



# CYBER THREATS & SECURITY OVERVIEW

## OVERVIEW OF TOPICS



- THREATS: ACTORS & TECHNIQUES
- CYBER SECURITY AWARENESS & EXAMPLES
- REGULATOR VS INVESTIGATOR
- TAKEAWAYS
- RESOURCES

# MEET THE CYBER HACKERS



## HACKTIVIST

Cause mischief  
Not organized  
Release  
Data/PII  
Low-tech social  
engineering



## CRIMINAL

Want Money  
Well-organized  
& financed  
Business email  
compromise  
Ransomware  
Identity theft



## APT

Data exfil  
Nation-state  
sponsored  
Spear phishing  
emails  
Technically  
advanced

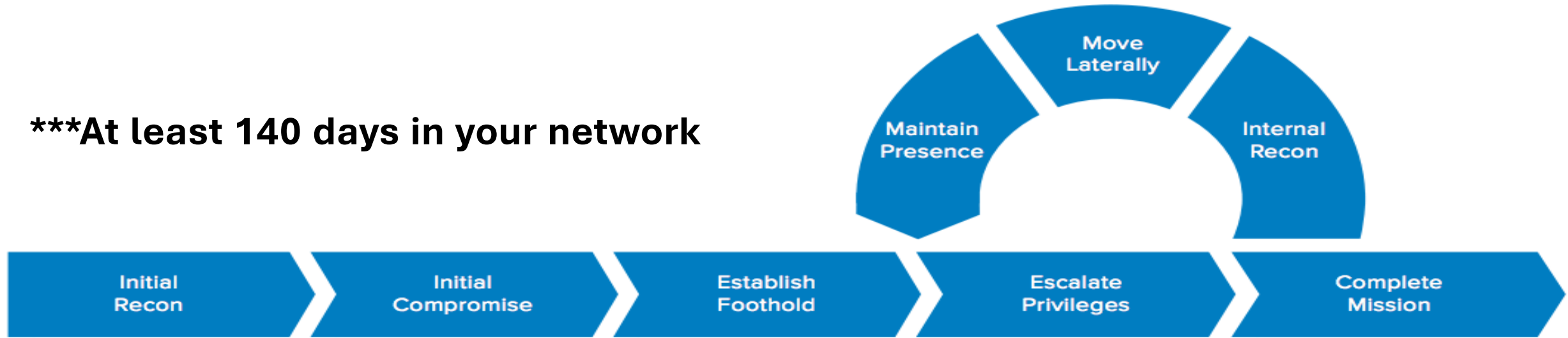


## TERRORIST

Destroy or  
Disrupt  
Nation-states  
or ad-hoc  
groups  
Similar to  
hacktivist

# COMPUTER INTRUSION CYCLE

**\*\*\*At least 140 days in your network**



- 1) Research on a target, may look for Internet-facing services or individuals to exploit.
- 2) Execute malicious code on the network (usually occurs through social engineering/spear phishing) or by exploiting a vulnerability
- 3) Attacker installs a persistent backdoor or malware
- 4) Attacker attempts to escalate their privileges
- 5) Attacker explores the victim's environment for better exploitation
- 6) Attacker uses access to move from system to system
- 7) Attacker ensures continued access through backdoors & remote access

# CYBER PHISHING - THE LINGO

Scammers send an individual(s) a malicious communication impersonating a known individual, a business partner, a service provider, a known company, a promise of a prize or similar. (Social Engineering)

**Vishing** - over the phone

**Smishing** - done over text message (malicious link)



**Search Engine Phishing** - fake webpage/specific keywords

**Spear Phishing** - emails designed to target a particular user/organization

**Whaling** - spear phishing high level employees/positions

# QR CODES - QUISHING



QR codes replace traditional hyperlinks and are useful when the end user is utilizing a smartphone. However, they can often be used as part of a cyberattack, especially phishing (quishing).

- Don't scan a random QR code
- Be suspicious if it takes you to a site asking for sensitive info
- Some scammers are putting bogus codes over legitimate ones
- Use the same caution for ads that you pick up or get in the mail

From: authenticationmail@trust.ameribank7.com  
To: johnsmith@email.com  
Subject: **A new login to your bank account**

---



Bank of America

Dear account holder,

There has been a recent login to your bank account from a new device:

IP address: 192.168.0.1

Location: Miami, Florida

**4 new transactions have been made with this account since your last login.**

**If this was not you, please reset your password immediately with this link:**

<https://trust.ameribank7.com/reset-password>

Thank you,

Bank America

**W** UNIVERSITY of WASHINGTON

Due to recent security, This email is to confirm 2-Factor authentication for all University of Washington email recipients. You're hereby required to complete exercise with the mobile number you want your 2-Factor Authentication set to.

Scan QR Code below to complete authentication.



1,800 malicious emails sent to the company in this campaign.

50 emails reached user inboxes.

14 emails were clicked on, launching malware.

1 instance of malware installed.

1,800 

50 

14 

1 

1,750 

36 

13 

1,750 emails were stopped by an email filtering service that identified that malware was present.

36 emails were ignored or reported by staff, using a button in their email client.

25 were reported in total, including some after having been clicked on.

This was the first indication that the attack had got through the initial layer of defences.

13 malware installations were unsuccessful because a patching regime had ensured that nearly all devices were up-to-date.

The malware's call home to its operator was detected, reported and blocked. 1 device was seized, investigated and cleaned within a few hours.

### How was the organisation attacked?

A financial sector company of around 4,000 employees received 1,800 emails which contained a number of variants of Dridex malware. The email claimed to be an invoice that needed urgent attention, which was relevant to the role of some of the recipients. It was not targeted at individual users with any personal information, but was well written, with good spelling and grammar.



# Ransomware

A type of malware that blocks access to your system or threatens to release your data unless a ransom is paid.

- Typically sent via spear-phishing email
- Encrypts hard drive
- Demands financial payment to decrypt data
- Broad set of victims

All your personal files are **LOCKED!**



## WHAT'S HAPPENED?

- \* All your important files( including => hard disks, network disks, flash, USB ) are encrypted.
- \* All the files are locked with asymmetric algorithm using AES-256 and then RSA-2048 cipher.
- \* You can't restore your files because all your backups have been deleted.
- \* Only way to recover your files is to pay us 1 BTC
- \* As a proof you can decrypt 1 file FOR FREE by clicking here:

## HOW TO PAY US AND DECRYPT YOUR FILES?

1. If you are OFFLINE you can contact us via e-mail: dma4004@zeroblit.er and we will provide you instructions about how to decrypt your files.
2. To pay us, you have to use Bitcoin currency. You can easily buy Bitcoins at following sites:
  - \* <https://coincafe.com/>
  - \* <https://www.bitquick.co/>
  - \* <https://www.coinbase.com/>
3. If you already have Bitcoins, pay us 1 BTC to the following Bitcoin address:
4. If you have paid, enter following site to get your transaction id.  
Click this button to show tutorial how to locate your transaction id:
5. When you have located Transaction ID, paste it to 'TRANSACTION ID' field below and, click the "CHECK PAYMENT" button. Confirming your payment by our servers can take up to several hours (we require some bitcoin transaction confirmations). When your payment has been confirmed, the 'DECRYPT FILES' button will enabled, just click it to decrypt your files.

## Ransom increase time:

If you don't pay us within this time, the amount you will have to pay will increase to: 1.5 BITCOINS

TRANSACTION ID:

PAYMENT STATUS:

# RANSOMWARE HELP

nomoreransom.org

## Decryption Key from Law Enforcement

</> NO MORE RANSOM

**NEED HELP**  
unlocking your digital  
life without paying  
your attackers\*?

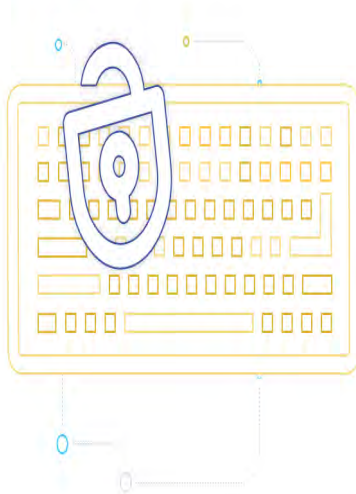
YES

NO

At the moment, not every type of ransomware has a solution. Keep checking this website as new keys and applications are added when available.

Partners About the Project English

Home Crypto Sheriff Ransomware: Q&A Prevention Advice Decryption Tools Report a Crime



Ransomware is malware that locks your computer and mobile devices or encrypts your electronic files. When this happens, you can't get to the data unless you pay a ransom.

**However this is not guaranteed and you should never pay!**

New decryptor for  
**RanHassan** available,

OK, I'VE READ IT

We use cookies on No More Ransom's website to support technical features that enhance your user experience. For more information, see our [Website Disclaimer](#).

**02. EXECUTION**  
Malware targets systems, documents and files and downloads into the network

**04. DEMAND**  
User is notified of the ransom demand in exchange for the key to decrypt affected networks and files



**01. INFECTION**  
Malicious email  
Malicious website  
Vulnerability exploit

**03. ENCRYPTION**  
Systems and files are locked via unique encryption keys held by fraudster

**05. PAYMENT**  
Payment in crypto currency and delivery of the exchange of decryption key

## OVERVIEW OF TOPICS



- THREATS: ACTORS & TECHNIQUES
- CYBER SECURITY AWARENESS & EXAMPLES
- REGULATOR VS INVESTIGATOR
- TAKEAWAYS
- RESOURCES

# MEET THE CYBER HACKERS



## HACKTIVIST

Cause mischief  
Not organized  
Release  
Data/PII  
Low-tech social  
engineering



## CRIMINAL

Want Money  
Well-organized  
& financed  
Business email  
compromise  
Ransomware  
Identity theft



## APT

Data exfil  
Nation-state  
sponsored  
Spear phishing  
emails  
Technically  
advanced

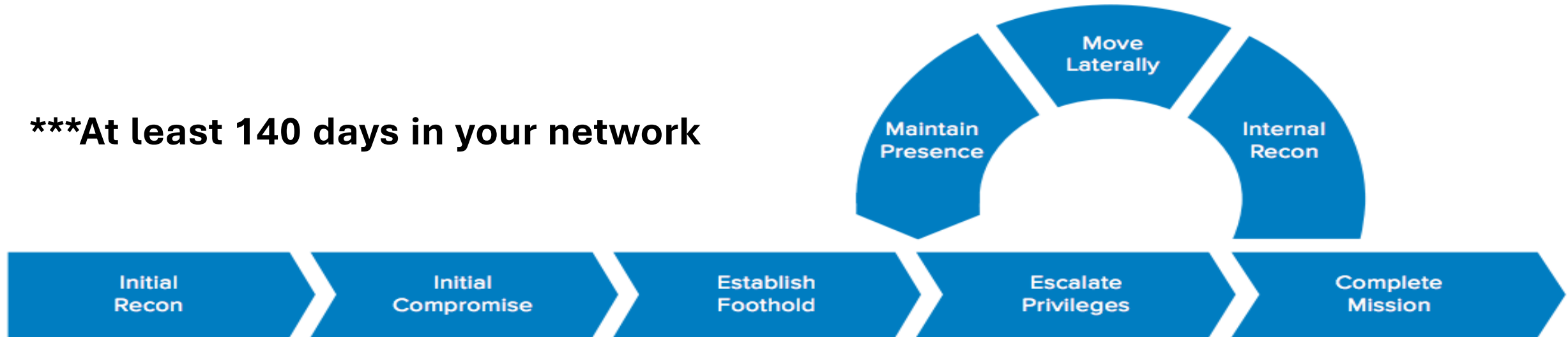


## TERRORIST

Destroy or  
Disrupt  
Nation-states  
or ad-hoc  
groups  
Similar to  
hacktivist

# COMPUTER INTRUSION CYCLE

**\*\*\*At least 140 days in your network**



- 1) Research on a target, may look for Internet-facing services or individuals to exploit.
- 2) Execute malicious code on the network (usually occurs through social engineering/spear phishing) or by exploiting a vulnerability
- 3) Attacker installs a persistent backdoor or malware
- 4) Attacker attempts to escalate their privileges
- 5) Attacker explores the victim's environment for better exploitation
- 6) Attacker uses access to move from system to system
- 7) Attacker ensures continued access through backdoors & remote access

# CYBER PHISHING - THE LINGO

Scammers send an individual(s) a malicious communication impersonating a known individual, a business partner, a service provider, a known company, a promise of a prize or similar. (Social Engineering)

**Vishing** - over the phone

**Smishing** - done over text message (malicious link)



**Search Engine Phishing** - fake webpage/specific keywords

**Spear Phishing** - emails designed to target a particular user/organization

**Whaling** - spear phishing high level employees/positions

# QR CODES - QUISHING



QR codes replace traditional hyperlinks and are useful when the end user is utilizing a smartphone. However, they can often be used as part of a cyberattack, especially phishing (quishing).

- Don't scan a random QR code
- Be suspicious if it takes you to a site asking for sensitive info
- Some scammers are putting bogus codes over legitimate ones
- Use the same caution for ads that you pick up or get in the mail

From: authenticationmail@trust.ameribank7.com  
To: johnsmith@email.com  
Subject: **A new login to your bank account**

---



Bank of America

Dear account holder,

There has been a recent login to your bank account from a new device:

IP address: 192.168.0.1

Location: Miami, Florida

**4 new transactions have been made with this account since your last login.**

**If this was not you, please reset your password immediately with this link:**

<https://trust.ameribank7.com/reset-password>

Thank you,

Bank America

**W** UNIVERSITY of WASHINGTON

Due to recent security, This email is to confirm 2-Factor authentication for all University of Washington email recipients. You're hereby required to complete exercise with the mobile number you want your 2-Factor Authentication set to.

Scan QR Code below to complete authentication.



1,800 malicious emails sent to the company in this campaign.

50 emails reached user inboxes.

14 emails were clicked on, launching malware.

1 instance of malware installed.

1,800 

50 

14 

1 

1,750 

36 

13 

1,750 emails were stopped by an email filtering service that identified that malware was present.

36 emails were ignored or reported by staff, using a button in their email client.

25 were reported in total, including some after having been clicked on.

This was the first indication that the attack had got through the initial layer of defences.

13 malware installations were unsuccessful because a patching regime had ensured that nearly all devices were up-to-date.

The malware's call home to its operator was detected, reported and blocked. 1 device was seized, investigated and cleaned within a few hours.

### How was the organisation attacked?

A financial sector company of around 4,000 employees received 1,800 emails which contained a number of variants of Dridex malware. The email claimed to be an invoice that needed urgent attention, which was relevant to the role of some of the recipients. It was not targeted at individual users with any personal information, but was well written, with good spelling and grammar.



# Ransomware

A type of malware that blocks access to your system or threatens to release your data unless a ransom is paid.

- Typically sent via spear-phishing email
- Encrypts hard drive
- Demands financial payment to decrypt data
- Broad set of victims

All your personal files are **LOCKED!**



## WHAT'S HAPPENED?

- \* All your important files( including => hard disks, network disks, flash, USB ) are encrypted.
- \* All the files are locked with asymmetric algorithm using AES-256 and then RSA-2048 cipher.
- \* You can't restore your files because all your backups have been deleted.
- \* Only way to recover your files is to pay us 1 BTC
- \* As a proof you can decrypt 1 file FOR FREE by clicking here:

## HOW TO PAY US AND DECRYPT YOUR FILES?

1. If you are OFFLINE you can contact us via e-mail: dma4004@zeroblit.er and we will provide you instructions about how to decrypt your files.
2. To pay us, you have to use Bitcoin currency. You can easily buy Bitcoins at following sites:
  - \* <https://coincafe.com/>
  - \* <https://www.bitquick.co/>
  - \* <https://www.coinbase.com/>
3. If you already have Bitcoins, pay us 1 BTC to the following Bitcoin address:
4. If you have paid, enter following site to get your transaction id.  
Click this button to show tutorial how to locate your transaction id:
5. When you have located Transaction ID, paste it to 'TRANSACTION ID' field below and, click the "CHECK PAYMENT" button. Confirming your payment by our servers can take up to several hours (we require some bitcoin transaction confirmations). When your payment has been confirmed, the 'DECRYPT FILES' button will enabled, just click it to decrypt your files.

## Ransom increase time:

If you don't pay us within this time, the amount you will have to pay will increase to: 1.5 BITCOINS

TRANSACTION ID:

PAYMENT STATUS:

# RANSOMWARE HELP

nomoreransom.org

## Decryption Key from Law Enforcement

</> NO MORE RANSOM

**NEED HELP**  
unlocking your digital  
life without paying  
your attackers\*?

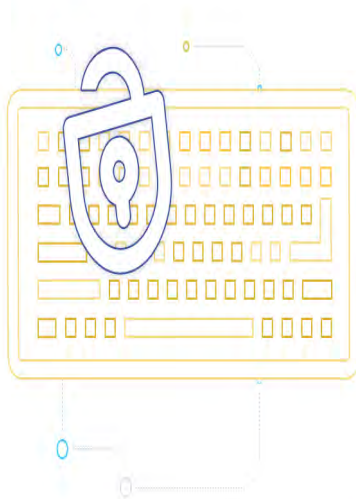
YES

NO

At the moment, not every type of ransomware has a solution. Keep checking this website as new keys and applications are added when available.

Partners About the Project English

Home Crypto Sheriff Ransomware: Q&A Prevention Advice Decryption Tools Report a Crime



Ransomware is malware that locks your computer and mobile devices or encrypts your electronic files. When this happens, you can't get to the data unless you pay a ransom.

**However this is not guaranteed and you should never pay!**

New decryptor for  
RanHassan available,

OK, I'VE READ IT

We use cookies on No More Ransom's website to support technical features that enhance your user experience. For more information, see our [Website Disclaimer](#).

**02. EXECUTION**  
Malware targets systems, documents and files and downloads into the network

**04. DEMAND**  
User is notified of the ransom demand in exchange for the key to decrypt affected networks and files



**01. INFECTION**  
Malicious email  
Malicious website  
Vulnerability exploit

**03. ENCRYPTION**  
Systems and files are locked via unique encryption keys held by fraudster

**05. PAYMENT**  
Payment in crypto currency and delivery of the exchange of decryption key