

The background image is a dark, atmospheric scene of a lighthouse on a beach at night. A bright lightning bolt strikes the sea in the distance, illuminating the dark clouds and water. The lighthouse is silhouetted against the dark sky, with its light glowing from the top. The overall color palette is dominated by deep blues, purples, and blacks, creating a sense of mystery and danger.

axians

# INSIDE RANSOMWARE

Presented by Martin Lutz



# Martin Lutz



## Senior Security Professional

Martin Lutz is a Senior Security Professional with a demonstrated history of growing brands, products, and ideas. He is skilled in leading international teams with a cross-cultural mindset to achieve EBIT, CAPEX and OPEX targets. Through his years of experience as Country Manager, Head of Business Development, Senior Product Manager and Head of Operations in Switzerland, Singapore, and Germany, he gained first-hand knowledge of what it takes to develop and execute brand strategies, establish, and enforce improvement programs and expand businesses into new markets.

He held P&L responsibility of up to USD 25 million, forged strong relationships with clients and strategic partners, and led international teams of >15 FTE. His passion is to lead, inspire and encourage industry specialists to maximize their capabilities to the fullest potential and delivering high quality, customer-centric products.

Mr. Lutz holds a bachelor's degree in Business Informatics from the Cooperative State University Mannheim (DHBW) and was also within Deutsche Telekom's Manager Development Program to further enhance his management and leadership skills.

## DISCLAIMER:

The following content is my personal view. The purpose in this presentation is to raise awareness and not to promote hacking or any other criminal activities. Any actions and or activities related to the material contained within this presentation is only for awareness purposes. The misuse of this information can result in criminal charges brought against the persons in question. The author will not be held responsible in the event any criminal charges be brought against any individuals misusing the information in this presentation to break the law.



This is not about  
me. This is about  
Hugo.

axians



Hugo just lost his  
job.

## What he thinks:

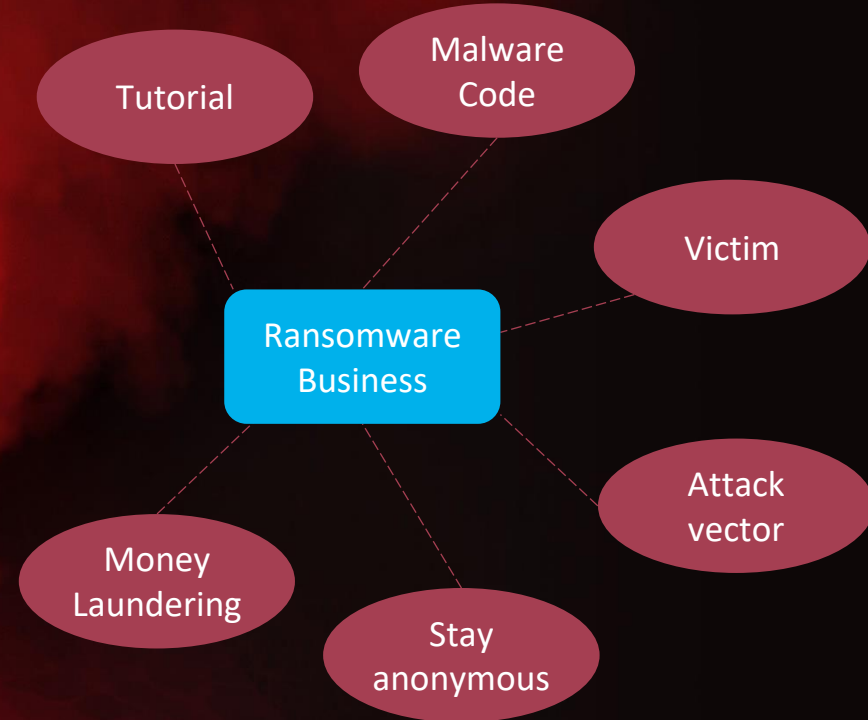
- Costs: Low
- Risk: Low
- Outcome: Big

He is desperate. So  
he makes a decision.





What does it  
need to build  
a ransomware  
business?



First Step

axians





First Step

axians

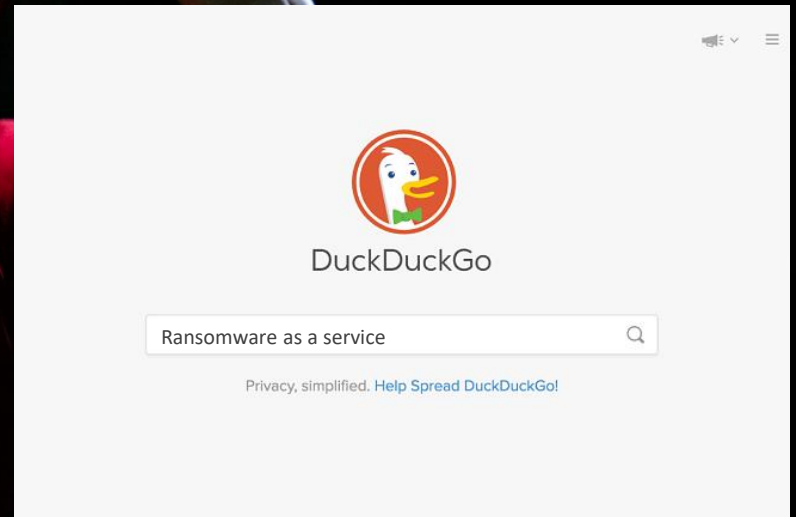
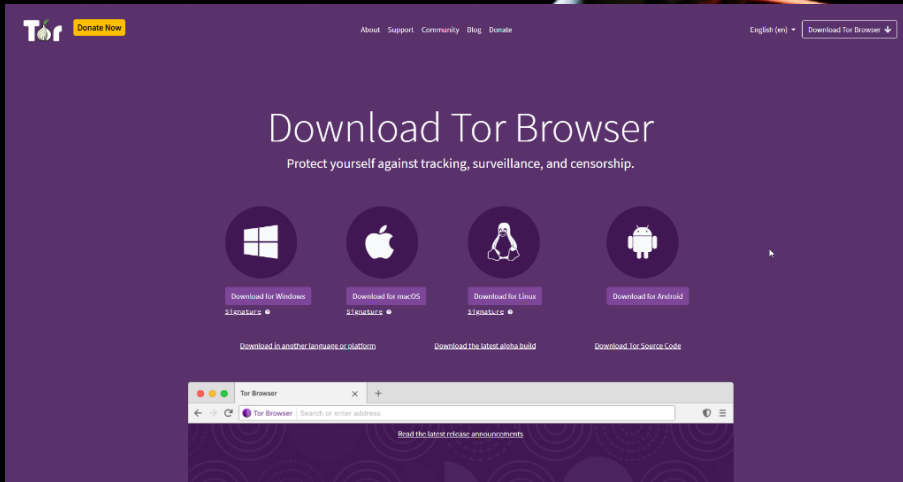
Google

And Then...

axians



# Find the entry point





# BUY "KARMEN" THE RANSOMWARE-AS-A-SERVICE

axians

Karmen Hello, DevBit0x

Dashboard Statistics Overview

1 Clients 0 Payments 0 Earned 1284\$ Bitcoin Price

Updates

- New Design + Bug fix 22 Feb
- Critical bug fixed 20 Feb
- New program design 20 Feb
- Fix program bug 18 Feb
- Release new version 15 Feb
- Test new version 14 Feb

Infos

- Current version: 2.4
- Price to unlock: 1,283 BTC
- Don't forget update you key!
- Contact jabber: devbit0x@sig.ms
- Contact Telegram: @DevBit0x

Karmen Hello, DevBit0x

Settings

Dashboard / Settings

New password

Enter new password

Enter password here

Change password

New API Key

New key

New key here

Change API Key

New price

Enter price in satoshi Convert | Example

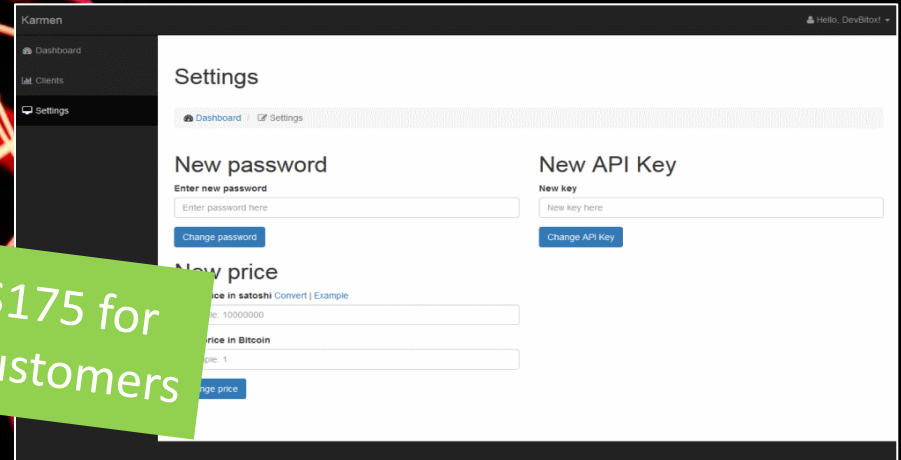
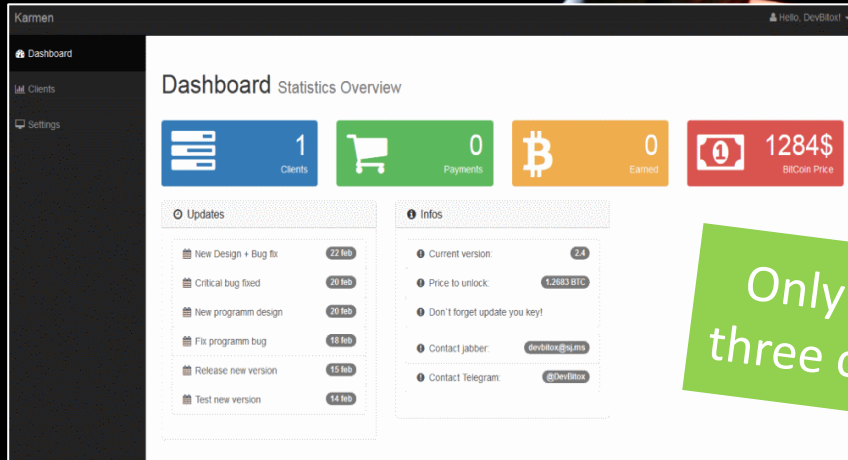
Example: 10000000

Enter price in Bitcoin

Example: 1

Change price

# BUY "KARMEN" THE RANSOMWARE-AS-A-SERVICE



Only \$175 for  
three customers

## Benefits:

- Multi-language
- Encryption algorithm: AES-256
- Adaptive admin panel
- Encrypts all discs and files
- Separate BTC wallet for each victim
- Automatic deletion of malware after payment was received
- Minimal connection with control server

NEXT STEP: FIND AND PROFILE A VICTIM

axians





## NEXT STEP: FIND AND PROFILE A VICTIM

axians



The diagram illustrates a search process. At the top, a Google search bar contains the text 'ask google'. A large blue arrow points from the search bar to a webpage. The webpage is for ResearchFDI, featuring a navigation menu with links for HOME, ABOUT, SERVICES, PRODUCTS, OUR WORK, and CONTACT, along with a 'LET'S TALK' button. The main content area has the heading 'INDUSTRIES THAT SAW GROWTH DURING THE COVID-19 PANDEMIC' and a byline 'BY BRUCE FRANKLIN | JUNE 22ND, 2020 | NEWS & MEDIA'. The ResearchFDI logo is visible in the top left of the page.

## NEXT STEP: FIND AND PROFILE A VICTIM

axians



Maltego is an open-source intelligence and forensics application which gathers information of victims and represents it in a graph.



Follow  
Youtube  
Tutorial

Source: Youtube.com

# NEXT STEP: FIND AND PROFILE A VICTIM

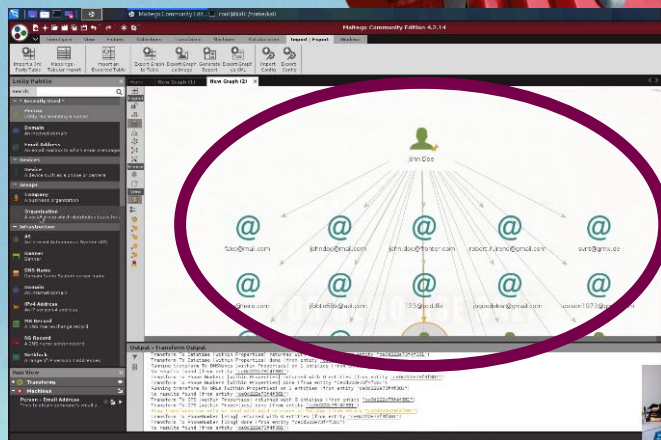


Maltego is an open-source intelligence and forensics application which gathers information of victims and represents it in a graph.

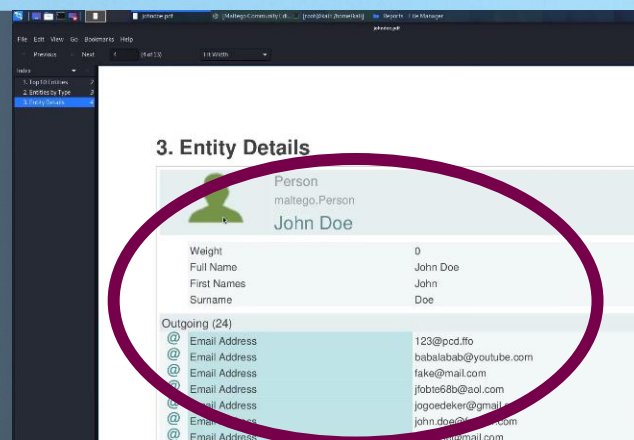


Follow Youtube Tutorial

Source: Youtube.com



"John Doe" will be our (random) victim to be attacked.





## WHAT HUGO FOUND OUT

axians



## WHAT HUGO FOUND OUT

axians



Plan: Build an email with a special offer for an boat some time before John Doe typically goes on vacation. This email will have an attachment with the ransomware.

ALRIGHT. LET'S BUILD THE ATTACHMENT

axians

What does Hugo need?





ALRIGHT. LET'S BUILD THE ATTACHMENT

axians

What does Hugo need?



Google

# ALRIGHT. LET'S BUILD THE ATTACHMENT

axians



The screenshot shows a web page with a dark navigation bar containing categories like 'WONDERHOWTO', 'GADGET HACKS', 'NEXT REALITY', 'NULL BYTE', 'CYBER WEAPONS LAB', 'FORUM', 'METASPLOIT BASICS', 'FACEBOOK HACKS', 'PASSWORD CRACKING', 'TOP WI-FI ADAPTERS', 'WI-FI HACKING', 'LINUX BASICS', and 'MR. ROBOT HACKS'. The main content area has a green 'HOW TO' tag and a title 'Create & Obfuscate a Virus Inside of a Microsoft Word Document' by 'CODE'. The text describes a VBA script macro for a mass mailer attack. A 'Bonus' section mentions a PDF of the post. A red-bordered box at the bottom contains the word 'Metasploit'.

W

hen performing something such as a mass mailer attack on a company, sending executables usually isn't the best option. That's why, in this tutorial, I'll be teaching you how to code a VBA script macro into a Word document in order to compromise a system. Combined with a little social engineering, this can be a very effective technique.

**Bonus:** There's a really nice [PDF](#) of this post thanks to [TRT](#) (who has some really well-written tutorials by the way) in case you're having trouble with the formatting of this website.

**Metasploit**

Source: <https://null-byte.wonderhowto.com/>

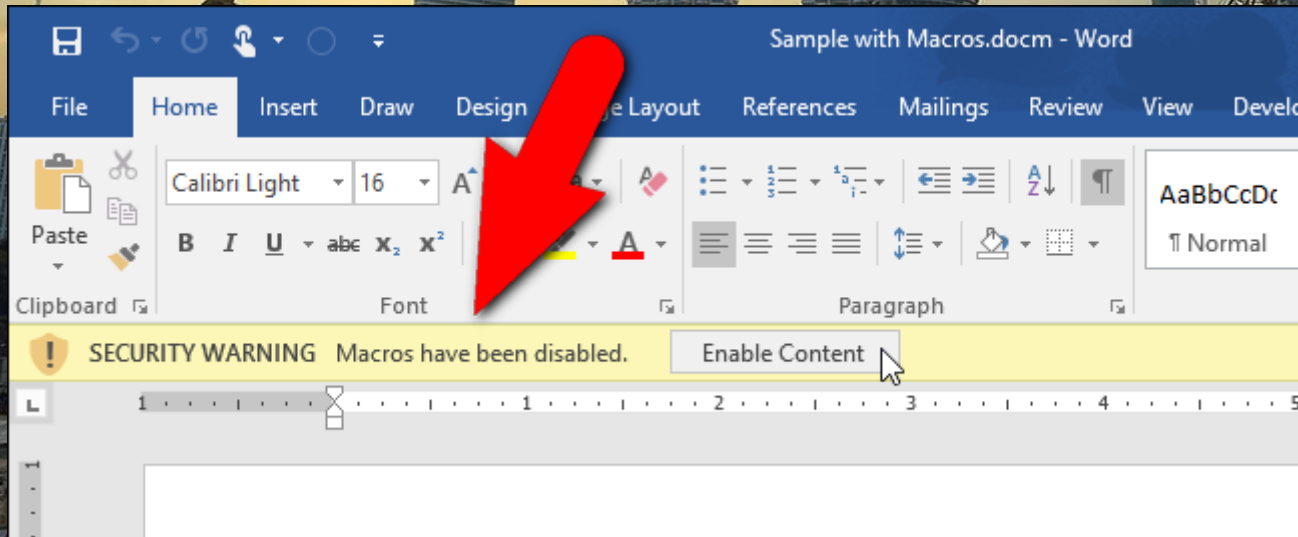
## Requirements to follow tutorial:

1. Microsoft Word
2. The Social-Engineer Toolkit (preinstalled on Kali)
3. Apache web server (preinstalled on Kali)
4. The Metasploit Framework (also preinstalled on Kali)



# ALRIGHT. LET'S BUILD THE ATTACHMENT

Disadvantage Word: John Doe has to enable macros before being able execute Hugos Ransomware.







# AND NOW THE EMAIL

Feel Good Weeks: Now special offer for boats, Mr. Doe

Miles & More <mail@mailing.milesandmore.com>

Special Offer.docx  
.docx-Datei

Open E-Mail in Browser

Miles & More | Lufthansa

World Shop  
Lufthansa

Feel Good Weeks: Save up to 30% on boat rental

This week you can look forward to a 20% discount on boat rental. A selection of products from our sports range with the promotional code Boat201. Get more details within the document attached.

Make it look like it is really coming from Miles and More. But it is not...

Word document with ransomware

READY TO BE SEND. BUT HOW TO STAY ANONYMOUS?

axians

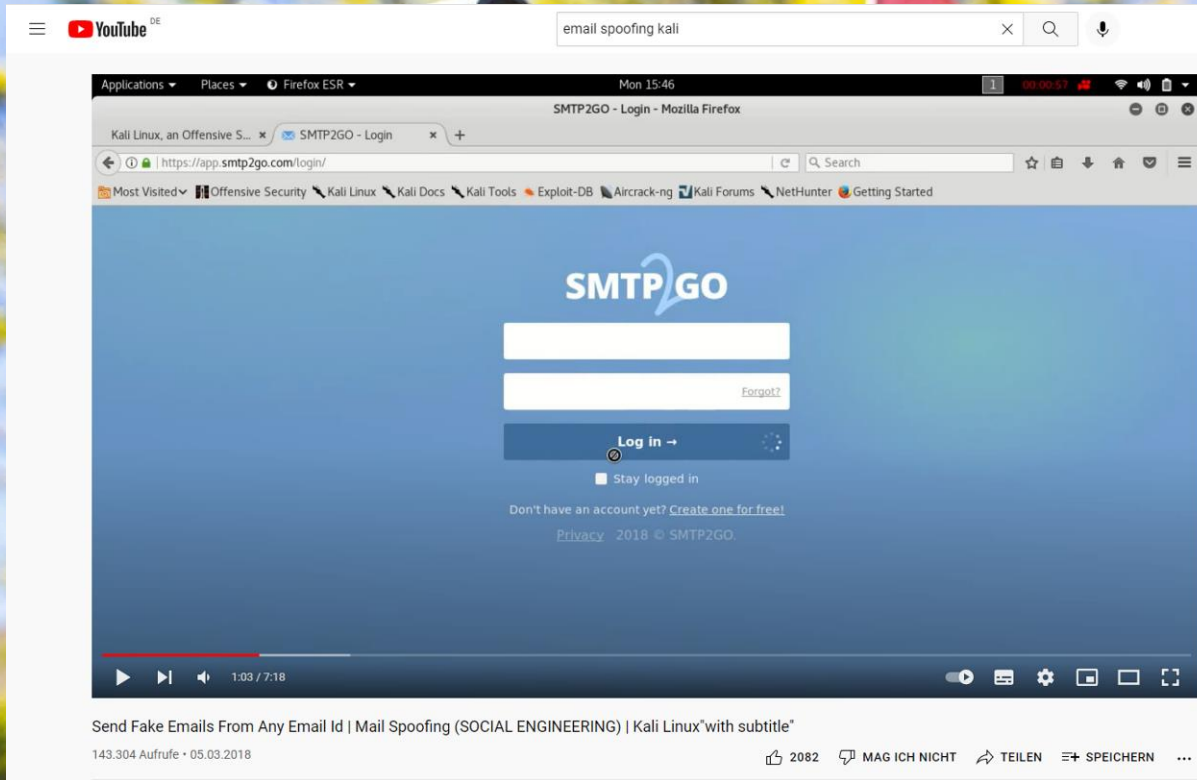
**Easy: Spoofing!**

U.S. MAIL  
APPROVED BY THE  
POSTMASTER GENERAL



READY TO BE SEND. BUT HOW?

axians



The screenshot shows a YouTube video player. The video content is a browser window displaying the SMTP2GO login page. The browser's address bar shows the URL `https://app.smtp2go.com/login/`. The login page has a blue background with the SMTP2GO logo at the top. Below the logo are two white input fields for email and password, with a 'Forgot?' link next to the password field. A blue 'Log in →' button is positioned below the fields, with a 'Stay logged in' checkbox underneath. At the bottom of the page, there is a link to 'Create one for free!' and a footer with 'Privacy 2018 © SMTP2GO.' The video player interface includes a progress bar at 1:03 / 7:18 and a title: 'Send Fake Emails From Any Email Id | Mail Spoofing (SOCIAL ENGINEERING) | Kali Linux® with subtitle\*'. The video has 2082 likes and was uploaded on 05.03.2018.

All Hugo needs:

1. Again Kali Linux
2. SMTP2Go as Email Delivery Service

Source: Youtube.com

HUGO'S PRESENT IS ON ITS WAY

axians



Send email using SMTP2Go through  
the Tor network to John Doe.



THEN...

WAIT...

AND...





THEN...

WAIT...

AND...



WARNING: YOUR FILES HAVE BEEN LOCKED BY HUGO

### ? What happened?

All **your files** have been encrypted. This includes (but is not limited to) Photos, Documents and Spreadsheets.

### ? What now?

You can make a payment of (exactly) 3.33 bitcoin to the following address:  
`bc1q5q38z3qtleglms`

Once the payment has been made we'll follow up with a transaction to the same address, this transaction will include the **decryption key** as part of the transaction details. [[more information](#)]

JOHN DOE PAID.

axians



BUT HOW TO SPEND THE MONEY LEGALLY?

# BUT HOW TO GET THE MONEY?

## Using Google... Again...

Products

Technology

About



Tookitaki  
a Thunes. company

Webinars

Resources

Contact

Subscribe  
to our  
Newsletter

### Money Laundering via Cryptocurrencies: All You Need to Know



Money laundering via cryptocurrency has been going on for a while now. We've all heard of Bitcoin, Ethereum and Dogecoin. Crypto is used by financial criminals globally but how are they getting away with it? It's time we lifted the lid on this crime and decoded what often sounds complicated but doesn't have to be.

This is everything you need to know.

#### What is cryptocurrency?

Simply put, Cryptocurrency is a digital or virtual currency that is protected by encryption, making counterfeiting and double-spending practically impossible. Many cryptocurrencies are built on blockchain technology, which is a distributed ledger



JOHN DOE PAID. BUT HOW TO GET THE MONEY?



WITH THE MONEY HUGO CAN FEED HIS FAMILY AND BOUGHT AN SMALL ISLAND. SOMETIMES HE IS SCARED TO BE CAUGHT. BUT...



HE IS JUST A SMALL FISH IN THE OCEAN



HAPPY END

Each of us will be happen to be a victim of Ransomware any time soon. But we can try to reduce the risk and impact. But how?

- Awareness Training
- Email Gateway Security and Sandboxing.
- Network segmentation.
- Endpoint Detection & Response (EDR) solutions.
- Backup, backup and backup.
- Incident Response Plans.
- Disabled Macros.
- Network Monitoring.



Thank you

