Insight in an
Advanced Ransomware Threat

Edwin Weijdema

Global Technologist, Product Strategy

@Viperian www.vmguru.com

CYBER SECURITY COALITION.be

Dramatic increase in frequency and severity of Cyber Attacks!

Data is the life blood of any organization!

© 2021 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Data is:

Critical

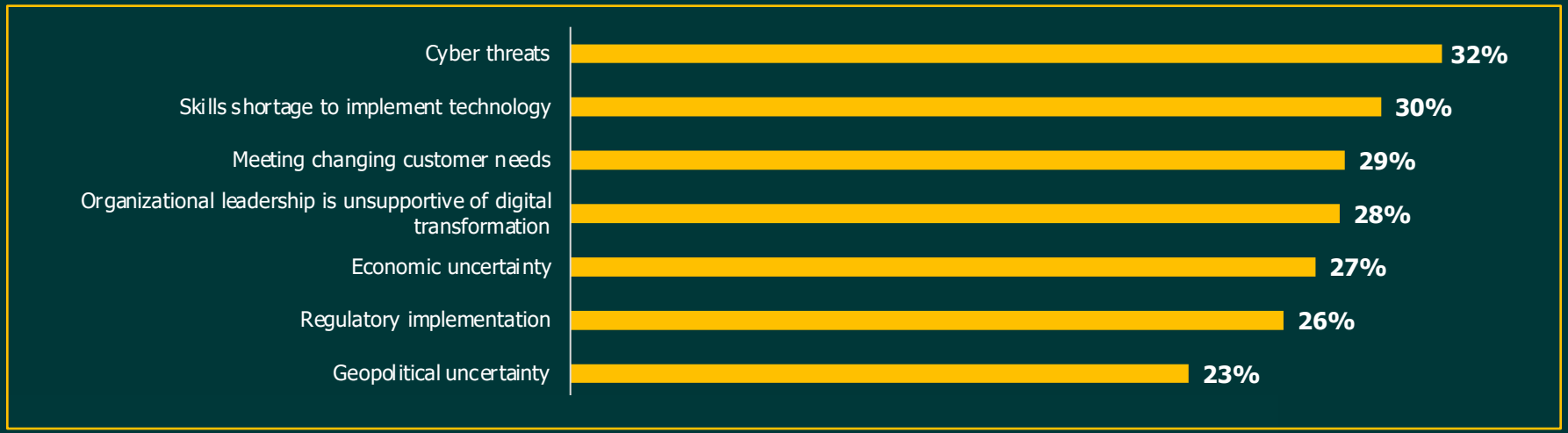
Growing

Sprawling

© 2021 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

What challenges do you anticipate in 2020?

Which of these challenges do you anticipate will impact your organization within the next 12 months? (n=1550)



Source: Veeam 2020 Data Protection Research

© 2021 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Now what?

Pay **Ransom**

Both are incredibly unfortunate outcomes

Lose **Data**

© 2021 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Cyber Attacks

Actions

- Data encryption
- Data deletion
- Data stealing
- Data leaking
- Device locking

Tools

- Phishing
- Malware
- Ransomware
- Denial of Service

© 2021 Veeam Software.

Disasters happen all the time

Earthquakes

Storms and floods

Accidental Fire

Malicious attacks from inside

© 2021 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

RANSOMWARE

© 2021 Veeam Software.

Some Ransomware Facts

- An attack in 2020 every 14 sec – estimate in 2021 is every 11 sec
- Average payment $180,000 (mainly bitcoins)
- 98% decryption tool delivered after payment
- 97% succesfully working decrypter – 3% loss of data
- Average 16 days downtime
- 84% via RDP and Email phishing
- Companies with 600+ employees

Source: http://coveware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate

© 2020 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Insights in an Advanced Ransomware Threat

© 2020 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

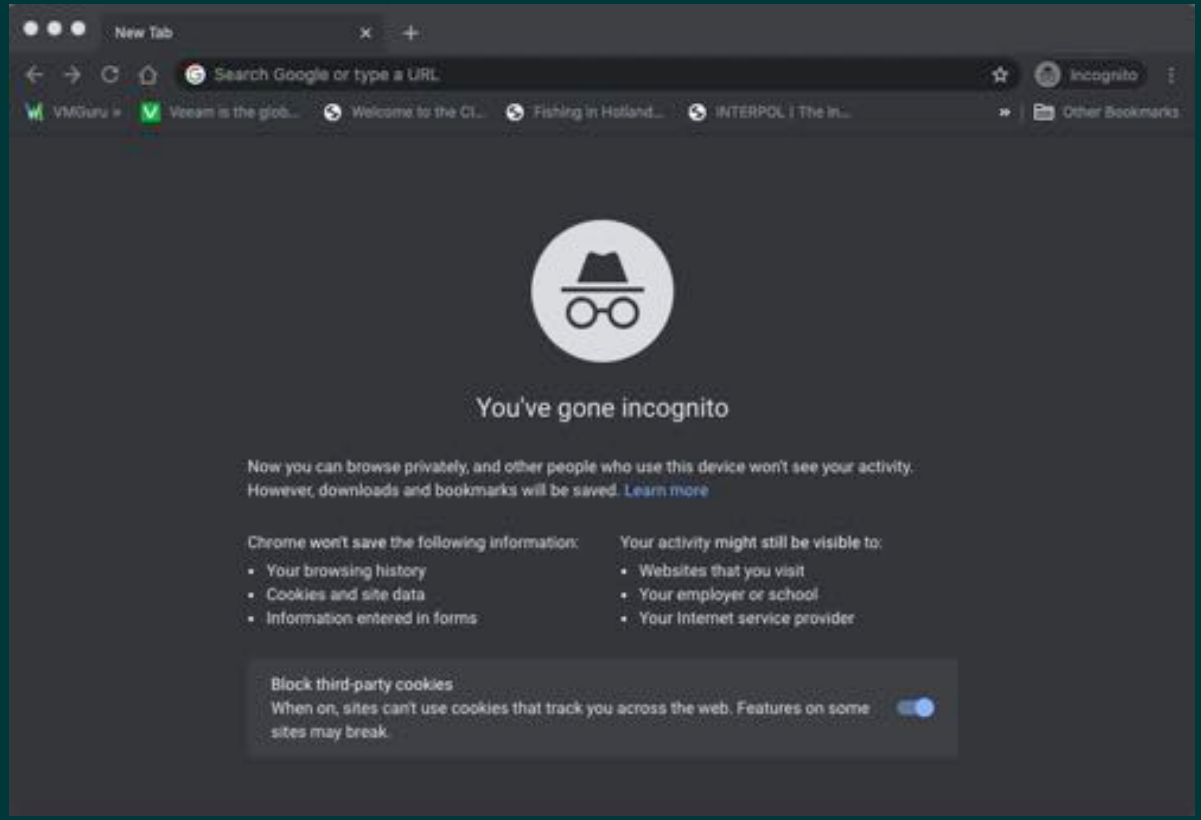
6 Stages of an Advanced Ransomware Attack

Stage 1: Observation

Information is gathered on the victim's people, processes and technology in play

© 2021 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Observation



VEEAM

@Viperian

© 2021 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Observation

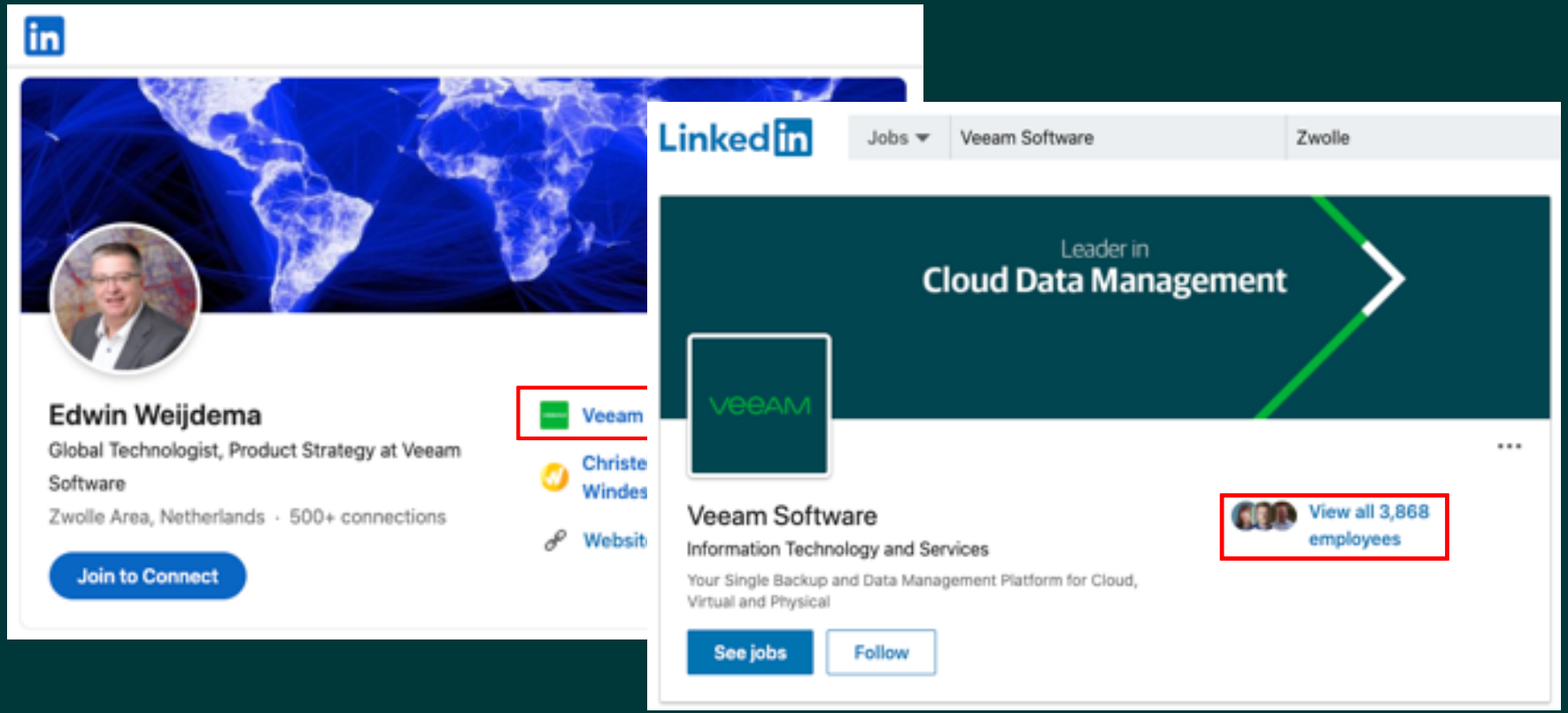
Local tournament, Volunteer, WVF, Veeam?

Is a soccer referee?

Lives in Zwolle, The Netherlands, uses an iPhone?

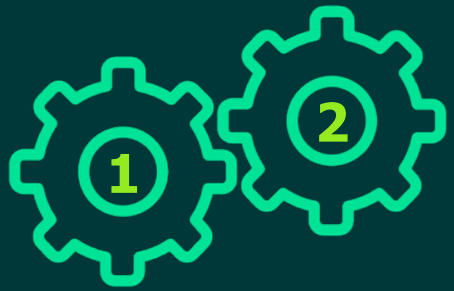
© 2021 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Observation



© 2021 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

6 Stages of an Advanced Ransomware Attack



Stage 1: Observation

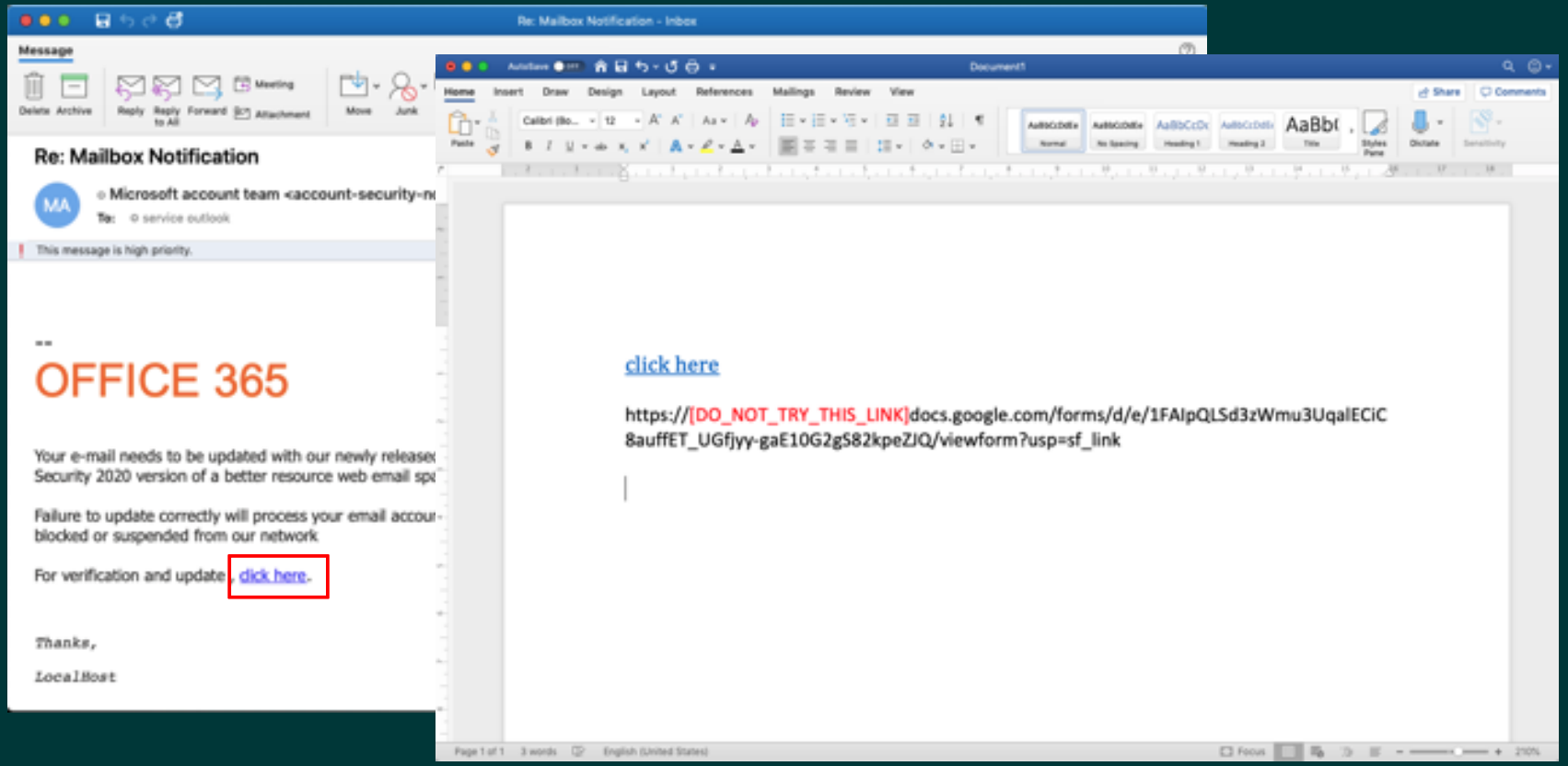
Information is gathered on the victim's people, processes and technology in play

Stage 2: Sneak in

Gain access to the victim, lets click a link!

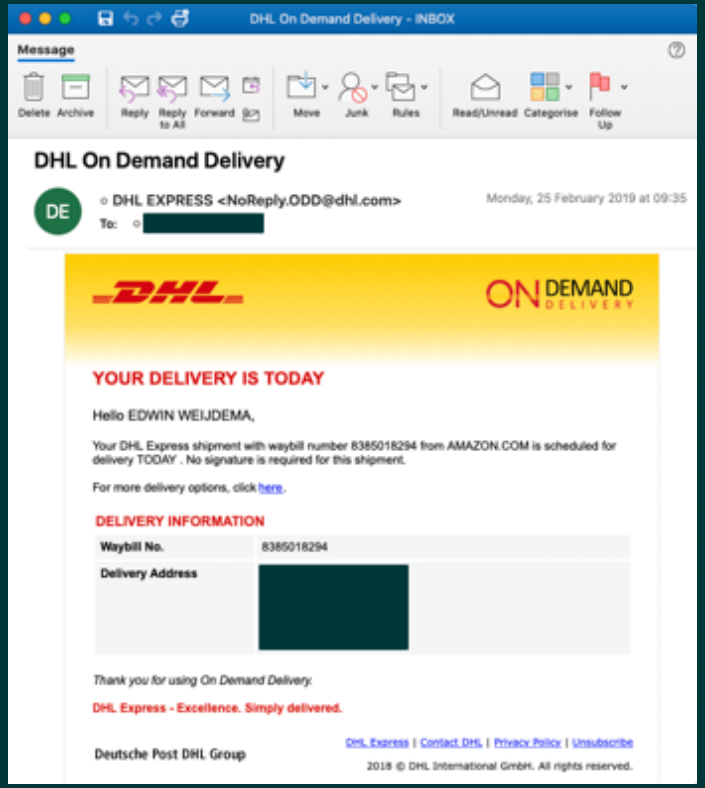
© 2021 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Sneak In – easy



© 2021 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Sneak In – Hard



Day 266 of quarantine

You told me,
the darkside had cookies…

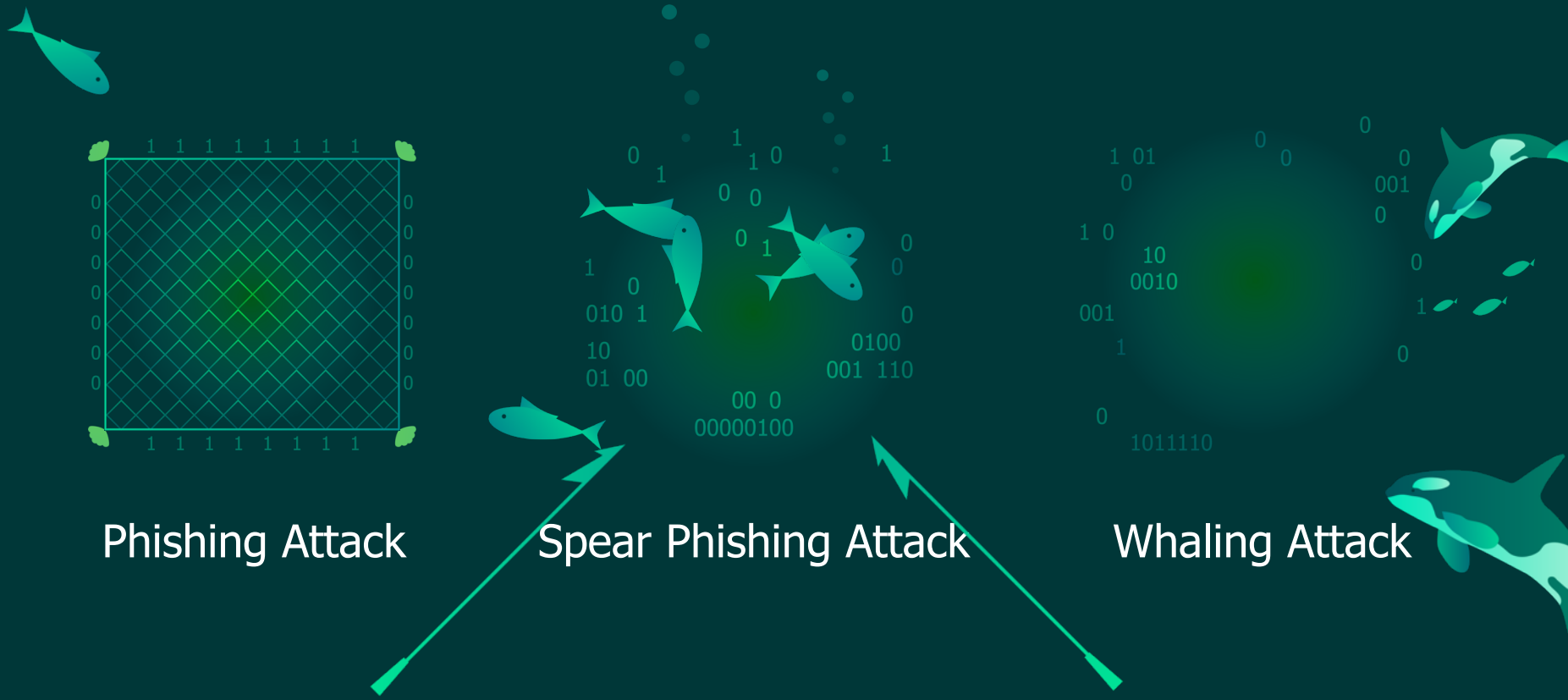
© 2021 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

What is Phishing?

Phishing is when scam artists send official-looking emails, attempting to fool you into disclosing your personal information — such as usernames, passwords, banking records or account numbers, or social security numbers — by replying to the email, clicking a link or entering it on a phone website.

© 2021 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Phishing flavors



Phishing Attack

Spear Phishing Attack

Whaling Attack

© 2021 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

How to Identify Malicous E-Mails

Identify the Sender

Do you know this Person? Were you expecting an e-mail from this person or does it fit in with your job role? If not, it is probably suspicious!

Reply-to

If the Reply-to address is different from the sending address, this should raise your suspicion for the whole message!

Links and Attachments

If you were not expecting an attachment or a link, and you do not know the sender, delete it right away! If you are uncertain check with the sender by another medium like phone (Do not use a phone number in the e-mail)

Grammar and Tone

Many of the malicious e-mails sent have poor grammar, punctuation and spelling. You should recognize how your co-workers communicate. Does this email sound like them? If not delete!

Emotions

Be wary of any e-mails trying to cause certain emotions. The most commonly-used malicious emotions are:

- Greed
- Curiosity
- Urgency
- Fear

© 2021 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Education example

Read Your Email

Look at the sender's address and look for grammatical errors or inconsistencies within the e-mail

Don't Click the Link

Hover over email links to view the URL's destination.
Still unsure? Right click the link and copy the link and paste it into Word or Notepad.

Report an Attack

If you click a link that is part of a phishing attack, it is crucial to contact your Service Desk immediately to avoid further breaches.

© 2021 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Stage 2: Sneak in

© 2021 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Stage 2: Sneak in

Know that most attackers target data, but they reach their target by hijacking accounts!

"90% of malware comes from emails..."

Source: https://enterprise.verizon.com/resources/reports/dbir/

© 2021 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

6 Stages of an Advanced Ransomware Attack

Stage 3: Setting up Shop
Creating a base of operations and let's make it redundant and highly available

Stage 2: Sneak in
Gain access to the victim, lets click a link!

Stage 1: Observation
Information is gathered on the victim's people, processes and technology in play

© 2021 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Base of Operations

Meterpreter Malware

- Metasploit attack
- Interactive shell
- Execute Code
- In memory DLL injection

© 2021 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Stage 3: Setting up Shop

© 2021 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Stage 3: Setting up Shop

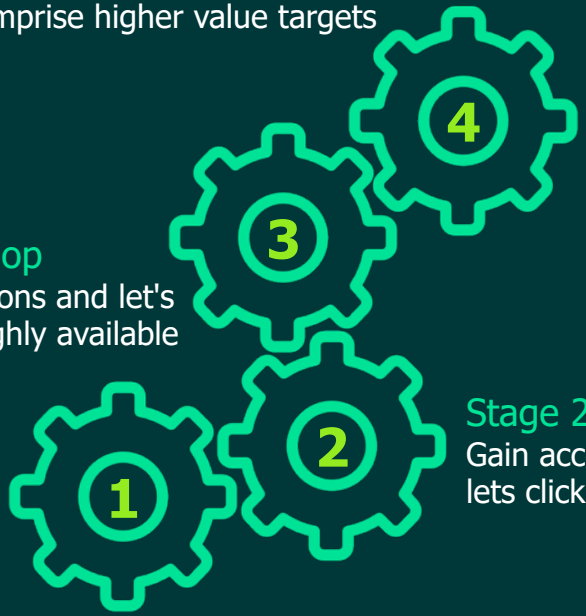
2003R2

Gained
system account

© 2021 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

6 Stages of an Advanced Ransomware Attack

Stage 4: Elevate Access
Snooping around without being detected and comprise higher value targets



Stage 3: Setting up Shop
Creating a base of operations and let's make it redundant and highly available

Stage 2: Sneak in
Gain access to the victim, lets click a link!

Stage 1: Observation
Information is gathered on the victim's people, processes and technology in play

© 2021 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

So what happens after clicking a link?

Link Clicked

In the background another document with a macro was loaded from another machine (e.g. Get2 downloader)

RAT Deployed

In the background the macro downloads and fires up a Remote Access Tool (RAT) Hides in registry! (e.g SDBbot RAT)

Call Home

Every 15 minute the RAT tool communicates with a server on the internet.

Snooping Around

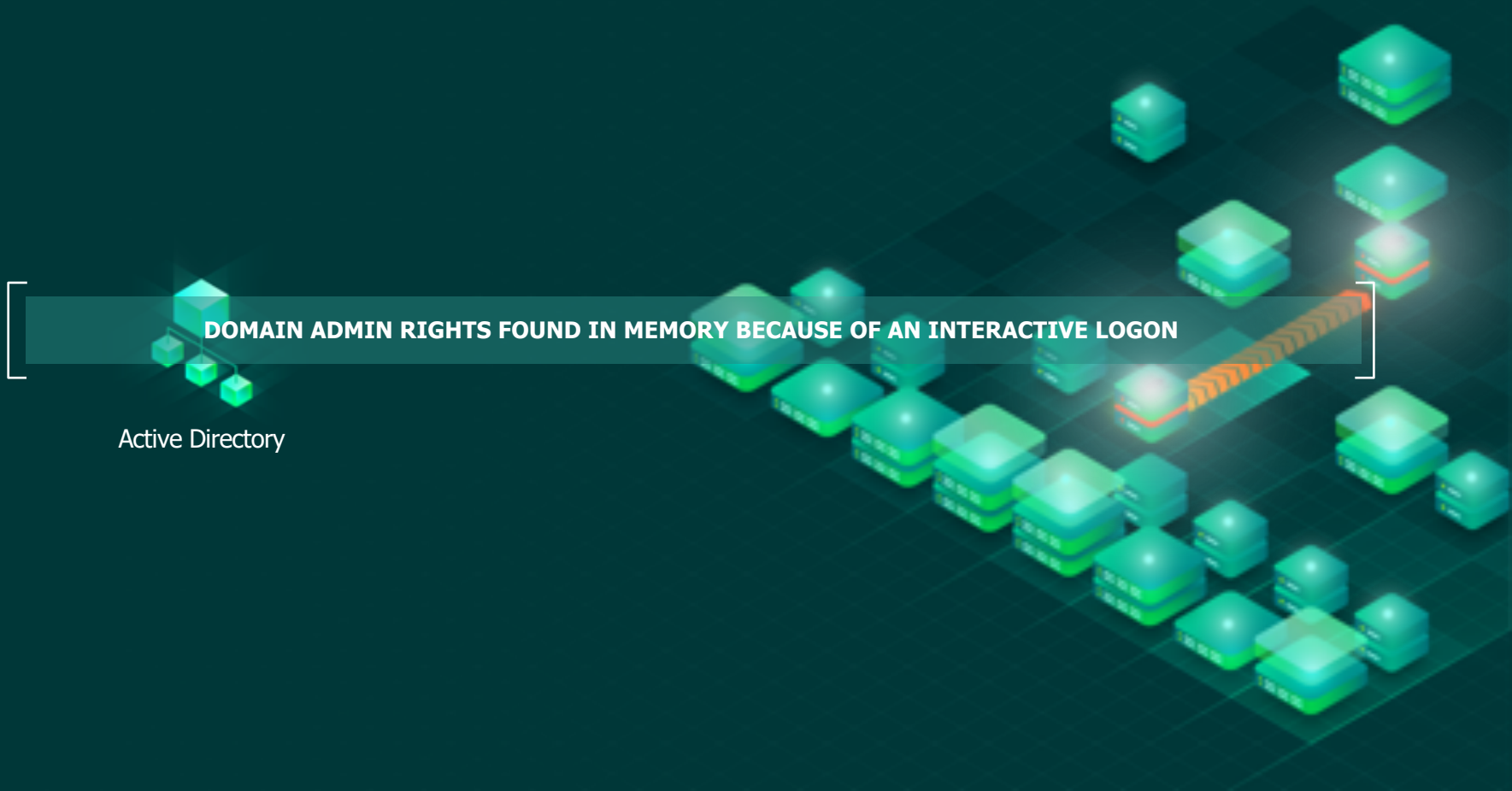
Attacker gains access to the network and deploys several keyloggers uses Meterpreter to use EternalBlue against unpatched Windows servers

© 2021 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

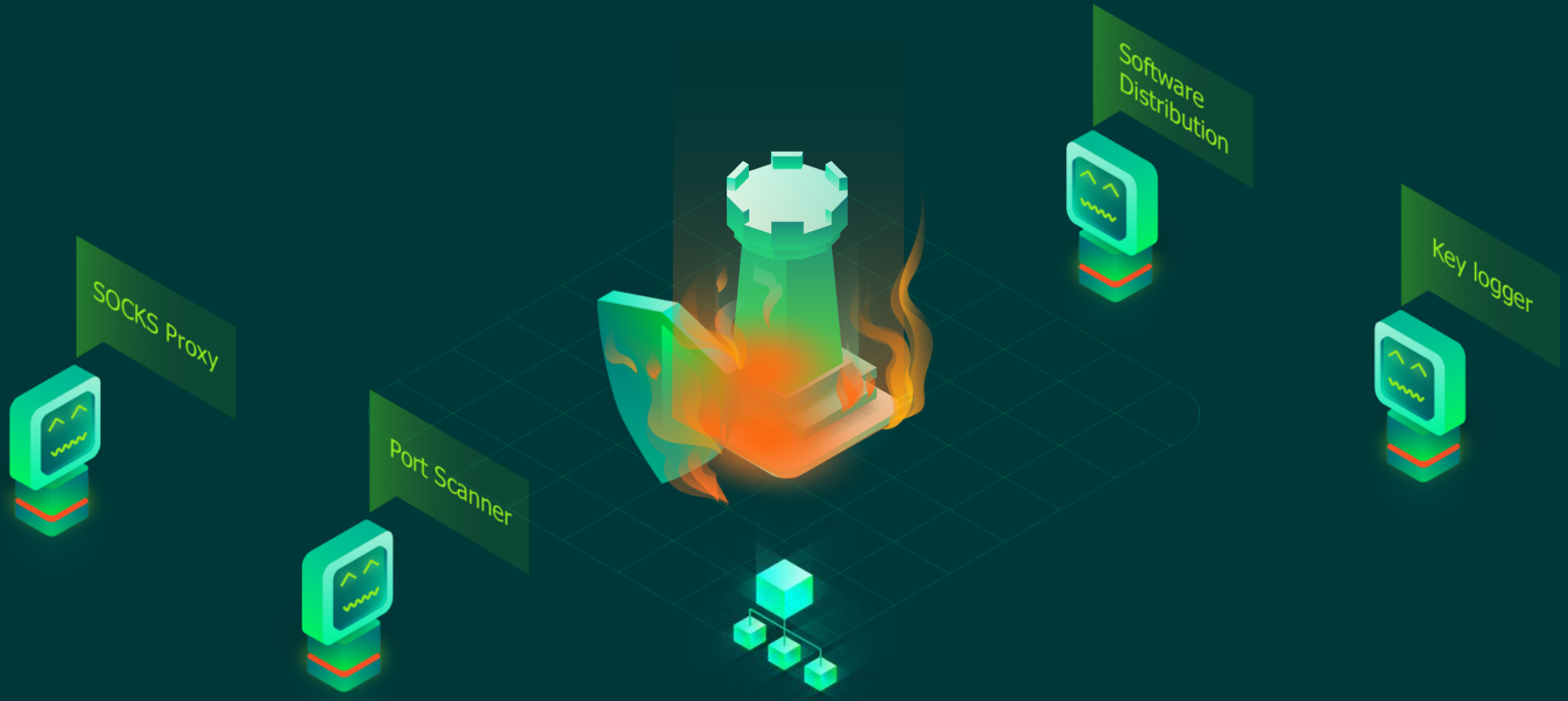
Stage 4: Elevate Access

Active Directory

Stage 4: Elevate Access



The Castle has Fallen

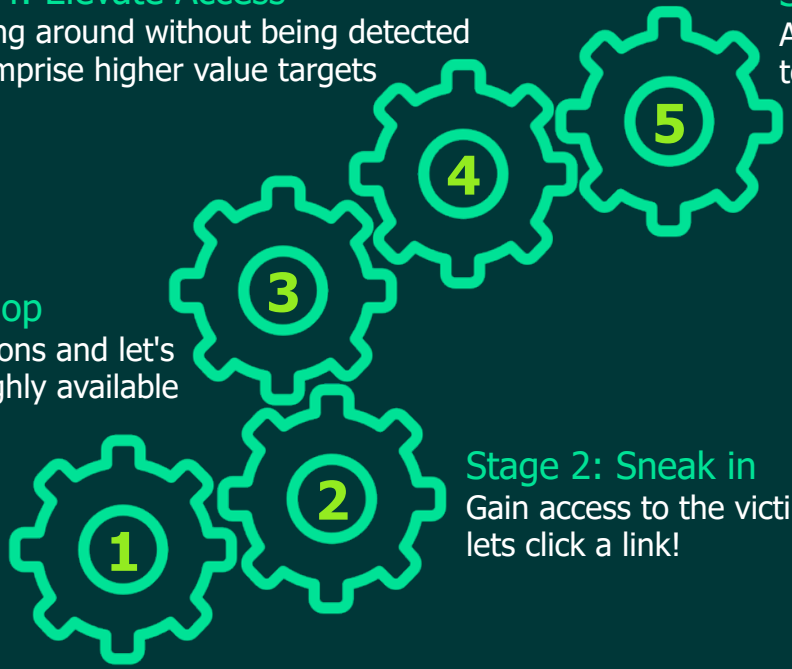


© 2021 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

6 Stages of an Advanced Ransomware Attack

Stage 4: Elevate Access
Snooping around without being detected and comprise higher value targets

Stage 5: Cripple Recoverability
Alter routines, documentation and systems to reduce/deny restore capabilities



Stage 3: Setting up Shop
Creating a base of operations and let's make it redundant and highly available

Stage 2: Sneak in
Gain access to the victim, lets click a link!

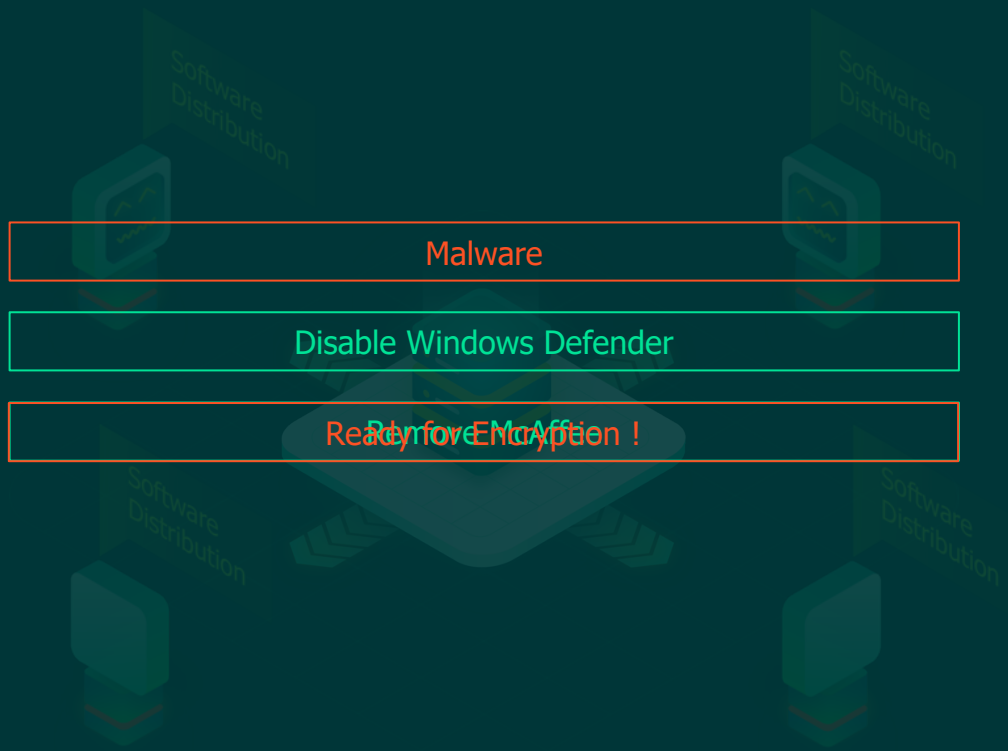
Stage 1: Observation
Information is gathered on the victim's people, processes and technology in play

© 2021 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Stage 5: Cripple Recoverability

© 2021 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

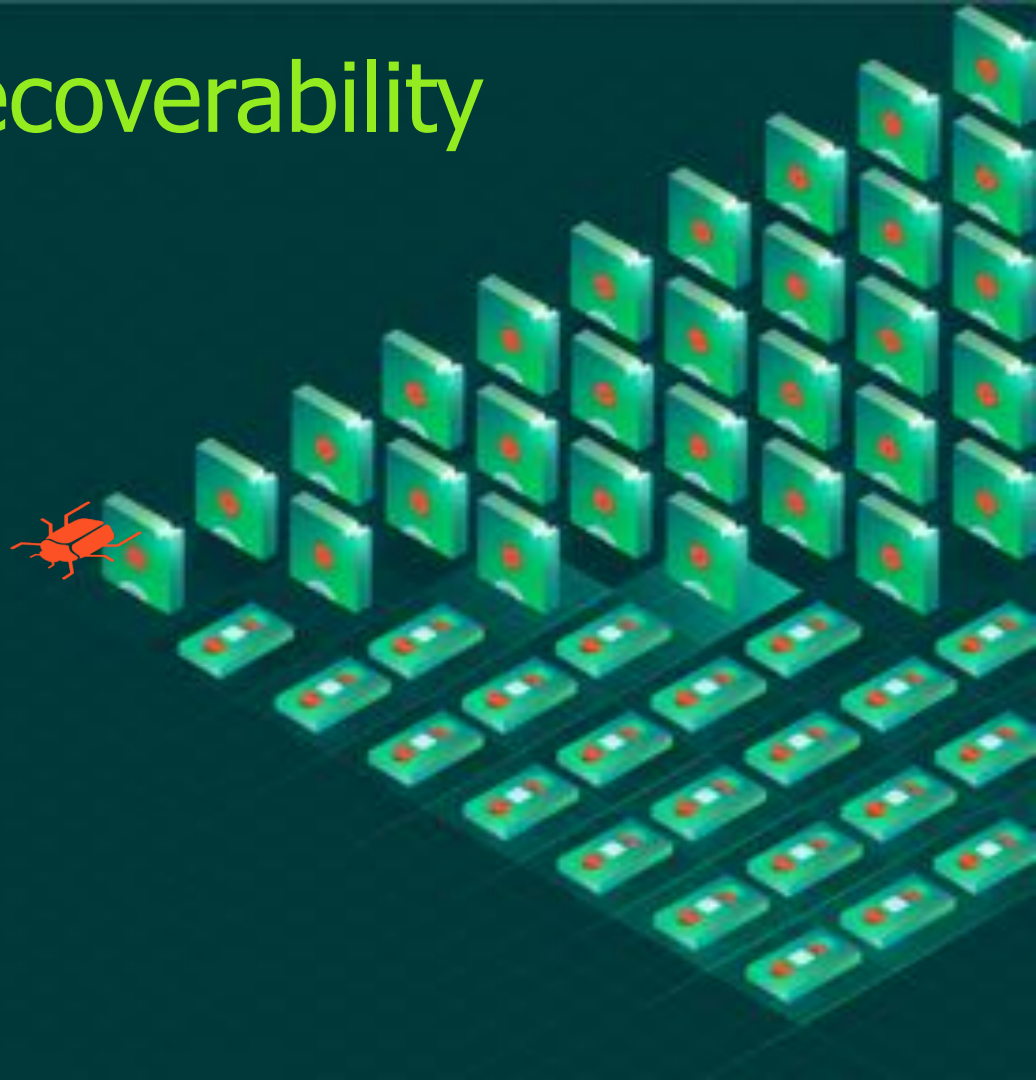
Stage 5: Cripple Recoverability



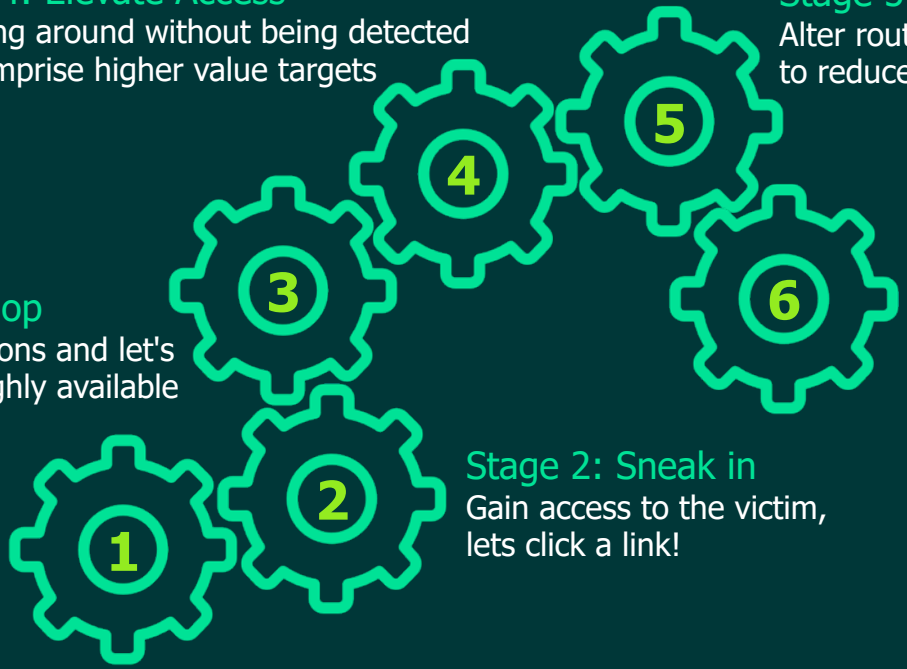
© 2021 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Stage 5: Cripple Recoverability

HACKER DID A TAPE FORMAT



6 Stages of an Advanced Ransomware Attack



Stage 1: Observation
Information is gathered on the victim's people, processes and technology in play

Stage 2: Sneak in
Gain access to the victim, lets click a link!

Stage 3: Setting up Shop
Creating a base of operations and let's make it redundant and highly available

Stage 4: Elevate Access
Snooping around without being detected and comprise higher value targets

Stage 5: Cripple Recoverability
Alter routines, documentation and systems to reduce/deny restore capabilities

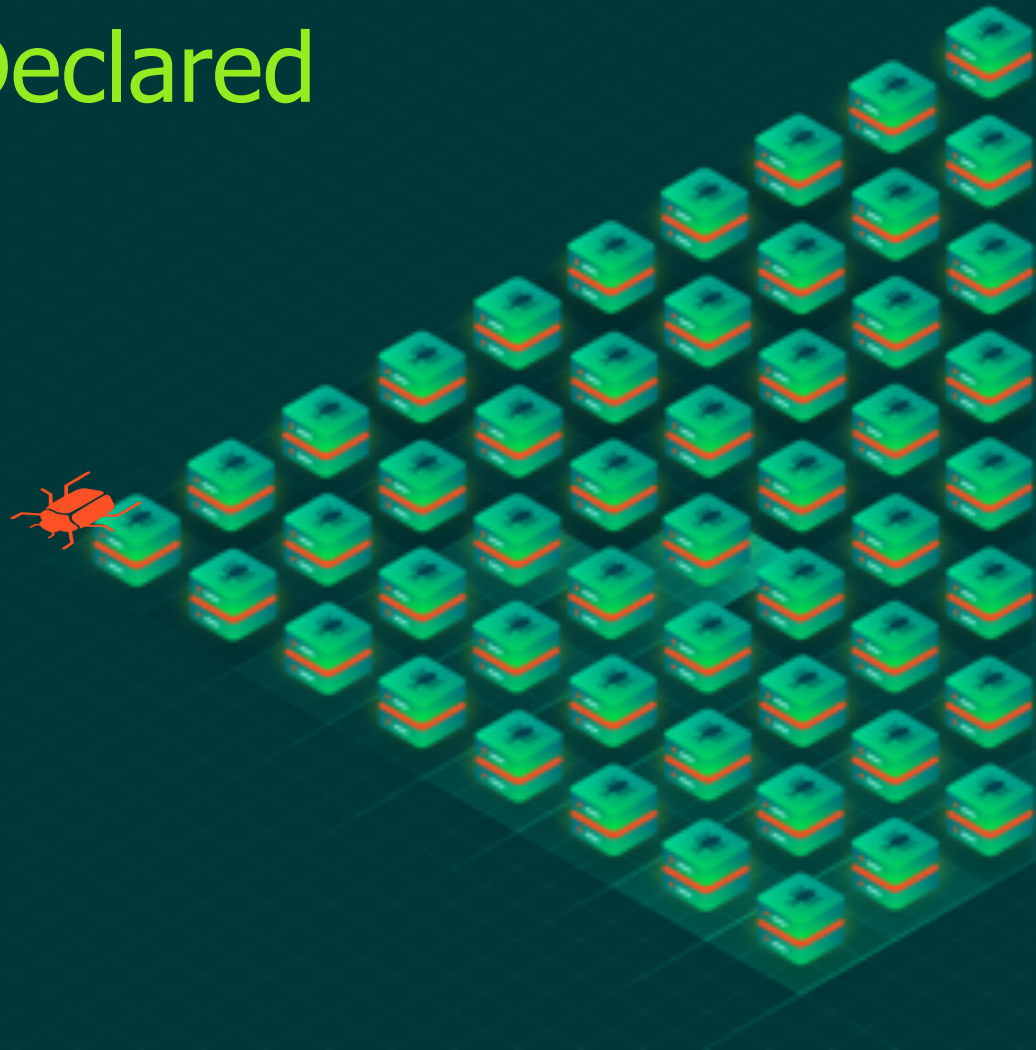
Stage 6: Ransom Declared!
Encrypt victim's data, wipe archives/backup/data, issue ransom demands!

© 2021 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

VEEAM

Stage 6: Ransom Declared

ALL 267 SERVER SYSTEMS ARE ENCRYPTED



Ransom Declared

ClopReadMe.txt - Notepad

File Edit Format View Help

Your network has been penetrated.
All files on each host in the network have been encrypted with a strong algorithm.
Backups were either encrypted or deleted or backup disks were formatted.
Shadow copies also removed, so F8 or any other methods may damage encrypted data but not recover.
We exclusively have decryption software for your situation
No decryption software is available in the public.
DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME OR MOVE the encrypted and readme files.
DO NOT DELETE readme files.
This may lead to the impossibility of recovery of the certain files.
Photorec, RannohDecryptor etc. repair tools are useless and can destroy your files irreversibly.
If you want to restore your files write to emails (contacts are at the bottom of the sheet) and a
(less than 5 Mb each, non-archived and your files should not contain valuable information
(Databases, backups, large excel sheets, etc.)).
You will receive decrypted samples and our conditions how to get the decoder.

Attention!!!
Your warranty - decrypted samples.
Do not rename encrypted files.
Do not try to decrypt your data using third party software.
We don't need your files and your information.

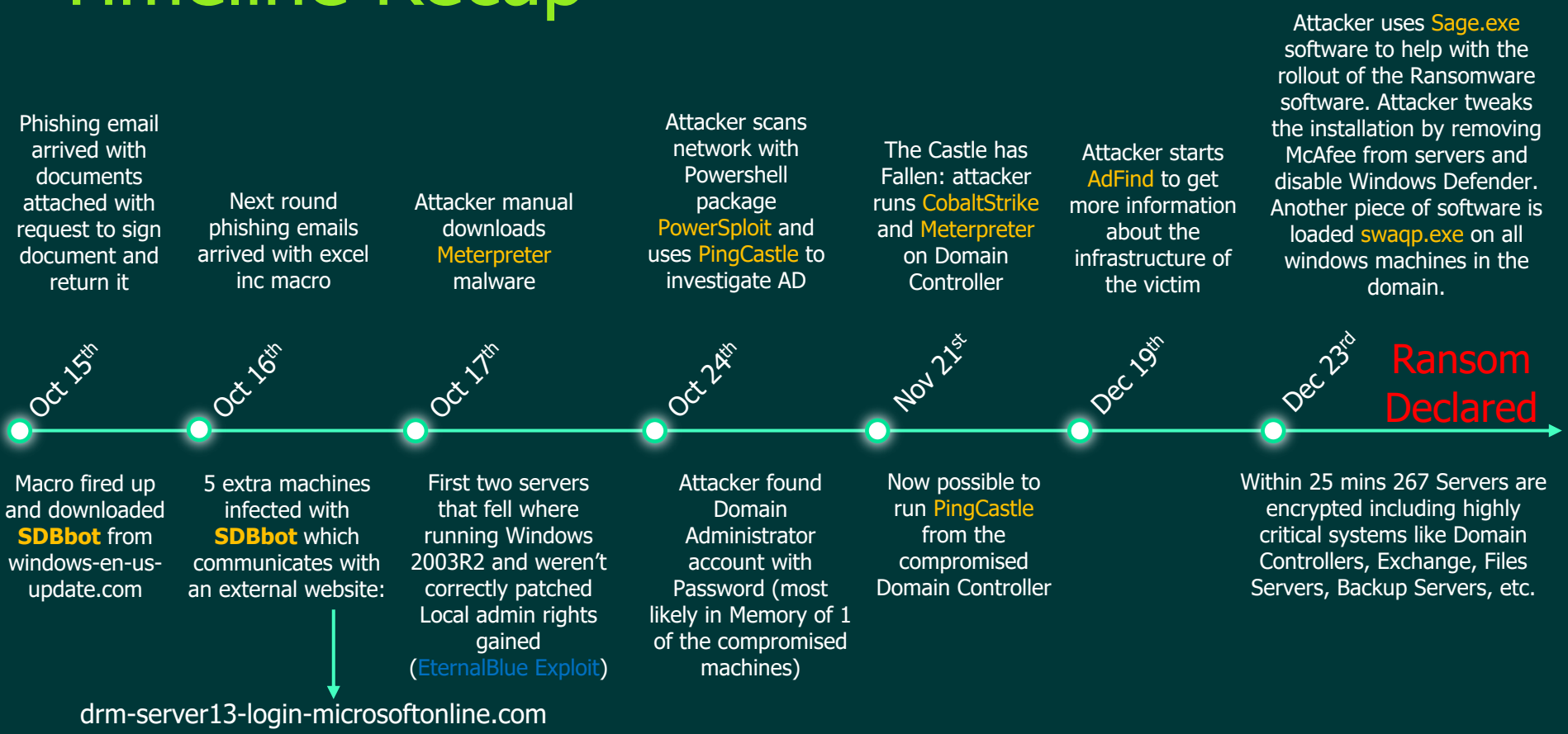
But after 2 weeks all your files and keys will be deleted automatically.
Contact emails:
[redacted]
or
[redacted]

The final price depends on how fast you write to us.

Clop

© 2021 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Timeline Recap



© 2021 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

VEEAM

6 Stages of an Advanced Ransomware Attack

Stage 1: Observation
Information is gathered on the victim's people, processes and technology in play

Stage 2: Sneak in
Gain access to the victim, lets click a link!

Stage 3: Setting up Shop
Creating a base of operations and let's make it redundant and highly available

Stage 4: Elevate Access
Snooping around without being detected and comprise higher value targets

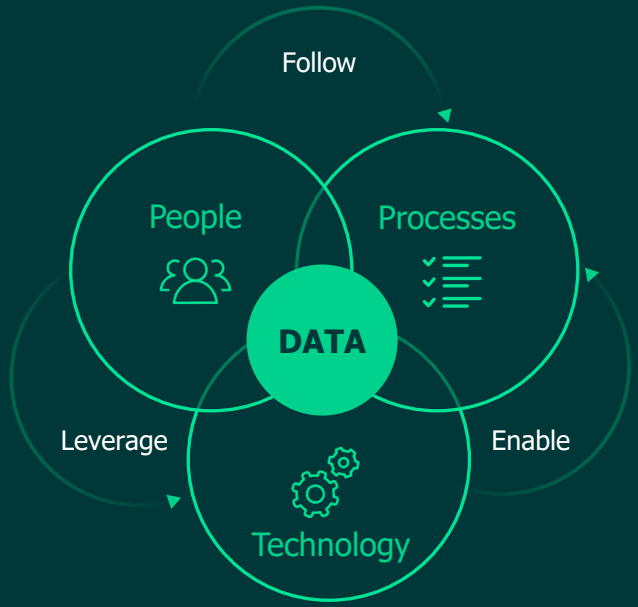
Stage 5: Cripple Recoverability
Alter routines, documentation and systems to reduce/deny restore capabilities

Stage 6: Ransom Declared!
Encrypt victim's data, wipe archives/backup/data, issue ransom demands!

© 2021 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

VEEAM

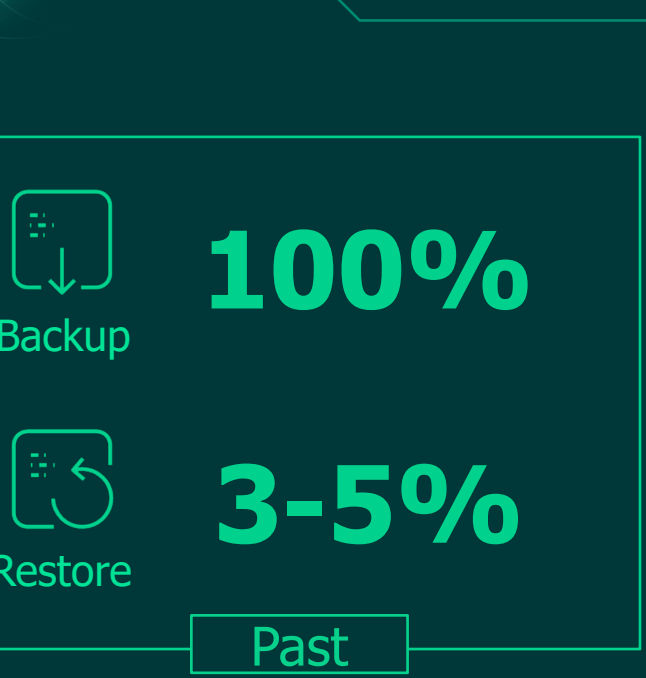
Organizations are being forced to place strategic bets



© 2021 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

VEEAM

Backups are essential but
Restore becomes critical



© 2021 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

There will be a surge of

The Ultimate Betrayal

Weakest Link

2020 Pandemic

Uncertain Economy

© 2021 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Data Management Protection Strategy

VEEAM

3

Different copies of data

2

Different media

1

Offsite copy

1

Of which is:
offline
air-gapped
or immutable

0

No errors after backup recoverability verification

© 2021 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Additional Resources

Ransomware:
http://vee.am/ransomwareseriespapers

Best Practices:
https://bp.veeam.com/vbr/VBP/Security/

Local Veeam Team contact:

Laurent Dumortier
Enterprise Account Manager
Mobile: +32 486 22 22 47
E-mail: laurent.dumortier@veeam.com

Twitter | LinkedIn | YouTube

© 2021 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

VEEAM
Thank
You!