



CYBER SYNC UP



Navigating New Zealand's Cyber Future

Key Trends and Guidance from the NCSC



TOM ROBERTS

Team Lead for Response and Investigations

NSCS

What we want you to know

- Who we are and what we do
- Understand the NZ cyber security risk environment
- Know what you can do to be more cyber resilient
- Understand how you can encourage your customers to be more secure



What do we do?



We are the lead operational cyber security agency



We detect & disrupt malicious cyber activity



We support individuals & organisations to raise cyber resilience

Geo strategic shift



A shift from rules to power

Multipolar world where rules are more contested



A shift from economics to security

Economic relationships are reassessed



A shift from efficiency to resilience

Building greater resilience becomes more prominent

New Zealand's cyber threat landscape - 5 judgements

State-sponsored actors are actively testing New Zealand targets

The commercialisation of cybercrime means cybercriminals have more tools

Hacktivists are targeting New Zealand organisations as global conflicts escalate

Threat actors are exploiting supply chains, hidden dependencies and organisational blind spots to cause impact

Known weaknesses and unpatched vulnerabilities are providing threat actors with easy access

Real world impact



According to our research, around half of **New Zealanders** have experienced an online **security threat** in the past six months:



We estimate \$1.6 billion is lost to **these threats** last year in NZ



830,000 people lost money



Average loss was **\$1260**



So, what can you do to protect your systems?

own
your
online





Data collection, storage and encryption

Data collection

Consider what information you really need to collect from clients and contacts. Your level of risk is based on the amount of data you have —

Data storage

If you use a cloud service for data storage, check the provider can give you the services and protection you need.

Encryption

Make sure you're encrypting any data you collect.

- in transit
- at rest

Least Privilege - Manage and limit access

Principle of least privilege:

- reduces the risk of data being accidentally shared.
- needs clear guidance for staff.

Create an incident response plan

Develop a response plan for what to do if your business is affected by a data breach.

Make sure your staff know to report any security breach to your IT person or team.





Actions you can take to protect yourself



Create a long, strong and unique password

- Longest is strongest: use at least 16 characters.
- Use a passphrase of four or more random words.
- Avoid common patterns and personal information.

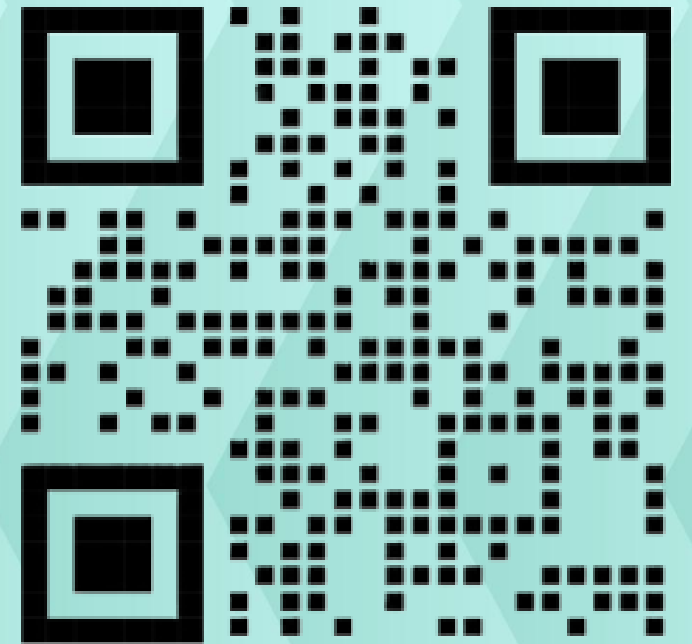




Reusing passwords

Reusing passwords means more damage if you are involved in a cyber incident.

- Many online accounts use your email address as your username.
- Many online accounts are accessed through your social media login.





2FA helps stop 99% of automated online attacks

- 2FA is an additional security step on top of your username and password
- 2FA is a way of ensuring that it's really you logging into an account.
- Find out how to do this for your bank, email and social media accounts at ownyouronline.govt.nz

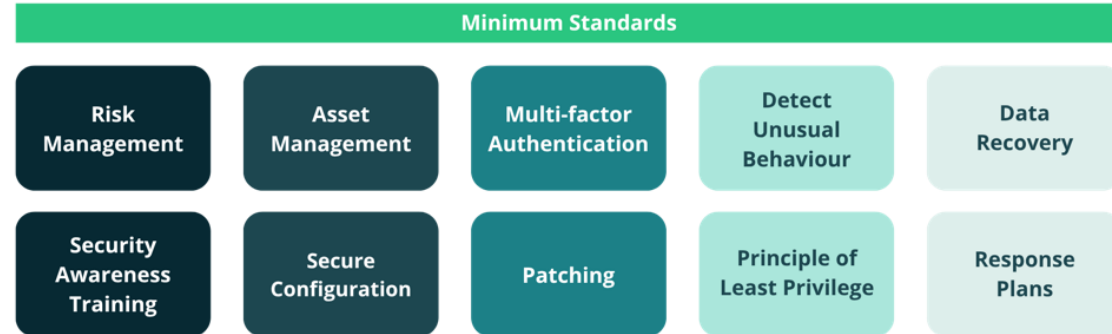


How we can support you

MFN



Minimum Standards



Vulnerability Alerting



Incident Response Support

Report to us via
www.ncsc.govt.nz/report



Key takeaways

State-sponsored actors are actively testing New Zealand targets

The commercialisation of cybercrime means cybercriminals have more tools.

Hacktivists are targeting New Zealand organisations as global conflicts escalate

Threat actors are exploiting supply chains, hidden dependencies and organisational blind spots to cause impact

Known weaknesses and unpatched vulnerabilities are providing threat actors with easy access

Doing some basics will make you and your customers more secure.



Ransomware

Cautionary Tales from the Front Lines



JAMES FINLAY

Lead Director of Incident
Response, Asia-Pacific

Coveware

SLIDES CAN'T BE SHARED DUE TO CONFIDENTIALITY



First-Hand Lessons

An Insured's Cyber Incident Story



EDWIN LIM

—
Partner

Hudson Gavin Martin



9:00am
DISCOVERY



notified Broker & Emergence IR

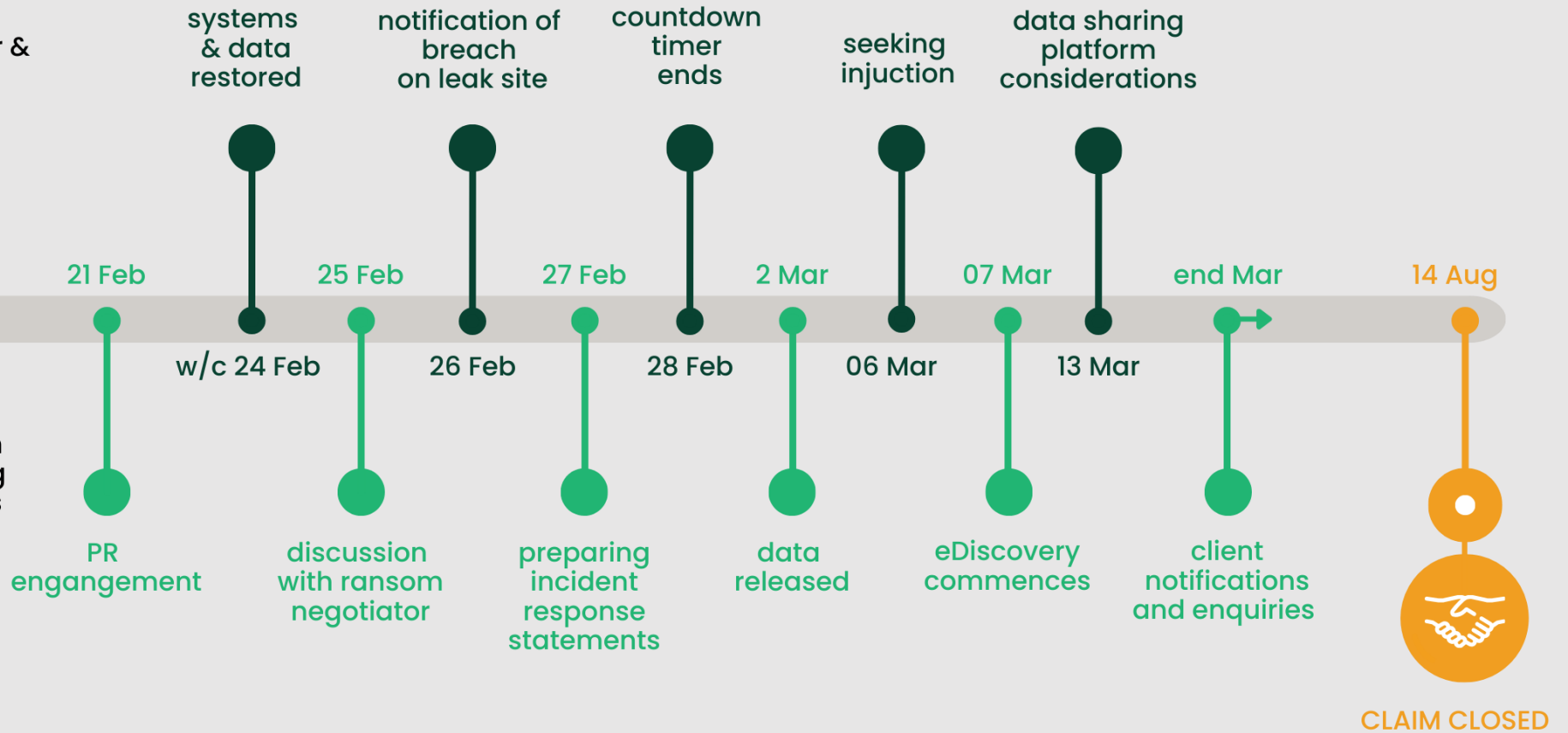


10:30am
initial IR call

18 Feb



forensic investigation & securing / restoring systems commences



CLAIM CLOSED



Demonstrating Real-World Threat Actor Tactics

Cyber-Attack
Simulations



BRENDAN PAYNE

—
Partner

McGrathNicol



ANDREW MCMASTER

—
Manager

McGrathNicol

Agenda

- Case Study 1: Ransomware
- Cyber-Attack Simulation 1: Info Stealer
- Case Study 2: Business Email Compromise
- Cyber-Attack Simulation 2: Multi-Factor Authentication Bypass
- Mitigation Strategies



Case Study 1

—
Ransomware



Ransomware Overview

Ransomware is a business disruption event, not just a cyber incident.



Decline in ransom payments



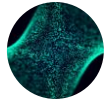
Preparedness varies



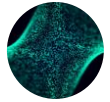
70+ Ransomware groups



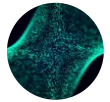
What is an Infostealer?



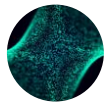
Infostealers are a class of malware designed to quietly steal sensitive information



Once installed, infostealers operate in the background



Stolen credentials are rapidly monetised or reused



Sold as malware-as-a-service, lowering the barrier to entry for cybercriminals and driving widespread adoption

Autumn is approaching 🍂🍂🍂🍂, it's time to get back to work.
Be sure to get your LummaC2 subscription at a discounted rate from 24.08 to 31.08.

Experienced ~~250\$~~ 225\$
Professional ~~500\$~~ 450\$
Corporate ~~1000\$~~ 900\$

Buy subscription right now - @lummaseller126

[Полное описание LummaC2 \(КЛИК\)](#)
[Full description of LummaC2 \(CLICK\)](#)
[Чат / Chat](#)

Save password?

Username

Password

Passwords are saved in your Google Account so that you can use them on any device



Lumma Infostealer – Information Captured

System information and stored credentials captured from the victim's device

LummaC2, Build 20231409

LID(Lumma ID): BhgGkI--IB2

- PC: [REDACTED]
- User: [REDACTED]
- Domain:
- Workgroup: [REDACTED]
- ComputerNameDnsHostname: [REDACTED]
- ComputerNameNetBIOS: [REDACTED]
- OS Version: Windows 10 (10.0.19045)
- HWID: [REDACTED]
- Screen Resoluton: 3840x2160
- Language: en-US
- CPU Name: Intel(R) Core(TM) i7-6700K CPU @ 4.00GHz
- GPU: NVIDIA GeForce RTX 3060
- Physical Installed Memory: 32768MB

- IP Address: [REDACTED]
- Country: AU

Брут и отработка криптоы 70/30 > <https://t.me/HUBHEAD>

Депозит на форумах 5BTC. Берем балансы от 1000\$. За время работы снято более 5.000.000\$
Brute and withdraw cryptowallets 70/30

SOFT: Chrome

URL: <https://www.bcf.com.au/Member/Login>

USER: [REDACTED]

PASS: [REDACTED]

SOFT: Chrome

URL: <http://www.entropialife.com/about/Signup.aspx>

USER: [REDACTED]

PASS: [REDACTED]

SOFT: Chrome

URL: <https://www.seek.com.au/jobdetails/29883139/apply>

USER: [REDACTED]

PASS: [REDACTED]

SOFT: Chrome

URL: <https://login.eveonline.com/Account/LogOn>

USER: [REDACTED]

PASS: [REDACTED]

SOFT: Chrome

URL: <https://www.polarpersonaltrainer.com/>

USER: [REDACTED]

PASS: [REDACTED]

SOFT: Chrome

URL: <https://careers.careersaustralia.edu.au/jobtools/jncustomlogin.JobSeekerToolBoxAction>

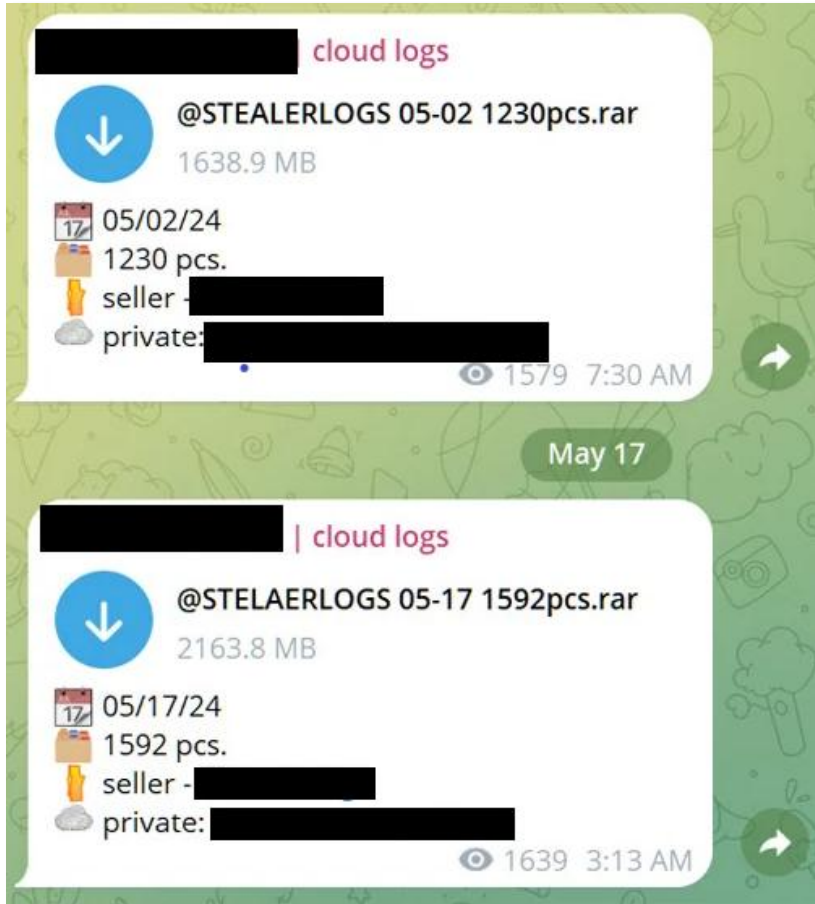
USER: [REDACTED]

PASS: [REDACTED]



Cyber Threat Intelligence – Credentials For Sale

Credentials sold and bough on dark web



"Brute and crypto mining 70/30 > <https://t.me/HUBHEAD>

Deposit on forums 5BTC. We take balances from \$1000. Over \$5,000,000 withdrawn during operation

Brute and withdraw cryptowallets 70/30"



Infostealers are a class of malware designed to quietly steal sensitive information



Once installed, infostealers operate in the background



Stolen credentials are rapidly monetised or reused



Threat Actor Group – LockBit 3.0

Dark web leak site

The screenshot shows the LockBit 3.0 website interface. At the top left is the LockBit 3.0 logo. A prominent red banner reads "LEAKED DATA". Navigation links include "TWITTER", "PRESS ABOUT US", "HOW TO BUY BITCOIN", "AFFILIATE RULES", "CONTACT US", and "MIRRORS". The main content area displays four data leak entries, each with a red or green header bar, a timestamp, and a view count. The first three entries have red headers and show update times from Feb 2025. The fourth entry has a green header with the word "PUBLISHED" and an update time from Jan 2025. On the right side, a grey box titled "Doxing" contains text describing a \$1 million payout for identifying affiliates.

Entry	Header	Update Time	View Count
1	Red	Updated: 10 Feb, 2025. 16:10 UTC	516
2	Red	Updated: 03 Feb, 2025. 16:23 UTC	5542
3	Red	Updated: 03 Feb, 2025. 16:19 UTC	6800
4	Green (PUBLISHED)	Updated: 26 Jan, 2025. 06:02 UTC	15975

Doxing

We pay exactly one million dollars, no more and no less, for doxing the affiliate program boss. Whether you're an FBI agent or a very clever hacker who knows how to find anyone, you can write us a TOX messenger, give us your boss's name, and get \$1 million in bitcoin or monero for it.

We have no payout limits - you can encrypt RDP individuals or companies with any income level, any payout is nice for us - both \$5,000,000 and \$50 million, because we love our work and the process itself, and money is just a nice addition.



Initial Access, Data Exfiltration and Deployment

Dark web leak site

Please Login

Name

Password

Login

Launch FortiClient

Recently.docx.lockbit	LOCKBIT File
ResetReceive.doc.lockbit	LOCKBIT File
Restore-My-Files.txt	Text Document
SavePush.vsd.lockbit	LOCKBIT File
ShowSuspend.xla.lockbit	LOCKBIT File

Negotiation Logs

Hello?

DATE REDACTED

Hello

DATE REDACTED

You will be sent a File List with the files we took from you, you can also choose 4-5 files to demonstrate decryption and send them to the chat room

Contacting any government agencies before this situation is resolved may negatively affect the negotiations.

A text file with a list of the stolen data: <http://temp.sh/QpBWi/filelist.txt>

DATE REDACTED

After transferring 300000\$ in Bitcoin you get:

1. A full report on your vulnerabilities and recommendations for their elimination.
2. Decryption key.
3. A log of your data deletion from our vaults.

DATE REDACTED

Ok thank you. We will review this. Is this a list of everything you took from us?

DATE REDACTED

Yes

DATE REDACTED

There are 6 days until your data is published and the decryption key is destroyed, by which time the transaction should be done

You can also send us 4 encrypted files, we will send you decrypted copies

DATE REDACTED

DATE REDACTED

We have looked at the list. Can you prove you have these files?

TEXT REDACTED



Stolen credentials belonged to corporate IT Administrator for corporate VPN



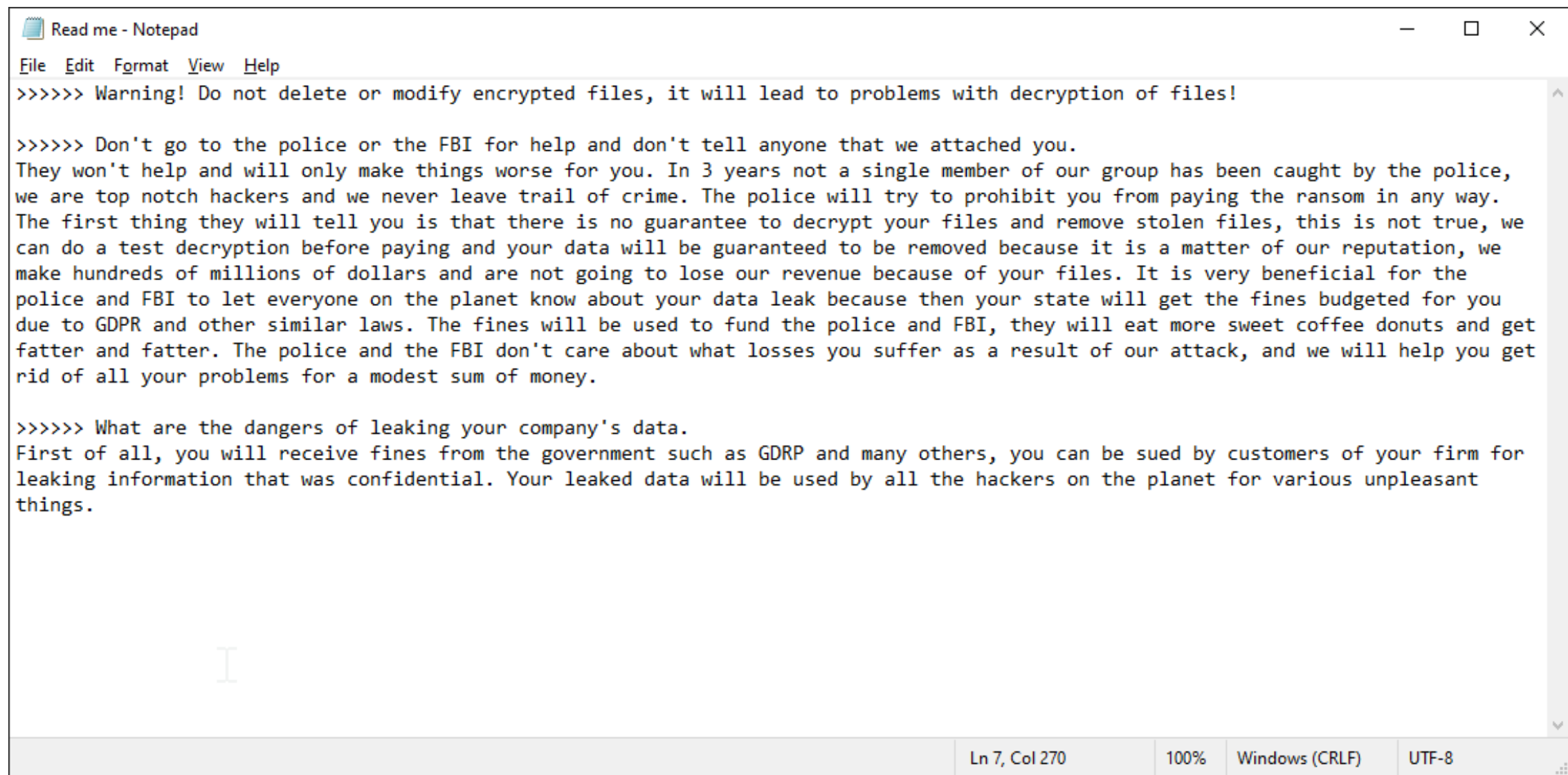
Remains undetected inside network for two weeks exfiltrating data



The ransomware payload is executed across the network, encrypting critical infrastructure such as operational servers.



The Ransom Note



Read me - Notepad

File Edit Format View Help

>>>>> Warning! Do not delete or modify encrypted files, it will lead to problems with decryption of files!

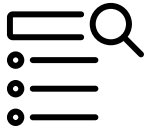
>>>>> Don't go to the police or the FBI for help and don't tell anyone that we attacked you. They won't help and will only make things worse for you. In 3 years not a single member of our group has been caught by the police, we are top notch hackers and we never leave trail of crime. The police will try to prohibit you from paying the ransom in any way. The first thing they will tell you is that there is no guarantee to decrypt your files and remove stolen files, this is not true, we can do a test decryption before paying and your data will be guaranteed to be removed because it is a matter of our reputation, we make hundreds of millions of dollars and are not going to lose our revenue because of your files. It is very beneficial for the police and FBI to let everyone on the planet know about your data leak because then your state will get the fines budgeted for you due to GDPR and other similar laws. The fines will be used to fund the police and FBI, they will eat more sweet coffee donuts and get fatter and fatter. The police and the FBI don't care about what losses you suffer as a result of our attack, and we will help you get rid of all your problems for a modest sum of money.

>>>>> What are the dangers of leaking your company's data. First of all, you will receive fines from the government such as GDRP and many others, you can be sued by customers of your firm for leaking information that was confidential. Your leaked data will be used by all the hackers on the planet for various unpleasant things.

Ln 7, Col 270 100% Windows (CRLF) UTF-8



Breach Announcement



lockbit

LOCKBIT 3.0

LEAKED DATA

TWITTER > HOW TO BUY BITCOIN > CONTACT US >
PRESS ABOUT US > AFFILIATE RULES > MIRRORS >

Deadline: [REDACTED]

[no logo] [REDACTED]

UPLOADED: 31 JAN, 2024 21:17 UTC UPDATED: 31 JAN, 2024 21:17 UTC

Until the files will be available left
14D 14h 25m 31s

*Download archives from reserve servers
14D 14h 25m 31s

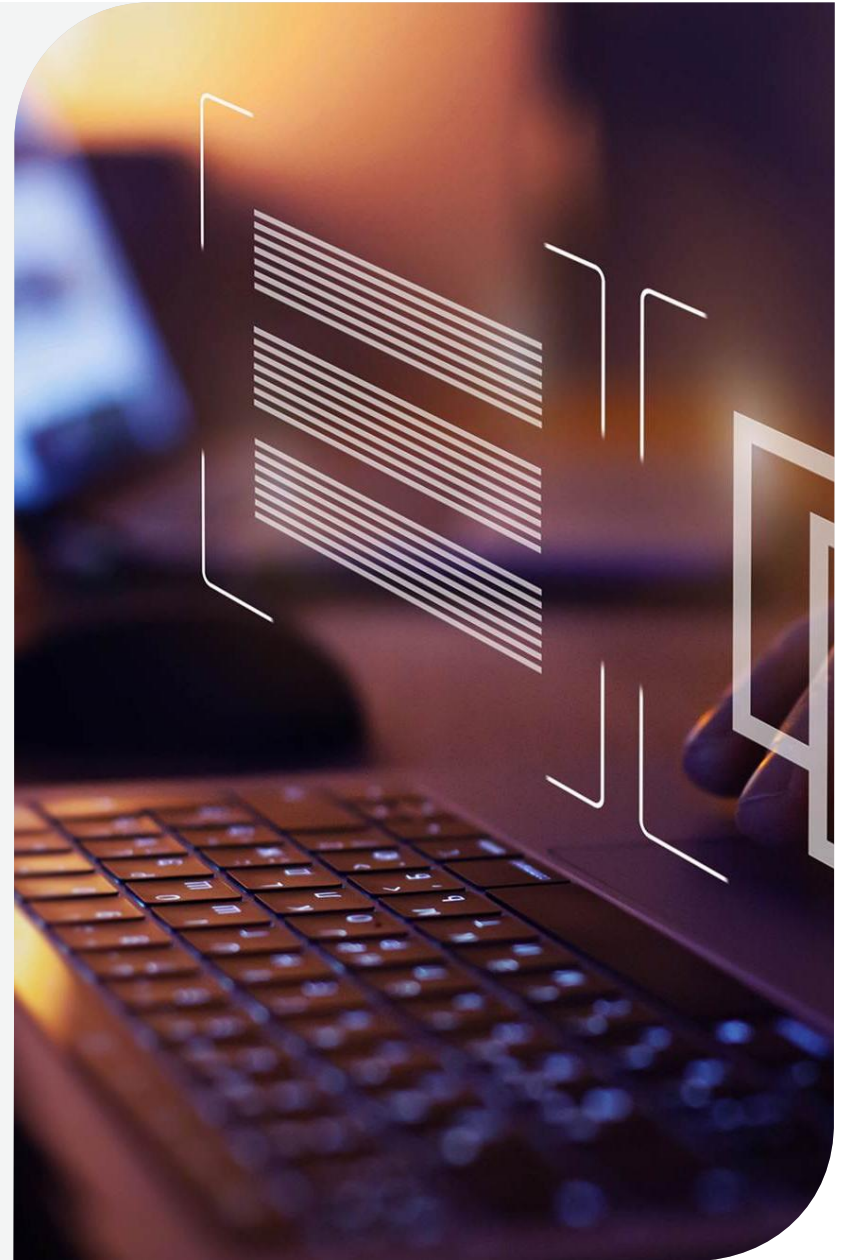
LINK #1



Cyber-Attack Simulation 1

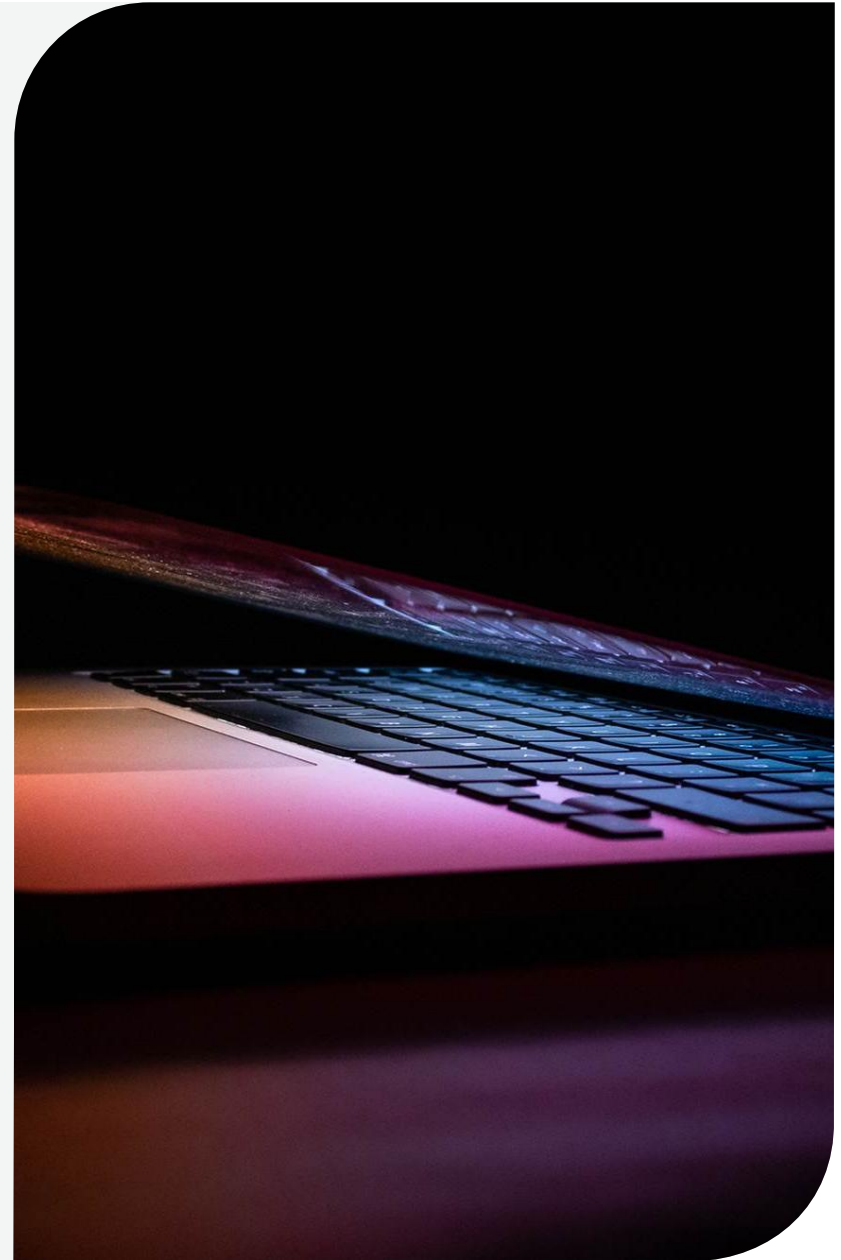
—

Attack Type: Infostealer



Case Study 2

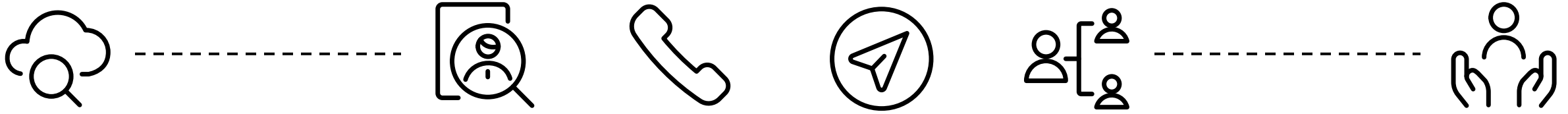
Business Email Compromise



Attack Vector



Phase 1 - Research



Bloomberg

THE WALL STREET JOURNAL.

LinkedIn

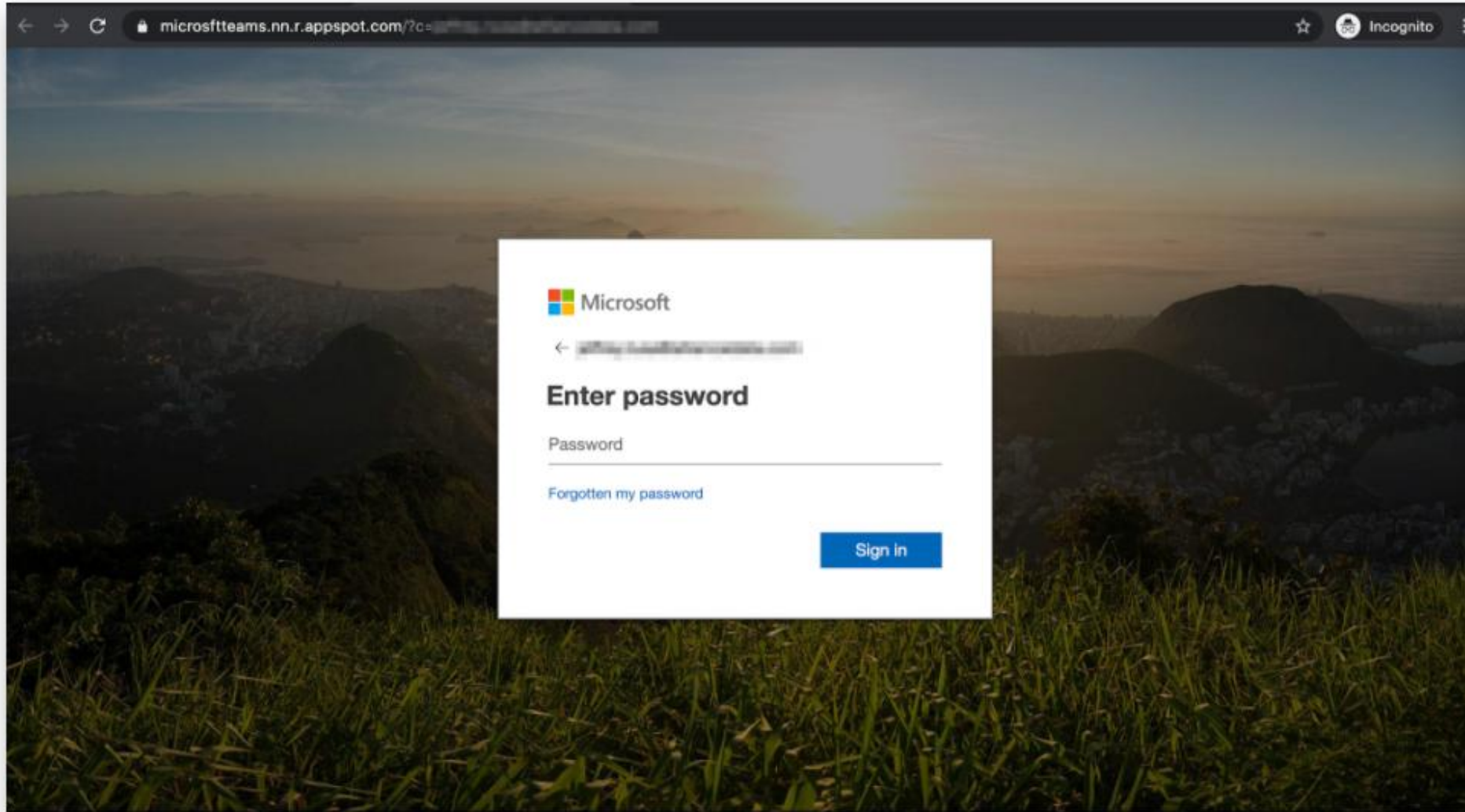
facebook



reddit



Phase 2 – Prepare



Phase 3 - Execution



Actioned by: Threat actor



Mailbox From: External user



Recipient: CFO

FP [redacted] 4:09 AM
Finance policy <rkayyar@lcnpl.com>
Updated [redacted]

To [redacted]
This message was sent with High importance.

attachments.html
448 bytes

Dear All,

Please find attached [redacted] Financial rules and policies for year [redacted]

All department Managers/heads are required to kindly contact your functional head for your goal setting process for [redacted]

Regards,
Human Resources
[redacted]



Phase 3 - Execution

The screenshot displays the Microsoft Outlook interface in a dark theme. The top ribbon includes tabs for File, Home, Send / Receive, Folder, View, MacroView, Help, McGrathNicol, and Acrobat. The Home tab is active, showing various action groups such as New, Delete, Respond, Teams, Quick Steps, MacroView, Move, Tags, Groups, and Find. A search bar is located at the top right.

The left-hand navigation pane shows a list of folders, with 'Conversation History' selected and highlighted. Below it, other folders like 'Inbox', 'Drafts', 'Sent Items', 'Deleted Items', 'Junk Email', 'Outbox', 'RSS Subscriptions', and 'Search Folders' are visible.

The main content area is divided into two panes. The left pane, titled 'Conversation History', shows a list of messages under the 'Today' group. The selected message is 'Example email to bank' from 'Brendan Payne' (Partner), dated '3:14 PM'. The right pane displays the details of this email, including the sender's profile picture and name 'Brendan Payne', the recipient 'To: Brendan Payne', and a 'Highly Confidential' warning icon.



Phase 3 - Execution



Actioned by: Threat actor



Mailbox From: CFO



Recipient: Bank

From: [REDACTED]
Sent: [REDACTED] 2:50 PM
To: [REDACTED]
Cc: [REDACTED]
Subject: EXTERNAL [REDACTED] New Online Banking Administrators

Hi folks.

I am delighted to introduce you all to the newly appointed Controller and Assistant Controller in persons of Christian [REDACTED] and David [REDACTED] (both copied on this email) and have them enrolled as Administrators in [REDACTED]

Christian and David should both be granted full authorities, approvals, and privileges in [REDACTED] banking with full access to Cash Management services (wire transfer) under dual control security setup where one person initiates a payment and the other approves.

Following their new roles, they would be handling all Treasury related activity, payments and operations going forward.

Christian and David resumed appointment on [REDACTED]

Thank you.



Phase 3 - Execution



Actioned by: Bank



Mailbox From: Bank



Recipient: CFO

From:

Sent: [REDACTED] 18:03

To:

Cc:

Subject: RE: EXTERNAL: [REDACTED] New Online Banking Administrators

Hi [REDACTED]

Thank you for the introduction and I look forward to working with you both, David and Christian.

Do you have two active System Admins on [REDACTED] If so, then you'll need to add them through the entitlement screens. I've attached a guide for you here, which is hopefully helpful.

In the event you don't have two System Admins, we can look into a work-around, but it's unfortunately not a simple process as we don't generally add users due to liability and security.

Thank you,



Phase 3 - Execution



Actioned by: Bank



Mailbox From: Bank



Recipient: CFO

Cc:

Subject: RE: EXTERNAL: Re: [REDACTED] New Online Banking Administrators

Hi

Absolutely. I'll start the process to have the additional administrators added. We'll need some personal information on Christian and David in order to populate the paperwork. In addition to what you've already provided us, can you please let us know the following:

- Date of birth
- Cell Phone and office phone numbers
- Address (can be an office address, but this would be for token delivery if required)
- If you would prefer a hard token or a mobile token for authentication

On an unrelated note, I was wondering if you had any availability next week for a call with our Senior Management. They just wanted to express to you directly how profusely apologetic we are for the delays and communication related to the [REDACTED].

Thank you,



Phase 3 - Execution



Actioned by: Threat Actor



Mailbox From: CFO



Recipient: Bank

From:
Sent: Thursday, [REDACTED] 9:26 AM
To:
Cc:
Subject: EXTERNAL: Re: Re: [REDACTED] - New Online Banking Administrators

Hi Cara,

As requested, please see the below information for Christian and David:

Christian
Date of birth: 06/28/1967
Cellphone: (847) 756-8330
Office: (847) 756-1772

David
Date of birth: 08/16/1962
Cellphone: (847) 756-8457
Office: (847) 756-2231

They would both prefer a mobile (soft) token.

Regarding the call, I will have to check my calendar on dates and times I am available next week. 😊

Thank you



Phase 3 - Execution



Actioned by: Bank



Mailbox From: Bank



Recipient: CFO

From:
Sent: [REDACTED] 10:21
To:

Cc:
Subject: RE: EXTERNAL: Re: Re: [REDACTED] - New Online Banking Administrators

H [REDACTED]

Thank you for these details. We'll get the request to add Christian and David as SAs right away.

I look forward to hopefully meeting you via Zoom next week and appreciate you looking into your availability.

Warm Regards,



Phase 3 - Execution



Actioned by: Bank



Mailbox From: Bank



Recipient: CFO

Sent: [REDACTED] 9:34:34 AM

Dear [REDACTED]

By way of introduction, my name is [REDACTED] and I work for [REDACTED] team. We have received a request to add new system administrator to the [REDACTED]

Attached is the required [REDACTED] document. Please print the document, complete and have it executed in accordance with the appropriate bank mandate(s) and reply to this e-mail with the scanned document for further review.

Post review, I will keep you posted on the next step for the setup. It is our goal to have your request completed at the earliest. Please ensure you inform us of any delays which may keep us from meeting this goal.

Your satisfaction with the way we implement your new products is very important to us. We may send you a survey so you can let us know how we did in meeting your expectations. If you do receive a survey, please take a few minutes to complete it so we can use your feedback.

Please feel free to call or email me, if you have any questions or need additional information.



Phase 3 - Execution



Actioned by: Bank



Mailbox From: Bank



Recipient: CFO

Sent: [REDACTED] 9:27:18 AM

Hi [REDACTED]

Unfortunately we received the below feedback from our [REDACTED] Verification Team:

Per the bank mandate, [REDACTED] is not authorized to sign. See below for authorized signers who must sign jointly.

Can you please have the forms re-signed according to the bank mandate?

Thank you,



Phase 3 - Execution



Actioned by: Threat Actor



Mailbox From: CFO



Recipient: Bank

Sent: [REDACTED] 1:47:28 PM

Hi Cara,

Please find the attached completed documents with 2 signatories present as requested.

Kindly confirm receipt.

Best Regards,



Phase 3 - Execution



Actioned by: Bank



Mailbox From: Bank



Recipient: CFO

Dear [REDACTED]

I am pleased to inform you that we have completed the implementation of the following Services:

Adding 2 new System Administrators

Please note that it may take 24 to 48 hours before the account/service is visible on their [REDACTED]

Please be sure to have the System Administrator(s) make the necessary changes to the Entitlements.

The Customer Relationship Center will serve as your main point of contact going forward. Their hours of operation are 8:00 - 21:00 EST. Their telephone numbers are listed below for your reference.

[REDACTED]

Should you have questions about adding new services, please contact your [REDACTED]

Your satisfaction with the way we implement your new products is very important to us. We may send you a survey so you can let us know how we did in meeting your expectations. If you do receive a survey, please take a few minutes to complete it so we can use your feedback.

It was a pleasure working with you and your team and we thank you for your business and look forward to working with you in the future.



Phase 3 - Execution



Actioned by: CFO



Mailbox From: CFO



Recipient: Bank

From: [REDACTED]
Sent: [REDACTED] 3:17
To: [REDACTED]
Subject: EMERGENCY. Fraud \$3.1M

Please call me ASAP.

[REDACTED]

Or

[REDACTED]



Phase 3 - Execution



Actioned by: Threat Actor



Mailbox From: CFO



Recipient: Bank

From: [REDACTED]
Sent: Monday [REDACTED] 1:25:38 PM
To: [REDACTED]
Cc: [REDACTED] (Spoofed email address)
Subject: EXTERNAL: Re: EMERGENCY. Fraud \$3.1M

Never mind. I just rectified with [REDACTED] (copied) that the payment was for a [REDACTED] request that was received today.

Please ignore the initial fraud alert.

Thanks



Phase 3 - Execution



Actioned by: Bank



Mailbox From: Bank



Recipient: CFO

Re: EXTERNAL: Re: EMERGENCY. Fraud \$3.1M



To
Cc



If there are problems with how this message is displayed, click here to view it in a web browser.

No problem [REDACTED] Sorry for calling you back late. Let me know if any further assistance is required

Regards,



Phase 3 - Execution



Actioned by: Threat Actor



Mailbox From: Spoofed



Recipient: CFO

EXTERNAL: Re: EMERGENCY. Fraud \$3.1MPR



[Redacted] (Spoofed bank email address)

To [Redacted]

Hello [Redacted],

I have submitted a request to our fraud department and immediate action has been taken to recover funds and [Redacted] access has been suspended for the meantime due to fraud protection.

I will let you know once I hear back from the fraud department.

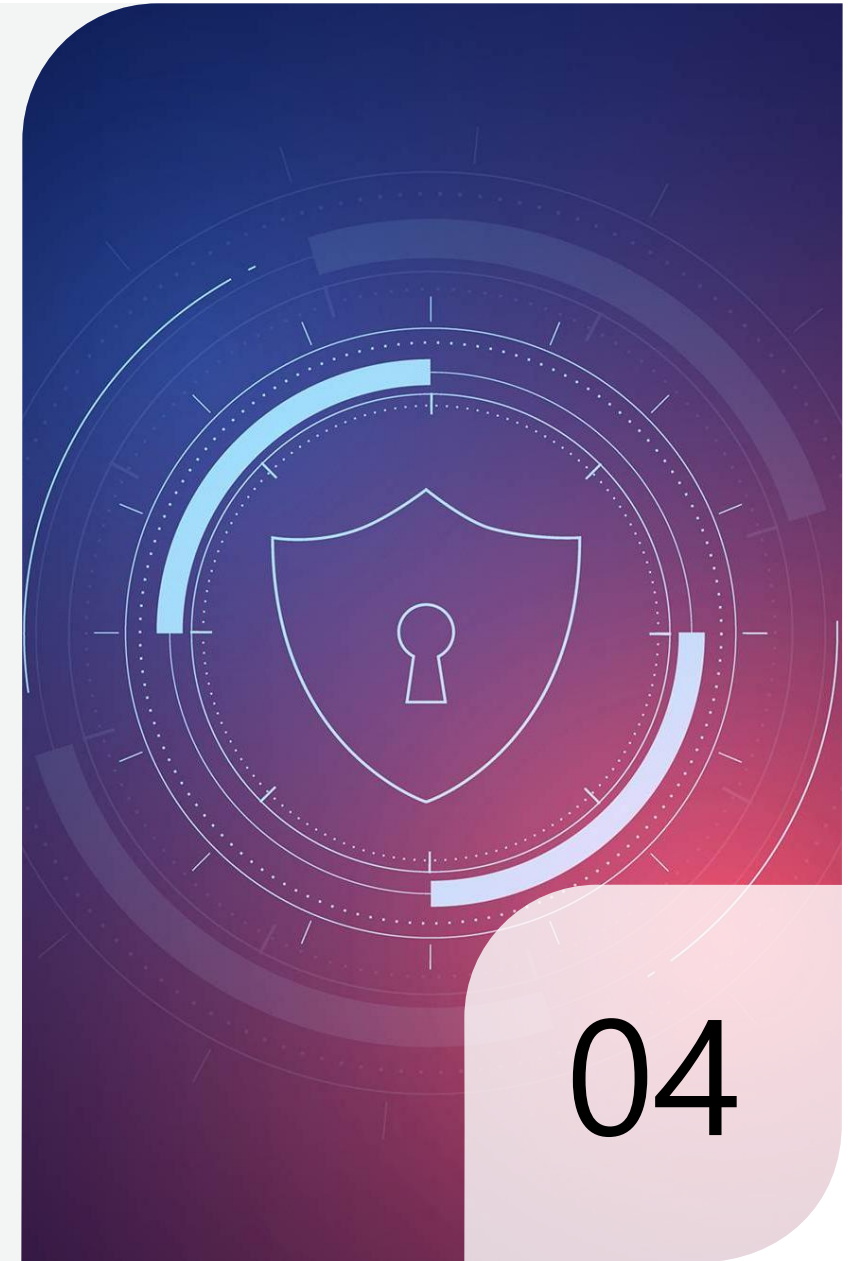
Regards,



Cyber-Attack Simulation 2

—

Attack Type: Multi-Factor Authentication Bypass



Mitigation Strategies



Protect

- Multi-factor authentication
- Email filtering
- Patch management policy
- Security awareness training



Detect

- Extended detection & response
- Account monitoring
- Centralised logging & alerting
- Threat intelligence monitoring



Contain

- Principle of least privilege
- Network segmentation
- Automated endpoint isolation
- Pre-defined IR workbook



Recover

- Immutable backups & testing
- Disaster recovery plan
- Post-incident review
- Cyber insurance policy





The Anatomy of Cyber Incident Response



Shane Bell

CEO

NSB Cyber



Joseph Fitzgerald

Partner

Wotton & Kearney



Russell Pilcher

Strategic Communications Principal

NCSC



Troy Filipcevic

CEO

Emergence Insurance



THANK YOU



CYBER SYNC UP

