Common Attack Vectors and Threats

Authentication and Authorisation for Research and Collaboration

Hannah Short

IT-DI-CSO

CERN

ISGC, Taipei

12-18 March, 2016

Agenda

Trends in Cyber-Crime

- Attackers
- Attacks

The Federated Landscape

The Risk to R&E

Trends in Cyber-Crime

Profit

Risk

Interpol: Cyber-crime is bigger than cocaine, heroin and marijuana trafficking put together

Attackers

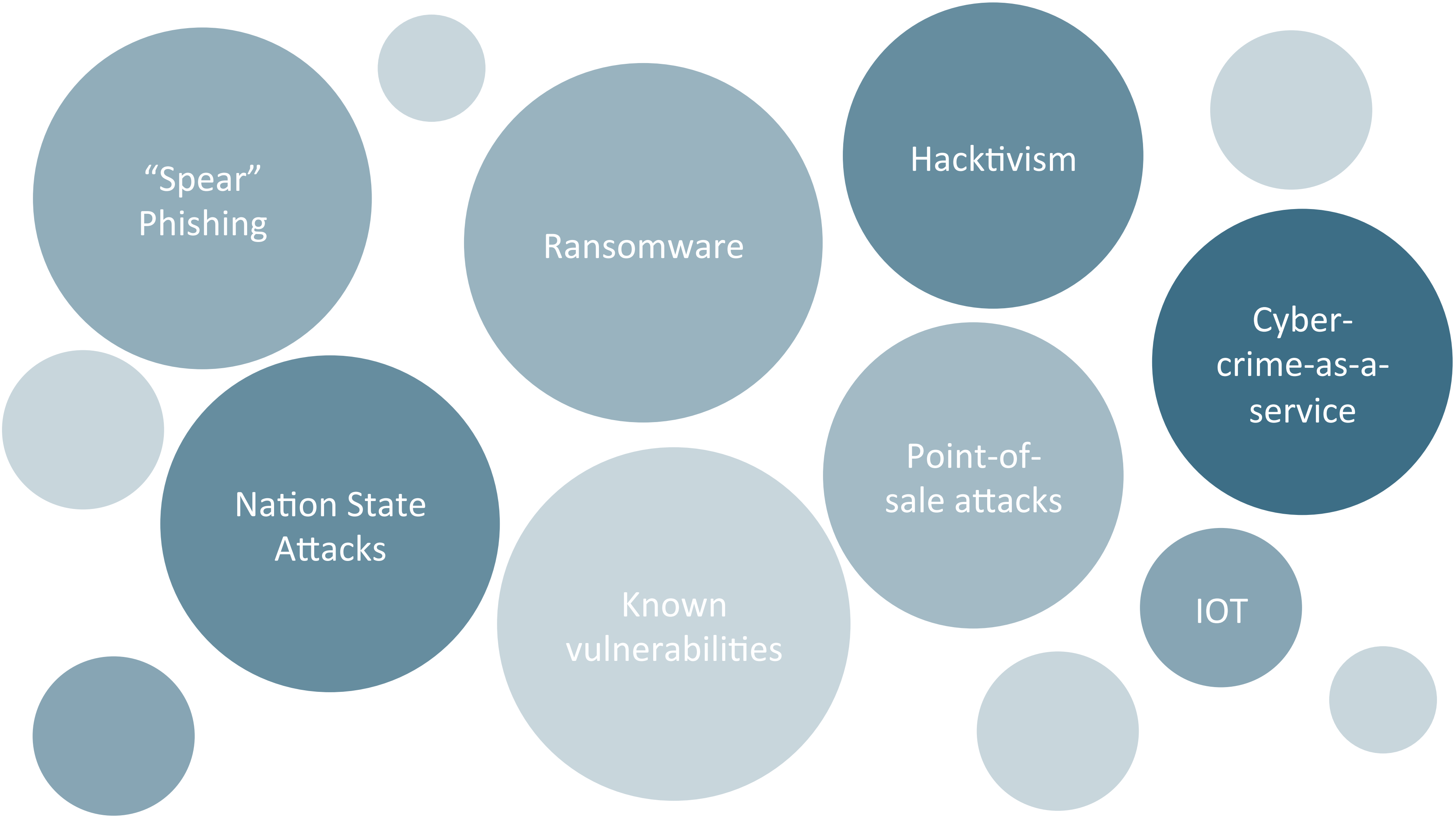
Who might be attacking you?

- **Cyber criminals**
  interested in making money through fraud or from the sale of valuable information.
- **Industrial competitors and foreign intelligence services**
  interested in gaining an economic advantage for their companies or countries.
- **Hackers**
  who find interfering with computer systems an enjoyable challenge.
- **Hacktivists**
  who wish to attack companies for political or ideological motives.
- **Employees**
  or those who have legitimate access, either by accidental or deliberate misuse.

Common Cyber Attacks, GCHQ, UK[1]

Plus, it can be outsourced!

Attacks



“Spear” Phishing

Ransomware

Hacktivism

Cyber-crime-as-a-service

Nation State Attacks

Known vulnerabilities

Point-of-sale attacks

IOT

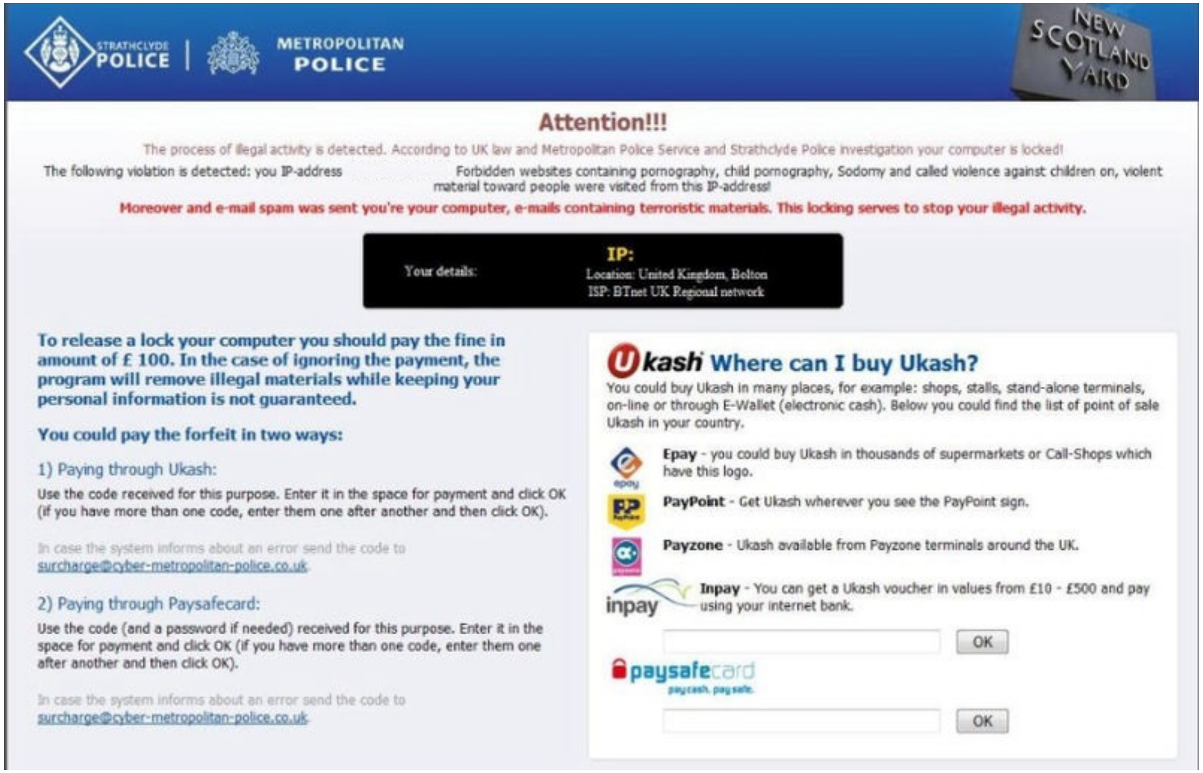
"Spear" Phishing

- Target executive individuals
  - Access to financial data
  - High security clearance
- Anti-phishing training courses are statistically ineffective
- Attacks becoming more sophisticated

Photo by Cat Vinton, Travel Photographer of the Year Finalist

It is likely that the next high profile R&E incident will be the result of targeted phishing

Ransomware



Attention!!!

The process of illegal activity is detected. According to UK law and Metropolitan Police Service and Strathclyde Police investigation your computer is locked!

The following violation is detected: you IP-address Forbidden websites containing pornography, child pornography, Sodomy and called violence against children on, violent material toward people were visited from this IP-address!

Moreover and e-mail spam was sent you're your computer, e-mails containing terroristic materials. This locking serves to stop your illegal activity.

Your details: **IP:**
Location: United Kingdom, Belton
ISP: BTnet UK Regional network

To release a lock your computer you should pay the fine in amount of £ 100. In the case of ignoring the payment, the program will remove illegal materials while keeping your personal information is not guaranteed.

You could pay the forfeit in two ways:

1) Paying through Ukash:

Use the code received for this purpose. Enter it in the space for payment and click OK (if you have more than one code, enter them one after another and then click OK).

In case the system informs about an error send the code to surcharge@cyber-metropolitan-police.co.uk.

2) Paying through Paysafecard:

Use the code (and a password if needed) received for this purpose. Enter it in the space for payment and click OK (if you have more than one code, enter them one after another and then click OK).

In case the system informs about an error send the code to surcharge@cyber-metropolitan-police.co.uk.

Ukash Where can I buy Ukash?

You could buy Ukash in many places, for example: shops, stalls, stand-alone terminals, on-line or through E-Wallet (electronic cash). Below you could find the list of point of sale Ukash in your country.

Epay - you could buy Ukash in thousands of supermarkets or Call-Shops which have this logo.

PayPoint - Get Ukash wherever you see the PayPoint sign.

Payzone - Ukash available from Payzone terminals around the UK.

Inpay - You can get a Ukash voucher in values from £10 - £500 and pay using your internet bank.

- Social engineering
- Easy profit
- Take backups!

Ransomware has caused an estimated $325 million in damages so far – Cyber Threat Alliance

http://nakedsecurity.sophos.com/2012/02/13/metropolitan-police-malware-warning/, https://en.wikipedia.org/w/index.php?curid=35026462

Known vulnerabilities

- The spread of freely-available, open source software has accelerated development but also impacted the risk of including vulnerabilities

- Patching times vary…

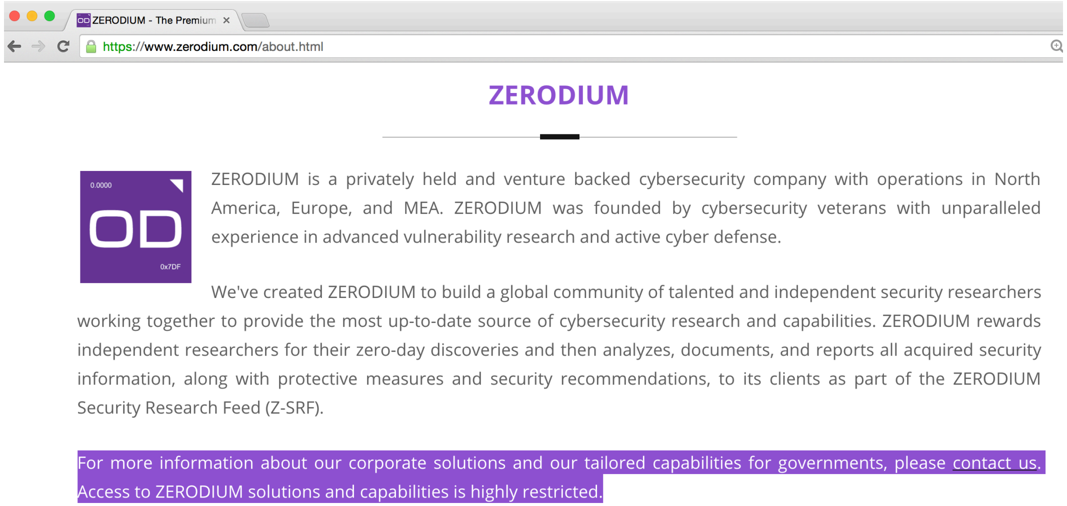
44% of 2014 breaches came from vulnerabilities that are two to four years old – HP Cyber Security Risk Report

Cyber-crime-as-a-service

- Companies paying for 0-days

- Clients include governments and corporations

- Organised, highly profitable business

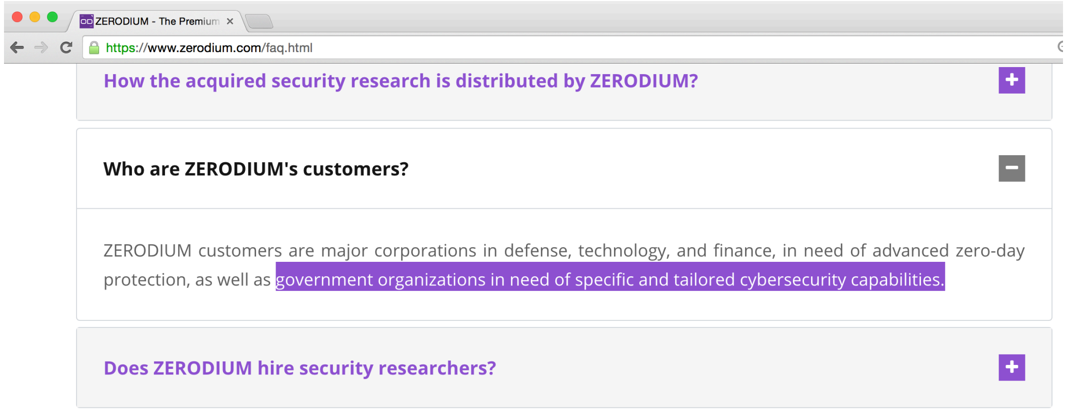


ZERODIUM

ZERODIUM is a privately held and venture backed cybersecurity company with operations in North America, Europe, and MEA. ZERODIUM was founded by cybersecurity veterans with unparalleled experience in advanced vulnerability research and active cyber defense.

We've created ZERODIUM to build a global community of talented and independent security researchers working together to provide the most up-to-date source of cybersecurity research and capabilities. ZERODIUM rewards independent researchers for their zero-day discoveries and then analyzes, documents, and reports all acquired security information, along with protective measures and security recommendations, to its clients as part of the ZERODIUM Security Research Feed (Z-SRF).

For more information about our corporate solutions and our tailored capabilities for governments, please contact us. Access to ZERODIUM solutions and capabilities is highly restricted.



How the acquired security research is distributed by ZERODIUM? +

Who are ZERODIUM's customers? −

ZERODIUM customers are major corporations in defense, technology, and finance, in need of advanced zero-day protection, as well as government organizations in need of specific and tailored cybersecurity capabilities.

Does ZERODIUM hire security researchers? +

Nation state attacks

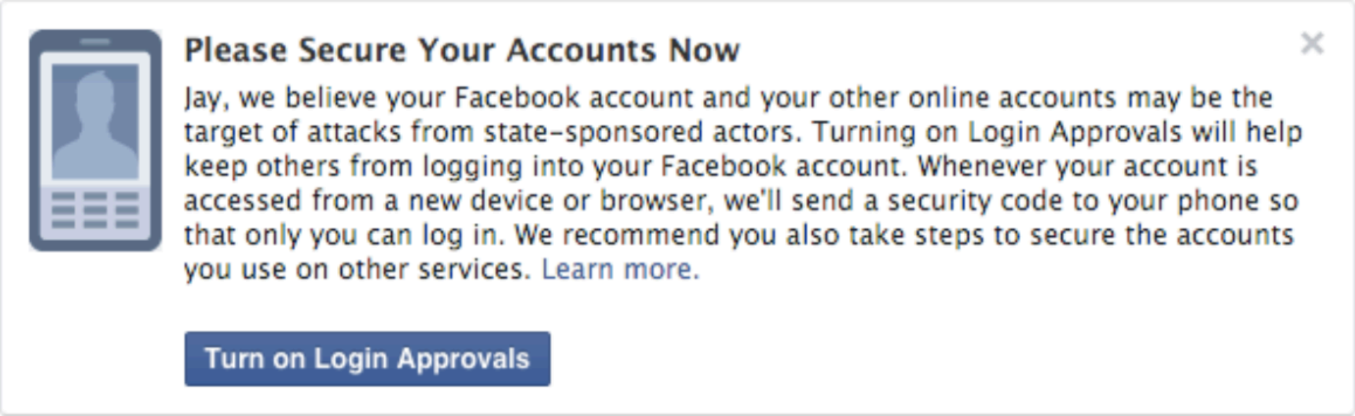
- Tools
  - Complex frameworks, many years of development
  - Targeted Social Engineering
  - Undermine encryption and install backdoors
- Plausible deniability through outsourcing
- According to Symantec, 70% APT victims profile
  - Research, innovation, IT.
  - “forward looking technologies” highly sellable
- Objectives include corporate espionage, political advantage…

Nation state attacks

Belgacom Attack: Britain's GCHQ Hacked Belgian Telecoms Firm

REUTERS

A cyber attack on Belgacom raised considerable attention last week. Documents leaked by Edward Snowden and seen by SPIEGEL indicate that Britain's GCHQ intelligence agency was responsible for the attack.

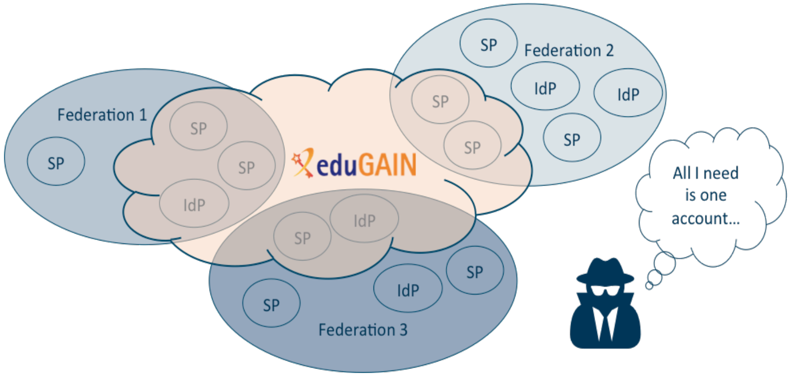


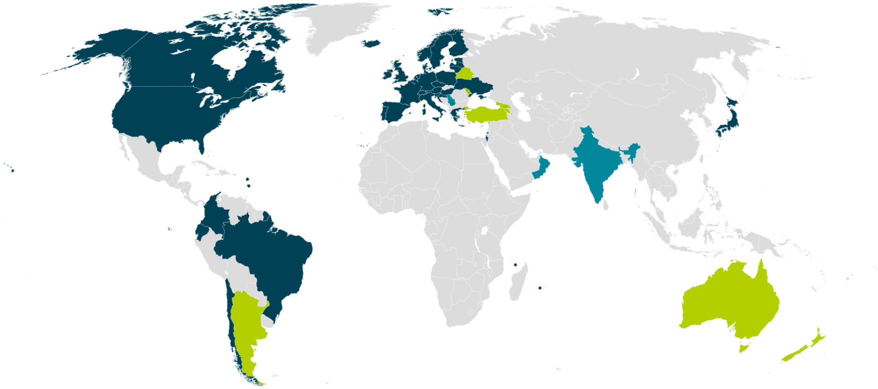
Please Secure Your Accounts Now

Jay, we believe your Facebook account and your other online accounts may be the target of attacks from state-sponsored actors. Turning on Login Approvals will help keep others from logging into your Facebook account. Whenever your account is accessed from a new device or browser, we'll send a security code to your phone so that only you can log in. We recommend you also take steps to secure the accounts you use on other services. Learn more.

The federated landscape

61 national federations





40 federations in eduGAIN

Why the interest in Research and Education?

Most of our data is public, plus we have little money… why would someone go to all that trouble?

Common known objectives of intrusions

- Politics
- Strategy
- Trends in a sector, tender purchasing strategy
- Trade secrets, pricing discussions, competitor pricing information
- Gain a competitive edge
- Insider trading

Besides.. customers may not know that our data is publicly available!

For further reading

1. Common Cyber Attacks, CERT-UK, CESG
   https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/400106/Common_Cyber_Attacks-Reducing_The_Impact.pdf
2. Common Attack Patterns 2014, David Bisson, Tripwire,
   http://www.tripwire.com/state-of-security/security-data-protection/cyber-security/the-5-most-common-attack-patterns-of-2014/
3. Security Predictions 2015, WIRED,
   http://www.wired.com/2015/01/security-predictions-2015/
4. The Year in Cybersecurity, NBC,
   http://www.nbcnews.com/tech/security/year-cybersecurity-5-threats-watch-2015-n270271
5. Cyber Threat Alliance
   http://cyberthreatalliance.org/cryptowall-executive-summary.pdf
6. Sophos
   https://www.sophos.com/threat-center/medialibrary/PDFs/other/sophos-trends-and-predictions-2015.pdf
7. Cyber Security Risk Report, HP,
   http://www8.hp.com/us/en/software-solutions/cyber-risk-report-security-vulnerability/index.html?jumpid=ba_r329_hhoaffiliate&aid=38293&pbid=je6NUbpObpQ&aoid=35252&siteid=je6NUbpObpQ-RpZVcUyV_oRAC_GmDfYpxQ

Thank you

Any Questions?

hannah.short@cern.ch

AARC

https://aarc-project.eu

The work leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 653965 (AARC).