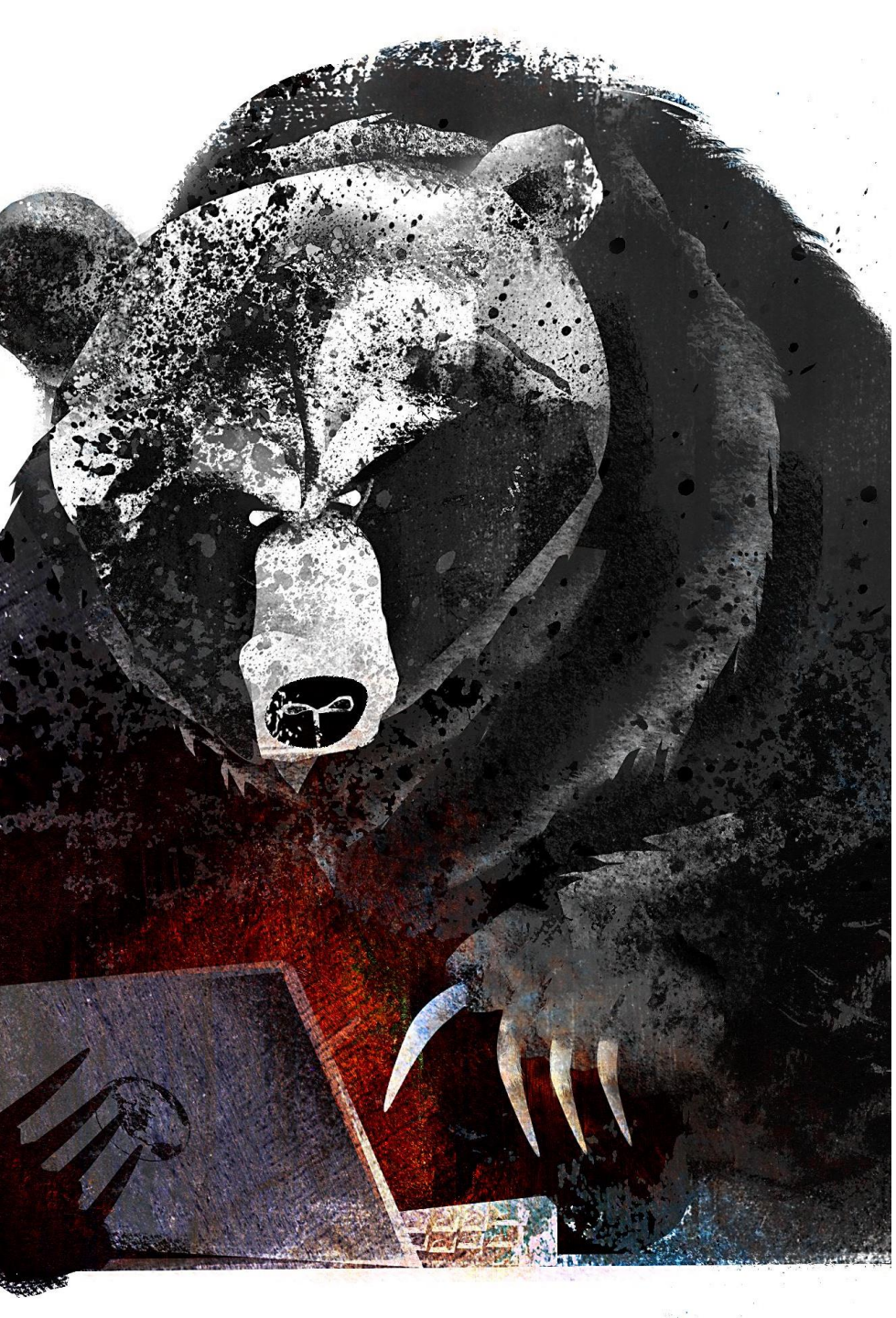
WannaCry Ransomware and its Lessons

John Ellis
Principal Consultant

ANDGIET
SECURING YOUR BUSINESS JOURNEY



Who am I?

- New Zealander
- Started my career in the military
- 23 years working on information “cyber” security
- Worked in banks, telco and hi-tech firms
- Live in Singapore and still occasionally play rugby
- Lastly, enjoy learning from everyone

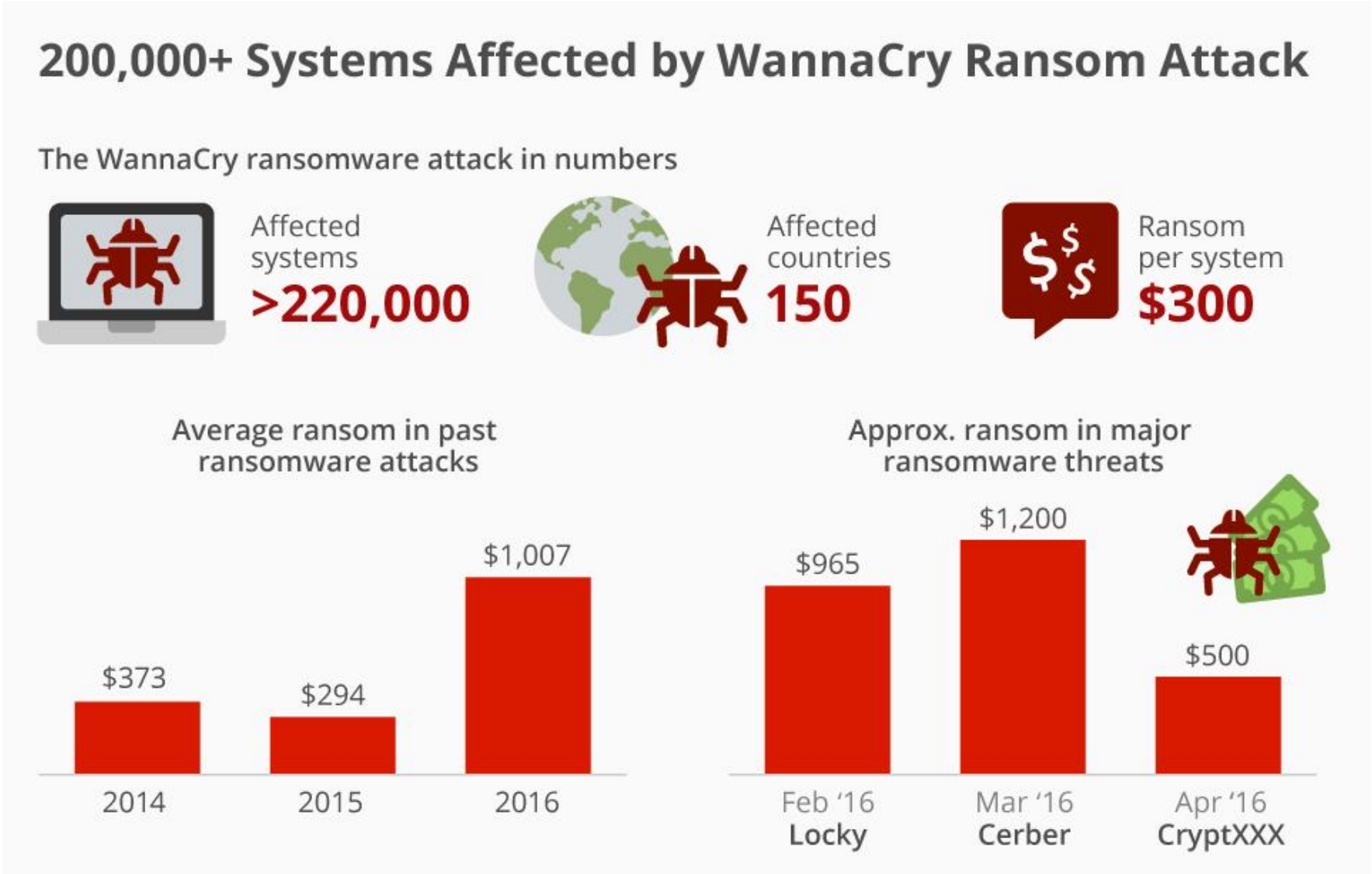
- Connect with me: https://www.linkedin.com/in/johnellis/
- Follow me: @zenofsecurity or @andgietsecurity

Today's Agenda

1. The WannaCry Ransomware Attack
2. Ransomware Trends
3. Anatomy of a Ransomware Attack
4. Combating the Ransomware Threat
5. Final Words

ANDGIET

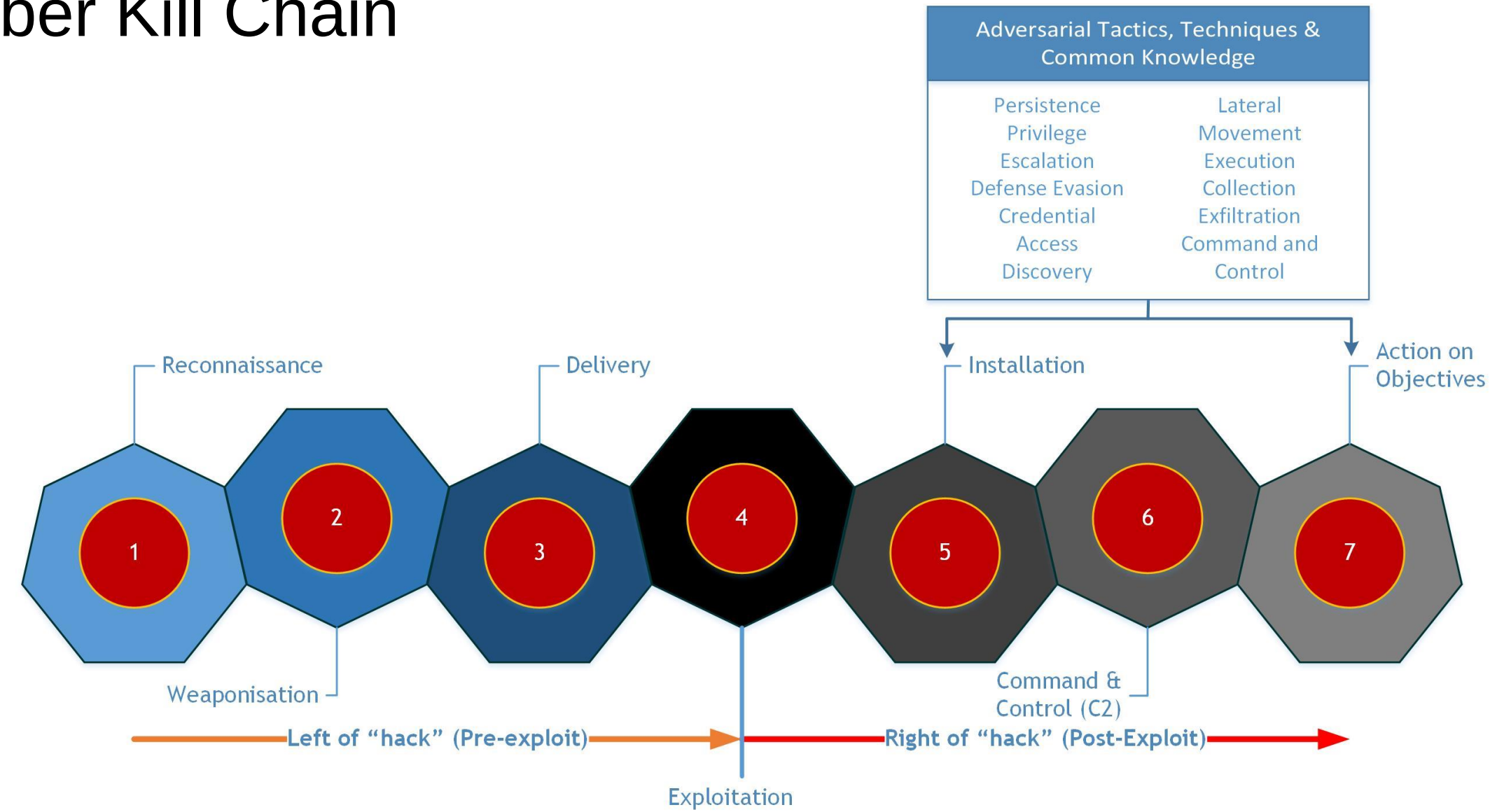
SECURING YOUR BUSINESS JOURNEY



Source: Media Reports, Symantec, infographic by statista

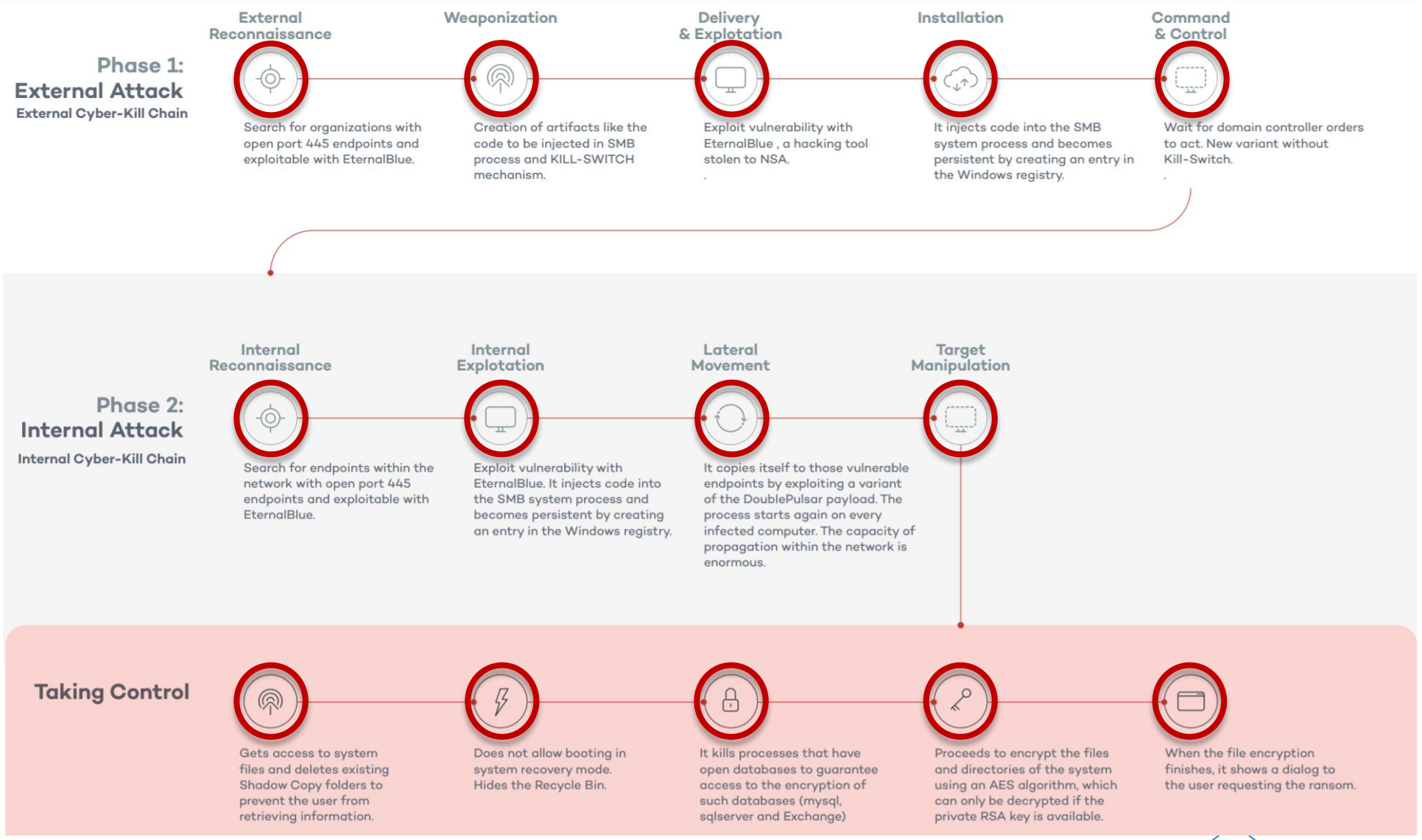
ANDGIET
SECURING YOUR BUSINESS JOURNEY

Cyber Kill Chain



Source: http://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html

ANDGIET
SECURING YOUR BUSINESS JOURNEY



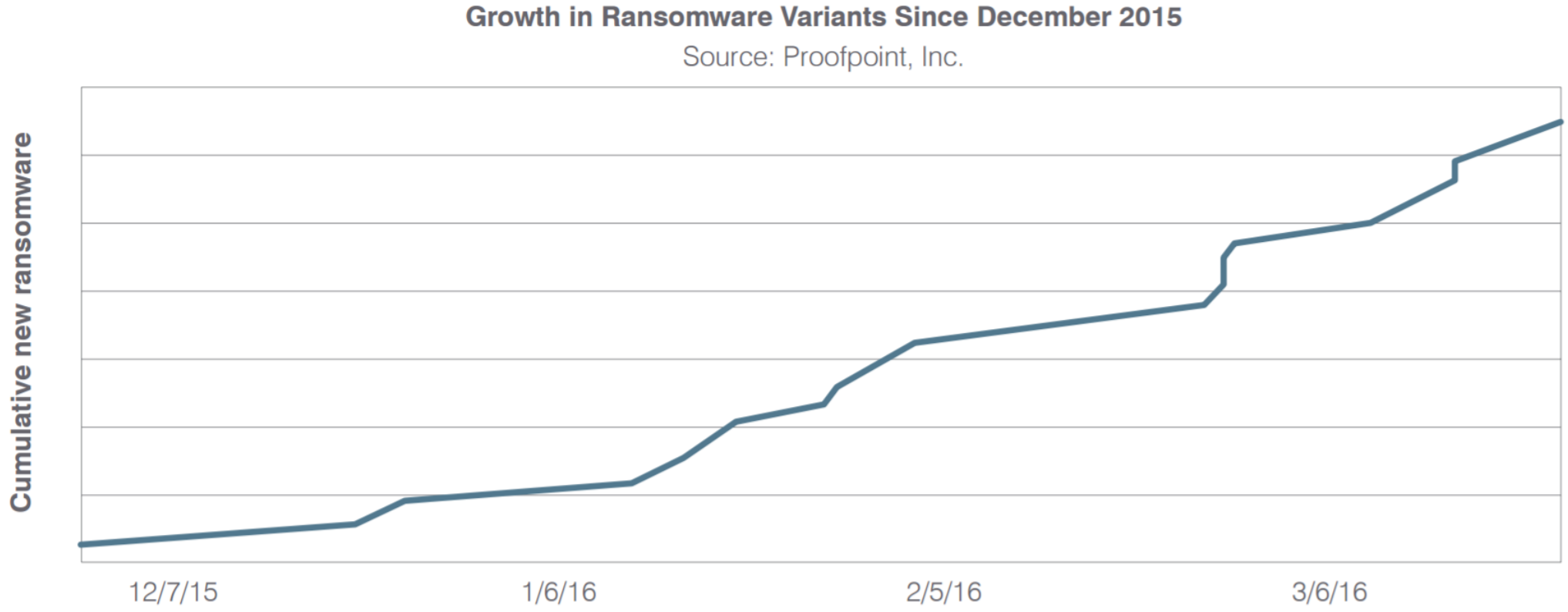
Source: Panda Security

ANDGIET
SECURING YOUR BUSINESS JOURNEY


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 18:47:17
Time Left
02:23:59:28
Your files will be lost on
5/19/2017 18:47:17
Time Left
06:23:59:28
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin ACCEPTED HERE
Send $300 worth of bitcoin to this address:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
Copy
Check Payment
Decrypt

Ransomware Trends

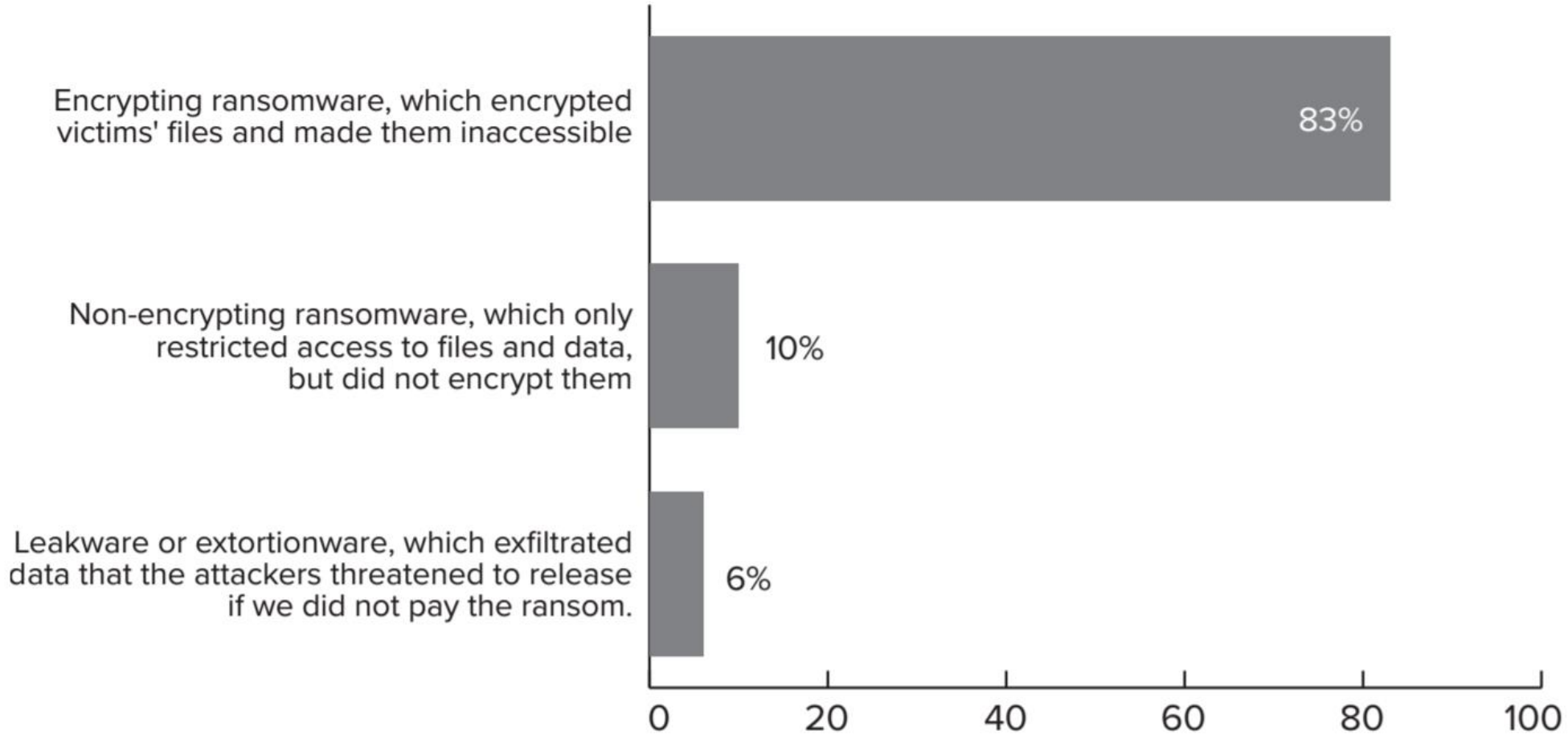
Ransomware and extortion rackets have been the new gold rush with cyber criminals reportedly making over a $1 billion USD in 2016 (IBM, 2017) with an increase of 50% on 2015 and



Source: Proofpoint, IBM

ANDGIET
SECURING YOUR BUSINESS JOURNEY

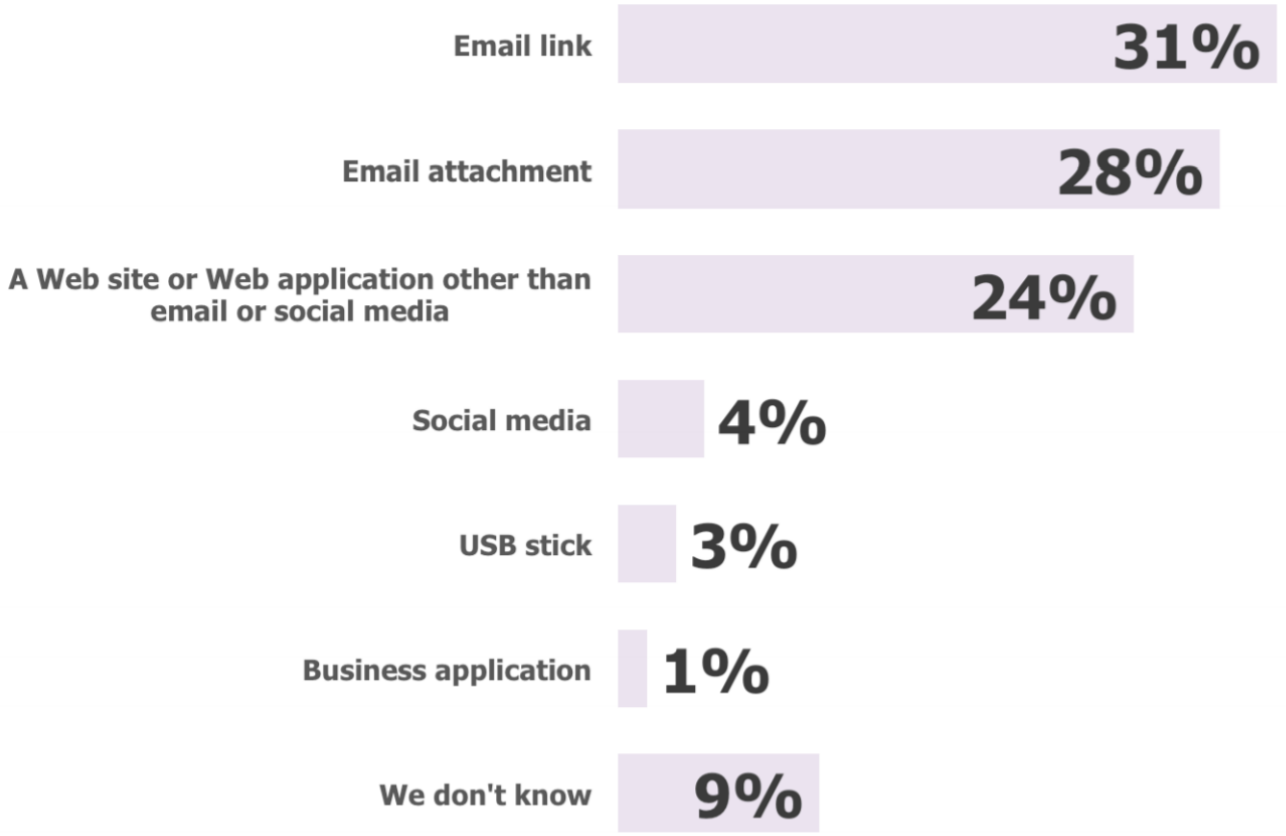
Which Type of Ransomware?



Source: Osterman Research

ANDGIET
SECURING YOUR BUSINESS JOURNEY

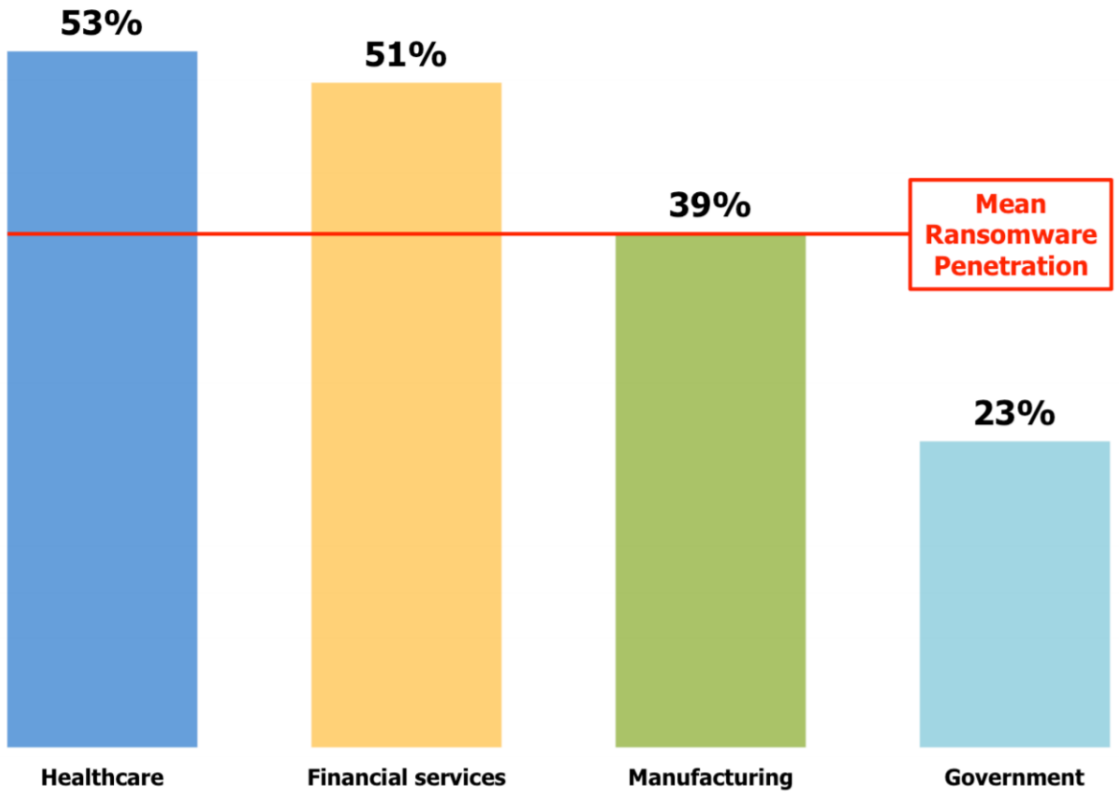
How Ransomware Entered the Organisation



Source: Osterman Research

ANDGIET
SECURING YOUR BUSINESS JOURNEY

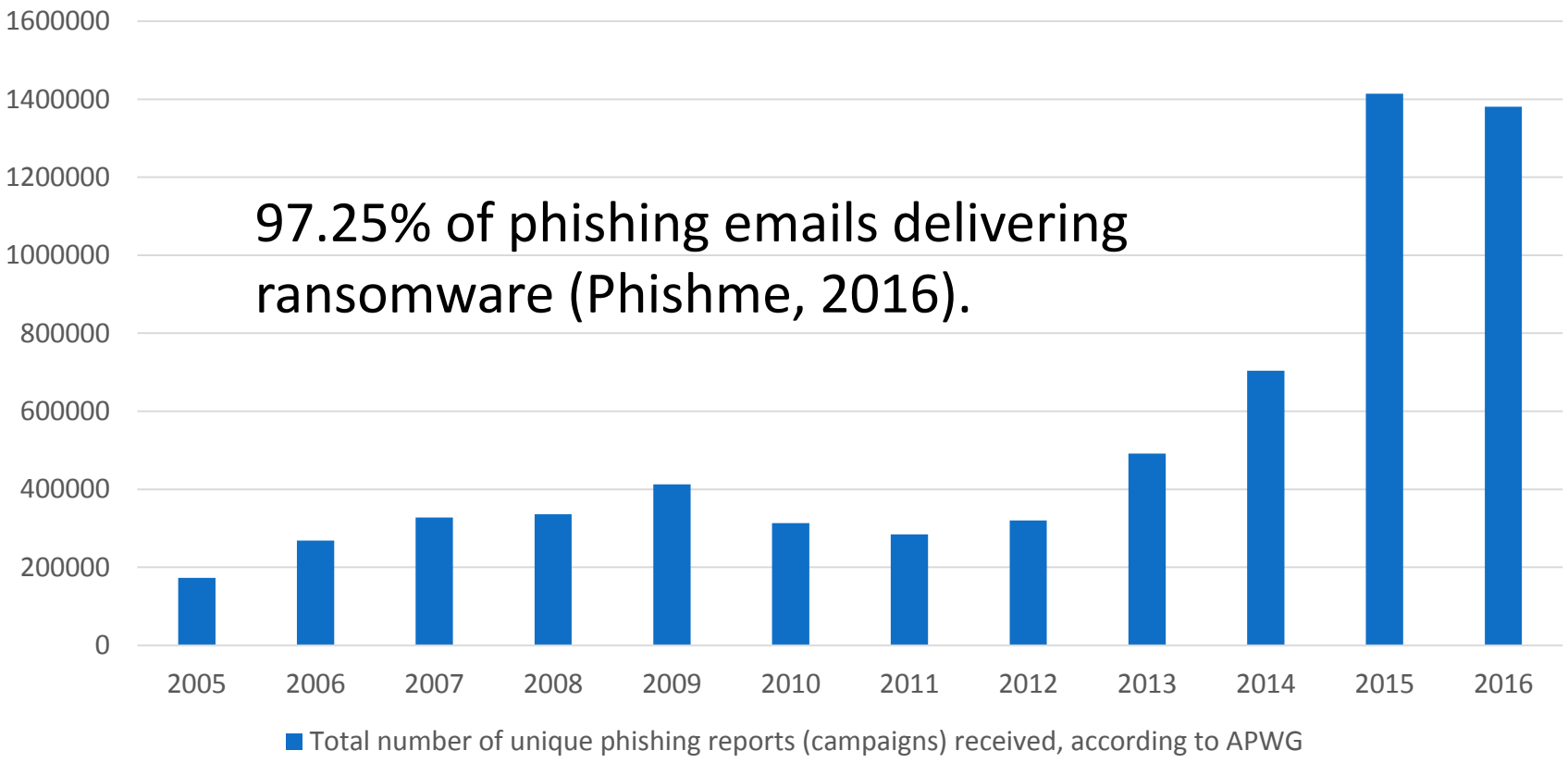
Ransomware Attacks That Have Occurred During the Previous 12 Months



Source: Osterman Research

ANDGIET
SECURING YOUR BUSINESS JOURNEY

Phishing



Source: Anti-Phishing Working Group

ANDGIET
SECURING YOUR BUSINESS JOURNEY

Bitcoin - Cryptocurrency

Source: blockchain.info

ANDGIET
SECURING YOUR BUSINESS JOURNEY

Ransomware Attacks Against Hospitals

Los Angeles Times

Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating

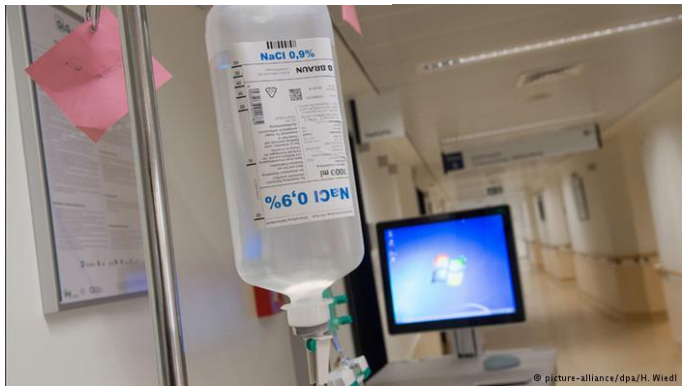
ANDGIET
SECURING YOUR BUSINESS JOURNEY

Ransomware Attacks Against Hospitals

Deutsche Welle

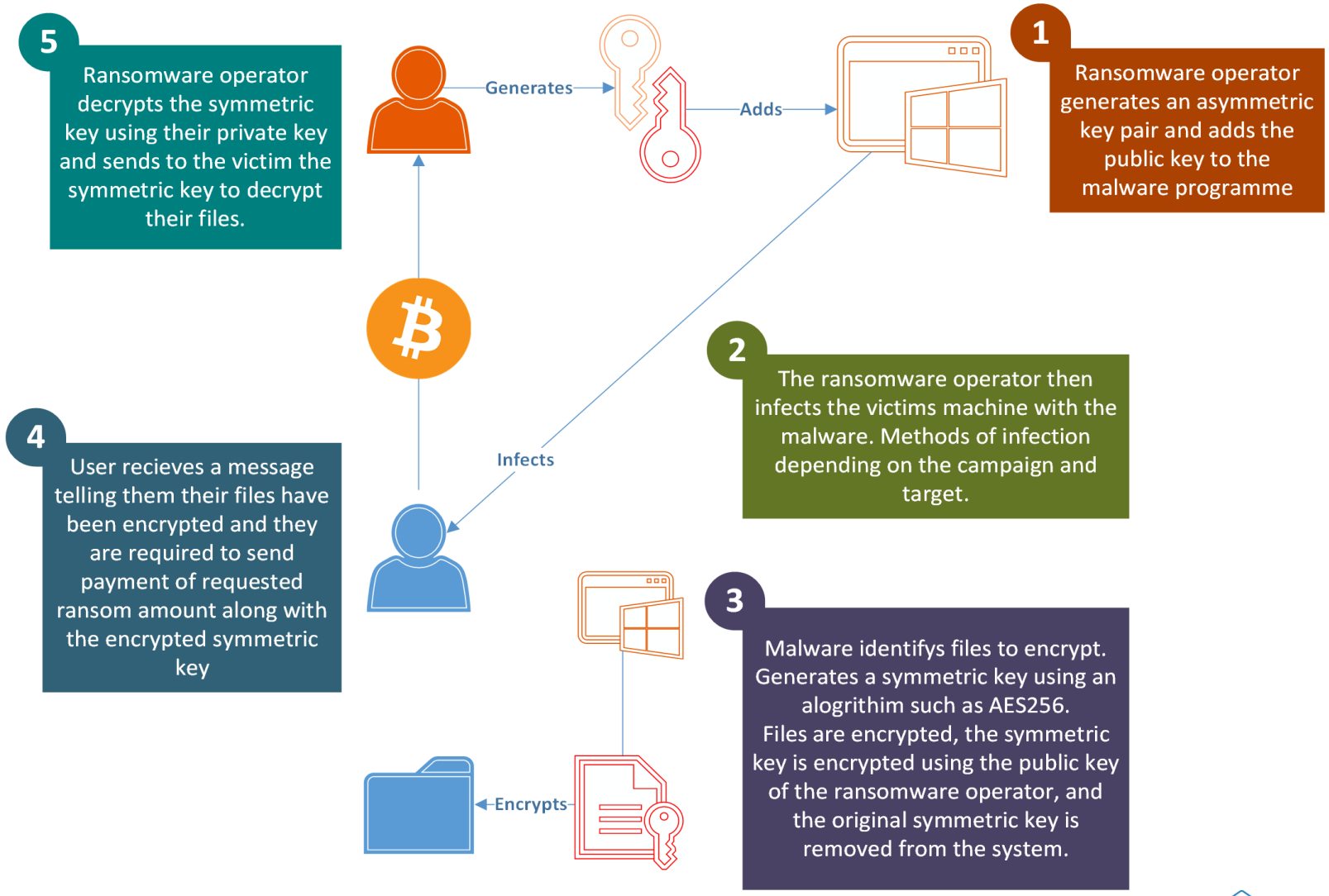
Hackers hold German hospital data hostage

Several hospitals in Germany have come under attack by ransomware, a type of virus that locks files and demands cash to free data it maliciously encrypted. It will take weeks until all systems are up and running again.



ANDGIET
SECURING YOUR BUSINESS JOURNEY

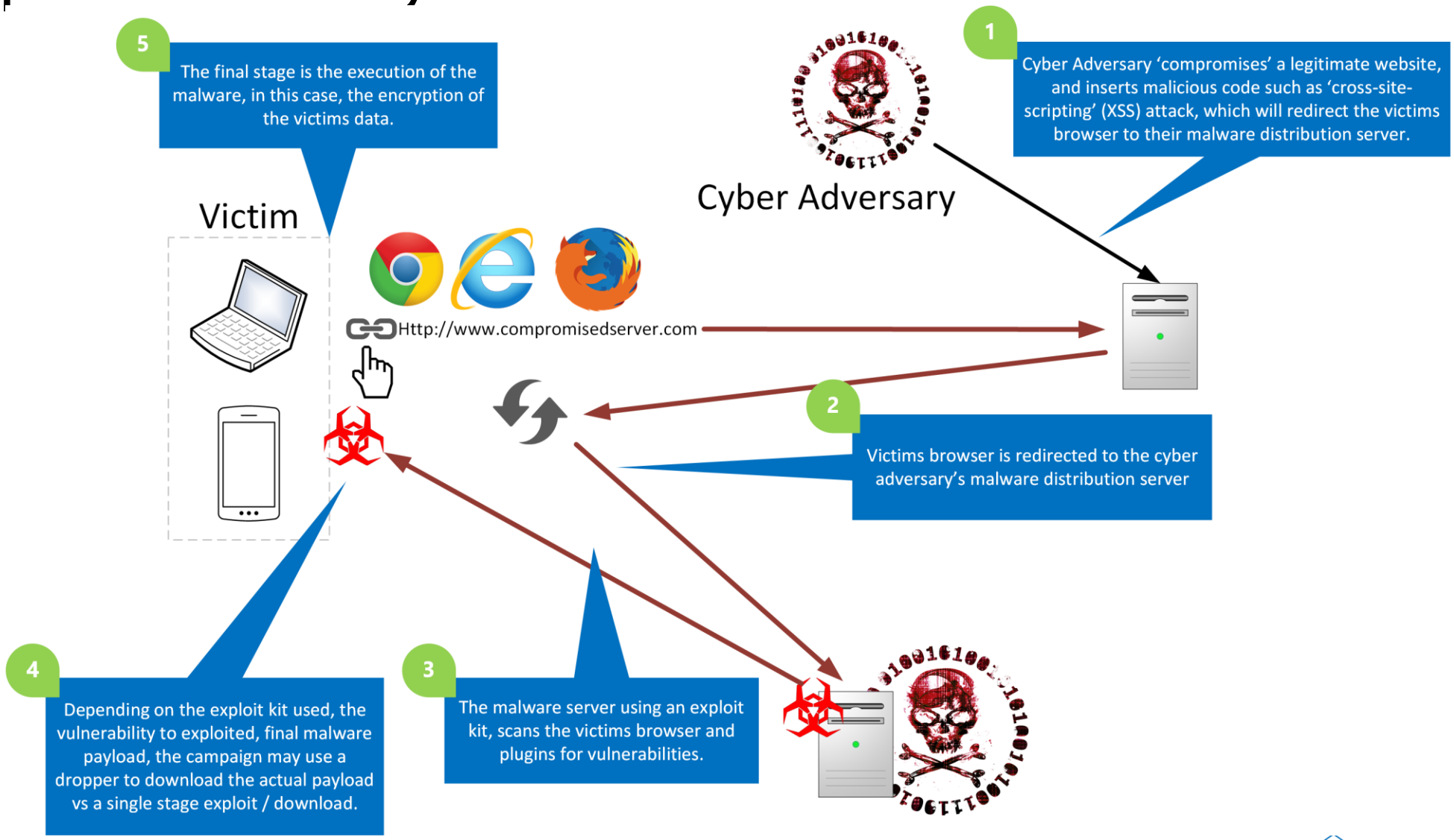
Typical Workflow of a Crypto-Ransomware



Source: Andgiet Security

ANDGIET
SECURING YOUR BUSINESS JOURNEY

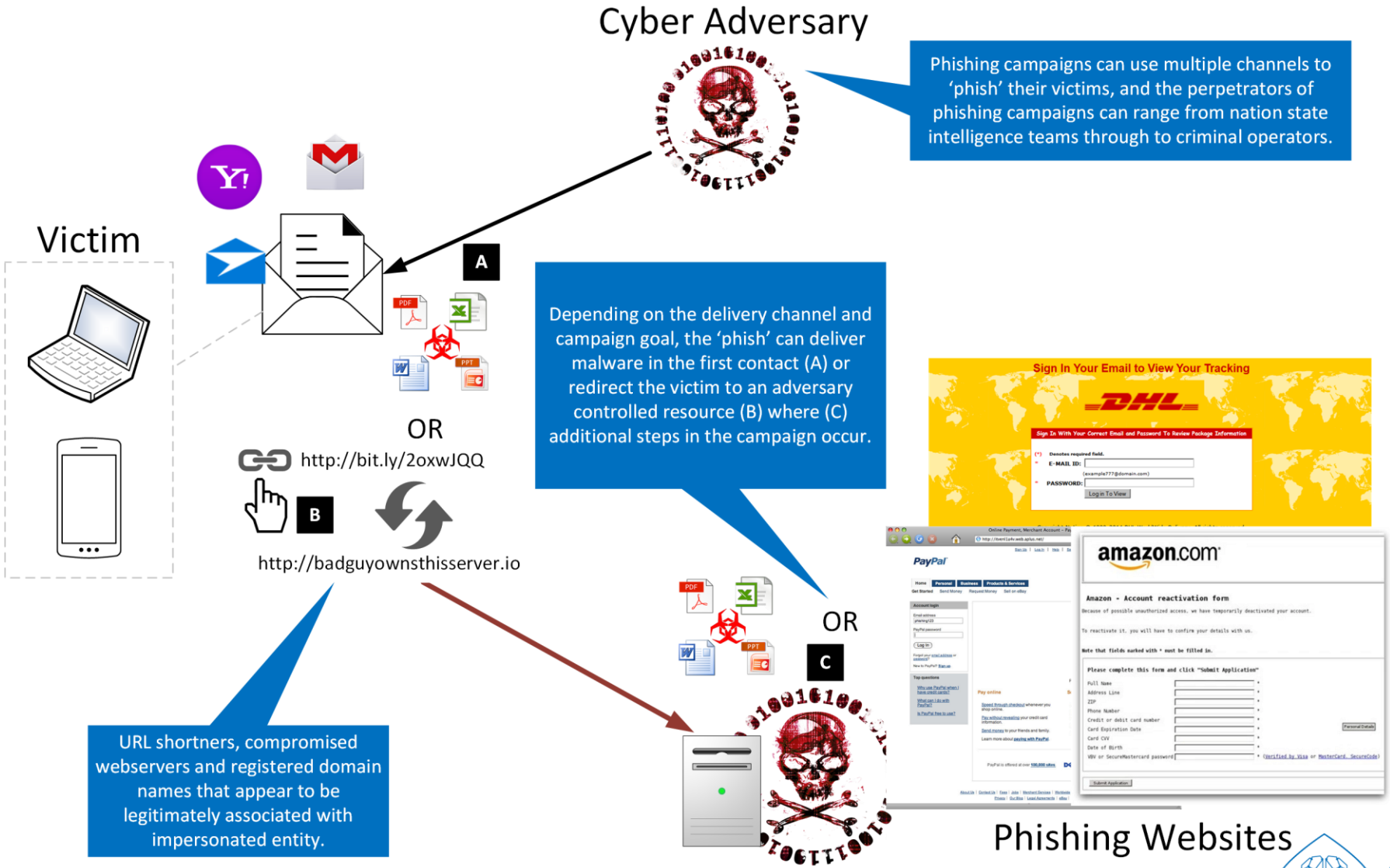
Typical Drive-by-download workflow



Source: Andgiet Security

ANDGIET
SECURING YOUR BUSINESS JOURNEY

Typical Phishing Email Workflow



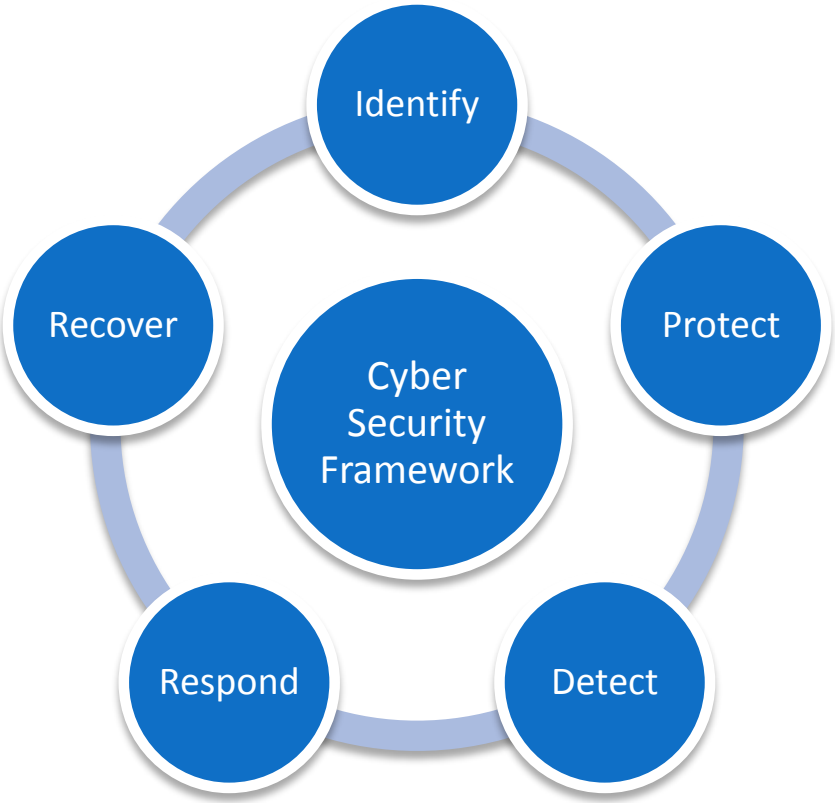
Source: Andgiet Security

ANDGIET
SECURING YOUR BUSINESS JOURNEY

Combating Ransomware

Big Five Tactics

1. Identify and backup Critical Systems & Data
2. Implement Network Segmentation
3. Patch your systems
4. Harden your systems
5. Practice your recovery processes



Source: NIST Cyber Security Framework

ANDGIET
SECURING YOUR BUSINESS JOURNEY

The Seven Knows – Identify

1. Know the value of your data and systems
2. Know who and what has access to your data and systems
3. Know where your data and systems are
4. Know what threats and vulnerabilities are putting your data and systems at risk
5. Know who is protecting your data and systems
6. Know how well your data and systems are protected
7. Know how well your recovery practices work

ANDGIET
SECURING YOUR BUSINESS JOURNEY

Protect

To prevent malware running:

Application Whitelisting TOP 4	**Patch Applications** TOP 4
A whitelist only allows selected software applications to run on computers. ***Why?*** All other software applications are stopped, including malware.	A patch fixes security vulnerabilities in software applications. ***Why?*** Adversaries will use known security vulnerabilities to target computers.
Disable untrusted Microsoft Office macros	**User application hardening**
Microsoft Office applications can use software known as “macros” to automate routine tasks. ***Why?*** Macros are increasingly being used to enable the download of malware. Adversaries can then access sensitive information, so macros should be secured or disabled.	Block web browser access to Adobe Flash player (uninstall if possible), web advertisements and untrusted Java code on the internet. ***Why?*** Flash, Java and web ads have long been popular ways to deliver malware to infect computers.

Source: The Australian Signals Directorate (ASD) Essential Eight

ANDGIET
SECURING YOUR BUSINESS JOURNEY

Protect

To limit the extent of incidents and recover data:

Restrict administrative privileges [TOP 4] Only use administrator privileges for managing systems, installing legitimate software and applying software patches. These should be restricted to only those that need them. ***Why?*** Admin accounts are the 'keys to the kingdom', adversaries use these accounts for full access to information and systems.	**Patching operating systems** [TOP 4] A patch fixes security vulnerabilities in operating systems. ***Why?*** Adversaries will use known security vulnerabilities to target computers.
Multi-factor authentication This is when a user is only granted access after successfully presenting multiple, separate pieces of evidence. Typically: Something you know, like a passphrase. Something you have, like a physical token. And/or something you are, like biometric data. ***Why?*** Having multiple levels of authentication makes it a lot harder for adversaries to access your information.	**Daily backup of important data** Regularly back up all data and store it securely offline. ***Why?*** That way your organisation can access data again if it suffers a cyber security incident.

[TOP 4] strategies to mitigate targeted cyber intrusions

Source: The Australian Signals Directorate (ASD) Essential Eight

ANDGIET
SECURING YOUR BUSINESS JOURNEY

Detection

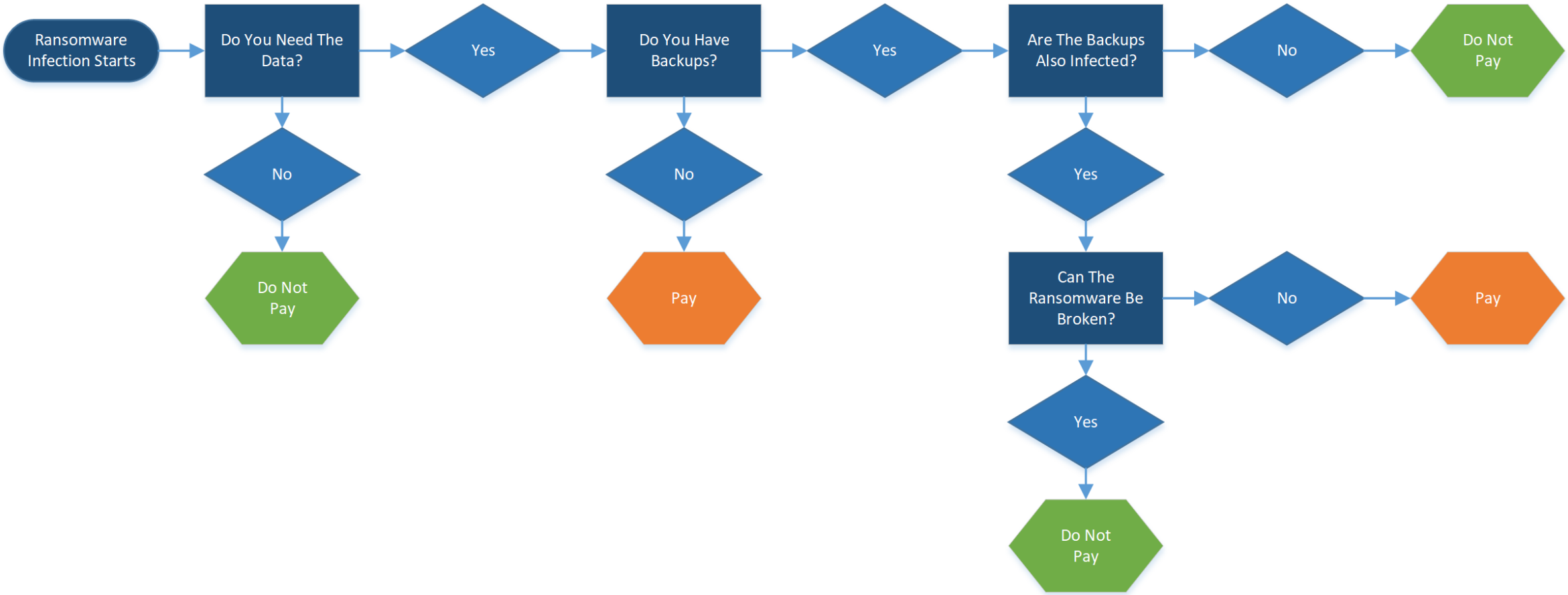
1. Detection coverage: If an active attacker were operating inside your network, would your systems see an operational activity and set off an alert?

2. Detection quantity: Can you investigate all the relevant alerts? Is it clear which are relevant?

3. Detection quality: When an alert is investigated, can you reach a conclusion?

ANDGIET
SECURING YOUR BUSINESS JOURNEY

Respond



Source: Ransomware Decision Tree – Control Risks

ANDGIET
SECURING YOUR BUSINESS JOURNEY

Recovery

- Can you recover to a known good state and meet your organisations Recovery Time Objective (RTO)?
- What does recovery for medical devices look like? Do you need support from the application vendor? Does the equipment need calibration and certification?
- What does recovery look like for cloud services?
- How often do you practice complete recovery/restore of devices and data? Can you trust your backups and build processes when you need them most?

ANDGIET
SECURING YOUR BUSINESS JOURNEY

Wrapping up

- Failing to plan, is planning to fail. Hope is not a strategy
- Technology is just a ‘part’ not the ‘whole’ – don’t forget the people and process
- Know the seven knows

As our dependency on technology increases, so does our vulnerability…

…our adversaries know this, and seek to exploit it.

…they are further aided by the ever reducing barrier to entry.

They have the asymmetrical advantage!

ANDGIET
SECURING YOUR BUSINESS JOURNEY

Thank you

@zenofsecurity or @andgietsecurity

https://sg.linkedin.com/in/johnellis

https://www.andgietsecurity.com

ANDGIET
SECURING YOUR BUSINESS JOURNEY