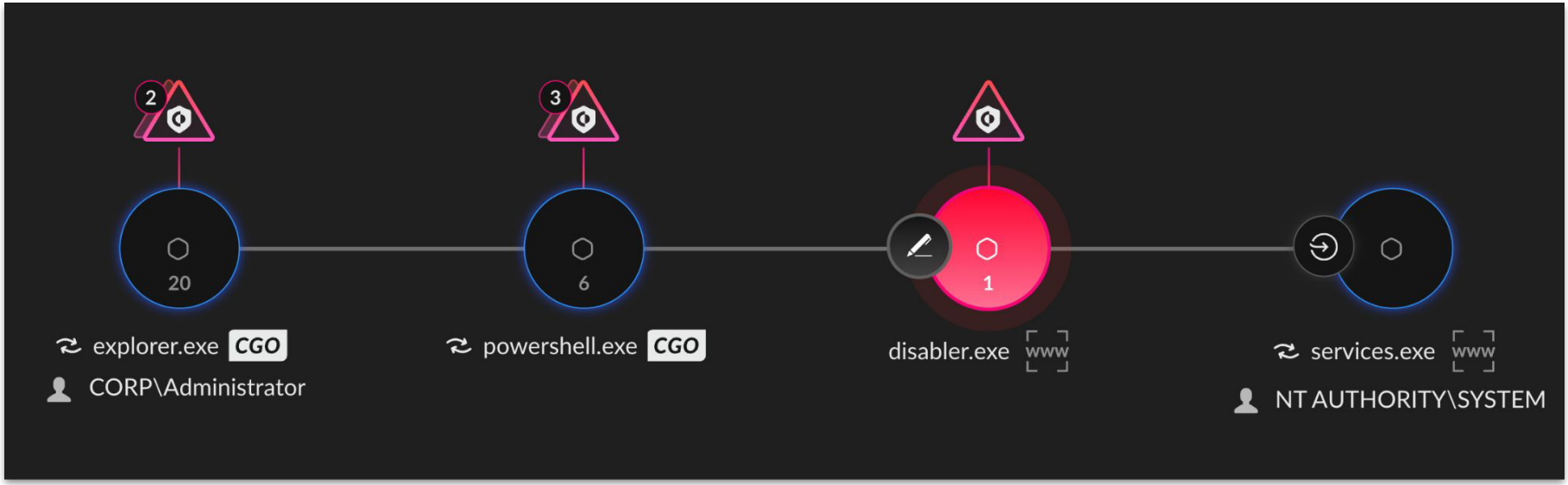
PowerShell session where the **disabler.exe** tool was executed, displaying its inspection of loaded DLLs for user-mode hooks.

Defense Evasion

```
[===== KERNEL MODE =====]

[+] Loading required offsets for ntoskrnl.exe...
[*] System's ntoskrnl.exe file version is: ntoskrnl_20348-4050.exe
Ntoskrnl version is ntoskrnl_20348-4050.exe, hashed: 289408374
[*] System's fltmgr.sys file version is: fltmgr_20348-3932.sys
[+] Installing vulnerable driver...
[*] 'iqmKagGq' service was not present
[+] 'iqmKagGq' service is successfully registered
[+] 'iqmKagGq' service ACL configured to for Everyone
[+] 'iqmKagGq' service started


[+] Checking if any EDR kernel notify rountines are set for image loading, process and thread creations...
[+] [NotifyRoutines]    Enumerating process creation callbacks
[+] [NotifyRoutines]    No EDR driver(s) found!
[+] [NotifyRoutines]    Enumerating thread creation callbacks
[+] [NotifyRoutines]    No EDR driver(s) found!
[+] [NotifyRoutines]    Enumerating image loading callbacks
[+] [NotifyRoutines]    No EDR driver(s) found!

[+] Checking if EDR callbacks are registered on processes and threads handle creation/duplication...
[+] [ObjectCallblacks]  Enumerating Process object callbacks :
Unexpected value in callback entry (ObjectTypeField), exiting...
PS C:\Users\Administrator\Desktop\Demo>
```

Kernel-mode execution phase of **disabler.exe**, where it loads a vulnerable driver (**WNBIOS.sys**) as a new service (**iqmKagGq**) to gain kernel-level access.

Defense Evasion



Command & Control

\\<IP Address>\admin$**5d01c51.exe**

\\<IP Address>\admin$**3d85fd4.exe**

\\<IP Address>\admin$**74b1e10.exe**

\\<IP Address>\admin$**8c5c39c.exe**

\\<IP Address>\admin$**0a648e4.exe**

\\<IP Address>\admin$**d06e15b.exe**

\\<IP Address>\admin$**f5dbf1b.exe**

\\<IP Address>\admin$**5bb646d.exe**

\\<IP Address>\admin$**0bffbb8.exe**

Threat actor abusing the **Atera RMM** platform as a C2 channel to manage and control compromised systems. Through Atera, they remotely deployed multiple **Cobalt Strike** beacon executables across endpoints using **admin$** shares for lateral movement and persistence

Command & Control

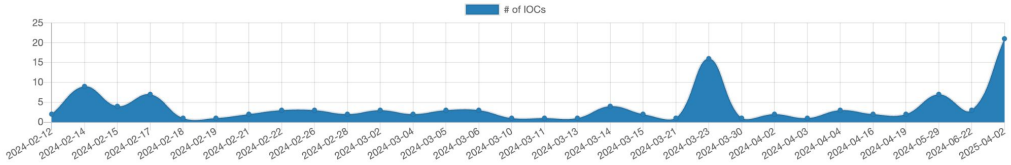
ThreatFox Database

Indicators of Compromise (IOCs) on ThreatFox are usually associated with certain tags. Every IOC can associated with one or more tags. Using tags, it is easy to navigate through the huge amount of IOCs in the ThreatFox corpus. The page below gives you an overview on IOCs that are tagged with cs-watermark-1357776117.

You can also get this data through the ThreatFox API.

Database Entry

Tag:	cs-watermark-1357776117
First seen:	2023-09-26 23:19:48 UTC
Last seen:	2025-04-02 22:16:04 UTC
Sightings:	182



license-id **1357776117**

```
File: vm32.dll
payloadType: 0x00000001
payloadSize: 0x00000000
intxorkey: 0x00000000
id2: 0x00000000
Skipping 32 bytes
payloadType: 0x00002430
payloadSize: 0x0004b007
intxorkey: 0xe26a7260
id2: 0x00000000
MZ header found position 11
Config found: xorkey b'.' 0x00044440 0x0004affc
0x0001 payload type 0x0001 0x0002 0 windows-beacon_http-reverse_http
0x0002 port 0x0001 0x0002 80
0x0003 sleeptime 0x0002 0x0004 19299
0x0004 maxgetsize 0x0002 0x0004 1864740
0x0005 jitter 0x0001 0x0002 39
0x0007 publickey 0x0003 0x0100
30819f300d06092a864886f70d010101050003818d0030818902818100dcbdc317b1bcbbc7024bc854786653d8eed66c1d
773904ddee1ad75ea2fac708f51b2e6b921ecb3e14e0bf3cde1aebe372cda42704dd82f6b08f195d3458d06bd6faad0ee6
59b2966c894705aca576d5a8ad069c9bc08000bd19fc07f17359857beb5b0775503ac4f636cb45a1e953e0fadabe09ecf0
64a5831ba716982cbf4102030100010000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000
0x0008 server,get-uri 0x0003 0x0100

0x0043 DNS_STRATEGY 0x0001 0x0002 0
0x0044 DNS_STRATEGY_ROTATE_SECONDS 0x0002 0x0004 -1
0x0045 DNS_STRATEGY_FAIL_X 0x0002 0x0004 -1
0x0046 DNS_STRATEGY_FAIL_SECONDS 0x0002 0x0004 -1
0x000e SpawnTo 0x0003 0x0010 (NULL ...)
0x001d spawnto_x86 0x0003 0x0040 '%windir%\\syswow64\\regsvr32.exe'
0x001e spawnto_x64 0x0003 0x0040 '%windir%\\sysnative\\regsvr32.exe'
0x001f CryptoScheme 0x0001 0x0002 0
0x001a get-verb 0x0003 0x0010 'GET'
0x001b post-verb 0x0003 0x0010 'POST'
0x0025 license-id 0x0002 0x0004 1357776117
0x0024 deprecated 0x0003 0x0020 'jUVfDVP0+DGkN4BZEYjDNw=='
0x0026 bStageCleanup 0x0001 0x0002 1
0x0027 bCFGCaution 0x0001 0x0002 0
0x004c 0x0002 0x0004 16
0x0047 MAX_RETRY_STRATEGY_ATTEMPTS 0x0002 0x0004 0
0x0048 MAX_RETRY_STRATEGY_INCREASE 0x0002 0x0004 0
0x0049 MAX_RETRY_STRATEGY_DURATION 0x0002 0x0004 0
0x0009 useragent 0x0003 0x0100 'Mozilla/5.0 (Linux; Android 8.0.0; SM-G960F Build/R16NW)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202'
0x000a post-uri 0x0003 0x0040 '/avatars'
0x000b Malleable_C2_Instructions 0x0003 0x0100
Transform Input: [7:Input,4,2:600,3,3]
Print
Remove 600 bytes from begin
BASE64
BASE64
0x000c http_get_header 0x0003 0x0200

Const_header Connection: close
Const_header Accept: */*
Const_header Accept-Language: en-GB;q=0.9, *;q=0.7
Build Metadata: [7:Metadata,11,3,2:LSID=,6:Cookie]
```

Persistence

```
C:\>
schtasks /query /v /fo LIST /tn Indexer

Folder: \
HostName:
TaskName:                                 \Indexer
Next Run Time:
Status:                                   Ready
Logon Mode:                               Interactive/Background
Last Run Time:
Last Result:                              -1
Author:
Task To Run:                              C:\Windows\System32\rundll32.exe C:\Windows\temp\vm32.dll,StartW
Start In:                                 N/A
Comment:                                  N/A
Scheduled Task State:                     Enabled
Idle Time:                                Disabled
Power Management:                         Stop On Battery Mode, No Start On Batteries
Run As User:                              SYSTEM
Delete Task If Not Rescheduled:           Disabled
Stop Task If Runs X Hours and X Mins:     72:00:00
Schedule:                                 Scheduling data is not available in this format.
Schedule Type:                            One Time Only, Minute
Start Time:
Start Date:
End Date:                                 N/A
Days:                                     N/A
Months:                                   N/A
Repeat: Every:                            0 Hour(s), 5 Minute(s)
Repeat: Until: Time:                      None
Repeat: Until: Duration:                  Disabled
Repeat: Stop If Still Running:            Disabled

C:\>
schtasks /delete /tn "Indexer" /f
SUCCESS: The scheduled task "Indexer" was successfully deleted.
```

Malicious scheduled task named **Indexer** that was set to execute rundll32.exe with **vm32.dll** (a Cobalt Strike beacon) from the **C:\Windows\temp** directory, configured to re-run every **5 minutes indefinitely** as a persistence mechanism

Data Exfiltration

```
C:\Users\dfir\Desktop>vmware.exe -h

Rclone syncs files to and from cloud storage providers as well as
mounting them, listing them in lots of different ways.

See the home page (https://rclone.org/) for installation, usage,
documentation, changelog and configuration walkthroughs.

Usage:
  rclone [flags]
  rclone [command]
```

Users > dfir > Downloads > rclone.conf > ⚙ rclone.conf

```
1  [remote]
2  type = sftp
3  host = [redacted]
4  user = [redacted]
5  pass = [redacted]1Z3vACkUgRDQKdg
6  md5sum_command = md5sum
7  sha1sum_command = sha1sum
```

Data Exfiltration

Rclone "REVEAL" Command

IMPORTANT!

rclone.conf

[redacted] > Drop Zone > rclone.conf

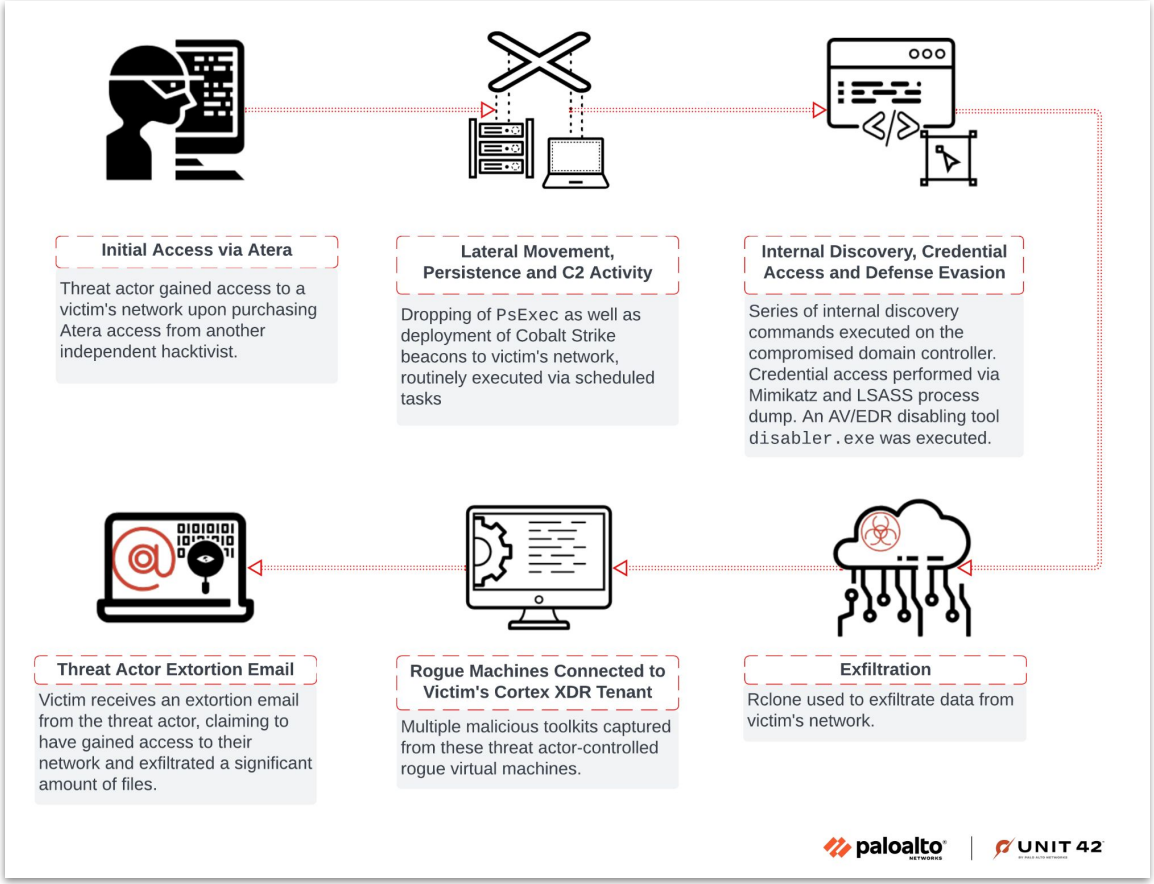
```
1  [remote]
2  type = sftp
3  host = [redacted]
4  user = [redacted]
5  pass = [redacted]ACkUgRDQKdg
6  md5sum_command = md5sum
7  sha1sum_command = sha1sum
```

rclone — -zsh — 98×8

```
dfir@Mac rclone % ./rclone reveal -- [redacted]vACkUgRDQKdg
zte0CKg0C
dfir@Mac rclone %
```

THIS IS THE ORIGINAL PASSWORD!

High Level Chain of Events



Threat Actor Communication & Negotiation

Negotiation with the Threat Actor

As I have told you before, I have gained access to the network and downloaded 97 GB of data.
What I want to offer:
- I will provide you with the electronic wallet address
- <CLIENT> pays $350,000 to this wallet
-When I receive payment the data will be deleted
- <CLIENT> gets data deletion log
- <CLIENT> get details of data breach incident if needed
- <CLIENT> never see me again
- Everyone is happy

Otherwise I will have to start terrorizing <CLIENT> social media and disturbing business. That is the plan.

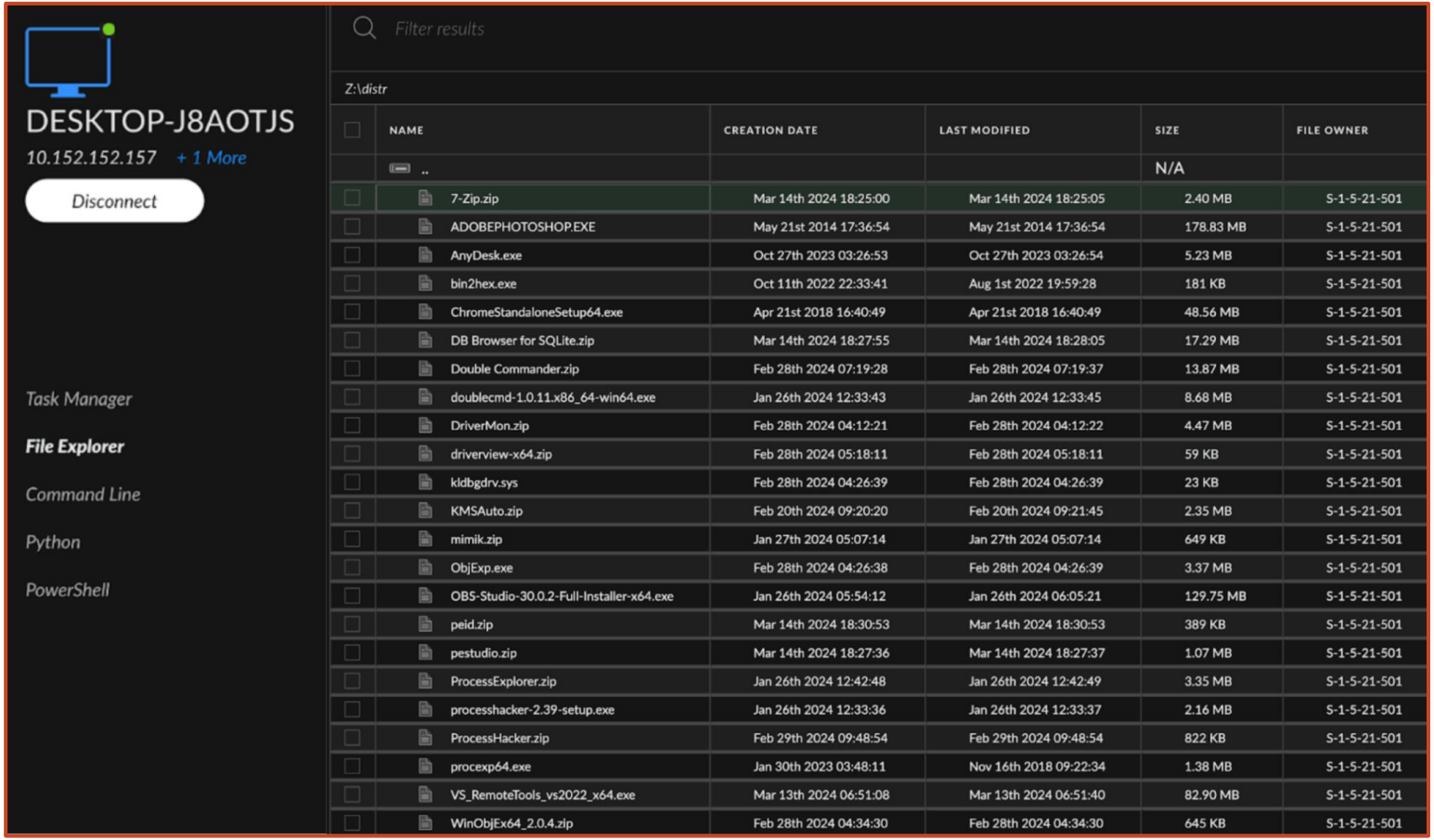
Hello, Sir. **You are doing very good job** over there, but i am afraid this amount is still low. You have just cut 50% from already cutted price. Let's make it at least $225,000, i can wait until tomorrow.$125,000 is a good discount; it cuts more than 33.3% off the original price.
We are getting very close to close the deal, a little bit of effort from you and we are finally done with this.

Negotiation with the Threat Actor

Such a tough negotiator you are. Ok, let it be so. I accept BTC. Wallet address to perform the payment would be provided soon.

Initial Demand: $350,000
Final Demand: $180,000
Percent Reduction: 46%

One morning with DESKTOP-J8AOTJS

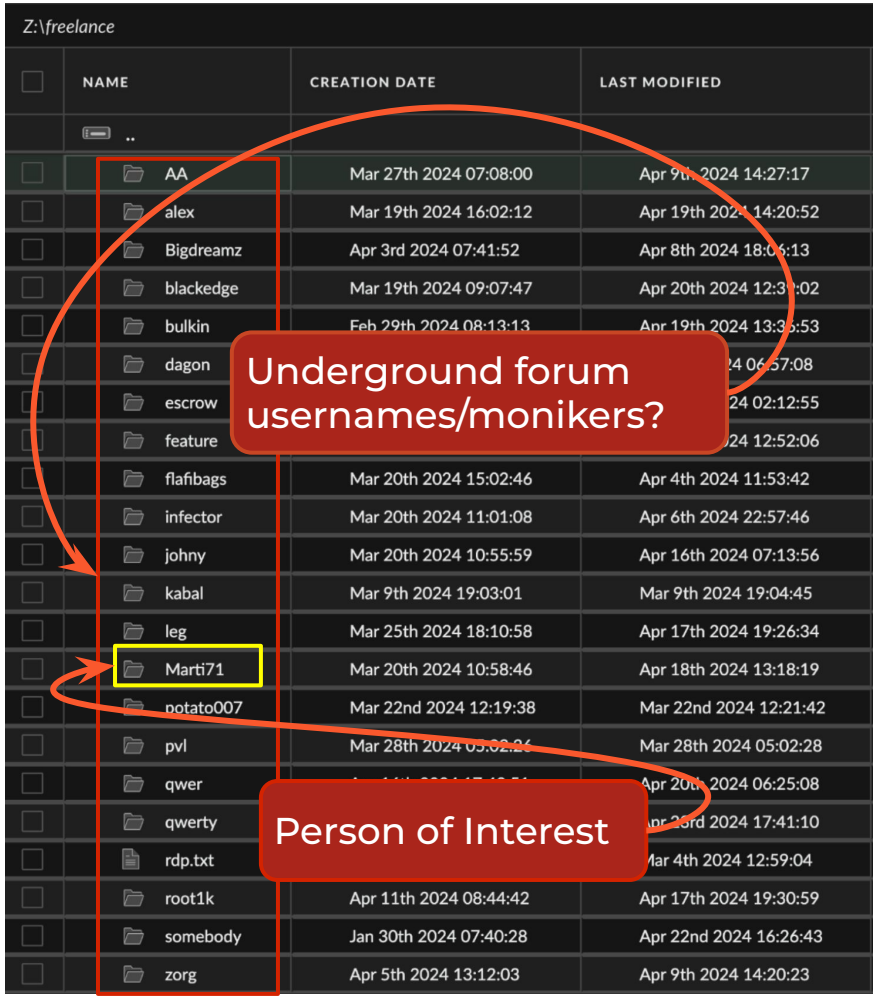


NAME	CREATION DATE	LAST MODIFIED	SIZE	FILE OWNER
..			N/A	
7-Zip.zip	Mar 14th 2024 18:25:00	Mar 14th 2024 18:25:05	2.40 MB	S-1-5-21-501
ADOBEPHOTOSHOP.EXE	May 21st 2014 17:36:54	May 21st 2014 17:36:54	178.83 MB	S-1-5-21-501
AnyDesk.exe	Oct 27th 2023 03:26:53	Oct 27th 2023 03:26:54	5.23 MB	S-1-5-21-501
bin2hex.exe	Oct 11th 2022 22:33:41	Aug 1st 2022 19:59:28	181 KB	S-1-5-21-501
ChromeStandaloneSetup64.exe	Apr 21st 2018 16:40:49	Apr 21st 2018 16:40:49	48.56 MB	S-1-5-21-501
DB Browser for SQLite.zip	Mar 14th 2024 18:27:55	Mar 14th 2024 18:28:05	17.29 MB	S-1-5-21-501
Double Commander.zip	Feb 28th 2024 07:19:28	Feb 28th 2024 07:19:37	13.87 MB	S-1-5-21-501
doublecmd-1.0.11.x86_64-win64.exe	Jan 26th 2024 12:33:43	Jan 26th 2024 12:33:45	8.68 MB	S-1-5-21-501
DriverMon.zip	Feb 28th 2024 04:12:21	Feb 28th 2024 04:12:22	4.47 MB	S-1-5-21-501
driverview-x64.zip	Feb 28th 2024 05:18:11	Feb 28th 2024 05:18:11	59 KB	S-1-5-21-501
kldbgdrv.sys	Feb 28th 2024 04:26:39	Feb 28th 2024 04:26:39	23 KB	S-1-5-21-501
KMSAuto.zip	Feb 20th 2024 09:20:20	Feb 20th 2024 09:21:45	2.35 MB	S-1-5-21-501
mimik.zip	Jan 27th 2024 05:07:14	Jan 27th 2024 05:07:14	649 KB	S-1-5-21-501
ObjExp.exe	Feb 28th 2024 04:26:38	Feb 28th 2024 04:26:39	3.37 MB	S-1-5-21-501
OBS-Studio-30.0.2-Full-Installer-x64.exe	Jan 26th 2024 05:54:12	Jan 26th 2024 06:05:21	129.75 MB	S-1-5-21-501
peid.zip	Mar 14th 2024 18:30:53	Mar 14th 2024 18:30:53	389 KB	S-1-5-21-501
pestudio.zip	Mar 14th 2024 18:27:36	Mar 14th 2024 18:27:37	1.07 MB	S-1-5-21-501
ProcessExplorer.zip	Jan 26th 2024 12:42:48	Jan 26th 2024 12:42:49	3.35 MB	S-1-5-21-501
processhacker-2.39-setup.exe	Jan 26th 2024 12:33:36	Jan 26th 2024 12:33:37	2.16 MB	S-1-5-21-501
ProcessHacker.zip	Feb 29th 2024 09:48:54	Feb 29th 2024 09:48:54	822 KB	S-1-5-21-501
procexp64.exe	Jan 30th 2023 03:48:11	Nov 16th 2018 09:22:34	1.38 MB	S-1-5-21-501
VS_RemoteTools_vs2022_x64.exe	Mar 13th 2024 06:51:08	Mar 13th 2024 06:51:40	82.90 MB	S-1-5-21-501
WinObjEx64_2.0.4.zip	Feb 28th 2024 04:34:30	Feb 28th 2024 04:34:30	645 KB	S-1-5-21-501

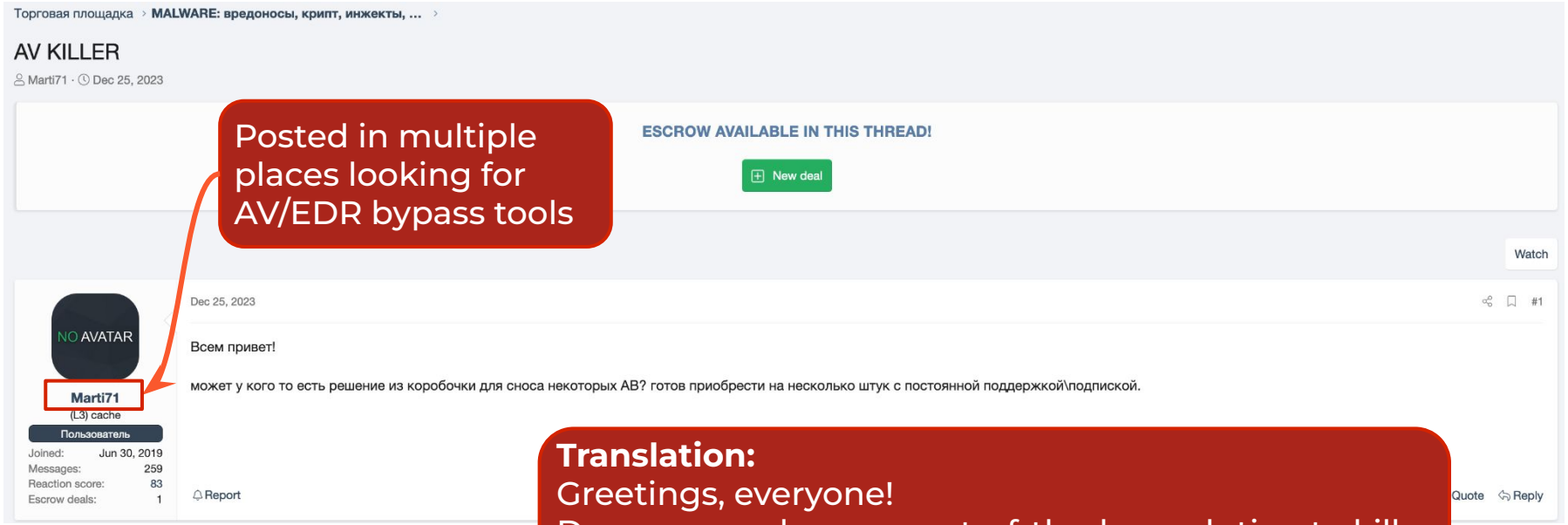
Who is selling this Bypass Tool?

Initial Leads: Identifying Potential Aliases

- Discovered suspicious folder names in the Z:\freelance directory.
- Pivoted to search these names on cybercrime forums like XSS and Exploit.
- Relevant hits suggested some names were potential threat actor aliases.



Hunting down the Seller



Translation:
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.

Hunting down the Seller

KernelMode

Kernel mode developer

Premium

Joined:	Apr 27, 2023
Messages:	92
Reaction score:	31
Escrow deals:	12

Jan 25, 2024

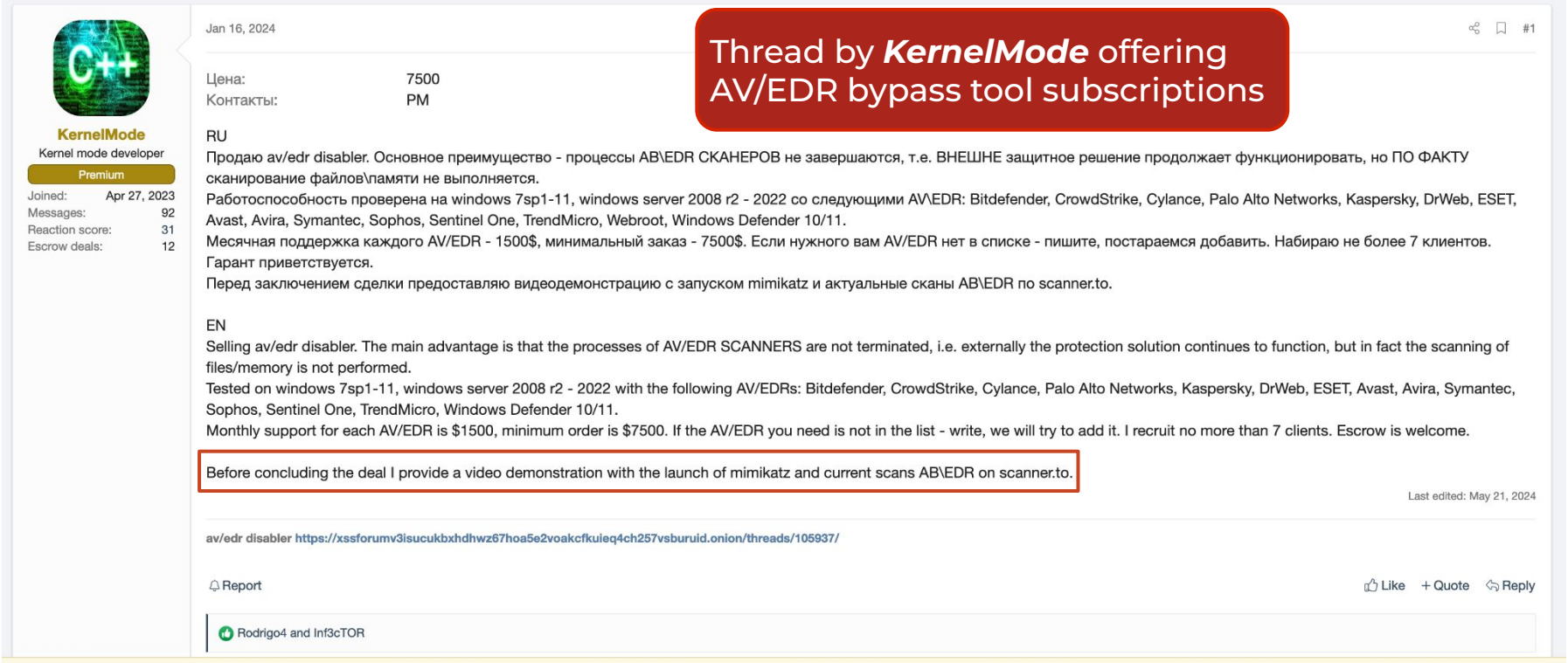
предлагаю - https://xssforumv3isucukbxhdhwz67hoa5e2voakcfkuieq4ch257vsburuid.onion/threads/105937/

av/edr disabler https://xssforumv3isucukbxhdhwz67hoa5e2voakcfkuieq4ch257vsburuid.onion/threads/105937/

Report

User ***KernelMode*** suggesting an AV/EDR bypass tool.

Hunting down the seller



KernelMode
Kernel mode developer
Premium
Joined: Apr 27, 2023
Messages: 92
Reaction score: 31
Escrow deals: 12

Jan 16, 2024 #1

Thread by ***KernelMode*** offering AV/EDR bypass tool subscriptions

Цена: 7500
Контакты: PM

RU
Продаю av/edr disabler. Основное преимущество - процессы AB\EDR СКАНЕРОВ не завершаются, т.е. ВНЕШНЕ защитное решение продолжает функционировать, но ПО ФАКТУ сканирование файлов\памяти не выполняется.
Работоспособность проверена на windows 7sp1-11, windows server 2008 r2 - 2022 со следующими AV\EDR: Bitdefender, CrowdStrike, Cylance, Palo Alto Networks, Kaspersky, DrWeb, ESET, Avast, Avira, Symantec, Sophos, Sentinel One, TrendMicro, Webroot, Windows Defender 10/11.
Месячная поддержка каждого AV/EDR - 1500$, минимальный заказ - 7500$. Если нужного вам AV/EDR нет в списке - пишите, постараемся добавить. Набираю не более 7 клиентов. Гарант приветствуется.
Перед заключением сделки предоставляю видеодемонстрацию с запуском mimikatz и актуальные сканы AB\EDR по scanner.to.

EN
Selling av/edr disabler. The main advantage is that the processes of AV/EDR SCANNERS are not terminated, i.e. externally the protection solution continues to function, but in fact the scanning of files/memory is not performed.
Tested on windows 7sp1-11, windows server 2008 r2 - 2022 with the following AV/EDRs: Bitdefender, CrowdStrike, Cylance, Palo Alto Networks, Kaspersky, DrWeb, ESET, Avast, Avira, Symantec, Sophos, Sentinel One, TrendMicro, Windows Defender 10/11.
Monthly support for each AV/EDR is $1500, minimum order is $7500. If the AV/EDR you need is not in the list - write, we will try to add it. I recruit no more than 7 clients. Escrow is welcome.

Before concluding the deal I provide a video demonstration with the launch of mimikatz and current scans AB\EDR on scanner.to.

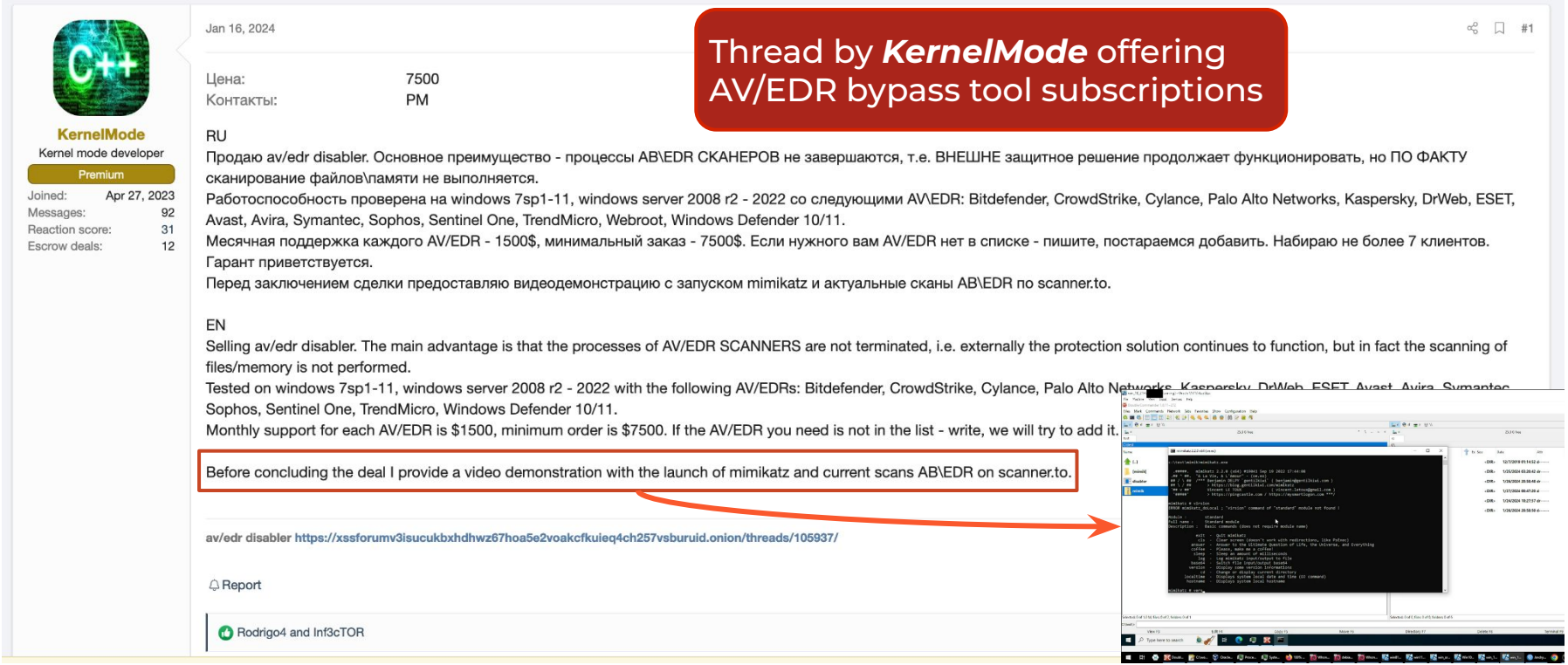
Last edited: May 21, 2024

av/edr disabler https://xssforumv3isucukbxhdhwz67hoa5e2voakcfkuieq4ch257vsburuid.onion/threads/105937/

Report Like + Quote Reply

Rodrigo4 and Inf3cTOR

Hunting down the seller



KernelMode
Kernel mode developer
Premium
Joined: Apr 27, 2023
Messages: 92
Reaction score: 31
Escrow deals: 12

Jan 16, 2024 #1

Thread by ***KernelMode*** offering AV/EDR bypass tool subscriptions

Цена: 7500
Контакты: PM

RU
Продаю av/edr disabler. Основное преимущество - процессы AB\EDR СКАНЕРОВ не завершаются, т.е. ВНЕШНЕ защитное решение продолжает функционировать, но ПО ФАКТУ сканирование файлов\памяти не выполняется.
Работоспособность проверена на windows 7sp1-11, windows server 2008 r2 - 2022 со следующими AV\EDR: Bitdefender, CrowdStrike, Cylance, Palo Alto Networks, Kaspersky, DrWeb, ESET, Avast, Avira, Symantec, Sophos, Sentinel One, TrendMicro, Webroot, Windows Defender 10/11.
Месячная поддержка каждого AV/EDR - 1500$, минимальный заказ - 7500$. Если нужного вам AV/EDR нет в списке - пишите, постараемся добавить. Набираю не более 7 клиентов.
Гарант приветствуется.
Перед заключением сделки предоставляю видеодемонстрацию с запуском mimikatz и актуальные сканы AB\EDR по scanner.to.

EN
Selling av/edr disabler. The main advantage is that the processes of AV/EDR SCANNERS are not terminated, i.e. externally the protection solution continues to function, but in fact the scanning of files/memory is not performed.
Tested on windows 7sp1-11, windows server 2008 r2 - 2022 with the following AV/EDRs: Bitdefender, CrowdStrike, Cylance, Palo Alto Networks, Kaspersky, DrWeb, ESET, Avast, Avira, Symantec, Sophos, Sentinel One, TrendMicro, Windows Defender 10/11.
Monthly support for each AV/EDR is $1500, minimum order is $7500. If the AV/EDR you need is not in the list - write, we will try to add it.

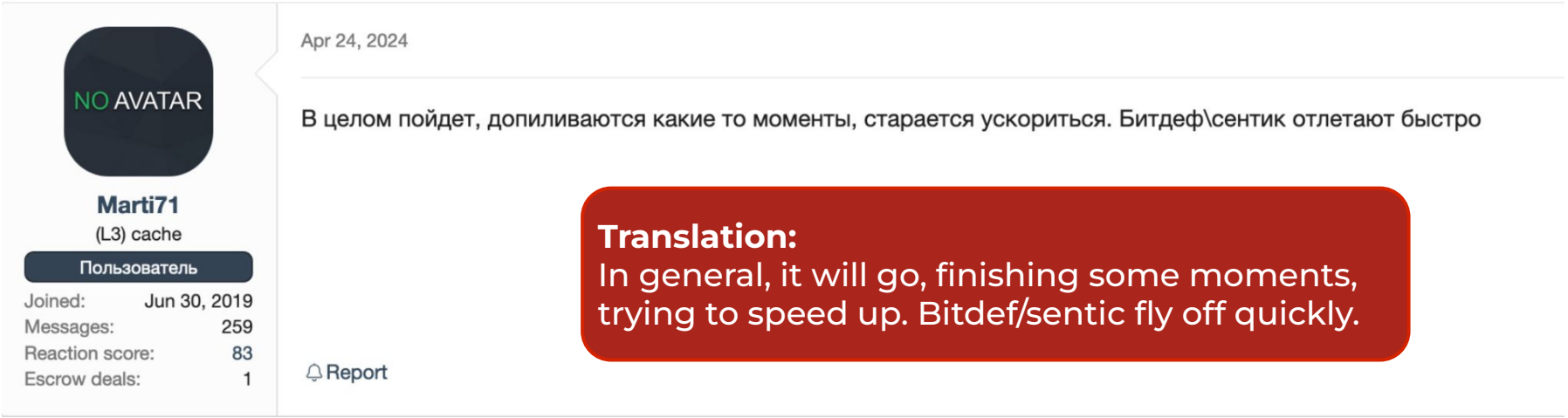
Before concluding the deal I provide a video demonstration with the launch of mimikatz and current scans AB\EDR on scanner.to.

av/edr disabler https://xssforumv3isucukbxhdhwz67hoa5e2voakcfkuieq4ch257vsburuid.onion/threads/105937/

Report

Rodrigo4 and Inf3cTOR

Hunting down the seller



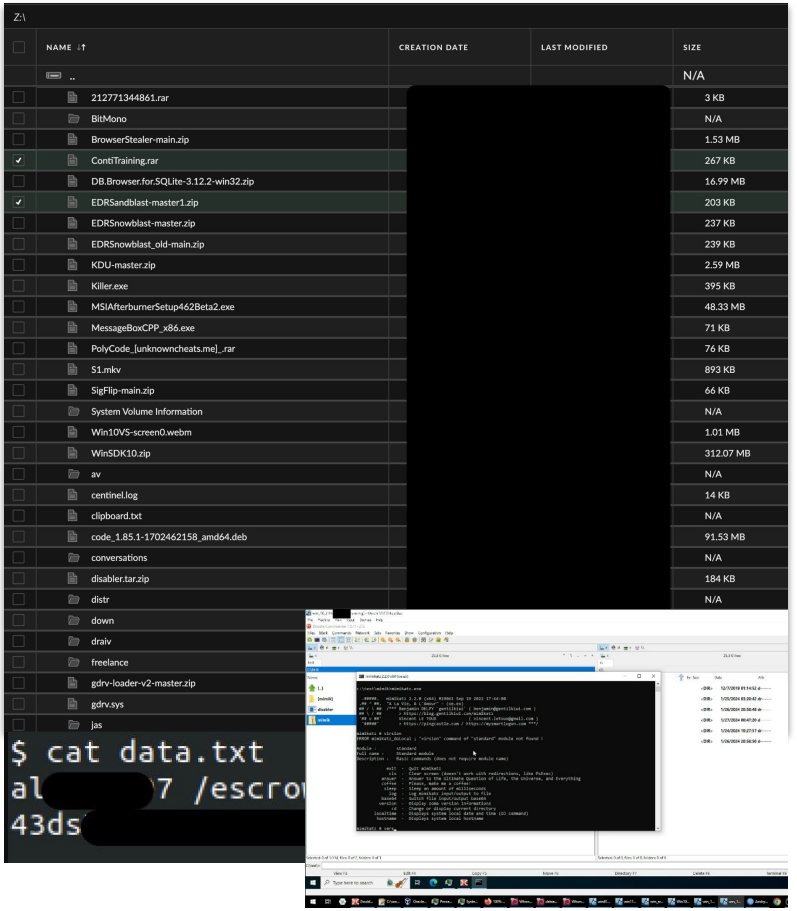
Translation:
In general, it will go, finishing some moments, trying to speed up. Bitdef/sentic fly off quickly.

Marti71 seemingly provided a positive feedback for the tool

Peek into Rogue System

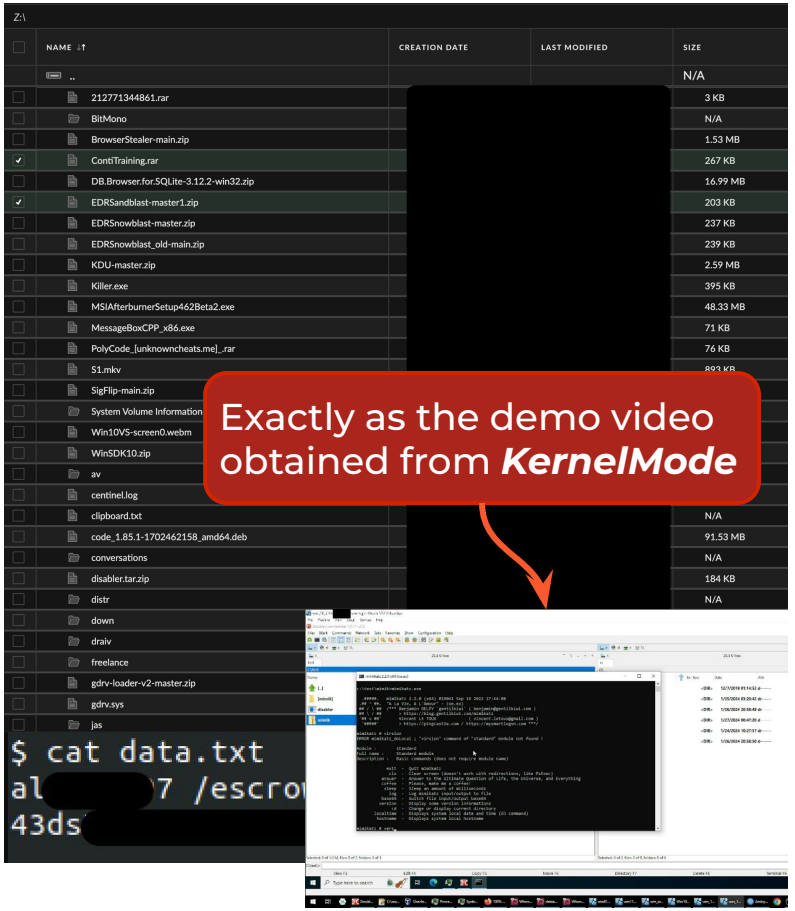
Peek into Rogue System

- Conti ransomware playbook
- Suite of tools and documents
- Host IP addresses and credentials
- File with possible escrow details
- Expense spreadsheet (P-1 form)
- Demo recordings



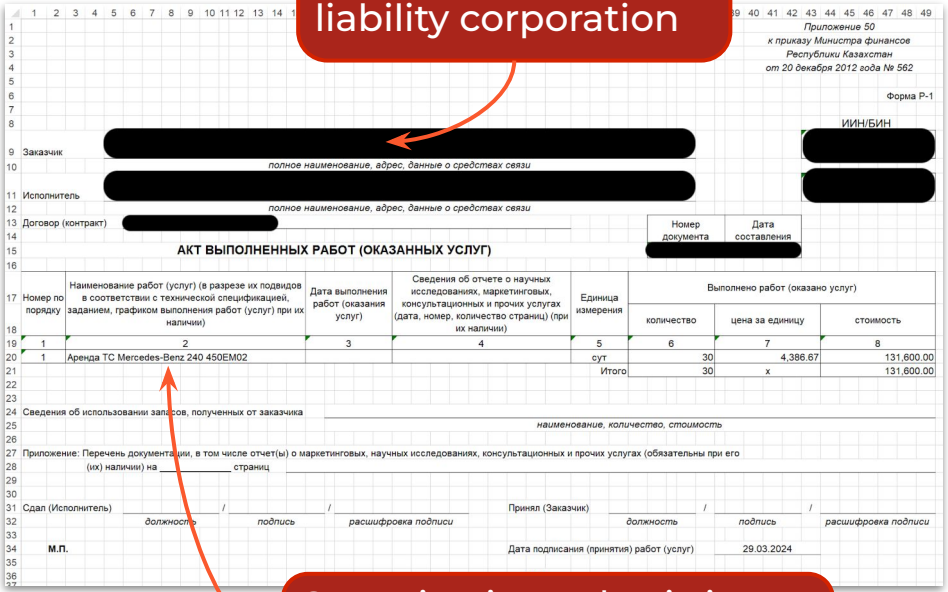
Peek into Rogue System

- Conti ransomware playbook
- Suite of tools and documents
- Host IP addresses and credentials
- File with possible escrow details
- Expense spreadsheet (P-1 form)
- Demo recordings



The P-1 Form

- A document used for invoices, completed work, and services rendered.
- Exposed the name of a specific corporation.
- This information was vital for identifying one of the threat actors.



Приложение 50
к приказу Министра финансов
Республики Казахстан
от 20 декабря 2012 года № 562

Форма Р-1

ИИН/БИН

Заказчик [redacted]
полное наименование, адрес, данные о средствах связи

Исполнитель [redacted]
полное наименование, адрес, данные о средствах связи

Договор (контракт) [redacted]

Номер документа | Дата составления

АКТ ВЫПОЛНЕННЫХ РАБОТ (ОКАЗАННЫХ УСЛУГ)

Номер по порядку	Наименование работ (услуг) (в разрезе их подвидов в соответствии с технической спецификацией, заданием, графиком выполнения работ (услуг) при их наличии)	Дата выполнения работ (оказания услуг)	Сведения об отчете о научных исследованиях, маркетинговых, консультационных и прочих услугах (дата, номер, количество страниц) (при их наличии)	Единица измерения	Выполнено работ (оказано услуг)		
					количество	цена за единицу	стоимость
1	2	3	4	5	6	7	8
1	Аренда ТС Mercedes-Benz 240 450EM02			сут	30	4,386.67	131,600.00
				Итого	30	x	131,600.00

Сведения об использовании запасов, полученных от заказчика
наименование, количество, стоимость

Приложение: Перечень документации, в том числе отчет(ы) о маркетинговых, научных исследованиях, консультационных и прочих услугах (обязательны при его (их) наличии) на _____ страниц

Сдал (Исполнитель) _____ / _____ / _____
должность *подпись* *расшифровка подписи*

Принял (Заказчик) _____ / _____ / _____
должность *подпись* *расшифровка подписи*

М.П.

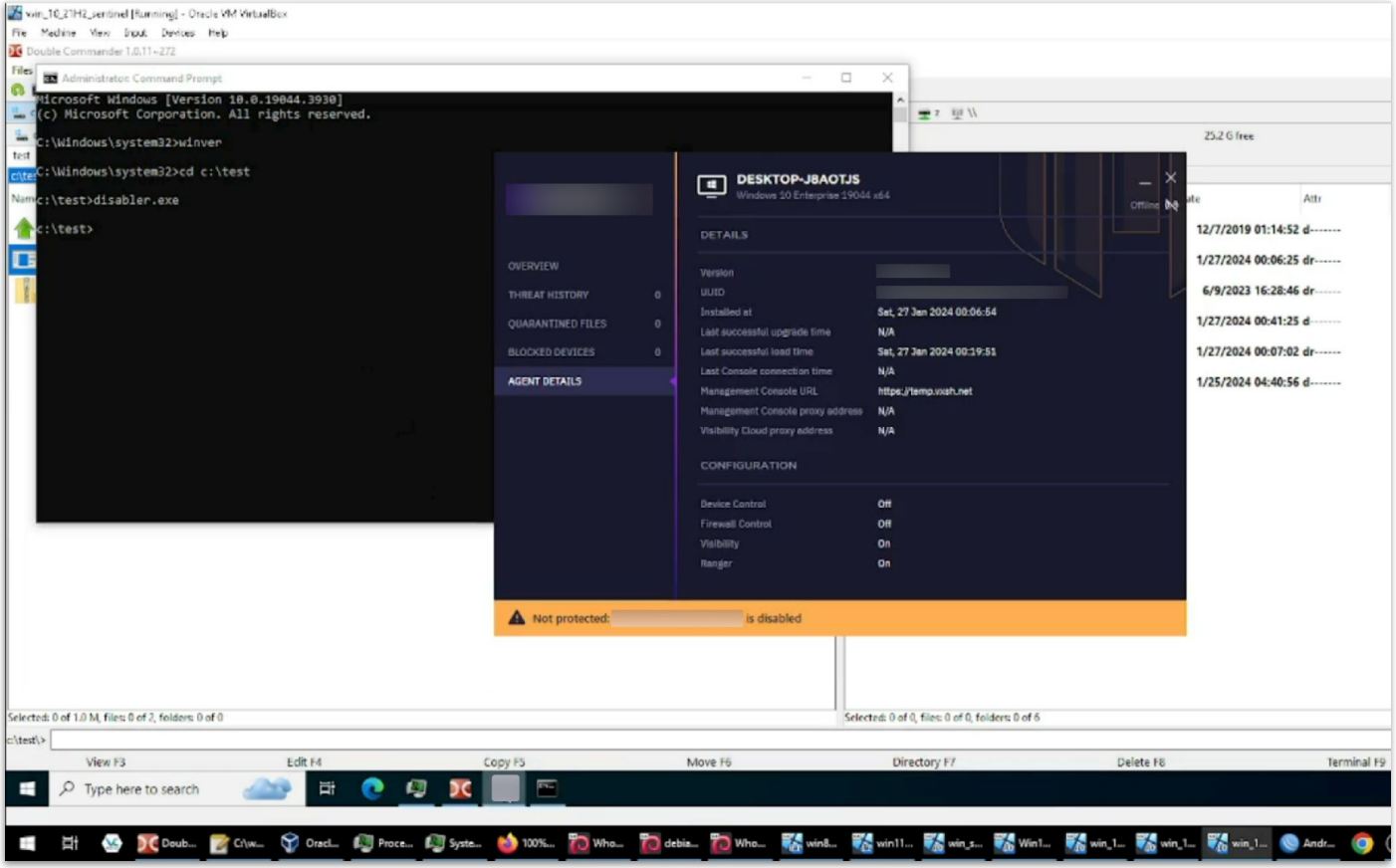
Дата подписания (принятия) работ (услуг) 29.03.2024

Name of Kazakhstan based limited liability corporation

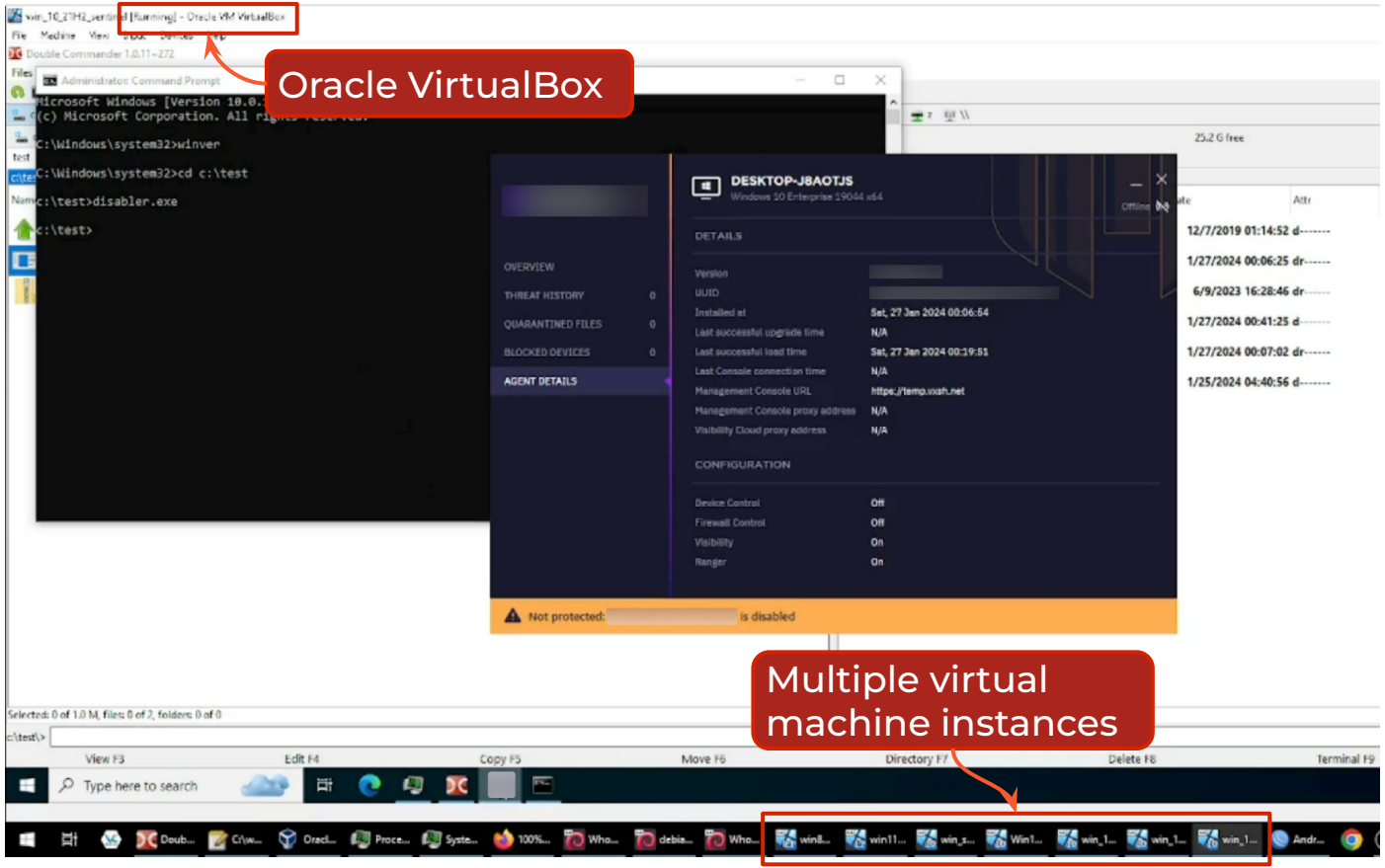
Organization submitting an expense for renting 30 Mercedes.

Hiding in Plain Sight: Clues in the Recordings

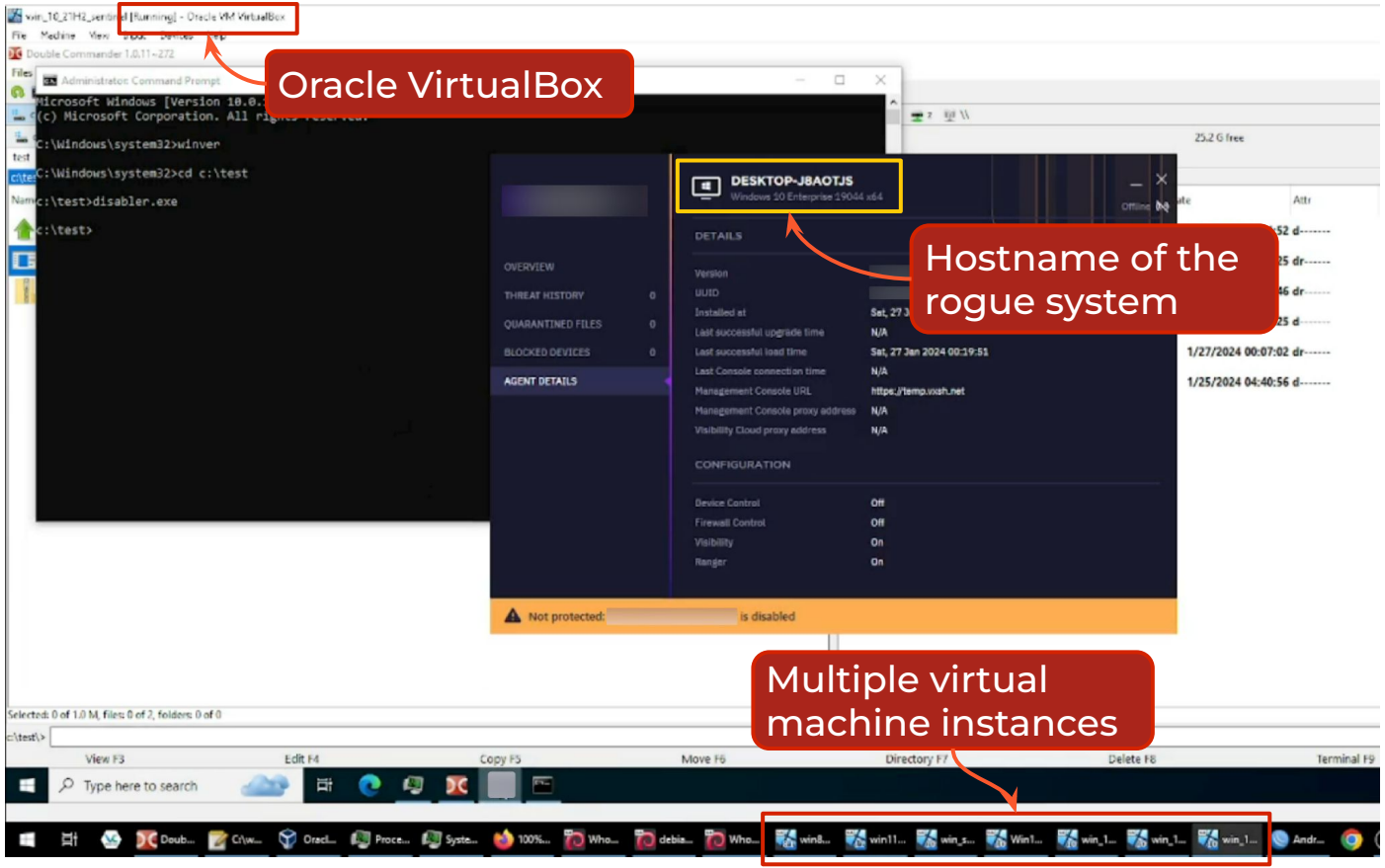
Analysis of Demo Recording



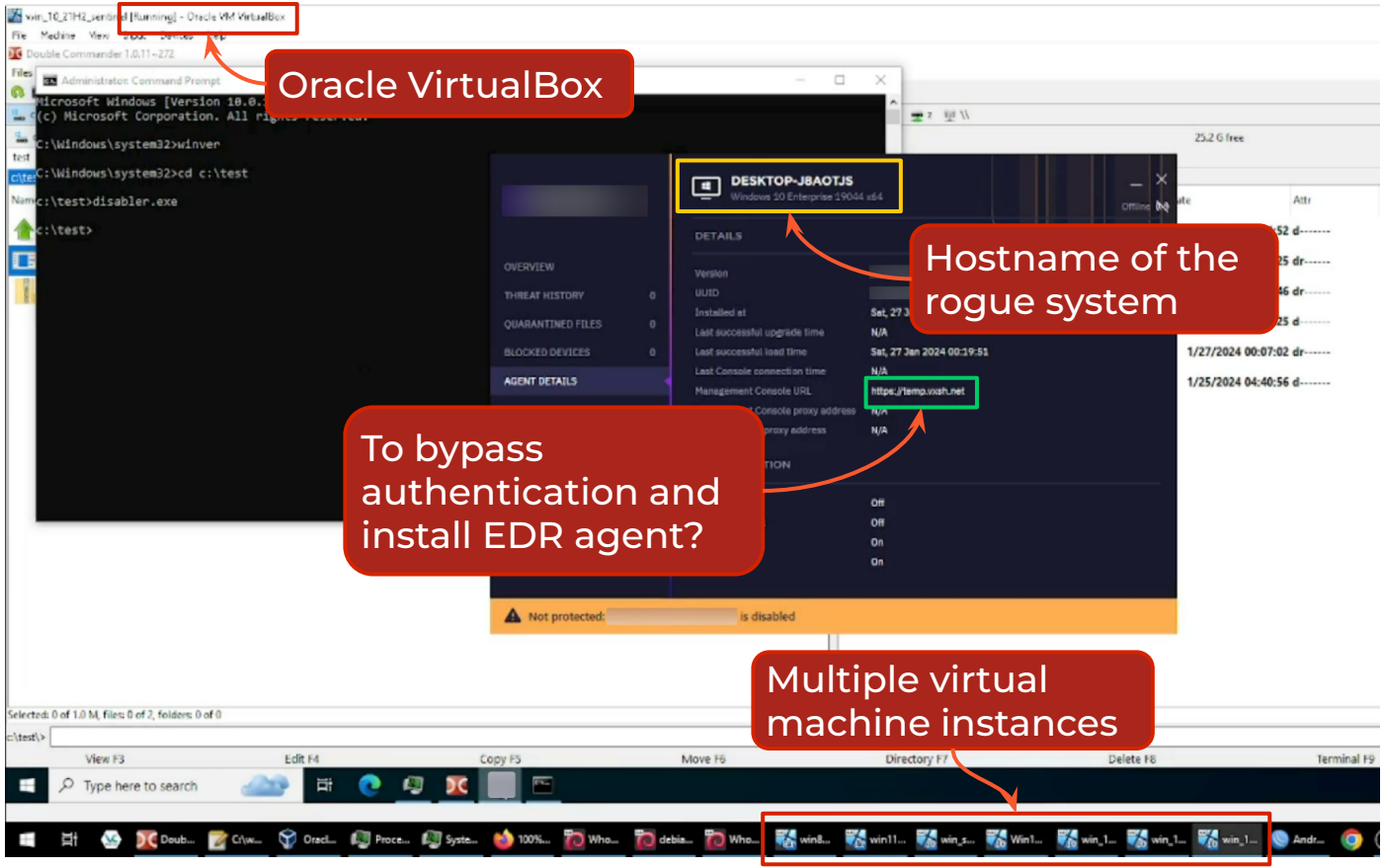
Analysis of Demo Recording



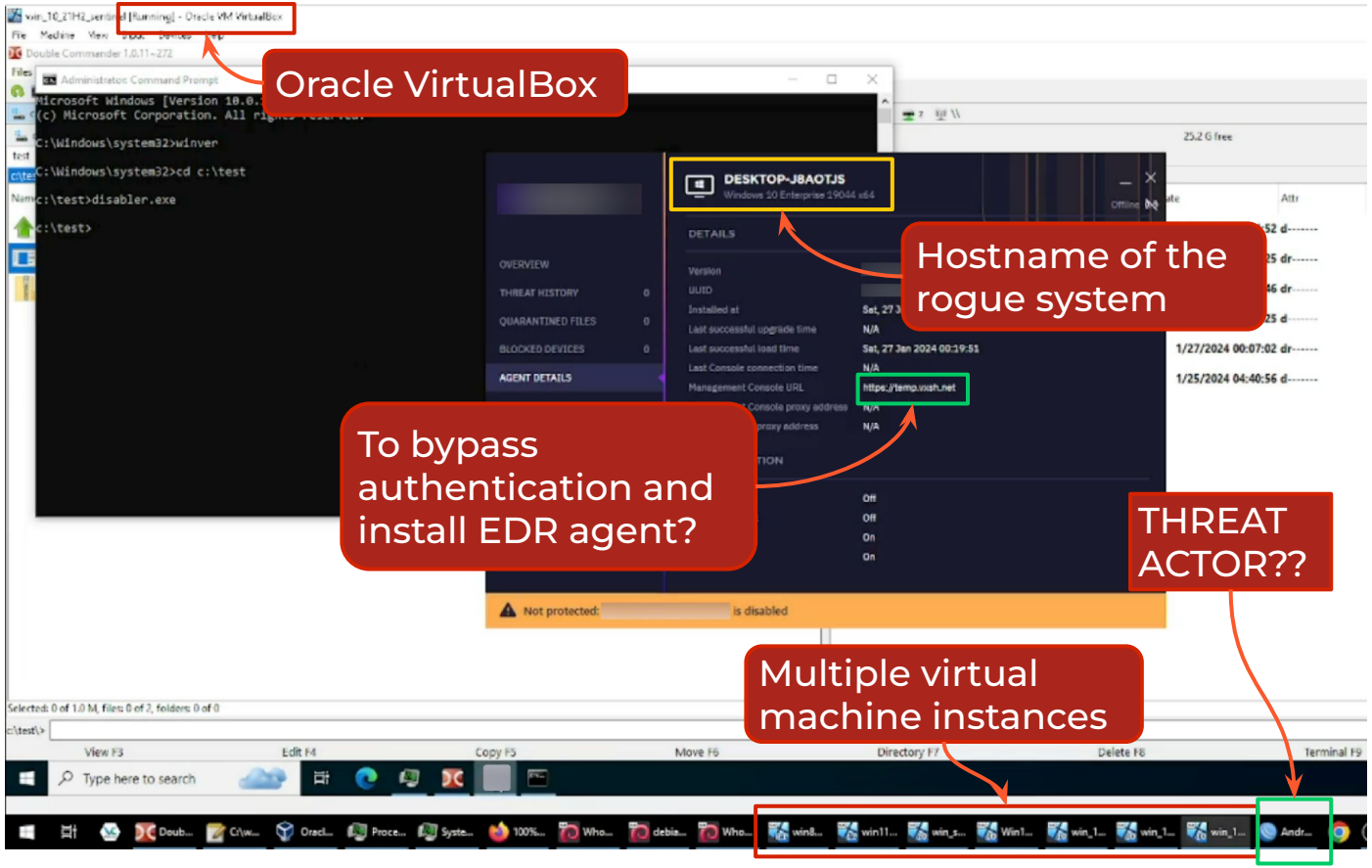
Analysis of Demo Recording



Analysis of Demo Recording



Analysis of Demo Recording



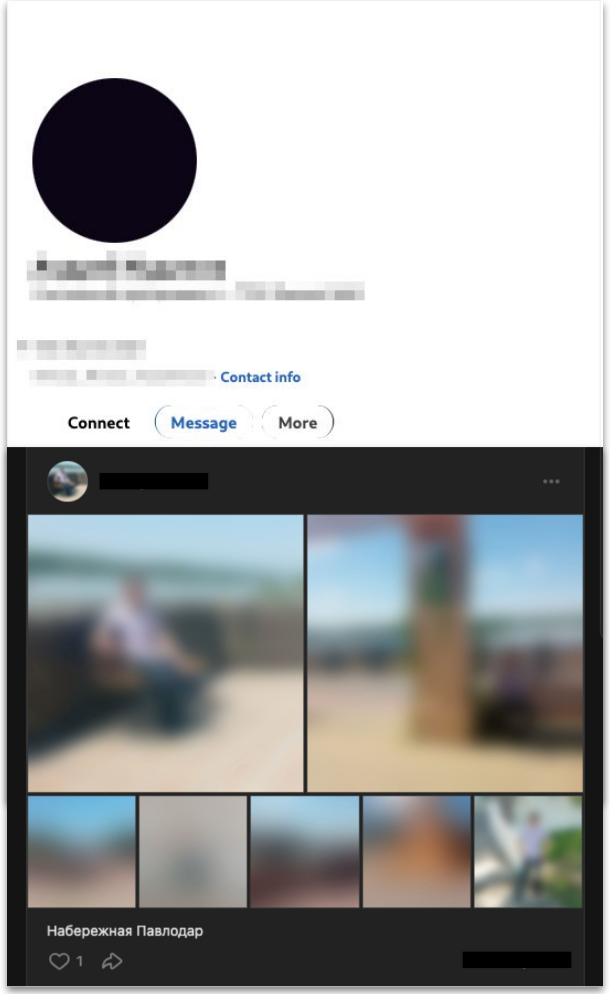
Analysis of Demo Recording

- Another video recording revealed a critical clue: a larger portion of the actor's username was now visible.

Unmasking KernelMode

Unmasking the Actor

- **OpSec Failure**: The demo video and P-1 form exposed two key identifiers: the name **"Andry"** and a specific company.
- **LinkedIn Pivot**: Identified a profile for "Andry" showing employment at the company from the P-1 form.
- **Corroboration**: Found a matching profile on VKontakte (VK), further confirming the individual's identity.



Profiling the Organization

- **Company Background**: Registered in early 2023 as a "software development" business.
- **Location**: Multiple sources list the company's legal address in Saran, Kazakhstan.
- **The Critical Link**: The actor's VK profile lists Saran as their hometown, connecting them to the company's location.

Connecting the Dots

- Recordings of an AV/EDR bypass tool were found on the rogue system.
- These videos matched those sold by the user *KernelMode* on cybercrime forums.
- Demo recordings exposed a name ("Andry") and a P-1 form revealed a company name.
- We pivoted on these two data points to uncover the actor's identity.

Assessment: The KernelMode Connection

- **Moderate Confidence**: The identified individual is the actor *KernelMode*.
- **Likely Role**: We believe they are also the primary developer of the AV/EDR bypass tool.
- **Caveat**: No evidence suggests the rogue system was used for anything beyond testing the AV/EDR bypass.

paloalto NETWORKS | UNIT 42

Thank You

paloaltonetworks.com