Forensic analysis on real incidents inside Microsoft Remote Desktop Services

Troopers 2023

TROOPERS

WITH secure

$ whoami

- Catarina DE FARIA CRISTAS
  - **Incident Response consultant** at WithSecure in Helsinki 🇫🇮
  - Former **security researcher** and **malware analyst** at F-Secure / WithSecure
  - **Guest lecturer** at the Finnish **Aalto University** 🏫
    - Windows forensics, Android malware

@c_defaria

www.linkedin.com/in/catarinadfc

Premise of the talk

The rise of **remote work** and **cloud computing** forced companies to take a closer look at **remote access solutions**.

Remote work, BYOD deployments, task or shift work, graphic-intensive applications, etc.

citrix™

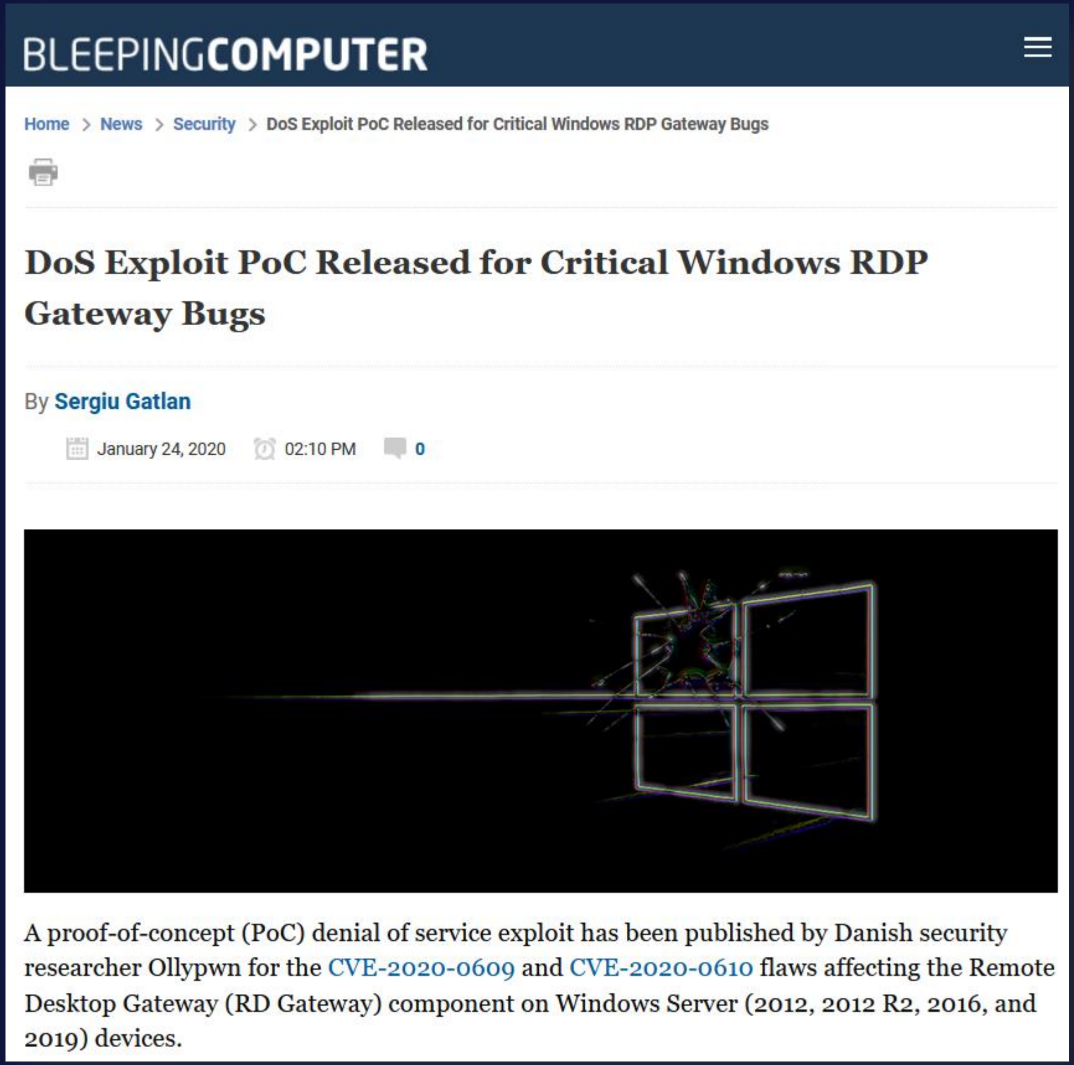
VMware Horizon®

Microsoft Remote Desktop Services

Azure Virtual Desktop

Multiple **threat actors** and **malware campaigns** target **RDS** infrastructures

Premise of the talk



BLEEPINGCOMPUTER

Home > News > Security > DoS Exploit PoC Released for Critical Windows RDP Gateway Bugs

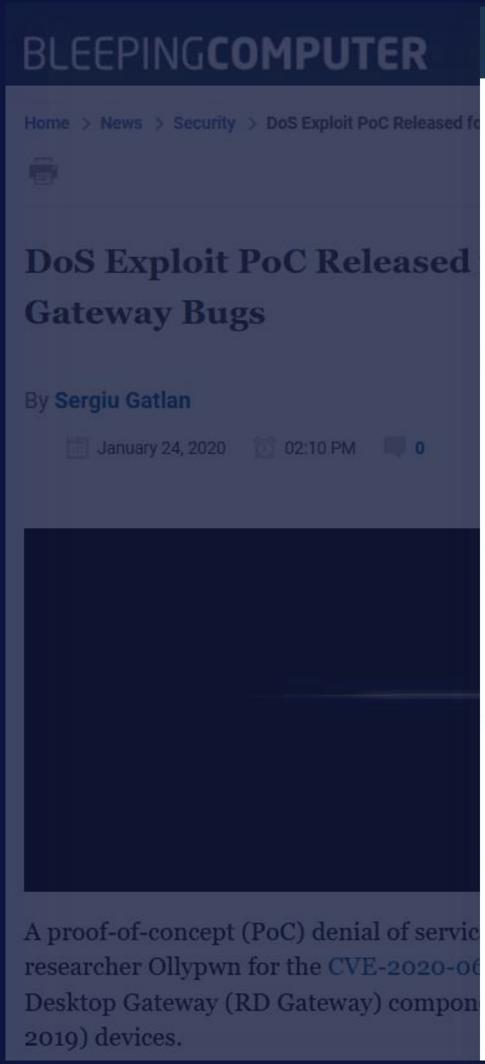
DoS Exploit PoC Released for Critical Windows RDP Gateway Bugs

By Sergiu Gatlan

January 24, 2020 02:10 PM 0

A proof-of-concept (PoC) denial of service exploit has been published by Danish security researcher Ollypwn for the CVE-2020-0609 and CVE-2020-0610 flaws affecting the Remote Desktop Gateway (RD Gateway) component on Windows Server (2012, 2012 R2, 2016, and 2019) devices.

Premise of the talk



BLEEPINGCOMPUTER

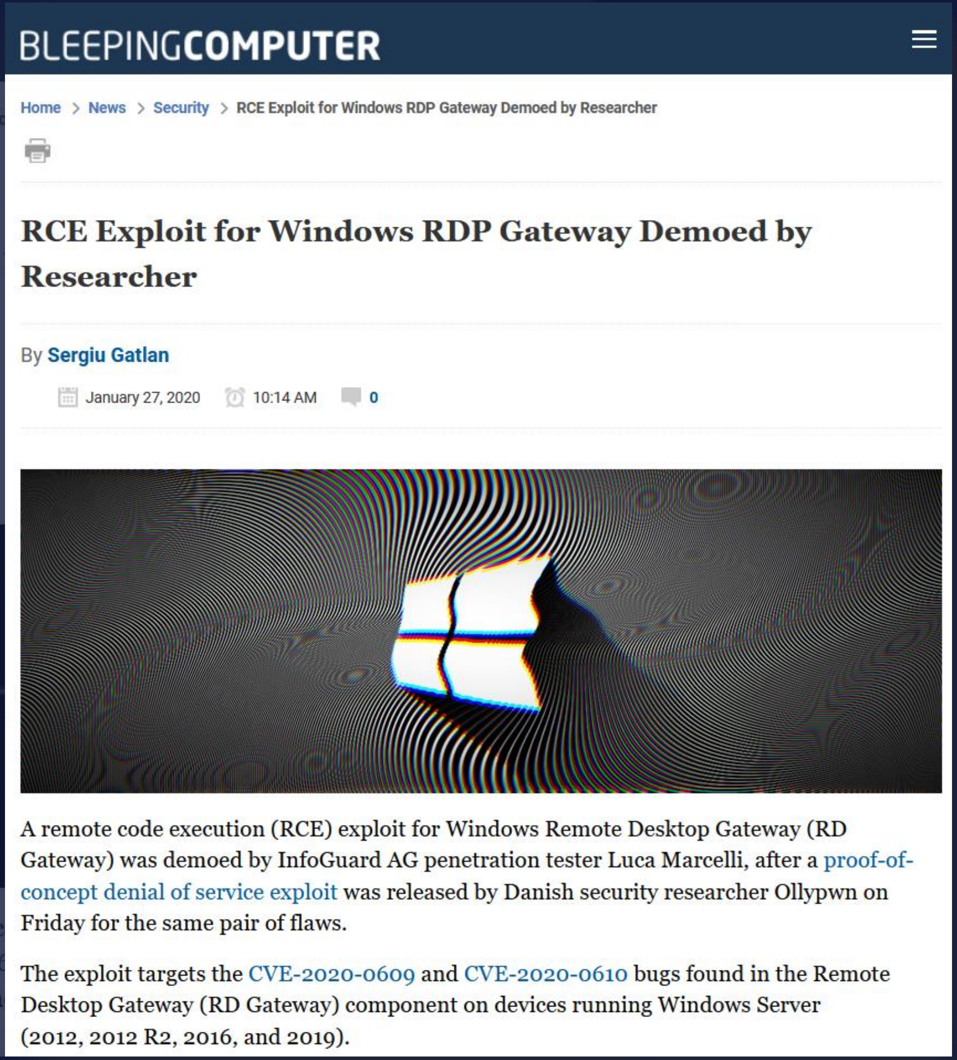
Home > News > Security > DoS Exploit PoC Released f

DoS Exploit PoC Released
Gateway Bugs

By Sergiu Gatlan

January 24, 2020 02:10 PM 0

A proof-of-concept (PoC) denial of servic
researcher Ollypwn for the CVE-2020-0
Desktop Gateway (RD Gateway) compon
2019) devices.



BLEEPINGCOMPUTER

Home > News > Security > RCE Exploit for Windows RDP Gateway Demoed by Researcher

RCE Exploit for Windows RDP Gateway Demoed by Researcher

By Sergiu Gatlan

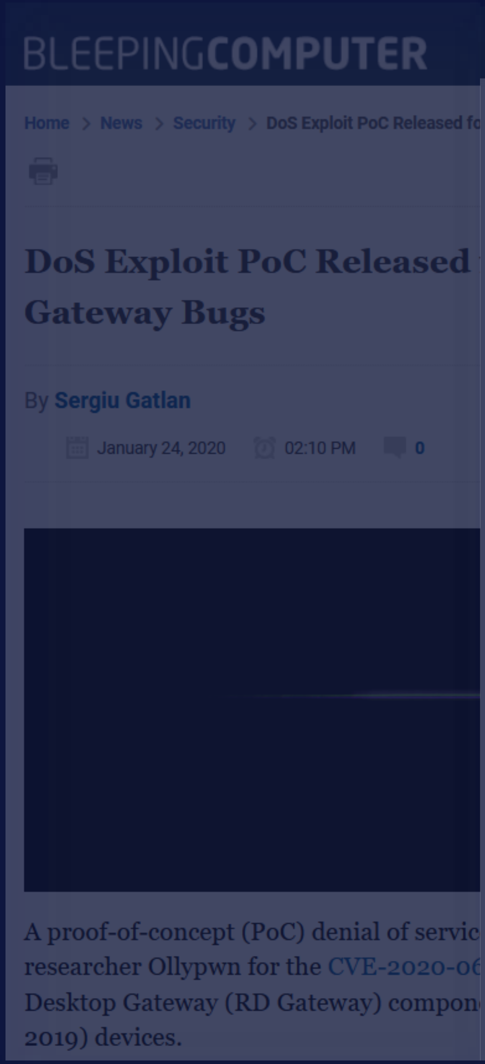
January 27, 2020 10:14 AM 0

A remote code execution (RCE) exploit for Windows Remote Desktop Gateway (RD Gateway) was demoed by InfoGuard AG penetration tester Luca Marcelli, after a proof-of-concept denial of service exploit was released by Danish security researcher Ollypwn on Friday for the same pair of flaws.

The exploit targets the CVE-2020-0609 and CVE-2020-0610 bugs found in the Remote Desktop Gateway (RD Gateway) component on devices running Windows Server (2012, 2012 R2, 2016, and 2019).

TROOPERS WITH secure

Premise of the talk



BLEEPINGCOMPUTER

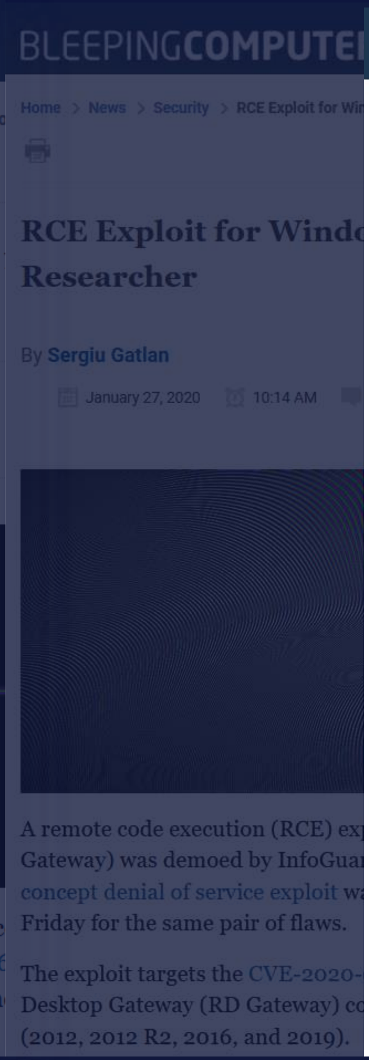
Home > News > Security > DoS Exploit PoC Released fo

DoS Exploit PoC Released f Gateway Bugs

By Sergiu Gatlan

January 24, 2020 02:10 PM 0

A proof-of-concept (PoC) denial of servic researcher Ollypwn for the CVE-2020-06 Desktop Gateway (RD Gateway) compon 2019) devices.



BLEEPINGCOMPUTE

Home > News > Security > RCE Exploit for Wi

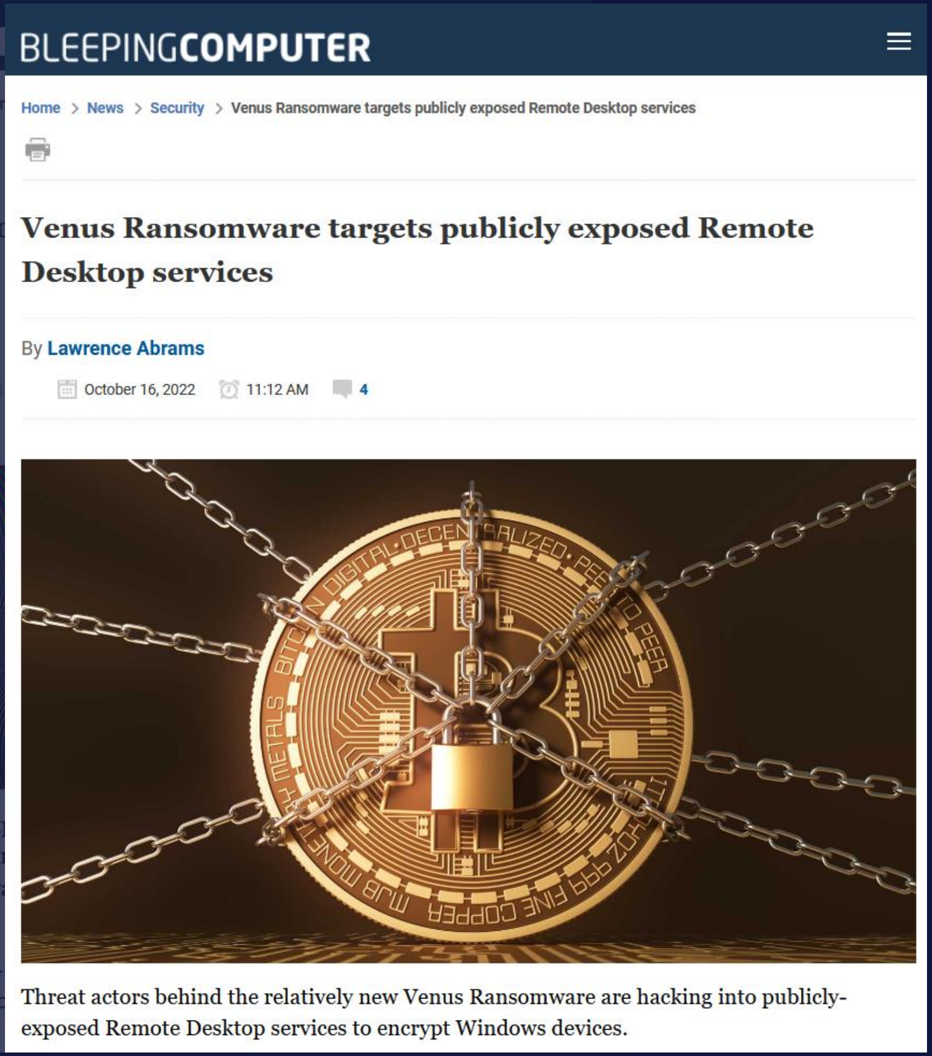
RCE Exploit for Windo Researcher

By Sergiu Gatlan

January 27, 2020 10:14 AM

A remote code execution (RCE) ex Gateway) was demoed by InfoGuar concept denial of service exploit wa Friday for the same pair of flaws.

The exploit targets the CVE-2020- Desktop Gateway (RD Gateway) c (2012, 2012 R2, 2016, and 2019).



BLEEPINGCOMPUTER

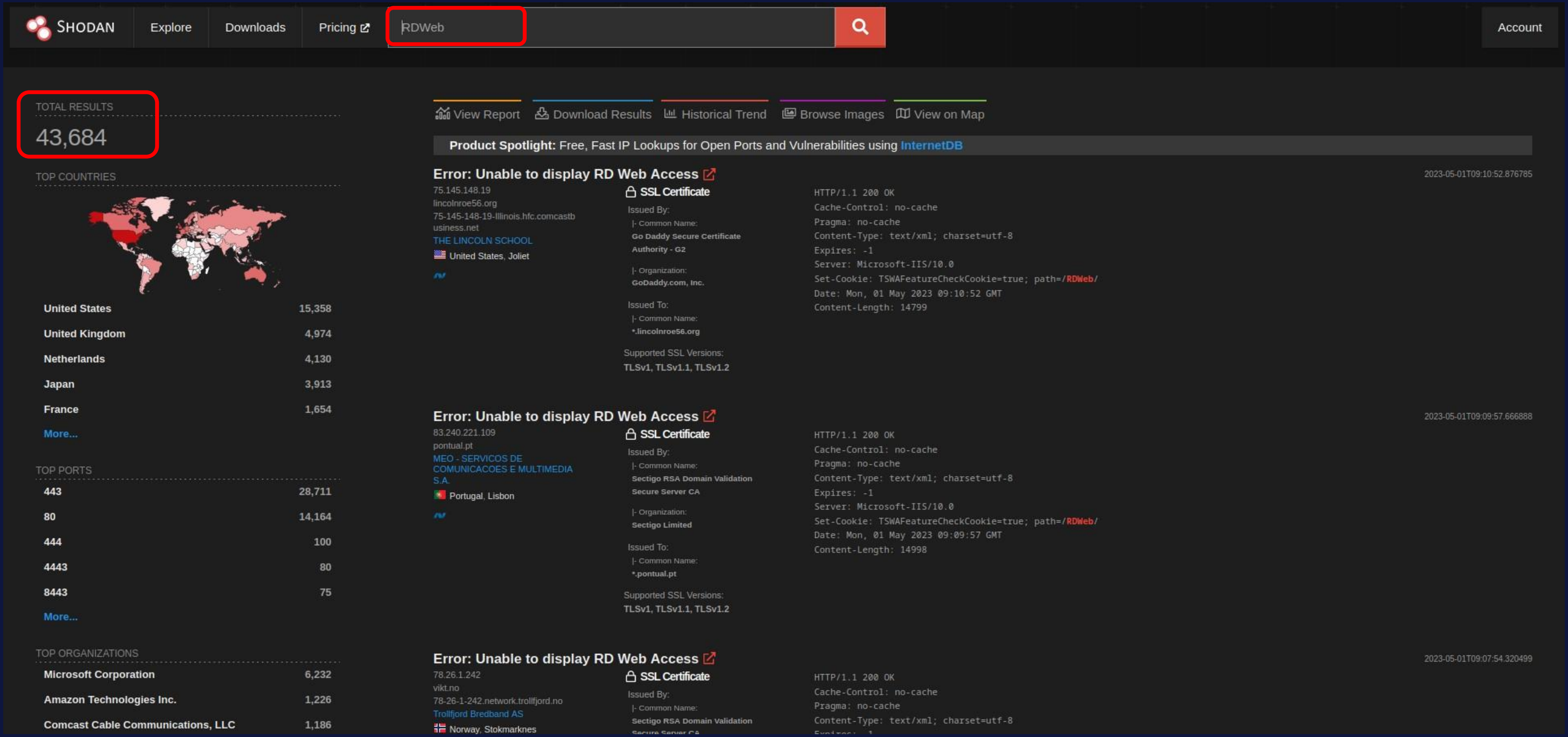
Home > News > Security > Venus Ransomware targets publicly exposed Remote Desktop services

Venus Ransomware targets publicly exposed Remote Desktop services

By Lawrence Abrams

October 16, 2022 11:12 AM 4

Threat actors behind the relatively new Venus Ransomware are hacking into publicly-exposed Remote Desktop services to encrypt Windows devices.



TOTAL RESULTS

43,684

TOP COUNTRIES

United States	15,358
United Kingdom	4,974
Netherlands	4,130
Japan	3,913
France	1,654

More...

TOP PORTS

443	28,711
80	14,164
444	100
4443	80
8443	75

More...

TOP ORGANIZATIONS

Microsoft Corporation	6,232
Amazon Technologies Inc.	1,226
Comcast Cable Communications, LLC	1,186

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB

Error: Unable to display RD Web Access

2023-05-01T09:10:52.876785

75.145.148.19
lincolnroe56.org
75-145-148-19-Illinois.hfc.comcastbusiness.net
THE LINCOLN SCHOOL
United States, Joliet

SSL Certificate

Issued By:
|- Common Name:
Go Daddy Secure Certificate Authority - G2
|- Organization:
GoDaddy.com, Inc.

Issued To:
|- Common Name:
*.lincolnroe56.org

Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2

```
HTTP/1.1 200 OK
Cache-Control: no-cache
Pragma: no-cache
Content-Type: text/xml; charset=utf-8
Expires: -1
Server: Microsoft-IIS/10.0
Set-Cookie: TSWAFeatureCheckCookie=true; path=/RDWeb/
Date: Mon, 01 May 2023 09:10:52 GMT
Content-Length: 14799
```

Error: Unable to display RD Web Access

2023-05-01T09:09:57.666888

83.240.221.109
pontual.pt
MEO - SERVICOS DE COMUNICACOES E MULTIMEDIA S.A.
Portugal, Lisbon

SSL Certificate

Issued By:
|- Common Name:
Sectigo RSA Domain Validation Secure Server CA
|- Organization:
Sectigo Limited

Issued To:
|- Common Name:
*.pontual.pt

Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2

```
HTTP/1.1 200 OK
Cache-Control: no-cache
Pragma: no-cache
Content-Type: text/xml; charset=utf-8
Expires: -1
Server: Microsoft-IIS/10.0
Set-Cookie: TSWAFeatureCheckCookie=true; path=/RDWeb/
Date: Mon, 01 May 2023 09:09:57 GMT
Content-Length: 14998
```

Error: Unable to display RD Web Access

2023-05-01T09:07:54.320499

78.26.1.242
vikt.no
78-26-1-242.network.trollfjord.no
Trollfjord Bredband AS
Norway, Stokmarknes

SSL Certificate

Issued By:
|- Common Name:
Sectigo RSA Domain Validation Secure Server CA

```
HTTP/1.1 200 OK
Cache-Control: no-cache
Pragma: no-cache
Content-Type: text/xml; charset=utf-8
```

Shodan - RD Web Access servers

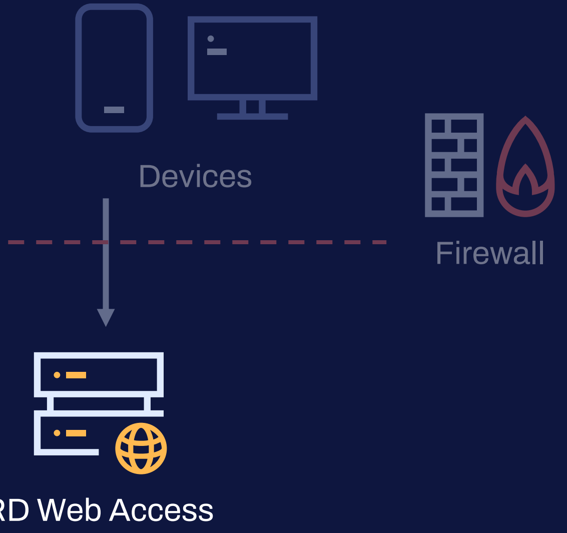
II. Microsoft Remote Desktop Services (RDS)

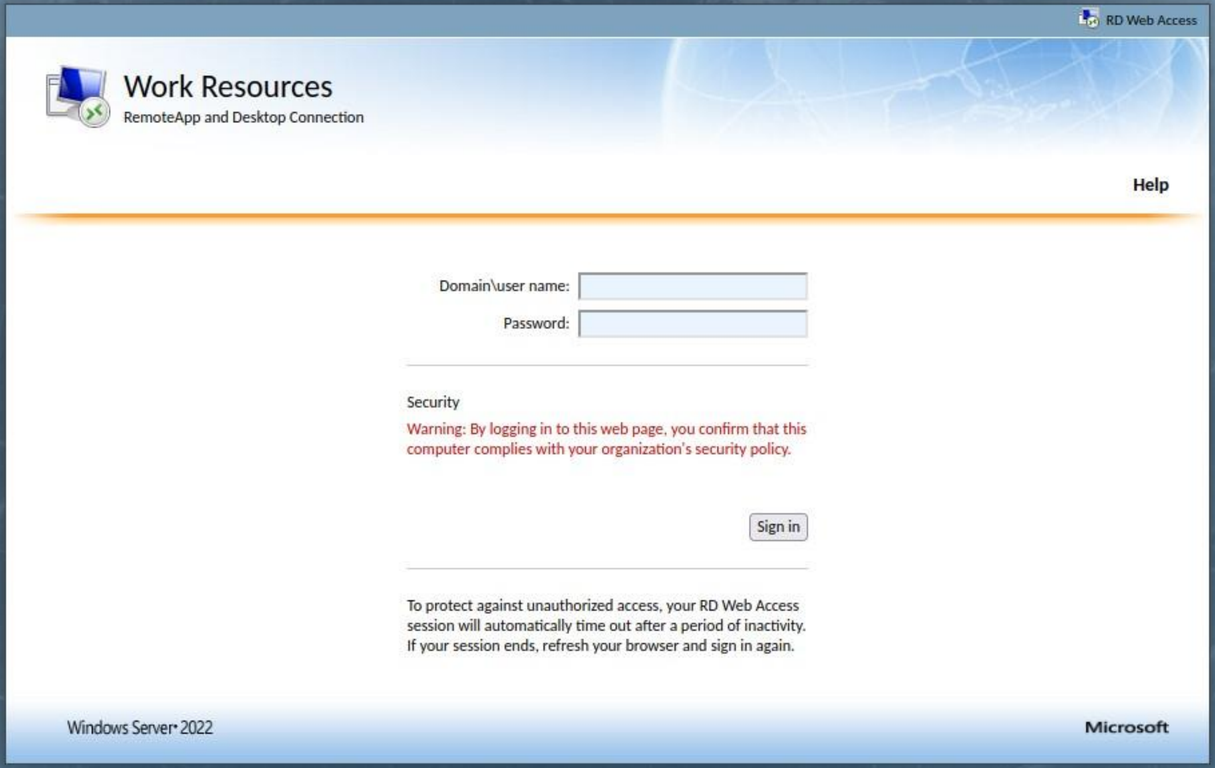
Roles

Roles – RD Web Access

Microsoft Remote Desktop Services (RDS)

- **RD Web Access**
  - Remote desktops and/or RemoteApps via a **web page**
  - **RDP configuration file**





Domain\user name:

Password:

Security

Warning: By logging in to this web page, you confirm that this computer complies with your organization's security policy.

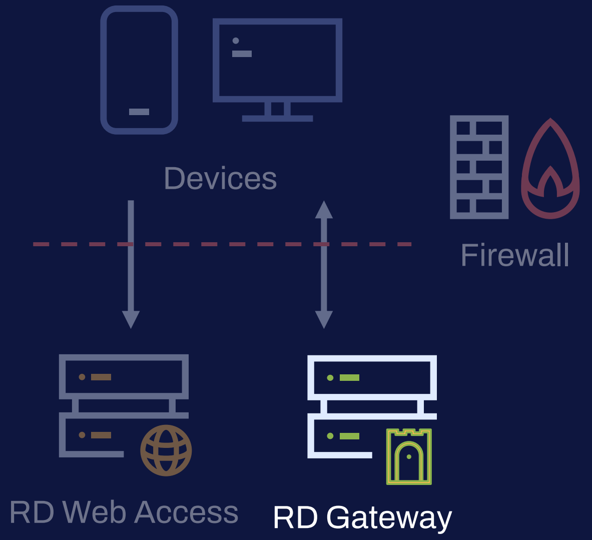
To protect against unauthorized access, your RD Web Access session will automatically time out after a period of inactivity. If your session ends, refresh your browser and sign in again.

RD Web Access login page

Roles – RD Gateway

Microsoft Remote Desktop Services (RDS)

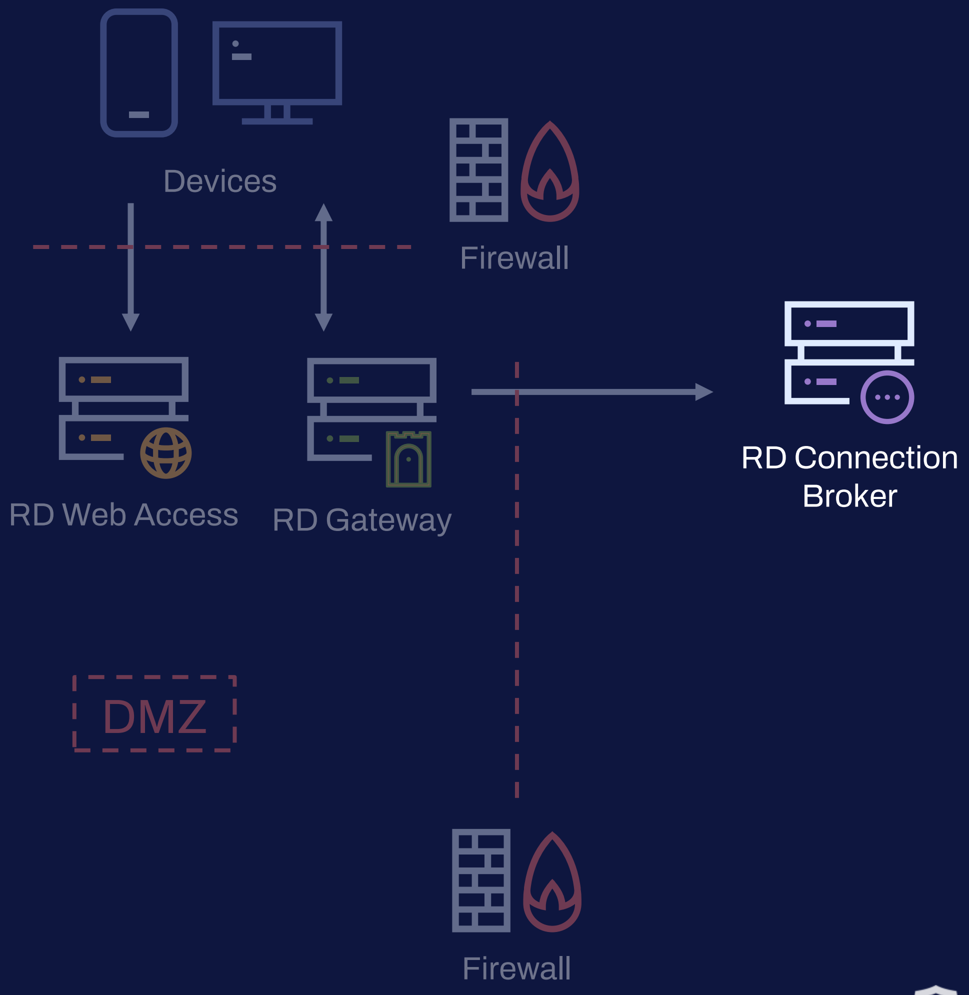
- **RD Gateway**
  - **RD Session Hosts** are not **publicly available**.
  - **RDP sessions** are encapsulated in **TLS**.
  - **RD Authorization Policies:**
    - **RD CAPs** (Connection)
    - **RD RAPs** (Resource)



Roles - RD Connection Broker

Microsoft Remote Desktop Services (RDS)

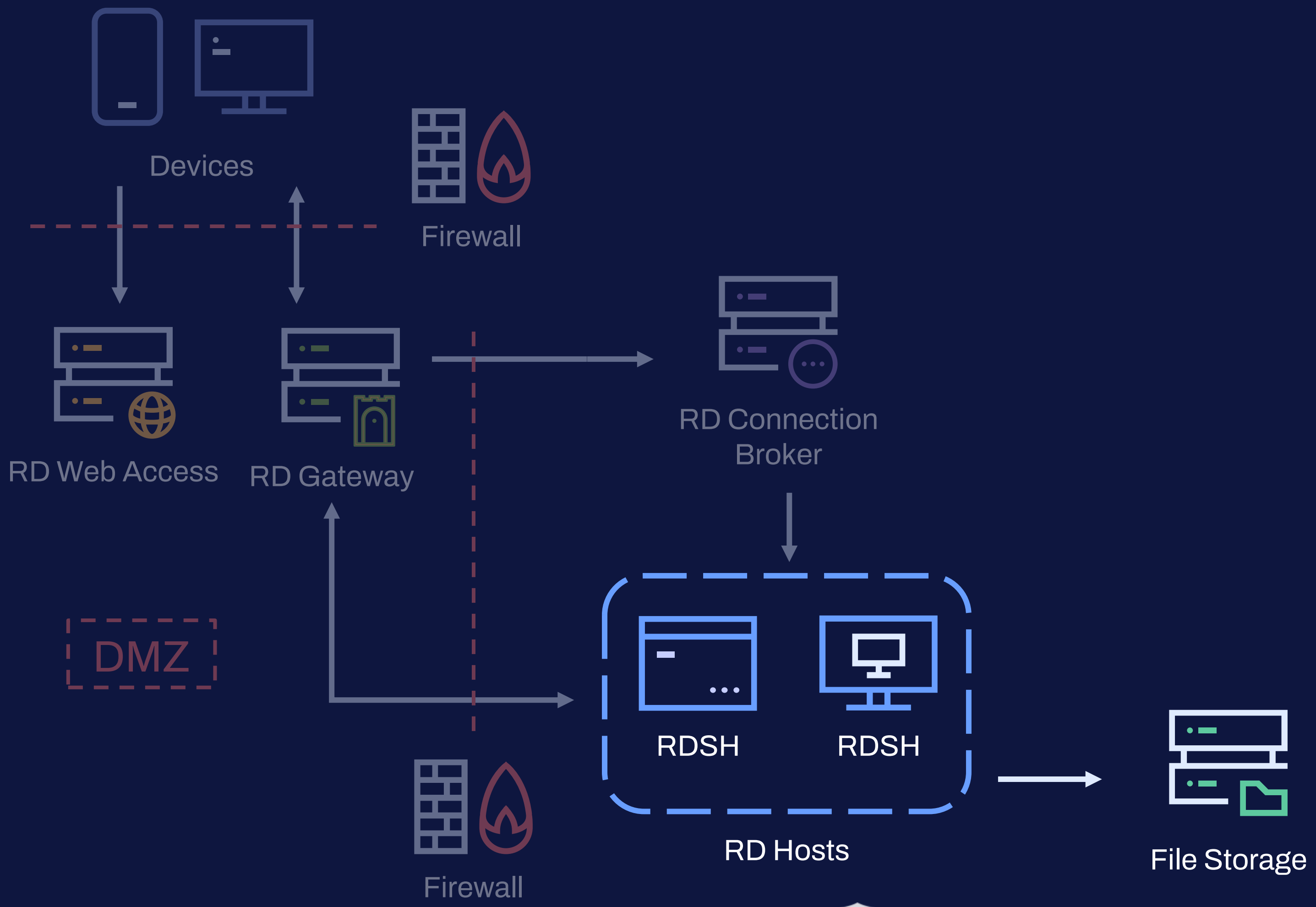
- RD Connection Broker
  - **Forward** the RDP sessions to the RD Session Hosts
  - **Load balancer**



Roles - RD Session Host

Microsoft Remote Desktop Services (RDS)

- **RD Session Host**
  - Session-based virtualization or VDI
  - Desktop or RemoteApp
- **File Storage**
  - **User Profile Disks (UPD)**
    - VHD format

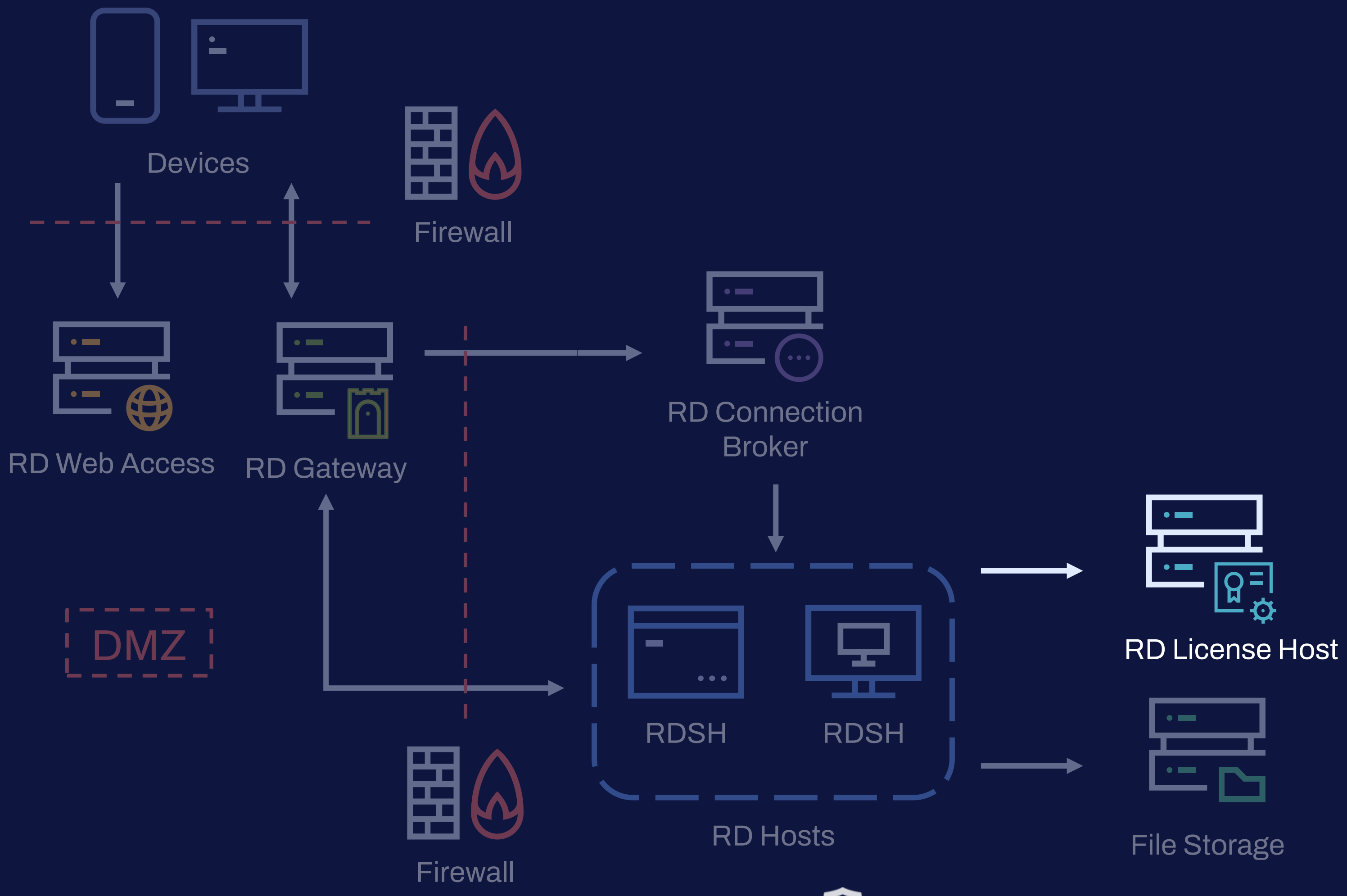


TROOPERS W/TH secure

Roles – RD License Host

Microsoft Remote Desktop Services (RDS)

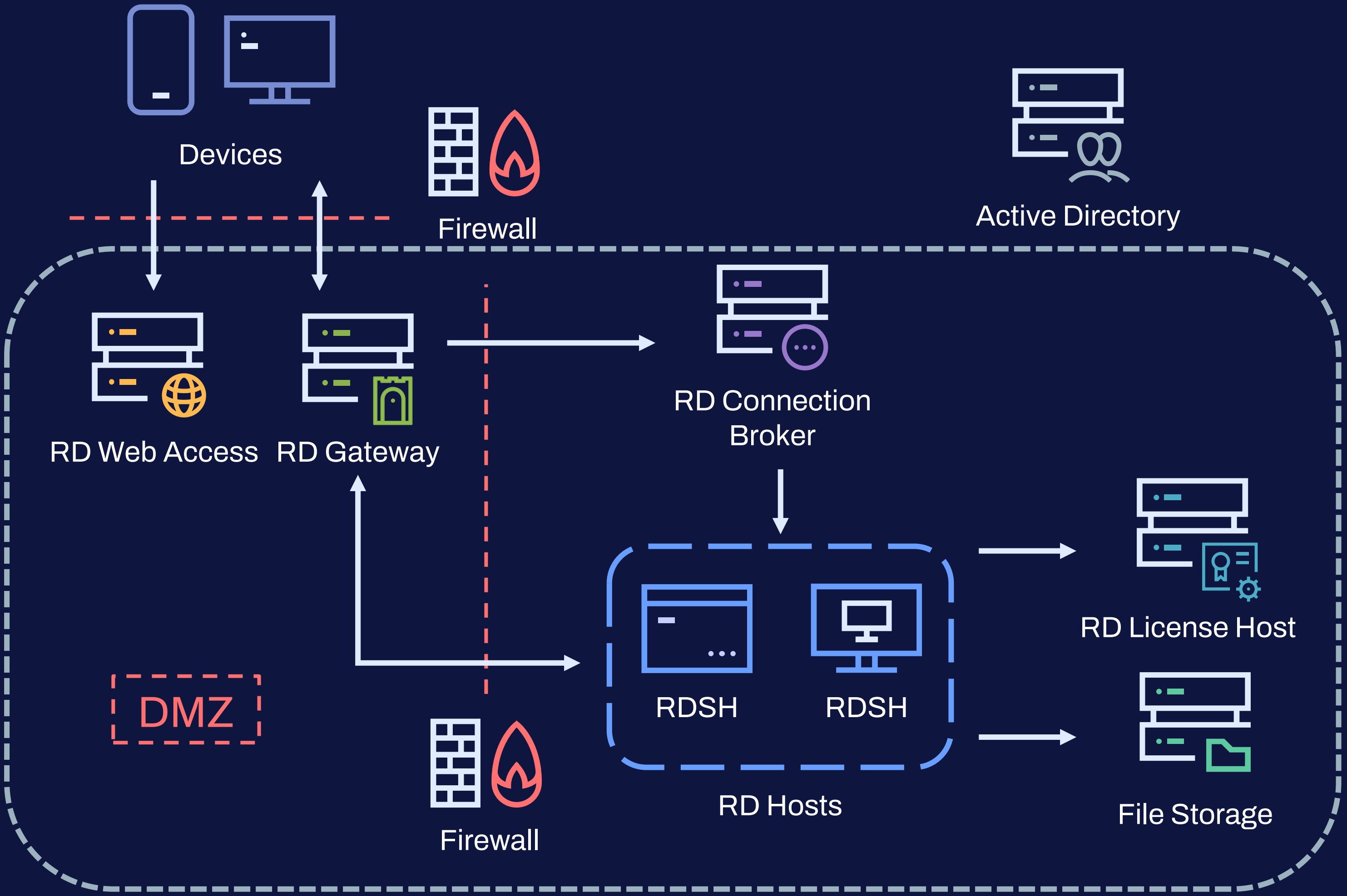
- **RD License Host**
  - RDS licenses



TROOPERS W/TH secure

On-premises deployment

Microsoft Remote Desktop Services (RDS)



TROOPERS WITH secure

III. How to compromise and investigate an RDS infrastructure

Gaining an initial foothold

Gaining an initial foothold

How to compromise and investigate an RDS infrastructure

RD Gateway & RD Web Access

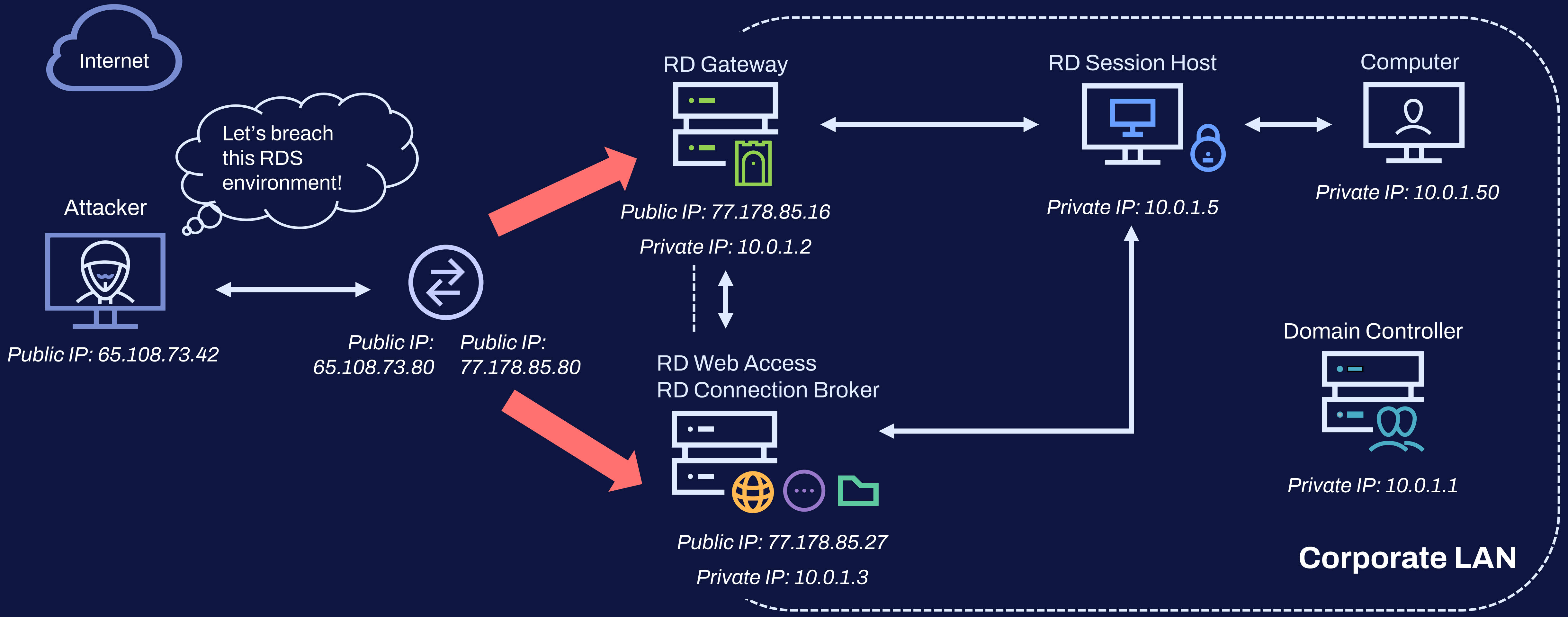
- **Publicly exposed** servers
- More **secure** than **RDP alone**
- **False sense of security**

Attacks

- **Brute force** attacks
- **Account compromise**
- Exploiting **vulnerabilities**

Gaining an initial foothold

How to compromise and investigate an RDS infrastructure



Gaining an initial foothold

How to compromise and investigate an RDS infrastructure

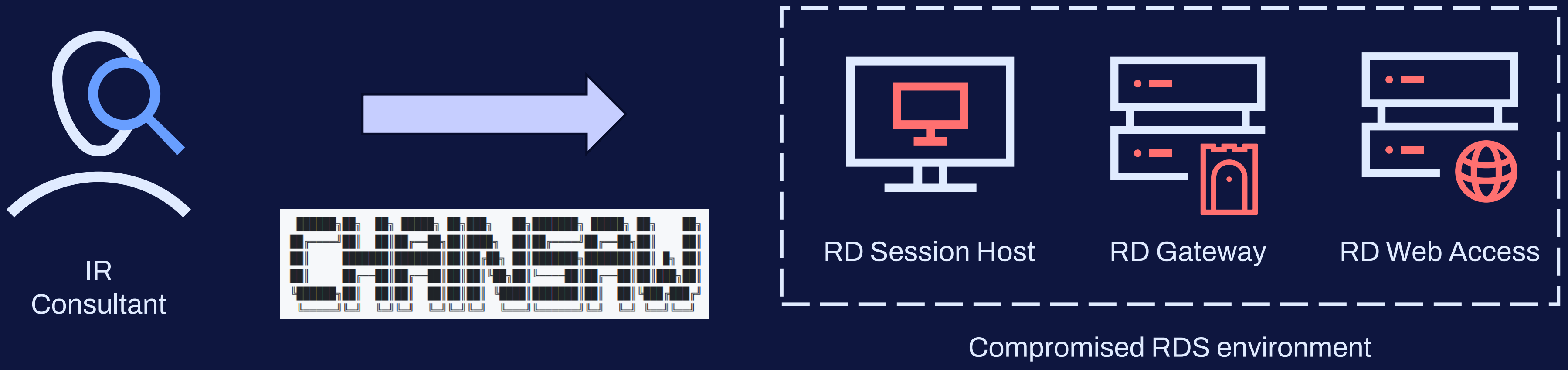
Goal: Acquire domain credentials

1. Figure out the **domain name** and the **username pattern**
   - The **WorkSpaceID** hidden input field in the **RD Web access login page**
   - **Work email** on **LinkedIn**
2. Identify **valid domain user accounts** by leveraging the **RD Web Access** server
   - Anonymous authentication timing attack
3. Obtain a **domain account's password**
   - Brute-force / Password spraying attack
   - Phishing email

Gaining an initial foothold

How to compromise and investigate an RDS infrastructure

- **Chainsaw**, an **open-source tool** developed by **WithSecure**, to perform **rapid triage of Windows event logs** and **hunt threats**.
- A **new version** of **Chainsaw** will be published to **parse lesser-known Windows event logs** relevant while investigating a compromised RDS environment.

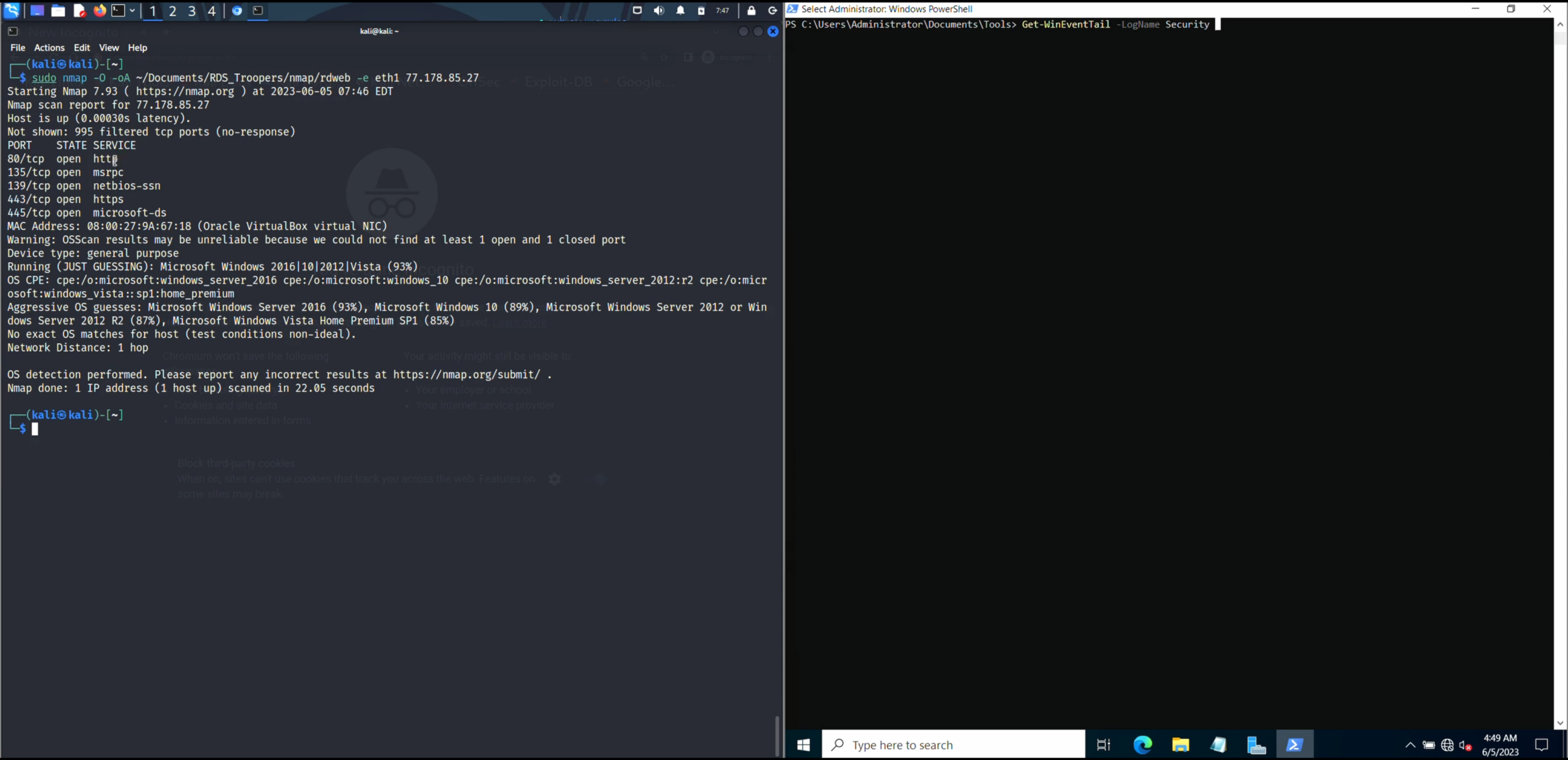


https://github.com/WithSecureLabs/chainsaw

Gaining an initial foothold

How to compromise and investigate an RDS infrastructure

DEMO


1 2 3 4
7:47
kali@kali: ~
File Actions Edit View Help
Select Administrator: Windows PowerShell
Type here to search
4:49 AM
6/5/2023

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O -oA ~/Documents/RDS_Troopers/nmap/rdweb -e eth1 77.178.85.27
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-05 07:46 EDT
Nmap scan report for 77.178.85.27
Host is up (0.00030s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
135/tcp open  msrpc
139/tcp open  netbios-ssn
443/tcp open  https
445/tcp open  microsoft-ds
MAC Address: 08:00:27:9A:67:18 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2016|10|2012|Vista (93%)
OS CPE: cpe:/o:microsoft:windows_server_2016 cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_server_2012:r2 cpe:/o:micr
osoft:windows_vista::sp1:home_premium
Aggressive OS guesses: Microsoft Windows Server 2016 (93%), Microsoft Windows 10 (89%), Microsoft Windows Server 2012 or Win
dows Server 2012 R2 (87%), Microsoft Windows Vista Home Premium SP1 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.05 seconds

┌──(kali㉿kali)-[~]
└─$
```

```
PS C:\Users\Administrator\Documents\Tools> Get-WinEventTail -LogName Security
```

Gaining an initial foothold

How to compromise and investigate an RDS infrastructure

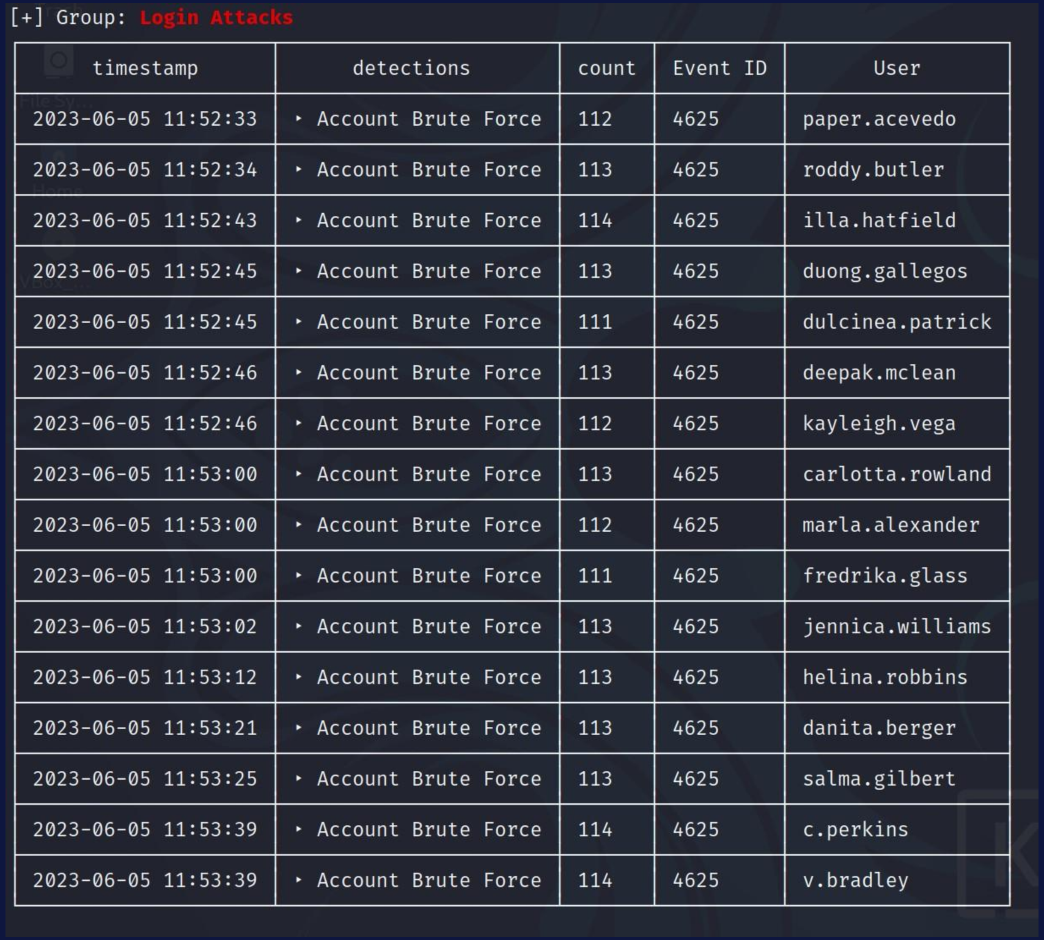
- What did we observe during the **brute-force** attack?

RD Web Access & RD Gateway events

- **Security**
  - **EID 4625**: Failed logon
  - **EID 4624**: Successful logon

Gaining an initial foothold

How to compromise and investigate an RDS infrastructure



```
[+] Group: Login Attacks
┌─────────────────────┬───────────────────────┬───────┬──────────┬──────────────────┐
│      timestamp      │      detections       │ count │ Event ID │       User       │
├─────────────────────┼───────────────────────┼───────┼──────────┼──────────────────┤
│ 2023-06-05 11:52:33 │ ‣ Account Brute Force │ 112   │ 4625     │ paper.acevedo    │
├─────────────────────┼───────────────────────┼───────┼──────────┼──────────────────┤
│ 2023-06-05 11:52:34 │ ‣ Account Brute Force │ 113   │ 4625     │ roddy.butler     │
├─────────────────────┼───────────────────────┼───────┼──────────┼──────────────────┤
│ 2023-06-05 11:52:43 │ ‣ Account Brute Force │ 114   │ 4625     │ illa.hatfield    │
├─────────────────────┼───────────────────────┼───────┼──────────┼──────────────────┤
│ 2023-06-05 11:52:45 │ ‣ Account Brute Force │ 113   │ 4625     │ duong.gallegos   │
├─────────────────────┼───────────────────────┼───────┼──────────┼──────────────────┤
│ 2023-06-05 11:52:45 │ ‣ Account Brute Force │ 111   │ 4625     │ dulcinea.patrick │
├─────────────────────┼───────────────────────┼───────┼──────────┼──────────────────┤
│ 2023-06-05 11:52:46 │ ‣ Account Brute Force │ 113   │ 4625     │ deepak.mclean    │
├─────────────────────┼───────────────────────┼───────┼──────────┼──────────────────┤
│ 2023-06-05 11:52:46 │ ‣ Account Brute Force │ 112   │ 4625     │ kayleigh.vega    │
├─────────────────────┼───────────────────────┼───────┼──────────┼──────────────────┤
│ 2023-06-05 11:53:00 │ ‣ Account Brute Force │ 113   │ 4625     │ carlotta.rowland │
├─────────────────────┼───────────────────────┼───────┼──────────┼──────────────────┤
│ 2023-06-05 11:53:00 │ ‣ Account Brute Force │ 112   │ 4625     │ marla.alexander  │
├─────────────────────┼───────────────────────┼───────┼──────────┼──────────────────┤
│ 2023-06-05 11:53:00 │ ‣ Account Brute Force │ 111   │ 4625     │ fredrika.glass   │
├─────────────────────┼───────────────────────┼───────┼──────────┼──────────────────┤
│ 2023-06-05 11:53:02 │ ‣ Account Brute Force │ 113   │ 4625     │ jennica.williams │
├─────────────────────┼───────────────────────┼───────┼──────────┼──────────────────┤
│ 2023-06-05 11:53:12 │ ‣ Account Brute Force │ 113   │ 4625     │ helina.robbins   │
├─────────────────────┼───────────────────────┼───────┼──────────┼──────────────────┤
│ 2023-06-05 11:53:21 │ ‣ Account Brute Force │ 113   │ 4625     │ danita.berger    │
├─────────────────────┼───────────────────────┼───────┼──────────┼──────────────────┤
│ 2023-06-05 11:53:25 │ ‣ Account Brute Force │ 113   │ 4625     │ salma.gilbert    │
├─────────────────────┼───────────────────────┼───────┼──────────┼──────────────────┤
│ 2023-06-05 11:53:39 │ ‣ Account Brute Force │ 114   │ 4625     │ c.perkins        │
├─────────────────────┼───────────────────────┼───────┼──────────┼──────────────────┤
│ 2023-06-05 11:53:39 │ ‣ Account Brute Force │ 114   │ 4625     │ v.bradley        │
└─────────────────────┴───────────────────────┴───────┴──────────┴──────────────────┘
```

Chainsaw: Login Attacks based on EID 4625 from Security

Gaining an initial foothold

How to compromise and investigate an RDS infrastructure

- What did we observe when there was a **successful connection**?

RD Web Access events

- **Security**
  - **EID 4624**: Successful logon
    - SubjectDomainName: IIS APPOOL
    - SubjectUserName: RDWebAccess

Gaining an initial foothold

How to compromise and investigate an RDS infrastructure

- What did we observe when there was a **successful connection**?

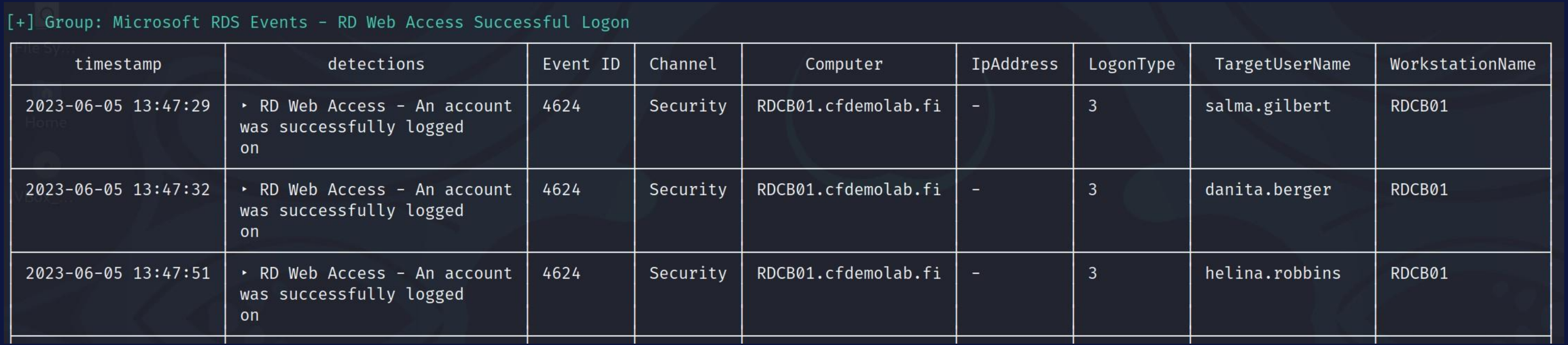
RD Web Access events	RD Gateway events
• **Security** • **EID 4624**: Successful logon • SubjectDomainName: IIS APPOOL • SubjectUserName: RDWebAccess	• **TerminalServices-Gateway** • **EID 300**: RD RAP requirements met • **EID 200**: RD CAP requirements met • **EID 302**: A user connected to an RD Session Host • **EID 303**: A user disconnected from an RD Session Host

Attacker's public IP address

Bytes transferred/received and RDP session duration (EID 303)

Gaining an initial foothold

How to compromise and investigate an RDS infrastructure

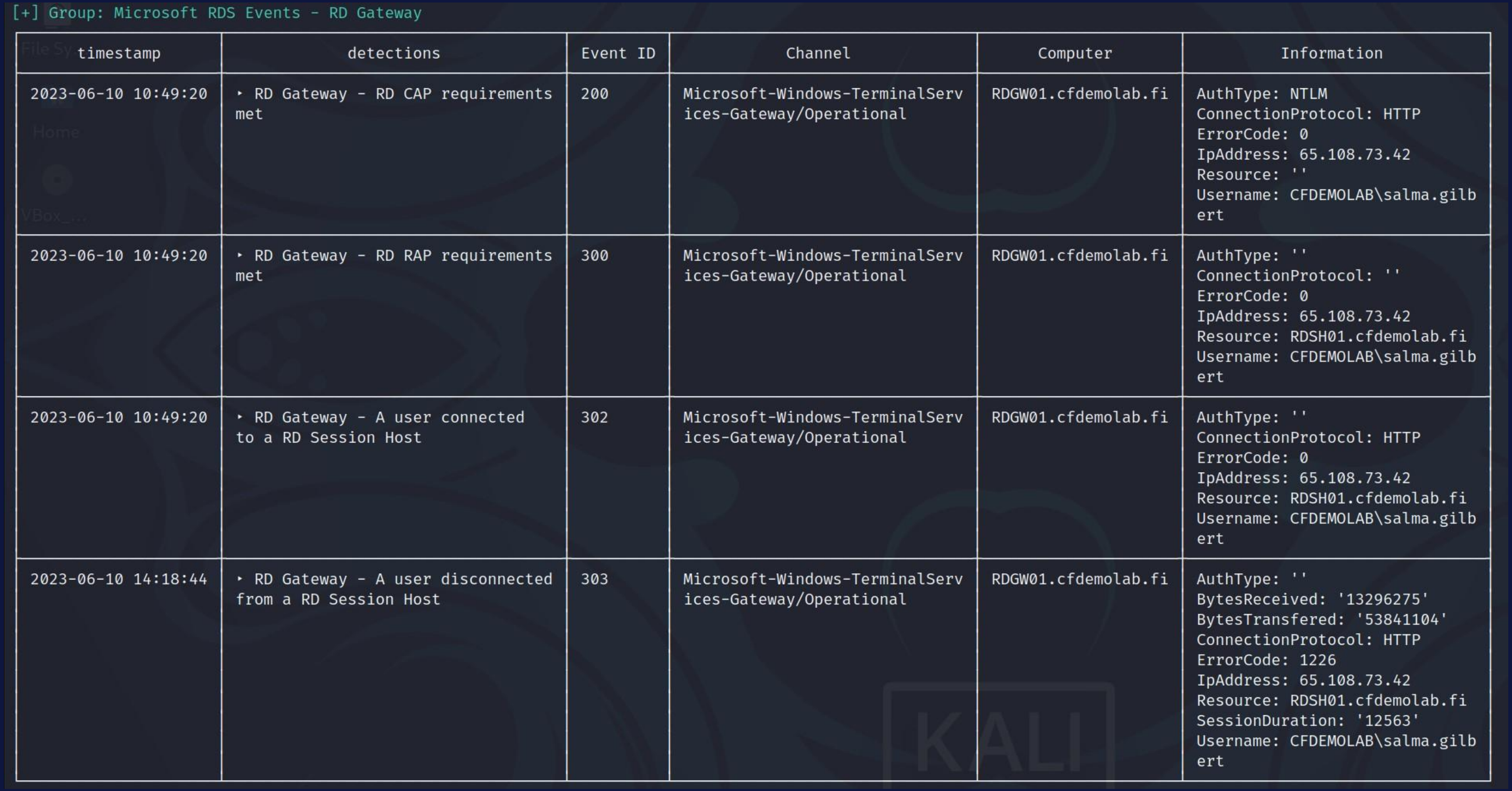


```
[+] Group: Microsoft RDS Events - RD Web Access Successful Logon
┌─────────────────────┬──────────────────────────────┬──────────┬──────────┬─────────────────────┬─────────────┬───────────┬─────────────────┬─────────────────┐
│      timestamp      │          detections          │ Event ID │ Channel  │      Computer       │ IpAddress   │ LogonType │ TargetUserName  │ WorkstationName │
├─────────────────────┼──────────────────────────────┼──────────┼──────────┼─────────────────────┼─────────────┼───────────┼─────────────────┼─────────────────┤
│ 2023-06-05 13:47:29 │ ‣ RD Web Access - An account │ 4624     │ Security │ RDCB01.cfdemolab.fi │ -           │ 3         │ salma.gilbert   │ RDCB01          │
│                     │ was successfully logged      │          │          │                     │             │           │                 │                 │
│                     │ on                           │          │          │                     │             │           │                 │                 │
├─────────────────────┼──────────────────────────────┼──────────┼──────────┼─────────────────────┼─────────────┼───────────┼─────────────────┼─────────────────┤
│ 2023-06-05 13:47:32 │ ‣ RD Web Access - An account │ 4624     │ Security │ RDCB01.cfdemolab.fi │ -           │ 3         │ danita.berger   │ RDCB01          │
│                     │ was successfully logged      │          │          │                     │             │           │                 │                 │
│                     │ on                           │          │          │                     │             │           │                 │                 │
├─────────────────────┼──────────────────────────────┼──────────┼──────────┼─────────────────────┼─────────────┼───────────┼─────────────────┼─────────────────┤
│ 2023-06-05 13:47:51 │ ‣ RD Web Access - An account │ 4624     │ Security │ RDCB01.cfdemolab.fi │ -           │ 3         │ helina.robbins  │ RDCB01          │
│                     │ was successfully logged      │          │          │                     │             │           │                 │                 │
│                     │ on                           │          │          │                     │             │           │                 │                 │
├─────────────────────┼──────────────────────────────┼──────────┼──────────┼─────────────────────┼─────────────┼───────────┼─────────────────┼─────────────────┤
```

Chainsaw: RD Web Access Successful Logon

Gaining an initial foothold

How to compromise and investigate an RDS infrastructure



[+] Group: Microsoft RDS Events - RD Gateway

timestamp	detections	Event ID	Channel	Computer	Information
2023-06-10 10:49:20	‣ RD Gateway - RD CAP requirements met	200	Microsoft-Windows-TerminalServices-Gateway/Operational	RDGW01.cfdemolab.fi	AuthType: NTLM ConnectionProtocol: HTTP ErrorCode: 0 IpAddress: 65.108.73.42 Resource: '' Username: CFDEMOLAB\salma.gilbert
2023-06-10 10:49:20	‣ RD Gateway - RD RAP requirements met	300	Microsoft-Windows-TerminalServices-Gateway/Operational	RDGW01.cfdemolab.fi	AuthType: '' ConnectionProtocol: '' ErrorCode: 0 IpAddress: 65.108.73.42 Resource: RDSH01.cfdemolab.fi Username: CFDEMOLAB\salma.gilbert
2023-06-10 10:49:20	‣ RD Gateway - A user connected to a RD Session Host	302	Microsoft-Windows-TerminalServices-Gateway/Operational	RDGW01.cfdemolab.fi	AuthType: '' ConnectionProtocol: HTTP ErrorCode: 0 IpAddress: 65.108.73.42 Resource: RDSH01.cfdemolab.fi Username: CFDEMOLAB\salma.gilbert
2023-06-10 14:18:44	‣ RD Gateway - A user disconnected from a RD Session Host	303	Microsoft-Windows-TerminalServices-Gateway/Operational	RDGW01.cfdemolab.fi	AuthType: '' BytesReceived: '13296275' BytesTransfered: '53841104' ConnectionProtocol: HTTP ErrorCode: 1226 IpAddress: 65.108.73.42 Resource: RDSH01.cfdemolab.fi SessionDuration: '12563' Username: CFDEMOLAB\salma.gilbert

Chainsaw: RD Gateway events

Gaining an initial foothold

How to compromise and investigate an RDS infrastructure

- What did we observe when there was a **successful connection**?

RD Connection Broker events

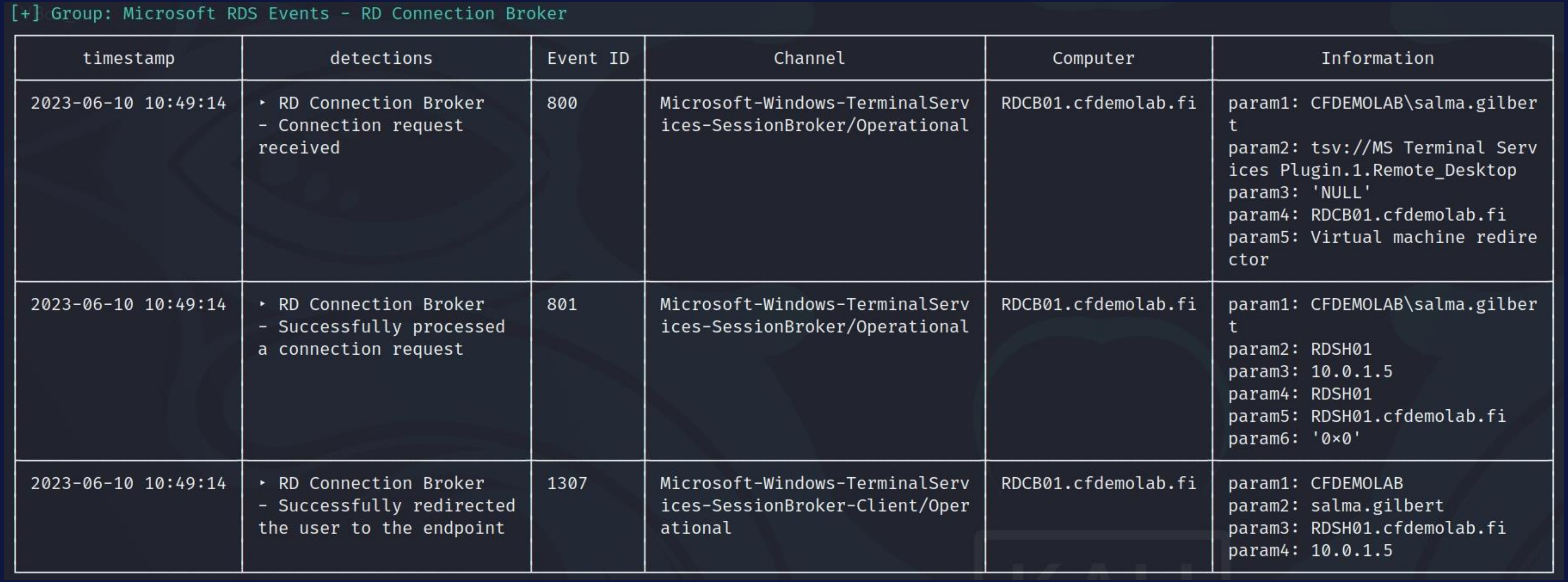
- **TerminalServices-SessionBroker**
  - **EID 800**: A connection request was received
  - **EID 801**: A connection request was processed
- **TerminalServices-SessionBroker-Client**
  - **EID 1307**: The user was redirected to the endpoint

RDP enabled

Short RDP sessions

Gaining an initial foothold

How to compromise and investigate an RDS infrastructure



[+] Group: Microsoft RDS Events - RD Connection Broker

timestamp	detections	Event ID	Channel	Computer	Information
2023-06-10 10:49:14	‣ RD Connection Broker - Connection request received	800	Microsoft-Windows-TerminalServices-SessionBroker/Operational	RDCB01.cfdemolab.fi	param1: CFDEMOLAB\salma.gilbert param2: tsv://MS Terminal Services Plugin.1.Remote_Desktop param3: 'NULL' param4: RDCB01.cfdemolab.fi param5: Virtual machine redirector
2023-06-10 10:49:14	‣ RD Connection Broker - Successfully processed a connection request	801	Microsoft-Windows-TerminalServices-SessionBroker/Operational	RDCB01.cfdemolab.fi	param1: CFDEMOLAB\salma.gilbert param2: RDSH01 param3: 10.0.1.5 param4: RDSH01 param5: RDSH01.cfdemolab.fi param6: '0×0'
2023-06-10 10:49:14	‣ RD Connection Broker - Successfully redirected the user to the endpoint	1307	Microsoft-Windows-TerminalServices-SessionBroker-Client/Operational	RDCB01.cfdemolab.fi	param1: CFDEMOLAB param2: salma.gilbert param3: RDSH01.cfdemolab.fi param4: 10.0.1.5

Chainsaw: RD Connection Broker events

Gaining an initial foothold

How to compromise and investigate an RDS infrastructure

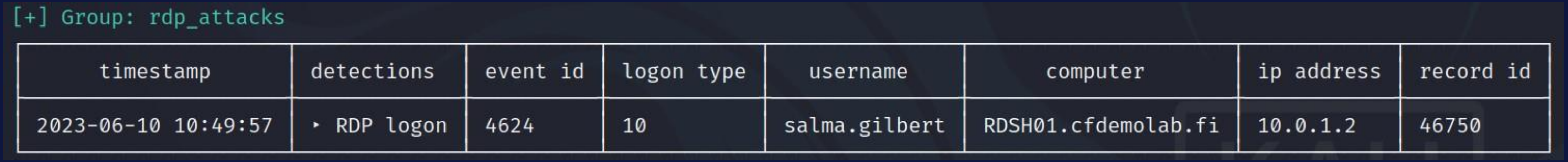
- What did we observe when there was a **successful connection**?

RD Session Host events

- **TerminalServices-RemoteConnectionManager**
  - **EID 1149**: RDS Network Connection
- **TerminalServices-LocalSessionManager**
  - **EID 21**: RDS Session logon succeeded
  - **EID 22**: File Explorer shell notification received
  - **EID 24**: RDP Session has been disconnected
  - **EID 23**: RDP Session logoff
- **Security**
  - **EID 4624**: Successful logon
    - WorkstationName: RDSH01 (10.0.1.5)
      LogonType: 10 (RDP)
      IpAddress: 10.0.1.2 (RD Gateway)
  - **EID 4647**: User-initiated logoff
- **User Profile Service**
  - **EID 5**: Registry file loaded

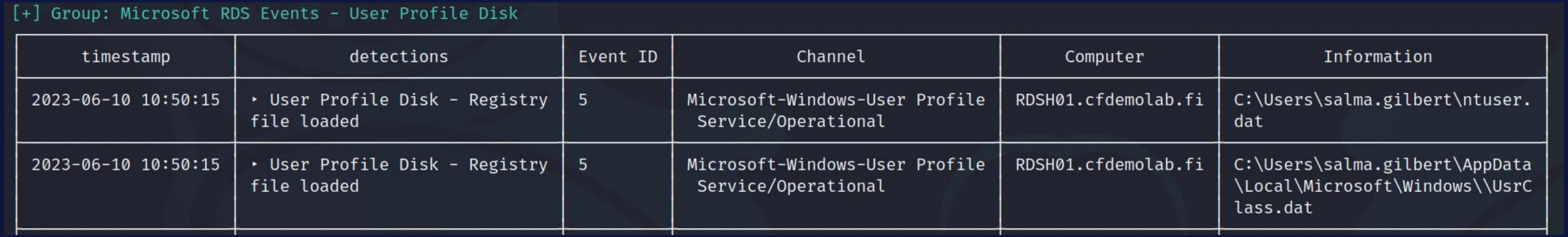
Gaining an initial foothold

How to compromise and investigate an RDS infrastructure



```
[+] Group: rdp_attacks
┌─────────────────────┬──────────────┬──────────┬─────────────┬────────────────┬─────────────────────┬─────────────┬───────────┐
│      timestamp      │  detections  │ event id │ logon type  │    username    │      computer       │ ip address  │ record id │
├─────────────────────┼──────────────┼──────────┼─────────────┼────────────────┼─────────────────────┼─────────────┼───────────┤
│ 2023-06-10 10:49:57 │ ‣ RDP logon  │ 4624     │ 10          │ salma.gilbert  │ RDSH01.cfdemolab.fi │ 10.0.1.2    │ 46750     │
└─────────────────────┴──────────────┴──────────┴─────────────┴────────────────┴─────────────────────┴─────────────┴───────────┘
```

Chainsaw: RD Session Host successful logon event



```
[+] Group: Microsoft RDS Events - User Profile Disk
┌─────────────────────┬─────────────────────────────────┬──────────┬──────────────────────────────────┬─────────────────────┬─────────────────────────────────┐
│      timestamp      │           detections            │ Event ID │             Channel              │      Computer       │           Information           │
├─────────────────────┼─────────────────────────────────┼──────────┼──────────────────────────────────┼─────────────────────┼─────────────────────────────────┤
│ 2023-06-10 10:50:15 │ ‣ User Profile Disk - Registry  │ 5        │ Microsoft-Windows-User Profile   │ RDSH01.cfdemolab.fi │ C:\Users\salma.gilbert\ntuser.  │
│                     │ file loaded                     │          │  Service/Operational             │                     │ dat                             │
├─────────────────────┼─────────────────────────────────┼──────────┼──────────────────────────────────┼─────────────────────┼─────────────────────────────────┤
│ 2023-06-10 10:50:15 │ ‣ User Profile Disk - Registry  │ 5        │ Microsoft-Windows-User Profile   │ RDSH01.cfdemolab.fi │ C:\Users\salma.gilbert\AppData  │
│                     │ file loaded                     │          │  Service/Operational             │                     │ \Local\Microsoft\Windows\\UsrC  │
│                     │                                 │          │                                  │                     │ lass.dat                        │
├─────────────────────┼─────────────────────────────────┼──────────┼──────────────────────────────────┼─────────────────────┼─────────────────────────────────┤
```

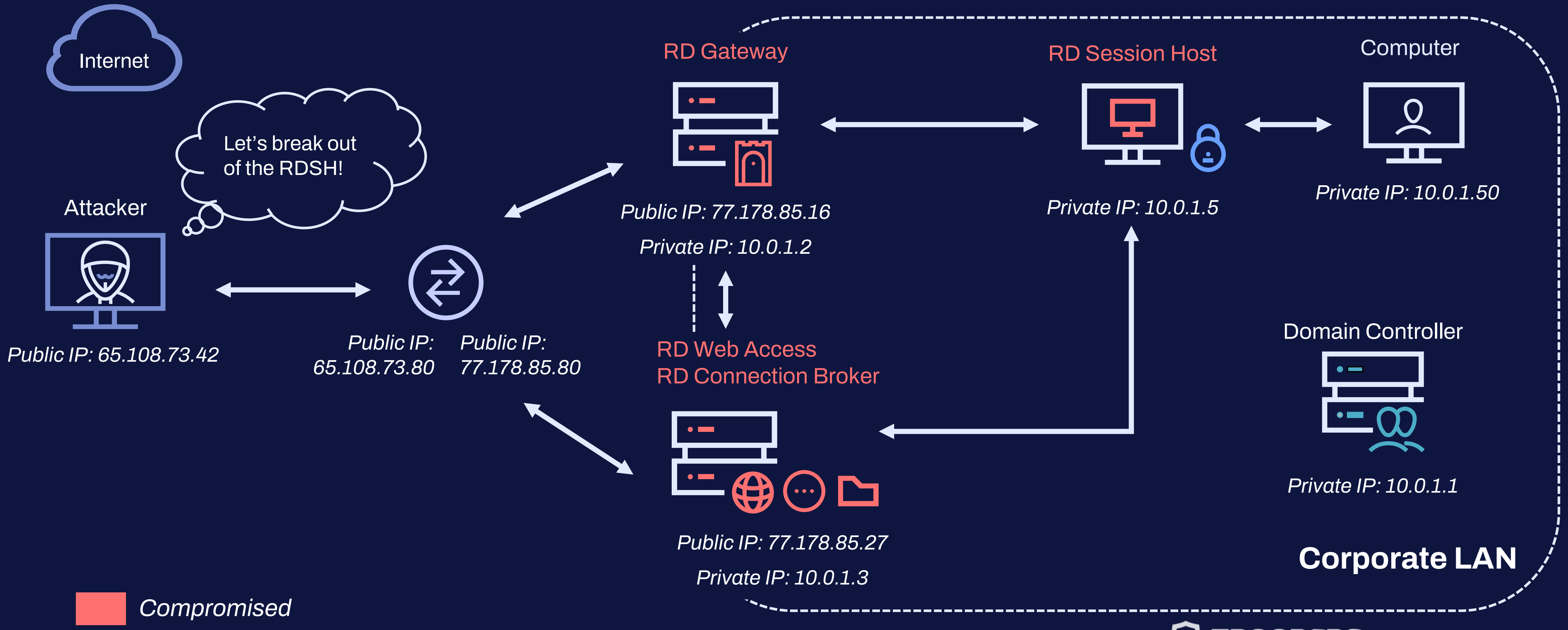
Chainsaw: User Profile Disk events

III. How to compromise and investigate an RDS infrastructure

Breaking out of RDS

Breaking out of RDS

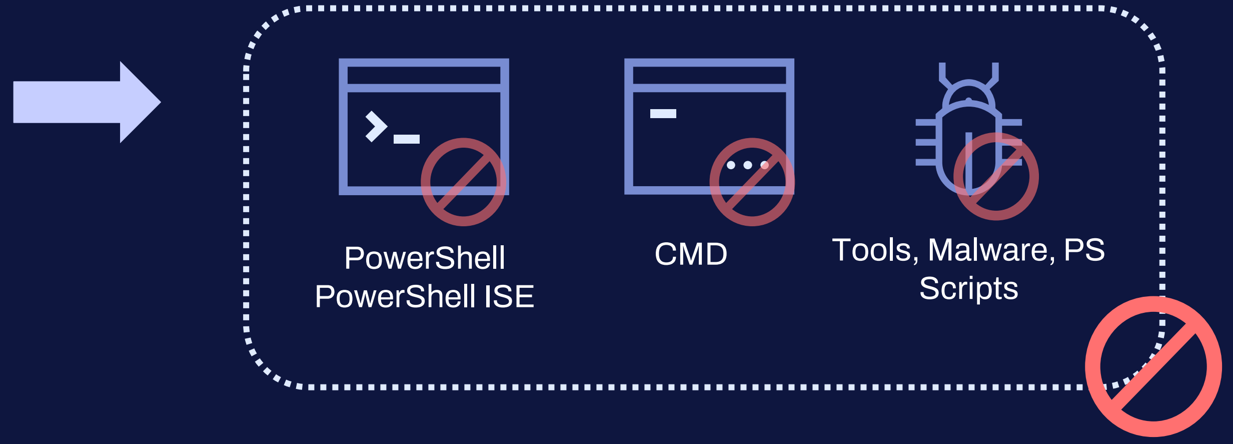
How to compromise and investigate an RDS infrastructure



TROOPERS WITH secure

Breaking out of RDS

How to compromise and investigate an RDS infrastructure



Cannot be used

- Cannot **power off** the machine
- **Local Group Policy** to **block CMD**
- **AppLocker Default Rules** and additional **rules** to block **PowerShell** and **PowerShell ISE**

Breaking out of RDS

How to compromise and investigate an RDS infrastructure

CMD ✓

- **ReactOS CMD**
- **LOLBins** such as **ftp.exe** or the **WMIC CLI**

PowerShell
PowerShell ISE ✓

- **Powershell runspaces**

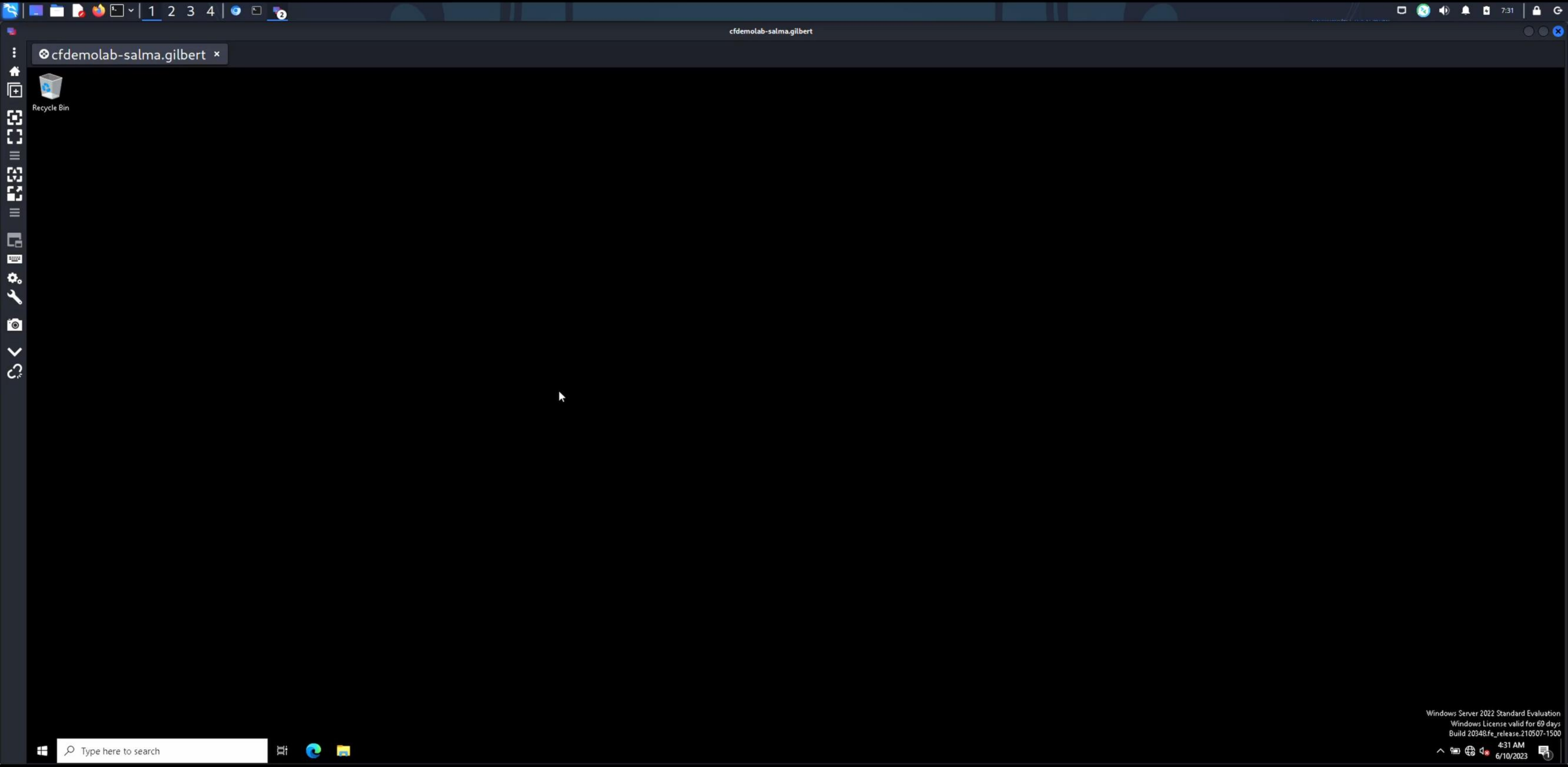
Tools, Malware,
PS Scripts ✓

- **Writable authorized directories** e.g., C:\Windows\Tasks

Breaking out of RDS

How to compromise and investigate an RDS infrastructure

DEMO



Windows Server 2022 Standard Evaluation
Windows License valid for 69 days
Build 20348.fe_release.210507-1500

Breaking out of RDS

How to compromise and investigate an RDS infrastructure

- What did we observe?

RD Session Host events

- **AppLocker/EXE and DLL**
  - **EID 8002**: EXE/DLL allowed to run
  - **EID 8004**: EXE/DLL prevented from running
- **AppLocker/MSI and Script**
  - **EID 8007**: MSI and Script prevented from running

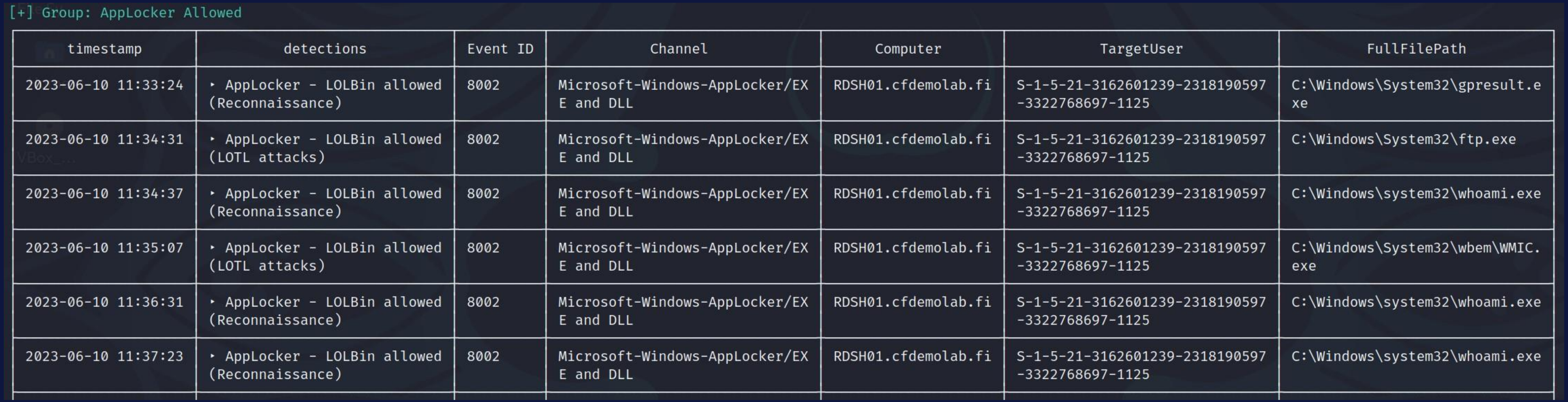
- **PowerShell**
  - **EID 4104**: Script Block auditing

- **Windows Defender**
  - **EID 1116**: Malware Detected

PowerShell history file: ***ConsoleHost_history.txt***

Breaking out of RDS

How to compromise and investigate an RDS infrastructure



```
[+] Group: AppLocker Allowed
┌─────────────────────┬──────────────────────────────┬──────────┬───────────────────────────────┬─────────────────────┬───────────────────────────────┬───────────────────────────────┐
│      timestamp      │          detections          │ Event ID │            Channel            │      Computer       │          TargetUser           │         FullFilePath          │
├─────────────────────┼──────────────────────────────┼──────────┼───────────────────────────────┼─────────────────────┼───────────────────────────────┼───────────────────────────────┤
│ 2023-06-10 11:33:24 │ ‣ AppLocker - LOLBin allowed │ 8002     │ Microsoft-Windows-AppLocker/EX │ RDSH01.cfdemolab.fi │ S-1-5-21-3162601239-2318190597 │ C:\Windows\System32\gpresult.e │
│                     │ (Reconnaissance)             │          │ E and DLL                     │                     │ -3322768697-1125              │ xe                            │
├─────────────────────┼──────────────────────────────┼──────────┼───────────────────────────────┼─────────────────────┼───────────────────────────────┼───────────────────────────────┤
│ 2023-06-10 11:34:31 │ ‣ AppLocker - LOLBin allowed │ 8002     │ Microsoft-Windows-AppLocker/EX │ RDSH01.cfdemolab.fi │ S-1-5-21-3162601239-2318190597 │ C:\Windows\System32\ftp.exe   │
│                     │ (LOTL attacks)               │          │ E and DLL                     │                     │ -3322768697-1125              │                               │
├─────────────────────┼──────────────────────────────┼──────────┼───────────────────────────────┼─────────────────────┼───────────────────────────────┼───────────────────────────────┤
│ 2023-06-10 11:34:37 │ ‣ AppLocker - LOLBin allowed │ 8002     │ Microsoft-Windows-AppLocker/EX │ RDSH01.cfdemolab.fi │ S-1-5-21-3162601239-2318190597 │ C:\Windows\system32\whoami.exe │
│                     │ (Reconnaissance)             │          │ E and DLL                     │                     │ -3322768697-1125              │                               │
├─────────────────────┼──────────────────────────────┼──────────┼───────────────────────────────┼─────────────────────┼───────────────────────────────┼───────────────────────────────┤
│ 2023-06-10 11:35:07 │ ‣ AppLocker - LOLBin allowed │ 8002     │ Microsoft-Windows-AppLocker/EX │ RDSH01.cfdemolab.fi │ S-1-5-21-3162601239-2318190597 │ C:\Windows\System32\wbem\WMIC. │
│                     │ (LOTL attacks)               │          │ E and DLL                     │                     │ -3322768697-1125              │ exe                           │
├─────────────────────┼──────────────────────────────┼──────────┼───────────────────────────────┼─────────────────────┼───────────────────────────────┼───────────────────────────────┤
│ 2023-06-10 11:36:31 │ ‣ AppLocker - LOLBin allowed │ 8002     │ Microsoft-Windows-AppLocker/EX │ RDSH01.cfdemolab.fi │ S-1-5-21-3162601239-2318190597 │ C:\Windows\system32\whoami.exe │
│                     │ (Reconnaissance)             │          │ E and DLL                     │                     │ -3322768697-1125              │                               │
├─────────────────────┼──────────────────────────────┼──────────┼───────────────────────────────┼─────────────────────┼───────────────────────────────┼───────────────────────────────┤
│ 2023-06-10 11:37:23 │ ‣ AppLocker - LOLBin allowed │ 8002     │ Microsoft-Windows-AppLocker/EX │ RDSH01.cfdemolab.fi │ S-1-5-21-3162601239-2318190597 │ C:\Windows\system32\whoami.exe │
│                     │ (Reconnaissance)             │          │ E and DLL                     │                     │ -3322768697-1125              │                               │
├─────────────────────┼──────────────────────────────┼──────────┼───────────────────────────────┼─────────────────────┼───────────────────────────────┼───────────────────────────────┤
```

Chainsaw: AppLocker allowed EXE/DLL

III. How to compromise and investigate an RDS infrastructure

Additional compromise

Additional compromise

How to compromise and investigate an RDS infrastructure

- Adversaries will usually try to:
  - **avoid detection**
  - **gain knowledge** about the **system** and **internal network**
  - gain **higher-level permissions**
  - **pivot** until reaching the objective

Impair Defenses

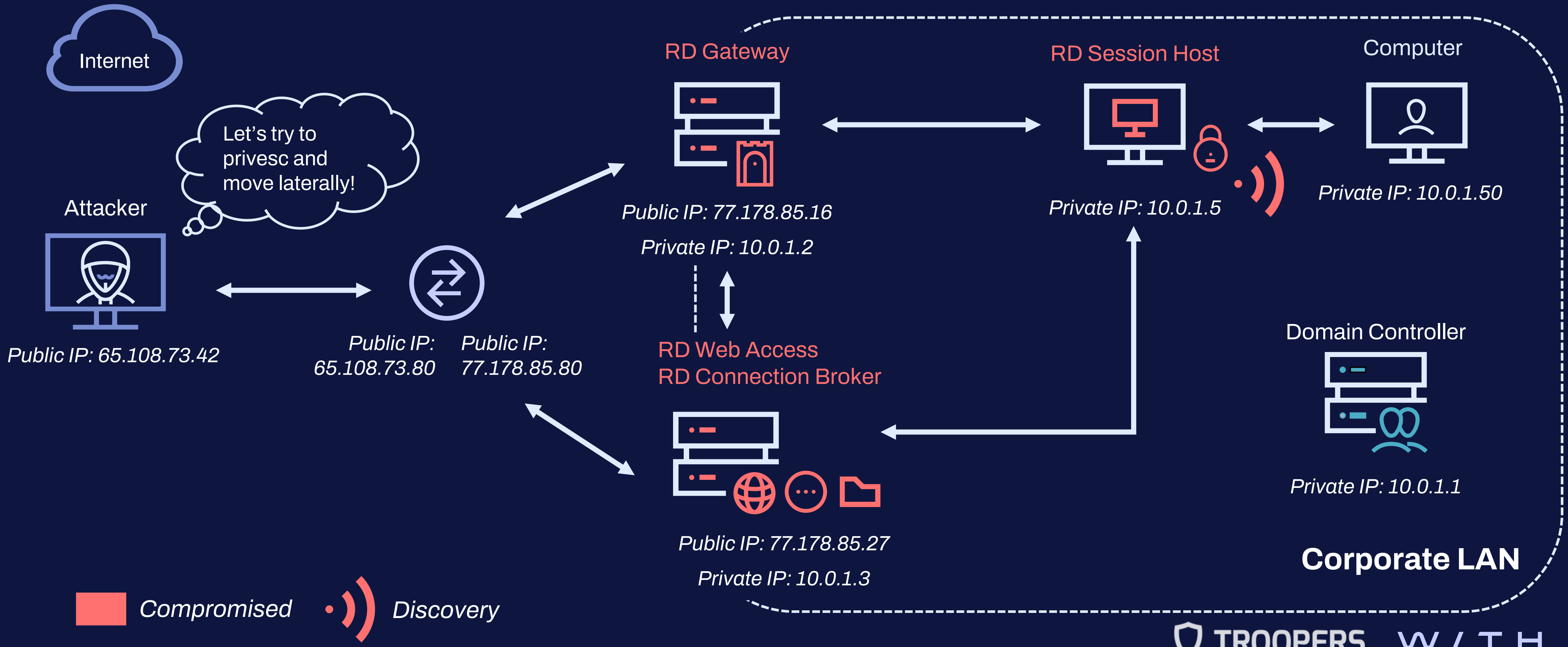
Discovery

Privilege Escalation

Lateral Movement

Additional compromise

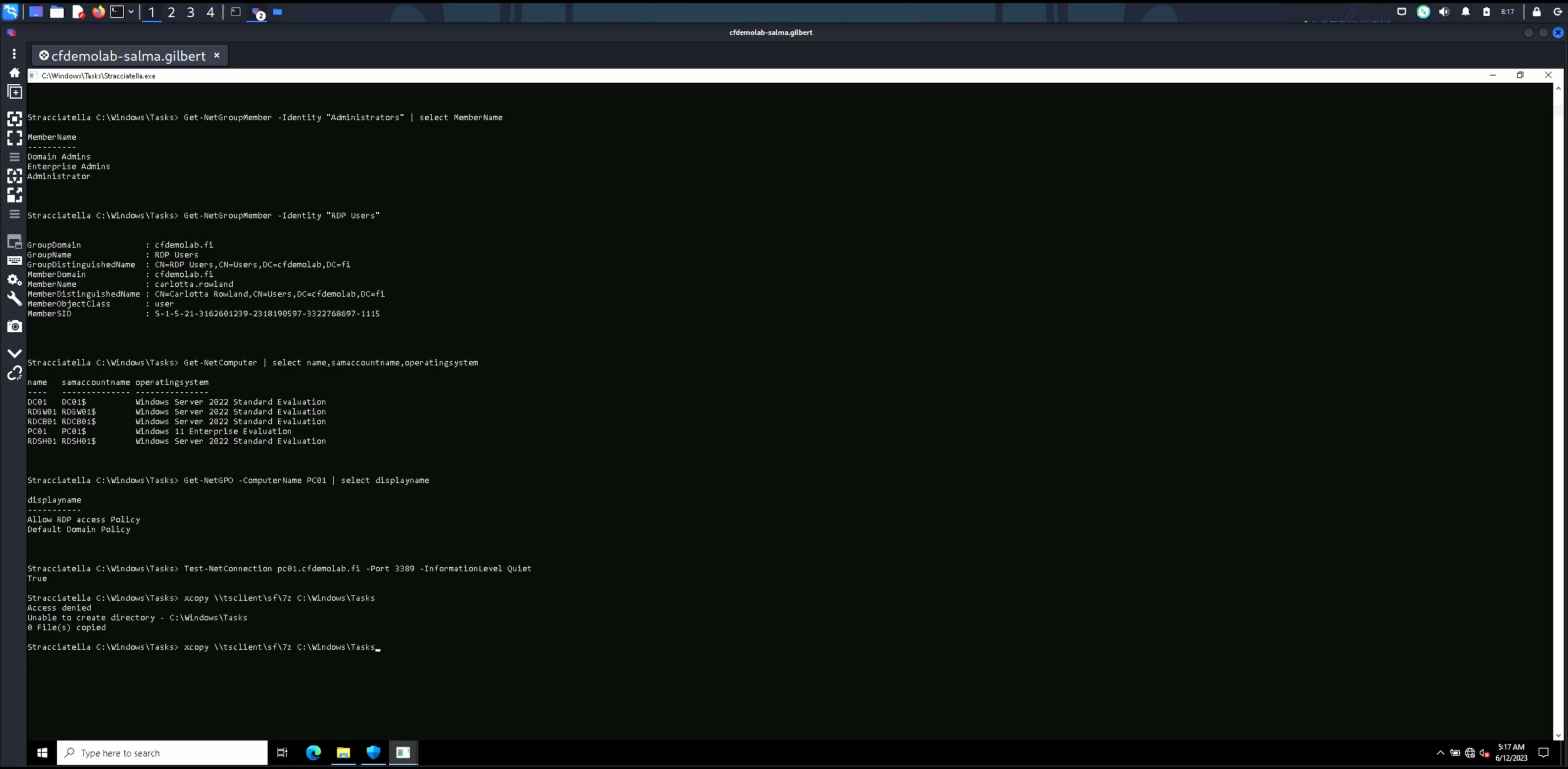
How to compromise and investigate an RDS infrastructure



Additional compromise

How to compromise and investigate an RDS infrastructure

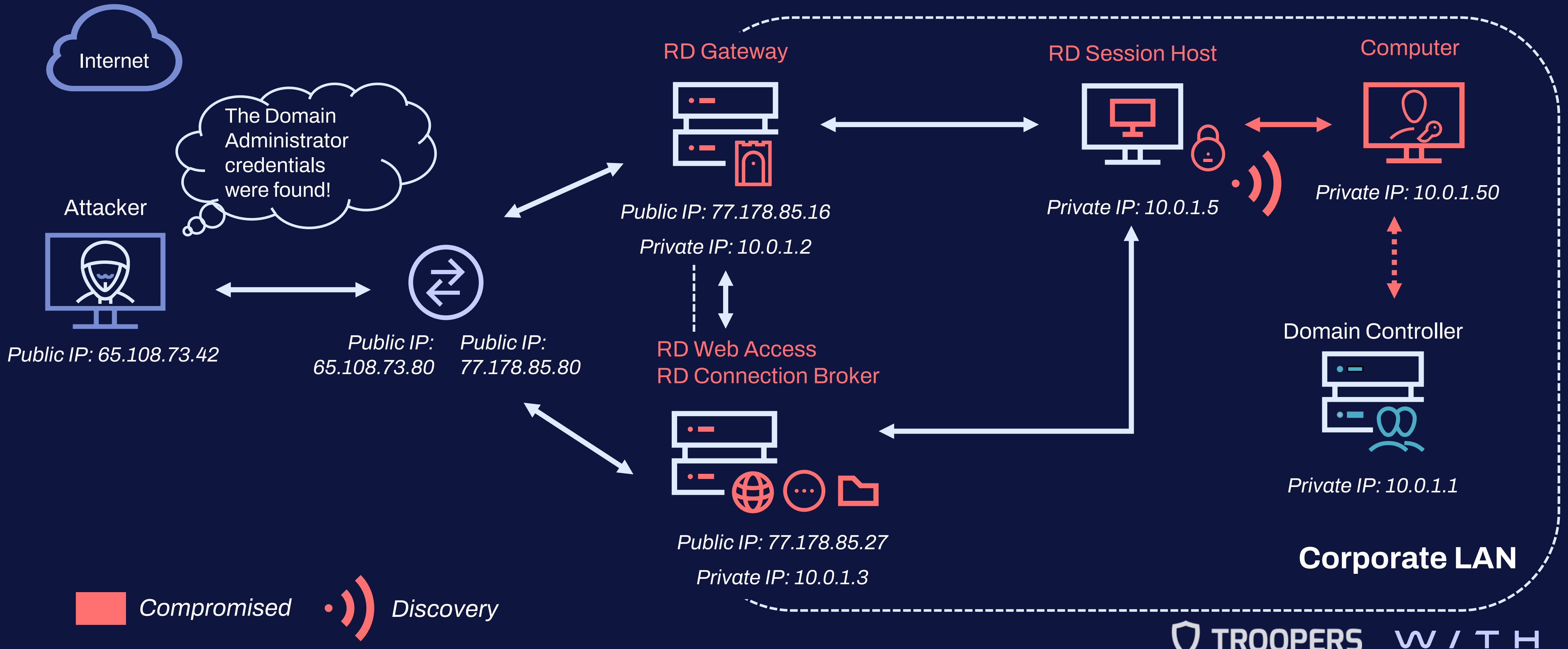
DEMO



```
Stracciatella C:\Windows\Tasks> Get-NetGroupMember -Identity "Administrators" | select MemberName

MemberName
----------
Domain Admins
Enterprise Admins
Administrator



Stracciatella C:\Windows\Tasks> Get-NetGroupMember -Identity "RDP Users"


GroupDomain             : cfdemolab.fi
GroupName               : RDP Users
GroupDistinguishedName  : CN=RDP Users,CN=Users,DC=cfdemolab,DC=fi
MemberDomain            : cfdemolab.fi
MemberName              : carlotta.rowland
MemberDistinguishedName : CN=Carlotta Rowland,CN=Users,DC=cfdemolab,DC=fi
MemberObjectClass       : user
MemberSID               : S-1-5-21-3162601239-2318190597-3322768697-1115



Stracciatella C:\Windows\Tasks> Get-NetComputer | select name,samaccountname,operatingsystem

name   samaccountname operatingsystem
----   -------------- ---------------
DC01   DC01$          Windows Server 2022 Standard Evaluation
RDGW01 RDGW01$        Windows Server 2022 Standard Evaluation
RDCB01 RDCB01$        Windows Server 2022 Standard Evaluation
PC01   PC01$          Windows 11 Enterprise Evaluation
RDSH01 RDSH01$        Windows Server 2022 Standard Evaluation



Stracciatella C:\Windows\Tasks> Get-NetGPO -ComputerName PC01 | select displayname

displayname
-----------
Allow RDP access Policy
Default Domain Policy



Stracciatella C:\Windows\Tasks> Test-NetConnection pc01.cfdemolab.fi -Port 3389 -InformationLevel Quiet
True

Stracciatella C:\Windows\Tasks> xcopy \\tsclient\sf\7z C:\Windows\Tasks
Access denied
Unable to create directory - C:\Windows\Tasks
0 File(s) copied

Stracciatella C:\Windows\Tasks> xcopy \\tsclient\sf\7z C:\Windows\Tasks_
```

Additional compromise

How to compromise and investigate an RDS infrastructure



TROOPERS WITH secure

III. How to compromise and investigate an RDS infrastructure

Real-world attacks: Case #1

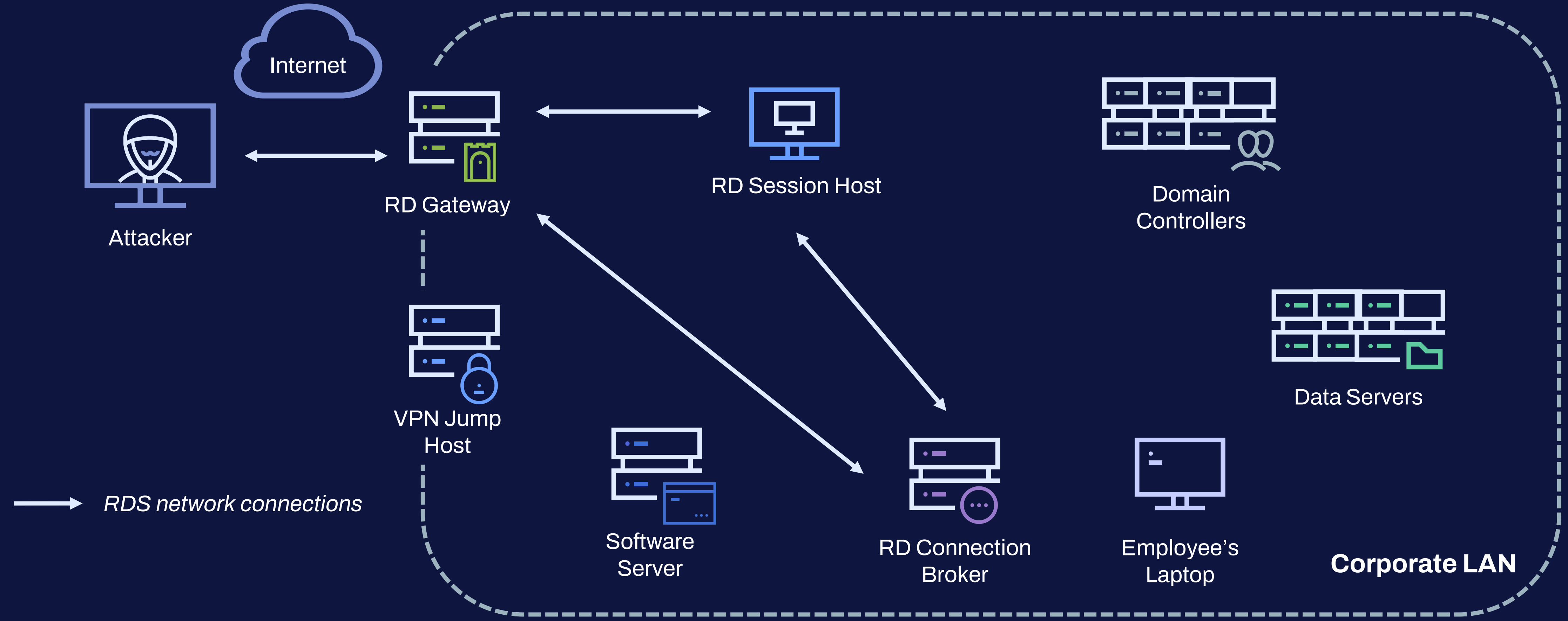
Real-world attacks: Case #1

How to compromise and investigate an RDS infrastructure

- **On-premises** RDS deployment
- **Employee's credentials** were used**,** no trace of a **brute-force attempt**
  - Drive sharing enabled (**kerberoast.exe**, **rubeus.exe**, etc.)
- **PowerShell console** from one of the RD Session Hosts

Real-world attacks: Case #1

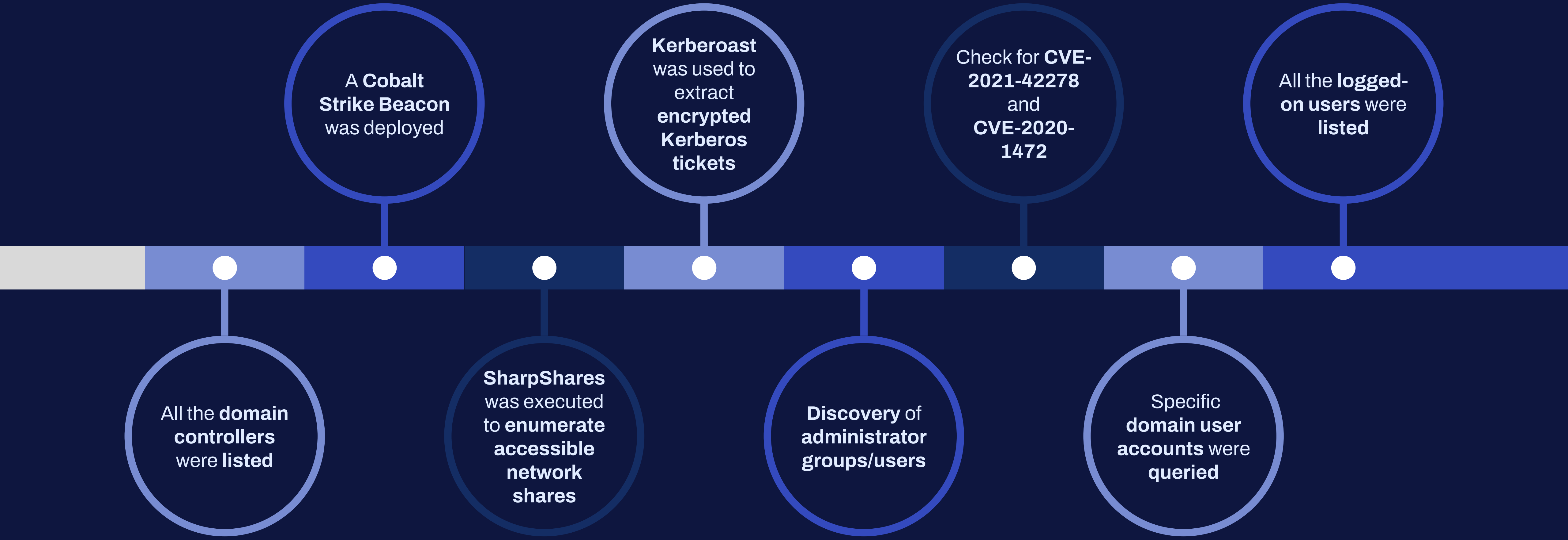
How to compromise and investigate an RDS infrastructure



Real-world attacks: Case #1

How to compromise and investigate an RDS infrastructure

RD Session Host



All the **domain controllers** were **listed**

A **Cobalt Strike Beacon** was deployed

SharpShares was executed to **enumerate accessible network shares**

Kerberoast was used to extract **encrypted Kerberos tickets**

Discovery of **administrator groups/users**

Check for **CVE-2021-42278** and **CVE-2020-1472**

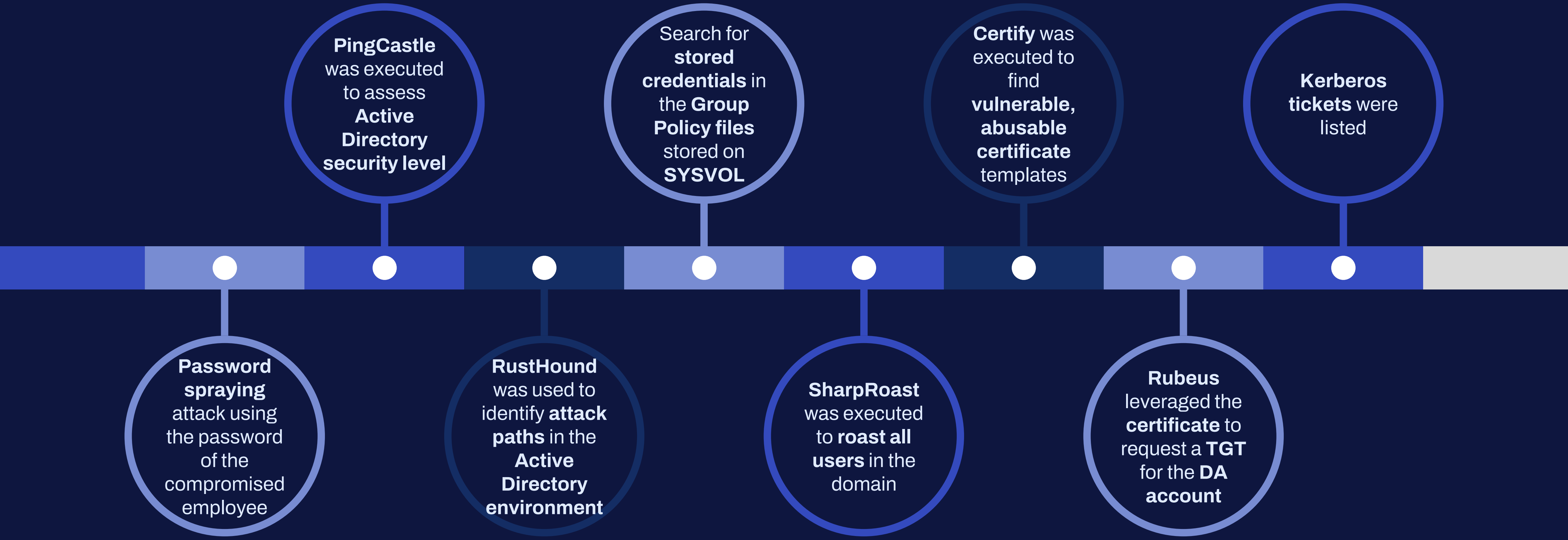
Specific **domain user accounts** were **queried**

All the **logged-on users** were **listed**

Real-world attacks: Case #1

How to compromise and investigate an RDS infrastructure

RD Session Host



Password spraying attack using the password of the compromised employee

PingCastle was executed to assess **Active Directory security level**

RustHound was used to identify **attack paths** in the **Active Directory environment**

Search for **stored credentials** in the **Group Policy files** stored on **SYSVOL**

SharpRoast was executed to **roast all users** in the domain

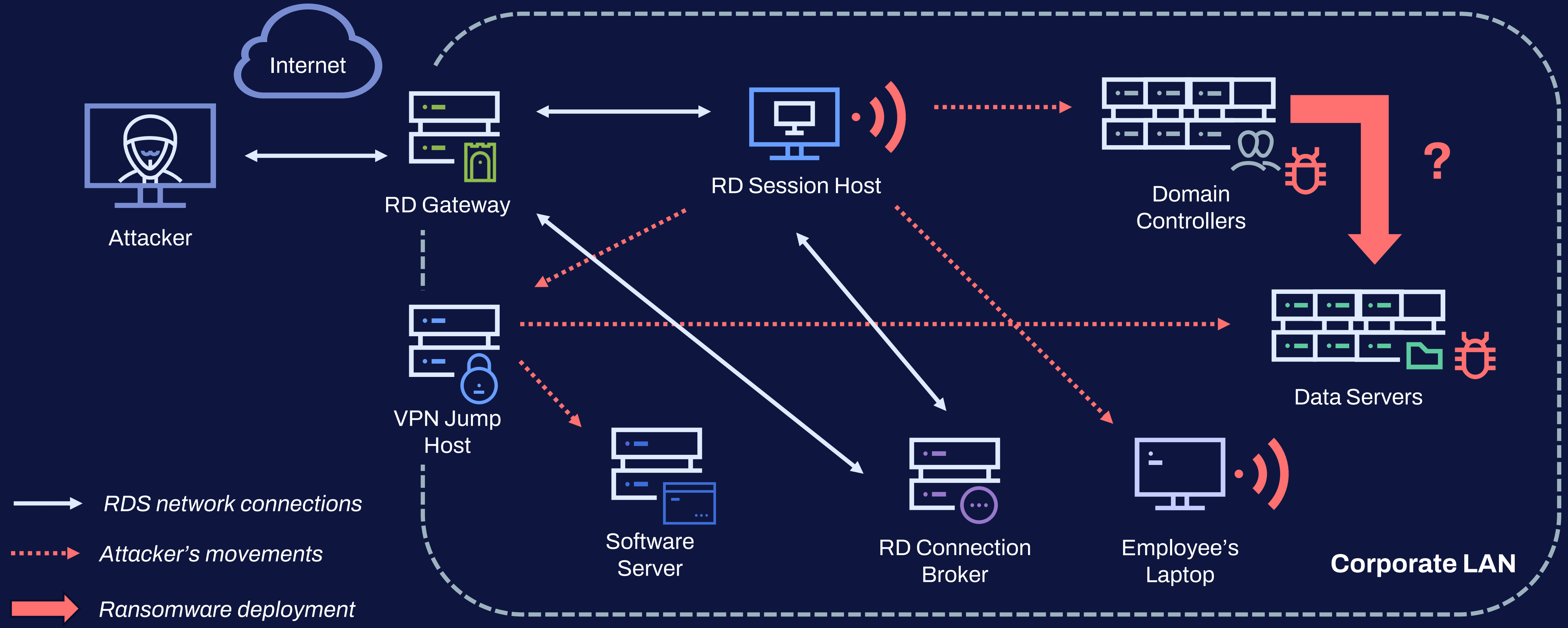
Certify was executed to find **vulnerable, abusable certificate** templates

Rubeus leveraged the **certificate** to request a **TGT** for the **DA account**

Kerberos tickets were listed

Real-world attacks: Case #1

How to compromise and investigate an RDS infrastructure



III. How to compromise and investigate an RDS infrastructure

Real-world attacks: Case #2

Real-world attacks: Case #2

How to compromise and investigate an RDS infrastructure

- RDS deployment on **Google Cloud Platform (GCP)**
- A **service account** was used to connect **directly** to RD Session Hosts.
  - Credentials probably obtained via **brute-force**
  - Service account configured as a **user/AD account** so it could be used for login
  - **Weak password**, never changed in 5 years
  - **Public-facing** RD Session Hosts
- The tool **“Angry IP”** was executed from the RD Session Hosts to perform a **network scan**.
- A few days later, the threat actor came back and started **moving laterally** using **RDP** until reaching the **internal network** on GCP.

Real-world attacks: Case #2

How to compromise and investigate an RDS infrastructure

- A second **service account** was compromised.
  - Capable of logging into to the RD Session hosts
  - Belonged to the **Backup Operators group**
- **DCSync** attack using **Mimikatz**.
  - EDR detected it but did not block it.
- Soon after, there were **RDP** connections from that host to the **Domain Controller** as the **Domain Administrator**.
- The **LV ransomware** was deployed using a **GPO**.

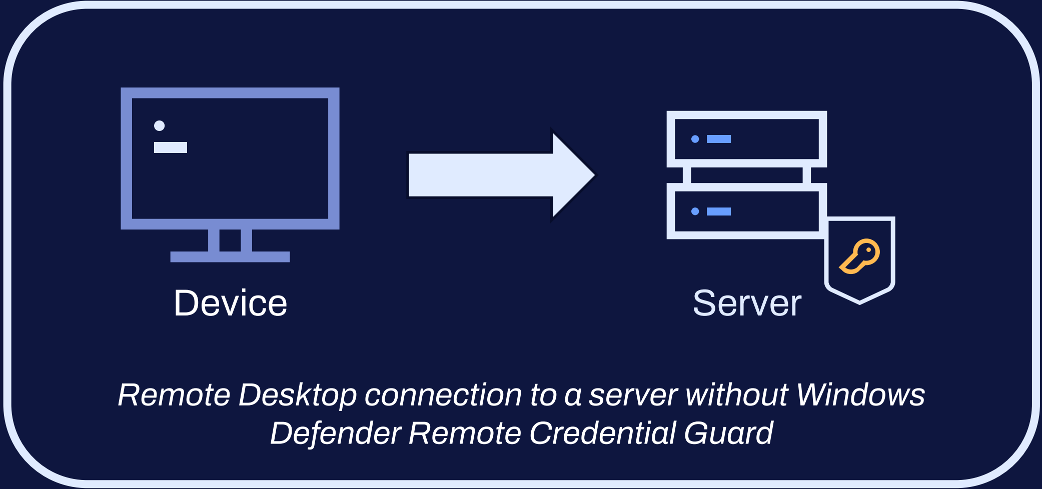
IV. How to protect against such attacks

Recommendations

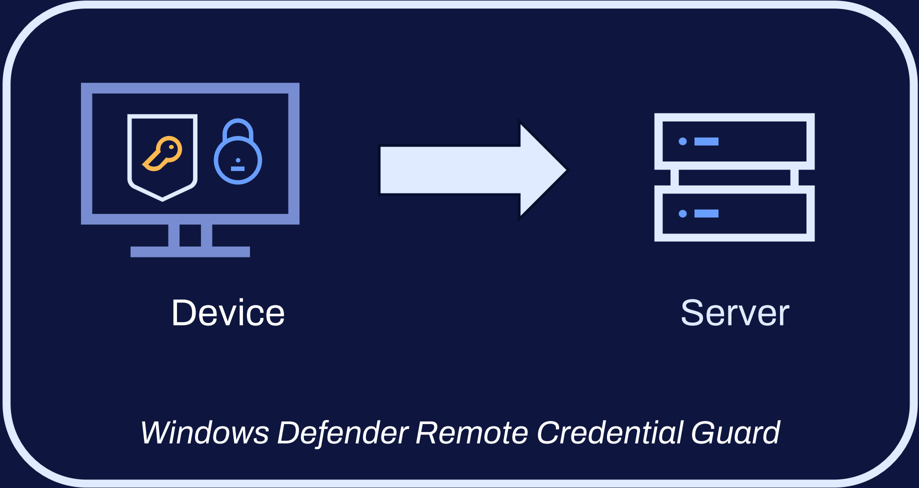
Recommendations

How to protect against such attacks

- **Windows Defender Remote Credential Guard**
  - **Isolated LSA process**, which runs in Virtual Secure Mode (VSM)
  - Blocks **NTLM** (allowing only Kerberos)
  - Prevents **Pass-the-Hash (PtH)** attacks, and the use of **credentials after disconnection**



Remote Desktop connection to a server without Windows Defender Remote Credential Guard



Windows Defender Remote Credential Guard

Recommendations

How to protect against such attacks

- Use **Multi-factor authentication (MFA)**
  - Prevent **dictionary attacks** and reduce the risk related to **compromised credentials**
    - **Duo Authentication** for Microsoft Remote Desktop Web and Remote Desktop Gateway
    - **Azure Multi-Factor Authentication** for RD Gateway using RADIUS
    - **Okta MFA Credential Provider** for RDS
    - **AuthLite**: 2FA with Remote Desktop Gateway / RemoteApp / RDWeb / RD Web Client

Recommendations

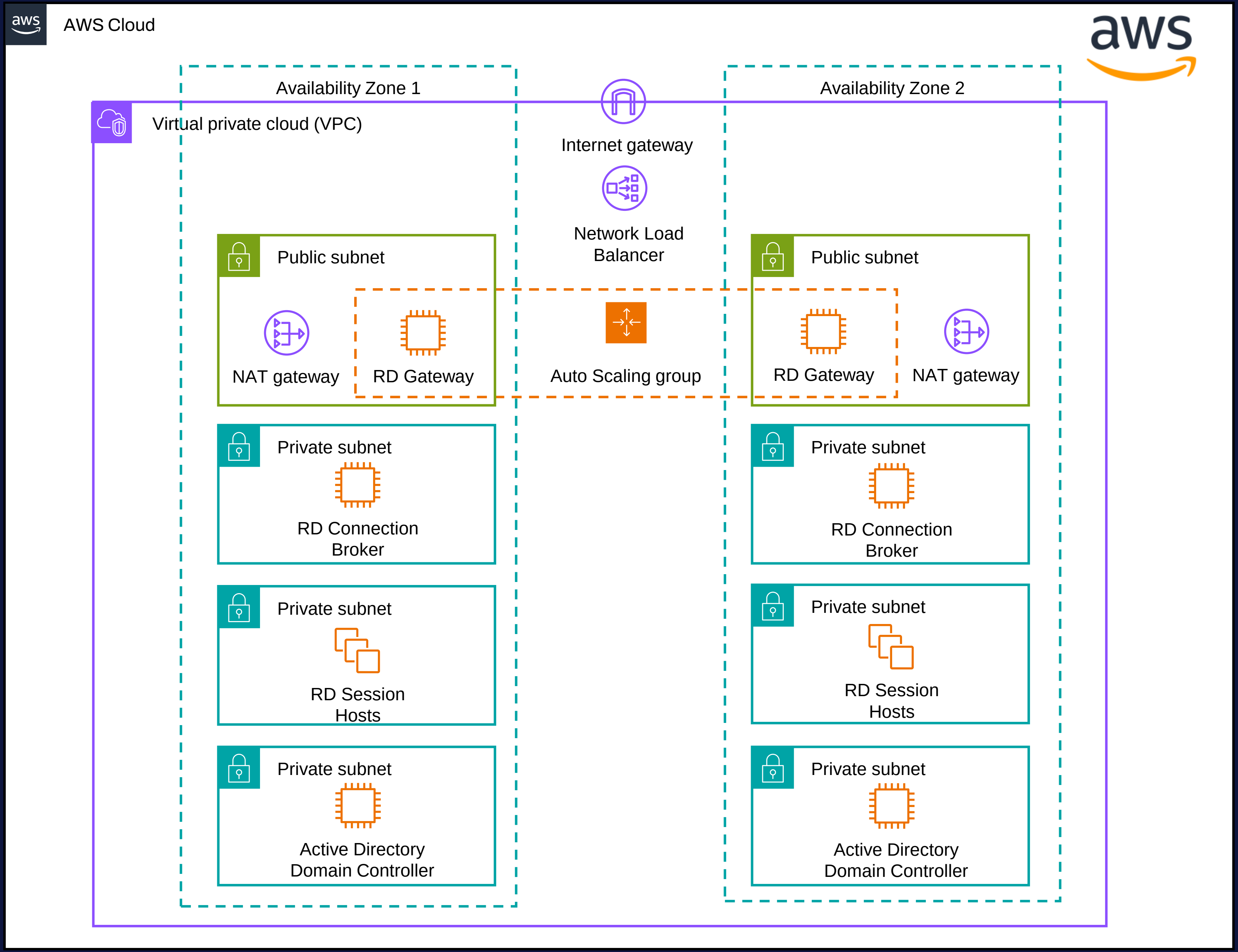
How to protect against such attacks

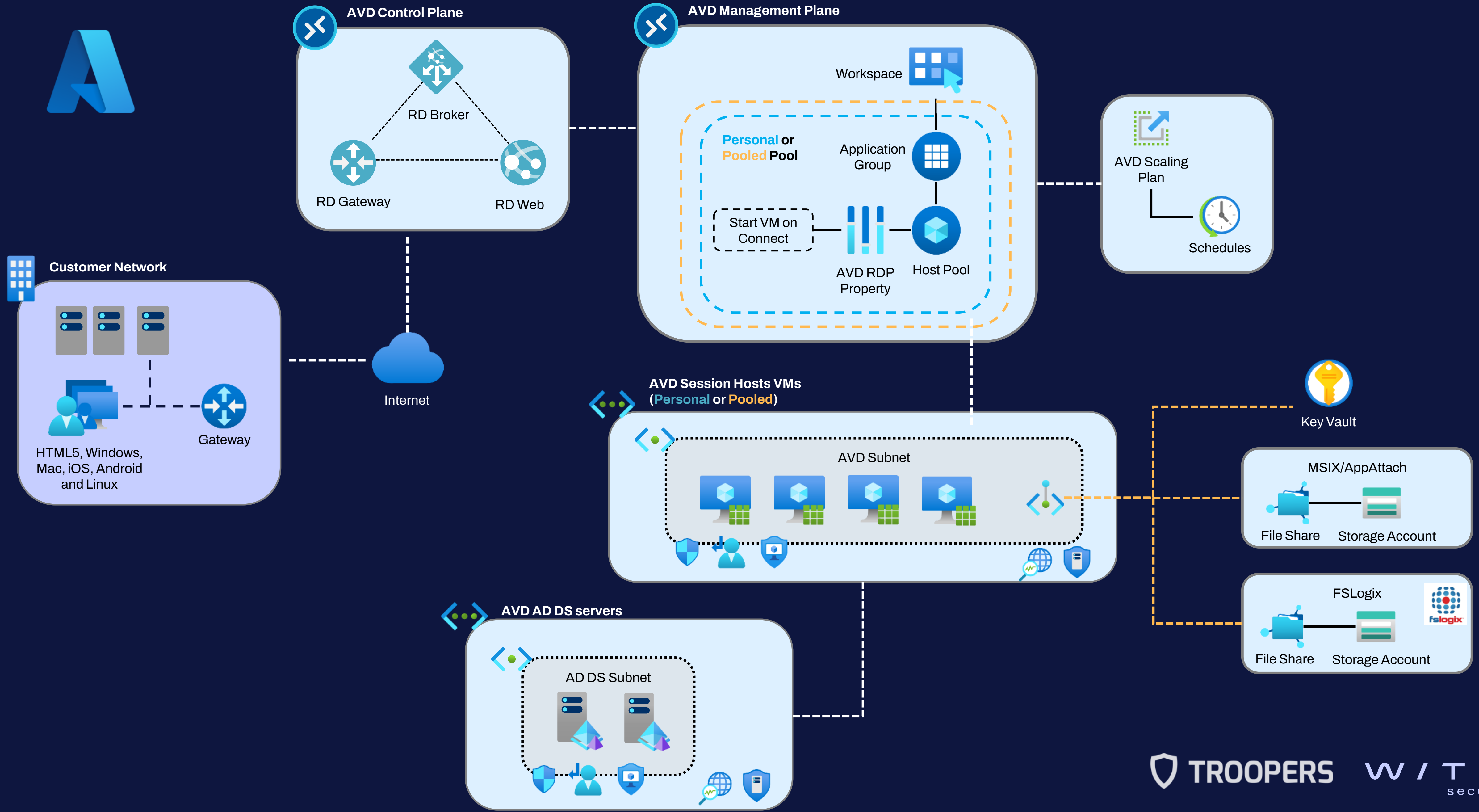
- **General mitigations**
  - Improve **logging**
  - **Harden** the RD Session Host
  - Keep all operating systems, software, and firmware **up to date**
  - Deploy the public facing RDS roles into a **DMZ**
  - Place RDS servers behind a **VPN** or an **RD Gateway** (**MFA** enabled)
  - Deploy **cloud bastions**
  - Strictly **limit** the use of **RDP** and other remote desktop services within the network

Thank you for your attention!

Questions

WITH®
secure


AWS Cloud
Availability Zone 1
Availability Zone 2
Virtual private cloud (VPC)
Internet gateway
Network Load Balancer
Public subnet
NAT gateway
RD Gateway
Auto Scaling group
Public subnet
RD Gateway
NAT gateway
Private subnet
RD Connection Broker
Private subnet
RD Connection Broker
Private subnet
RD Session Hosts
Private subnet
RD Session Hosts
Private subnet
Active Directory Domain Controller
Private subnet
Active Directory Domain Controller



AVD Control Plane

RD Broker

RD Gateway

RD Web

AVD Management Plane

Workspace

Personal or Pooled Pool

Application Group

Start VM on Connect

AVD RDP Property

Host Pool

AVD Scaling Plan

Schedules

Customer Network

HTML5, Windows, Mac, iOS, Android and Linux

Gateway

Internet

AVD Session Hosts VMs (Personal or Pooled)

AVD Subnet

Key Vault

MSIX/AppAttach

File Share

Storage Account

FSLogix

fslogix

File Share

Storage Account

AVD AD DS servers

AD DS Subnet

TROOPERS

W/TH secure