UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

CIVIL ACTION NO.

MICROSOFT CORPORATION,

Plaintiff

v.

DOES 1-7

Defendants

FILED UNDER SEAL

DECLARATION OF SEAN ENSZ IN SUPPORT OF PLAINTIFFS' MOTION FOR TEMPORARY RESTRAINING ORDER AND RELATED RELIEF

I, Sean Ensz, declare as follows:

1. I am a Principal Investigator in Microsoft Corporation's Digital Crimes Unit ("DCU"). I make this declaration based upon my personal knowledge, and upon information and belief from my review of documents and evidence collected during Microsoft's investigation into the matters described below.

2. I have been employed by Microsoft since July 2018. In my role at Microsoft, I investigate significant transnational cybercrime and develop threat intelligence to disrupt malicious cyber operations. Prior to joining Microsoft in 2018, I served as the Information Assurance Manager at Devon Energy and spent ten years in information technology at the University of Oklahoma conducting and managing forensic investigations and incident response teams.

3. One of the types of cybercrime I have observed and worked to defend against during the course of my duties at Microsoft is a social engineering tactic called phishing. Phishing attacks use deceptive emails tailored to use deceptive language to elicit fear or urgency by the recipient, to trick them into interacting with the email, such as clicking on a link or opening a file. The intent of phishing typically includes installing malware, stealing someone's account credentials, or to reveal personal information (such as credit card numbers, bank information, or passwords). These emails often include links to websites that appear legitimate but are, in fact, controlled by threat actors as part of their operation to steal information. Files attached in phishing emails may be infected with malicious computer software ("malware") or include hyperlinks to threat actor-controlled websites. Threat actors generally use this tactic on a grand scale ("phishing campaigns") involving repeated, persistent attempts to target multiple victims to achieve their objective.

4. A spear phishing campaign is a related type of attack where phishing emails are tailored to a specific group, organization, or person, to increase the likelihood of stealing their target's credentials and data by convincing them of the email's legitimacy. This often includes: (i) using local language for the subject, body, and sender's name to make it harder for users to identify email as a spear phishing attempt; (ii) email topics that correspond to the recipient's responsibilities in the organization, e.g., sending academic or policy papers; or (iii) using compromised or impersonated email accounts to send spear phishing emails that appear legitimate and from a known sender.

5. I am aware of reports that individuals conducting the types of crimes committed by the Does using the RedVDS infrastructure have employed artificial intelligence tools to both

scale the volume of their communications and tailor the content resulting in a more realistic and convincing email.

6. Another related type of cybercrime I have observed and worked to defend against is a business email compromise attack ("BEC"). A BEC typically involves gaining unauthorized access to a legitimate business email account and using that access to conduct financial fraud. For example, a threat actor may use a legitimate business email account to request that a co-worker or customer send money or information to a threat actor masquerading as the real owner of the legitimate-but-compromised business email address.

7. Another common fraud associated with such tactics involves the purchase and sale of real estate. Fraudsters have become proficient at targeting businesses and consumers during real estate transactions. The fraudsters specifically target such transactions during time sensitive periods, such as when deposits are due or during similar time sensitive money transfers are exchanged. Fraudsters inject themselves into the email communications typically substituting wire or ACH banking instructions to divert funds to accounts controlled by them. I have observed use of similar tradecraft in connection with Defendants financial fraud against Microsoft's co-plaintiffs in this case, which involved a deliberate effort to time fraudulent communications to coincide with expected payment transactions.

8. Email based attacks like those described above typically involve use of network infrastructure that permits threat actors to scale and anonymize their activities. For example, threat actors commonly use third party hosting services, virtual computer services, proxy services, and other such infrastructure to create a network of computers to remotely carry out such attacks. This eliminates the need for threat actors to maintain and use local computers and IP addresses that might be traced back directly to the threat actor.

9. I have been one of the Microsoft personnel responsible for investigating a group of operators distributing, monetizing, and using unauthorized copies of Windows Server 2022, including in connection with malicious BEC, phishing, and spear phishing campaigns. These threat actors are referred to collectively by Microsoft as Storm-2470 and/or as the "RedVDS Enterprise." Other Microsoft personnel I have worked with in investigating the RedVDS Enterprise include Director of Innovation and Research Donal Keating and Principal Investigator in Microsoft Corporation's Digital Crimes Unit Maurice Mason. In addition to relying on materials cited in this declaration, I have also relied on information provided by Mr. Keating and Mr. Mason, including the information stated in their declarations in this case. I have also relied on information provided by Geoffrey Noyes and Josh Blackwell.

Defendants and the RedVDS Enterprise

10. Microsoft has identified in its complaint 7 DOE Defendants associated with creating, distributing, operating, and selling unauthorized copies of Windows Server. Windows Server is Microsoft's enterprise server platform that enables organizations to run and secure applications, services, and workloads across on-premises, hybrid, and cloud environments. From a user interface perspective, Windows Server is similar to the common version of Windows that most users are familiar with, but Windows Server has additional features designed to help manage data and applications across multiple computers.

11. Defendants' scheme involves using unauthorized copies of Windows Server to provide software-as-a-service and infrastructure-as-service for malicious purposes like business email compromises and sophisticated phishing activities. Defendants are referred to collectively in the complaint as the persons responsible for conducting the affairs of the "RedVDS Enterprise."

12. DOE 1 is the creator, owner, and/or controller of the webpages located at the URLs redvds[.]com, redvds[.]pro, and vdspanel[.]space, and the subdomains of those URL ("RedVDS Domains"). The RedVDS Domains are used by the Defendants to market, sell, distribute, and/or operate the unauthorized copies of Windows Server and associated services described in Microsoft's complaint. RedVDS Domains host webpages that include a user portal that can be used to control virtual instances of Windows Server, webpages that facilitate end user purchases of additional unauthorized instances of Windows Server, and webpages offering customer support through chat sessions and a chat bot. The RedVDS Domains also facilitate API functionality that permits users to control numerous computers at scale. The RedVDS Domains also facilitate a referral bonus program and loyalty program through which end users can share in the ill-gotten profits generated by the RedVDS Enterprise. I believe that a reasonable opportunity for discovery will yield evidence that DOE 1 resides outside the United States. **Figure 1** below depicts the RedVDS user interface with annotations I created to show sub panel and backup site functionality built into the website.

Fig. 1

13. DOE 2 makes ongoing a use of the RedVDS Enterprise's services to send fraudulent emails to and from recipients located in the United States. DOE 2 has used unauthorized depictions of Microsoft's trademark and logo in executing a business email compromise (BEC) scheme. One of DOE 2's BEC schemes involved victim companies with locations in Washington and Florida. DOE 2 compromised one victim company's email system and used unauthorized access to that system to intercept private email communications and to send fraudulent emails to GDCA employees in March and April 2025, resulting in financial losses due to GDCA's reliance on DOE 2's fraudulent email communications. DOE 2 operates these types of fraudulent email campaigns at scale, resulting in transmission of thousands of emails containing false and misleading depictions of Microsoft's trademarks.

14. DOE 3 makes ongoing a use of the RedVDS Enterprise's services to send fraudulent emails to and from recipients located in the United States. One of DOE 3's BEC schemes involved a European corporation and a Florida corporation headquartered in Alabama,

H2. DOE 3 gained unauthorized access to H2's email system and used that unauthorized access to intercept private email communications and to send fraudulent emails to H2 commencing in mid-April 2025. H2 was deceived by DOE 3's emails and transferred money to an account controlled by DOE 3 in April and May 2025 in reliance on DOE 3's fraudulent emails, which impersonated an actual employee of the European corporation.

15. DOE 4 makes ongoing a use of the RedVDS Enterprise's services to send fraudulent emails to and from recipients located in the United States. One of DOE 4's phishing campaigns used attached pdf files impersonating HR compensation summaries that contained QR codes to deceive the recipients into providing their account credentials. DOE 4 operates these types of fraudulent email campaigns at scale, resulting in transmission of thousands of emails containing false and misleading attachments.

16. DOE 5 makes ongoing a use of the RedVDS Enterprise's services to send fraudulent emails to and from recipients located in the United States. DOE 5 is primarily engaged in unauthorized email account takeover, likely after a successful phishing attack where account credentials were stolen. I am informed and belief that DOE 5 attempted, and may have been successful, in accessing many user accounts in 2025. Some of the accounts accessed belong to Real Estate, Construction, and Insurance companies in the United States, and located in Florida, California, Wisconsin, and Alabama.

17. DOE 6 makes ongoing a use of the RedVDS Enterprise's services to send fraudulent emails to and from recipients located in the United States. DOE 6 is primarily engaged in unauthorized email account takeover, likely after a successful phishing attack where account credentials were stolen. DOE 6 attempted, and may have been successful, in accessing many accounts in 2025. Some of the accounts accessed belonging to Accounting and

Manufacturing companies in the United States, and located in Florida, California, and New York.

18. DOE 7 makes ongoing a use of the RedVDS Enterprise's services to send fraudulent emails to and from recipients located in the United States. DOE 7 is primarily engaged in unauthorized email account takeover, likely after a successful phishing attack where account credentials were stolen. DOE 7 attempted, and may have been successful, in accessing many accounts in 2025. Some of the accounts accessed belonging to Education Institutions in the United States, and located in Florida and Texas.

19. In conducting the RedVDS Enterprise, Defendants have taken advantage of the privilege of conducting business in Florida. For example, in carrying out the scheme described in this complaint, (i) RedVDS contracted with and used the hosting services of ReliableSite.Net LLC, a U.S. company headquartered in Miami, Florida, (ii) sent fraudulent communications to victims in Florida, (iii) received monies from victims located in Florida, and (iv) otherwise directed their activities towards Florida corporations and Florida residents, in addition to targeting other victims around the United States and the World.

20. In conducting the RedVDS Enterprise, Defendants have also taken advantage of the privilege of conducting business in the United States, for example by contracting with and/or utilizing the services of Cloudflare, Inc., a U.S. company headquartered in San Francisco, California that provides network infrastructure and proxy services, contracting with and/or utilizing the services of Interserver, Inc., a U.S. hosting company located in Secaucus, New Jersey, and contracting with and/or utilizing the services of Verisign, Inc., a U.S. Company, to register and use the RedVDS ".com" domains.

21. The RedVDS Enterprise markets, sells, hosts, and uses unauthorized evaluation copies of Windows Server 2022 in virtual environments that can be remotely accessed from any computer connected to the internet. DOE 1 markets RedVDS as a service that allows users to remotely access a virtual Windows desktop that can then be used as a server to facilitate network operations for multiple computers. For example, a user can use one computer to remote into a RedVDS virtual Windows Server running on a different computer and use that Windows Server computer as a hub for controlling networks of other computers. In other words, RedVDS is selling and operating a grey-market Windows Server evaluation copies over which Microsoft has no control. Because Microsoft cannot control RedVDS's distribution of images containing unauthorized copies of Windows Server, Microsoft cannot ensure that those instances of Windows Server have the latest security patches and cannot control what other software applications are installed on the image.

22. The RedVDS Enterprise distributes and controls unauthorized images and copies of the original Windows Server and Windows Server Key through websites accessible at the RedVDS Domains. I believe Defendants have distributed and used thousands of unauthorized copies of Windows Server through the RedVDS domain.

23. The RedVDS Enterprise engages and uses the services of other third-party hosting providers and installs unauthorized copies of Windows Server on those hosting providers' servers, including within the United States. RedVDS then sells access to these copies of Windows Server to end users at a rates ranging from $24 to $80 per month. RedVDS maintains a significant number of active virtual servers monthly. These servers are used by cybercriminals, facilitating a wide range of illicit activities targeting Microsoft and its customers. Microsoft's Digital Crimes Unit has linked RedVDS infrastructure to numerous security incidents and has

determined that RedVDS is a significant and persistent enabler of attacks against users of Microsoft's operating systems, communications services, and cloud computing services.

24. Commencing in 2024, Microsoft observed the existence of numerous malicious Windows virtual hosts, all using the same host name of "WIN-BUNS25TD77J". Further investigation revealed that the WIN-BUNS25TD77J identifier is associated with thousands of stolen credentials, invoices, mass mailers, and phish kits. Microsoft determined that the host machines associated with WIN-BUNS25TD77J were all created from the same virtual computer image. These images contain the cloned evaluation copy of Windows Server 2022 discussed above.

25. RedVDS's user interface makes prominent use of Microsoft's trademarks and logo. **Figure 2** below depicts the RedVDS user interface displaying Microsoft's trademarks and Windows logo:

Fig. 2

26. **Figures 3 and 4** below depict the user interface encountered by DOES 1-7 and other users of the RedVDS Enterprise's services upon executing RedVDS hosted copies of Windows Server.

Fig.3

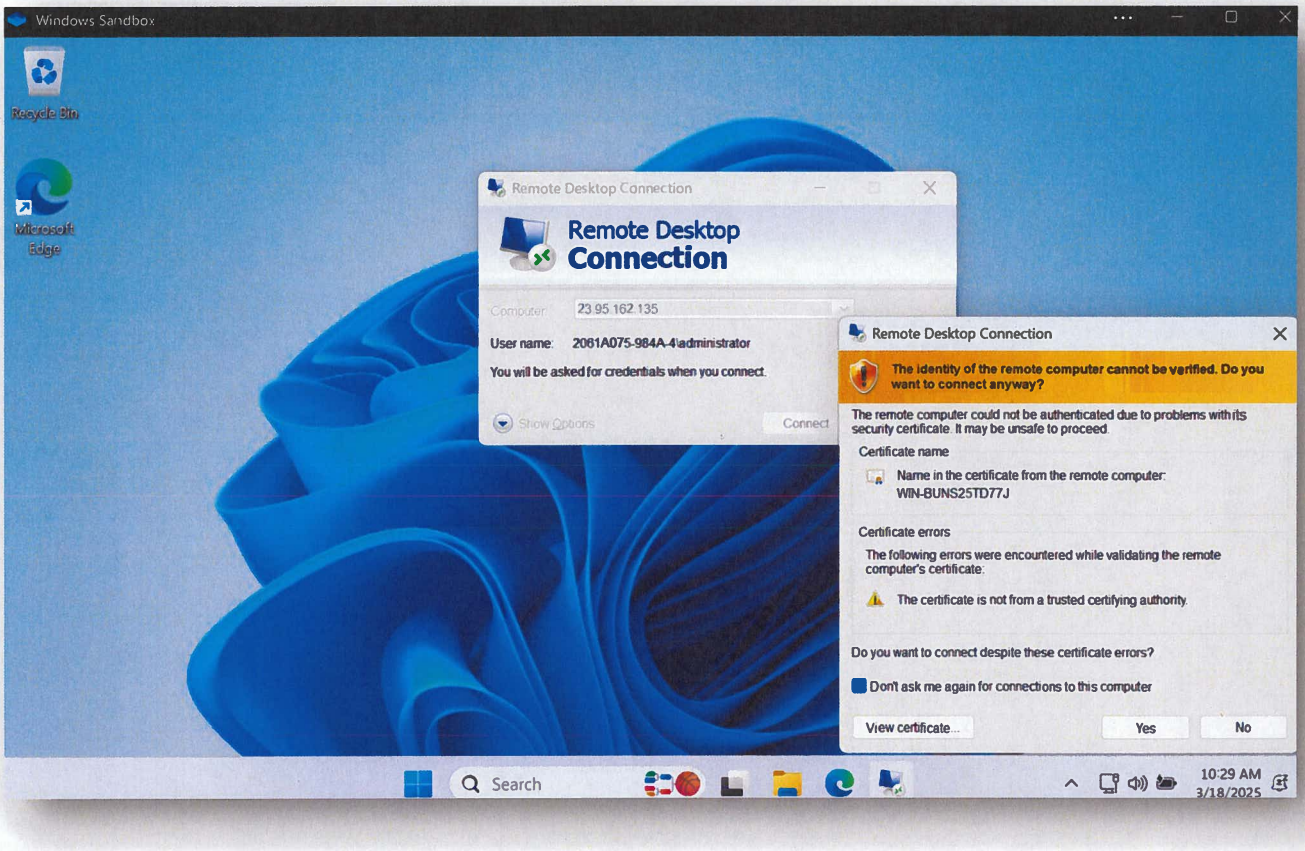
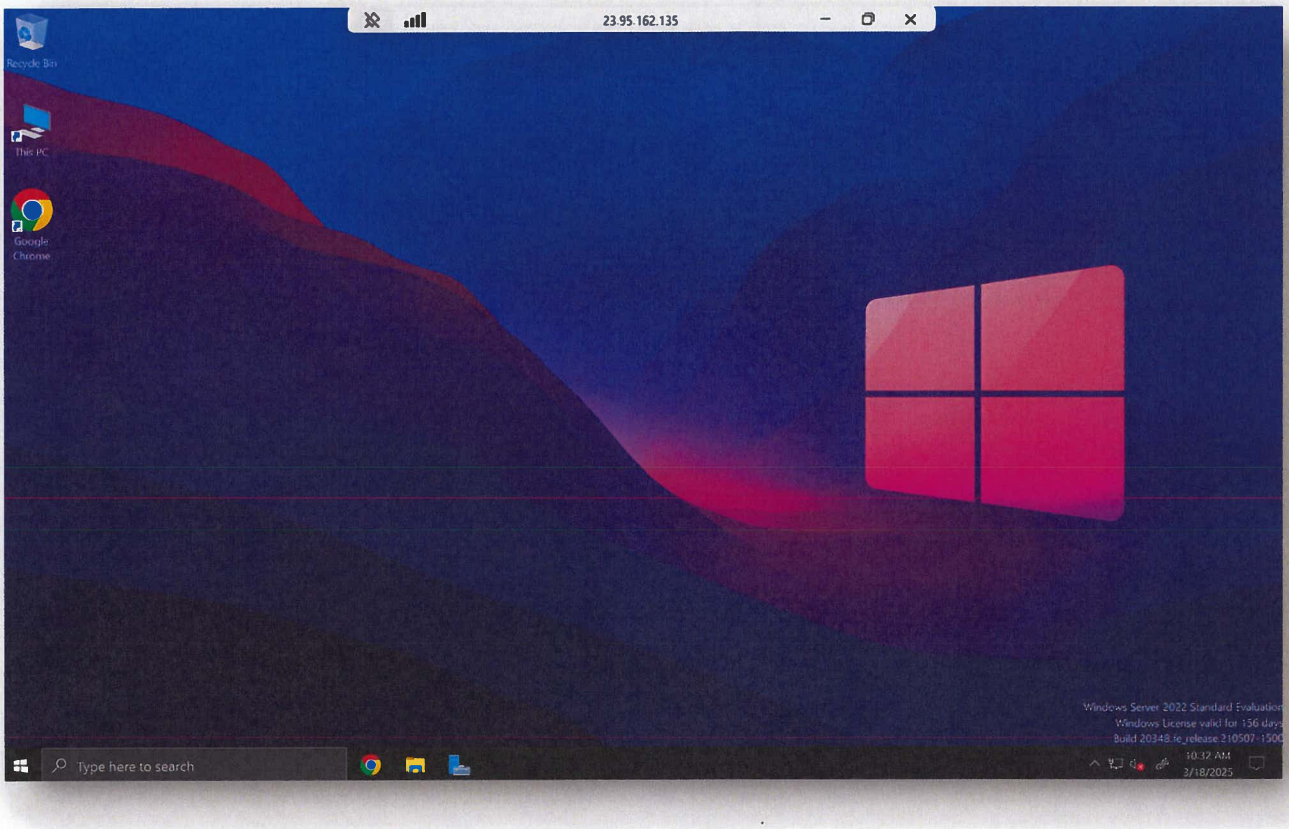

Windows Sandbox
Recycle Bin
Microsoft Edge
Remote Desktop Connection
Remote Desktop Connection
Computer: 23.95.162.135
User name: 2061A075-984A-4\administrator
You will be asked for credentials when you connect.
Show Options
Connect
Remote Desktop Connection
The identity of the remote computer cannot be verified. Do you want to connect anyway?
The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.
Certificate name
Name in the certificate from the remote computer:
WIN-8UNS25TD77J
Certificate errors
The following errors were encountered while validating the remote computer's certificate:
The certificate is not from a trusted certifying authority.
Do you want to connect despite these certificate errors?
Don't ask me again for connections to this computer
View certificate...
Yes
No
Search
10:29 AM
3/18/2025

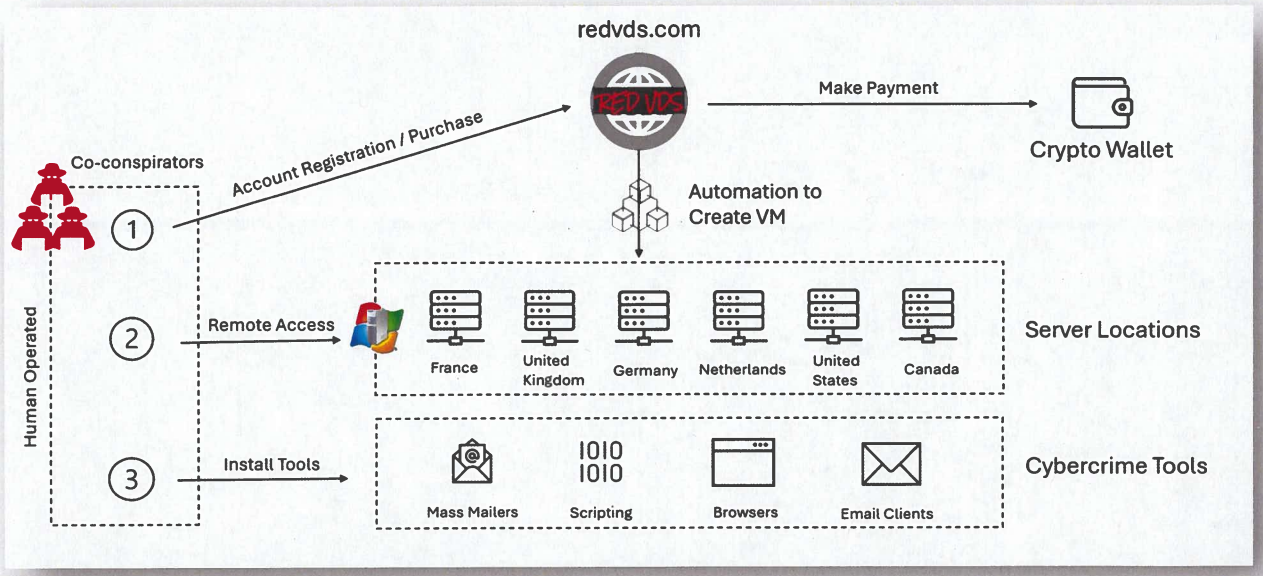
Fig. 4



27. End users purchasing and using services from the RedVDS Enterprise typically tender payment to DOE 1 via one or more crypto wallets. I understand from the declaration of Maurice Mason that DOE 1 has received over $5.3MM of BTC and LTC cryptocurrency payments since June 2023, and that it is likely that DOE 1 has made much more money this year in the form of other cryptocurrency payments.

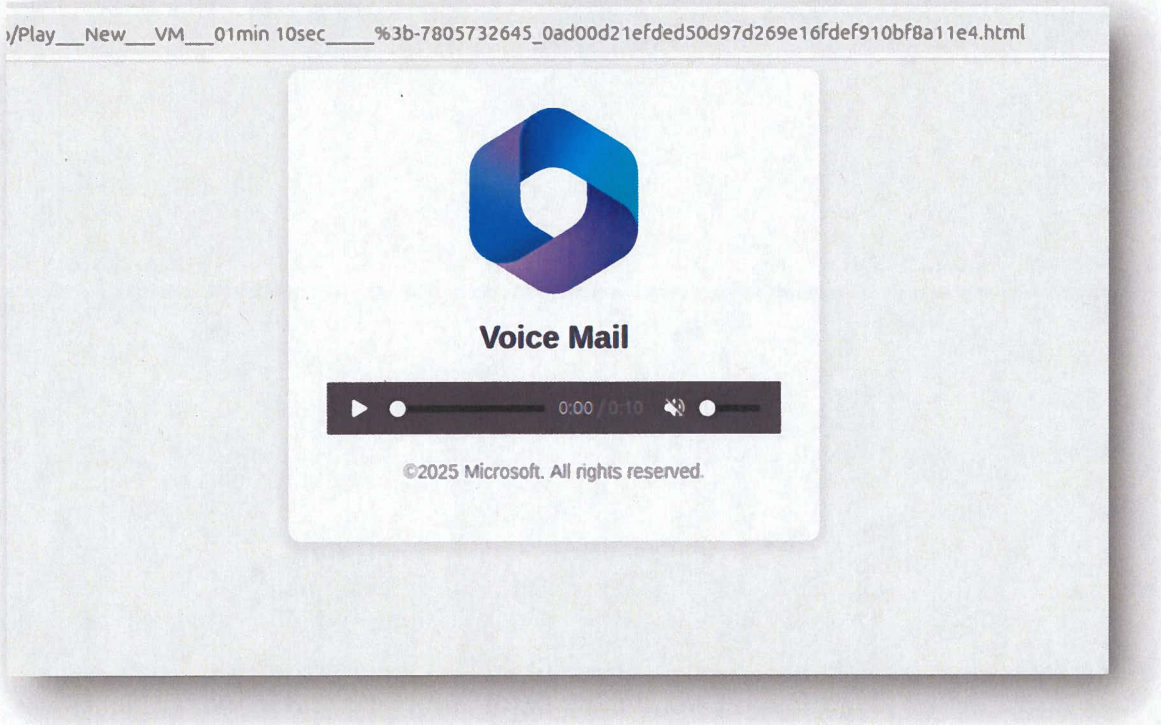
28. After receiving payment, the RedVDS Enterprise deploys an automated process to create a virtual machine for the end user using the image and copy of Windows Server 2022 discussed above. End users then use the virtual machine image, Windows Server software, and hosting services provided by the RedVDS Enterprise to remotely access and control a virtual computers, commonly for malicious purposes. **Figure 5** below depicts the basic architecture of the RedVDS hosting service.

Fig. 5



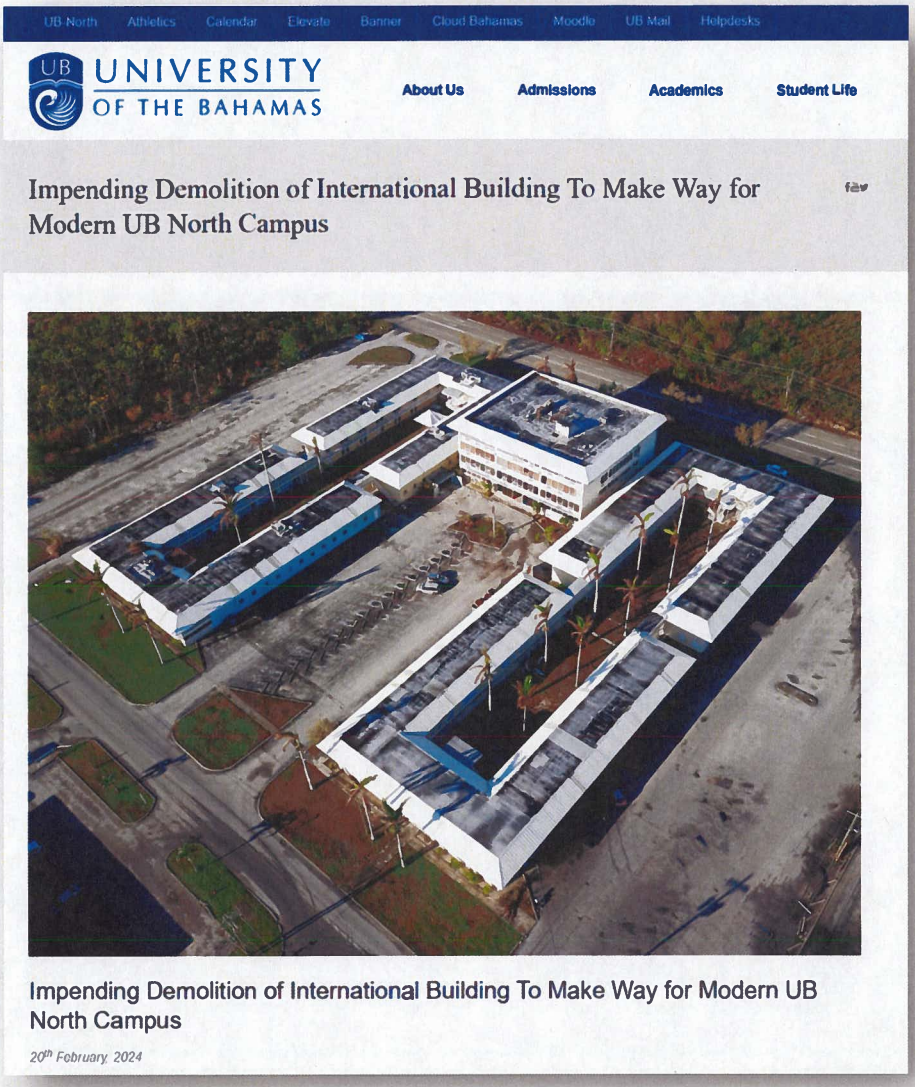
29. RedVDS users unlawfully use Microsoft's copyright protected software and/or Microsoft's well-known trademarks to carry out various forms of wire fraud. For example, **Figure 6** below depicts and DOE 2's misuse of Microsoft's trademark and Microsoft 365 logo in a malicious email.

Fig. 6



30. Investigation into the RedVDS Domains revealed that RedVDS is not a registered company or legal entity in any state or nation. The Terms of Service indicate it is governed by Bahamian Law, and the domain registration for the RedVDS URL provides what appears to be a fake name ("David Rico") and fake address. For example, the domain registrant address given for RedVDS corresponds to a University of the Bahamas International Building that has been demolished. **Figure 7** below depicts a University of the Bahamas webpage discussing the impending demolition of the subject building.

Fig. 7



31. The use of fake name and address information is consistent with trade craft commonly used by perpetrators of software piracy and cybercrime schemes.

32. Other elements of trade craft that I have observed being commonly used by cybercriminals are associated with RedVDS and its users. For example, the use of attachments and file types associated with known copyrighted software and well-known company trademarks are tactics frequently used by cybercriminals to bolster the effectiveness of their schemes.

33. As noted above, reports indicate the use of AI tools by persons associated with the RedVDS infrastructures. One victim report indicates the use of AI voice generation tools to impersonate individuals and further deceive recipients of such email communications. Based on my experience in such investigations, and my review of publications by other security experts in the field, I believe many of the same users of RedVDS infrastructure likely employed artificial intelligence face-swapping and voice cloning services while defrauding victims,[1] Such tactics are increasingly used by criminals, in particular actors engaged in fraud and scams, to impersonate others and to conceal their true identities, all for the purpose of deceiving victims. I similarly am aware that artificial intelligence is increasingly used by actors engaged in fraud and scams to not only generate compelling content—for example, to draft deceptive and professional messages, such as those included in phishing and other emails used to facilitate fraud—but also for translation purposes—namely, to translate those messages into different languages, which has the effect of eliminating spelling and grammatical mistakes and culturally unique nuances that frequently raised suspicions of potential victims.

Disruption Strategy

34. Microsoft is coordinating with industry partners and law enforcement to disrupt Defendants' operations and infrastructure. Microsoft's efforts, if successful, should effectively

---

[1] *See, e.g.,* The Rise of the AI-Cloned Voice Scam (https://www.americanbar.org/groups/senior_lawyers/resources/voice-of-experience/2025-september/ai-cloned-voice-scam/); Police warn of AI voice cloning scams « Euro Weekly News (https://euroweeklynews.com/2025/12/14/police-warning-ai-scams-are-cloning-loved-ones-voices-and-this-simple-trick-could-save-you/); The Ultra-Realistic AI Face Swapping Platform Driving Romance Scams | WIRED (https://www.wired.com/story/the-ultra-realistic-ai-face-swapping-platform-driving-romance-scams/); Popular property scam on rise as nearly every Aussie fooled - realestate.com.au (https://www.realestate.com.au/news/popular-property-scam-on-rise-as-nearly-every-aussie-fooled/).

disrupt the infrastructure needed to operate the RedVDS Enterprise and should yield additional information about Defendants and their activities. In this civil action, Microsoft seeks seizure of two RedVDS domains controlled by U.S.-based registries: "redvds.com" and "redvds.pro". Microsoft's requested relief will facilitate discovery and notice efforts in addition to preventing ongoing malicious use of the domains.

35. The domain "redvds.com" is subject to the authority of Verisign, Inc., a U.S. Company. An order directing Verisign to send traffic to this domain to computers controlled by Microsoft will remove Defendants control over the domain and will permit Microsoft to provide notice to users that they or their computers are attempting to communicate with unauthorized copies of Windows Server that are not genuine and that are associated with the RedVDS Enterprise's malicious activities.

36. The domain "redvds.pro" is subject to the authority of Identity Digital, Inc., a U.S. Company. An order directing Identity Digital to send traffic to this domain to computers controlled by Microsoft will remove Defendants control over the domain and will permit Microsoft to provide notice to users that they or their computers are attempting to communicate with unauthorized copies of Windows Server that are not genuine and that are associated with the RedVDS Enterprise's malicious activities.

37. In order for Microsoft's strategy to be effective, it is important that the Defendants not receive prior notice of this action. Prior notice would allow Defendants to set up new infrastructure that would diminish the effectiveness of the disruptive efforts of Microsoft and its partners and would create the potential for loss of evidence that is likely to be obtainable if Microsoft's ex parte TRO request is granted. I know from DCU's past experience in other actions that defendants in cases like this almost always move their infrastructure and/or attempt

to destroy evidence once they learn that Microsoft is bringing a civil case to disrupt their activities.

38. To date, it has not been possible to definitively determine precise physical addresses for Defendants. Defendants do not disclose their legal name, complete physical address, or other physical contact information if they can avoid doing so. Microsoft believes that a reasonable opportunity for discovery may yield attribution evidence for each Defendant or other information that can be used to communicate with Defendants.

39. Attached hereto as Exhibit 1 is a true and correct copy of a screen shot I created of the RedVDS user interface accessible via the URL redvds.com.

40. Attached hereto as Exhibit 2 is a true and correct copy of a screen shot I created of the RedVDS user interface accessible via the URL redvds.com that depicts Microsoft trademarks.

41. Attached hereto as Exhibit 3 is a true and correct copy of a screen shot I created of the user interface for the Windows Server software hosted by RedVDS.

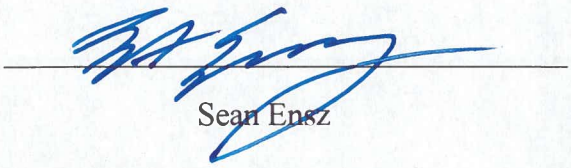
42. Attached hereto as Exhibit 4 is another true and correct copy of a screen shot I created of the user interface for the Windows Server software hosted by RedVDS.

43. Attached hereto as Exhibit 5 is a true and correct copy of diagram I created depicting the RedVDS Enterprise architecture.

44. Attached hereto as Exhibit 6 is a true and correct copy of a screenshot I created from an email reflecting DOE 2's misuse of Microsoft's trademark and Microsoft 365 logo in a malicious email.

45. Attached hereto as Exhibit 7 is a true and correct copy of a screenshot I created from a University of the Bahamas webpage.

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct to the best of my knowledge, information, and belief. Executed this 6th day of January, 2026.



Sean Ensz

Exhibit 1

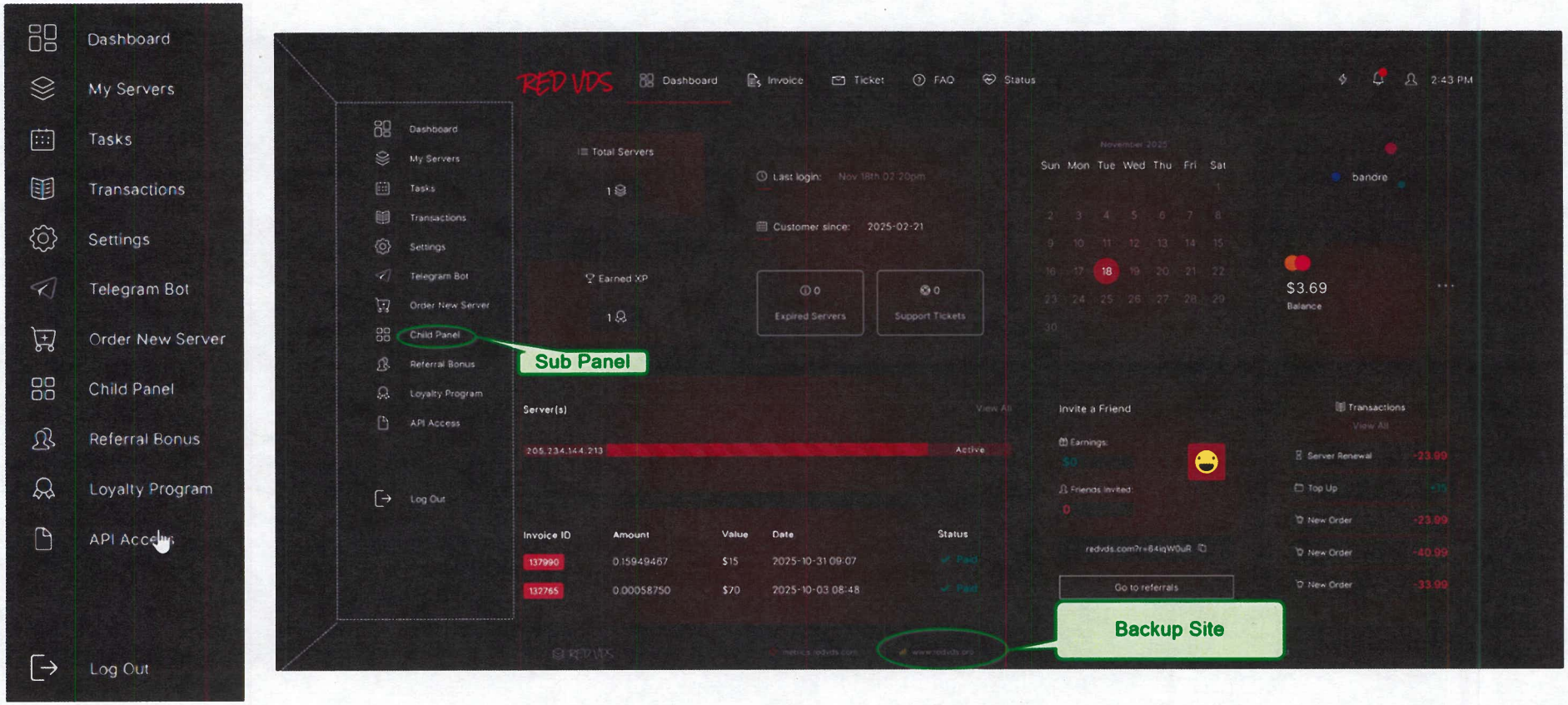

Dashboard
My Servers
Tasks
Transactions
Settings
Telegram Bot
Order New Server
Child Panel
Referral Bonus
Loyalty Program
API Access
Log Out
RED VDS
Dashboard
Invoice
Ticket
FAQ
Status
2:43 PM
Total Servers
Last login:
Customer since: 2025-02-21
Earned XP
Expired Servers
Support Tickets
Sub Panel
Server(s)
205.234.144.213
Active
Invoice ID
Amount
Value
Date
Status
137990
0.15949467
$15
2025-10-31 09:07
132765
0.00058750
$70
2025-10-03 08:48
Invite a Friend
Earnings:
Friends Invited:
Go to referrals
Transactions
Server Renewal
Top Up
New Order
New Order
New Order
$3.69
Balance
bandre
Backup Site

Exhibit 2

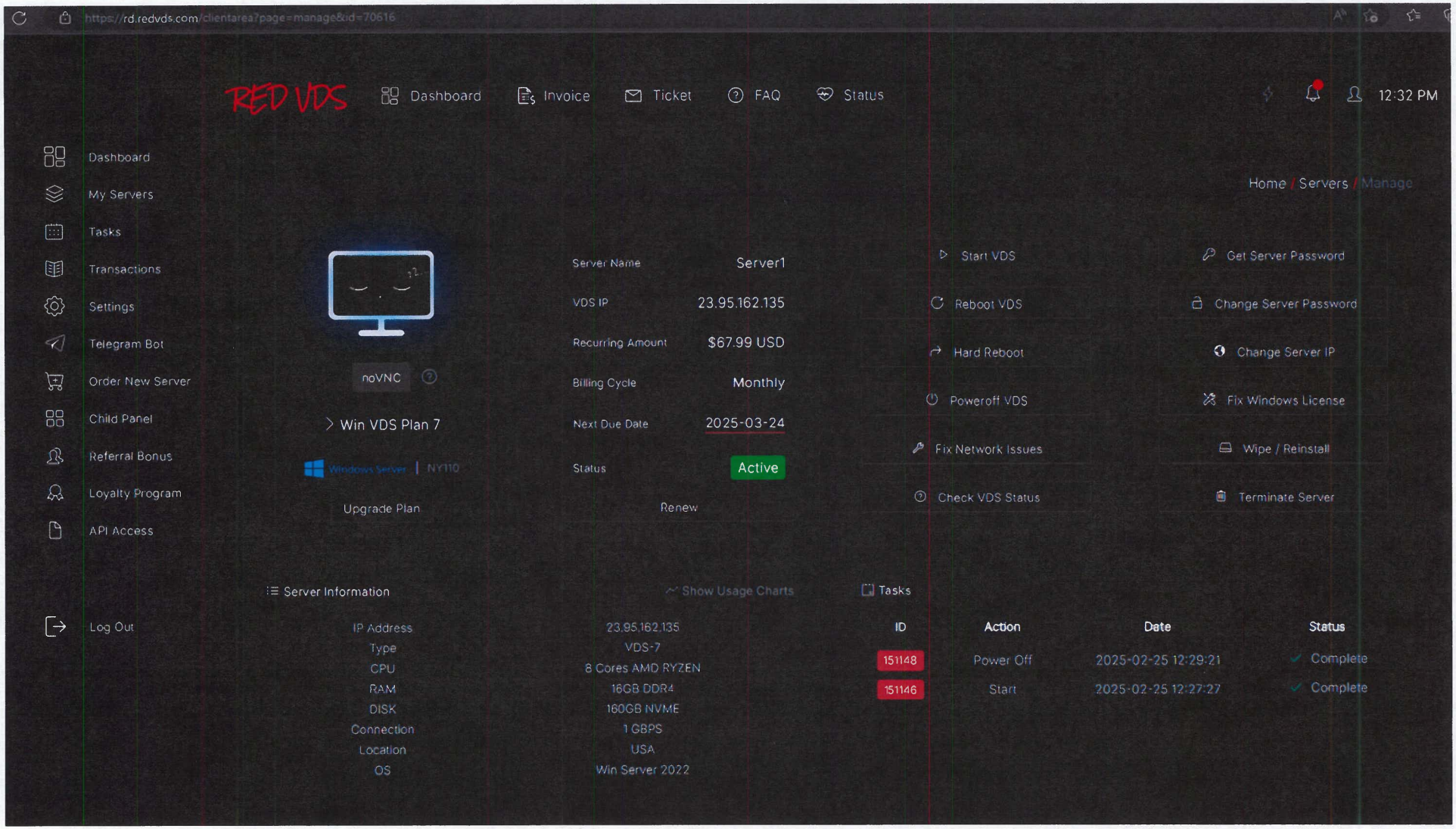

https://rd.redvds.com/clientarea?page=manage&id=70616
RED VDS
Dashboard
Invoice
Ticket
FAQ
Status
12:32 PM
Dashboard
My Servers
Tasks
Transactions
Settings
Telegram Bot
Order New Server
Child Panel
Referral Bonus
Loyalty Program
API Access
Log Out
Home / Servers / Manage
noVNC
Win VDS Plan 7
Windows Server | NY110
Upgrade Plan
Server Name
Server1
VDS IP
23.95.162.135
Recurring Amount
$67.99 USD
Billing Cycle
Monthly
Next Due Date
2025-03-24
Status
Active
Renew
Start VDS
Get Server Password
Reboot VDS
Change Server Password
Hard Reboot
Change Server IP
Poweroff VDS
Fix Windows License
Fix Network Issues
Wipe / Reinstall
Check VDS Status
Terminate Server
Server Information
Show Usage Charts
Tasks
IP Address
23.95.162.135
Type
VDS-7
CPU
8 Cores AMD RYZEN
RAM
16GB DDR4
DISK
160GB NVME
Connection
1 GBPS
Location
USA
OS
Win Server 2022
ID
Action
Date
Status
151148
Power Off
2025-02-25 12:29:21
Complete
151146
Start
2025-02-25 12:27:27
Complete

Exhibit 3

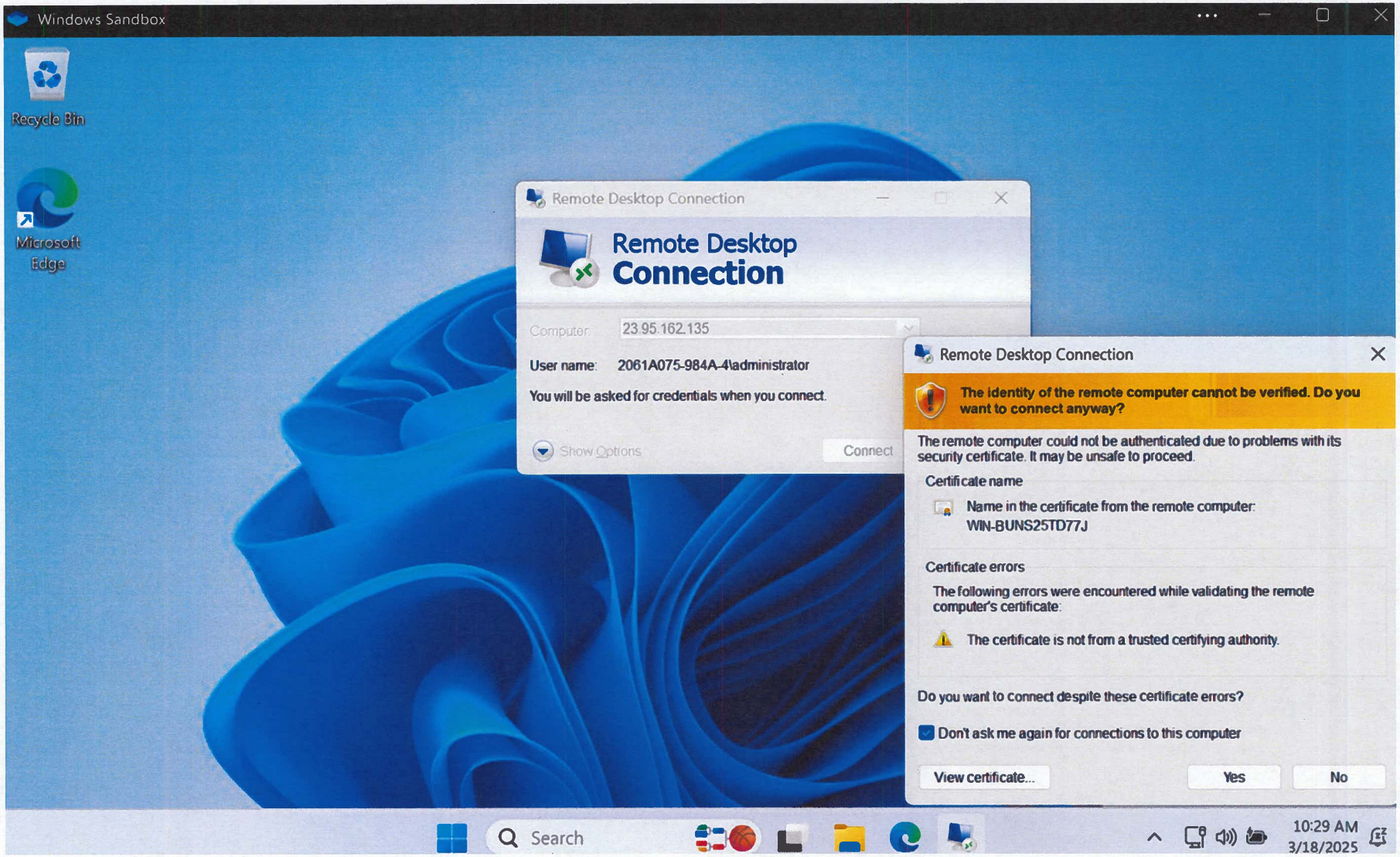

Windows Sandbox
Recycle Bin
Microsoft Edge
Remote Desktop Connection
Remote Desktop Connection
Computer: 23.95.162.135
User name: 2061A075-984A-4\administrator
You will be asked for credentials when you connect.
Show Options
Connect
Remote Desktop Connection
The identity of the remote computer cannot be verified. Do you want to connect anyway?
The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.
Certificate name
Name in the certificate from the remote computer:
WIN-BUNS25TD77J
Certificate errors
The following errors were encountered while validating the remote computer's certificate:
The certificate is not from a trusted certifying authority.
Do you want to connect despite these certificate errors?
Don't ask me again for connections to this computer
View certificate...
Yes
No
Search
10:29 AM
3/18/2025

Exhibit 4

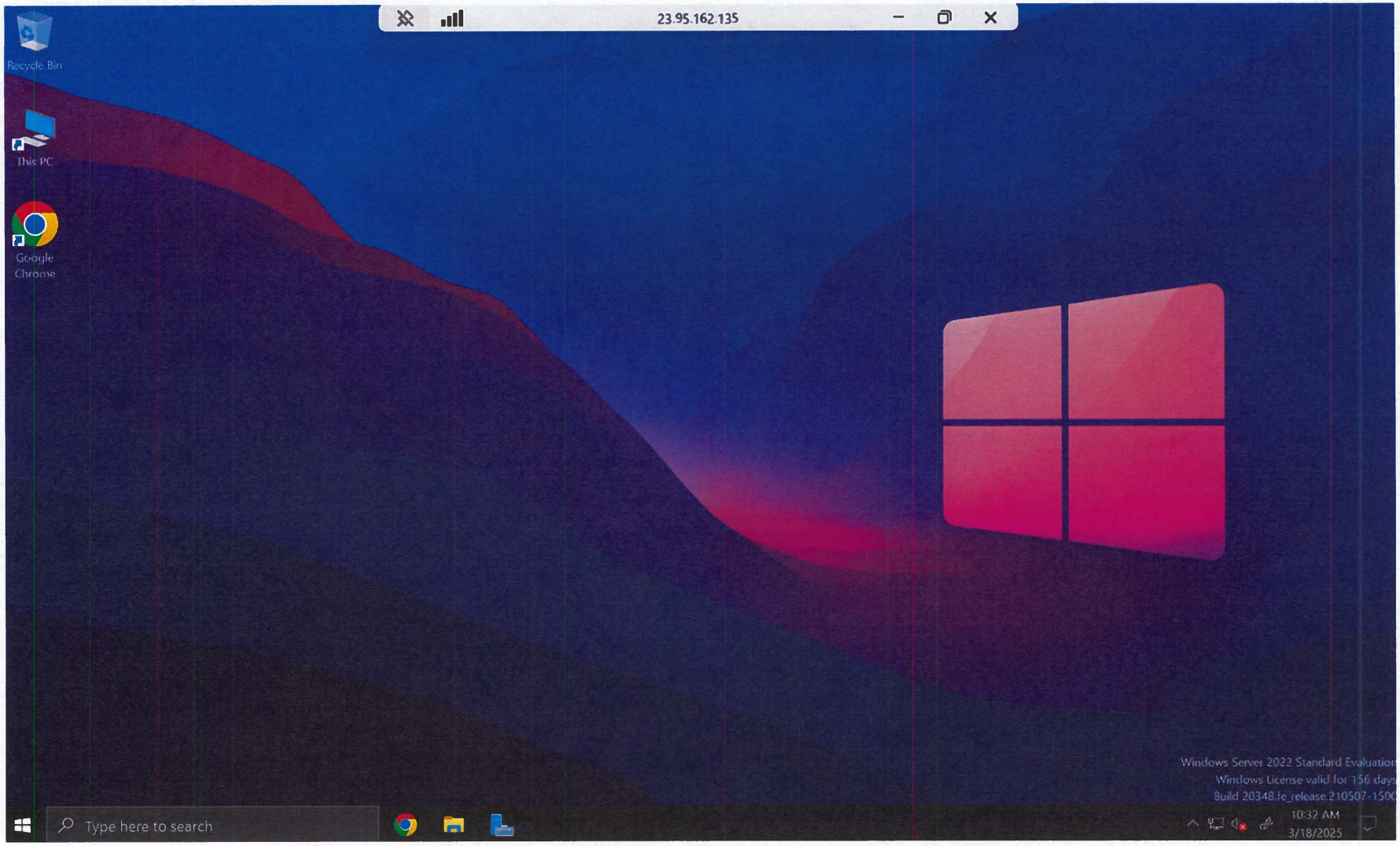

23.95.162.135
Recycle Bin
This PC
Google Chrome
Windows Server 2022 Standard Evaluation
Windows License valid for 156 days
Build 20348.fe_release.210507-1500
Type here to search
10:32 AM
3/18/2025

Exhibit 5

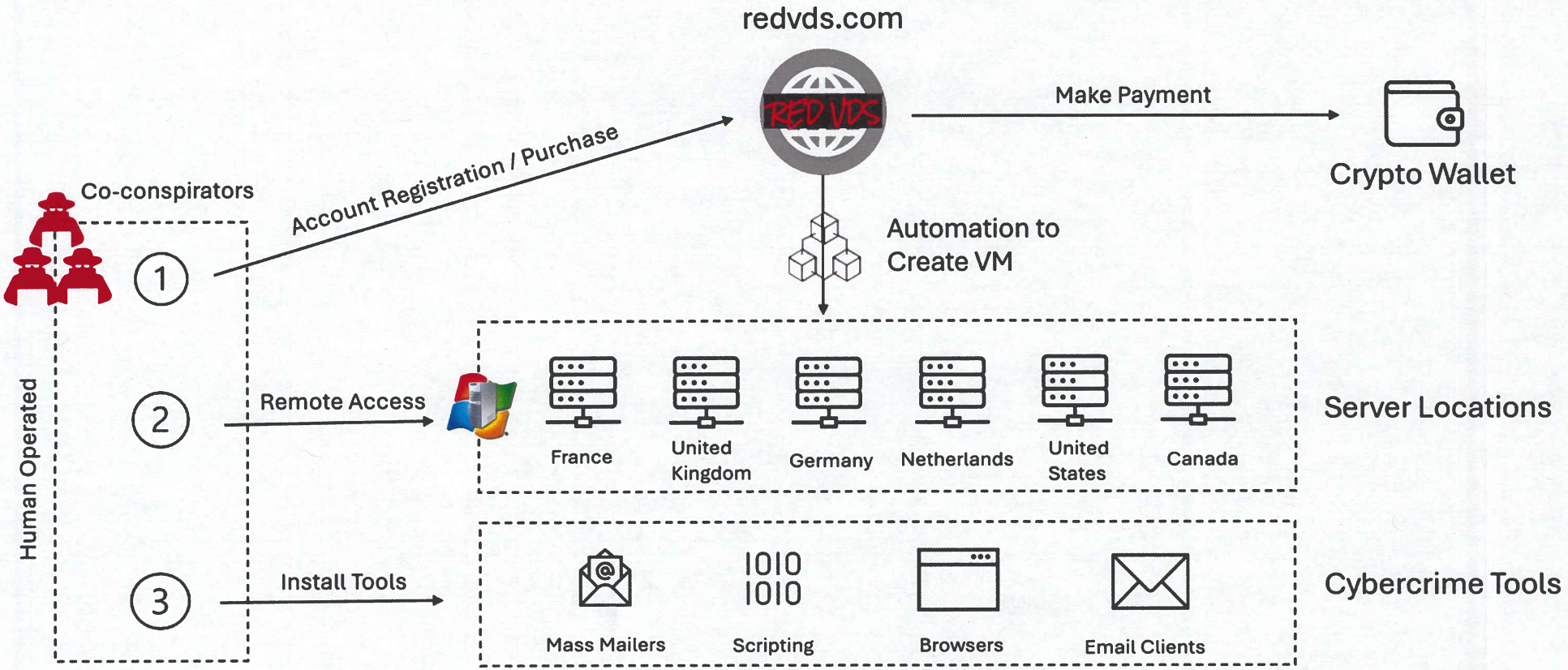

redvds.com
RED VDS
Make Payment
Crypto Wallet
Co-conspirators
Account Registration / Purchase
Automation to
Create VM
Human Operated
1
2
Remote Access
France
United
Kingdom
Germany
Netherlands
United
States
Canada
Server Locations
3
Install Tools
1010
1010
Mass Mailers
Scripting
Browsers
Email Clients
Cybercrime Tools

Exhibit 6

)/Play___New___VM___01min 10sec_____%3b-7805732645_0ad00d21efded50d97d269e16fdef910bf8a11e4.html

Voice Mail

Exhibit 7

Impending Demolition of International Building To Make Way for Modern UB North Campus

Impending Demolition of International Building To Make Way for Modern UB North Campus

20th February, 2024