1STRESPONDER

CYBERSECURITY & DIGITAL FORENSICS

CYBERSECURITY & RANSOMWARE

WITH RICOH DANIELSON

May 3, 2022

THE RISE OF RANSOMWARE

WHY ARE WE HERE?

THE TARGET

THE REALITY

An **82%** Increase in Ransomware-Related Data Leaks

As of 2021, there are **21** newly named adversaries

62% of Attacks are Malware-Free "Living-Off-The-Land"

Financial firms have an incentive to pay ransoms

74% of financial firms reported one or more attacks in 2021.

WHAT ARE WE UP AGAINST?

With the drastic change to the cybersecurity landscape, including the ever-increasing adversaries we are up against, expect to see a 136% increase in cyberattacks on businesses directly and indirectly. These types of attacks may be comprised of the following:

1. Industry Based Collaboration
2. Nation State Attacks
3. Disinformation Campaigns

Industry Based Threat Actors
There will be an increase of adversaries cross collaborating with each other.

Nation State Threat Actors
There will be an increase of Nation State sponsored attacks.

Disformation Threat Actors
There will be an increase of disinformation as a service.

LET'S MEET SOME ADVERSARIES...

CARBON SPIDER

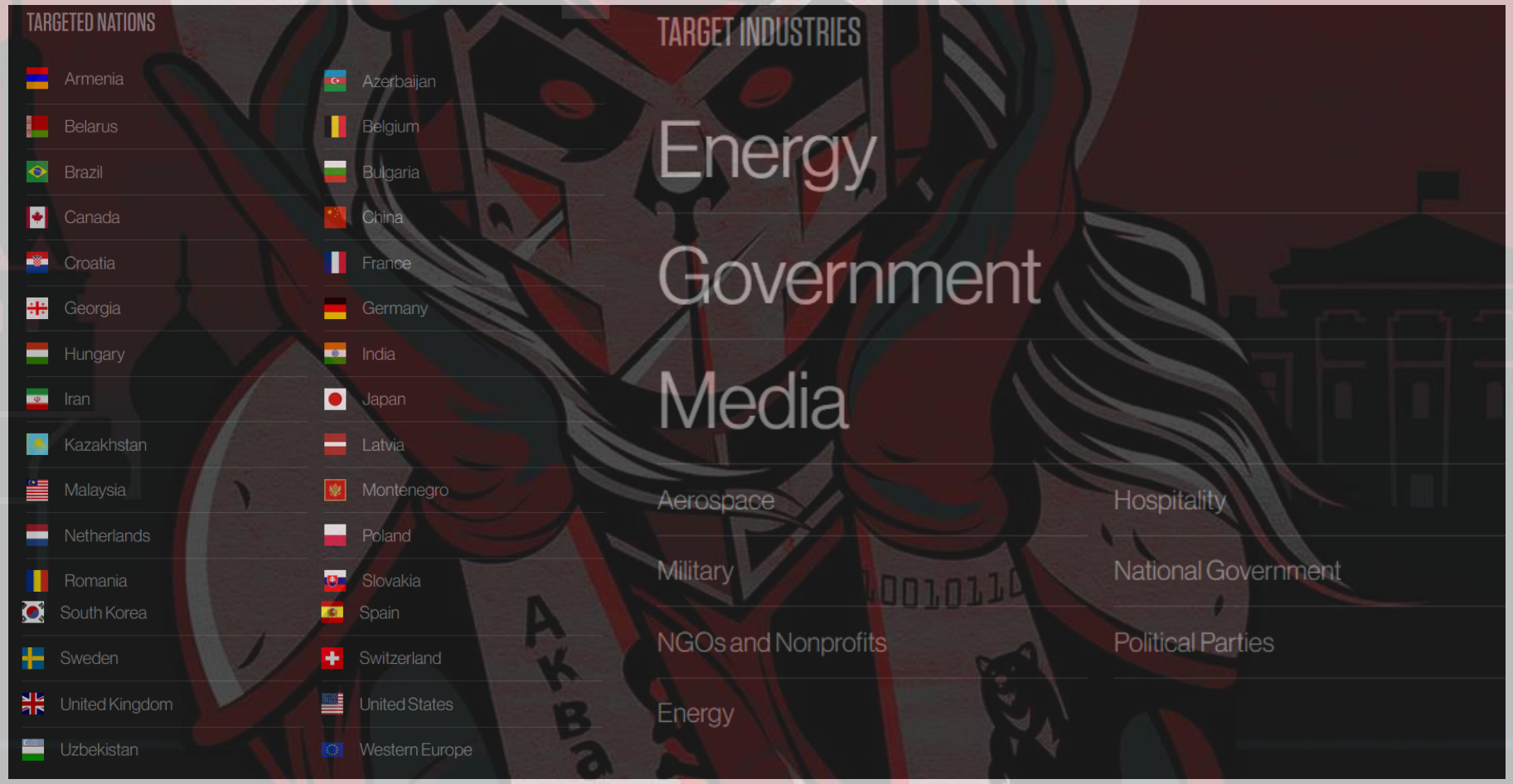
TARGETED NATIONS

- Bulgaria
- Czech Republic
- France
- Germany
- Ireland
- Kuwait
- Lebanon
- Norway
- Poland
- Romania
- Russian Federation
- Spain
- United Arab Emirates
- United Kingdom
- United States
- Yemen

TARGET INDUSTRIES

- Financial Services
- Government
- Healthcare
- Manufacturing
- Media
- Retail
- Technology

FANCY BEAR



WICKED PANDA

TARGETED NATIONS

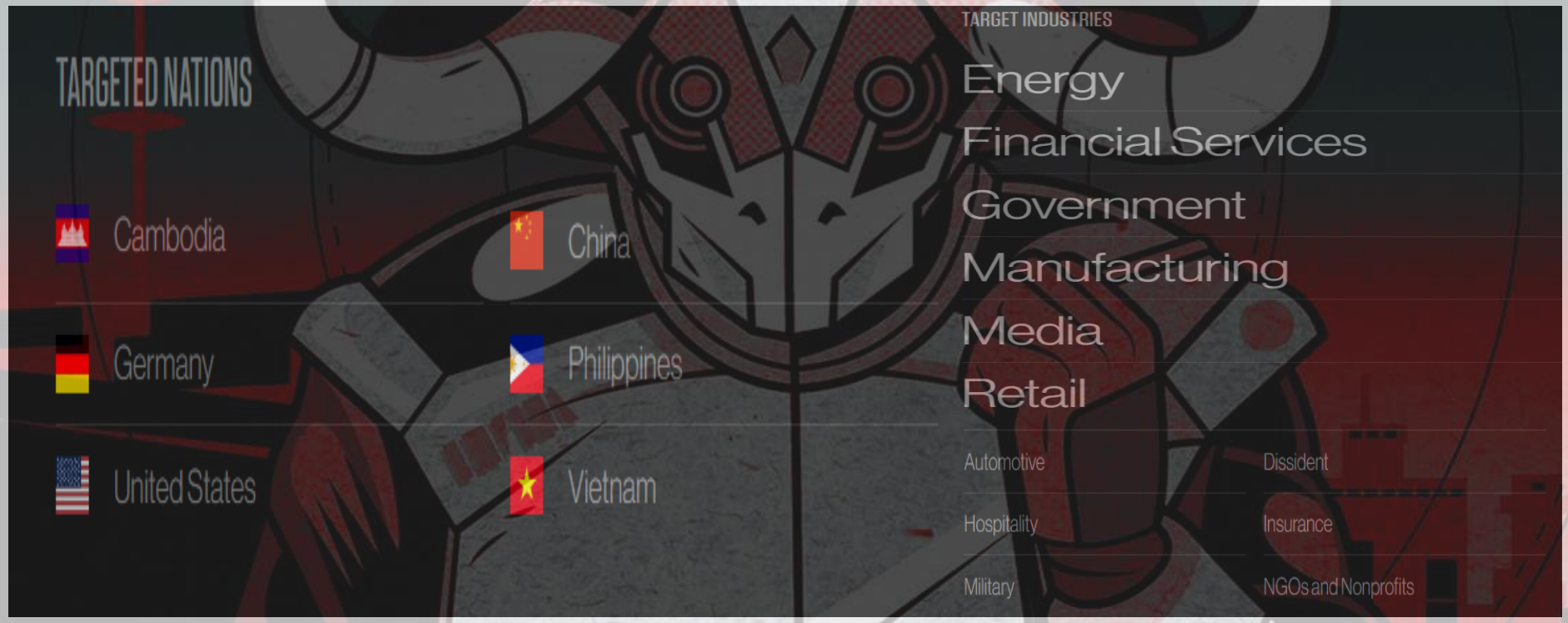
- Germany
- India
- South Korea
- United States
- Hong Kong
- Japan
- Taiwan

TARGET INDUSTRIES

- Academic
- Manufacturing
- Telecommunications
- Technology

VENOMOUS BEAR

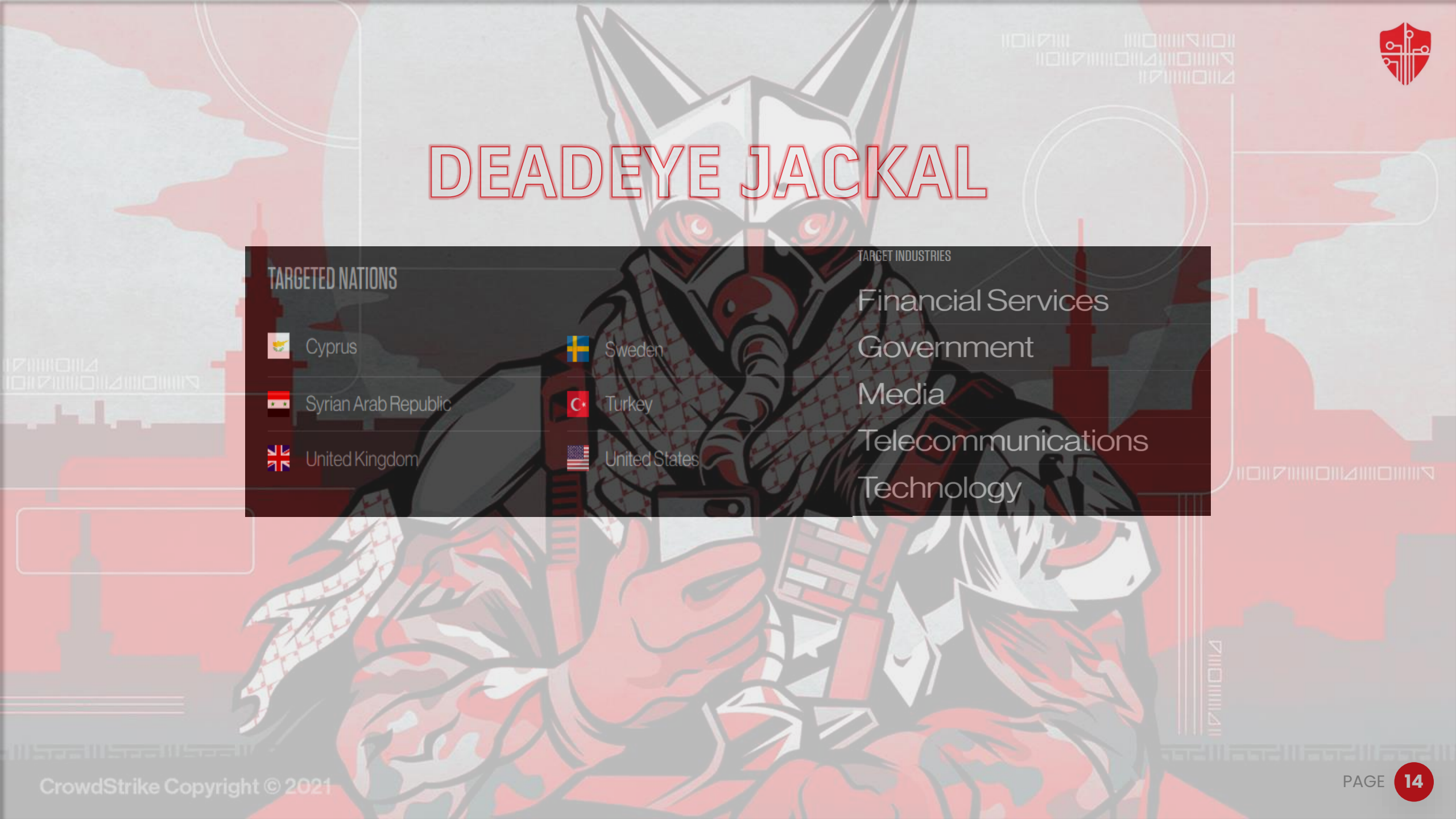
OCEAN BUFFALO



STARDUST CHOLLIMA

COLBALT SPIDER

DEADEYE JACKAL



TARGETED NATIONS

- Cyprus
- Sweden
- Syrian Arab Republic
- Turkey
- United Kingdom
- United States

TARGET INDUSTRIES

- Financial Services
- Government
- Media
- Telecommunications
- Technology

REMIX KITTEN

TARGETED NATIONS

- Canada
- Iran
- Israel
- Jordan
- Kuwait
- Saudi Arabia
- Turkey
- United Arab Emirates

TARGET INDUSTRIES

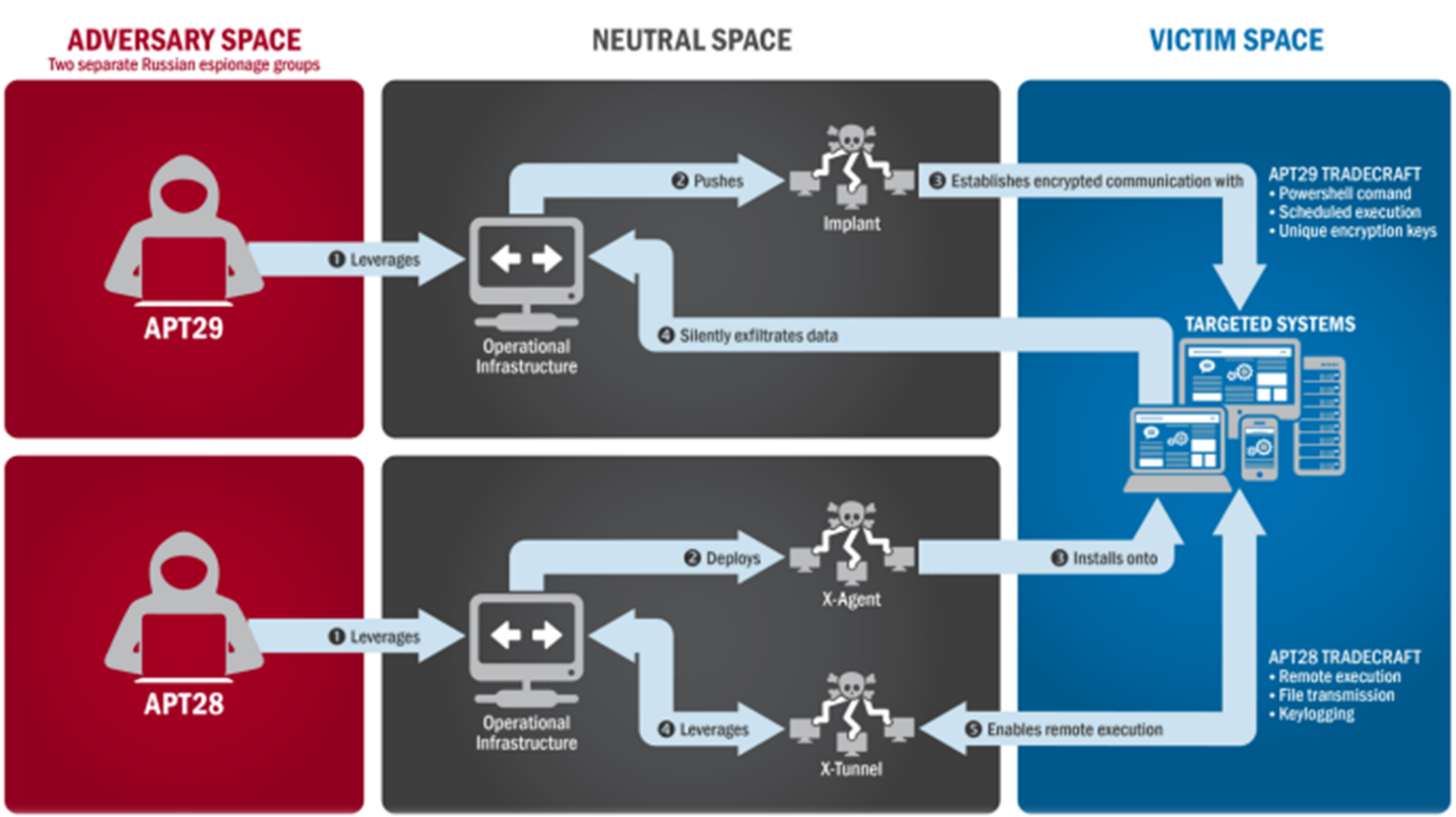
Aviation

Telecommunications

Technology

Hospitality

Travel


ADVERSARY SPACE
Two separate Russian espionage groups
NEUTRAL SPACE
VICTIM SPACE
APT29
1 Leverages
Operational Infrastructure
2 Pushes
Implant
3 Establishes encrypted communication with
APT29 TRADECRAFT
• Powershell comand
• Scheduled execution
• Unique encryption keys
4 Silently exfiltrates data
TARGETED SYSTEMS
APT28
1 Leverages
Operational Infrastructure
2 Deploys
X-Agent
3 Installs onto
4 Leverages
X-Tunnel
5 Enables remote execution
APT28 TRADECRAFT
• Remote execution
• File transmission
• Keylogging

CASE STUDIES

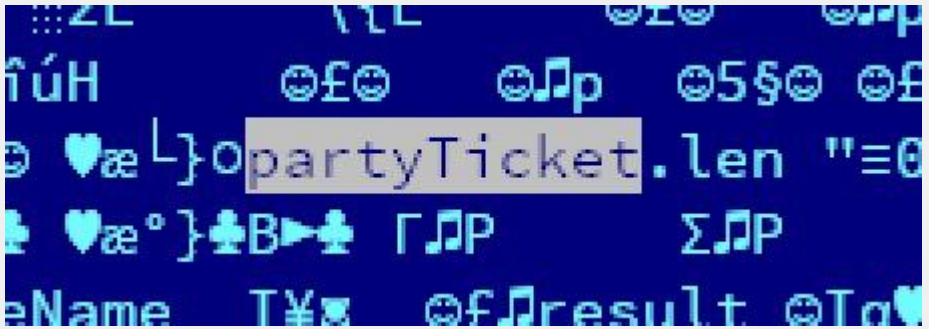
DARKSIDE & RAGNAR LOCKER

CNA FINANCIAL & INSURANCE FIRM

BLOCK FINANCIAL SERVICES

TACTICS, TECHNIQUES, & PROCEDURES

```
_/C_/projects/403forBiden/wHiteHousE.baggageGatherings
_/C_/projects/403forBiden/wHiteHousE.lookUp
_/C_/projects/403forBiden/wHiteHousE.primaryElectionProcess
_/C_/projects/403forBiden/wHiteHousE.GoodOffice1
_/C_/projects/403forBiden/wHiteHousE.init
C:/projects/403forBiden/main.go
C:/projects/403forBiden/wHiteHousE/wHiteHousE.go
```



Signature Verification

Signed file, valid signature

File Version Information

Signers

– Hermetica Digital Ltd

Name	Hermetica Digital Ltd
Status	Valid
Issuer	DigiCert EV Code Signing CA (SHA2)
Valid From	12:00 AM 04/13/2021
Valid To	11:59 PM 04/14/2022
Valid Usage	Code Signing
Algorithm	sha256RSA
Thumbprint	1AE7556DFACD47D9EFBE79BE974661A5A6D6D923
Serial Number	0C 48 73 28 73 AC 8C CE BA F8 F0 E1 E8 32 9C EC

"The only thing that we learn from new elections is we learned nothing from the old!"

Thank you for your vote! All your files, documents, photoes, videos, databases etc. have been successfully encrypted!

Now your computer has a special ID: [redacted]**d1e**

Do not try to decrypt then by yourself - it's impossible!

It's just a business and we care only about getting benefits. The only way to get your files back is to contact us and get further instuctions.

To prove that we have a decryptor send us any encrypted file (less than 650 kbytes) and we'll send you it back being decrypted. This is our guarantee.

NOTE: *Do not send file with sensitive content. In the email write us your computer's special ID (mentioned above).*

So if you want to get your files back contact us:

1) vote[redacted]@protonmail.com

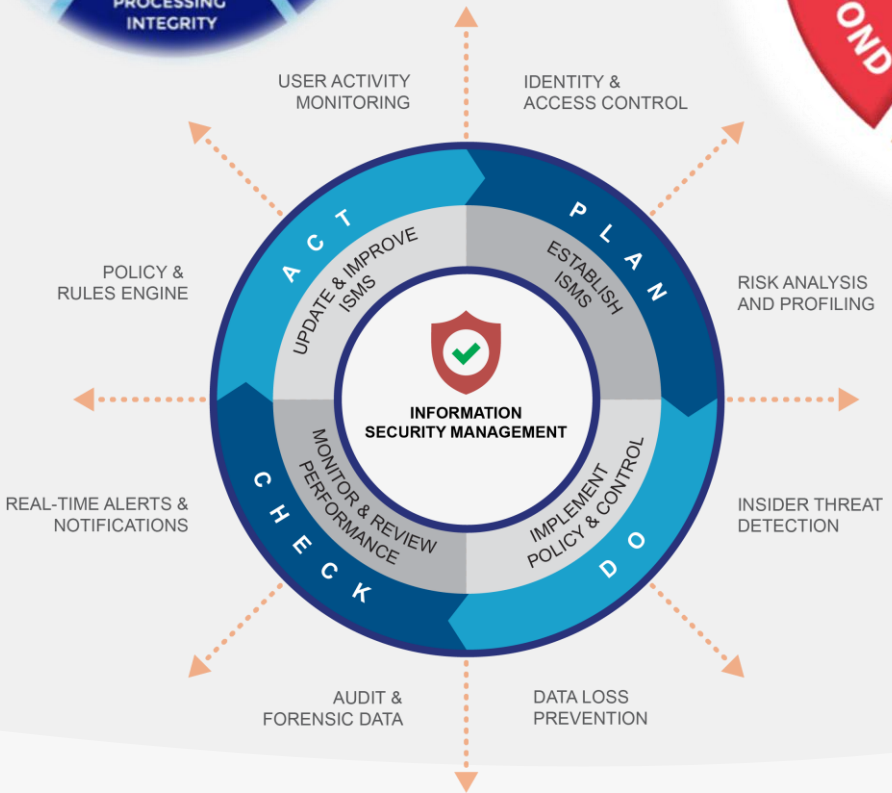
2) st[redacted]2024@protonmail.com - if we dont't answer you during 3 days

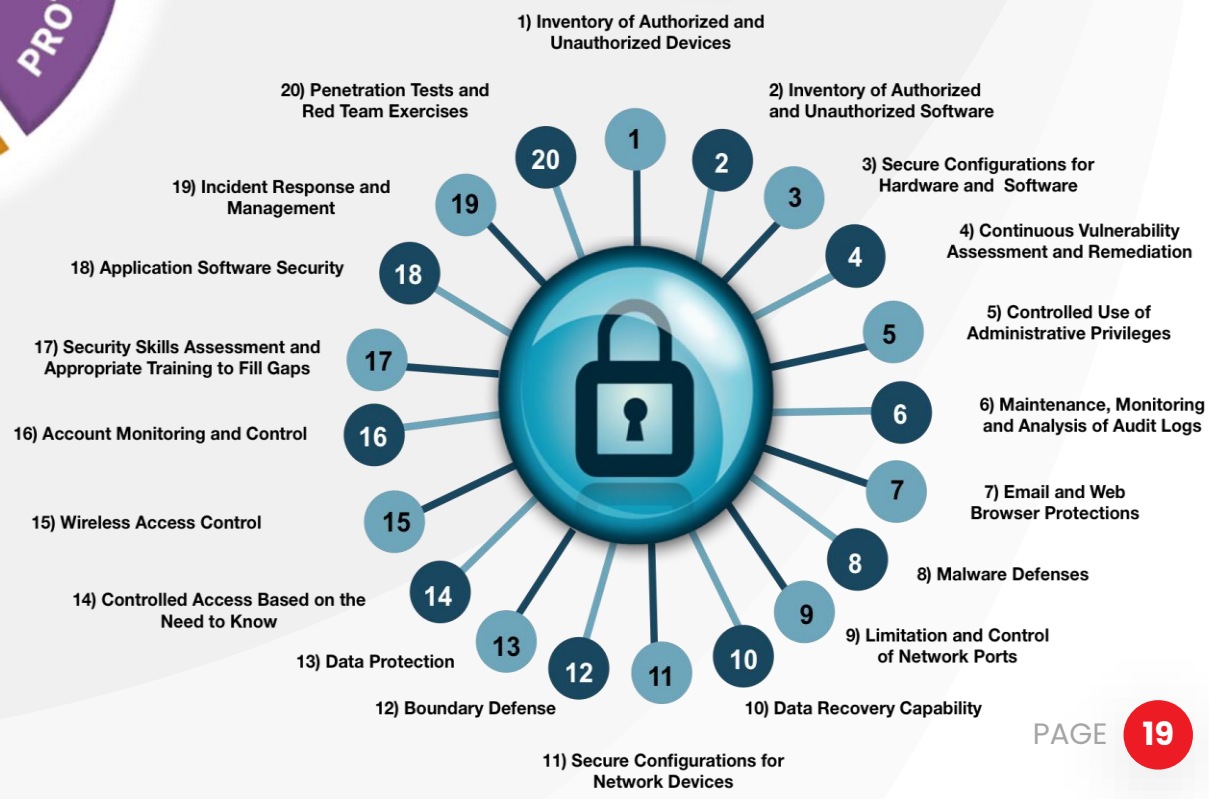
Have a nice day!

HERMETICWIPER

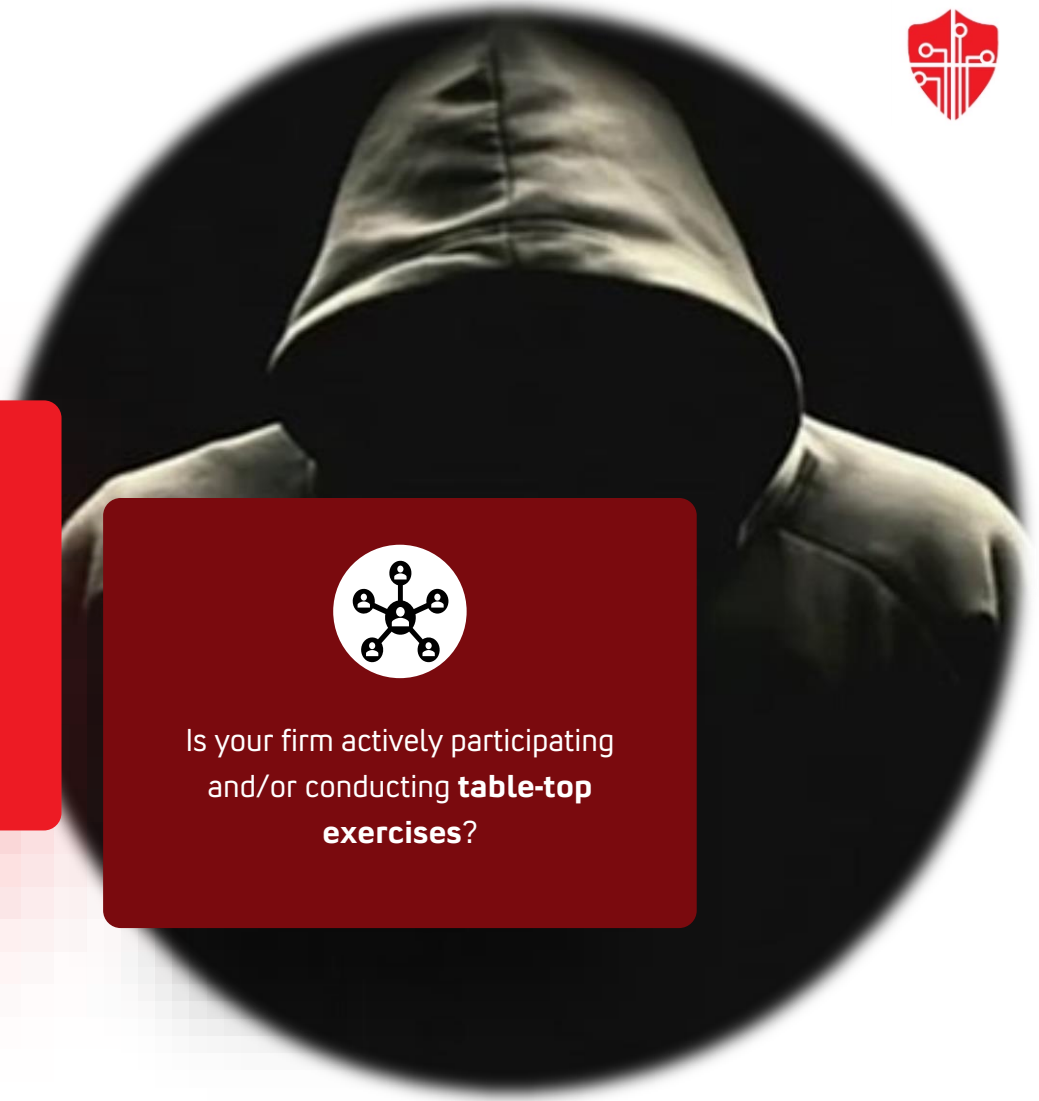
A 2022 SCENARIO THAT BROUGHT UPON A NEW RANSOMWARE

CYBER RISK FRAMEWORKS





ARE YOU PREPARED?



Do you have an **incident response plan (IRP)** in place?

When was the last time your firm **tested and reviewed your IRP**? Was it in the past 6-months?

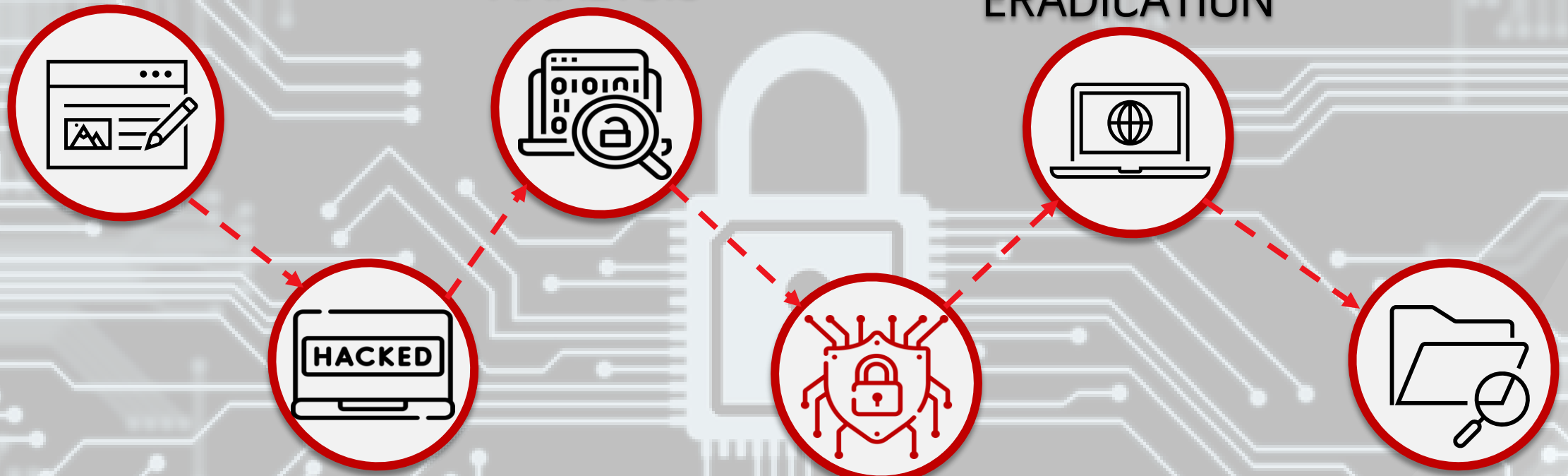
Is your firm actively participating and/or conducting **table-top exercises**?

THE SIX STEPS OF INCIDENT RESPONSE

PREPARATION

ANALYSIS

ERADICATION



DETECTION

CONTAINMENT

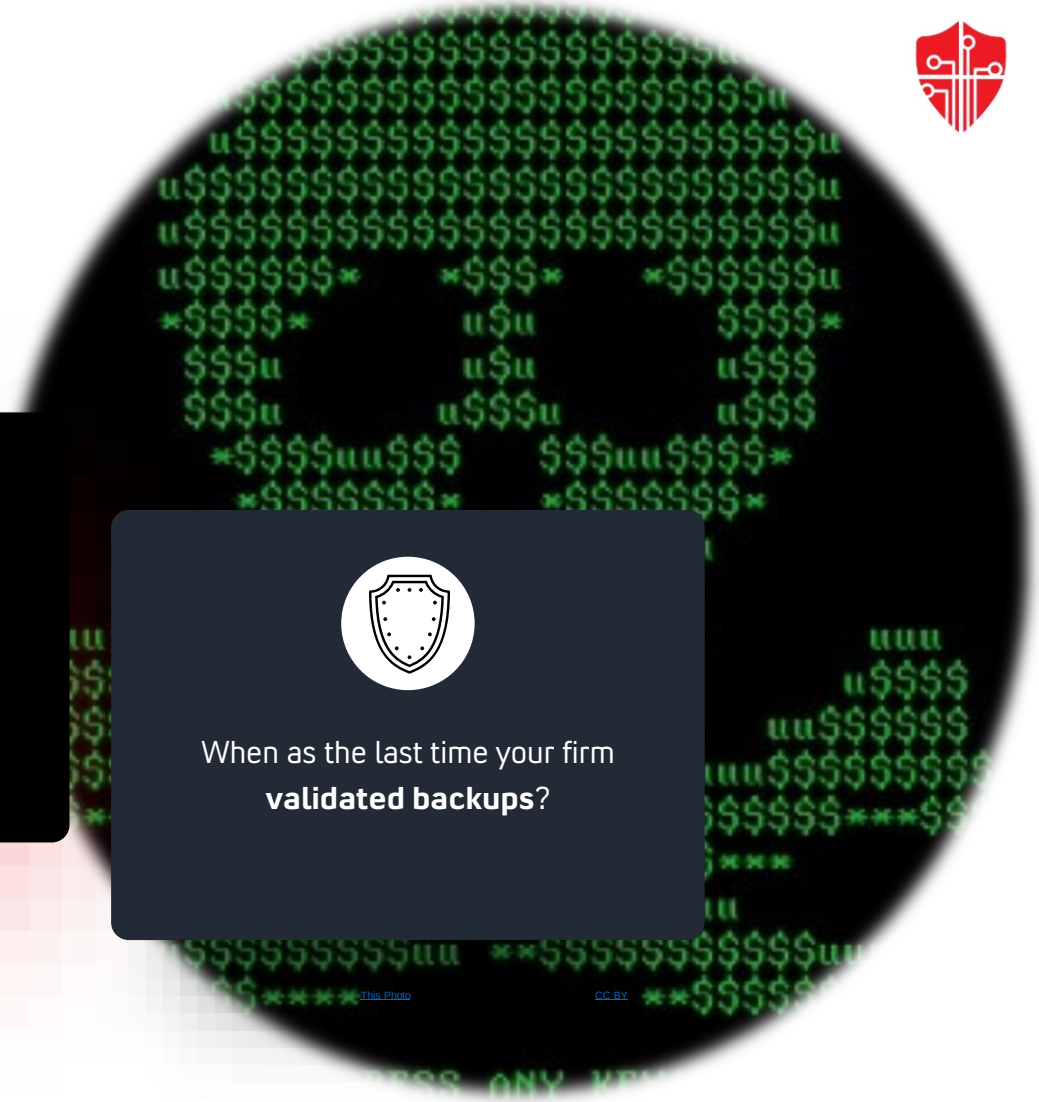
RECOVERY

CAN YOU RESPOND?

Can your firm **handle a cyberattack**? Can it **handle ransomware and a ransom**?

When was the last time your firm **tested and reviewed your BCP/DRP**?

When as the last time your firm **validated backups**?

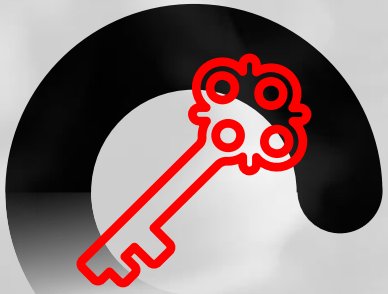


WHAT IS THE PROCESS TO RESPOND TO RANSOMWARE?

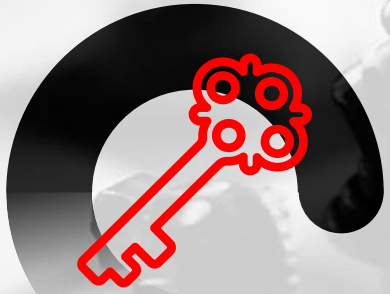

LAND
AIR
SEA


RANSOMWARE

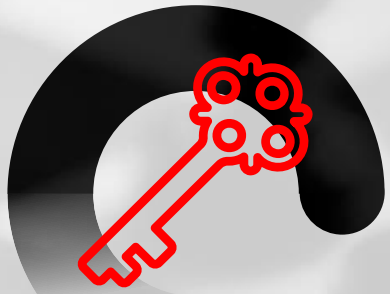
THE THREE KEYS TO RECOVERY



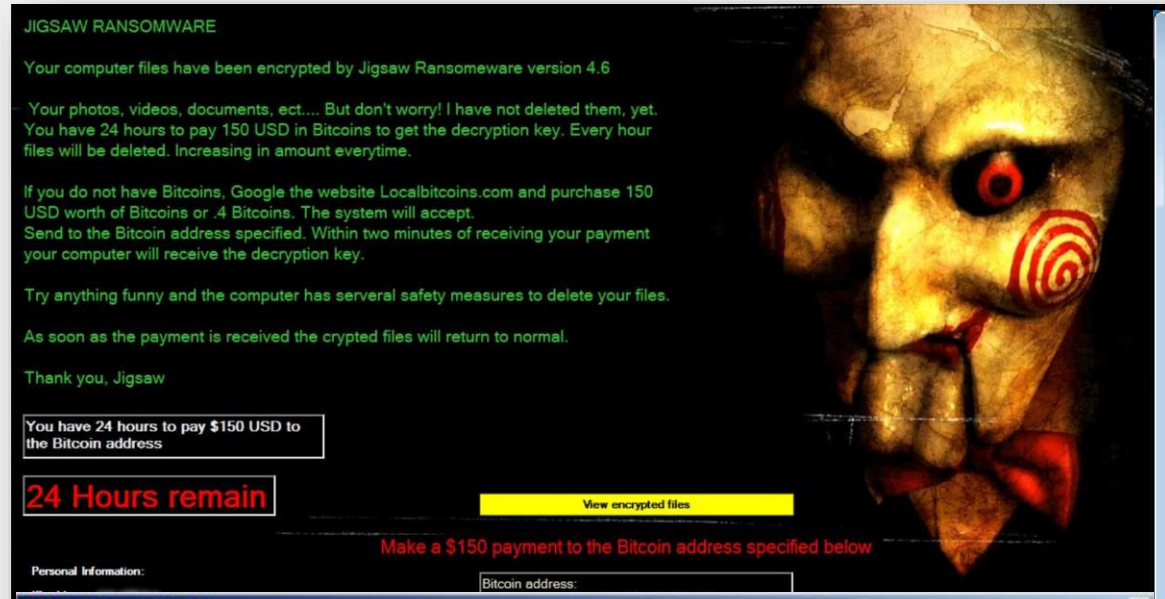
TEST
&
VALIDATE



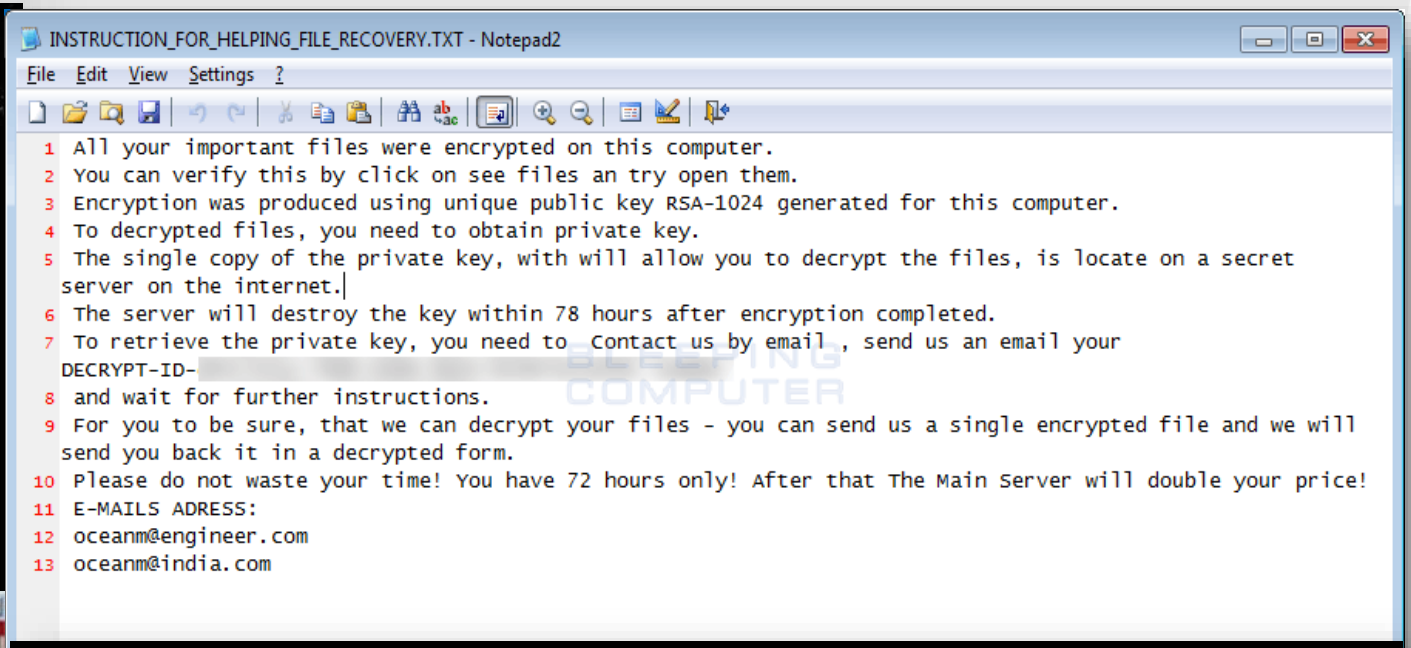
OFFENSIVE
&
DEFENSIVE

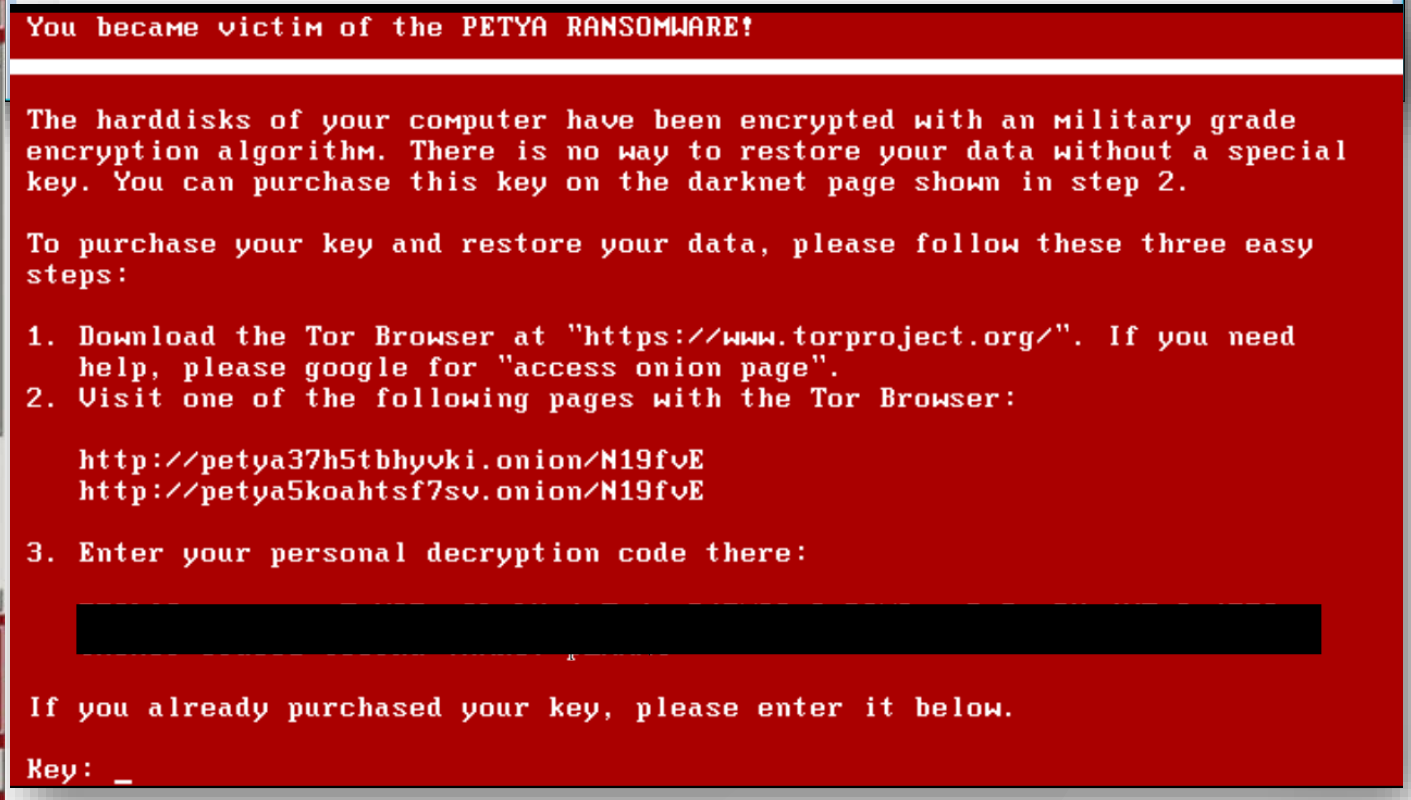


RESPOND
&
CONTROL


JIGSAW RANSOMWARE
Your computer files have been encrypted by Jigsaw Ransomeware version 4.6
Your photos, videos, documents, ect.... But don't worry! I have not deleted them, yet.
You have 24 hours to pay 150 USD in Bitcoins to get the decryption key. Every hour files will be deleted. Increasing in amount everytime.
If you do not have Bitcoins, Google the website Localbitcoins.com and purchase 150 USD worth of Bitcoins or .4 Bitcoins. The system will accept.
Send to the Bitcoin address specified. Within two minutes of receiving your payment your computer will receive the decryption key.
Try anything funny and the computer has serveral safety measures to delete your files.
As soon as the payment is received the crypted files will return to normal.
Thank you, Jigsaw
You have 24 hours to pay $150 USD to the Bitcoin address
24 Hours remain
View encrypted files
Make a $150 payment to the Bitcoin address specified below
Personal Information:
Bitcoin address:


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
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
Payment will be raised on
5/15/2017 15:58:08
Time Left
02:23:58:59
Your files will be lost on
5/19/2017 15:58:08
Time Left
06:23:58:59
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin ACCEPTED HERE
Send $300 worth of bitcoin to this address:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
Copy
Check Payment
Decrypt


INSTRUCTION_FOR_HELPING_FILE_RECOVERY.TXT - Notepad2
File Edit View Settings ?
All your important files were encrypted on this computer.
You can verify this by click on see files an try open them.
Encryption was produced using unique public key RSA-1024 generated for this computer.
To decrypted files, you need to obtain private key.
The single copy of the private key, with will allow you to decrypt the files, is locate on a secret server on the internet.
The server will destroy the key within 78 hours after encryption completed.
To retrieve the private key, you need to Contact us by email , send us an email your DECRYPT-ID-
and wait for further instructions.
For you to be sure, that we can decrypt your files - you can send us a single encrypted file and we will send you back it in a decrypted form.
Please do not waste your time! You have 72 hours only! After that The Main Server will double your price!
E-MAILS ADRESS:
oceanm@engineer.com
oceanm@india.com


You became victim of the PETYA RANSOMWARE!
The harddisks of your computer have been encrypted with an military grade encryption algorithm. There is no way to restore your data without a special key. You can purchase this key on the darknet page shown in step 2.
To purchase your key and restore your data, please follow these three easy steps:
1. Download the Tor Browser at "https://www.torproject.org/". If you need help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:
http://petya37h5tbhyvki.onion/N19fvE
http://petya5koahtsf7sv.onion/N19fvE
3. Enter your personal decryption code there:
If you already purchased your key, please enter it below.
Key: _


DATA BREACH
DATA BREACH
DATA
BREACH
DATA BREACH
DATA BREACH
DATA BREACH

THANKS FOR LISTENING

Ricoh Danielson, US Army Combat Veteran and multi rotation operator.

Ricoh regularly consults on some of the most newsworthy cyber incidents.

Contact Ricoh

480-747-5970

Nashville, TN

ricohd@1stResponder.us

www.1stResponder.us

www.1stresponder.us

ticker NEWS yahoo! finance NEW YORK POST KIMKOMANDO