Ransomware Empowerment Training

FIRST Multi-Stakeholder Ransomware SIG



Copyright

Copyright © by Forum of Incident Response and Security Teams, Inc.

FIRST.Org is name under which Forum of Incident Response and Security Teams, Inc. conducts business.

This training material is licensed under Creative Commons Attribution-Non-Commercial-Share-Alike 4.0 (CC BY-NC-SA 4.0)

FIRST.Org makes no representation, express or implied, with regard to the accuracy of the information contained in this material and cannot accept any legal responsibility or liability for any errors or omissions that may be made.

All trademarks are property of their respective owners.

Permissions beyond the scope of this license may be available at first-licensing@first.org

Acknowledgments

A big thank you to all the contributors who made this training possible!

Special thanks to:

- Nadia Meichtry (Oneconsult AG), Gregor Wegberg (Oneconsult AG), creators of the training
- Éireann Leverett (Concinnity Risks), Serge Droz (Swiss FDFA, FIRST) and Barry Greene (Senki)
- All members of the FIRST MSR SIG

Slides

You can download the actual version of the slides under:
https://www.first.org/education/trainings



Training Introduction

Photo by Chris Wormhoudt on Unsplash

Agenda

- Welcome and introductions
- Ransomware Attacks
- Preparation for ransomware attacks
- Darknet & Ransomware groups
- Incident Response Management
- Response to a ransomware attack
- The recovery phase
- A word on negotiation
- Q&A



Ransomware Attacks

Introduction into the world of ransomware attacks

Mikhail Golub @golub

What is Ransomware?

Ransomware (Attacks)

Ransomware = Ransom + ware

- It makes data inaccessible until a **ransom** is paid….
- Or it makes data universally available **unless a ransom** is paid
- It is a malicious software, i.e., **malware**.

Ransomware Attack

- An **incident** that **usually** employs a Ransomware.
- The focus begins to shift from holding data hostage until the ransom is paid to extortion by threatening to publish stolen data. Ransomware not necessarily involved.

A brief history of Ransomware

Ransomware is not a new phenomena

1989 there was the

- Aids virus, a wiper
- Aids trojan, a ransomware

~ 2010 PC Ransomware

~ 2015 Big game hunting → Go for orgs



By Joseph L. Popp, AIDS Information Trojan author

Ransomware took off with the emergence of cryptocurrencies

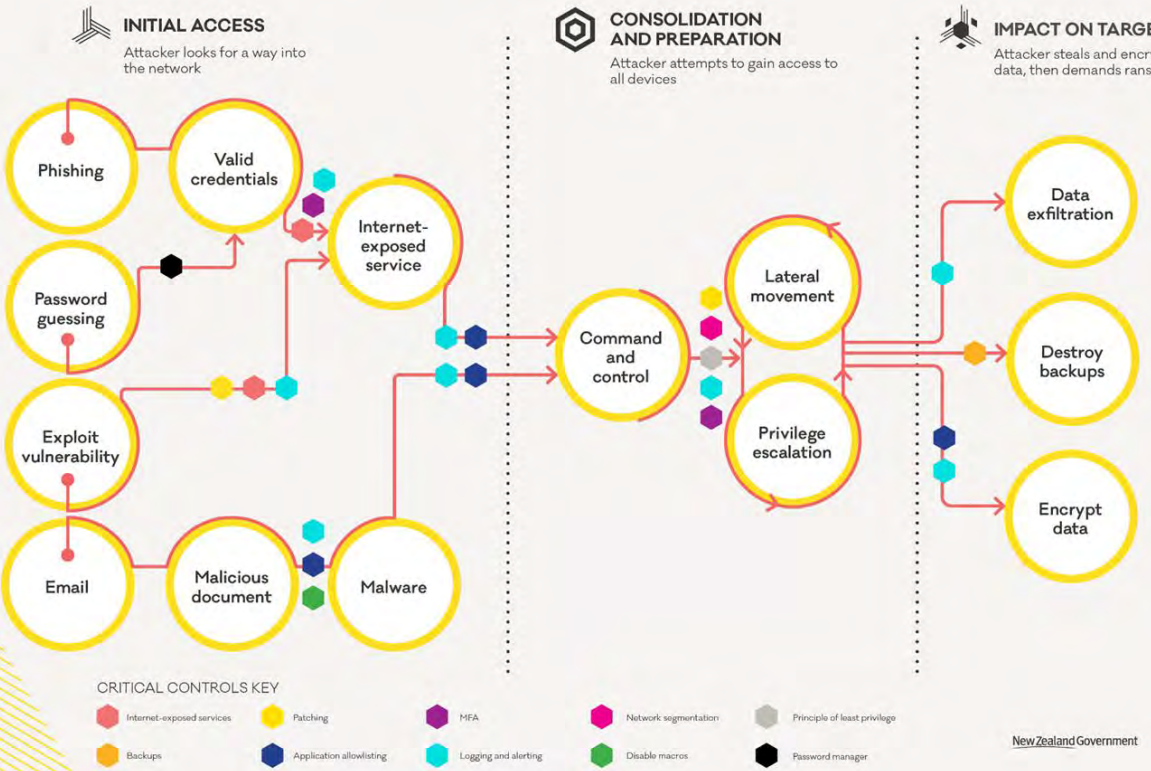
Ransomware Attack

1. Compromise target
2. Theft of sensitive data
3. Encrypt data (1st extortion)
4. Threaten to publish data (2nd extortion)
5. Optional: Public naming and shaming
6. Optional: Threat of distributed denial of service (3rd extortion)
7. Optional: Threaten customers, users, employees, etc.
8. Optional: Use stolen data for business email compromise (BEC), phishing, etc.
9. Optional: Publish stolen data

LIFECYCLE OF A RANSOMWARE INCIDENT

certnz

How the CERT NZ Critical Controls can help you stop a ransomware attack in its tracks.



Adversary Tactics & Techniques

- MITRE ATT&CK (https://attack.mitre.org/)
  - Source for ideas on which artefacts to analyze
  - Ideas what the attackers might have done before / after (starting from the event)!
  - Examples:
    - Valid accounts: https://attack.mitre.org/techniques/T1078/
    - Data encrypted for impact: https://attack.mitre.org/techniques/T1486/
- MITRE D3FEND (https://d3fend.mitre.org/)
  - Source for ideas on how to defend oneself

MITRE ATT&CK

Technique ID	Technique Name	Tactic	Count from CTI	Mapped Data Components	# Sigma Analytics	# Atomic Tests
T1486	**Data Encrypted for Impact**	Impact	50	6	10	5
T1082	**System Information Discovery**	Discovery	30	4	14	24
T1083	**File and Directory Discovery**	Discovery	29	3	17	6
T1490	**Inhibit System Recovery**	Impact	23	5	18	9
T1059.001	**PowerShell**	Execution	20	5	183	22
T1047	**Windows Management Instrumentation**	Execution	19	3	40	10
T1489	**Service Stop**	Impact	17	7	9	3
T1112	**Modify Registry**	Defense Evasion	16	6	65	44
T1562.001	**Disable or Modify Tools**	Defense Evasion	16	6	77	38
T1059.003	**Windows Command Shell**	Execution	14	2	21	5
T1190	**Exploit Public-Facing Application**	Initial Access	14	2	80	0
T1133	**External Remote Services**	Persistence, Initial Access	13	3	7	1
T1021.001	**Remote Desktop Protocol**	Lateral Movement	13	4	14	3
T1018	**Remote System Discovery**	Discovery	13	4	15	20

How bad is it?

Ransomware - Your Experience ~10Min

1. Who experienced ransomware attacks directly in the past?
2. Who works for an organization where a partner/supplier got hit by ransomware?
3. Who's hosting organization / management is aware of ransomware and takes the threat seriously?

How is victimisation distributed by country?

Detections: ransomware over time by geolocation

Source: FIRST22: Ransomware as a Science

Jul.21		Aug.21		Sep.21		Oct.21		Nov.21		Dec.21	
United States	25.5%	United States	20.2%	United States	19.5%	United States	23.4%	United States	21.1%	United States	22.2%
China	10.7%	France	7.2%	Hong Kong	9.9%	France	7.5%	France	6.3%	France	7.3%
India	6.1%	India	6.5%	Germany	7.9%	Italy	5.0%	Belgium	4.4%	Hong Kong	7.0%
Germany	4.8%	Hong Kong	5.8%	France	4.6%	Belgium	4.5%	Italy	4.4%	Italy	5.7%
Brazil	4.8%	Germany	4.6%	Turkey	4.2%	Brazil	3.8%	Hong Kong	4.3%	India	5.3%

How big is the problem

Detection by business size

Source: FIRST22: Ransomware as a Science

Dec-21	Top 1 - United States		Top 2 - France		Top 3 - Hong Kong		Top 4 - Italy		Top 5 - India	
	1 MAZE	220	WCRY	168	WCRY	41	WCRY	20	WCRY	1,274
	2 LOCKY	145	LOCKBIT	30	LOCKY	2	GANDCRAB	15	GANDCRAB	96
	3 CRYPTOR	125	HIDDENTEAR	15	RYUK	1	MOUNTLOCKER	12	MOUNTLOCKER	66
	4 MOUNTLOCKER	106	Gorf	12	Crypmodadv	1	SODINOKIBI	8	EGREGOR	42
	5 MORRISCRYPT	71	THANOS	7	Crypmod	1	EGREGOR	7	SODINOKIBI	33
					Enterprise					
	1 MAZE	176	WCRY	168	WCRY	41	WCRY	19	WCRY	1,131
	2 LOCKY	63	LOCKBIT	7	LOCKY	2	HIVE	2	GANDCRAB	94
	3 GANDCRAB	61	HIDDENTEAR	4	Crypmodadv	1	LOCKY	2	MOUNTLOCKER	66
	4 WCRY	46	WANA	3	ERIS	1	CRYPCTB	2	EGREGOR	42
	5 Filecoder	43	Gorf	3	WANA	1	CONTI	1	SODINOKIBI	33
					SMB					
	1 CRYPTOR	125	LOCKBIT	21	Genasom	1	GANDCRAB	15	WCRY	120
	2 MORRISCRYPT	71	Gorf	6			MOUNTLOCKER	12	StopCrypt	3
	3 MOUNTLOCKER	70	CRYPTESLA	1			SODINOKIBI	8	BABUK	3
	4 LOCKY	55	CRYTOX	1			EGREGOR	7	PolyRansom	2
	5 MAZE	44	CRYSIS	1			CONTI	5	LOCKBIT	2
					Consumers					
	1 CERBER	32	THANOS	6	RYUK	1	CERBER	6	WCRY	23
	2 LOCKY	27	HIDDENTEAR	5	Crypmod	1	StopCrypt	4	StopCrypt	12
	3 Crypmodadv	5	Gorf	3	COBRA	1	Gorf	2	VIRLOCK	6

How big is the problem

Detection by business size

US IC3 Extortion reports 2023: 49k

Global data leaks by ransomware gangs: 21K

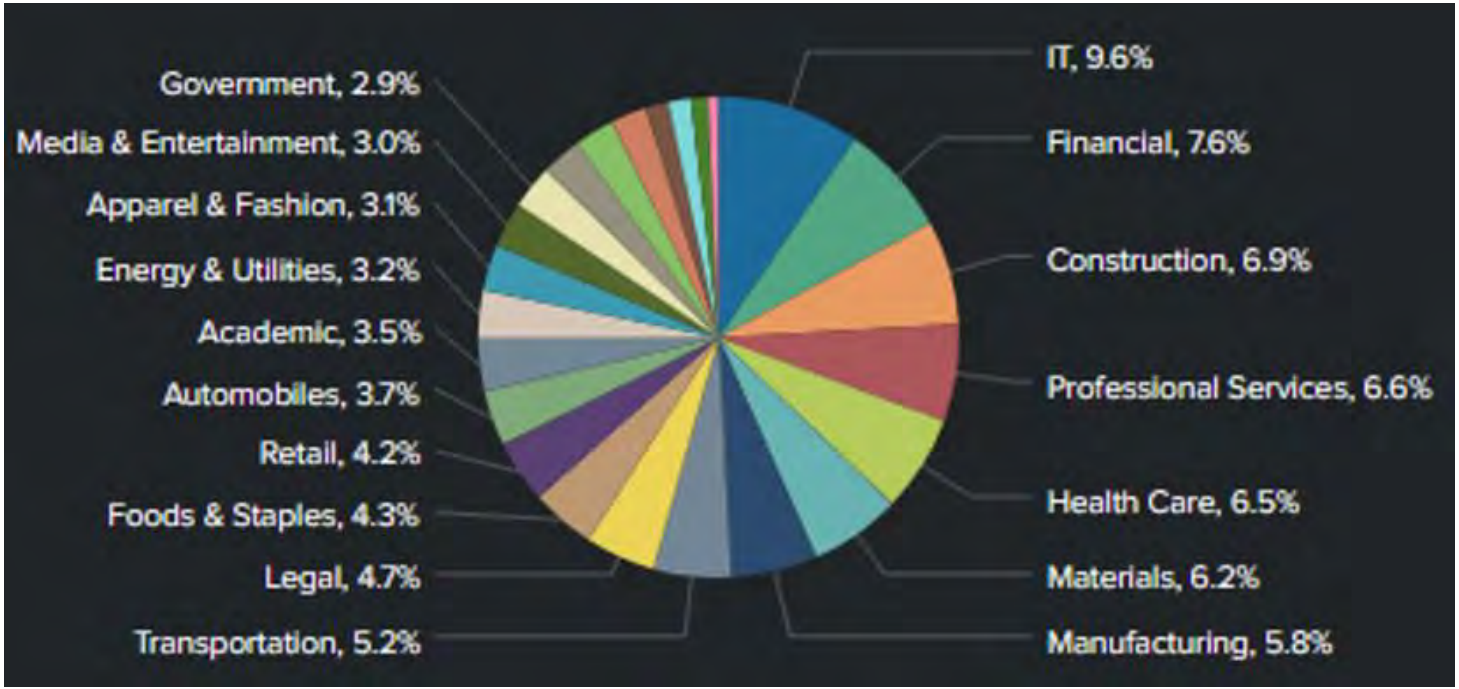
Both are underreported, but probably not more than 100k events globally.

We know number of events correlates to GDP: https://ccb.belgium.be/en/news/richer-country-more-ransomware-victims-it-has

Victim Landscape

Leaks: Targeted sector

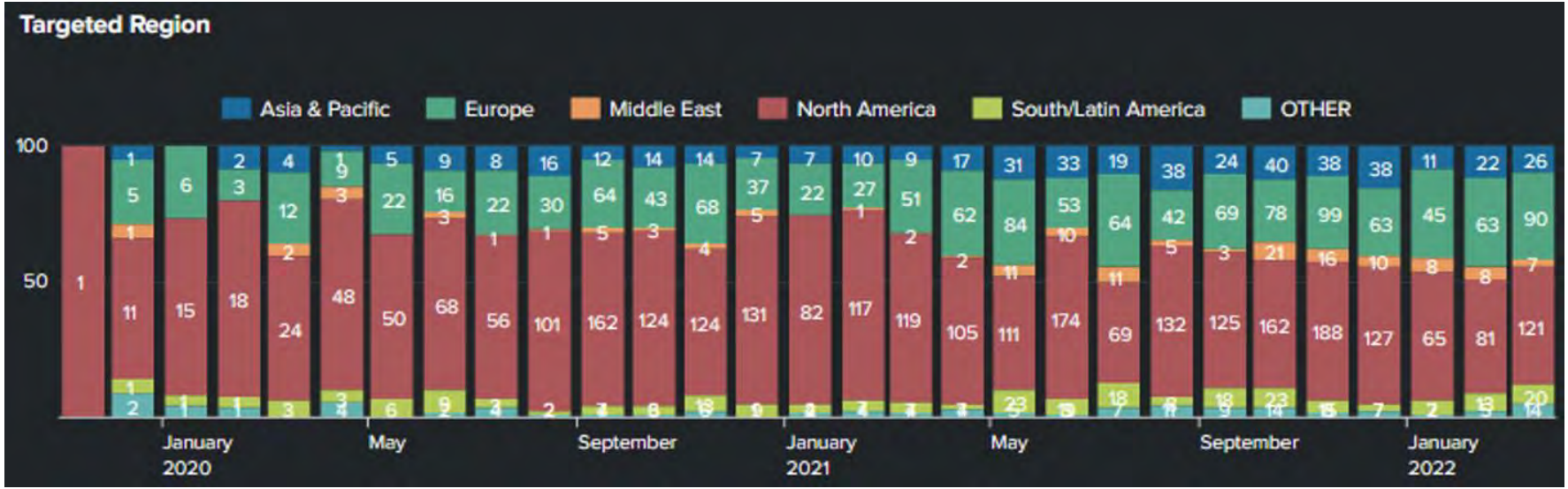
Source: FIRST22: Ransomware as a Science



Victim Landscape

Leaks: Targeted region over time

Source: FIRST22: Ransomware as a Science



Victim Landscape

“The threat landscape report on ransomware attacks published today by the European Union Agency for Cybersecurity (ENISA) uncovers the shortcomings of the current reporting mechanisms across the EU.”

https://www.enisa.europa.eu/news/ransomware-publicly-reported-incidents-are-only-the-tip-of-the-iceberg

Loss Comparison (USA)

2023 CRIME TYPES continued

By Complaint Loss

Crime Type	Loss	Crime Type	Loss
Investment	$4,570,275,683	Extortion	$74,821,835
BEC	$2,946,830,270	Employment	$70,234,079
Tech Support	$924,512,658	Ransomware*	$59,641,384
Personal Data Breach	$744,219,879	SIM Swap	$48,798,103
Confidence/Romance	$652,544,805	Overpayment	$27,955,195
Data Breach	$534,397,222	Botnet	$22,422,708
Government Impersonation	$394,050,518	Phishing/Spoofing	$18,728,550
Non-payment/Non-Delivery	$309,648,416	Threats of Violence	$13,531,178
Other	$240,053,059	Harassment/Stalking	$9,677,332
Credit Card/Check Fraud	$173,627,614	IPR/Copyright and Counterfeit	$7,555,329
Real Estate	$145,243,348	Crimes Against Children	$2,031,485
Advanced Fee	$134,516,577	Malware	$1,213,317
Identity Theft	$126,203,809		
Lottery/Sweepstakes/Inheritance	$94,502,836		

Descriptors**			
Cryptocurrency	$3,809,090,856	Cryptocurrency Wallet	$1,778,399,729

*Regarding ransomware adjusted losses, this number does not include estimates of lost business, time, wages, files, or equipment, or any third-party remediation services acquired by an entity. In some cases, entities do not report any loss amount to the FBI, thereby creating an artificially low overall ransomware loss rate. Lastly, the number only represents what entities report to the FBI via the IC3 and does not account for the entity direct reporting to FBI field offices/agents.

*Regarding ransomware adjusted losses, this number does not include estimates of lost business, time, wages, files, or equipment, or any third-party remediation services acquired by an entity. In some cases, entities do not report any loss amount to the FBI, thereby creating an artificially low overall ransomware loss rate. Lastly, the number only represents what entities report to the FBI via the IC3 and does not account for the entity direct reporting to FBI field offices/agents.

What do current attacks look like?

Ransomware as a Service (RaaS)

Industrialisation of ransomware attacks through division of labour:

- RaaS Operator
- RaaS Affiliate
- Initial Access Broker

Ransomware as a Service (RaaS)

RaaS Operator

- Develops necessary tooling, e.g. a ransomware builder
- Maintains the leak site
- Processes payments: Distributes payments to parties involved
- Negotiates with victims
- Provides guidance, recommendations and standards
- Maintains and develops its branding

Ransomware as a Service (RaaS)

RaaS Affiliate

- Purchases or gains access to a victim's environment
- Uses services provided by the RaaS Operators
- Executes the majority of the attack: Moves laterally, persists on systems, exfiltrates data, and executes ransomware

Ransomware as a Service (RaaS)

Initial Access Broker

- Focus is on gaining unauthorised access to an organisation's system(s)
- They often conduct automated reconnaissance to gain insight into the compromised organisation. They then use this information to find buyers.

Commodity / Automated Attacks

Low-effort, high-volume ransomware attacks

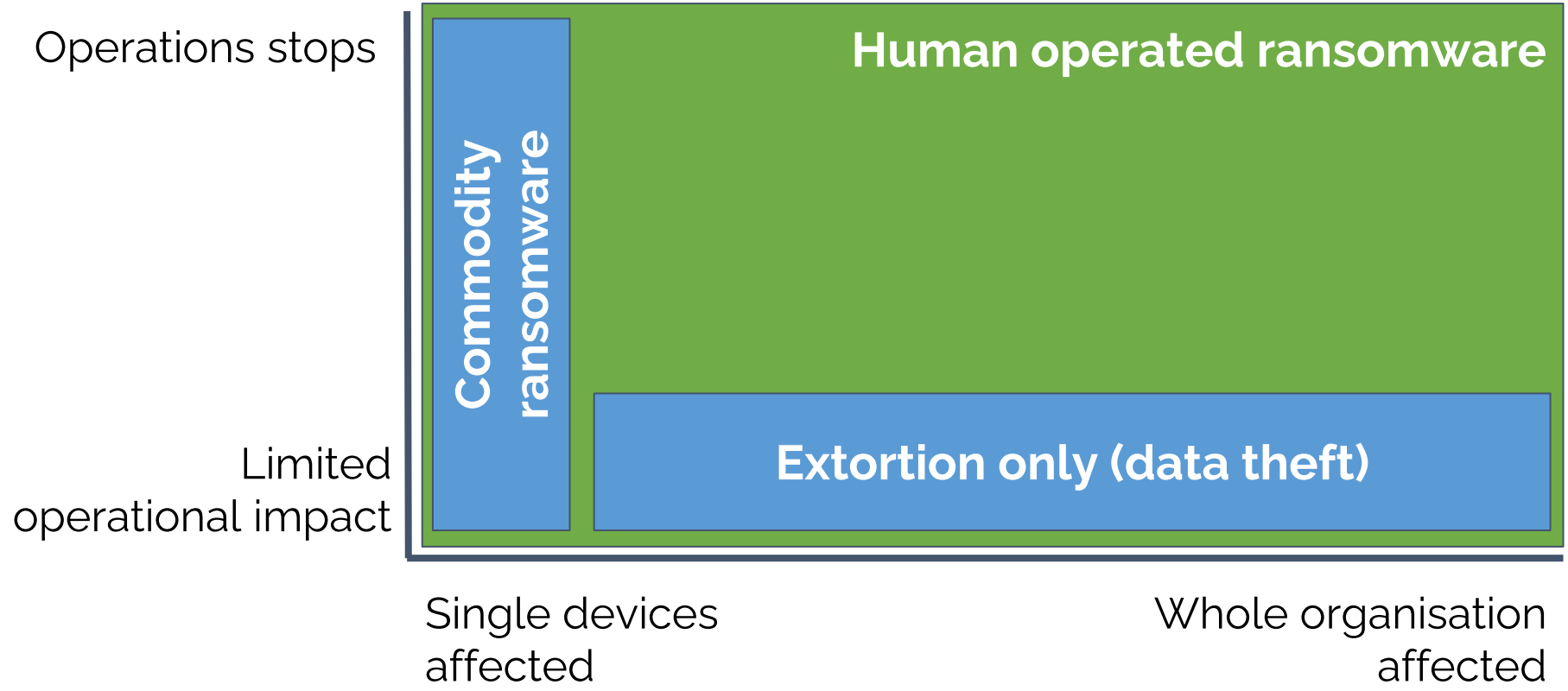
- Threat actor doesn't care who or what is affected
- Often starting with mass exploitation of easily exploitable vulnerabilities or scalable social engineering attacks (e.g. malspam, credential phishing)
- Common to target/affect individual systems or environments
- Highly automated
  - Hint: Public clouds have well-documented and common APIs, making it much easier to automate attacks across a large number of organisations.

Human Operated Ransomware

Ransomware attacks driven by a human at a keyboard

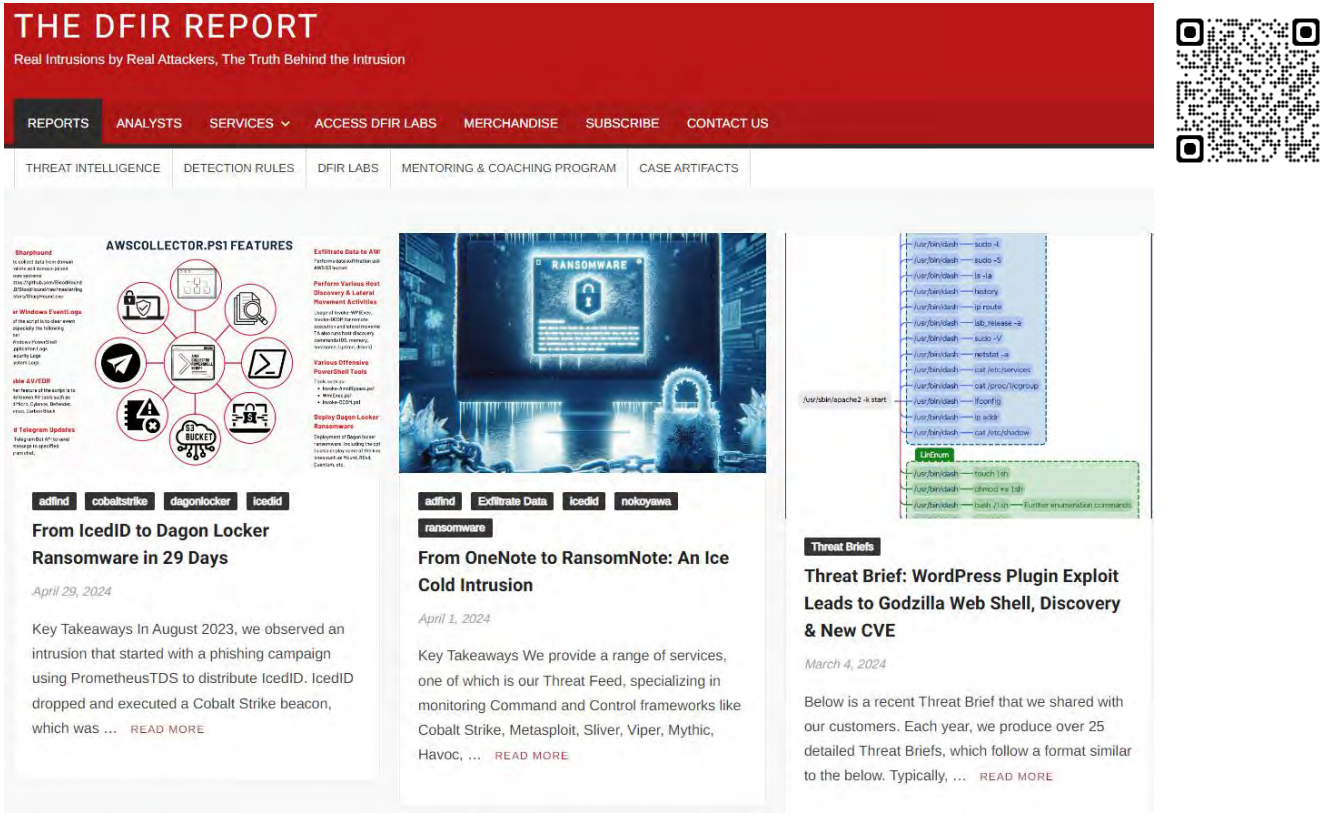
- Usually affects entire organisation, not just some systems
- Attackers adapt to the environment
  - Target recovery systems, e.g. destroy backups
  - Encrypts infrastructure services, e.g. hypervisors rather than virtual servers running on them
  - More difficult to kick off your networks
- Threat actor adapts to target organisation
  - Develops in-depth understanding of the organisation
  - Ransom/extortion amount based on accounting data
- Could still be a RaaS Affiliate

Ransomware Attacks



Based on https://learn.microsoft.com/en-us/security/ransomware/media/human-operated-ransomware/ransomware-extortion-based-attack.png

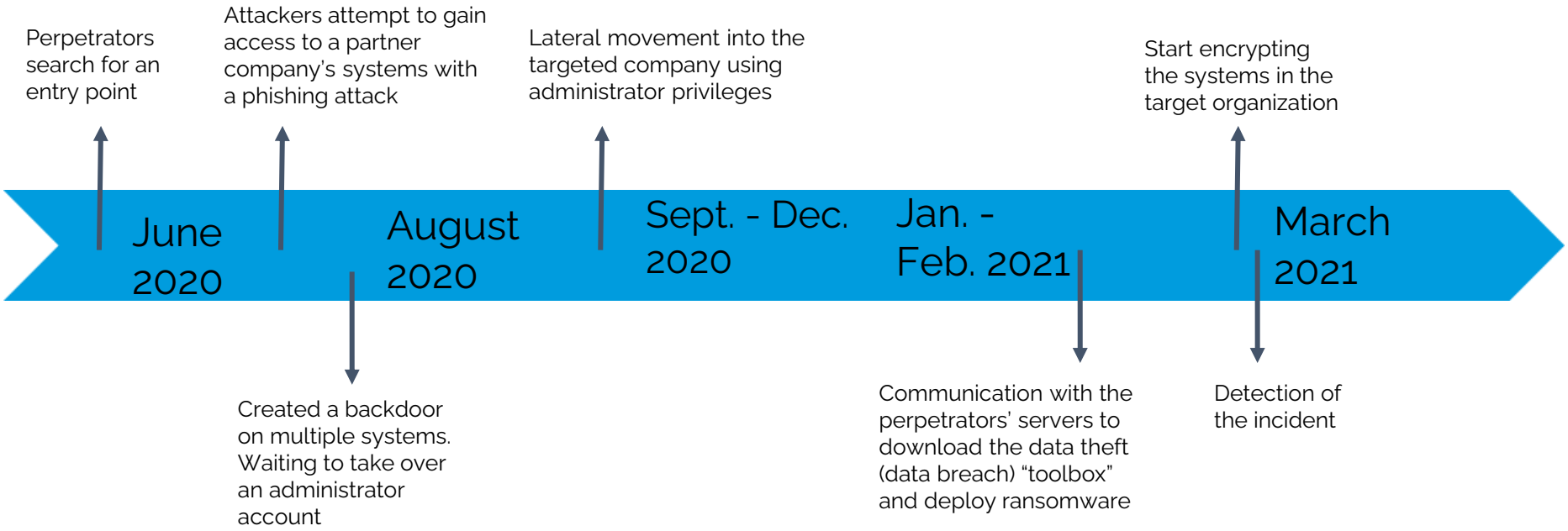
The DFIR Report



Example of a large logistics company

Example Case 1: large logistics company

What happened?



Example Case 1: large logistics company

During Incident Response

- Ransom: several million euros
- Chaos phase ended after 3 weeks
- Incident management ended after 8 months
- Return to normal operation after more than 1 year

Example Case 1: large logistics company

After the Incident

- 1 burnout
- 5 people left the company because of the stress
- Stress on family, private life, constant adrenaline level
- Other consequences?

Example Case 1: large logistics company

Lessons Learned - Things that did not go well

- Who has the lead and who decides?
  - Incident Management
  - Incident Response
- Keep overview over all ongoing tasks
  - Legal Aspects (GDPR)
  - Technical Aspects
  - Restore and Return to Normal
  - Protect the organization

Example Case 1: large logistics company

Lessons Learned - Things that did not go well

- Communication with stakeholders
  - Board of Directors
  - Media
  - Employees and Partners
- Communication with perpetrators
- Do the right tasks at the right time

Example Case 1: large logistics company

Lessons Learned

- Are all the necessary people present from the beginning?
  - Lawyers: data protection, reporting requirements, etc.
  - Data protection officer
  - Management: to be able to make decisions quickly
  - Board of directors: decisions and strategic issues
  - Marketing/Communication: Internally and externally
- Who are you going to call? IT service provider?
- If you think you will pay, see already how difficult it is to get larger amounts in BTC

Example of a small company

Example Case 2: small company

Timeline: The Start

Day X, Monday in the morning:

- Ransomware attack detected / realized
- External SOC calls in CSIRT for support
  - Incident management by external SOC
  - CSIRT to perform digital forensics and provide additional expertise
- Initial investigation with existing Microsoft Defender deployment
- Velociraptor deployed to ease the investigation

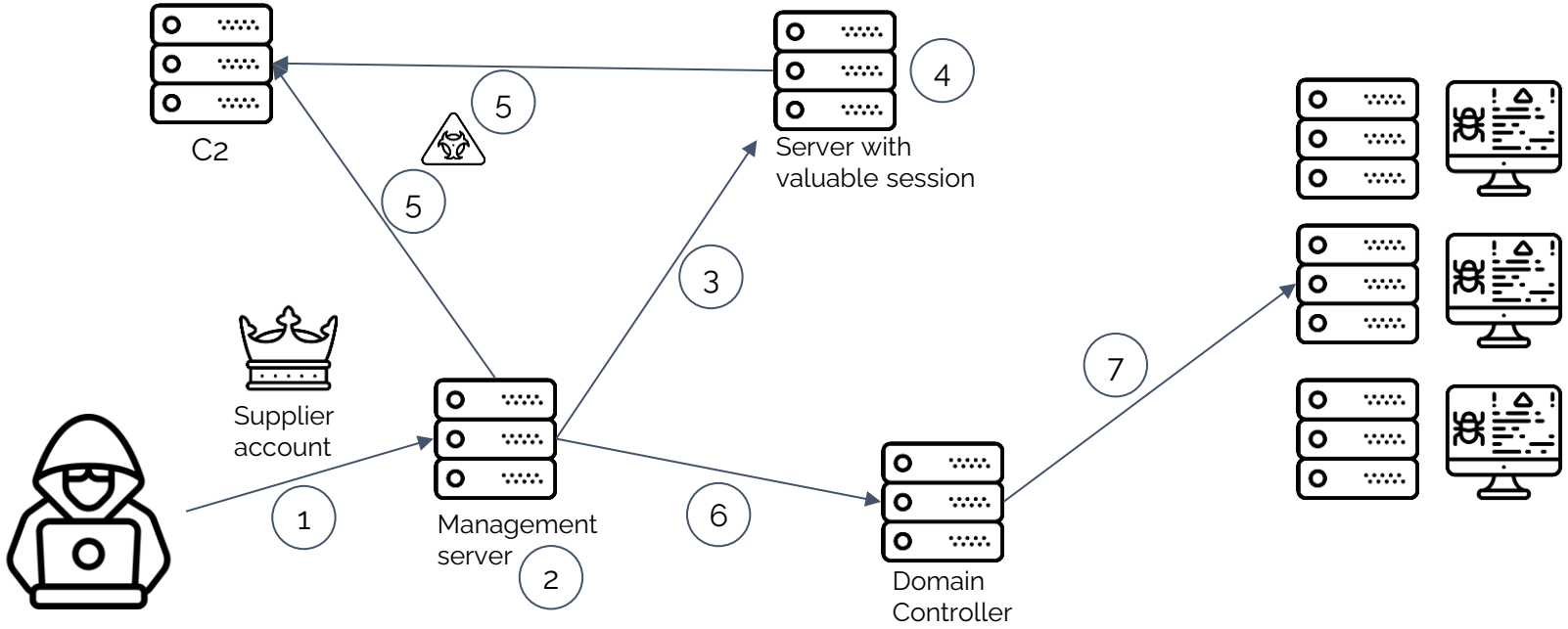
Example Case 2: small company

Timeline: Investigation

- Day X+1: 19 VM snapshots received for forensic analysis
- Day X+2: Meeting with law enforcement
- Day X till X+9: Investigation, analysis, documentation

Example Case 2: small company

Attacker's steps



Icons created by Smashicons from Flaticon

Example Case 2: small company

Lessons Learned

- MFA for everyone
- Improve AD password policy
- Deploy EDR on every system, enable it and regularly check the alerts
- Improve logging (default logs and some completely disabled)
- Harden AD & GPOs (lots of PingCastle findings)

- To discuss: Geoblock non-essential web services, e.g. remote access?

Ransomware Impact - Exercise Part 1

1. Form a group of 3
2. Each person shares with the group (~10 min):
   a. Describe what your organisation or constituency does / what its purpose is.
   b. Tell each other what a successful ransomware attack would mean for your organisation and your constituents: What would be the impact? Why?

Operational/Business Impact

- Everything in the organisation comes to a standstill
  - By encrypting critical/all systems
  - Loss of trust in your own environment
- Incident costs
- Regulatory notice periods
- Regulatory and compliance fees/penalties
- How would you:
  - Ensure resilience in the aftermath of an incident

Operational/Business Impact

- Damage to reputation, brand, and trust
  - Leaked customer / employee data
  - Trust in your services and products
- Regulatory and contractual consequences
  - Effort to check and comply with legal or contractual obligations
  - Possible penalties

The impact on victims has an impact on the economy.

Societal Impact

- The erosion of trust and confidence in and within the sector
  - What does it mean when hospitals are under constant and successful attack?
  - What effect does it have on me and our community if I keep reading about successful attacks on electricity and water suppliers?
- Contributes to mistrust of authorities/government
  - Are we just at the mercy of the attackers?
  - Why is nothing being done? Are they so powerless?

Human Impact

"An IT employee has a three-month-old daughter at home. He hasn't seen her for four days, he says." – from an article about a ransomware attack on a newspaper publisher

Source (German): https://web.archive.org/web/20240217115416/https%3A%2F%2Fwww.nzz.ch%2Ftechnologie%2Fkriminelle-hacker-greifen-die-nzz-an-und-erpressen-sie-cyberangriff-ransomware-ld.1778725%3Fmktcid%3Dsmsh%26mktcval%3DE-mail

Human Impact

Incidents take a toll on people!

- Employees can see and feel that something is not right, and this unsettles them
  - What does this mean for my job security?
  - What happens next? ⇒ Uncertainty
- Incident responders and their support will be working long hours (10-14 hours) for weeks

Human Impact

This is really hard for everyone involved: **Assume 50% of staff operates at 50% of normal capacity.**

How do you handle this?

- What does this mean for employees and management?
- How to counter risks on human wellbeing?

Technical Impact

- What is compromised? What not?
- How to communicate securely?
- Can we trust our own documentation (stored in digital form)?
  - Can we even access it?

Technical Impact

When will you be able to trust your systems again?

- Were the (immediate) measures sufficient?
- Are the backups infected?
- Is a recovered/rebuilt system now secure? Secure enough?
- Will the threat actor be able to do it again?

Ransomware Impact - Exercise Part 2

Discuss with your previous group (~10 min):

1. What additional impacts on your organisation and constituents have come up in the last few slides?
2. Which are the top 2? Why?

What are the risks to keep an eye on?

“Risk to whom?” - Dan Geer

Risks Before Incident

Technical stuff

CPE, CVE, CVSS, EPSS, Credential Stuffing, APIs, Phishing, Malware, Botnets, exposed services etc, etc, etc,

Revenue

Brand

Country

Sector

Risks During Incident

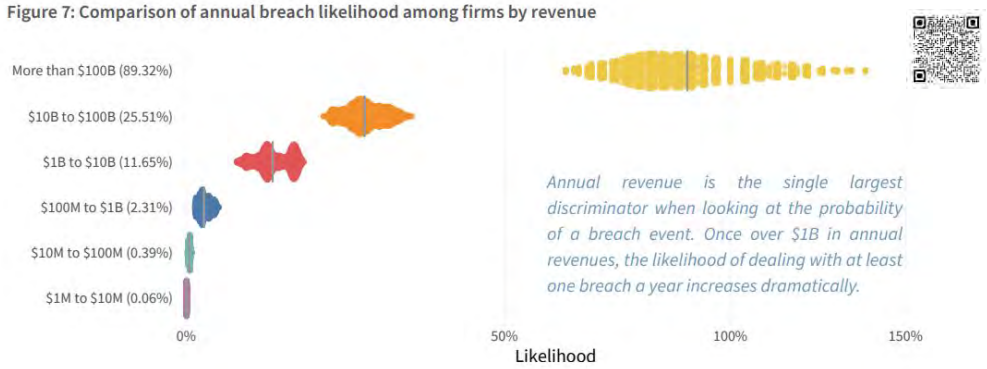
To the incident responders - burnout, bad decisions, communications, working shifts
To the CERT team - reputational, liability
To the victim executive team
To the victim Security Team
To the victim IT team

To the ransomware affiliate
To the negotiator
To the ransomware group

For an enterprise

- Most groups start their demands at 1-10% of a company's annual recurring revenue (ARR)
- Can be negotiated down 50% if you're lucky

⇒ **?% likelihood x 5% of ARR is a good idea of just the financial impact of the ransom**



For an enterprise

- Add the lost revenue from being offline for 2 weeks
- Add 2 weeks of 12 work hour days multiplied by the number of people needed to rebuild your critical systems (~2x-4x your own IT staff)
- The Gordon-Loeb model suggests that you should spend about a third of the impact to prevent it

⇒ 1/3 x ?% likelihood x 5% ARR + lost revenue
+ employee/support costs
= rough budget goal for ransomware prevention for any business.

For a CSIRT/PSIRT/SOC

- Frequency depends on your constituency
- Severity depends on your constituency
- It is possible to predict roughly
- Check your history of events and project and/or contact the MSR-SIG to estimate it

Cyber insurance

- Ransomware is currently (2024) the largest loss driver in the insurance world
- Insurance can save a victim from going bankrupt
- Insurers increasingly demand proof of good cyber-hygiene
- Insures increasingly reluctant to pay ransoms

Insurance companies have a lever to promote better cyber security

#1 Targeting “analysis”

Imagine 100 victims of ransomware

79 are under 100M in revenue

21 are above 100M in revenue

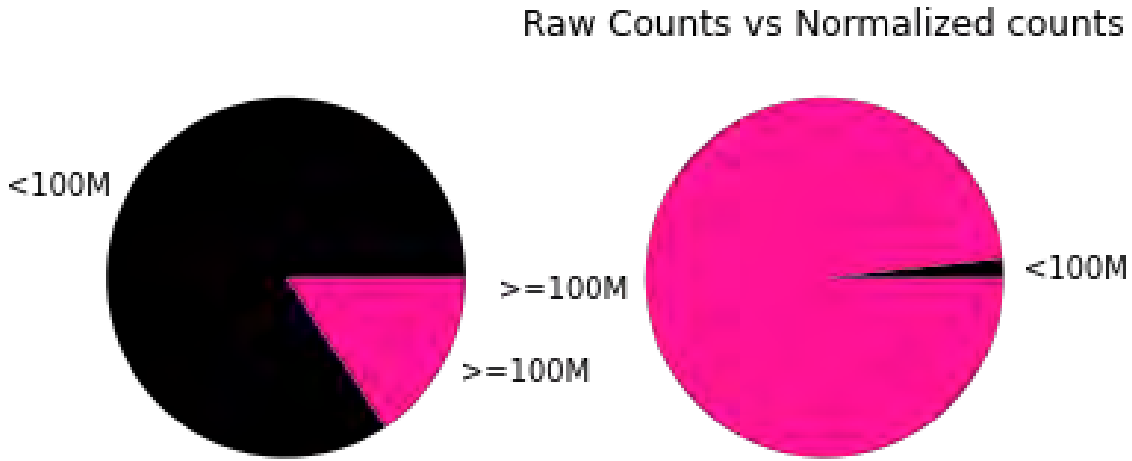
Clearly small business (<100M) are targeted right?

#1 mistake of targeting “analysis”

Imagine 100 victims of ransomware.

79 are under 100M in revenue / 15 Million Companies

21 are above 100M in revenue / 5000 companies



Who should be involved

Who is responsible?

1. Who/which team in your organisation is responsible for handling ransomware incidents?
2. Who else would be involved in such an incident?

Stakeholders Outside Your Team

When faced with a ransomware attack, it is important to get the following stakeholders involved in the response:

- Communication / Marketing / Public Relations for proactive communication
  - The attack could quickly become public knowledge, e.g. publication on the leak site
- Legal department for review and compliance with reporting requirements
- Senior management / C-level
  - Needed to decide which immediate actions can be taken (usually these have a significant operational impact), as well as to prioritise the recovery work according to what the business needs.

Without the support of these groups, technical staff will be overwhelmed and won't act in their and the organization's best interests!

Contacting Stakeholders

During a ransomware attack, your usual communication channels may be unavailable. What's more, key stakeholders are often unavailable, especially during an emergency or it happens after hours.

Prepare for it:

- Each role has at least one alternate, preferably two.
- For each key role, multiple ways to contact are specified, including not only work but also private phone numbers.

Challenge for the Entire Organization

During a ransomware attack

IT/OT works on this

Technology (IT & OT)	Incident Operations / Crisis Team	Legal	Communication
Understand the situation • Scope of attack • Objective of attack • Root cause Everyone wants and needs more information. Rebuild with more security controls.	Set up emergency operation • Enable limited operation • Establish crisis team Find a way back to normal • Take the business perspective • Stay focused Negotiations	Reporting obligations • Data protection laws • Contractual obligations • Stock exchange law Support negotiations • Check for sanctions Support activities • Public statements • Engage law enforcement	Map the stakeholders • Employees • Public • Customers • Partners • Shareholders Prepare and publish statements. Interact with the media. Monitor the conversation Rebuild trust.

Careful, this requires the involvement of the whole organization!

Resources: Measures

- https://www.cisa.gov/stopransomware/general-information
- https://www.cert.govt.nz/it-specialists/guides/how-ransomware-happens-and-how-to-stop-it/
- https://www.cert.govt.nz/business/guides/communicating-a-cyber-security-incident/public-communications-for-cyber-security-incidents-a-framework-for-organisations/

International Activities

International Counter Ransomware Initiative

- Initiated by the White House
- Country membership, nearly 50

FIRST Multi-Stakeholder Ransomware SIG

- Open to all!

Ransomware Task Force

- Mostly US private sector
- Initiated by the Institute for Security and Technology



Photo by Mathurin NAPOLY / matnapo on Unsplash

Preparation for Ransomware Attacks

Challenge for the Entire Organization

Prepare for a ransomware attack

IT/OT works on this

Technology (IT & OT)	Incident Operations / Crisis Team	Legal	Communication
• Practice incident scenarios • Plan, implement, and test security controls • Plan and test recovery • Run through possible scenarios with other business units (to increase awareness)	• Prepare and practice crisis management • Define recovery priorities • Prepare checklists • Define when and if the payment of the extortion/ransom is considered	• Clarify legal framework in advance • Prepare checklist for reporting obligations • Prepare reporting templates • Define reporting timelines	• Define who communicates with whom • Define communication timeline • Prepare statements for common scenarios

"It is IT's problem" does not hold true!

About recommending backups

We recommend backups:

But forget to say what to backup…

- Network configuration
- Identity management
- Payroll
- Credentials
- Safety Data*
- ERP

They also need to be tested/used/offline

If you look at leak data in bulk, most of it has backups in it. So we have to be mindful backups are also targets and a useful signafier of 'sensitive data' to a threat actor

Signed backups are ideal as they can demonstrate no corruption.

Multiple media is good too, in case one method fails.

How long does it take to restore

The number one cost to companies DURING the incident is downtime. So knowing your backups will take X long to restore is part of your key incident response plan.

Especially in situations where this is compared to the restoration time of the decryptor.

Ransomware Resistant Backup System

Threat actors may prevent effective recovery by compromising the **integrity** of your backups.

Prevent any (short-term) deletion or modification of backups once they have been created. Possible approaches (may need to be combined):

- Write Once Read Many (WORM) Backups
- Offline backups, e.g. tape cartridges outside of a tape drive
- Immutable cloud backups with unchangeable retention policy
- Delayed deletion or alteration of backups without a digital bypass path

Ransomware Resistant Backup System

Threat actors may deny access to backups, preventing effective recovery by compromising the **availability** of your backups.

Make sure you can always access your own backups:

- Prepare an emergency access account / break glass account
- Prepare for offline, i.e. physical, access to your backups

Ransomware Resistant Backup System

Threat actors may force the storage of corrupted or infected backup data. This could make both integer and clean backups unavailable.

Backups should be stored for a retention period appropriate to the **organisation's risk appetite**, and the integrity of backups should be monitored and tested regularly.

- Backups should be kept for a fixed period of time rather than a number of backups.
- Retain multiple backups of a system or of data, i.e. keep a version history.

Ransomware Resistant Backup System

It may be easier for a threat actor to attack a backup system than the actual systems or data.

- If backups are encrypted, make sure the key cannot be deleted or changed.
- Backups must meet the same security requirements as the systems or data they store.
- Monitor your backups and trigger alerts in case of significant events:
  - Significant changes, e.g. non-automatic deletion or modification
  - Execution of privileged operations

Ransomware Resistant Backup System

Scenarios to think through to identify problems in your current backup approach:

- Could a threat actor compromise the integrity of your backups by taking over an IT administrator's endpoint?
- What if the threat actor gains domain admin rights or root access?
- How do you access your backups when all of your organisation's existing IT systems and assets are unavailable?
- How would we do a rebuild of our core & critical infrastructure from a backup?
  - How much time will it take?
  - Who has the necessary knowledge?

Resources: Ransomware Resistant Backups

- https://www.ncsc.gov.uk/guidance/principles-for-ransomware-resistant-cloud-backups
- https://www.nccoe.nist.gov/data-integrity-identifying-and-protecting-assets-against-ransomware-and-other-destructive-events

(Opinionated) Measure Overview

- Write Once Read Many (WORM) or offline backups
- Create, maintain, and regularly exercise a (basic) incident response plan
- Use phishing-resistant multi-factor authentication
- Protect your endpoints / networks with current detection & response products
  - Make sure to monitor them!
- Reduce your cyber attack surface
  - Internet facing systems / services
  - Harden end user systems and key services (e.g. IAM)
- Vulnerability & patch management
- Observe current ransomware trends and apply lessons learned

Resources: Measures Against Ransomware Attacks

- https://www.cisa.gov/stopransomware/general-information
- https://www.cert.govt.nz/it-specialists/guides/how-ransomware-happens-and-how-to-stop-it/

Detection, detection, detection

Canary Tokens
Honeypots
Detection Engineering:

- Yara: https://github.com/Yara-Rules/rules
- SIGMA: https://github.com/SigmaHQ/sigma
- IDS
- XDR

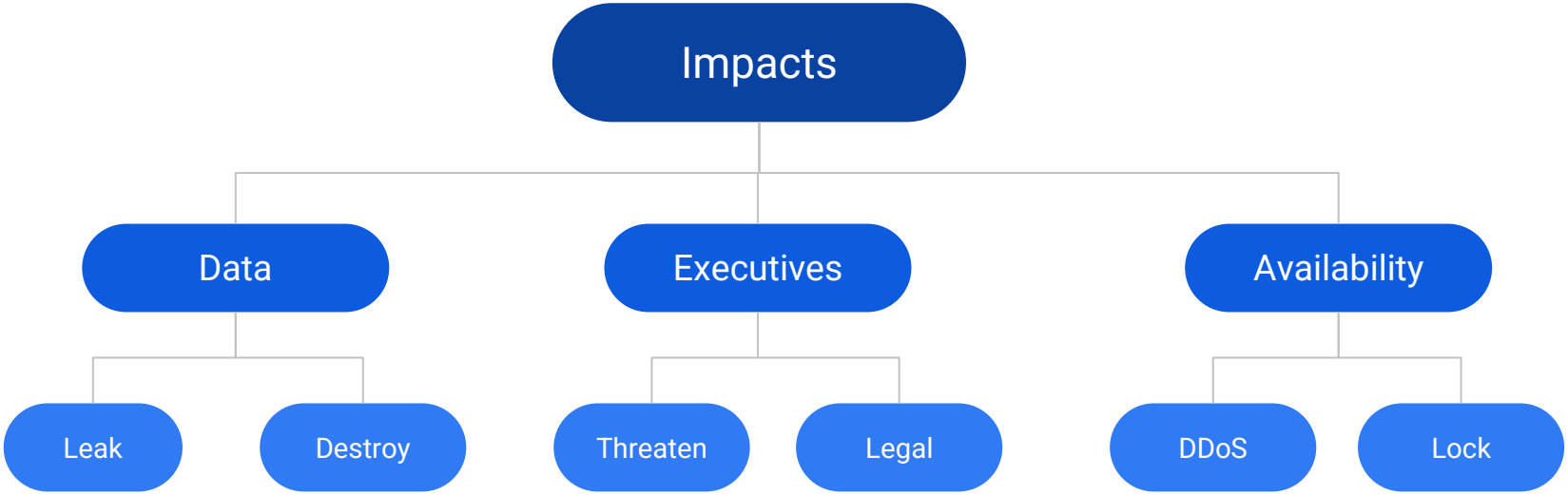
Log Files
Emails

*Note to IR; Sometimes the data is still in detection systems and the victim doesn't know it. Ask them about their detection systems.

Remember This Slide?

Technique ID	Technique Name	Tactic	Count from CTI	Mapped Data Components	# Sigma Analytics	# Atomic Tests
T1486	**Data Encrypted for Impact**	Impact	50	6	10	5
T1082	**System Information Discovery**	Discovery	30	4	14	24
T1083	**File and Directory Discovery**	Discovery	29	3	17	6
T1490	**Inhibit System Recovery**	Impact	23	5	18	9
T1059.001	**PowerShell**	Execution	20	5	183	22
T1047	**Windows Management Instrumentation**	Execution	19	3	40	10
T1489	**Service Stop**	Impact	17	7	9	3
T1112	**Modify Registry**	Defense Evasion	16	6	65	44
T1562.001	**Disable or Modify Tools**	Defense Evasion	16	6	77	38
T1059.003	**Windows Command Shell**	Execution	14	2	21	5
T1190	**Exploit Public-Facing Application**	Initial Access	14	2	80	0
T1133	**External Remote Services**	Persistence, Initial Access	13	3	7	1
T1021.001	**Remote Desktop Protocol**	Lateral Movement	13	4	14	3
T1018	**Remote System Discovery**	Discovery	13	4	15	20

Don’t just think about encrypted impacts





Darknet & Ransomware Groups

Photo by benjamin lehman on Unsplash

Surface, Deep & Dark

Surface Web

- Web content that is readily available and searchable with standard web search-engines
- Surface web (World Wide Web) runs on the “clearnet”

Deep Web

- Part of the World Wide Web that is not indexed by standard web search-engines
- Hidden behind access controls, only accessible with specific URL/IP addresses, etc.

Surface, Deep & Dark

Dark web

- World Wide Web content that exists on “darknets”
- Darknets are usually overlay networks that use the clearnet (Internet)
- Best known darknet: Tor (The Onion Router)

Tor

Tor is free and open-source software, mostly financed by the CIA that enables **anonymous communication**

- Using Tor as a user protects your privacy by hiding your location, and protects you from network surveillance and traffic analysis.
- So called “Onion services” provide the same anonymity to services, e.g. websites.

Be careful, just using Tor you or your service are not necessarily anonymous. See: https://support.torproject.org/faq/staying-anonymous/

Stay Safe & Secure

Even with Tor you leave traces behind

- Server knows which URLs were visited
  - Be careful with URLs that contain secrets or are not well known
- Software (browser) may be vulnerable or misconfigured, allowing some degree of deanonymization

If you really want to be anonymous, take the time and make the effort to stay hidden!

Use at least a virtual machine with a current and AV-equipped operating system and the official Tor browser.

Darkweb & Ransomware Groups

Most leaksides are Tor hidden services

- To interact with the threat actor you need to visit their site in the Tor network

Darknet - Exercise

Browse the darknet with TOR (~10 min)

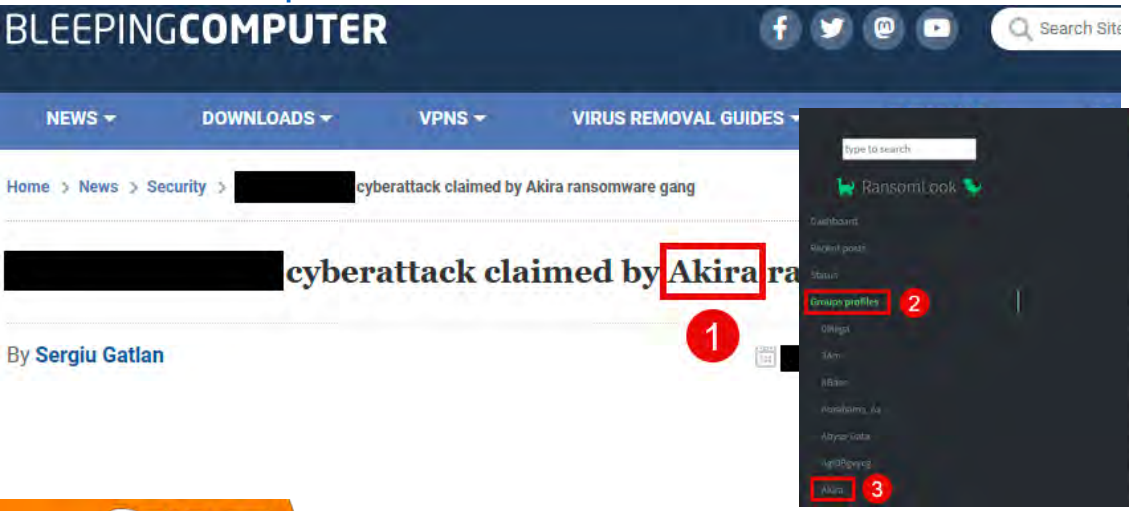
- Can you find data leak blogs?

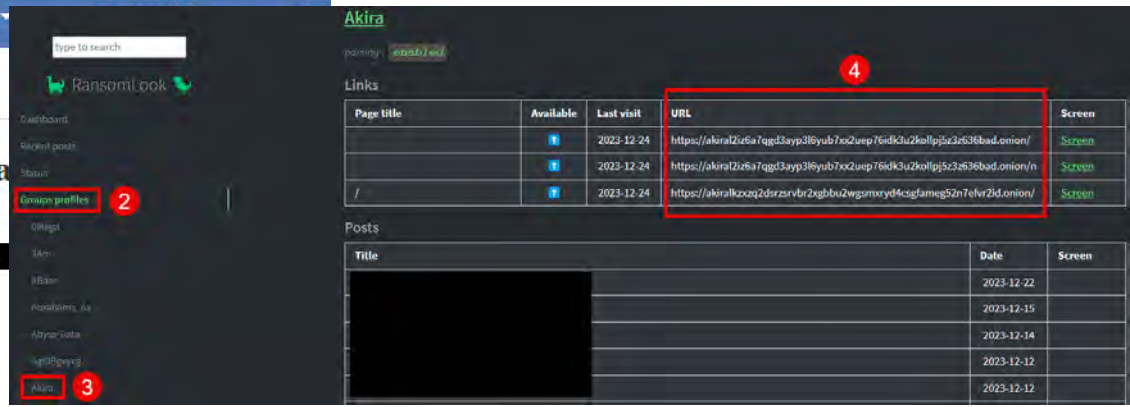
Visiting a Site on the Darkweb

Step 1: Get the Onion Address

Get the `.onion` address

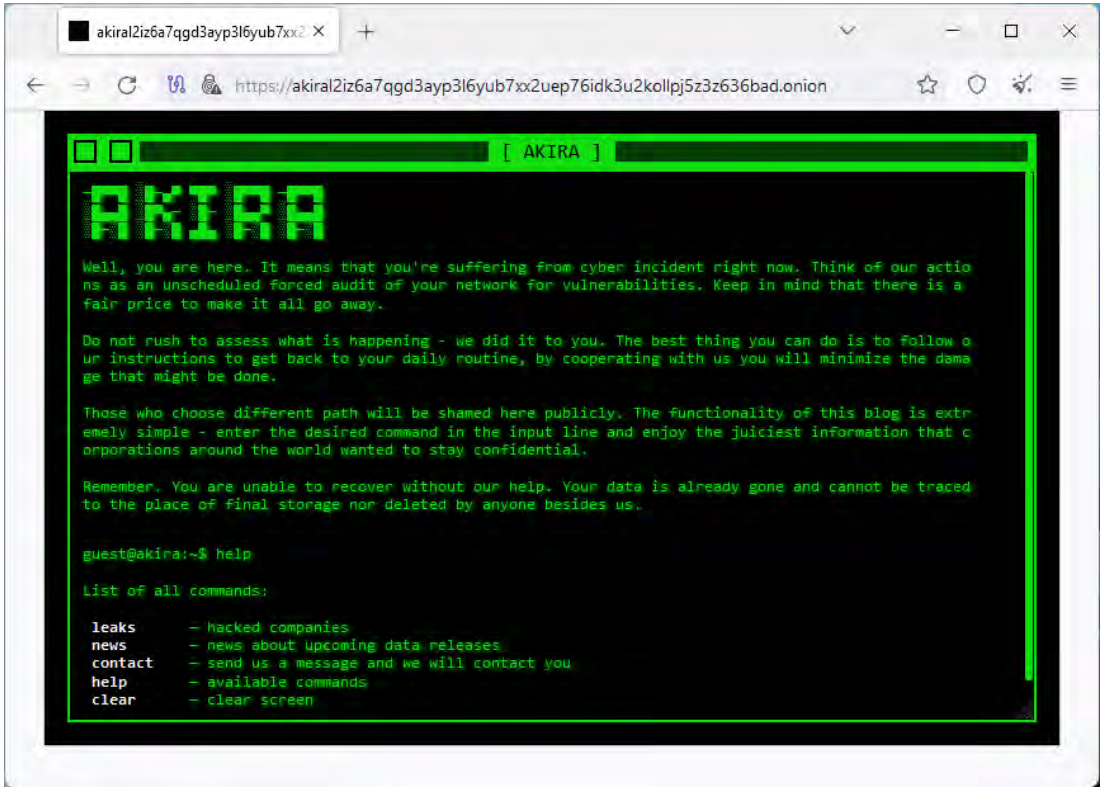
- From the ransomware note
- Search for their address in the clearweb, e.g. https://www.ransomlook.io/





Visiting a Site on the Darkweb

Step 2: Visit the site with Tor Browser



Incident Response Management
Ransomware Specific Lessons

General Guidance

ISO/IEC 27035 is a highly recommended source of reference.

Running through an attack in your head, or around a table with your colleagues, will help you identify what is missing in your organisation and incident response management so that you are prepared for an incident.

Reach out and talk to your peers!

Stakeholders Outside Your Team

When faced with a ransomware attack, it is important to get the following stakeholders involved in the response:

- Communication / Marketing / Public Relations for proactive communication
  - The attack could quickly become public knowledge, e.g. publication on the leak site
- Legal department for review and compliance with reporting requirements
- Senior management / C-level
  - Needed to decide which immediate actions can be taken (usually these have a significant operational impact), as well as to prioritise the recovery work according to what the business needs.

Without the support of these groups, technical staff will be overwhelmed and won't act in their and the organization's best interests!

Contacting Stakeholders

During a ransomware attack, your usual communication channels may be unavailable. What's more, key stakeholders are often unavailable, especially during an emergency or it happens after hours.

Prepare for it:

- Each role has at least one alternate, preferably two.
- For each key role, multiple ways to contact are specified, including not only work but also private phone numbers.

Keep it ready

Don't forget that during a ransomware attack, your entire technical infrastructure is likely to be unavailable!

- Keep your incident response plan and other supporting documentation physical or offline
  - Print it regularly or store it offline on removable media
  - Make sure more than one person has a copy in case some of you are away
- Train on a regular basis based on your incident response plan

Be First to Report & Don't Forget It

A growing number of organisations are required to report incidents. Make sure that the obligation to report is checked as early as possible and that it is carried out on time.

- Make it part of your incident response process and get the right people involved at an early stage.
- Threat actors may report you to the authorities to increase pressure or embarrass you.
- If you do have a cyber insurance policy, early notification may be necessary for your coverage and could lead to valuable third party support.

Response to a Ransomware Attack



Photo by Sandro Gautier on Unsplash

Incident Response Process

Incident Response Processes

There are several incident response processes. Overall they are very similar. Use the one that meets your needs or fits well with your other processes and policies.

- FIRST Incident Response Process
- SANS Incident Response Process
- NIST Incident Response Life Cycle (see NIST SP 800-61)
- ISO/IEC 27035

FIRST


Preparation
Postmortem Analysis
Detect
Triage
Respond
Analyze
Incident Response Cycle

Preparation

Prepare/maintain technical and organizational framework

- Establish guidelines, principles, rules, etc.
- Define process and procedure for incident management
- Communication plan: internal, external, partners etc.
- Define Computer Incident Response Team (CIRT)
- Provide necessary tools
- Train

Detect

Identify information security incidents

- How can we be informed about a potential attack?
  - Affected employees
  - AV / EDR solution
  - SOC / CDC / MDR
- What are the needed sources of information?
- Logs, but which logs?
  - Firewall, Proxy, DNS
  - Endpoint Logs
  - Application Logs (e.g., email)
  - Cloud

Detect

Make sure this is the case:

- Employees know how and to whom to report unexpected behaviour
  - Often the service desk. Does the service desk know how to identify an incident?
- AV/EDR alerts are processed
  - Especially with human-operated ransomware, it's common to see multiple alerts where the AV/EDR successfully blocked an activity. Think about why it stopped! Maybe the threat actor found a malware or variant that is no longer detected?
- You are responsive to your SOC / CDC / MDR, especially if it is a managed service.

Analyse

To analyse, first make sure you have the necessary **visibility**!

- There is no investigation without data
- Do we have visibility across all environments and system types?
  - What happens on the servers?
  - What happens on the clients?
  - What happens on the network / perimeter?
  - What happens in the cloud?

Respond - Containment

Preventing the threat from spreading across the network ("stop the bleeding") and stopping communication with command and control.

- Immediate measures
- Measures based on analysis
- Preservation of evidence

Respond - Immediate Measures

- Identify and isolate/disconnect affected devices
- Disable/lock users and invalidate their sessions and tokens
- Interrupt threat actor's command & control channel
- Protect/isolate backups
- Reduce the likelihood of the threat actor regaining access
  - Deactivate external access (VPN, Citrix, etc.)
- Secure evidence, if necessary

Respond - Eradication

Elimination of the threat and its remains

- Clean up systems
- Checking the backups
- Vulnerability analysis

Respond - Eradication

Typically includes:

- Change (admin) credentials, invalidate Kerberos ticket (twice)
- Establish a clean environment for recovery
- Validate the backups (if available)
- Restore strategy (see later in this course)
- Identify and fix vulnerabilities
- Patch and harden systems

Respond - Recovery

Restoration of the normal state with as little negative impact as possible

- Restore from backup or rebuild systems
  - What is the right strategy?
  - In which network do we restore or rebuild the system?
- Reintegration into a interconnected environment
  - To which network do we connect (likely) clean devices?
- Observe (Detect)

Postmortem Analysis - Learn Lessons

Learn from the incident

- Have a Learn Lessons Meeting
  - Debrief what went well and what not so well
- Improve your security controls longterm
- Improve incident response

Incident Response Process in Practice

Step 1: Assembling your IRT

Assemble the incident response team (IRT) to deal with the incident, using internal and external resources as necessary

- Initial meeting: discuss what happened, set goals and priorities, share contact details etc.
- Provide them with at least one physical space in which to work
- Decide on a digital space to work in and a way to communicate digitally

Step 2: Immediate action

Take immediate action to reduce impact

- Isolate affected systems/networks
  - Stop Command & Control communication
- Disable affected accounts and revoke their sessions
- Protect/isolate backups and other key systems
- Preserve at least some evidence
  - Snapshot virtual systems
  - Put some of the affected systems aside and don't touch them

Step 2: Immediate action

The simplest approach for on-premises environments: Disconnect from the Internet.

- See if this is possible, at least for the first few hours.
- This will give you time to think, plan and act.

Assumption: It's a cyber attack, i.e. the threat actor is using the internet to launch the attack.

Step 3: Set organisational goals

Ensure from the outset that the response to an incident is in line with the organisation's objectives

- In most cases, the primary objective is for the organisation to be able to pursue its purpose again!
  - Careful, it should be able to do this in the long term without another incident.
- Prioritise based on the primary objective. Do nothing else.
- Understand the non-technical implications as early as possible. Make sure the right people are managing them.

Step 4: Collect evidence?

Decide how much digital evidence you want/need to collect, e.g. for legal action.

- Very dependent on the organisation
- It is common, especially in the private sector, not to collect evidence that can be used in court.
- Gathering evidence takes a lot of time in many jurisdictions ⇒ Handling the incident will take much more time and cost more

Step 5: Gain visibility

Gain visibility with standard security tools

- Run AV-Scans, YARA-Scans
- Deploy EDR/NDR
- Deploy digital forensics / incident response tooling, e.g. Velociraptor or GRR

Step 6: What happened?

Understand what has happened so that gaps in security can be identified and closed

- How did it get in?
- How did it spread?
- How did it persist?

Be careful not to spend too many resources/time on your investigations.

Keep the overall goal in mind. Focus on analysis that can add significant value to the response.

Day 2

Management

- Decide whether to negotiate/pay the ransom
- Preparation for mandatory reporting begins and first reports go out
- Establish an escalation process if the attack worsens
  - Have a plan B in case the current approach fails

Day 2

DFIR Analysis

- The objective is to identify IOCs & TTPs for containment & eradication
- Understand the scope of the attack and its impact, particularly in relation to sensitive data
- Find initial entrypoint

First week

Management

- Decide on the priority order for restoration
- Plan recovery

Analysis

- Make sure you have documented everything so far and continue to document
- Focus on identifying IOCs & TTPs → block/eliminate them (Containment & Eradication) → repeat ↻

End of first week

Eradication & Recovery

- Prepare clean and isolated environment for restore
  - Plan and implement additional security controls
  - Plan and begin monitoring the new environment for signs of compromise or similar.
- Finalize company-wide reset of secrets
- Start restoring/rebuilding critical systems

Incident Response Steps - Deep Dive

Analysis steps

1. Ransomware identification
2. Look for decryptors
3. Identify affected systems
4. Triage: focus on high priority impacted systems
5. Identify root cause/entry point

Goal: identify attacker activity and actions on objective

Analysis - Artefacts

Goal	Artefact
Identify the ransomware	• Read-me file: text, domain/url, name mentioned within the file, wallet address • Encrypted file extension
Determine the features and capabilities of the ransomware	• Exe-file of the ransomware (if already found) • Derive from identified ransomware and public information on it
Provide clues to infection time and origin, entry vector, lateral movement, possible data leakage, and potentially infected systems	• Image/log files of infected systems • Perimeter logs (firewall, proxy, DNS, etc.)

Analysis - Ransomware identification

Use Read-me file and encrypted file extensions, AV/EDR detection, or exe file of the ransomware if already found

- https://www.nomoreransom.org/
- https://id-ransomware.malwarehunterteam.com
- https://malpedia.caad.fkie.fraunhofer.de/
- https://www.ransomlook.io/
- https://www.bitcoinabuse.com/
- https://www.virustotal.com/

Analysis - Decryptors

Publicly available decryptors:

- https://www.nomoreransom.org/
- https://id-ransomware.malwarehunterteam.com
- https://www.emsisoft.com/ransomware-decryption-tools/

Analysis

Identify high priority impacted systems:

- Focus the investigation on high priority impacted systems and crown-jewels, e.g. Domain Controller, Microsoft Exchange, public cloud environment, and similar systems used by nearly everyone and everything
- First focus on the time around the encryption (e.g. creation time of the Read-Me and encrypted files) and AV/EDR detections to find IOCs.
- Use them to pivot and discover further IOCs.

Useful tools: Velociraptor, GRR, KAPE

Analysis - Affected systems and users

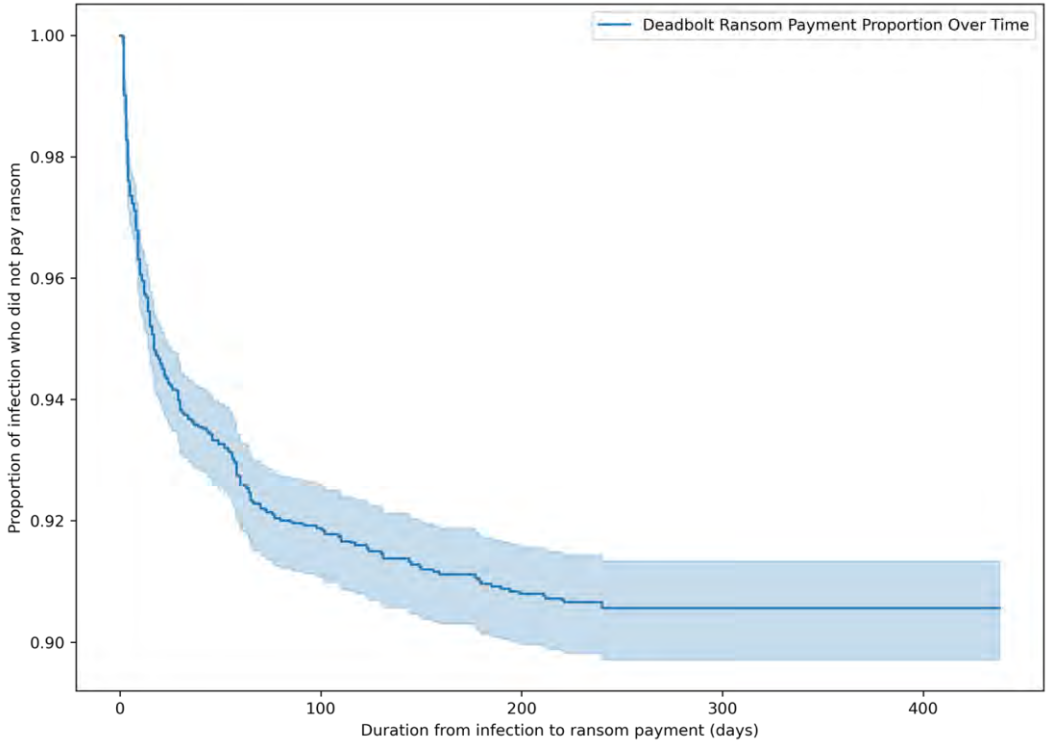
Identify affected systems and user accounts:

- Check owner of ReadMe files to find out affected user accounts and thus affected systems
- Find out affected systems by looking for IOCs with:
  - AV/EDR scans
  - Thor (Lite)
  - Chainsaw
  - Hayabusa
  - By hand

Deadbolt - Exercise (1 hour)

3 Malware File

? BTC addresses



Analysis - Disclaimer

In this training, we focus on Windows' artefacts as it's the most common OS used.

Of course, ransomware also targets Unix, ESXi, OT/ICS, Cloud, etc.

Analysis - Artefacts of high value

- Account activity
- Program execution
- Persistence
- Lateral movement
- Network communication

See the SANS Hunt Evil (the blue poster) and SANS Windows Forensic Analysis poster (the red poster).

Analysis - Network Communication

The aim is to find command and control communication and lateral movement. Some hints:

- Suspicious ports
  - Unusual port numbers on the listening side?
  - Protocol and targeted port mismatch
- Suspicious or unexpected connections
  - Connections to known bad IP addresses
  - Tor or Tor2Web requests
  - DNS requests for unusual domain names
  - Unexpected workstation to workstation communication
  - From/to regions outside the business radius
  - Communication outside usual working hours

Analysis - Network Analysis

- Full-packet capture (pcap)
- NetFlow
  - Contains 5-Tuple information (source IP, destination IP, source port, destination port, protocol used) + bytes transferred
- Useful tools:
  - Tcpdump
  - Wireshark/tshark
  - Zeek
  - Snort
  - Suricata

The Recovery Phase

The easy part, right?



Photo by Shivendu Shukla on Unsplash

Be aware why we perform recovery!

Overall objective: return to normal with as little negative impact as possible

Careful, do the recovery from your business point of view! It is important for the organisation to be able to pursue its purpose again.

Typical recovery goals

We want to get back to business!

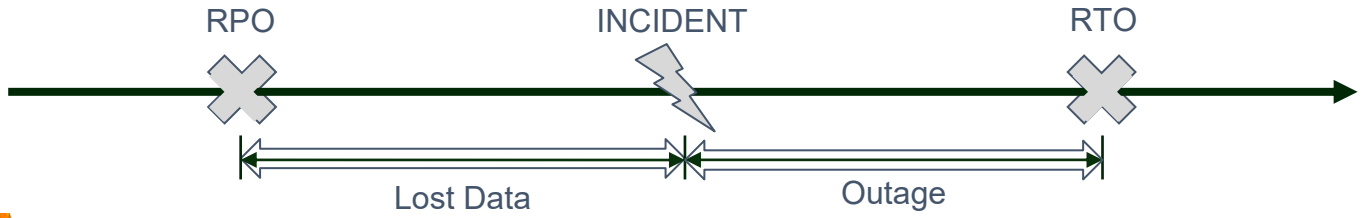
- Restore a clean IT infrastructure

Get back to normal as quickly as possible

- in BCM think of the Recovery Time Objective, RTO

Prevent any business data loss

- in BCM think of the Recovery Point Objective, RPO



Be aware of the challenges

Our infrastructure was successfully compromised

- Is our backup infrastructure even available?
- What if we re-enable or reconnect the backup infrastructure and it is destroyed by the threat actor?
- If we just restore everything to the way it was, what stops another compromise?
- What if the backup systems were also compromised?
  - Can we trust the backup systems itself?
  - Can we trust the backups and the data within them?

Be aware of the challenges

We are quickly talking about terabytes of data

- Where is the data located?
- How can we transfer the data?
  - How fast is your network?
  - Do we even have network connectivity?
  - Data drive shipping could be faster and more reliable
- This will take some time…

Be aware of the challenges

How do we properly restore a particular system?

- What other systems does it depend on? They must be recovered first
- Do we remember how we configured this system? It was built a long time ago…
- Do we have software, drivers, licence keys?
- How do we find out if a recovery was successful?
  - Who can test and confirm it for us?

The number of affected systems matters!

Scenario 1: Systems affected can be counted on one hand

Example case: Individual end-user systems must be considered compromised because their users fell for a phishing attack.

Typical approach for recovery:

1. Disconnect affected device from any network
2. Transfer necessary data from the infected device to an external storage medium
3. Set up a fresh device
4. Run antimalware scan on the data
5. If nothing is found, transfer data to the new system
6. Destroy old system (logically), e.g. completely format built-in storage
7. Done

Scenario 2: Significant number of devices affected

Example case: An entire network with its devices has been compromised, for example by a ransomware attack.

Contains the same elements as scenario 1 but is much more complex and requires a well-thought-out strategy!

From here on, we will assume this scenario and thus automatically also talk about scenario 1 and how to address the simpler case.

Prepare the recovery environment

Step 1

The existing environment

The compromised environment already exists

- It got compromised
- All our (potentially) affected devices are in this environment
- All our (potentially) affected logical objects (e.g. user accounts) are in this environment

Important:

- We do not trust this environment
- Everything that it touches might be/get compromised
- We assume the threat is still in this environment

The new environment

This environment will replace the compromised environment

- Must stay clean
- Objects are only connected/added if they have been classified as clean and secured
- Must be more secure than the compromised environment

Important:

- We must keep an eye on the environment and detect if something unexpected happens
- Visibility, detection and protection is key

The environment in between

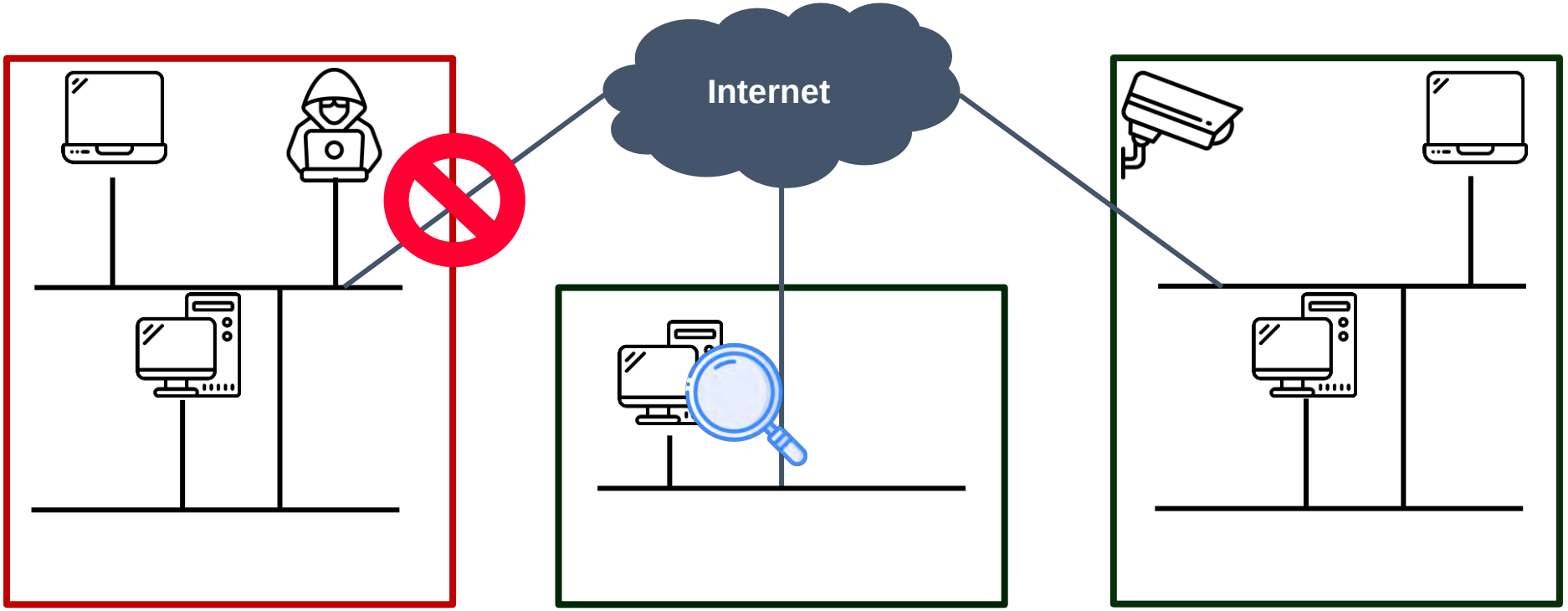
Think of it as a DMZ between the infected and clean environment

- Here we check devices, data and other object for indicators of compromise before they may move into the clean environment
- Here we prepare backups to be restored in the clean environment
- Here we cleanup devices, if there is no other way

Important:

- Internet access only as far as necessary to perform the tasks
- No network connectivity between the three environments
- No network connectivity between devices within the network

The three environments for recovery



Icons created by Smashicons from Flaticon

Decide on a recovery approach

Step 2 for every device

Option 1: Complete Restore from Backup

You have a full backup of a system

- Operating system, business software, configuration and all the business data
- Common for virtual machines and appliances

Great! Restore is (theoretically) easy

- Prepare the hardware and/or virtual environment
- Restore the backup and start the restored system

Option 1: Complete Restore from Backup

However, some open questions remain

- Is the restored system secure and clean?
- Which restoration point (backup) to use?
- How much time will it take and what dependencies need to be taken care of first?

Option 1: Complete Restore from Backup

1. Make sure you do protect your backup first (we will discuss it later)
2. Restore the system in the Test Environment
3. Improve the system's security
4. Make sure the system has no indicators of a compromise
5. Move the system into the clean environment

Option 2: Partial Restore from Backup

You have a **partial backup** of an affected system or it's data

- Common for complex systems where, for example, the data is backed up but not the entire environment with all its components
- Also, valuable when we have a full backup
  - We do not trust the whole backup, just parts of it (usually business data)
  - We want to restore just part of the backup, the one that is likely safe

Same questions remain as with a full backup

Option 2: Partial Restore from Backup

1. Make sure you do protect your backup first (we will discuss it later)
2. Prepare data within the Test Environment
   a. Restore the system in the Test Environment
   b. Extract the necessary data to another system (often an external storage medium)
   c. Make sure the selected data has no indicators of malicious data
3. Rebuild the system in the Clean Environment
4. Improve the system's security
5. Move the data from the Test Environment to the new system in the Clean Environment

Option 3: No Backup Available, Greenfield Recovery

You have **no backup** of a system

- Recommended approach: Build it from scratch

Recovery Approach

1. Rebuild the system in the Clean Environment
2. Improve the system's security

Option 4: Cleanup a system

You have **no backup and building from scratch is not realistic**

- Must check for any indicator of infection or malicious content
- If an indicator of compromise is identified on the system: please, rebuild from scratch
- If no indicators identified: Dangerous approach, can introduce malware into the Clean environment

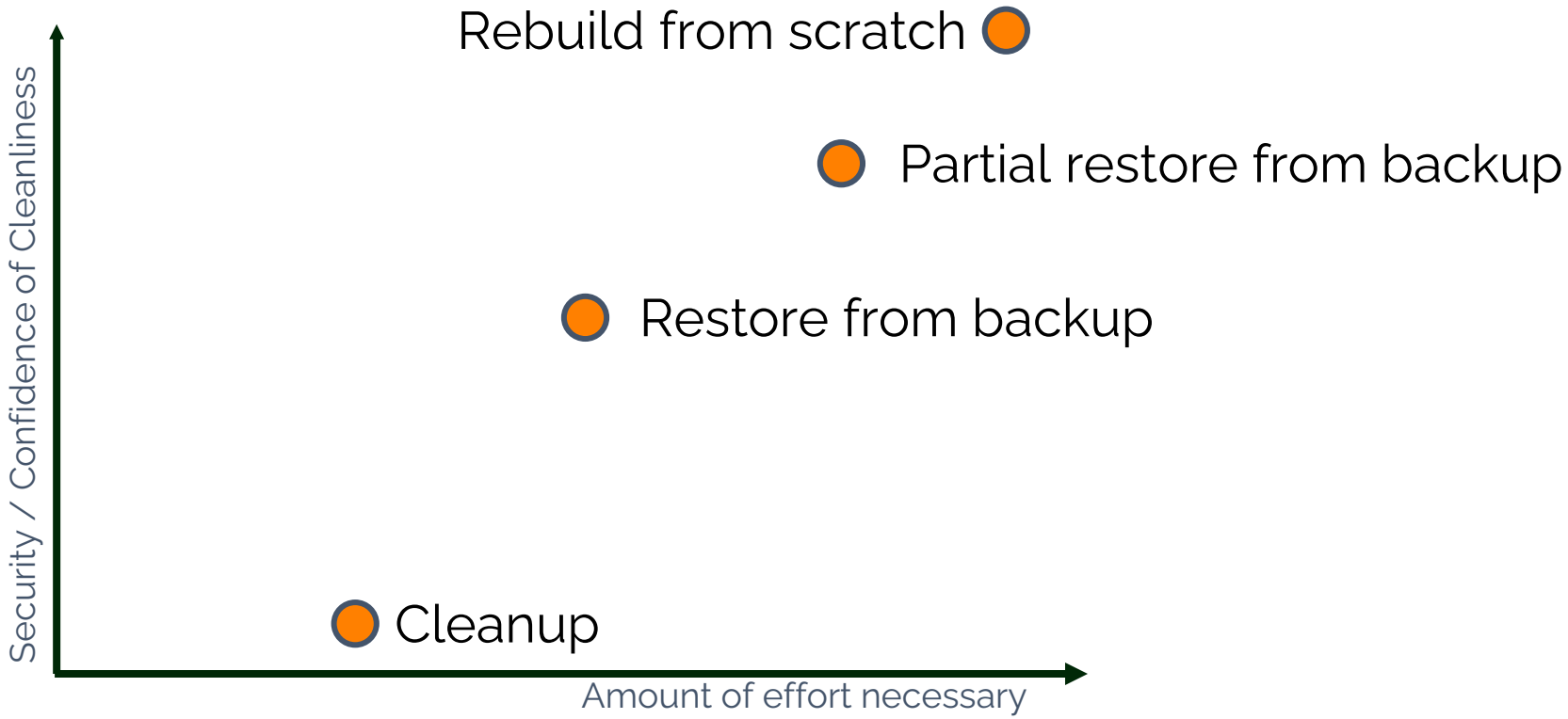
Be aware:

- It is mostly done to save time
- Poses a realistic threat to recovery efforts
- Should be considered only at the beginning for particularly critical systems

Option 4: Cleanup a system

1. Remove any known malware and indicators of compromise from system while it is still in the Compromised Environment
2. Move system into the Test Environment
3. Check system again for any indicators of malicious data and remove them
4. Improve the system's security
5. If possible, do a final check for malicious data on system
6. Move system into the Clean Environment

Options - From a Security Perspective



Option 5: Decrypt System

1. Create a backup copy of all data and store it separately from the network to have a second chance in case of complications during decryption.
    - For e.g. VMs, a snapshot can simply be created and copied away.
2. Optional: After receiving the decryptor (publicly available or after ransom payment), scan it and verify its functionality.
    - The check is ideally done in a sandbox, while the functionality can be verified in a VM with a separate network by decrypting some files.

Option 5: Decrypt System

3. Decryption can then take place directly on the affected systems or in a VM.
   - In the first case, the decryptor is executed directly on the systems.
   - In the second case, the encrypted data to be restored is first copied away and then only the data and not the entire system is decrypted.

The procedure here depends to a certain extent on the strategy chosen with regard to returning to normal operation.

You have the option of

a) completely rebuilding all systems (recommended) or
b) decrypting and disinfecting.

Option 5a: Decrypt System + Rebuilding

If complete rebuild of all systems:

1. Either decrypt affected systems or data only.
2. Extract data and scan for malware with AV/EDR solution.
3. Migrate data to the new environment

Option 5b: Decrypt System + Disinfecting

1. Decrypt affected systems (ideally separate from the network).
2. Perform a full scan of all systems in the entire IT environment with the AV/EDR solution.
3. Scan systems with e.g. Microsoft Safety Scanner and Thor-Lite for remnants of the ransomware infection. Clean up findings. The scan results can provide information about the entry vector and possible vulnerabilities in the system.
4. Update and harden systems and take basic measures to prevent reinfection.
   a. Change all passwords (enforce organisation-wide, service, user, domain admin passwords, Kerberos ticket, etc.).
   b. Enforce multi-factor authentication (2FA) at least on all interfaces to the outside world.
   c. The CIS benchmarks can be consulted as an aid to system hardening.
   d. A security scan/port scan can be performed internally and externally to identify vulnerable and accessible services.
   e. PingCastle can be used to check the health of the Active Directory.
5. Return to normal operation, reconnect systems to the network, etc.

Open Questions on Backups

- Do we have backups?
  - Full or partial?
- Is the restored system secure and clean?
- Which restoration point (backup) to use?
- How much time will it take and what dependencies need to be taken care of first?

Keep an eye on the Clean Environment

Step 3

How to protect the Clean Environment?

Use Endpoint & Network Detection

- Every endpoint is protected by an EDR
- Network Intrusion Detection System is in place
- In the environment, block and monitor for known Indicators of Compromise (IOCs), which could indicate an infected system
- Regularly check for any alerts in all of the deployed security products!

How to protect the Clean Environment?

Use additional security products for detection, visibility, and protection

- DNS based security products (e.g. Quad9, Cisco Umbrella)
- Start building up a Security Operation Center with Information Security Event Management services
- Deploy multi-factor authentication (MFA)

How to protect the Clean Environment?

Reduce your attack surface

- Limit accessibility to services from the internet
- Assess the security of your Active Directory configuration and improve it
- Perform vulnerability scans and mitigate critical vulnerabilities
- Patch systems

If necessary, perform regular Threat Hunts based on known threat actor and malware activity.

Generally speaking: Ensure basic protection that was probably forgotten in the past.

Finalize the recovery

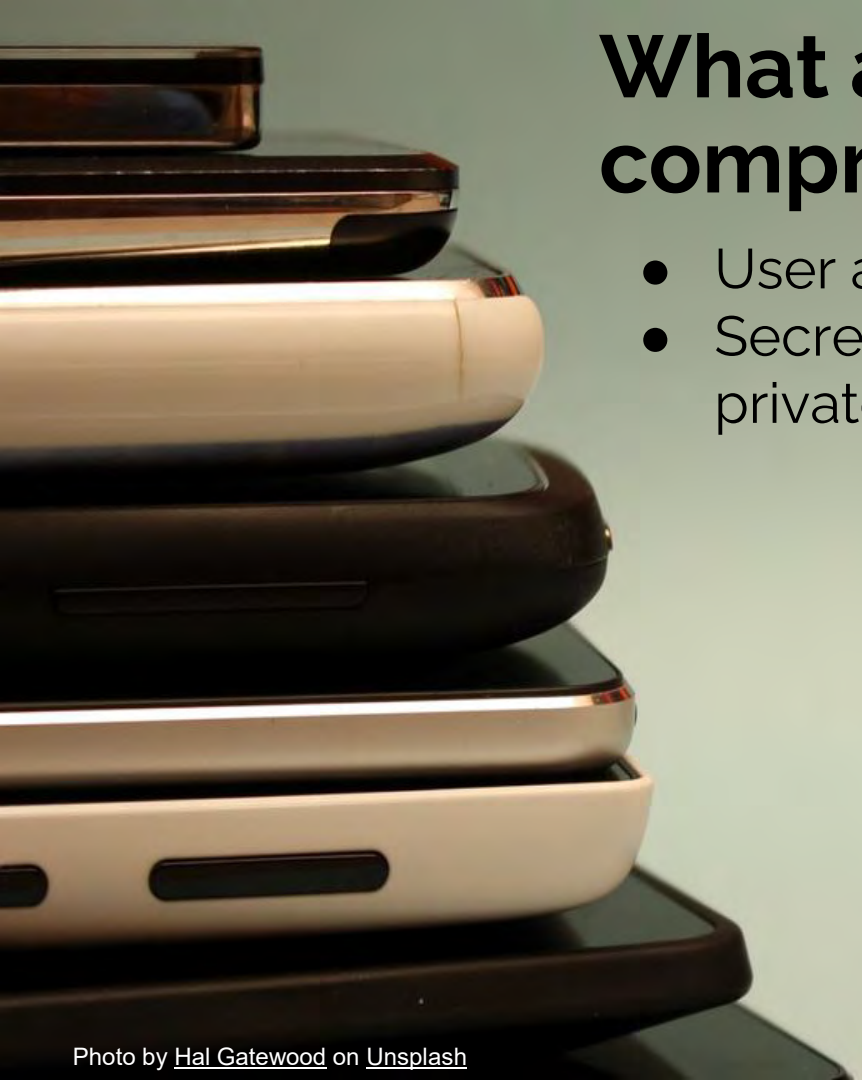
Step 4

The last steps

Shut down and remove environments and systems that are no longer needed

- Shut down the Compromised Environment
- Shut down the Test Environment
- Ensure that all potentially malicious or compromised devices/objects are completely removed and cannot be accidentally reconnected to the Clean Environment

Make security a habit: Any additional security measures for the Clean Environment should be operationalized.



What about all the other compromised objects?

- User and service accounts
- Secrets: passwords in configuration files, private keys, tickets, tokens, …

Photo by Hal Gatewood on Unsplash

It really depends on the object

Accounts and any kind of secret

- Reset it again (should have already been done during containment)
- Use the chance to improve its security
  - Use current security functions & algorithms
  - Make them harder to guess
  - Check if there is a more secure way to keep/use them
  - Invalidate any open session

For everything else it depends on the particular object and event

Details that we have not yet clarified

Protect your backup

If a working backup exists, protect it!

- Very first step, before you use it for recovery
- Make a copy of the backups and keep it stored offline or in a cloud environment with a retention policy
- Alternatively, implement security measures to protect the backup from compromise and destruction

Checking in test environments

Goal: Make sure that the system is probably trustworthy, and data does not contain anything malicious

Usually a four-step approach:

1. Install an Endpoint Detection & Response (EDR) product on the system to check or the system used to check the data
2. Check for known Indicators of Compromise (IOCs)
3. Perform a full scan with an antivirus software (ideally with the installed EDR product)
4. Perform a YARA-scan and check the results for true positives

Do the restored systems work at all?

Identify individuals outside of IT who can test systems for functionality and verify that all data is likely to be present. This frees up time for IT.

What can we prepare today?

Ideally start with Business Continuity Management (BCM)

Otherwise, it helps to prepare the following:

- Know the most critical systems for your business
- Know their dependencies
- Create priority list for recovery
- Prepare recovery plans and playbooks (follow your priority list)
- Plan and exercise how the additional networks for the Test and Clean Environments are created

Generally: Do a tabletop exercise, identify weaknesses and improve on them.

Ransom Negotiations



Photo by Headway on Unsplash

Their goal is to get paid

Ransomware operators have an economic interest

- They have already invested resources and want to recover their costs and make a profit
  - Time spent to perform the attack
  - Costs for the storage to store the stolen data, malware, access, operation of the darknet site, etc.
- Making the attack and stolen data public has little economic value

They want to negotiate with you because of that!

Ways they will try to achieve their goal

Exerting pressure is their most powerful weapon

- Threat of publication
- Threat of contacting customers, partners, etc.
- Time pressure (countdowns, limit time for reply)
- Inconsistent communication style
- Threat of further attacks (e.g., DDoS)
- Threat of leaving incriminating data on your devices

Prepare for and expect these situations, and try to remain calm in the midst of them.

Be the first to report

If reporting is necessary, ensure that the incident has already been reported

- Make sure that the threat actor cannot pressure you with it

Even if you are not required to report it, it may still be beneficial to make some information on the attack public in order to alleviate pressure.

You might be lucky

Sometimes you can use the ransomware group's own rules against them!

- Read their own rules and check if they claim not to target your sector, e.g. medical facilities, schools, etc.
- Pointing out that they are hitting someone they claim not to be hitting could lead to a quick release of the decryptor without payment.

Our recommendation

Do NOT pay!

Do NOT pay

- We do not want to encourage and support the attackers
- No guarantee to recover the data
- No guarantee that the leaked data will be deleted
- There could be legal consequences
- This does not remove the attack vectors! A new attack could occur via a backdoor

The End

You have been empowered!