Cyber Threat Landscape of 2021

Dr Erdal Ozkaya

Dr. Erdal Ozkaya
Regional CISO

- Master of IT Security,
- Master of Computing Research,
- MCT, MCSE, ISO27001, ISO30000, CEH, C|CISO…
- Author of many Security Certifications Courseware
- Researcher @ Australian Charles Sturt University

My Books

Cybersecurity - Attack and Defense Strategies
Second Edition
Yuri Diogenes
Erdal Ozkaya
Packt
Dr. Erdal Ozkaya
Learn Social Engineering
Packt
INSIDE THE DARK WEB
Erdal Ozkaya • Rafiqul Islam
CRC Press
Cybersecurity: The Beginner's Guide
Packt
Defence Against Terrorism Review
DATR
COE-DAT
Dr. Erdal Ozkaya
Getting Started in Cybersecurity
Cybersecurity Incident Response Best Practices
Dr Erdal Ozkaya Dr. Orhan Sari
Bookauthority
BEST BOOKS OF ALL TIME
WINNER
SOSYAL MÜHENDISLIK
SIBER GÜVENLIK
Charles Sturt University
School of Computing and Mathematics
Book of Short Papers
2017
Higher Degree Research Symposium
Hands-On Cybersecurity for Finance
Packt
THE ART OF HUMAN HACKING
20411B
Administering Windows Server 2012
Microsoft Official Course
CYBERSECURITY CANON
Essential Reading for the Security Professional
HALL OF FAME
CDM
CYBER DEFENSE MAGAZINE
THE PREMIER SOURCE FOR IT SECURITY INFORMATION

Keep in Touch

@Erdal_Ozkaya

Dr Erdal Ozkaya

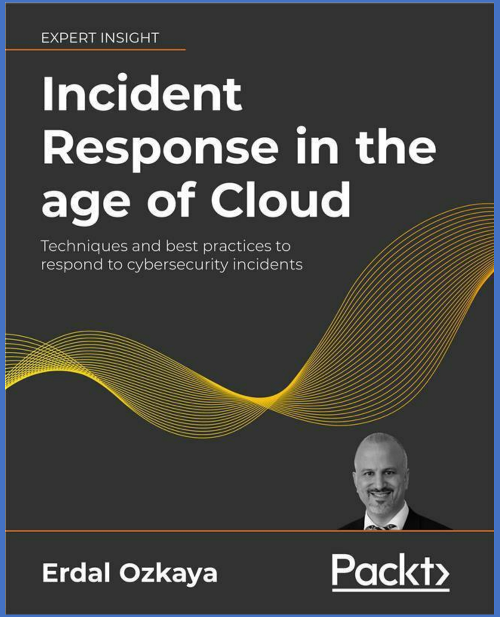
www.ErdalOzkaya.com

@drerdalozkaya

https://www.youtube.com/erdalozkaya

Tweet & Subscribe to win

@Erdal_Ozkaya

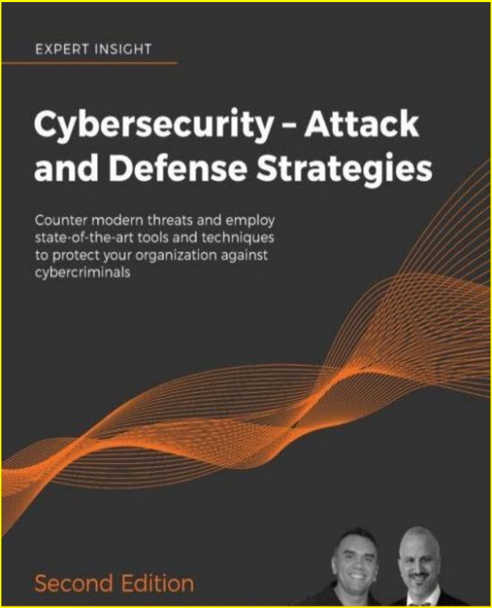

EXPERT INSIGHT

Incident Response in the age of Cloud

Techniques and best practices to respond to cybersecurity incidents

Erdal Ozkaya

Packt>


EXPERT INSIGHT

Cybersecurity – Attack and Defense Strategies

Counter modern threats and employ state-of-the-art tools and techniques to protect your organization against cybercriminals

Second Edition

Dr. Erdal Ozkaya

Foreword by: Troy Hunt
Founder, Have I Been Pwned

Learn Social Engineering

Learn the art of human hacking with an internationally renowned expert

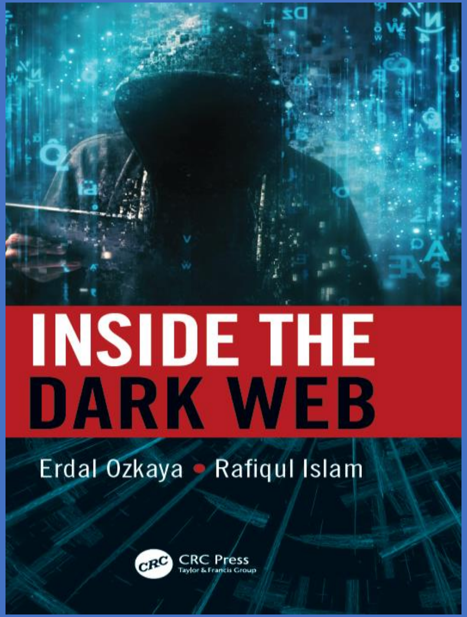
Packt>

Cybersecurity: The Beginner's Guide

The ultimate guide to getting started in cybersecurity

Dr. Erdal Ozkaya

Packt>
www.packt.com

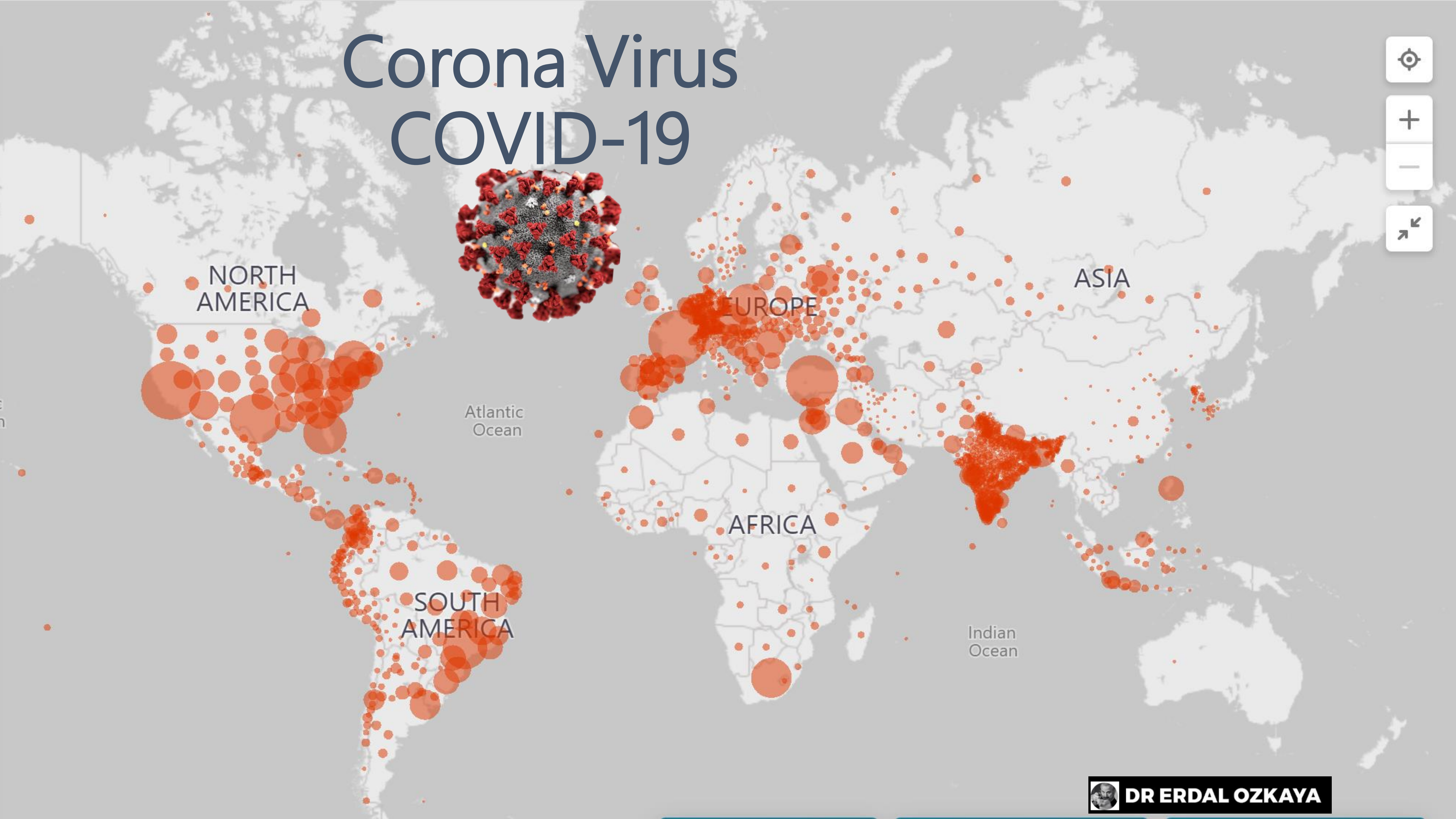

INSIDE THE DARK WEB

Erdal Ozkaya • Rafiqul Islam

CRC Press
Taylor & Francis Group

Our world has changed

Corona Virus COVID-19



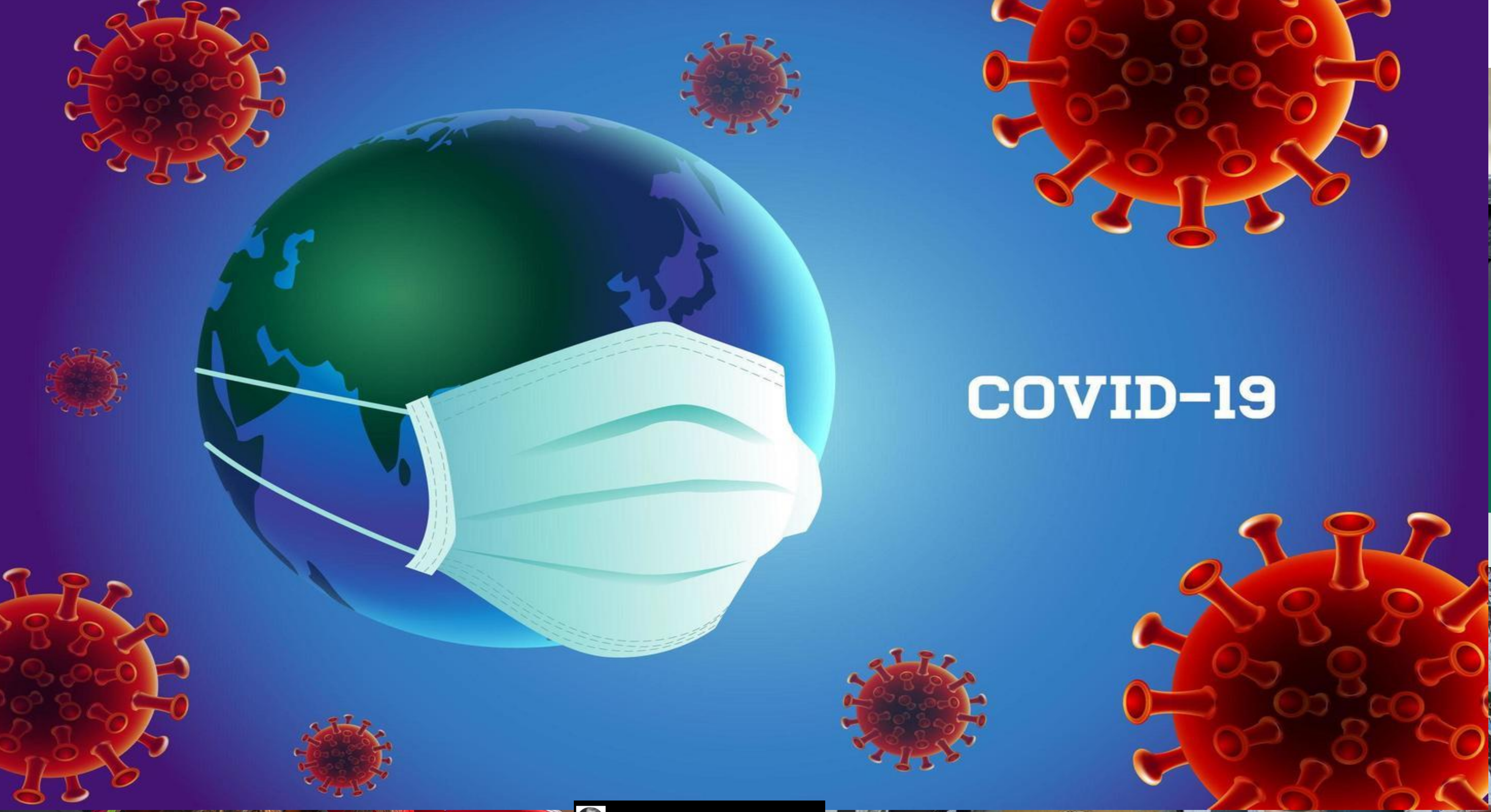
DR ERDAL OZKAYA

AFTER THE PANDEMIC

OUR NEW WORLD

DR ERDAL OZKAYA

The way we live


COVID-19

THEN

NOW

PREVENTION OF COVID-19 SPREAD:
SOCIAL DISTANCING

The way we work

Remote Work

DR ERDAL OZKAYA

The way we attend conferences

CYBER
SECURITY
HACKING
CRIME
INFORMATION
HACKER
confide
DATA
INFORM

You think you know what is running on your computer…?

Let’s be honest !

Who will win ☺

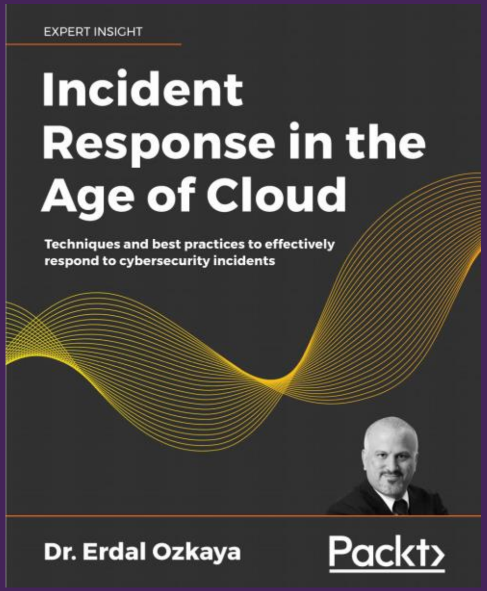
VS

Human
Error

Those who realize they've been hacked.

There are two types of organizations.

Those who haven't yet realized they've been hacked.



EXPERT INSIGHT

Incident Response in the Age of Cloud

Techniques and best practices to effectively respond to cybersecurity incidents

Dr. Erdal Ozkaya

Packt>

Will 2021 be Sunny in terms of Cybersecurity ?

THOSE WHO DO NOT REMEMBER THE PAST ARE CONDEMNED TO REPEAT IT.

Do you still remember !!!

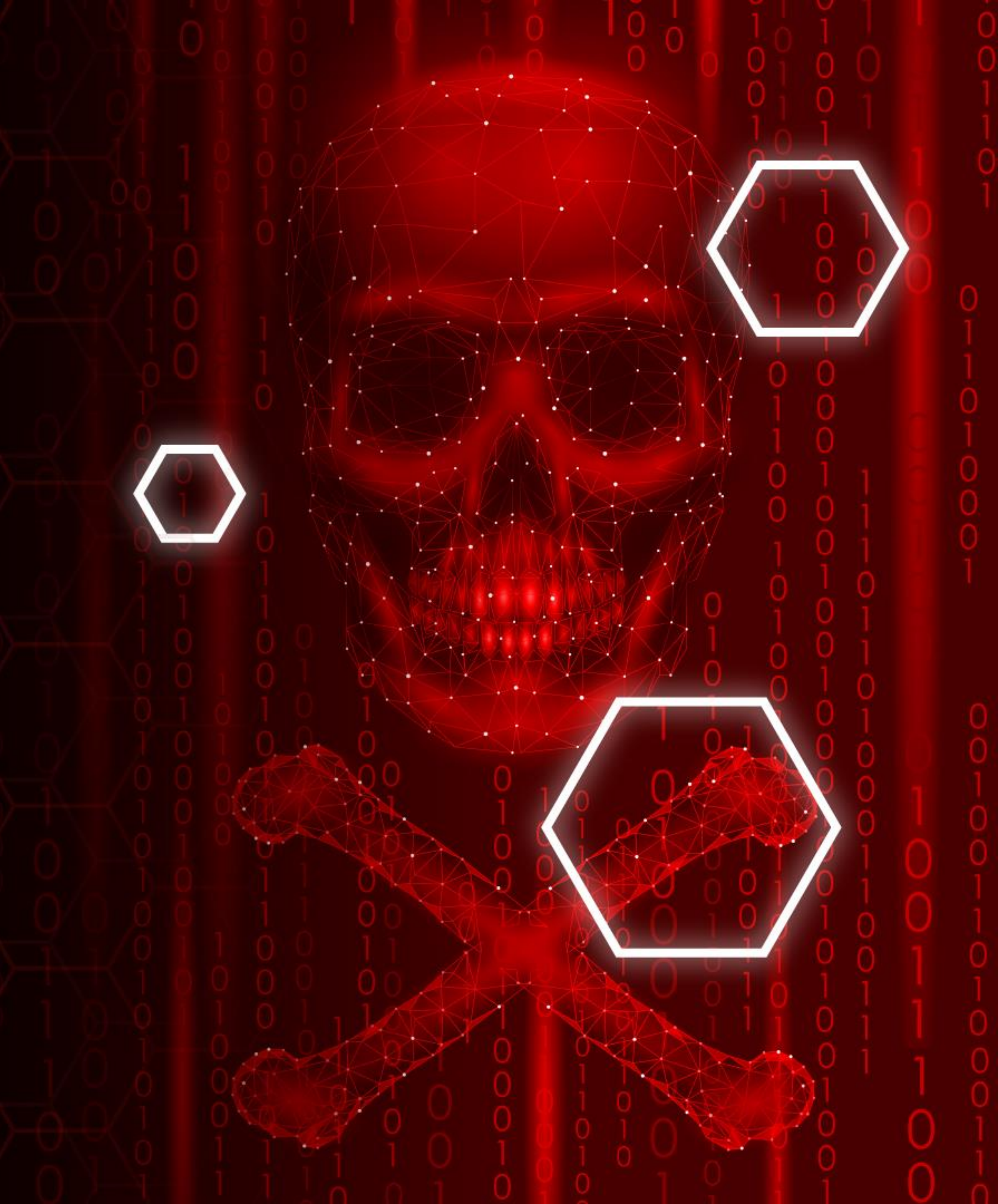
2020 Cybersecurity Rewind

Quick highlights on what happened ?

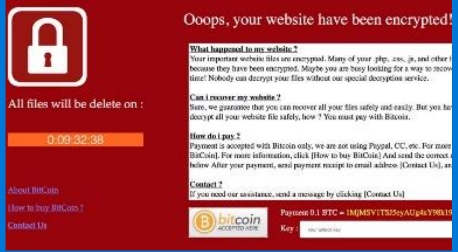
DR ERDAL OZKAYA

! CYBER ATTACK !
! CYBER ATTACK !
! WARNING !
! WARNING !

Ransomware



The Evolution of Ransomware



Ooops, your website have been encrypted!

All files will be delete on :

0:09:32:38

What happened to my website ?
Your important website files are encrypted. Many of your .php, .css, .js, and other f
because they have been encrypted. Maybe you are busy looking for a way to recov
time! Nobody can decrypt your files without our special decryption service.

Can i recover my website ?
Sure, we guarantee that you can recover all your files safely and easily. But you ha
decrypt all your website file safely, how ? You must pay with Bitcoin.

How do i pay ?
Payment is accepted with Bitcoin only, we are not using Paypal, CC, etc. For more
BitCoin]. For more information, click [How to buy BitCoin] And send the correct
below After your payment, send payment receipt to email address [Contact Us], an

Contact ?
If you need our assistance, send a message by clicking [Contact Us]

About BitCoin

How to buy BitCoin ?

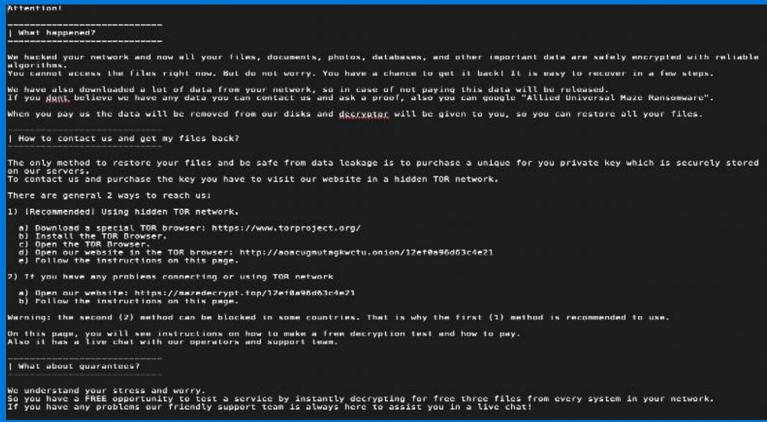
Contact Us

Payment 0.1 BTC = 1MJMSV1TSJ5eyAUg4zY98k19

Key :

- Ransomware is a growing problem for organizations of every size with the numbers of attacks and the money spent to clean up the damage on the rise.
- The origins of ransomware attacks trace back to the 1980s when malicious actors used floppy disks to install malware on unsuspecting victims at Healthcare industry
- In 2016 Wanna cry – Eternal Blue : Is known as “reborn of the Ransomware attacks” which was followed by NoPetya, BadRabbit, Robin Hood,
- Ransomware creators are getting more sophisticated in how they infect systems, avoid detection and foil decryption efforts :
- Sodin (okibi) ransomware as one example –, it can burrow deep into a system to elevate privileges by planting itself in CPU architecture. This makes it much harder to detect and, therefore, less likely to be removed.
- Recent big Ransoms payers :
- **Garmin , Carlson Wagonlit Travel (July 2020) Lion Breweries, Travelex …**
- Solution : **Tested Backups, Structured, Regular Updates,**

  Defense in Depth Strategy, Cyber Hygiene, Least Privilege ,

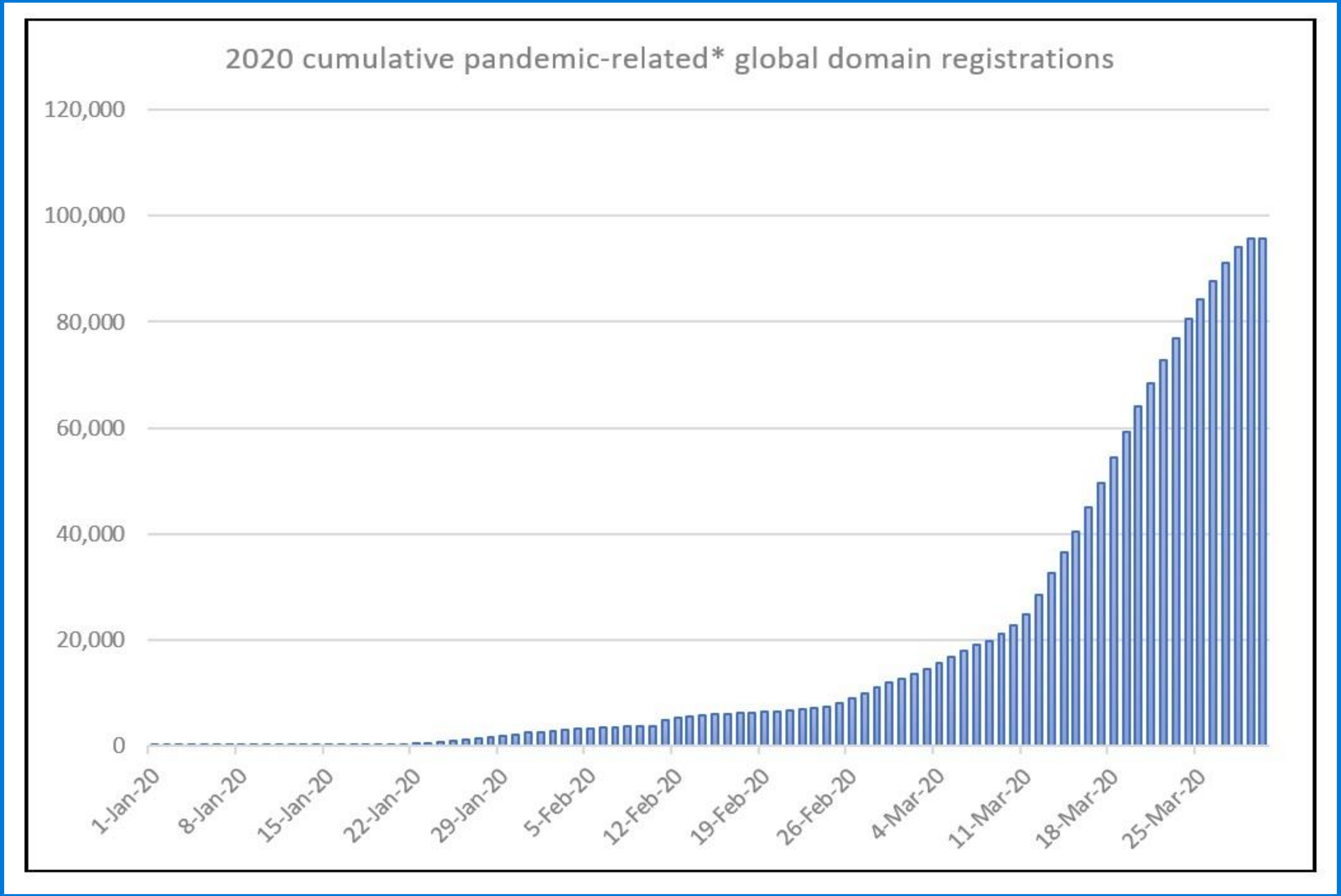


```
Attention!

----------------------------
| What happened?
----------------------------

We hacked your network and now all your files, documents, photos, databases, and other important data are safely encrypted with reliable
algorithms.
You cannot access the files right now. But do not worry. You have a chance to get it back! It is easy to recover in a few steps.

We have also downloaded a lot of data from your network, so in case of not paying this data will be released.
If you dont believe we have any data you can contact us and ask a proof, also you can google "Allied Universal Maze Ransomware".

When you pay us the data will be removed from our disks and decryptor will be given to you, so you can restore all your files.

----------------------------
| How to contact us and get my files back?
----------------------------

The only method to restore your files and be safe from data leakage is to purchase a unique for you private key which is securely stored
on our servers.
To contact us and purchase the key you have to visit our website in a hidden TOR network.

There are general 2 ways to reach us:

1) [Recommended] Using hidden TOR network.

  a) Download a special TOR browser: https://www.torproject.org/
  b) Install the TOR Browser.
  c) Open the TOR Browser.
  d) Open our website in the TOR browser: http://aoacugmutagkwctu.onion/12ef0a96d63c4e21
  e) Follow the instructions on this page.

2) If you have any problems connecting or using TOR network

  a) Open our website: https://mazedecrypt.top/12ef0a96d63c4e21
  b) Follow the instructions on this page.

Warning: the second (2) method can be blocked in some countries. That is why the first (1) method is recommended to use.

On this page, you will see instructions on how to make a free decryption test and how to pay.
Also it has a live chat with our operators and support team.

----------------------------
| What about guarantees?
----------------------------

We understand your stress and worry.
So you have a FREE opportunity to test a service by instantly decrypting for free three files from every system in your network.
If you have any problems our friendly support team is always here to assist you in a live chat!
```

Corona Based “Attacks”

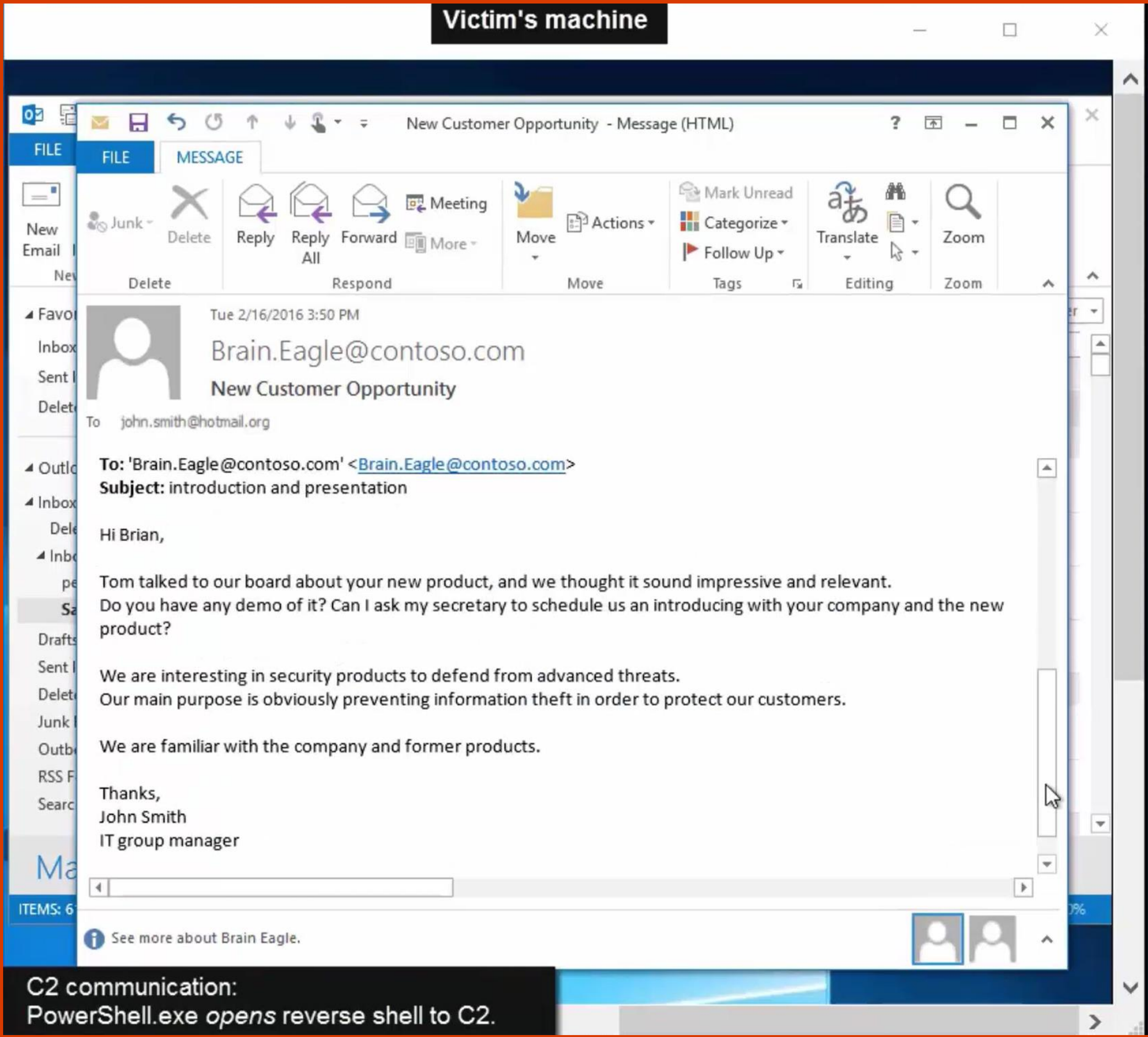
- 33,000 unemployment applicants were exposed to a data security breach from the Pandemic Unemployment Assistance program in May 2020. (NBC)
- Scams increased by 400% over the month of March, making COVID-19 the largest-ever security threat. (ReedSmith)
- In April, Google blocked 18 million daily malware and phishing emails related to Coronavirus. (Google)
- Half a million Zoom user accounts were compromised and sold on a dark web forum. (CPO Magazine)
- There are 1,767 high-risk Coronavirus themed domain names created each day. (Palo Alto Networks)
- 471 fake online shops selling fraudulent COVID-19 items were taken down in the UK. (ZDNet)
- 450 active WHO email addresses and thousands of COVID-19 response team’s email addresses were leaked in April. (WHO)
- Visits to popular hacker websites and forums increased by 66% between March and May. (cybernews)

COVID related Domains



DR ERDAL OZKAYA

Victim's machine



Tue 2/16/2016 3:50 PM

Brain.Eagle@contoso.com

New Customer Opportunity

To john.smith@hotmail.org

To: 'Brain.Eagle@contoso.com' <Brain.Eagle@contoso.com>
Subject: introduction and presentation

Hi Brian,

Tom talked to our board about your new product, and we thought it sound impressive and relevant.
Do you have any demo of it? Can I ask my secretary to schedule us an introducing with your company and the new product?

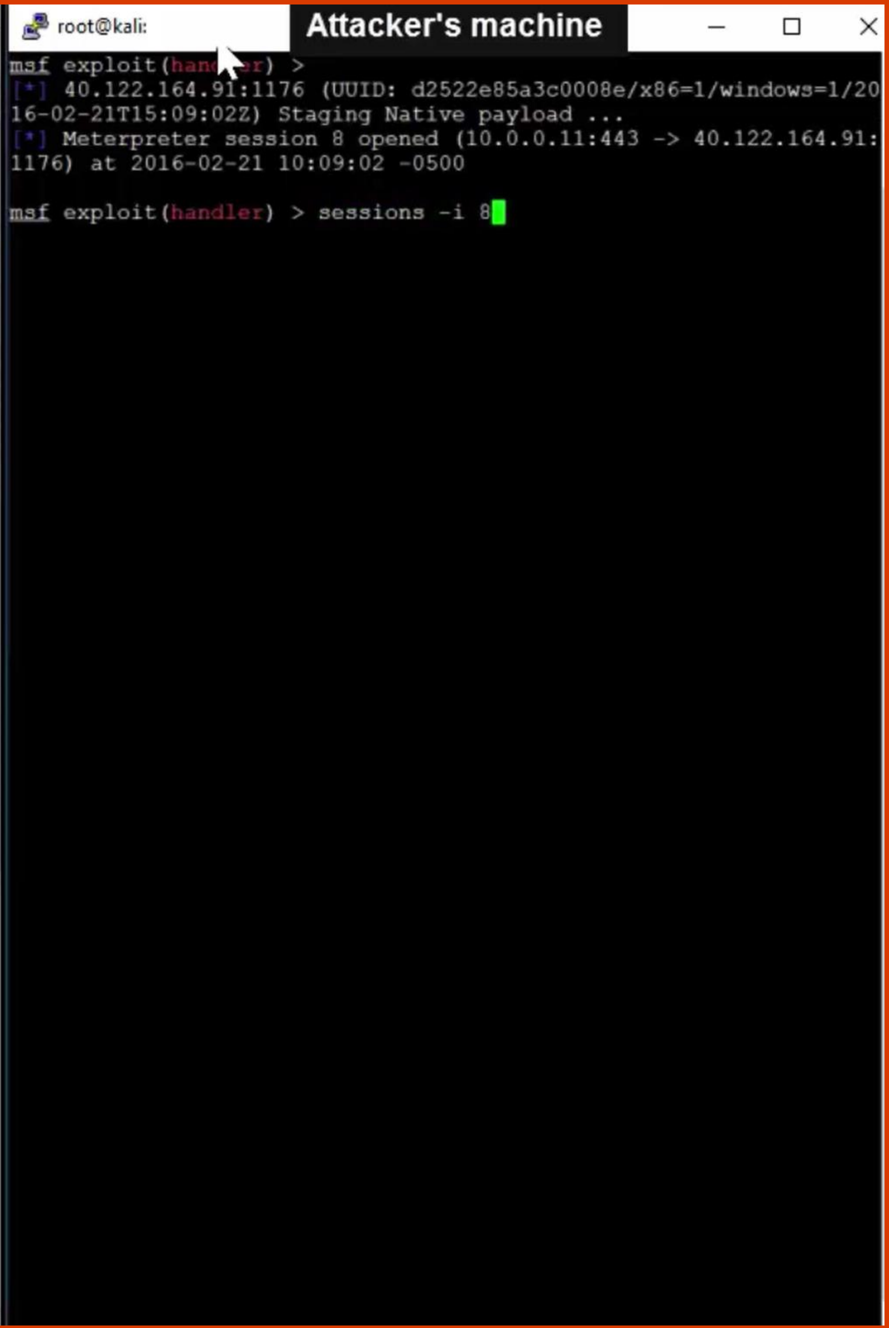
We are interesting in security products to defend from advanced threats.
Our main purpose is obviously preventing information theft in order to protect our customers.

We are familiar with the company and former products.

Thanks,
John Smith
IT group manager

See more about Brain Eagle.

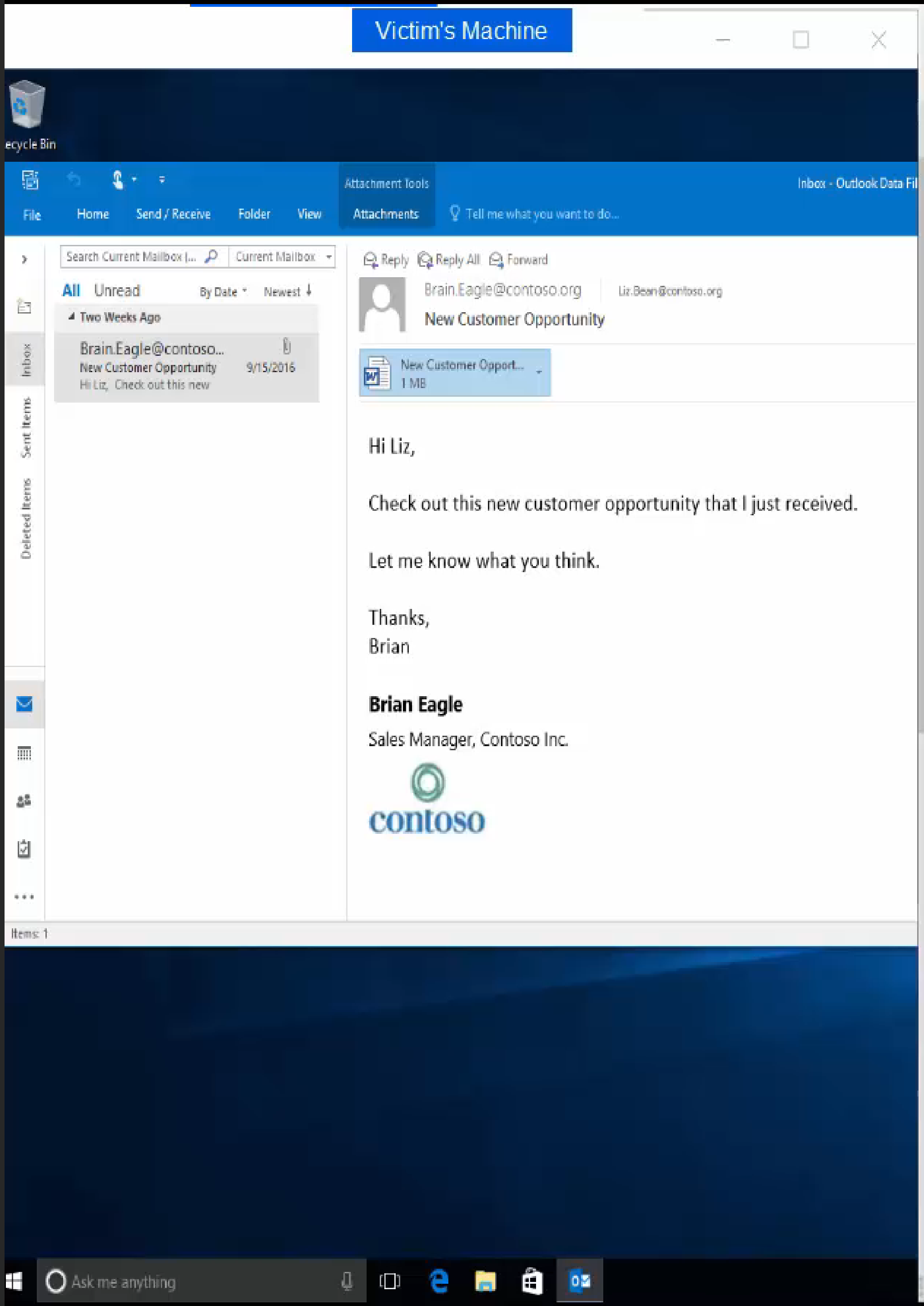
Attacker's machine



```
msf exploit(handler) >
[*] 40.122.164.91:1176 (UUID: d2522e85a3c0008e/x86=1/windows=1/20
16-02-21T15:09:02Z) Staging Native payload ...
[*] Meterpreter session 8 opened (10.0.0.11:443 -> 40.122.164.91:
1176) at 2016-02-21 10:09:02 -0500

msf exploit(handler) > sessions -i 8
```

C2 communication:
PowerShell.exe *opens* reverse shell to C2.

Victim's Machine



Brain.Eagle@contoso... New Customer Opportunity 9/15/2016 Hi Liz, Check out this new

Brain.Eagle@contoso.org Liz.Bean@contoso.org

New Customer Opportunity

New Customer Opport... 1 MB

Hi Liz,

Check out this new customer opportunity that I just received.

Let me know what you think.

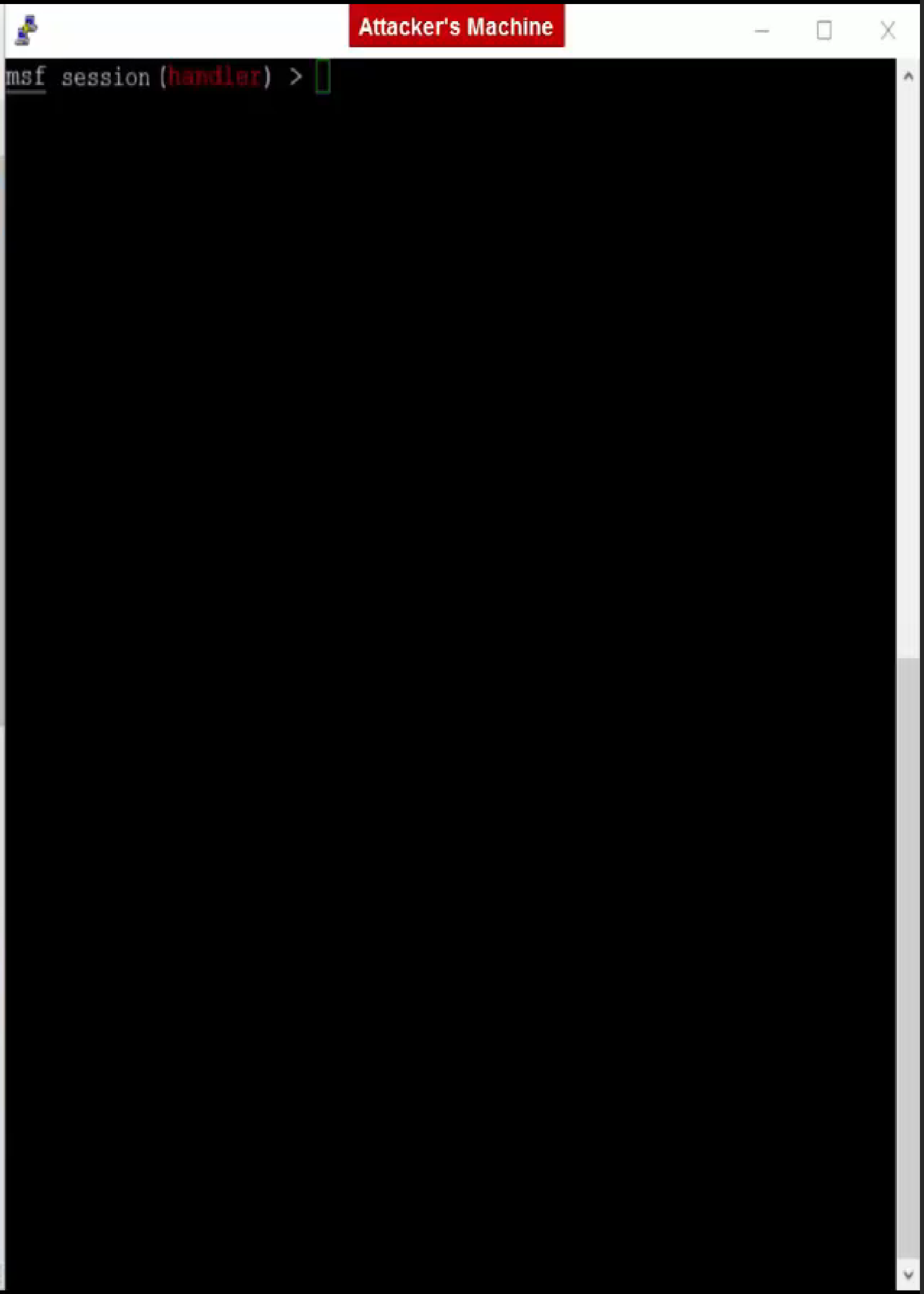
Thanks,
Brian

Brian Eagle

Sales Manager, Contoso Inc.

contoso

Attacker's Machine

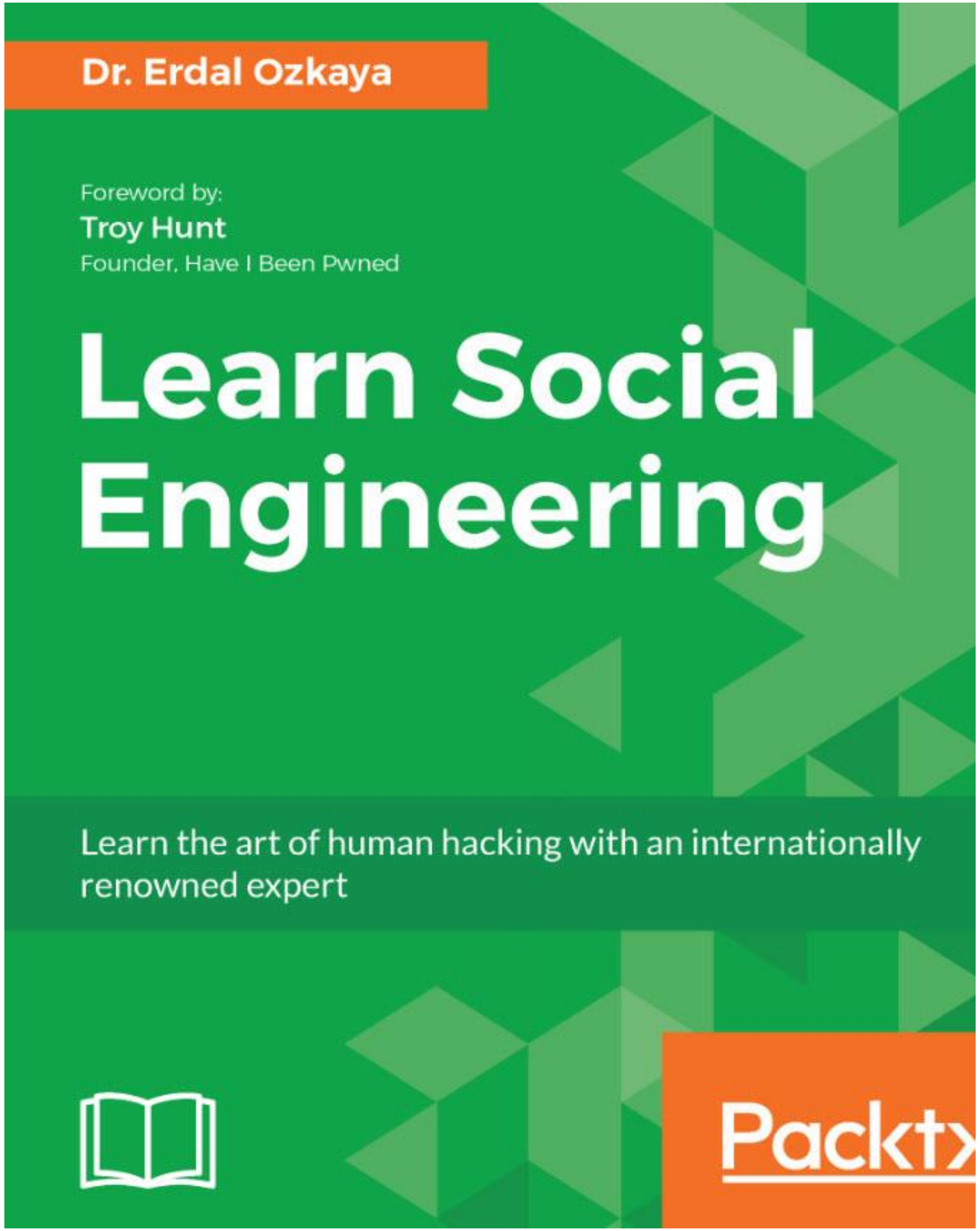


```
msf session (handler) > 
```

The rise of Social Engineering

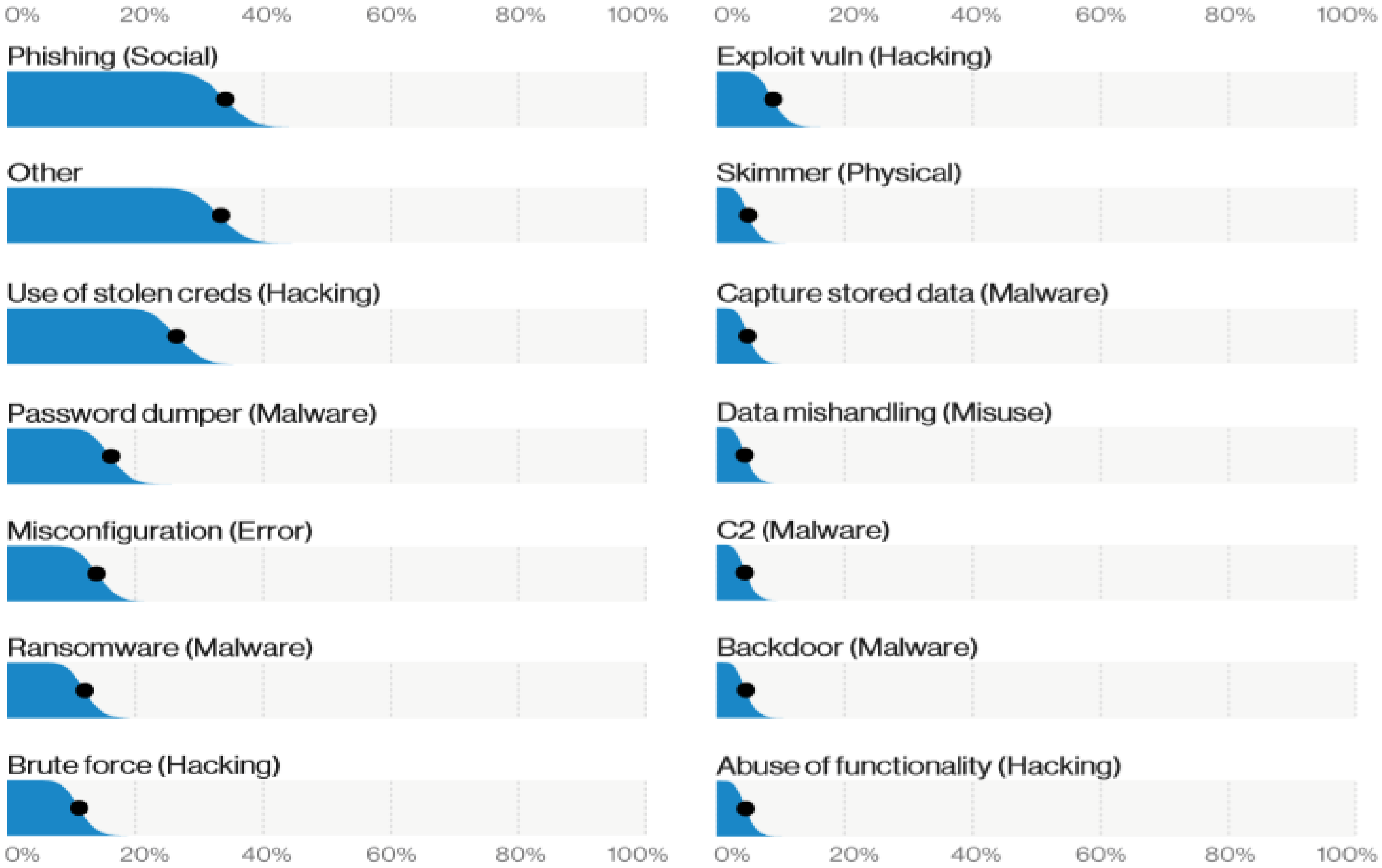
This is social engineering-based attacks are increasing — not because People are becoming more gullible during COVID; but they’ve become used to big changes in small messages and when news headlines is all about safety or sickness, it’s much easier to them to believe to the information given .”

Dr Erdal Ozkaya


Dr. Erdal Ozkaya
Foreword by:
Troy Hunt
Founder, Have I Been Pwned
Learn Social Engineering
Learn the art of human hacking with an internationally renowned expert
Packt

Never ending attacks

Attack Vectors Globally



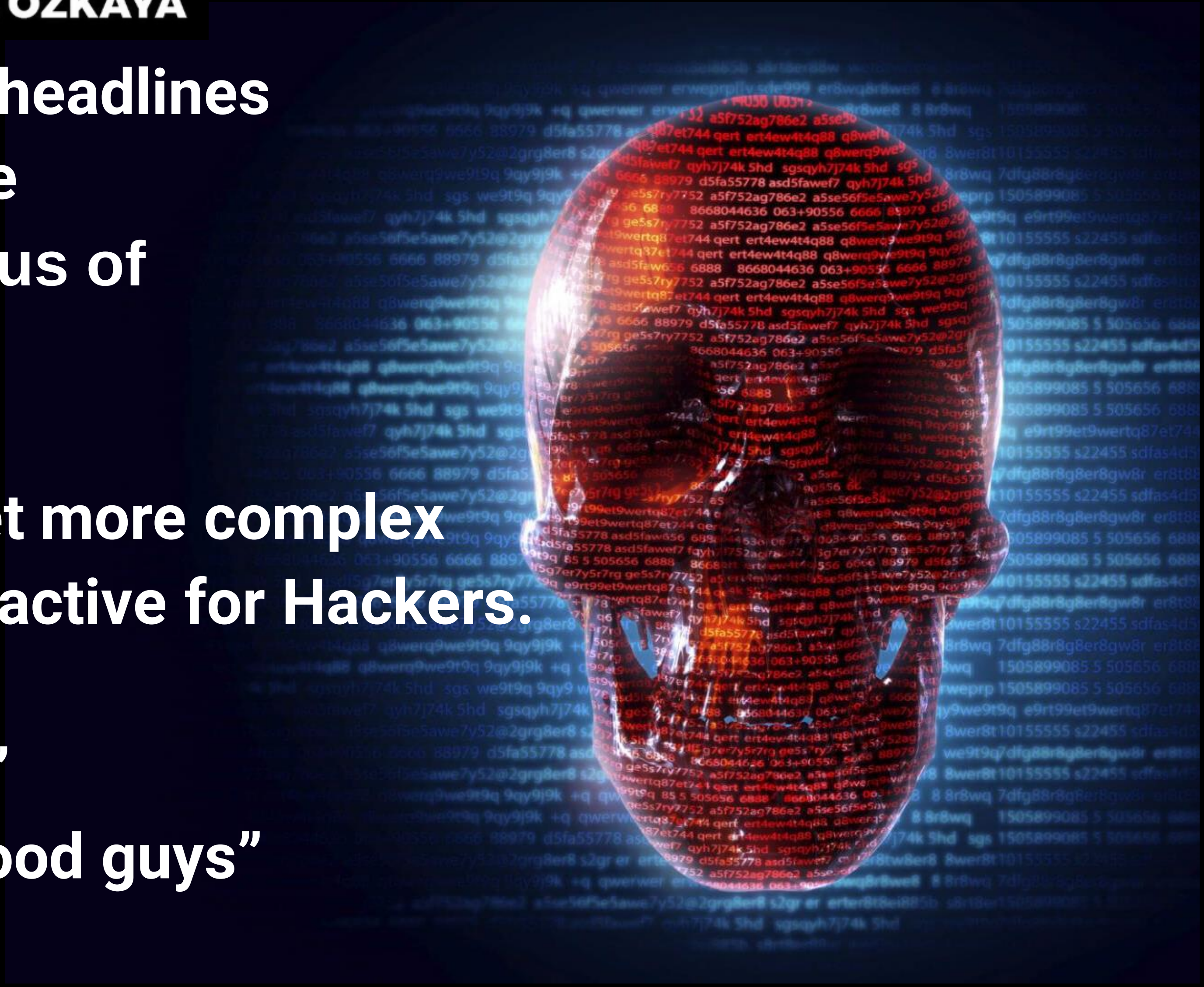
Cybersecurity Facts and Figures in 2020

- A cyberattack occurs every 39 seconds
- Cybercrime costs the global economy around $445 billion per year
- Globally, 30,000 websites are hacked daily
- Over 4,000 ransomware attacks take place around the world daily.(%363)
- 23,000 DDoS attacks are happening somewhere on the internet every 24 hours.
- The average life cycle of a data breach is about 11 months.
- $64.2 billion was spent in 2019 on managed security services
- Mobile malware variation has increased by 54 percent
- 94 Percent of malware arrives via email
- Nearly $1.5 billion is lost to phishing each year
- Social Engineering is still TOP trending
- 99.9 percent of all mobile malware comes from third-party app stores

Hacks of 2021 ?

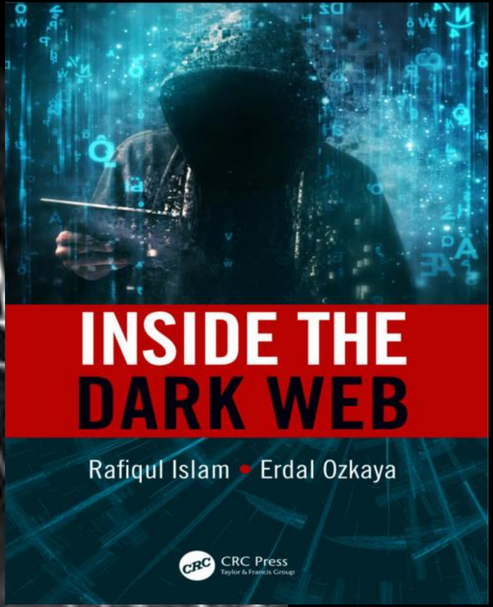
Cybersecurity predictions for 2021

DR ERDAL OZKAYA



- Ransomware attacks will stay in headlines
- State-sponsored hacking will rise
- Remote workers will be the focus of cybercriminals through 2021.
- Don’t ignore your IoT devices…
- Social engineered attacks will get more complex
- 5G , its new its complex = Its attractive for Hackers.
- Expect “cloud related attacks”
- Expect “financial sector attacks ”
- AI will be used not just by the “good guys”

DR ERDAL OZKAYA

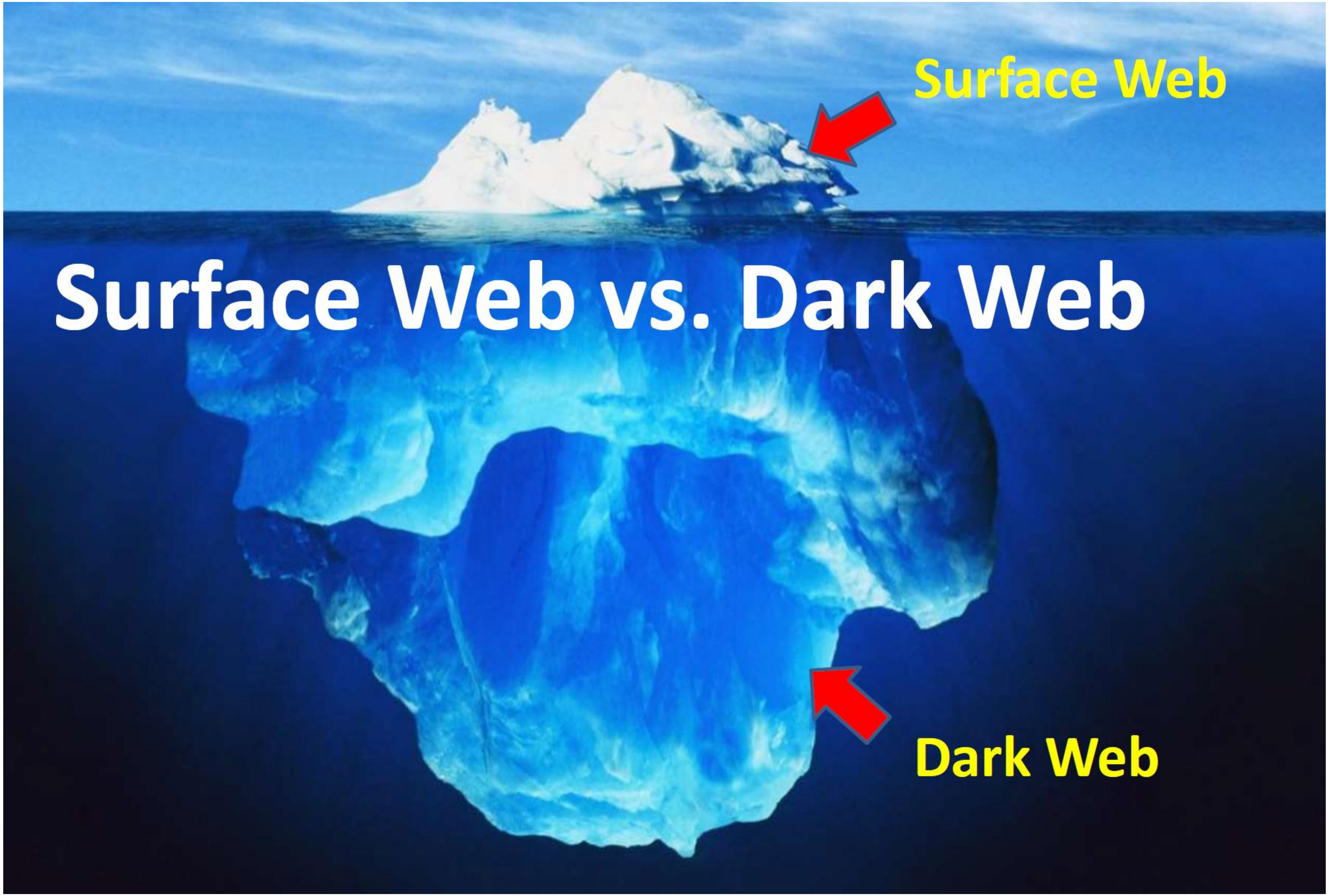


INSIDE THE DARK WEB

Rafiqul Islam • Erdal Ozkaya

CRC Press
Taylor & Francis Group

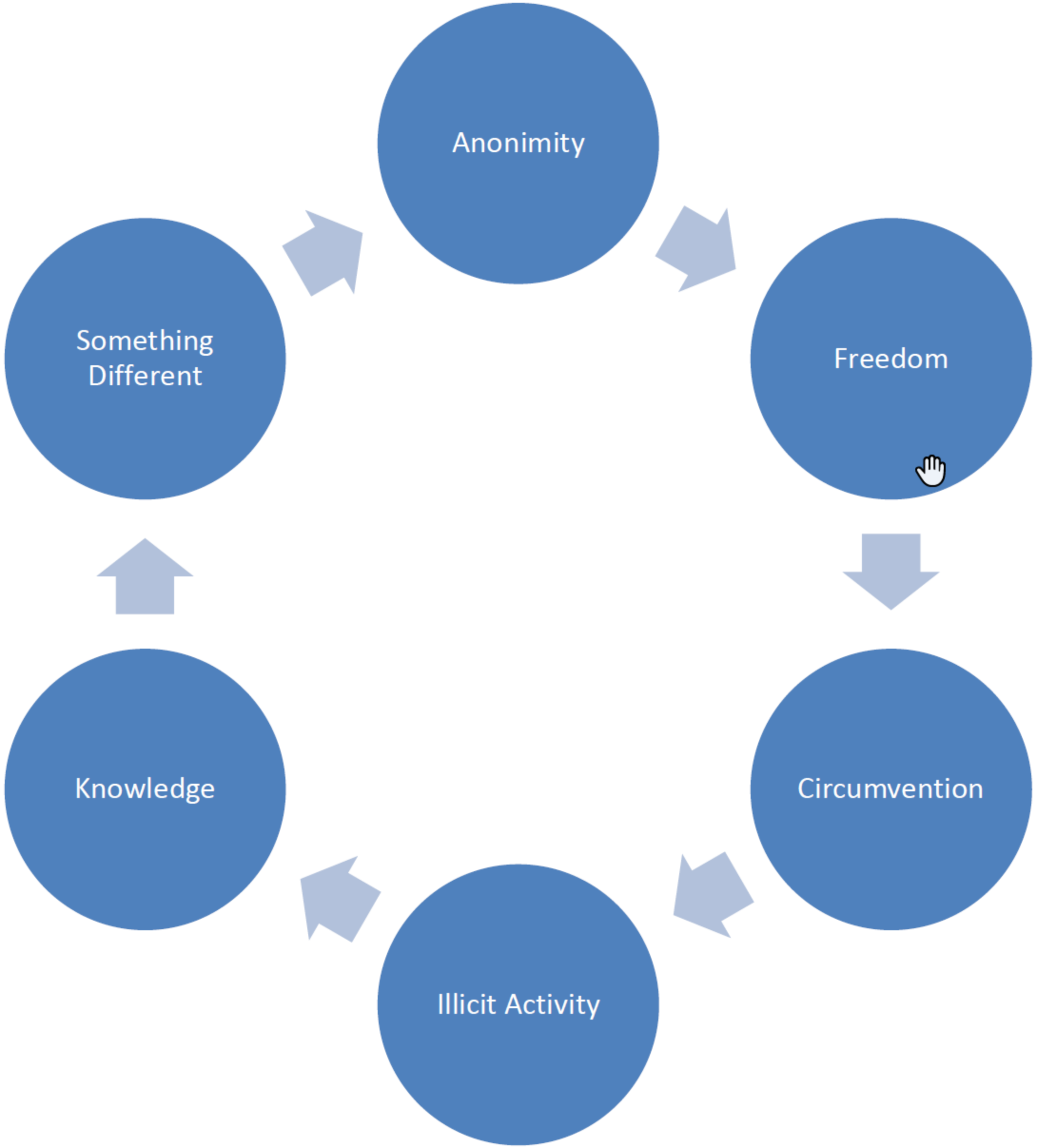
Surface Web vs. Dark Web

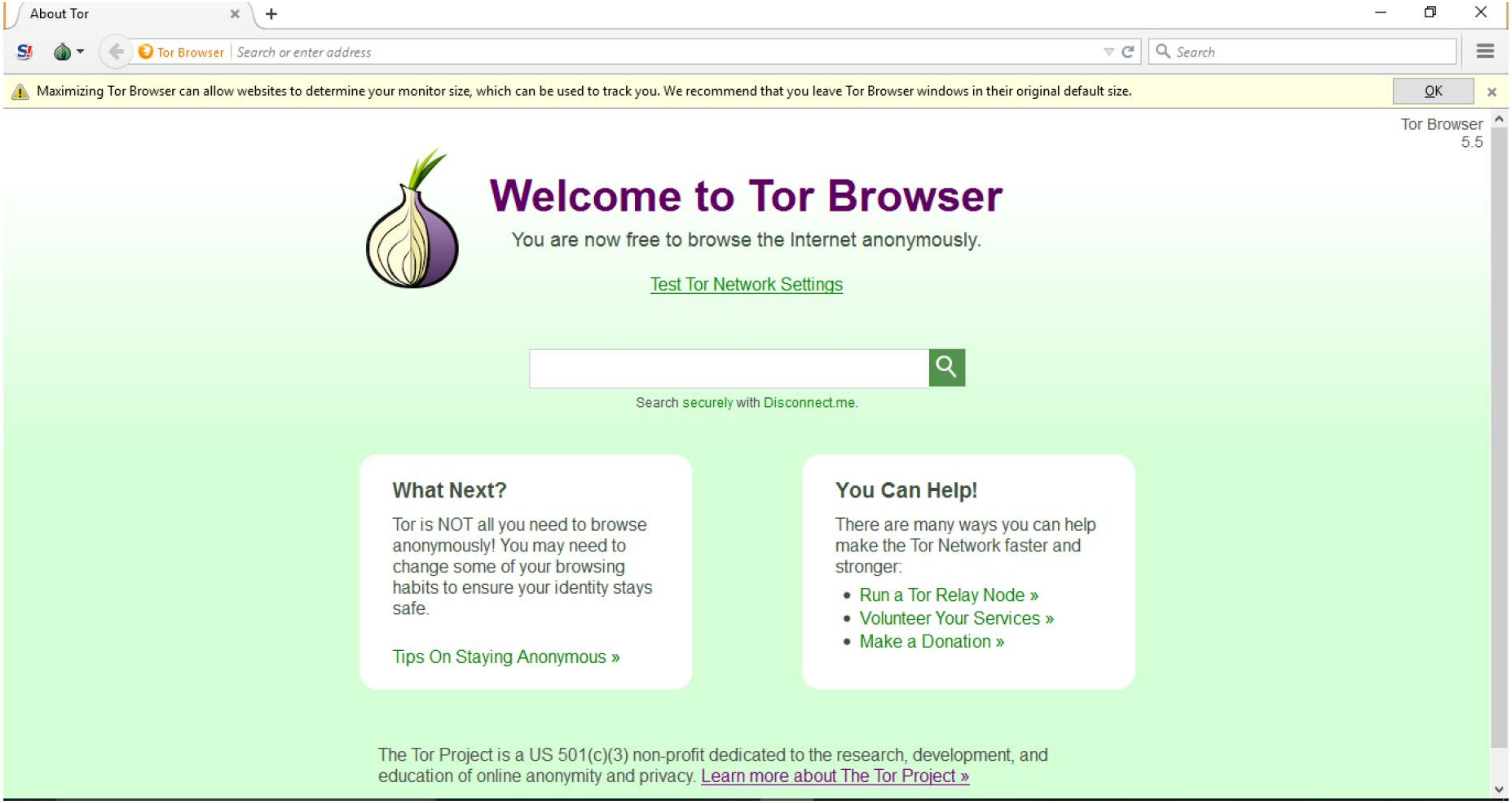


Surface Web

Dark Web

Why The Dark Web ?





⚠ Maximizing Tor Browser can allow websites to determine your monitor size, which can be used to track you. We recommend that you leave Tor Browser windows in their original default size.

Tor Browser
5.5

Welcome to Tor Browser

You are now free to browse the Internet anonymously.

Test Tor Network Settings

Search securely with Disconnect.me.

What Next?

Tor is NOT all you need to browse anonymously! You may need to change some of your browsing habits to ensure your identity stays safe.

Tips On Staying Anonymous »

You Can Help!

There are many ways you can help make the Tor Network faster and stronger:

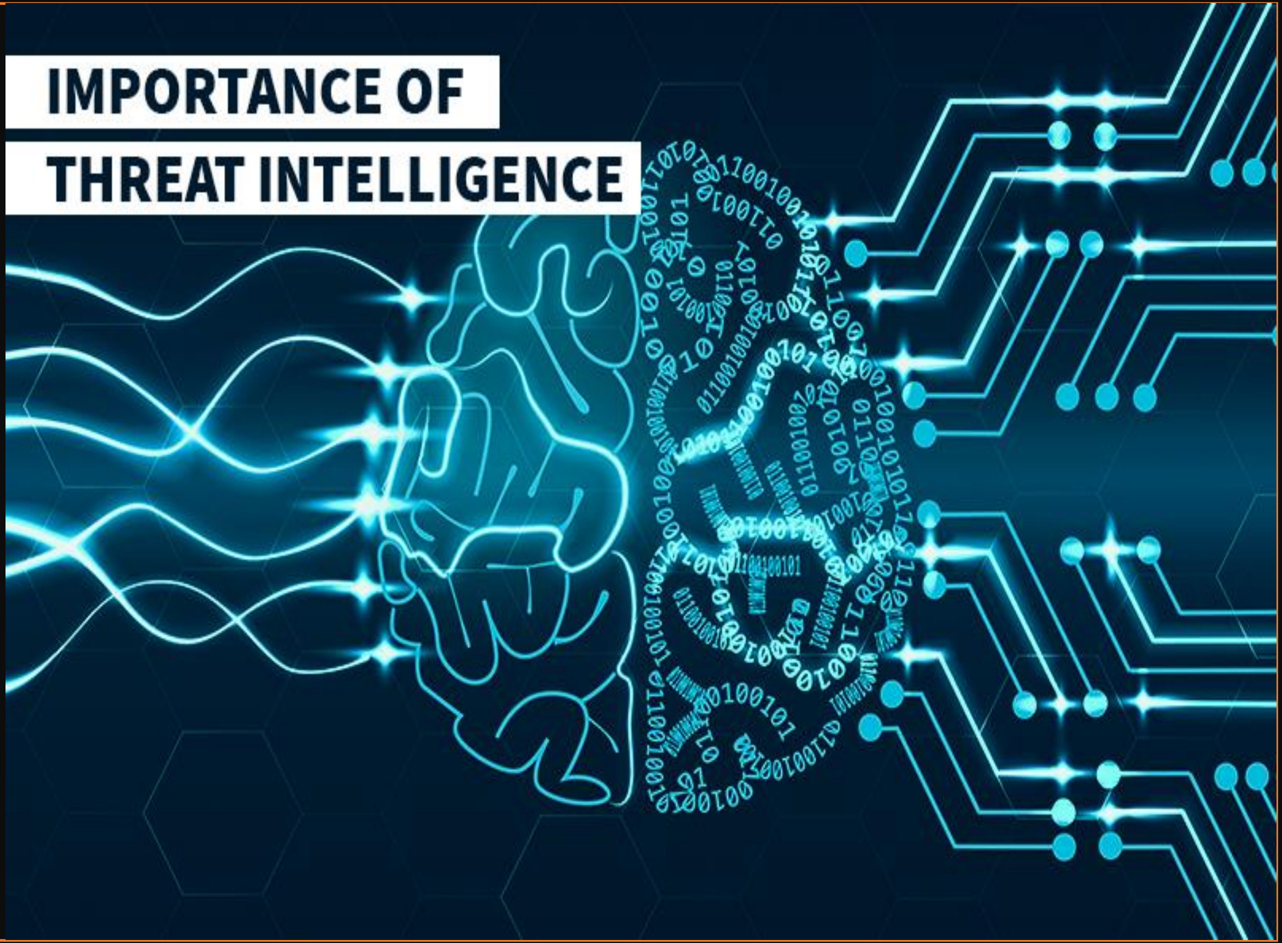
- Run a Tor Relay Node »
- Volunteer Your Services »
- Make a Donation »

The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. Learn more about The Tor Project »

The Importance of

Threat intelligence is **data that is collected, processed, and analyzed to understand a threat actor's motives, targets, and attack behaviors**. Threat intelligence enables us to make faster, more informed, data-backed security decisions and change their behavior from reactive to proactive in the fight against threat actors.

Advanced persistent threats (APTs) and defenders are constantly trying to outsmart each other. Organizations want to know the adversary’s next moves so they can proactively adapt their defenses and anticipate future attacks.



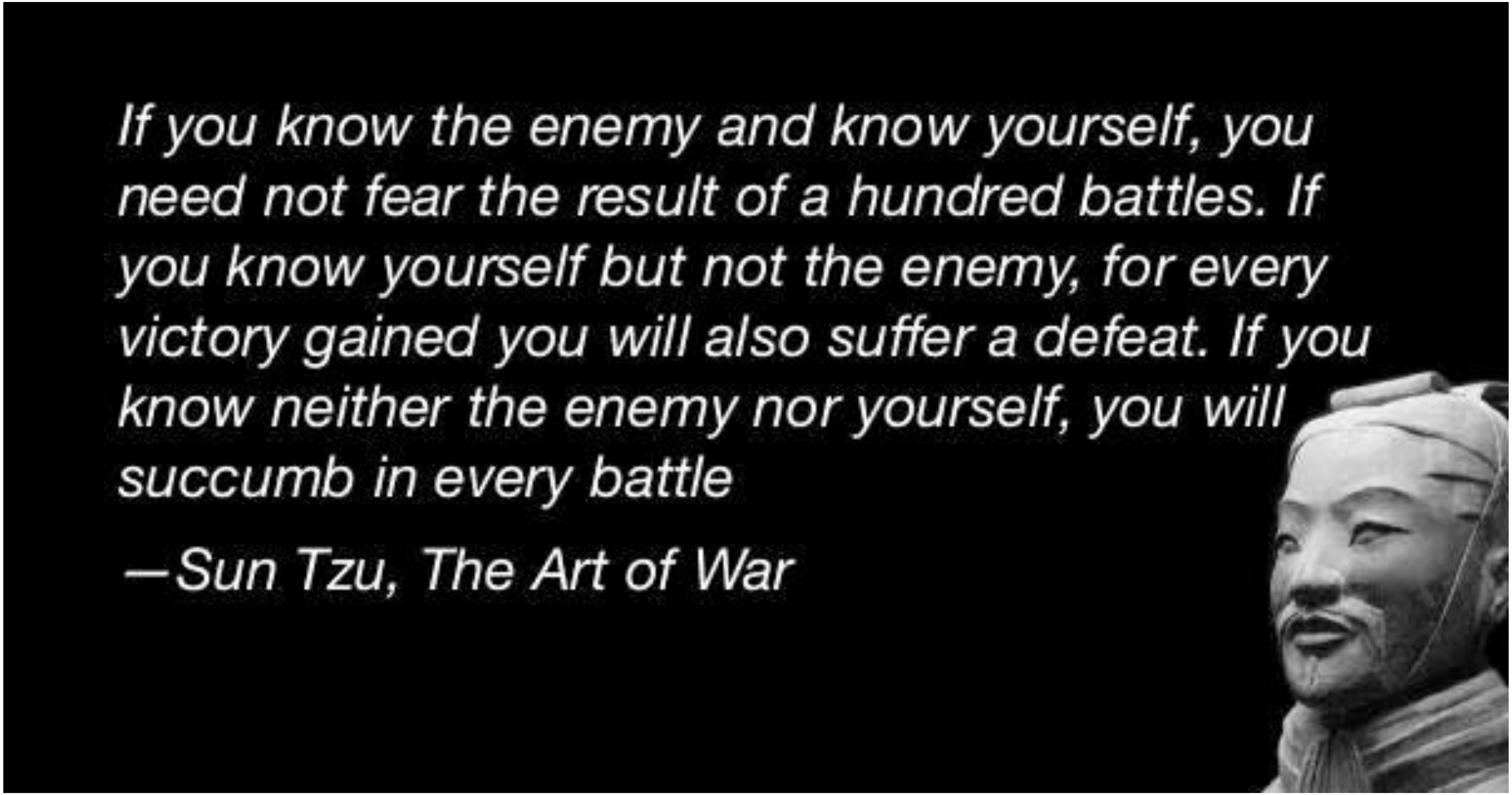
Internal threat intelligence

The information that an organization’s security and operations teams have from previous experiences with vulnerabilities, malware incidents and data breaches. This information, if properly documented, can provide the business with some meaningful content on how their enterprise networks were compromised and if there were any recurring methodologies that worked against the

Can be collected in some type of log management System or SIEM. It can provide invaluable insight into security gaps that can be remediated.

External threat intelligence

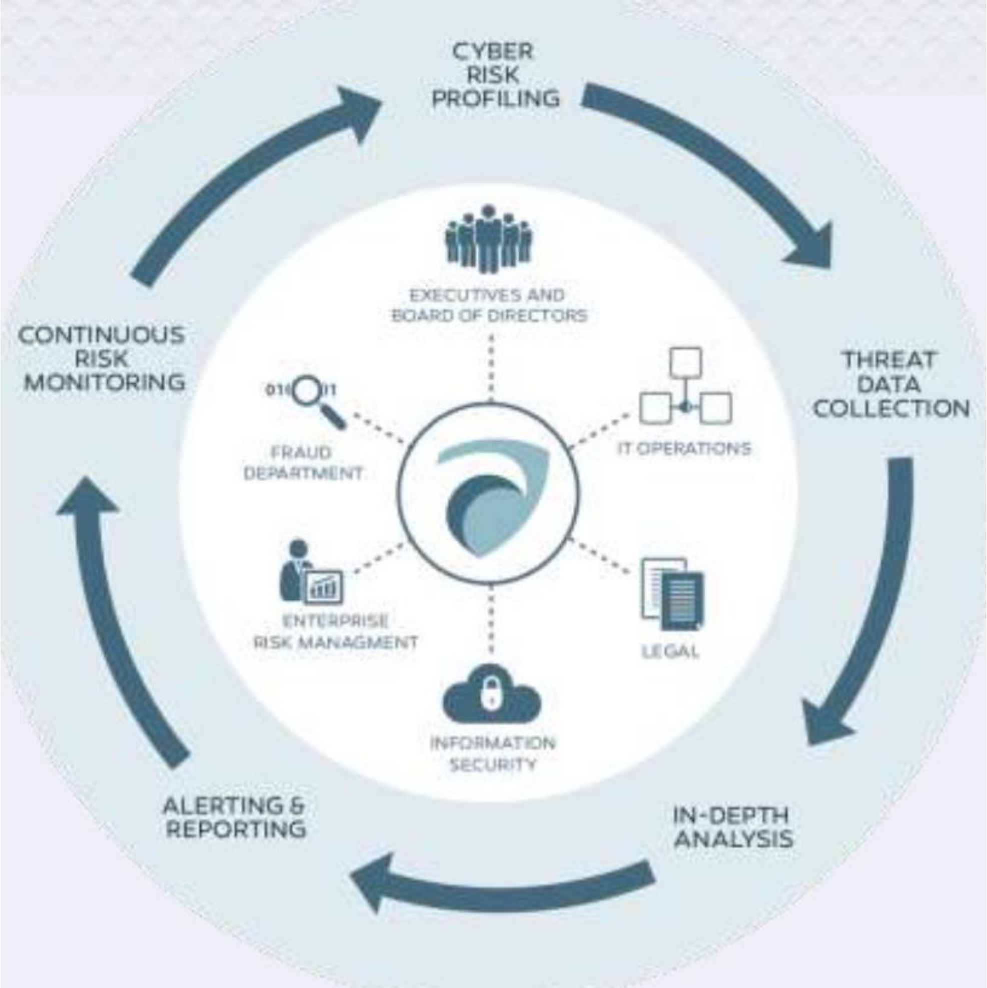
- Besides internal sources, organizations will typically subscribe to multiple external CTI data sources.
- Some of these sources are digital data feeds incorporated as a module, or service directly into security endpoint solutions or deployed assets like firewalls and security gateways.
- Other sources will be in a report format, available through email or a CTI portal



If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle

—Sun Tzu, The Art of War

Mitigating Risk with a Practical Intelligence Operation



- Outsource Your Dark Web Intel –

Complement your intel and facilitate faster, more effective risk management decisions

- Focus on Analysis –

It's less about getting more data and more about enabling sound analysis

- Link Intel to Business Impact –

Avoid alert fatigue by worrying about threats specific to your business

- People, Process, Technology –

Good intelligence leverages automation, expert human analysis and a process for using the intel

“Knowing the Threat Actors will help you build a better cyber strategy. Knowing your weakness will strengthen your defense. Knowing your Technology will empower you. Knowing your threat actors together with your weaknesses and the technology will master your defense “

Dr Erdal Ozkaya

You can't defeat the threats of the present with tools from past

Photo credit: Wikimedia Cannon from Galera Forte

ASSUME

BREACH

- Dankie
- Faleminderit
- Shukran
- Chnorakaloutioun
- Hvala
- Blagodaria

- Děkuji
- Tak
- Bedankt
- Tänan
- Kiitos
- Merci
- Danke
- Ευχαριστώ
- A dank

- Mahalo
- תודה.
- Dhanyavād
- Köszönöm
- Takk
- Terima kasih
- Grazie
- Grazzi

Thank you!

- 감사합니다
- Paldies
- Choukrane
- Ačiū
- Благодарам
- ありがとうございました

- 谢谢
- Баярлалаа
- Dziękuję
- Obrigado
- Mulţumesc
- Спасибо
- Ngiyabonga

- Ďakujem
- Tack
- Nandri
- Kop khun
- Teşekkür ederim
- Дякую
- Хвала
- Diolch

Keep in Touch

@Erdal_Ozkaya

Dr Erdal Ozkaya

www.ErdalOzkaya.com

@drerdalozkaya

https://www.youtube.com/erdalozkaya