SUREFIRE CYBER

Anatomy of a Ransomware Incident

Billy Gouveia

November 19, 2024

Ransomware – A Multifaceted Problem

- What is ransomware?:
  - A threat actor encrypts data demands a ransom in exchange for a decryption key, or
  - A threat actor steals data and demands a ransom in exchange for a promise to not publish it, or
  - Both (referred to as *double extortion*)

- Ransomware is the perfect crime:
  - Easy to commit,
  - Enormously lucrative, and
  - Done with (near) impunity

- Ransomware is a multidimensional problem:
  - Network Intrusion
  - Data Theft
  - Business Interruption
  - Legal, Regulatory, & Reputational Risk

```
Your computer files have        pted. Your photos, videos
But, don't worry! I ha          them, yet.
You have 24 hours to            itcoins to get the dec
Every hour files wil            easing in amount every
After 72 hours all t            be deleted.

If you do not have              website localbitcoins
Purchase 150 America            Bitcoins or .4 BTC.
Send to the Bitcoins            .
Within two minutes o            payment your computer
Try anything funny and          has several safety meas
As soon as the payment is       d the crypted files will b

      Thank you
```

Stages of a Ransomware Attack

1. **Reconnaissance**
   Finding the target
2. **Point of Entry**
   Breaking in
3. **Privilege Escalation**
   Getting more access
4. **Lateral Movement**
   Moving around
5. **Exfiltration**
   Stealing data
6. **Encryption**
   Locking up your files

Stage 1 Reconnaissance

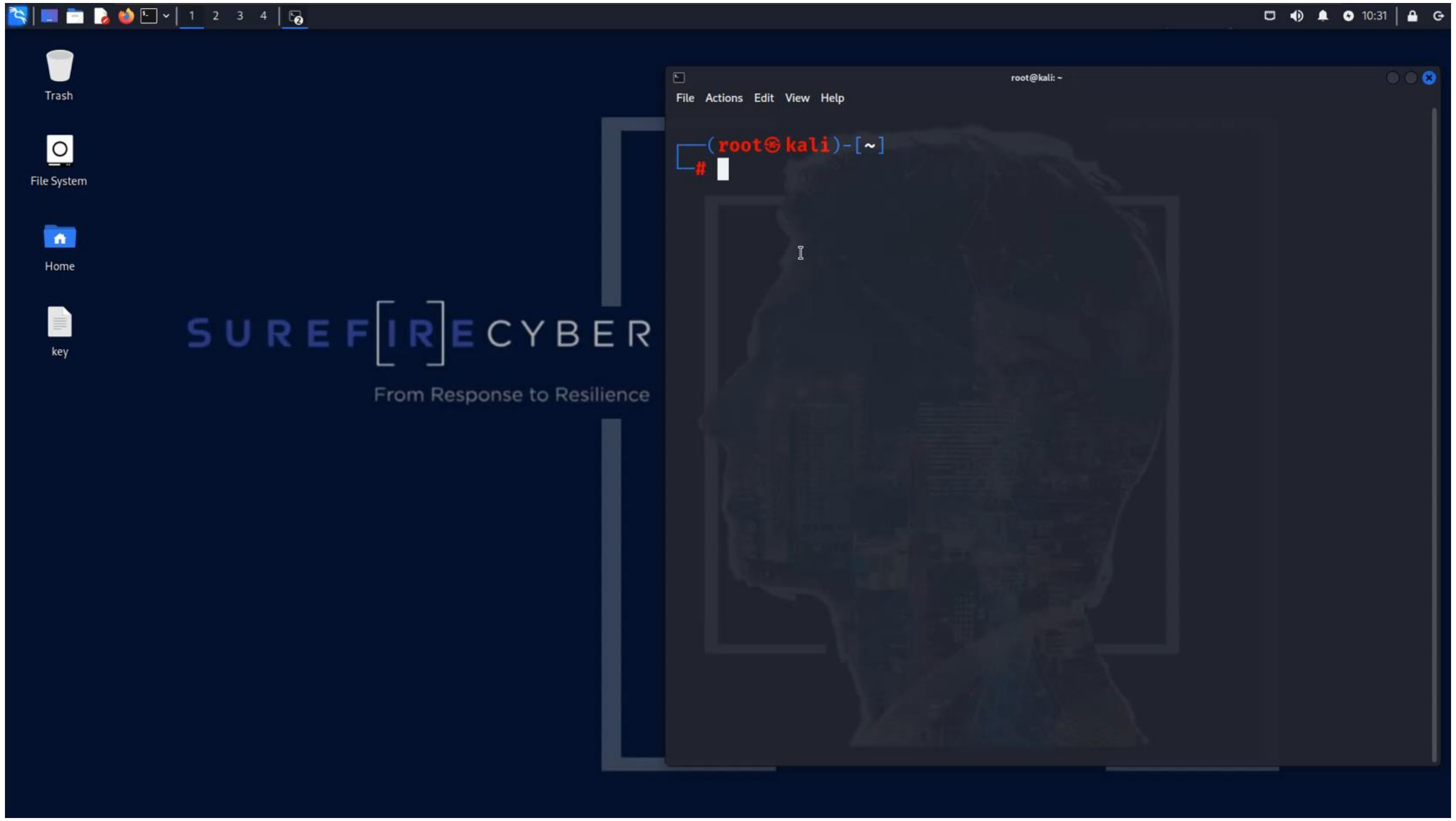
Finding the Target

Setting the Scene

- Threat actors are ALWAYS scanning the complete internet to find weaknesses or looking to buy access
- Full scan of the internet can take as little as 45 minutes

Takeaways

- Threat actors don't need to be "targeting" you to discover an exploitable weakness
- Securing your internet-facing perimeter will help prevent cyber incidents



```
┌──(root㉿kali)-[~]
└─# 
```

Stage 2 Point of Entry

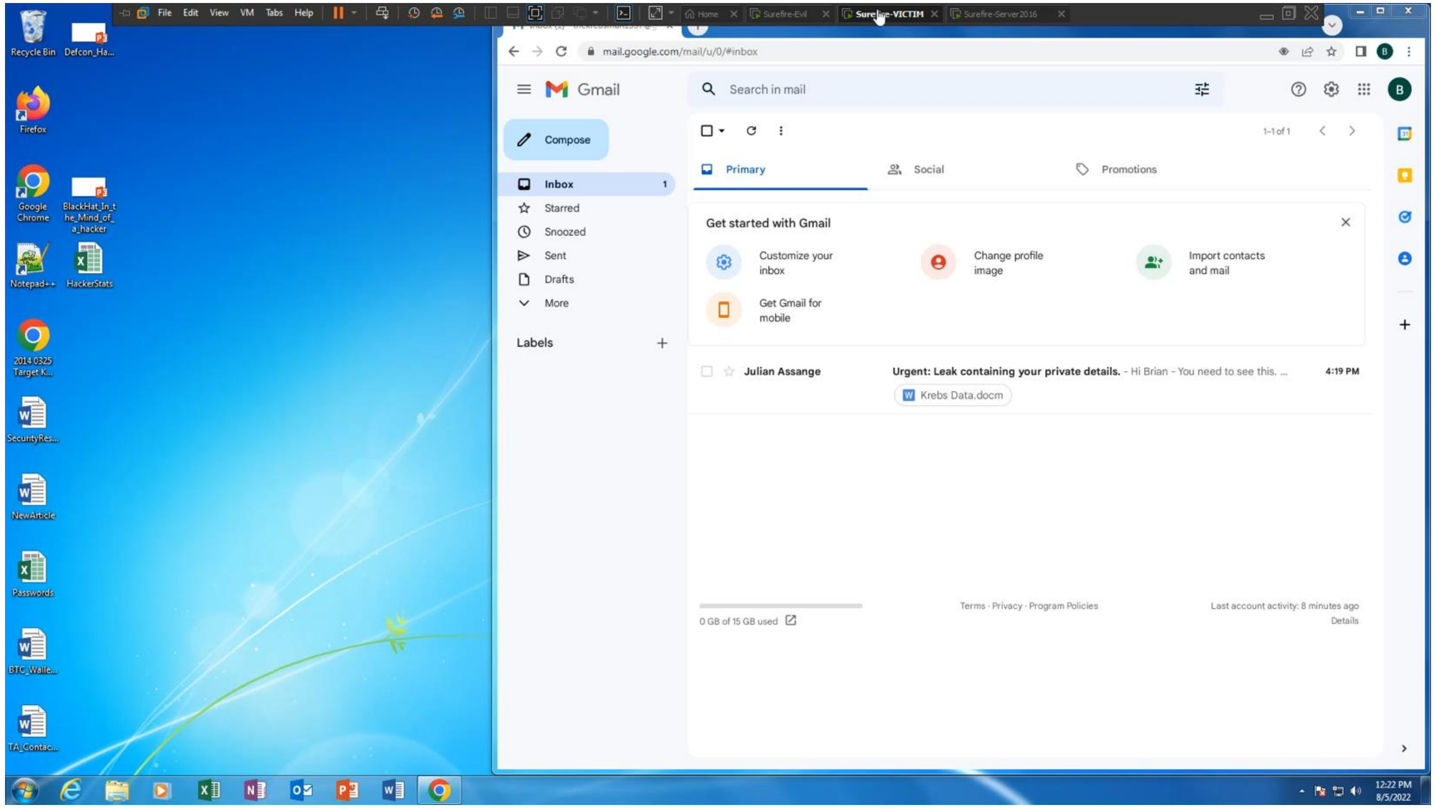
Patient Zero

Setting the Scene

- Not finding an external weakness, the threat actor sends an email embedded with malware
- Phishing is very common and can be generic (“Singles in Your Area”) or targeted (“Kevin’s Year End Bonus”)

Takeaways

- User awareness training and email filtering lower risk of phishing
- Multi-factor authentication is the best way to stop phishing
- Endpoint Security Solution



mail.google.com/mail/u/0/#inbox

Julian Assange — Urgent: Leak containing your private details. - Hi Brian - You need to see this. ... — 4:19 PM

Krebs Data.docm

Stage 3 Privilege Escalation

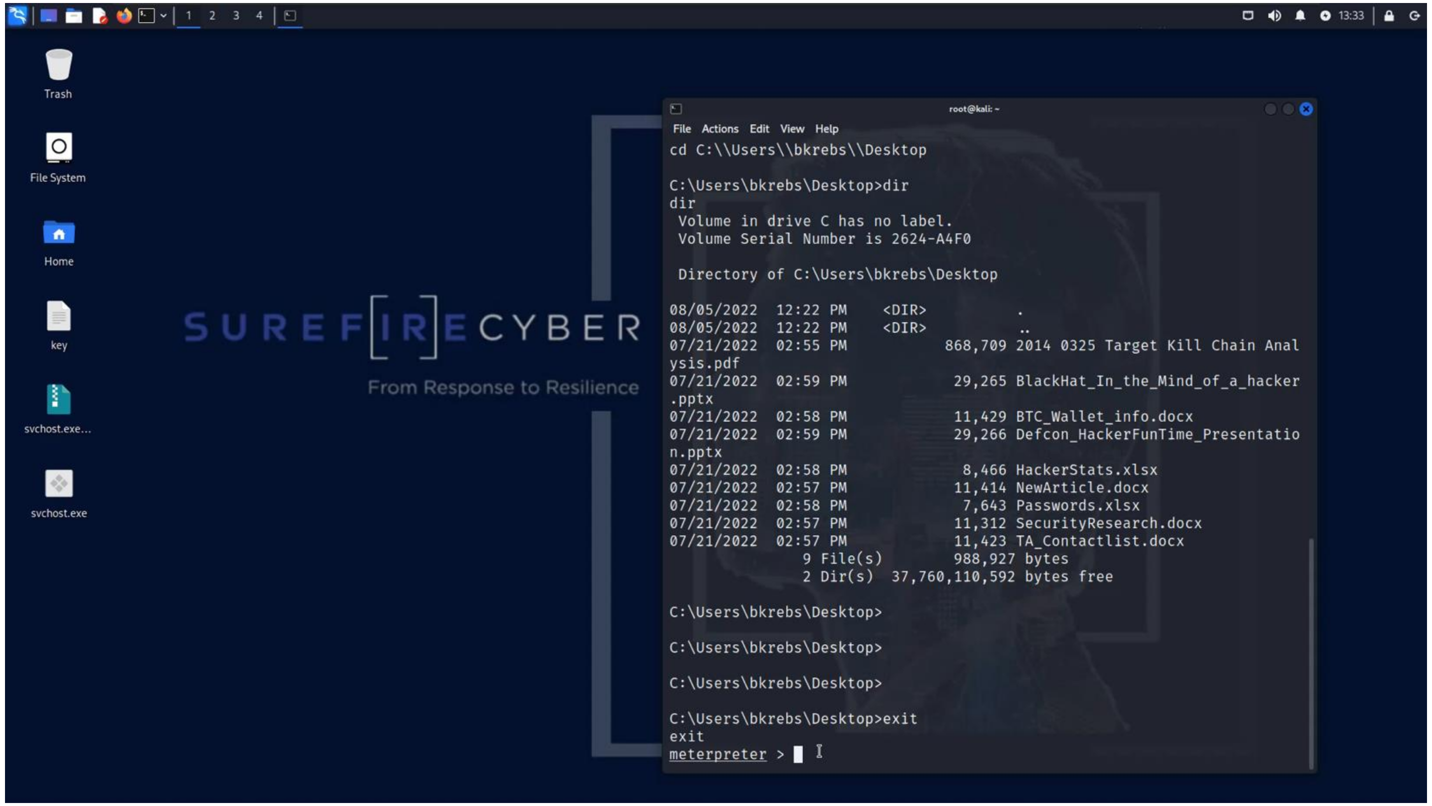
Getting More Access

Setting the Scene

- The threat actor’s goal is to move from a normal user account to the network administrator’s account
- Threat actor gains elevated permissions using a common tool called Mimikatz

Takeaways

- Minimize privileged accounts and administrative access
- Invest in tools that detect and stop malicious actions
- Keep systems up-to-date with patches



```
cd C:\\Users\\bkrebs\\Desktop

C:\Users\bkrebs\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 2624-A4F0

 Directory of C:\Users\bkrebs\Desktop

08/05/2022  12:22 PM    <DIR>          .
08/05/2022  12:22 PM    <DIR>          ..
07/21/2022  02:55 PM           868,709 2014 0325 Target Kill Chain Anal
ysis.pdf
07/21/2022  02:59 PM            29,265 BlackHat_In_the_Mind_of_a_hacker
.pptx
07/21/2022  02:58 PM            11,429 BTC_Wallet_info.docx
07/21/2022  02:59 PM            29,266 Defcon_HackerFunTime_Presentatio
n.pptx
07/21/2022  02:58 PM             8,466 HackerStats.xlsx
07/21/2022  02:57 PM            11,414 NewArticle.docx
07/21/2022  02:58 PM             7,643 Passwords.xlsx
07/21/2022  02:57 PM            11,312 SecurityResearch.docx
07/21/2022  02:57 PM            11,423 TA_Contactlist.docx
               9 File(s)        988,927 bytes
               2 Dir(s)  37,760,110,592 bytes free

C:\Users\bkrebs\Desktop>

C:\Users\bkrebs\Desktop>

C:\Users\bkrebs\Desktop>

C:\Users\bkrebs\Desktop>exit
exit
meterpreter > 
```

Stage 4 Lateral Movement

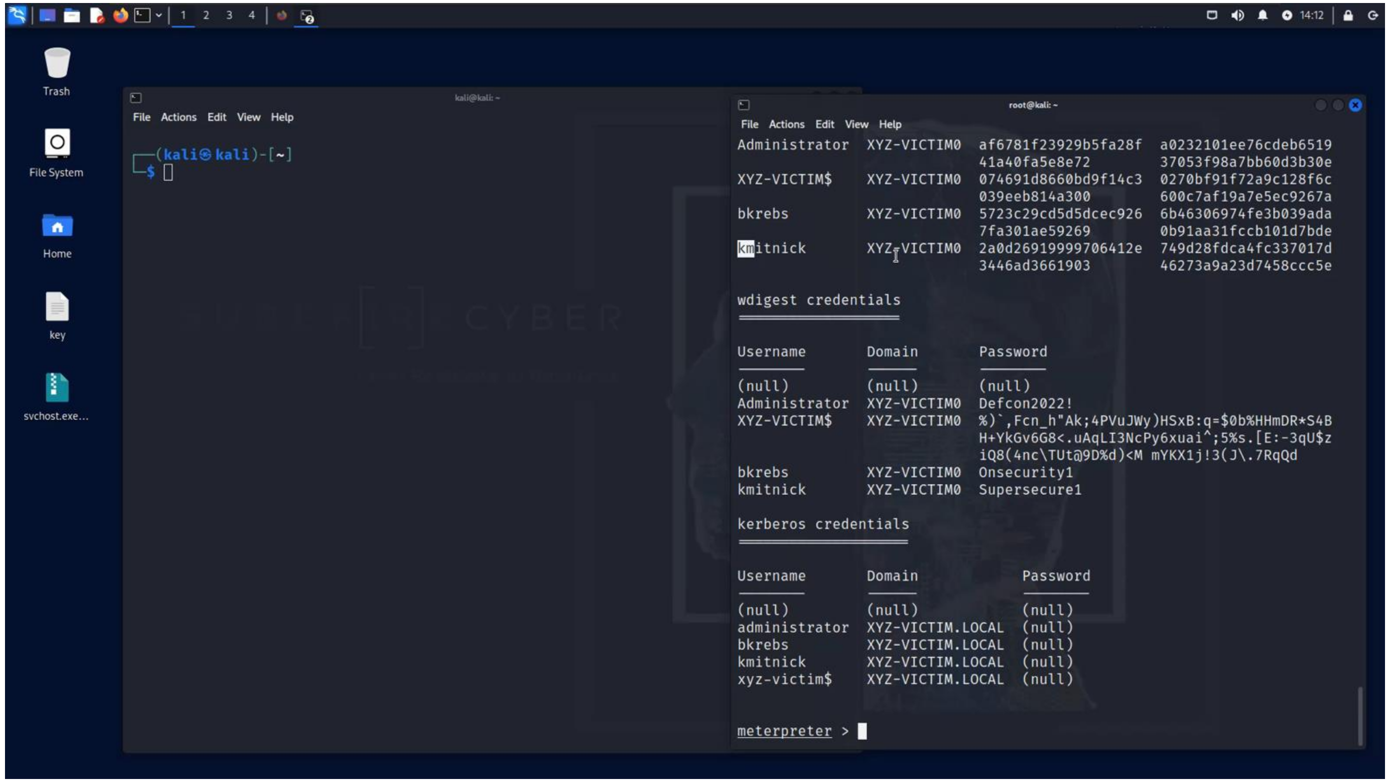
Moving Around

Setting the Scene

- Threat actor cracks the password and uses the administrator's credentials to login
- In the middle of the night, the threat actor accesses the server with everyone's passwords

Takeaways

- Use strong and long passwords
- Network tools detect internal scans and malicious activity, so you stop a hacker in their tracks



```
┌──(kali㉿kali)-[~]
└─$ 
```

```
Administrator  XYZ-VICTIM0  af6781f23929b5fa28f  a0232101ee76cdeb6519
                            41a40fa5e8e72        37053f98a7bb60d3b30e
XYZ-VICTIM$    XYZ-VICTIM0  074691d8660bd9f14c3  0270bf91f72a9c128f6c
                            039eeb814a300        600c7af19a7e5ec9267a
bkrebs         XYZ-VICTIM0  5723c29cd5d5dcec926  6b46306974fe3b039ada
                            7fa301ae59269        0b91aa31fccb101d7bde
kmitnick       XYZ-VICTIM0  2a0d26919999706412e  749d28fdca4fc337017d
                            3446ad3661903        46273a9a23d7458ccc5e

wdigest credentials
===================

Username       Domain       Password
--------       ------       --------
(null)         (null)       (null)
Administrator  XYZ-VICTIM0  Defcon2022!
XYZ-VICTIM$    XYZ-VICTIM0  %)`,Fcn_h"Ak;4PVuJWy)HSxB:q=$0b%HHmDR*S4B
                            H+YkGv6G8<.uAqLI3NcPy6xuai^;5%s.[E:-3qU$z
                            iQ8(4nc\TUt@9D%d)<M mYKX1j!3(J\.7RqQd
bkrebs         XYZ-VICTIM0  Onsecurity1
kmitnick       XYZ-VICTIM0  Supersecure1

kerberos credentials
====================

Username       Domain             Password
--------       ------             --------
(null)         (null)             (null)
administrator  XYZ-VICTIM.LOCAL   (null)
bkrebs         XYZ-VICTIM.LOCAL   (null)
kmitnick       XYZ-VICTIM.LOCAL   (null)
xyz-victim$    XYZ-VICTIM.LOCAL   (null)


meterpreter > 
```

Stage 5 Exfiltration and Backup Deletion

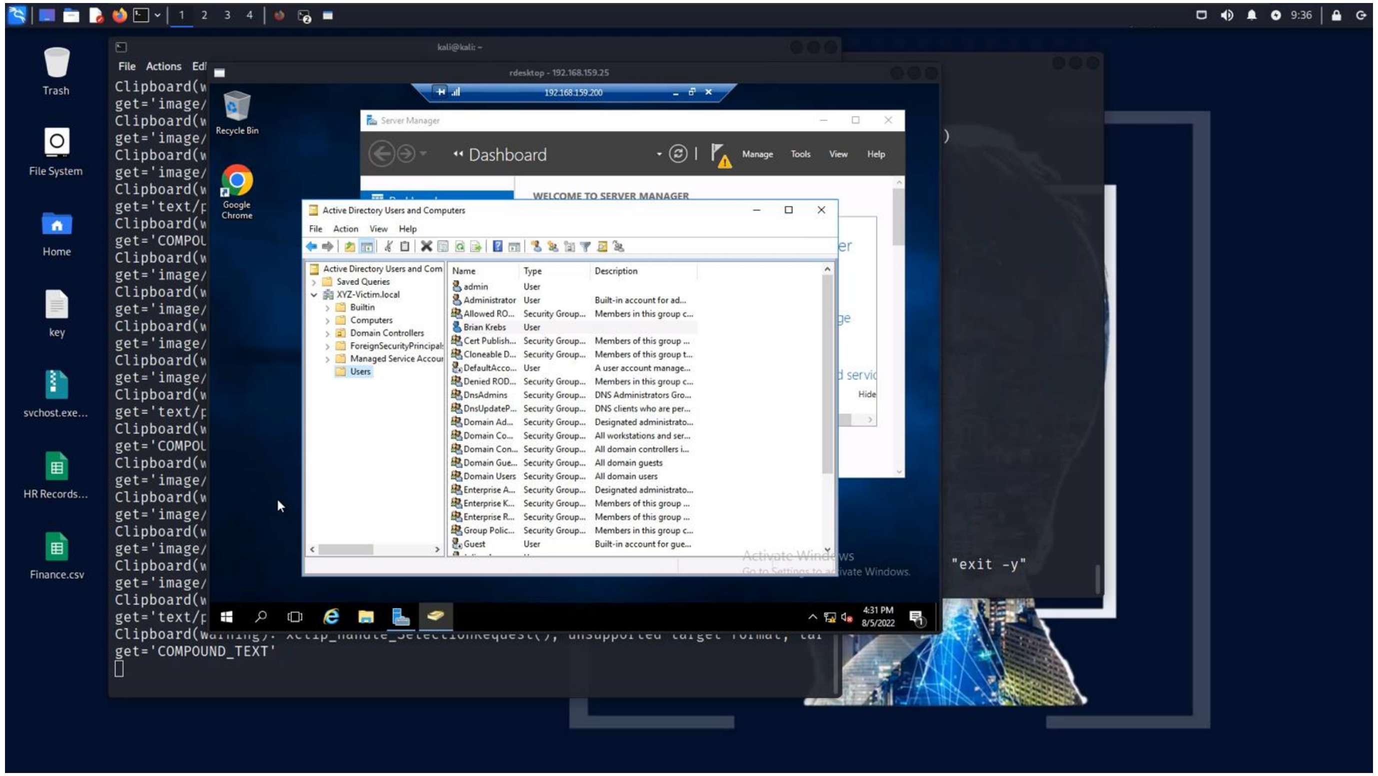
Stealing Data

Setting the Scene

- Threat actor will look for sensitive files and steal them
- Threat actor will then delete any backups they discover
- Data could be uploaded to the dark web or sold

Takeaways

- Unauthorized access to personal information can trigger legal obligations (even if files weren't taken)
- Use a strong backup solution and test it often



```
Clipboard(w
get='image/
Clipboard(w
get='image/
Clipboard(w
get='image/
Clipboard(w
get='text/p
Clipboard(w
get='COMPOU
Clipboard(w
get='image/
Clipboard(w
get='image/
Clipboard(w
get='image/
Clipboard(w
get='image/
Clipboard(w
get='text/p
Clipboard(w
get='COMPOU
Clipboard(w
get='image/
Clipboard(w
get='image/
Clipboard(w
get='image/
Clipboard(w
get='image/
Clipboard(w
get='text/p
Clipboard(warning): xclip_handle_SelectionRequest(), unsupported target format, tar
get='COMPOUND_TEXT'
```

Name	Type	Description
admin	User	
Administrator	User	Built-in account for ad...
Allowed RO...	Security Group...	Members in this group c...
Brian Krebs	User	
Cert Publish...	Security Group...	Members of this group ...
Cloneable D...	Security Group...	Members of this group t...
DefaultAcco...	User	A user account manage...
Denied ROD...	Security Group...	Members in this group c...
DnsAdmins	Security Group...	DNS Administrators Gro...
DnsUpdateP...	Security Group...	DNS clients who are per...
Domain Ad...	Security Group...	Designated administrato...
Domain Co...	Security Group...	All workstations and ser...
Domain Con...	Security Group...	All domain controllers i...
Domain Gue...	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
Enterprise A...	Security Group...	Designated administrato...
Enterprise K...	Security Group...	Members of this group ...
Enterprise R...	Security Group...	Members of this group ...
Group Polic...	Security Group...	Members in this group c...
Guest	User	Built-in account for gue...

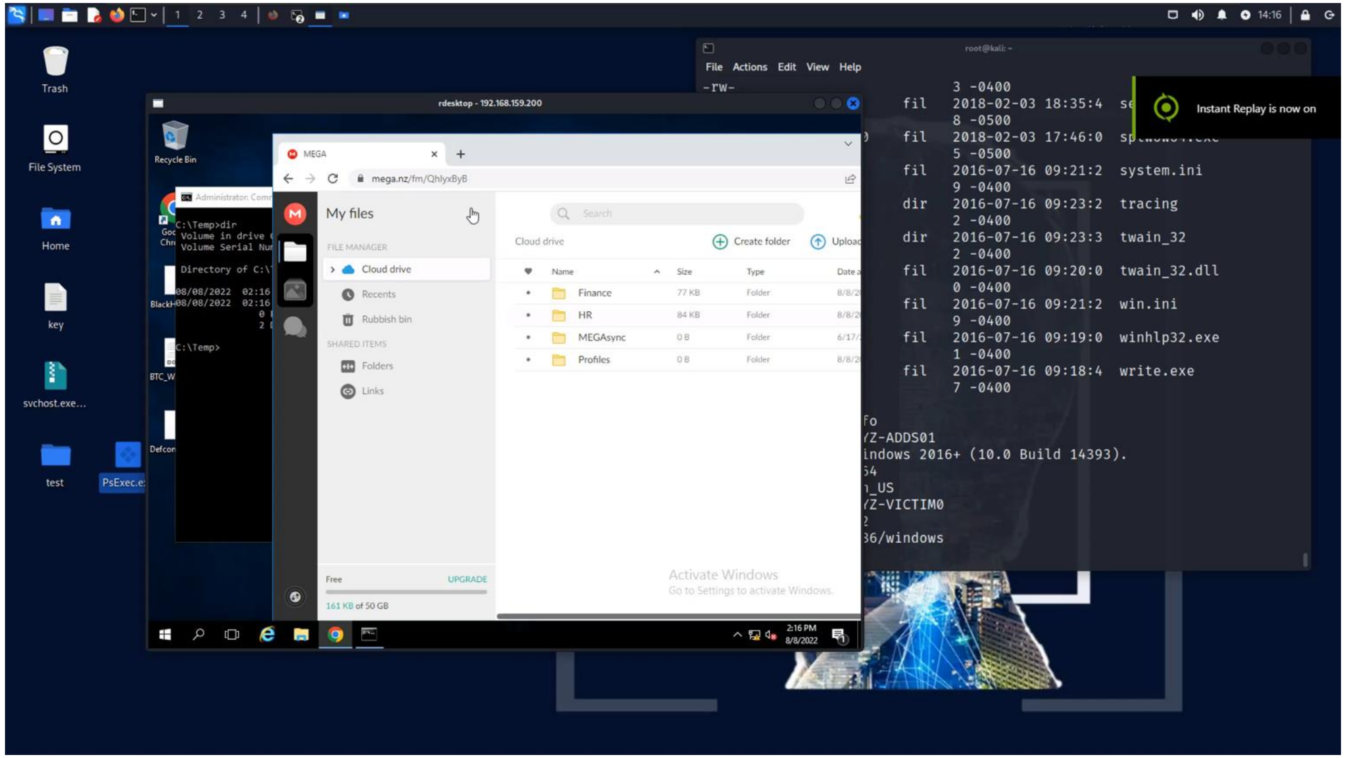
Stage 6 Ransomware Execution

Setting the Scene

- Threat actor executes the ransomware as quickly as possible on as many systems as possible
- This is often done on a Friday night or Thanksgiving morning

Takeaways

- Disconnect, don’t power off, encrypted systems to preserve evidence
- Have a plan for how you are going to access resources to help you through this



```
C:\Temp>dir
 Volume in drive
 Volume Serial Nu

 Directory of C:\

08/08/2022  02:16
08/08/2022  02:16
               0
               2

C:\Temp>
```

	Name	Size	Type	Date a
•	Finance	77 KB	Folder	8/8/2
•	HR	84 KB	Folder	8/8/2
•	MEGAsync	0 B	Folder	6/17/
•	Profiles	0 B	Folder	8/8/2

```
-rw-
                3 -0400
      fil   2018-02-03 18:35:4  se
            8 -0500
)     fil   2018-02-03 17:46:0  sp
            5 -0500
      fil   2016-07-16 09:21:2  system.ini
            9 -0400
      dir   2016-07-16 09:23:2  tracing
            2 -0400
      dir   2016-07-16 09:23:3  twain_32
            2 -0400
      fil   2016-07-16 09:20:0  twain_32.dll
            0 -0400
      fil   2016-07-16 09:21:2  win.ini
            9 -0400
      fil   2016-07-16 09:19:0  winhlp32.exe
            1 -0400
      fil   2016-07-16 09:18:4  write.exe
            7 -0400

fo
/Z-ADDS01
indows 2016+ (10.0 Build 14393).
54
1_US
/Z-VICTIM0
2
36/windows
```

Ransomware Response Framework

Intake & Scoping

- 24/7 availability
- Kick-off call to advise on immediate actions
- Structured approach outlining our services

Containment, Monitoring & Control

- Deploy security tools
- Monitor endpoints and isolate malicious activity
- Secure environment
- Apply cyber intelligence

Forensic Analysis

- Ingestion of forensic artifacts
- Analysis of forensic evidence
- Forensic investigation report

Negotiation & Recovery

- Develop a negotiation strategy
- Conduct threat actor communications
- Facilitate payment
- Restore data from back-ups or decryptor

Remediation

- Rebuild systems and restore services
- Strengthen security posture

Contact Us

SUREF[IR]E CYBER

Billy Gouveia
CEO
billy@surefirecyber.com
+1 301 938 1542

response@surefirecyber.com
1-800-270-9034

This document (including any attachments) may contain privileged, confidential, or protected information intended only for the intended recipient. If you are not the intended recipient, any unauthorized review, use, disclosure, or distribution is prohibited. If you have received this document in error, you are required to notify the sender, then delete this document and any attachment from your computer and any of your electronic devices where the document is stored.