Baker McKenzie.

Cybersecurity – current trends and what's next

Paul Glass, Stephen Reynolds | Tuesday 9 November 2021

Speakers

Paul Glass
Partner

Stephen Reynolds
Partner

Agenda

1. INTRO TO CYBERSERCURITY
2. TRENDING CYBER ATTACKS
3. HOW TO PREVENT
4. COMPLIANCE
5. QUESTIONS

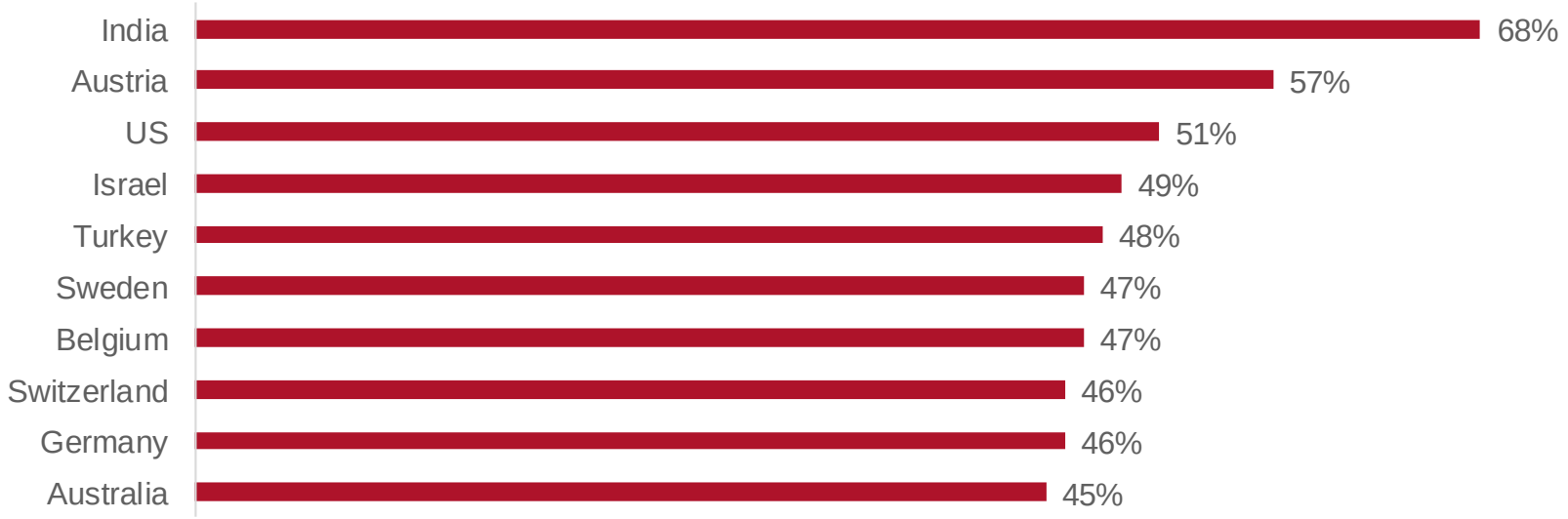
1

Intro to Cybersecurity

Why Should You Care?

Ransomware is a Global Issue

Share of Organizations, by Country, That Were Affected by Ransomware



Source: Statistica, https://www.statista.com/statistics/1246438/ransomware-attacks-by-country/

Why Should You Care?

THE WHITE HOUSE
WASHINGTON

TO: Corporate Executives and Business Leaders

FROM: Anne Neuberger, Deputy Assistant to the President and Deputy National Security Advisor for Cyber and Emerging Technology

SUBJECT: What We Urge You To Do To Protect Against The Threat of Ransomware

DATE: June 2, 2021

The number and size of ransomware incidents have increased significantly, and strengthening our nation's resilience from cyberattacks – both private and public sector – is a top priority of the President's.

Joint Statement of the Ministers and Representatives from the Counter Ransomware Initiative meeting October 2021

"Having gathered virtually on October 13 and 14 to discuss the escalating global security threat from ransomware, we the Ministers and Representatives of Australia, Brazil, Bulgaria, Canada, Czech Republic, the Dominican Republic, Estonia, European Union, France, Germany, India, Ireland, Israel, Italy, Japan, Kenya, Lithuania, Mexico, the Netherlands, New Zealand, Nigeria, Poland, Republic of Korea, Romania, Singapore, Saudi Arabia, South Africa, Sweden, Switzerland, Ukraine, United Arab Emirates, the United Kingdom, and the United States, recognize that ransomware is an escalating global security threat with serious economic and security consequences."

2

Trending Cyber Attacks

Trending Cyber Attacks

"Amateurs hack computers, professionals hack people."

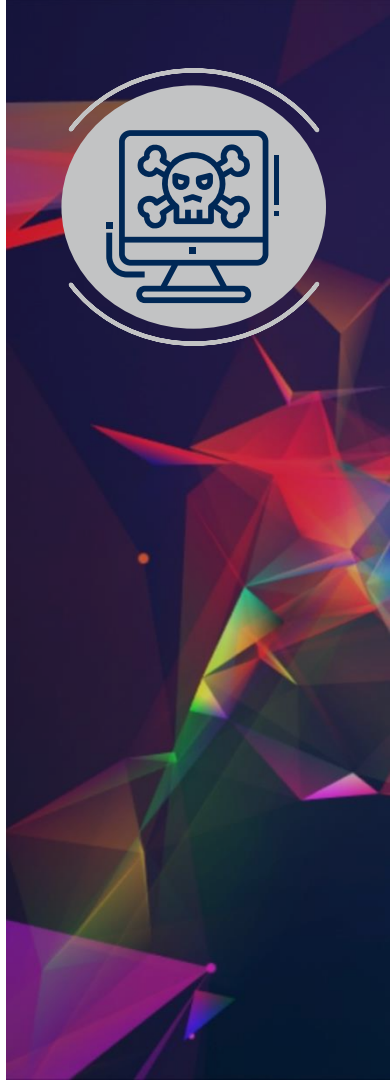
- Some Hacker

Trending Cyber Attacks

How are People Hacked?

Hackers try to trick people into…

- Running the hacker's malware
- Handing over credentials to the hacker
- Directly working for the hacker



Trending Cyber Attacks

Ransomware Example

From: Candidate, Joe <joe.candidate@gmail.com>
Sent: Monday, September 15, 2015 10:58 AM
To: <hrdirector@yourcompany.com>
Subject: Open Position
Attachments: Resume.pdf

Dear HR Director,

Please see my resume attached.

Thanks,

Joe

Trending Cyber Attacks

Ransomware Example

From:
Sent:
To:
Subject:
Attachments:

Dear HR Direct

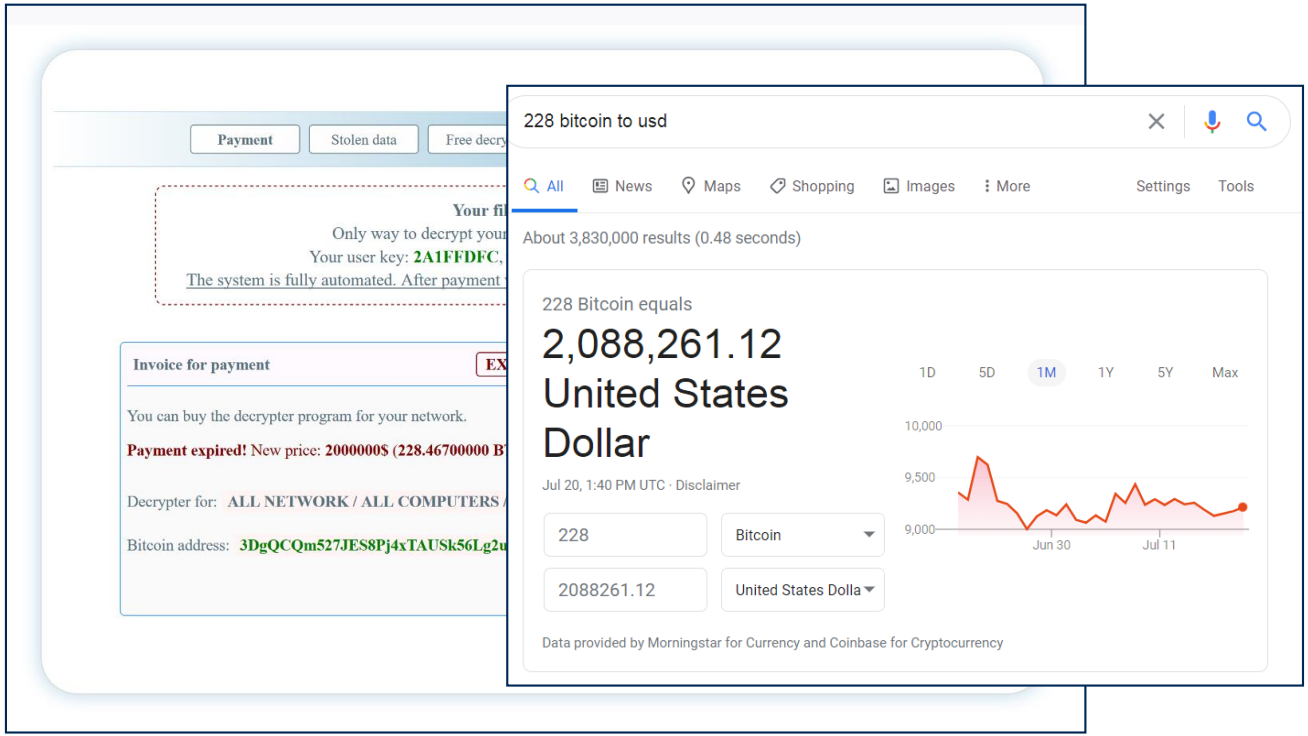
Please see my re

Thanks,

Joe

Trending Cyber Attacks

Another Ransomware Example



Your files are encrypted.
--
Rebooting, shutting down will cause you to lose files without the possibility of recovery.
--
Our encryption algorithms are very strong and your files are very well protected, you can't hope to recover them without our help. The only way to get your files back is to cooperate with us and get the decrypter program. Do not try to recover your files without a decrypt program, you may damage them and then they will be impossible to recover.

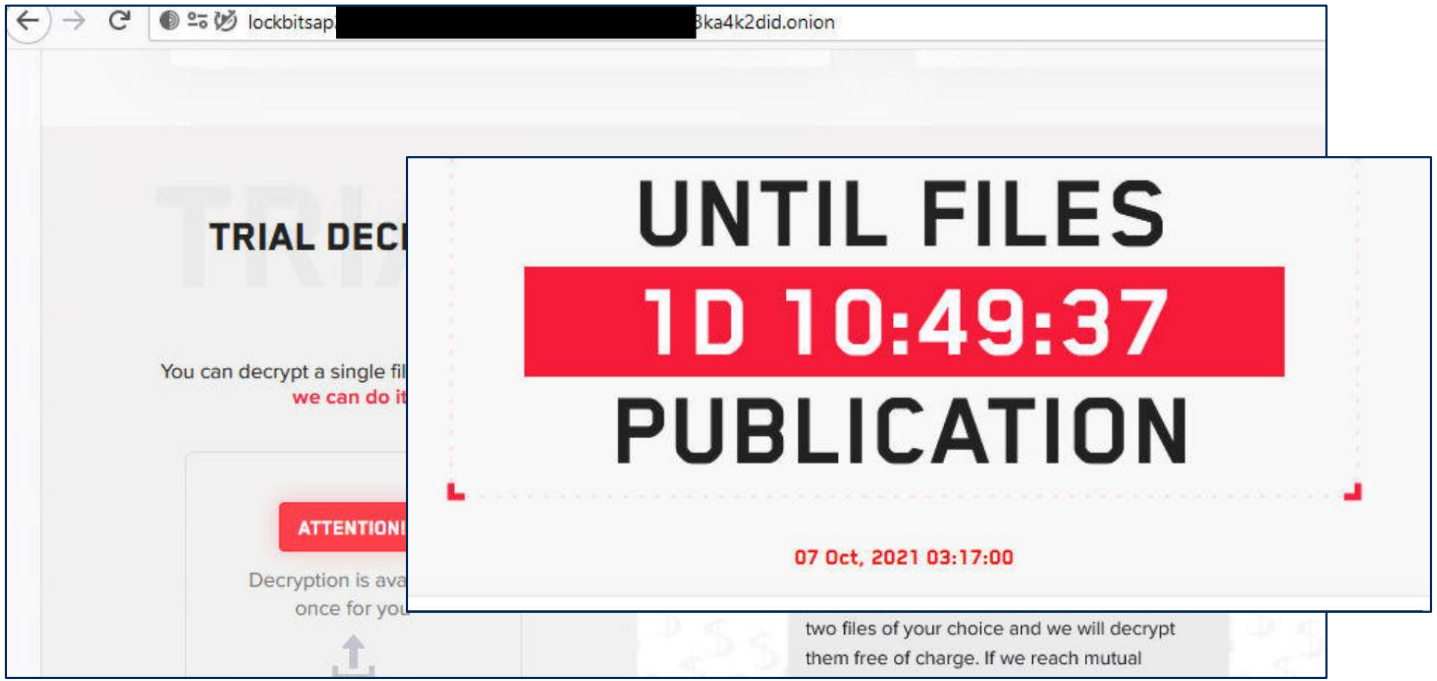
We advise your organization to contact us as soon as possible, otherwise your files will be published online on 25 January 2022. To avoid publication and recover your files, pay the amount of EUR 10 million.

Contact us at: xxxxxxxxx@tuta.li

Don't forget to include your code in the email:
{code_8379f5b_i8jsb:wYYAaXJLOHSsifho26qph+XqlmWWMoiK9f+khUG987idho987BUbj9817hBIGulkj}

Trending Cyber Attacks

Current Ransomware Example

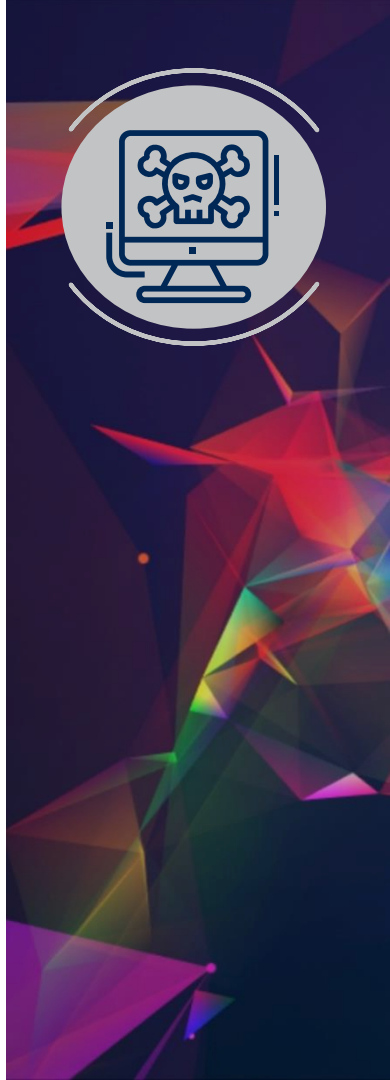


Trending Cyber Attacks

Triple extortion…

"Unfortunately, [your biggest customer's] security isn't as good as it should be. We've encrypted all of their data and systems, so you aren't going to be paid for your last deliveries any time soon. Sorry about that ☺

We also copied all their data. Don't worry, it's safe with us, for now. But if [customer] doesn't pay, we'll publish it. We found a lot of your data in there too. Unless you pay us 50BTC by [date], we'll publish your data too. You can contact us at [xxxxxxx]



3

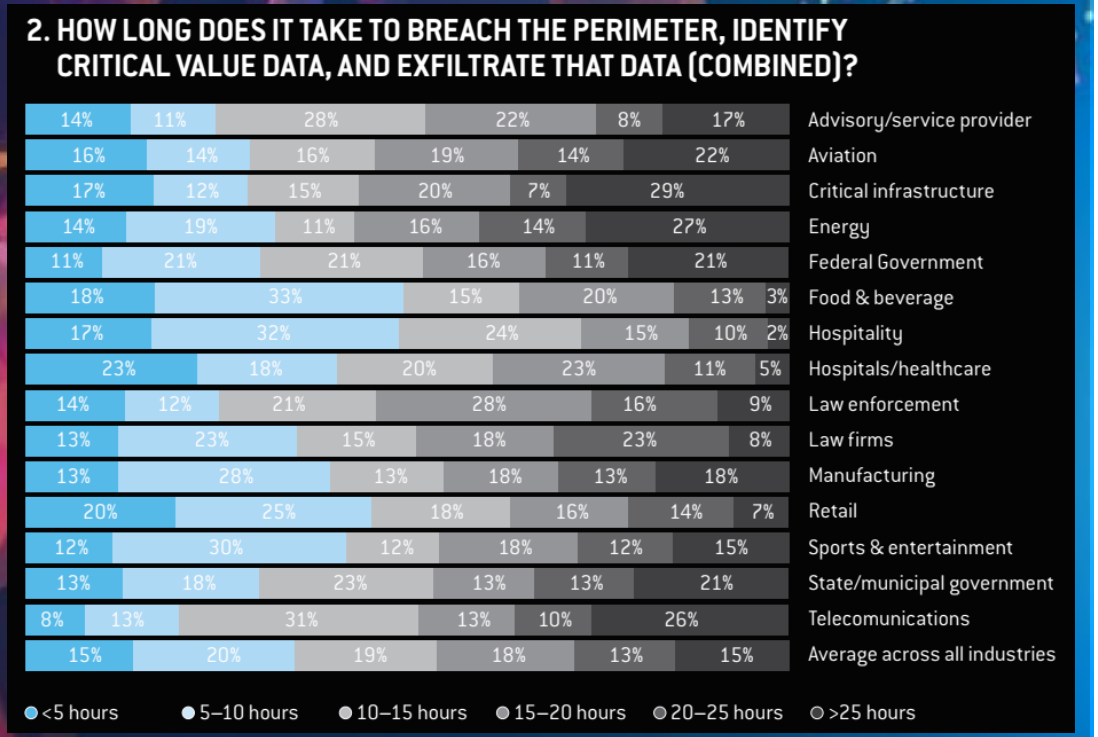
How to Prevent

How to Prevent

Think Like a Hacker

THE BLACK REPORT 2018

DECODING THE MINDS OF HACKERS



How to Prevent

Think Like a Hacker

6. What is your favorite type of social engineering attack?

16%
Phone

22%
Physical

62%
Phishing

How to Prevent

What Can You Do?

1. **Use Multi-Factor Authentication**

How to Prevent

What Can You Do?

2 **User Learning**

How to Prevent

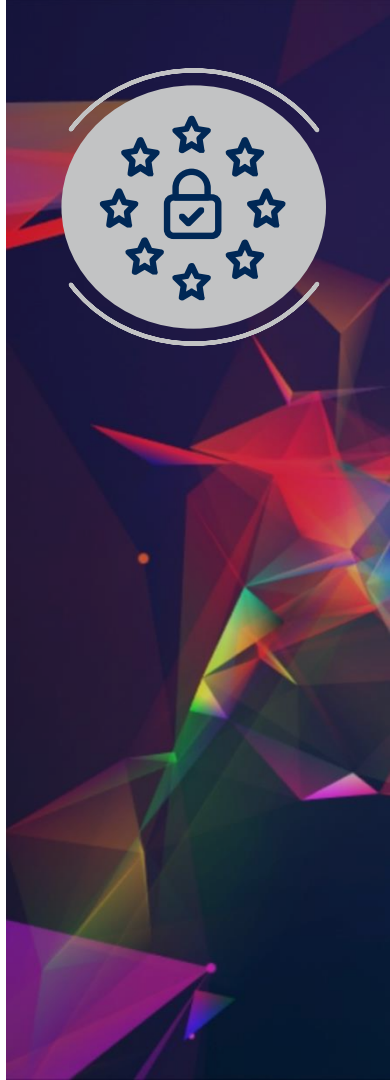
What Can You Do?

3 **Have an Incident Response Plan (and test it)**

4

Compliance

Compliance



NIST
National Institute of Standards and Technology
U.S. Department of Commerce

ISO

IEC

COBIT 5
AN ISACA® FRAMEWORK

ISA
GLOBAL CYBERSECURITY ALLIANCE

Questions

Baker McKenzie.

bakermckenzie.com