Spotlight on Security

the past, present and future

Thomas Ljungberg Kristensen, thomas@welcomesecurity.net

Thomas Ljungberg Kristensen

96 Aarhus Universitet, Datalog

03 Systematic, Systems Engineer

07 Danske Bank, Developer

12 Kamstrup, Systems Engineer

14 FortConsult, Senior Security Consultant

15 WelcomeSecurity, Security Advisor

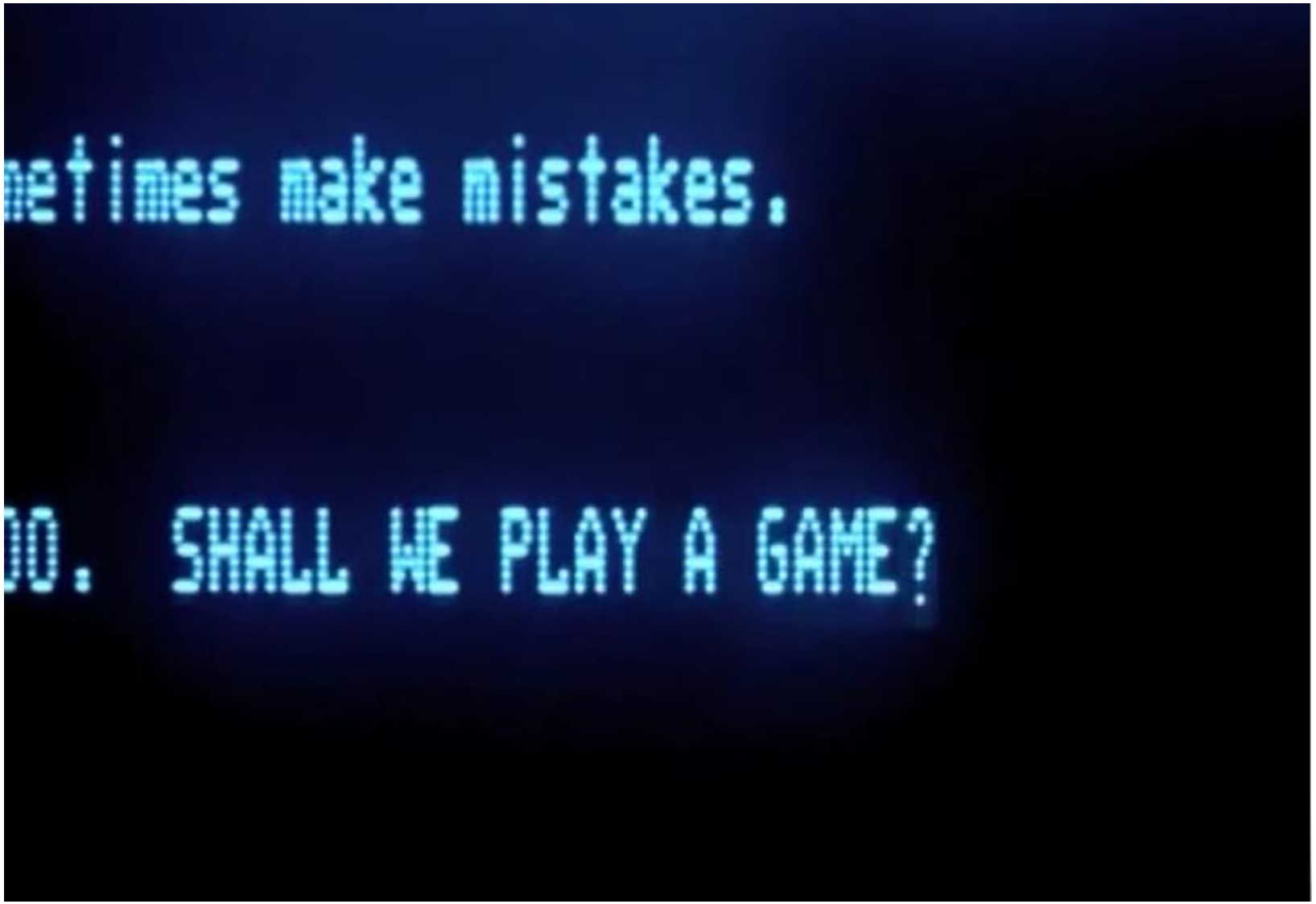
19 OWASP, Co-chapter Lead - Aarhus

19 Deloitte, Senior Manager, Cyber

20 Norlys, IT security architect

The Past

“Shall we play a game?”



Source: Wargames, 1983, MGM, https://www.mgm.com/#/our-titles/2117/WarGames-(1983)

Mitnick served five years in prison—four and a half years pre-trial and eight months in solitary confinement—because, according to Mitnick, law enforcement officials convinced a judge that he had the ability to "start a nuclear war by whistling into a pay phone",[23] meaning that law enforcement told the judge that he could somehow dial into the NORAD modem via a payphone from prison and communicate with the modem by whistling to launch nuclear missiles.[24] In addition, a number of media outlets reported on the unavailability of Kosher meals at the prison where he was incarcerated.[25]

Source: Wikipedia (https://en.wikipedia.org/wiki/Kevin_Mitnick) and https://twitter.com/kevinmitnick

The Present

"We cannot be breached!"

Fra: Info Nets <noreply@nets.com>
Dato: 8. marts 2017 kl. 10.07.57 CET
Til:
Emne: Adgang Til Dine Konto

Kære kunder Nets,

Det ser ud til, at en anden bruger din konto.

For din sikkerhed, har vi blokeret din konto
Vi har brug for nogle oplysninger for at løse dette problem

> Klik her https://www.nets.eu/dk-da/l%C3%B8sninger/dankort/022136

© Nets i Danmark (HQ)-kontoteamet

POST

Du har uforløste pakken

Vi har modtaget din pakke **CT5389919582DK** på **2015/09/21**. Courier var ude af stand til at levere denne pakke til dig

Få og udskrive forsendelsesetiketten, og vise det på det nærmeste posthus for at få din pakke.

Få en adresselapp

Hvis pakken ikke er modtaget inden 20 arbejdsdage PostNord AB vil være berettiget til at kræve kompensation fra dig - 55 kroner for hver dag i at holde. Du kan finde oplysninger om fremgangsmåden ved og betingelserne af pakken holde i det nærmeste kontor.

Dette er en automatisk genereret meddelelse. Klik her for at afmelde

Fra: **Skat.dk** <skat@skat.dk>
Dato: 1. okt. 2013 12.00
Emne: ID:38933 - tilbagebetaling af skat - DKK 6940,00
Til: XXX

SKAT

Bemærk: Tilbagebetaling af skat for året 2012

Kære skatteyder,

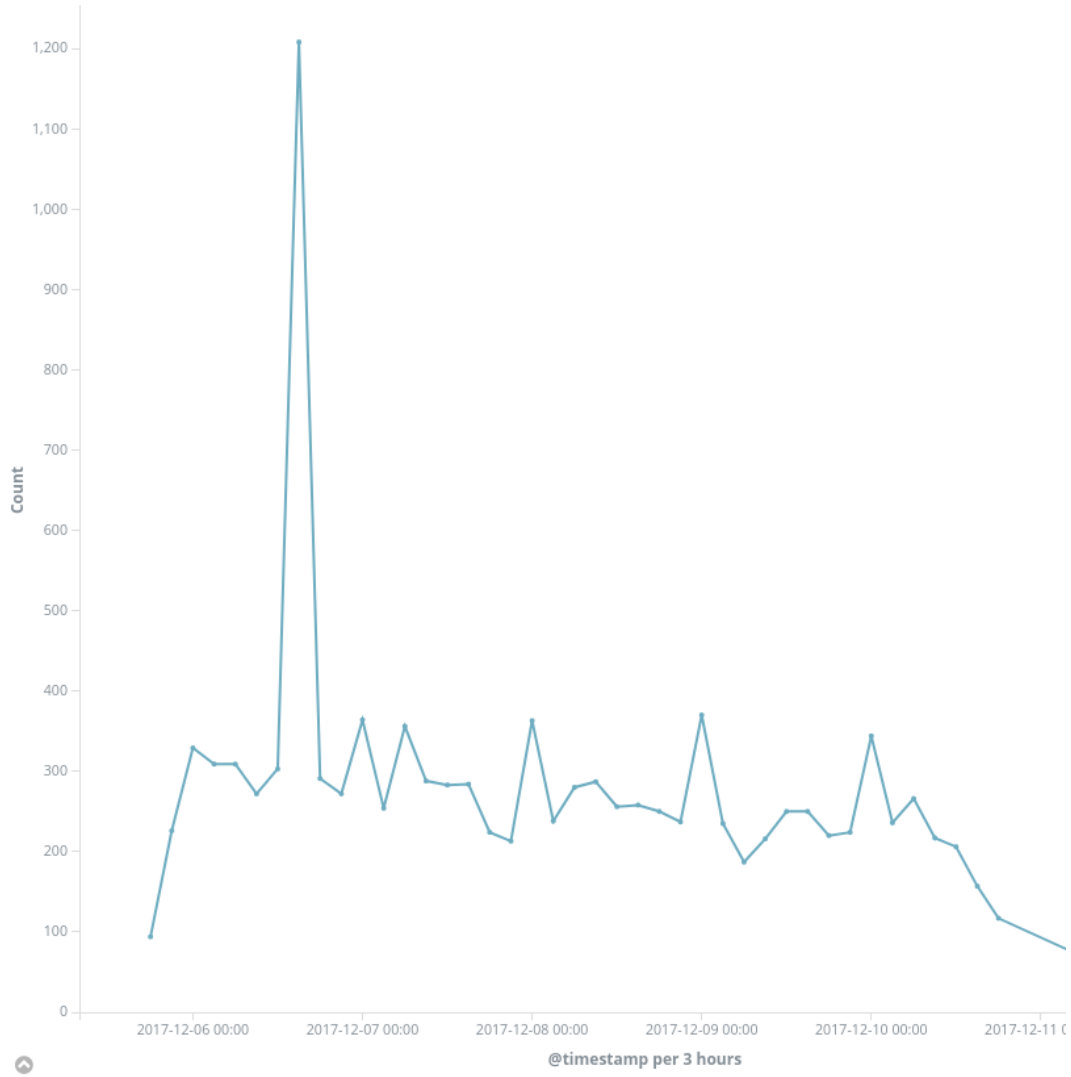
Vores registreringer viser, at du er kvalificeret til en tilbagebetaling af skat af:
DKK 6940,00

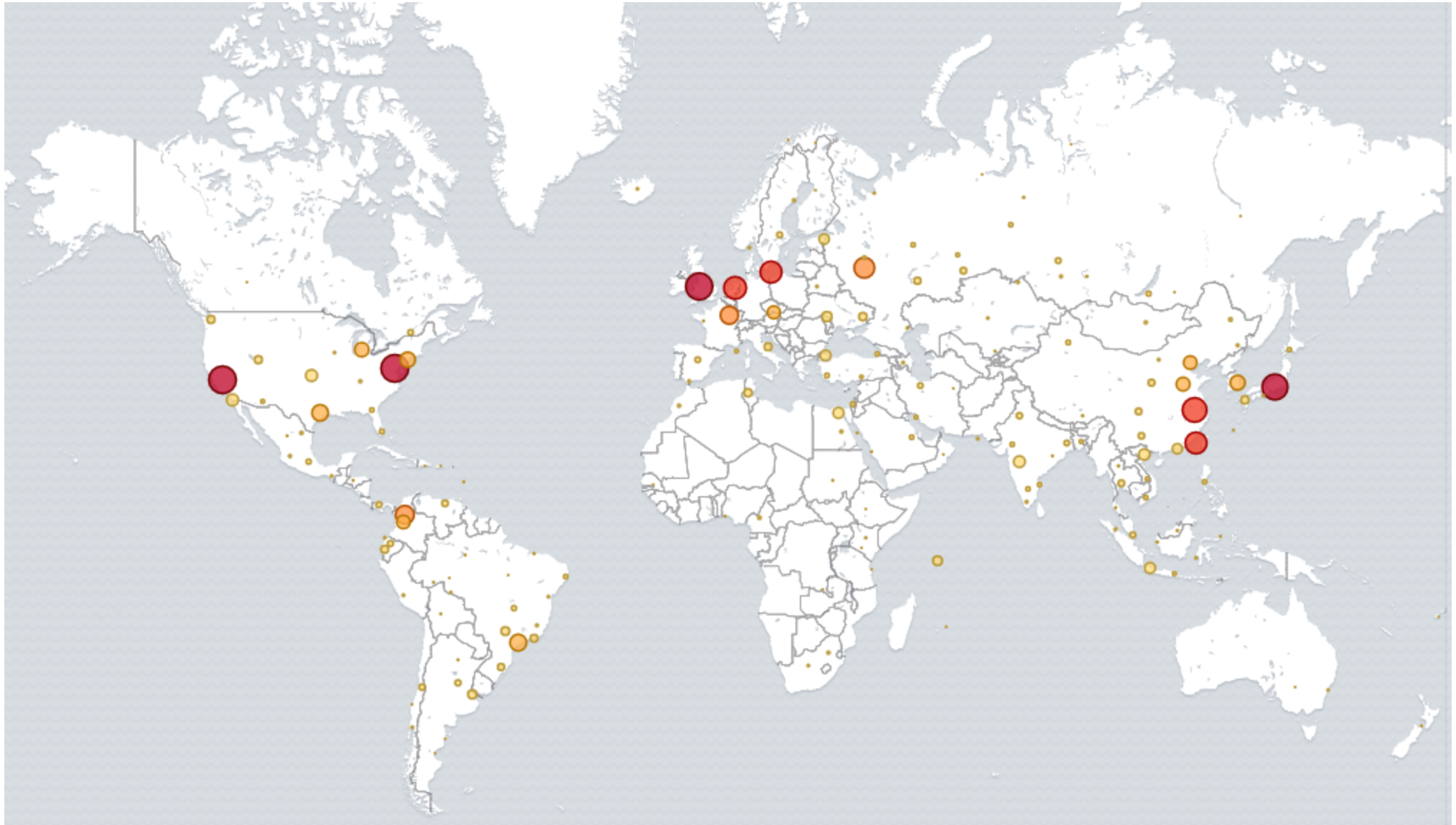
For at få adgang til din skat tilbagebetaling, klik venligst her.

Udfyld venligst formularen indtil d. **02-10-2013.**
Den hurtigste og nemmeste måde at modtage din tilbagebetaling på er ved direkte inc
check/opsparingskonto.

Vores hovedkontor adresse kan findes på vores hjemmeside på
http://www.skat.dk

Source : http://www.it-blogger.dk/post-nord-virus-rammer-danmark/, http://skat.dk/SKAT.aspx?oId=68747 og https://www.nets.eu/dk-da/digital-sikkerhed/Pages/Phishing.aspx


1,200
1,100
1,000
900
800
700
600
500
400
300
200
100
0
Count
2017-12-06 00:00
2017-12-07 00:00
2017-12-08 00:00
2017-12-09 00:00
2017-12-10 00:00
@timestamp per 3 hours



DU ER EN SKYDESKIVE

Brugernavn og passwords

Hvis du er blevet hacket, kan IT-kriminelle installere programmer på din computer, der opfanger alt, hvad du taster inklusiv dine brugernavne og passwords. Den information bruges til at logge på dine online-konti så som:

- *Dine bankkonti, hvorfra de kan stjæle eller overføre dine penge.*
- *Din iCloud, Google Drev eller Dropbox konto hvilket kan give adgang til dine følsomme data.*
- *Dine konti til online indkøb, så kan de handle i dit navn og for dine penge.*

Høste informationer fra din e-mail

Hvis du er blevet hacket, har IT-kriminelle adgang til din e-mail og kan finde information de kan sælge. Det kan eksempelvis være:

- *Alle navne, e-mailadresser og telefonnumre fra din kontaktliste/telefonbog.*
- *Alle dine personlige e-mails og arbejds e-mail.*

Virtuelle varer

Hvis du er blevet hacket, kan IT-kriminelle kopiere og stjæle alle dine virtuelle varer og sælge dem til andre. Det drejer sig om:

- *Dine karakterer, varer og valuta i online spil.*
- *Alle licenser til software, operativsystemer og spil.*

Botnet

Hvis du er blevet hacket, kan din computer blive forbundet til et netværk af hackede computere, der bliver kontrolleret af den IT-kriminelle. Dette netværk kaldes et Botnet og kan blive brugt til at:

- *Sende spam til millioner personer.*
- *Overbelaste andres systemer og få dem til at gå ned.*

Du ved det måske ikke, men du er et mål for IT-kriminelle. Din computer, dine mobile enheder, dine (online) konti og dine informationer har en meget høj værdi. Denne plakat sætter fokus på, hvordan IT-kriminelle kan tjene penge på at hacke dig. Heldigvis kan du beskytte dig og din familie ved at følge nogle simple råd. Hvis du vil vide mere kan du abonnere på det månedlige nyhedsbrev om IT-sikkerhed fra OUCH!

www.securingthehuman.org/ouch

Identitetstyveri

Hvis du er blevet hacket, kan IT-kriminelle benytte din online profil til at begå svindel eller sælge din identitet til tredjepart. Det kan være:

- *Din Facebook, Twitter eller LinkedIn konto.*
- *Din e-mail konto.*
- *Din Skype konto.*

Web Server

Hvis du er blevet hacket, kan IT-kriminelle benytte din computer som server til:

- *At forsøge at stjæle andres brugernavne og passwords.*
- *Programmer, der hacker andre computere.*
- *Distribution af børneporno, piratkopier af film og stjålet musik.*

Økonomisk

Hvis du er blevet hacket, kan IT-kriminelle lede efter værdifuld information i dit system så som:

- *Information om dine kreditkort.*
- *Dine skatteoplysninger.*
- *Dine investeringer og pension.*

Afpresning

Hvis du er blevet hacket, kan IT-kriminelle overtage din computer og kræve penge. Dette kan de gøre ved at:

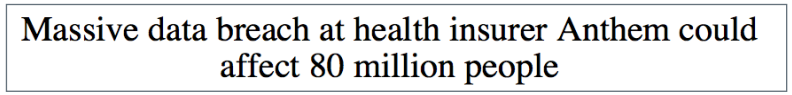
- *Tage billede med dit indbyggede kamera og kræve penge for at destruere det eller for ikke at offentliggøre det.*
- *Kryptere al data på din computer og kræve penge for at dekryptere det.*
- *True med at offentliggøre hvilke hjemmesider du har besøgt.*

Denne plakat er baseret på arbejde udført af Brian Krebs. Du kan lære mere om IT-kriminalitet ved at følge hans blog http://krebsonsecurity.com

Source: http://securingthehuman.sans.org/media/resources/STH-Poster-YouAreATarget-Danish.zip

http://www.nytimes.com/2014/08/06/business/target-puts-data-breach-costs-at-148-million.html

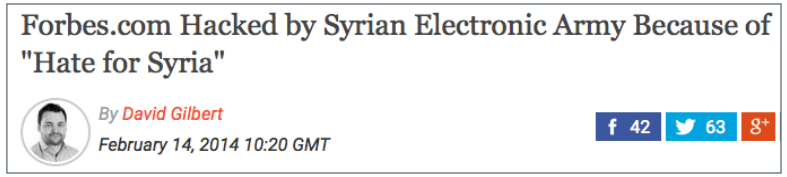
http://www.bbc.com/news/technology-26971363



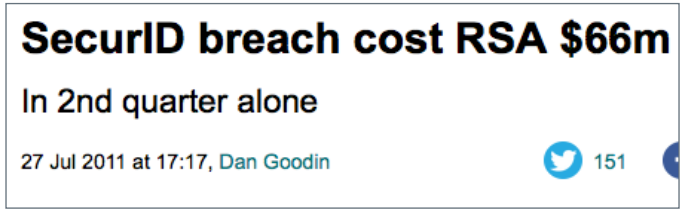
http://theweek.com/5things/537729/massive-data-breach-health-insurer-anthem-could-affect-80-million-people

http://www.huffingtonpost.com/2011/06/08/sony-hack-problems_n_873443.html

http://www.cnet.com/news/lenovo-hit-by-lawsuit-over-superfish-adware/

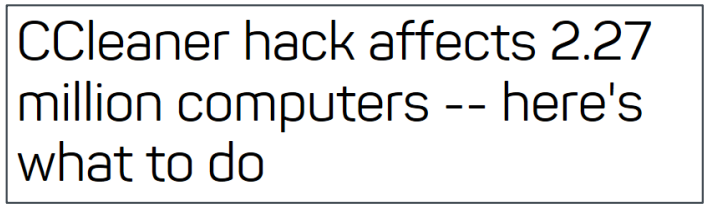


http://www.ibtimes.co.uk/forbes-com-hacked-by-syrian-electronic-army-because-hate-syria-1436415



http://www.theregister.co.uk/2011/07/27/rsa_security_breach/

http://www.usatoday.com/story/tech/2014/10/02/jp-morgan-security-breach/16590689/



https://www.cnet.com/how-to/ccleaner-was-hacked-heres-what-to-do-next/

NYHEDER

DR

TEMA HACKERANGREB

37 ARTIKLER

Hackerangreb koster Mærsk milliardbeløb

Mærsk anslår, at hackerangrebet fra juni og juli vil koste selskabet 1,3 til 1,9 milliarder kroner.

Source: https://www.dr.dk/nyheder/penge/hackerangreb-koster-maersk-milliardbeloeb

1 Cyber-angreb er den største risiko for virksomheder i Europa og medfører store økonomiske tab og potentielt konkurser

44% af de danske borgere har være udsat for: Infektion med skadelig software, misbrug af fortrolige oplysninger, økonomisk tab og tab af data

20 nye sårbarheder bliver offentliggjort om dagen

73% af danske virksomheder er blevet angrebet – eller forsøgt angrebet!

1/4 million angreb fra internettet hver dag!

2 minutter tager det, før en ny enhed på Internettet bliver ramt

https://www.danskerhverv.dk/siteassets/mediafolder/downloads/analysenotater-2017/66-cybersikkerhed.pdf,
https://digst.dk/media/18755/danskernes_informationssikkerhed_december_2018_191218.pdf,
https://www.weforum.org/reports/regional-risks-for-doing-business,
https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf

Bring a company offline?

Source: https://www.youtube.com/watch?v=vn-lU3Zu3dw

Annual license: $ 1500
Half-year license: $ 1000
3-month license: $ 700

Update cryptor $ 50
Changing domain $ 20 multidomain $ 200 to license.
During the term of the license all the updates are free.

Rent on our server:

1 week (7 full days): $ 200
2 weeks (14 full days): $ 300
3 weeks (21 full day): $ 400
4 weeks (31 full day): $ 500
24-hour test: $ 50

- There is restriction on the volume of incoming traffic to a leasehold system, depending on the time of the contract.

Providing our proper domain included. The subsequent change of the domain: $ 35
No longer any hidden fees, rental includes full support for the duration of the contract.

Source: http://nakedsecurity.sophos.com/exploring-the-blackhole-exploit-kit-3/

…an emerging trend with traditional organized crime syndicates and criminally minded technology professionals working together and pooling their resources and expertise…

Source: http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime

The most common 'positions' or specializations according to the FBI are:

1. **Programmers**. Who develop the exploits and malware used to commit cyber-crimes.

2. **Distributors**. Who trade and sell stolen data and act as vouchers for the goods provided by other specialists.

3. **Tech experts**. Who maintain the criminal enterprise's IT infrastructure, including servers, encryption technologies, databases, and the like.

4. **Hackers**. Who search for and exploit applications, systems and network vulnerabilities.

5. **Fraudsters**. Who create and deploy various social engineering schemes, such as phishing and spam.

6. **Hosted systems providers**. Who offer safe hosting of illicit content servers and sites.

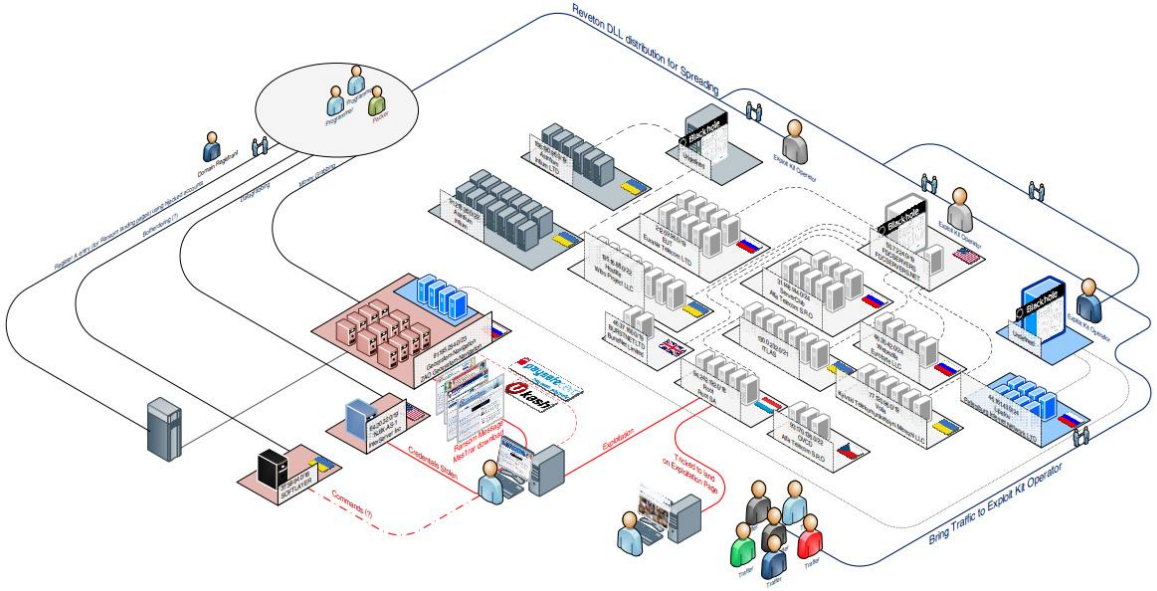
7. **Cashiers**. Who control drop accounts and provide names and accounts to other criminals for a fee.

8. **Money mules**. Who complete wire transfers between bank accounts. The money mules may use student and work visas to travel to the U.S. to open bank accounts.

9. **Tellers**. Who are charged with transferring and laundering illicitly gained proceeds through digital currency services and different world currencies.

10. **Organization Leaders**. Often "people persons" without technical skills. The leaders assemble the team and choose the targets.

Sources: "The Cyber-crime black market uncovered" by Panda Security



Sources: http://krebsonsecurity.com/2012/08/inside-a-reveton-ransomware-operation/

Dedicated server (powerful servers)	0.50 – 1 (10 – 20)
1000 downloads in EU	80
Programming Services	? (100 – 250)
1 day DDoS	30 – 70
Cheap email spamming	10 per 1,000,000 emails
Email spamming, custom database	50 – 500 per 50,000 to 1,000,000 emails
SMS spamming	3 – 150 per 100 – 10,000 SMS
1 hour call flooding	2 – 5
Bots	200 for 2,000 bots
Copy of scanned EU passport	5
Windows 7 Ultimate license	7
Fake website	5 – 20
Credit card details	2 – 90 (add 190 for physical card)
Bank Credentials (with guaranty)	80 – 700
Purchase and forward of products	30 – 300

Sources: ”Russian Underground 101” by Trend Micro and ”The Cyber-crime black market uncovered” by Panda Security

Fake web site	$20
1,000,000 spam emails	$10
5 Servers to host site	$70
	$100

Break-even at 0.005% (or 50) people entering credit card details

Advanced Persistent Threat (APT): The Uninvited Guest

How attackers remain in your network harvesting informationand avoiding detection over time

1. INCURSION
Attackers break into network by using social engineering to deliver targeted malware to vulnerable systems and people.

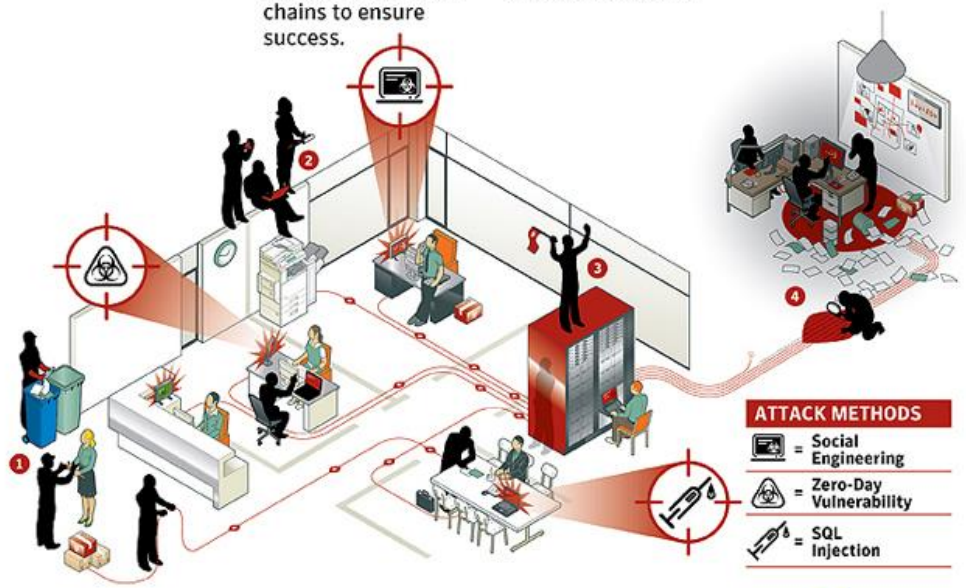
2. DISCOVERY
Once in, the attackers stay "low and slow" to avoid detection.

They then map the organization's defenses from the inside and create a battle plan and deploy multiple parallel kill chains to ensure success.

3. CAPTURE
Attackers access unprotected systems and capture information over an extended period.

They may also install malware to secretly acquire data or disrupt operations.

4. EXFILTRATION
Captured information is sent back to attack team's home base for analysis and further exploitation fraud—or worse.



ATTACK METHODS

- = Social Engineering
- = Zero-Day Vulnerability
- = SQL Injection

Symantec.

Source: http://www.symantec.com/theme.jsp?themeid=apt-infographic-1

WIRED

NSA HACKER CHIEF EXPLAINS HOW TO KEEP HIM OUT OF YOUR

Share

SHARE

TWEET

COMMENT

EMAIL

KIM ZETTER

IT WAS THE talk most anticipated
Usenix Enigma security conferen
that even the other speakers wer

How the NSA Gets You

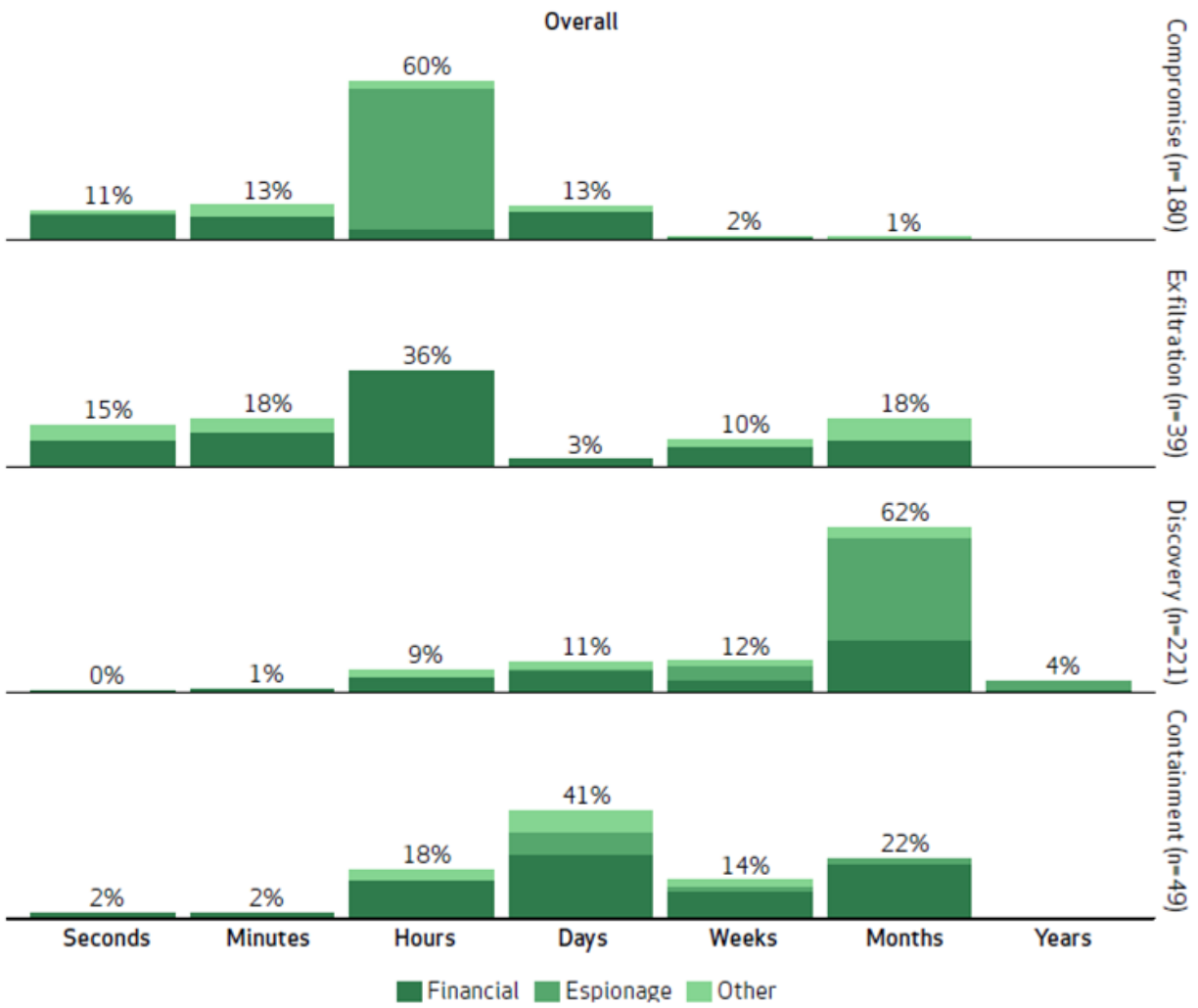
In the world of advanced persistent threat actors (APT) like the NSA, credentials are king for gaining access to systems. Not the login credentials of your organization's VIPs, but the credentials of network administrators and others with high levels of network access and privileges that can open the kingdom to intruders. Per the words of a recently leaked NSA document, the NSA hunts sysadmins.

The NSA is also keen to find any hardcoded passwords in software or passwords that are transmitted in the clear—especially by old, legacy protocols—that can help them move laterally through a network once inside.

Source: https://www.wired.com/2016/01/nsa-hacker-chief-explains-how-to-keep-him-out-of-your-system/

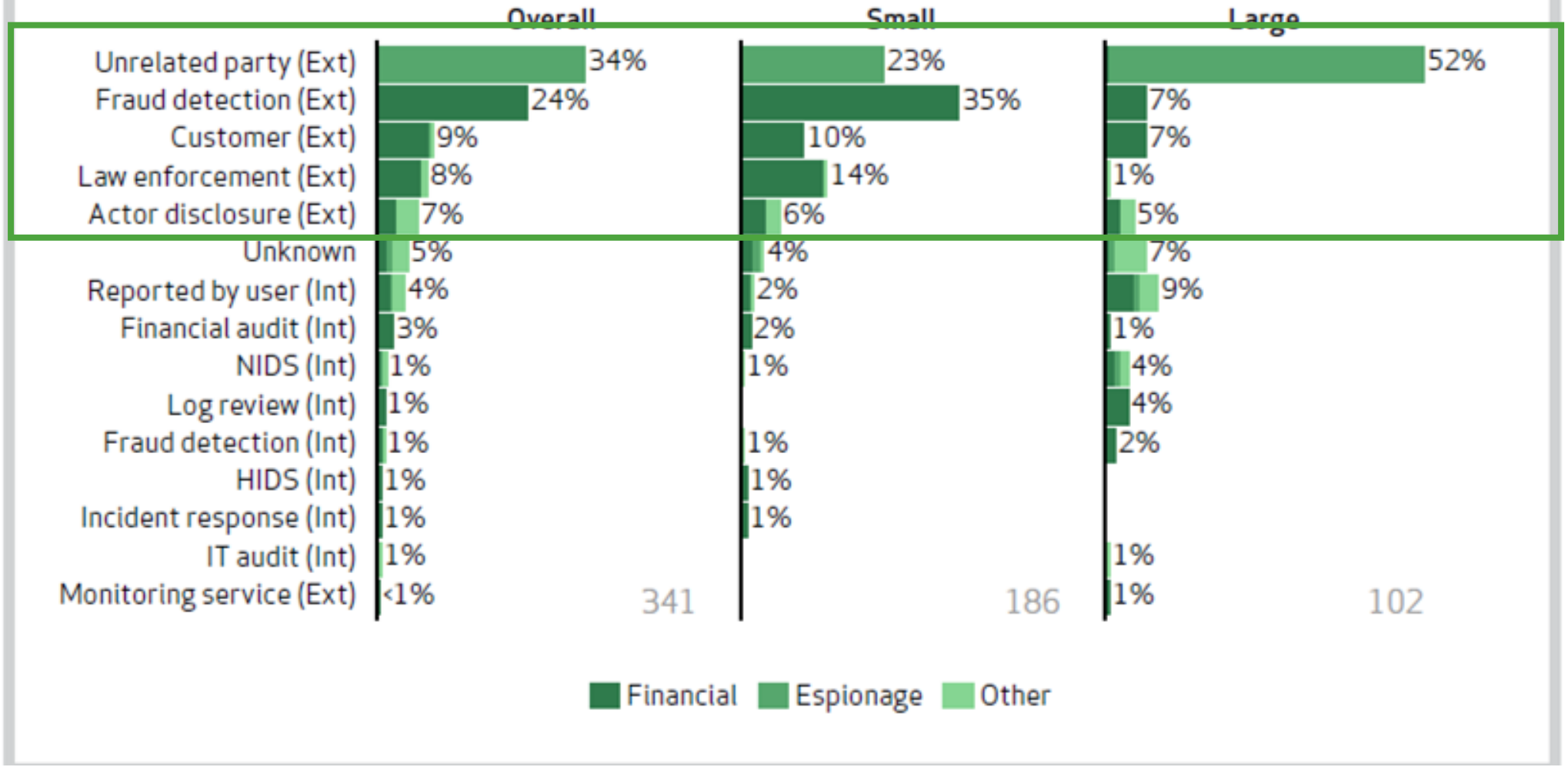
Compromise
Exfiltration
Discovery
Containment

Figure 41: Timespan of events



Sources: Verizon, 2013 Data Breach Investigations Report

Figure 44: Discovery methods



Sources: Verizon, 2013 Data Breach Investigations Report

“There are only two types of companies: Those that have been hacked, and those that will be.”

Former FBI Director Rubert Muller

The Future

"Assume Breach – Detect Compromise"

Trusselsvurdering: Cybertruslen mod Danmark 2019

Formålet med denne årlige, nationale trusselsvurdering er at redegøre for den samlede cybertrussel, der møder danske myndigheder og virksomheder. Truslen er størst fra cyberspionage udført at stater og fra cyberkriminalitet.

Hovedvurdering

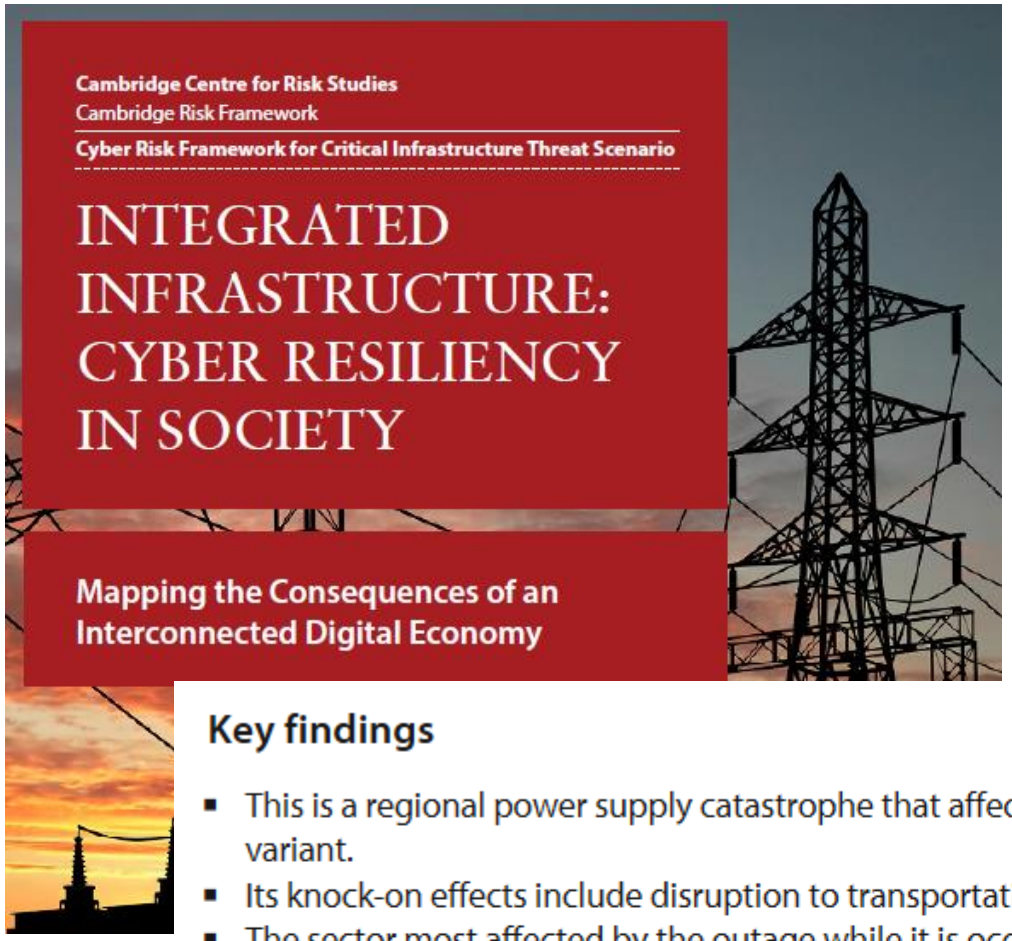
- Truslen fra cyberspionage er **MEGET HØJ**. Truslen er særligt udtalt mod de dele af staten, der beskæftiger sig med udenrigs, sikkerheds- og forsvarspolitik. Truslen er også rettet mod myndigheder og virksomheder i samfundsvigtige sektorer, da hver sektor har forskellige typer viden, som fremmede stater har interesse i. Flere stater forsøger at udføre cyberspionage mod danske interesser, og det er en udvikling, der fortsætter, i takt med at flere stater opbygger og udvikler deres cyberkapaciteter.
- Truslen fra cyberkriminalitet er **MEGET HØJ**. Myndigheder og virksomheder i samtlige sektorer i Danmark kan forvente løbende at blive udsat for cyberkriminalitet. Visse typer cyberkriminalitet kan have alvorlige konsekvenser for myndigheder og virksomheder i samfundsvigtige sektorer og derfor for det danske samfund.
- Truslen fra cyberaktivisme er **MIDDEL**. Cyberaktivister retter sjældent deres fokus mod danske myndigheder og virksomheder. Nogle hackergrupper og individer i cyberaktivistiske netværk har dog væsentlige kapaciteter. Truslen kan derfor stige pludseligt, hvis danske myndigheder eller virksomheder kommer i cyberaktivisters søgelys.
- Truslen fra cyberterror er **LAV**. Militante ekstremister har i få tilfælde vist interesse i at udføre cyberterror, men de har fortsat ikke kapacitet til dette.
- Det er mindre sandsynligt, at fremmede stater har til hensigt at rette destruktive cyberangreb mod samfundsvigtig infrastruktur i Danmark på kort sigt. Det er dog muligt, at danske virksomheder og myndigheder kan blive ramt som følgevirkning af destruktive cyberangreb mod mål uden for Danmark.
- Teknologiske udviklinger, såsom Internet of Things og kunstig intelligens, vil medføre nye muligheder til gavn for samfundet, men vil også åbne for en større angrebsflade for hackere. Der vil også være en øget risiko for, at cyberangreb kan medføre fysiske ødelæggelser, da enheder koblet til internettet i højere grad styrer fysiske systemer.

Source: https://fe-ddis.dk/cfcs/publikationer/Documents/Cybertruslen-mod-Danmark-2019.pdf

INTERNATIONALT

FE-chefen: Rusland vil hacke vores forvaltning og Kina vores virksomheder

Source: https://www.berlingske.dk/internationalt/fe-chefen-rusland-vil-hacke-vores-forvaltning-og-kina-vores-virksomheder



Key findings

- This is a regional power supply catastrophe that affects between 9 million and 13 million electricity customers depending on the scenario variant.
- Its knock-on effects include disruption to transportation, digital communications, and water services for 8 to 13 million people.
- The sector most affected by the outage while it is occurring is Financial Services, which loses an estimated £1.3 billion during the period of the outage, in the baseline scenario.
- The secondary economic impacts remain for some time after the initial disaster as confidence continues to wane, perishable products are no longer fit for sale, businesses suffer, international relations are damaged and supply chains take considerable time to recover.
- The economic losses to sectors are in the range of £11.6 billion to £85.5 billion in the different variants of the scenario.
- The overall GDP impact of the attack amounts to a loss between £49 billion to £442 billion across the entire UK economy in the five years following the outage, when compared against baseline estimates for economic growth.

Source: https://www.jbs.cam.ac.uk/faculty-research/centres/centre-for-risk-studies/publications/space-and-technology/integrated-infrastructure-cyber-resiliency-in-society/

CYBERSECURITY

Chinese spy chips are found in hardware used by Apple, Amazon, Bloomberg says; Apple, AWS say no way

PUBLISHED THU, OCT 4 2018 • 6:15 AM EDT | UPDATED FRI, OCT 5 2018 • 7:36 PM EDT

Kate Fazzini
@KATEFAZZINI

Source: https://www.cnbc.com/2018/10/04/chinese-spy-chips-are-said-to-be-found-in-hardware-used-by-apple-amazon-apple-denies-the-bloomberg-businessweek-report.html

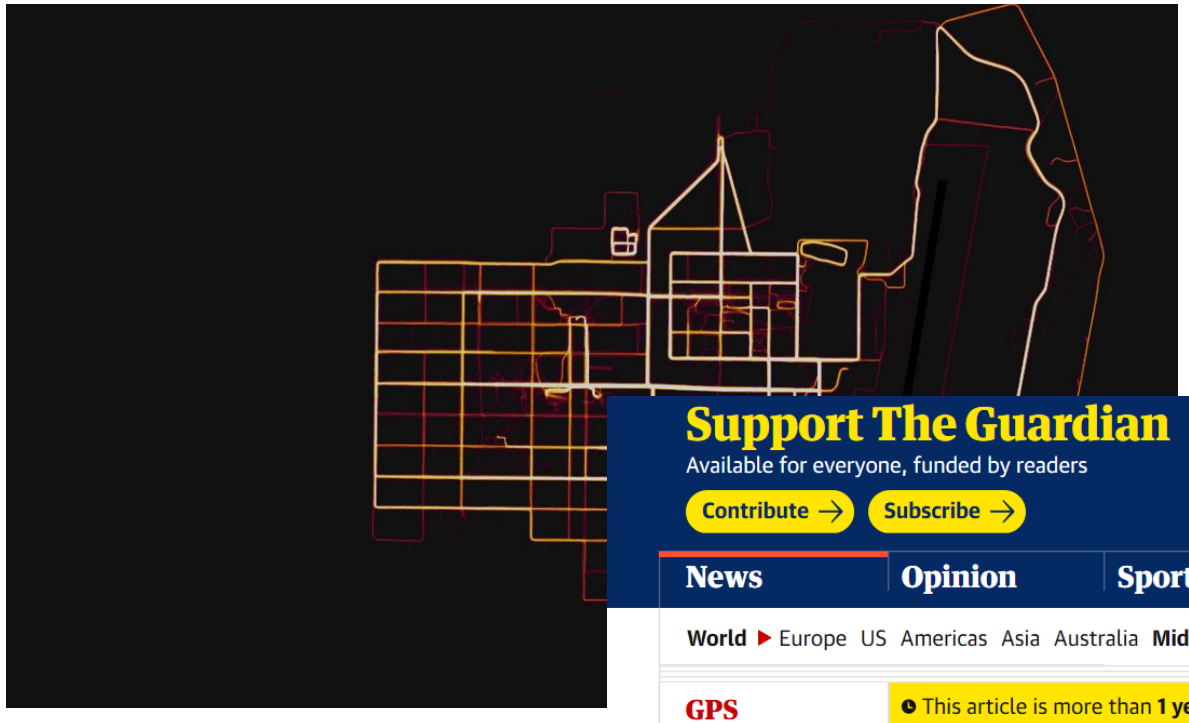
Security Notes from All Over: Coca-Cola and the NSA

Coca-Cola has a new contest. Hidden inside 100 cans of Coke there's a SIM card, GPS transmitter, and a microphone. The winners activate the Coke can by pressing a button, which will call a central monitoring facility. Then Coke tracks the winners down using the GPS transmitter and surprises them with their prize.

NSA engineers drink Coke. Lots and lots of Coke. The possibility that an active microphone in a Coke can could be in one of the NSA's highly secure facilities is worth considering. A reasonable threat analysis might look like this: "You know, the chances that one of these 100 cans out of hundreds of millions of cans ends up in our building is extremely small -- somewhere around 1 in 100,000 -- so it's not worth worrying about."

But the NSA's Information Staff Security Office) decreed differently: "It is important that ALL cans of Coca-Cola within our spaces be inspected. This includes cans already in our buildings and those being delivered on a daily basis. If you discover one of these cans, DO NOT activate it. Instead, you should alert your ISSO immediately and report the incident."

Source: https://www.schneier.com/crypto-gram/archives/2004/0715.html#8



Support The Guardian

Available for everyone, funded by readers

Contribute → Subscribe →

Search jobs | Sign in

News | Opinion | Sport | Culture | Lifestyle

World ▸ Europe US Americas Asia Australia **Middle East** Africa Inequality Cities Global development

GPS

This article is more than **1 year old**

Fitness tracking app Strava gives away location of secret US army bases

Data about exercise routes shared online by soldiers can be used to pinpoint overseas facilities

Latest: Strava suggests military users 'opt out' of heatmap as row deepens

Source: https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases

Hvad er ISO 27001?

ISO 27001 er en international standard til etablering af et ledelsessystem for informationssikkerhed. Standarden tager udgangspunkt i en risikobaseret tilgang til styring af informationssikkerhed.

ISO 27001 er valgt som statslig sikkerhedsstandard og har været obligatorisk at følge for statslige institutioner siden januar 2014. Standarden skulle være implementeret af myndighederne primo 2016.

ISO 27000-serien består af en række standarder med indbyrdes relationer. Nogle af disse standarder opstiller krav (normative), mens andre er vejledende i forhold til forskellige aspekter af implementering af et ledelsessystem for informationssikkerhed.

Baggrund

I DS484 var det forudbestemt, at en organisation skulle leve op til en række basale krav. Uanset virksomhed og uanset om kravene var relevante eller ej. Med beslutningen om at overgå til den internationale standard for informationssikkerhed, ISO 27001 er DS484 udfaset og ikke længere relevant for statslige institutioner.

Beslutningen om brug af ISO 27001 som standard for sikkerhedsstyringen i stedet for

Source: https://digst.dk/sikkerhed/iso-27001/hvad-er-iso-27001/

THE CYBER KILL CHAIN®

The New York Times

Stolen Data Is Tracked to Hacking at Lockheed

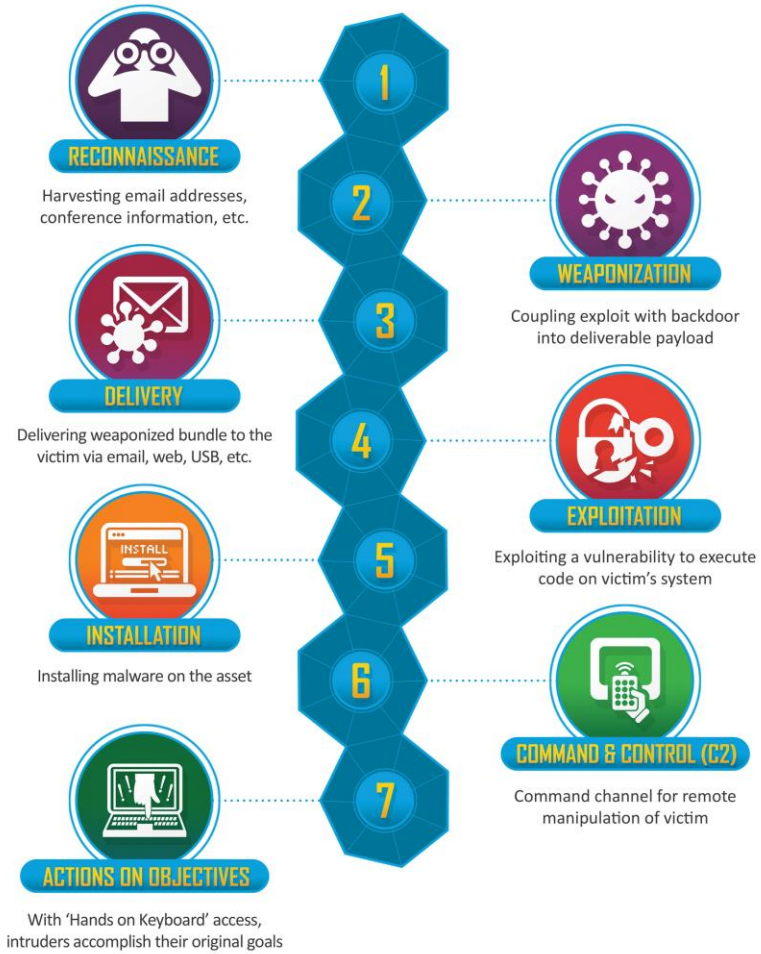
By **CHRISTOPHER DREW** JUNE 3, 2011

Lockheed Martin said Friday that it had proof that hackers breached its network two weeks ago partly by using data stolen from a vendor that supplies coded security tokens to tens of millions of computer users.

Lockheed's finding confirmed the fears of security experts about the safety of the SecurID tokens and heightened concerns that other companies or government agencies could be vulnerable to hacking attacks.

The tokens, which are used to protect remote access to computer networks, are sold by the RSA Security Division of the EMC Corporation. RSA officials said Friday that they accepted Lockheed's findings and were working with customers to offset the risks through other measures.

Source: https://www.nytimes.com/2011/06/04/technology/04security.html



Source: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Source: Center for Internet Security (https://cisecurity.org)

Implementation Group 1:

An IG1 organization is small to medium-sized with limited IT and cybersecurity expertise to dedicate toward protecting IT assets and personnel. The principal concern of these organizations is to keep the business operational as they have a limited tolerance for downtime. The sensitivity of the data that they are trying to protect is low and principally surrounds employee and financial information. However, there may be some small to medium-sized organizations that are responsible for protecting sensitive data and, therefore, will fall into a higher Group. Sub-Controls selected for IG1 should be implementable with limited cybersecurity expertise and aimed to thwart general, non-targeted attacks. These Sub-Controls will also typically be designed to work in conjunction with small or home office commercial-off-the-Shelf (COTS) hardware and software.

Implementation Group 2:

An IG2 organization employs individuals responsible for managing and protecting IT infrastructure. These organizations support multiple departments with differing risk profiles based on job function and mission. Small organizational units may have regulatory compliance burdens. IG2 organizations often store and process sensitive client or company information and can withstand short interruptions of service. A major concern is loss of public confidence if a breach occurs. Sub-Controls selected for IG2 help security teams cope with increased operational complexity. Some Sub-Controls will depend on enterprise-grade technology and specialized expertise to properly install and configure.

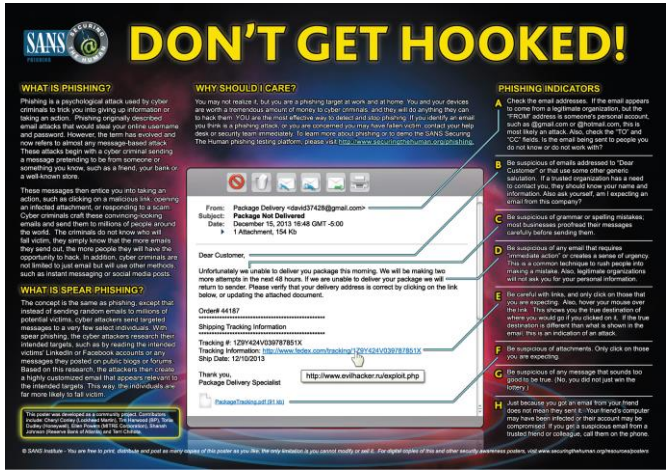
Implementation Group 3:

An IG3 organization employs security experts that specialize in the different facets of cybersecurity (e.g., risk management, penetration testing, application security). IG3 systems and data contain sensitive information or functions that are subject to regulatory and compliance oversight. A IG3 organization must address availability of services and the confidentiality and integrity of sensitive data. Successful attacks can cause significant harm to the public welfare. Sub-Controls selected for IG3 must abate targeted attacks from a sophisticated adversary and reduce the impact of zero-day attacks.

While this approach provides generalized guidance for prioritizing usage of the CIS Controls, this should not replace an organization's need to understand their own organizational risk posture. Organizations should still seek to conduct their own duty of care analysis and tailor their implementation of the CIS Controls based on what is appropriate and reasonable given their resources, mission, and risks. Using these types of methods, such as those described in CIS RAM, organizations of different Implementation Groups can make risk-informed decisions about which Sub-Controls in their Group they may not want to implement and which higher Group's they should strive for. The intention is to help organizations focus their efforts based on the resources they have available and integrate into any pre-existing risk management process.

Flere informationer!

https://securingthehuman.sans.org/media/resources/STH-Poster-CyberSecureHome-Print.pdf



https://securingthehuman.sans.org/resources/posters

OUCH! 2017 Newsletters

Jan | Feb | Mar | Apr | May | Jun | Jul | Aug | Sep | Oct | Nov | Dec | Full Archive

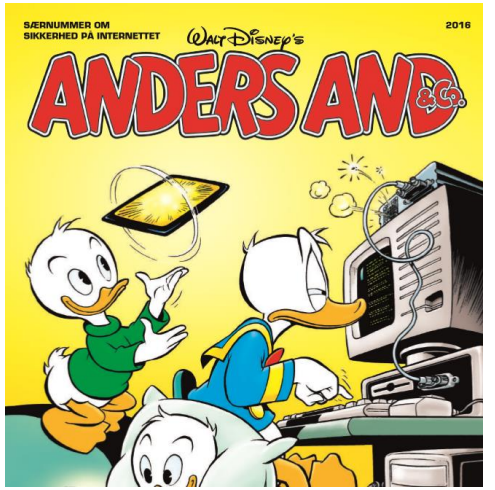
December 2017: Lock Down Your Login

- **English:** Lock Down Your Login - *SHA256*
- **English (epub):** Lock Down Your Login - *SHA256*
- **Arabic:** تأمين بيانات الدخول - *SHA256*
- **Bahasa Indonesia:** Amankan Akun Anda - *SHA256*
- **Bulgarian:** Заключете входа - *SHA256*
- **Chinese, Simplified:** 锁定登录 - *SHA256*
- **Chinese, Traditional:** 鎖定您的登錄 - *SHA256*
- **Chinese, Traditional (Taiwanese):** 鎖定登入 - *SHA256*
- **Danish:** Sådan sikrer du dit login - *SHA256*
- **Farsi:** صفحه ورود خود را قفل کنید - *SHA256*
- **Finnish:** Kaksivaiheinen tunnistautuminen - *SHA256*
- **French:** Verrouillez votre connexion - *SHA256*

https://securingthehuman.sans.org/resources/newsletters/ouch/2017

https://www.cert.dk/da/vejled

https://di.dk/Virksomhed/Produktion/IT/itsikkerhed/Pages/default.aspx



https://børneulykkesfonden.dk/laeringsmaterialer/hjemmet/tryg-pa-nettet-med-anders-and

- “There are only two types of companies: Those that have been hacked, and those who don’t know they have been hacked.”

Former CEO, CISCO John Chamber

Source: http://www.deloitte.co.uk/ers/cyber/companies.htm

WelcomeSecurity
Enabling value through IT security

TAK!

www.welcomesecurity.net

+45 2158 1410
Info@welcomesecurity.net