Make Technology Great Again

Michał „rysiek” Woźniak

rysiek@occrp.org

Everything is Broken

– Quinn Norton

https://medium.com/message/everything-is-broken-81e5f33a24e1

"Malicious Word Doc Uses ActiveX To Infect"

https://www.vmray.com/blog/malicious-word-doc-uses-activex-infect/

"Word Malware: OLE Exploited in Zero-Day Attack"

https://www.vadesecure.com/en/word-doc-malware/

"Dynamic Data Exchange was first introduced in 1987 with the release of Windows 2.0"

https://en.wikipedia.org/wiki/Dynamic_Data_Exchange

"Dynamic Data Exchange was first introduced in 1987 with the release of Windows 2.0"

https://en.wikipedia.org/wiki/Dynamic_Data_Exchange

"As part of the December 2017 Patch Tuesday, Microsoft has shipped an Office update that disables the DDE feature in Word applications, after several malware campaigns have abused this feature to install malware."

https://www.bleepingcomputer.com/news/microsoft/microsoft-disables-dde-feature-in-word-to-prevent-further-malware-attacks/

"Microsoft Office macro malware targets Macs"

https://blog.malwarebytes.com/cybercrime/2017/02/microsoft-office-macro-malware-targets-macs/

"Beware PowerSniff! Malware uses Word macros and PowerShell scripts"

https://www.grahamcluley.com/beware-powersniff-malware/

"20-year-old Windows bug lets printers install malware – patch now"

https://arstechnica.com/information-technology/2016/07/20-year-old-windows-bug-lets-printers-install-malware-patch-now/

"Outlook Bug Allowed [Cybercriminals] To Use .rtf Files To Steal Windows Passwords"

https://threatpost.com/outlook-bug-allowed-hackers-to-use-rtf-files-to-steal-windows-passwords/131169/

"Antivirus products riddled with security flaws, researcher says”

https://www.pcworld.com/article/2459760/antivirus-products-riddled-with-security-flaws-researcher-says.html

"Antivirus products riddled with security flaws, researcher says"

https://www.pcworld.com/article/2459760/antivirus-products-riddled-with-security-flaws-researcher-says.html

"Critical vulnerability found in Microsoft Malware Protection Engine"

https://www.cyberscoop.com/critical-vulnerability-hits-microsoft-malware-protection-engine/

"Dumb bug of the week: Apple's macOS reveals your encrypted drive's password in the hint box"

https://www.theregister.co.uk/2017/10/05/apple_patches_password_hint_bug_that_revealed_password/

"Dumb bug of the week: Apple's macOS reveals your encrypted drive's password in the hint box"

https://www.theregister.co.uk/2017/10/05/apple_patches_password_hint_bug_that_revealed_password/

„If macOS High Sierra shows your password instead of the password hint for an encrypted APFS volume"

https://support.apple.com/en-us/HT208168

"Anyone Can [Break Into] Macos High Sierra Just By Typing 'root'"

https://www.wired.com/story/macos-high-sierra-hack-root/

"How to crash any iPhone or iPad within WiFi range"

https://www.tripwire.com/state-of-security/security-data-protection/crash-iphone-wifi/

„This Text Message Can Crash, Reboot Any iPhone Instantly"

http://www.redmondpie.com/this-text-message-can-crash-reboot-any-iphone-instantly/

```
effective.
Power
لُلُصّبُلُلصّبُررً ॣ ॣh ॣ ॣ
冗
```

"[T]he CDs installed (…) software which provided a form of digital rights management (DRM) by modifying the operating system (…) and they created vulnerabilities"

https://en.wikipedia.org/wiki/Sony_BMG_copy_protection_rootkit_scandal

"Latest Adobe Flash vulnerability allowed [cybercriminals] to plant malware"

https://www.engadget.com/2017/10/16/adobe-flash-vulnerability-hackers-plant-malware/

"Java Malware Becomes a Cross-Platform Threat"

https://securityintelligence.com/news/java-malware-becomes-a-cross-platform-threat/

"Mirai then identifies vulnerable IoT devices using a table of more than 60 common factory default usernames and passwords, and logs into them to infect them with the Mirai malware."

https://en.wikipedia.org/wiki/Mirai_(malware)

"IoT worm can [break into] Philips Hue lightbulbs, spread across cities"

https://www.theregister.co.uk/2016/11/10/iot_worm_can_hack_philips_hue_lightbulbs_spread_across_cities/

"[Security Researchers] Remotely Kill A Jeep On The Highway – with Me In It"

https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

"[Security Researchers] Remotely Kill A Jeep On The Highway – with Me In It"

https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

„Vehicle manufacturers dismissed prior warnings about flawed security"

https://www.eff.org/deeplinks/2015/07/jeep-hack-shows-why-dmca-must-get-out-way-vehicle-security-research

"[R]esearchers have managed to [break into] and gain access to the self-aiming sniper rifle's computer system."

https://www.hackread.com/computer-controlled-sniper-rifle-hacked/

"[Cybercriminals] stole a casino's high-roller database through a thermometer in the lobby fish tank"

http://www.businessinsider.com/hackers-stole-a-casinos-database-through-a-thermometer-in-the-lobby-fish-tank-2018-4

"Drupalgeddon vulnerability (…) affected millions of websites back in 2014"

https://www.drop-guard.net/blog/drupalgeddon-panama-papers

„WordPress Sites Under Attack from New Zero-Day in WP Mobile Detector Plugin"

http://news.softpedia.com/news/wordpress-sites-under-attack-from-new-zero-day-in-wp-mobile-detector-plugin-504818.shtml

„Attacks Accelerate Against Joomla Zero Day"

https://threatpost.com/attacks-ramp-up-against-joomla-zero-day/115638/

"The Kremlin reportedly wants to create a state-operated center for issuing SSL certificates"

https://meduza.io/en/news/2016/02/15/the-kremlin-reportedly-wants-to-create-a-state-operated-center-for-issuing-ssl-certificates

„Google Bans China's Website Certificate Authority After Security Breach"

https://techcrunch.com/2015/04/01/google-cnnic/

„[A]fter it had become clear that a security breach had resulted in the fraudulent issuing of certificates, the Dutch government took over operational management of DigiNotar's systems."

https://en.wikipedia.org/wiki/DigiNotar

"Two researchers (...) have uncovered vulnerabilities that would allow an attacker to masquerade as any website"

https://www.wired.com/2009/07/kaminsky/

„The Heartbleed Bug (...) allows stealing the information protected (...) by the SSL/TLS encryption used to secure the Internet.”

http://heartbleed.com

"Equifax announced a cybercrime identity theft event potentially impacting approximately 145.5 million U.S. consumers."

https://en.wikipedia.org/wiki/Equifax

"Equifax announced a cybercrime identity theft event potentially impacting approximately 145.5 million U.S. consumers."

https://en.wikipedia.org/wiki/Equifax

„Equifax offered a website for consumers to learn whether they were victims of the breach. (…) [T]he website had many traits in common with a phishing website (...). These issues led Open DNS to classify it as a phishing site and block access.”

https://en.wikipedia.org/wiki/Equifax#Criticism

"Equifax announced a cybercrime identity theft event potentially impacting approximately 145.5 million U.S. consumers."

https://en.wikipedia.org/wiki/Equifax

„Equifax offered a website for consumers to learn whether they were victims of the breach. (…) [T]he website had many traits in common with a phishing website (...). These issues led Open DNS to classify it as a phishing site and block access."

https://en.wikipedia.org/wiki/Equifax#Criticism

„On October 12, 2017, Equifax's website was reported to have been offering visitors malware via drive-by download. The malware was disguised as an update for Adobe Flash."

https://en.wikipedia.org/wiki/Equifax#Website_malware

"Panera Bread website had leaked between 7 million and 37 million customer records (...). Panera was notified privately about the vulnerability in August 2017, but failed to fix it until after it was disclosed publicly eight months later"

https://en.wikipedia.org/wiki/Panera_Bread

"Panera Bread website had leaked between 7 million and 37 million customer records (...). Panera was notified privately about the vulnerability in August 2017, but failed to fix it until after it was disclosed publicly eight months later"

https://en.wikipedia.org/wiki/Panera_Bread

„Mike Gustavison, the Director of Information Security who I reported this to, used to work at Equifax from 2009–2013"

https://medium.com/@djhoulihan/no-panera-bread-doesnt-take-security-seriously-bf078027f815

Does T-Mobile Austria in fact store customers' passwords in clear text @tmobileat? @PWTooStrong @Telekom_hilft

@c_pellegrino

https://twitter.com/tmobileat/status/982187919061303296

Does T-Mobile Austria in fact store customers' passwords in clear text @tmobileat? @PWTooStrong @Telekom_hilft

@c_pellegrino

Hello Claudia! The customer service agents see the first four characters of your password. We store the whole password, because you need it for the login for http://mein.t-mobile.at ^andrea

@tmobileat

https://twitter.com/tmobileat/status/982187919061303296

Does T-Mobile Austria in fact store customers' passwords in clear text @tmobileat? @PWTooStrong @Telekom_hilft

@c_pellegrino

Hello Claudia! The customer service agents see the first four characters of your password. We store the whole password, because you need it for the login for http://mein.t-mobile.at ^andrea

@tmobileat

Well, what if your infrastructure gets breached and everyone's password is published in plaintext to the whole wide world?

@Korni22

https://twitter.com/tmobileat/status/982187919061303296

Does T-Mobile Austria in fact store customers' passwords in clear text @tmobileat? @PWTooStrong @Telekom_hilft

@c_pellegrino

Hello Claudia! The customer service agents see the first four characters of your password. We store the whole password, because you need it for the login for http://mein.t-mobile.at ^andrea

@tmobileat

Well, what if your infrastructure gets breached and everyone's password is published in plaintext to the whole wide world?

@Korni22

@Korni22 What if this doesn't happen because our security is amazingly good? ^Käthe

@tmobileat

https://twitter.com/tmobileat/status/982187919061303296

„WhatsApp Web Security Bug Puts 200 Million Users At Risk”

http://www.ibtimes.com/whatsapp-web-security-bug-puts-200-million-users-risk-2088418

"TL;DR: No, Telegram is not secure."

https://security.stackexchange.com/questions/49782/is-telegram-secure#49802

„Here we go again: Viber mobile messenger app leaves user data unencrypted”

https://nakedsecurity.sophos.com/2014/04/24/here-we-go-again-viber-mobile-messenger-app-leaves-user-data-unencrypted/

"Yahoo! later affirmed in October 2017 that all 3 billion of its user accounts were impacted."

https://en.wikipedia.org/wiki/Yahoo_data_breaches

"The Bangladesh Bank robbery (...) took place in February 2016, when instructions to fraudulently withdraw US$ 1 billion (...) were issued via the SWIFT network."

https://en.wikipedia.org/wiki/Bangladesh_Bank_robbery

"Paris Orly airport had to close temporarily last Saturday after the failure of a system running Windows 3.1 – yes, the operating system from 1992 – left it unable to operate in fog."

https://arstechnica.com/information-technology/2015/11/failed-windows-3-1-system-blamed-for-taking-out-paris-airport/

US CERT budget: **$93mln**

https://en.wikipedia.org/wiki/United_States_Computer_Emergency_Readiness_Team

NSA budget (that we know of): **$10bn**

https://www.statista.com/statistics/283545/budget-of-the-us-national-security-agency/

US intelligence budget: **$57.7bn**

https://en.wikipedia.org/wiki/United_States_intelligence_budget

„Vault 7 is a series of documents that (…) that detail activities and capabilities of the [CIA] to perform electronic surveillance and cyber warfare.”

https://en.wikipedia.org/wiki/Vault_7

„The Shadow Brokers (TSB) is a hacker group who (…) published several leaks containing [cyberattack] tools from the [NSA], including several zero-day exploits.”

https://en.wikipedia.org/wiki/The_Shadow_Brokers

"EternalBlue is an exploit developed by the [NSA] according to testimony by former NSA employees. It was leaked by the Shadow Brokers"

https://en.wikipedia.org/wiki/EternalBlue

"EternalBlue is an exploit developed by the [NSA] according to testimony by former NSA employees. It was leaked by the Shadow Brokers"

https://en.wikipedia.org/wiki/EternalBlue

„The WannaCry ransomware attack (...) propagated through EternalBlue"

https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

„In June 2017, a new variant of Petya was used for a global cyberattack, primarily targeting Ukraine. The new variant propagates via the EternalBlue exploit"

ttps://en.wikipedia.org/wiki/Petya_(malware)

China: Scarlet Mimic, C0d0so, SVCMONDR, Big Panda, Electric Panda, Eloquent Panda, Pale Panda, Sabre Panda, Spicy Panda, Hammer Panda, Wisp Team, Mana Team, TEMP.Zhenbao, SPIVY, Mofang, PassCV, DragonOK, Group 27, Tonto Team, TA459, Tick, Lucky Cat, TEMP.Periscope, BARIUM, LEAD

Russia: Sofacy, APT 29, Turla Group , Energetic Bear, Sandworm, Anunak, FIN7, Inception Framework, TeamSpy Crew, BuhTrap, Carberb, FSB 16th & 18th Centers, Cyber Berkut, WhiteBear, GRU GTsST

North Korea: Lazarus Group, APT 37, Bluenoroff, Andariel, Kimsuki, NoName, OnionDog, TEMP.Hermit

Iran: Cutting Kitten, Shamoon, Clever Kitten, Madi, Cyber fighters of Izz Ad-Din Al Qassam, Chafer, Cadelle, Prince of Persia, Sima, Oilrig, CopyKittens, Charming Kitten, Greenbug , Magic Hound, Rocket Kitten, ITSecTeam, MuddyWater, Mabna Institute

Israel: Unit 8200, Duqu Group, SunFlower

NATO: Equation Group, Snowglobe, Slingshot

Middle East: Molerats, AridViper, Volatile Cedar, Syrian Electronic Army (SEA), Cyber Caliphate Army (CCA), Ghost Jackal, Corsair Jackal, Extreme Jackal, Dark Caracal

Others: Corsair Jackal, The Mask, El Machete, Patchwork, Hellsing APT, Wild Neutron, Sykipot , Platinum, Magnetic Spider, Danti, SVCMONDR, Transparent Tribe, Singing Spider, Union Spider, Andromeda Spider, Dextorous Spider, APT 32, BlackOasis, NEODYMIUM, PROMETHIUM, Boson Spider, Carbon Spider, Hound Spider, Indrik Spider, Mimic Spider, Pizzo Spider, Shark Spider, Static Spider, Wicked Spider, Wold Spider, Zombie Spider, Cobalt Spider, Overlord Spider, Bamboo Spider, Monty Spider, Wizard Spider, Curious Jackal, Extreme Jackal, Gekko Jackal, Shifty Jackal, Dundeon Spider, Mummy Spider, Skeleton Spider, Mythic Leopard

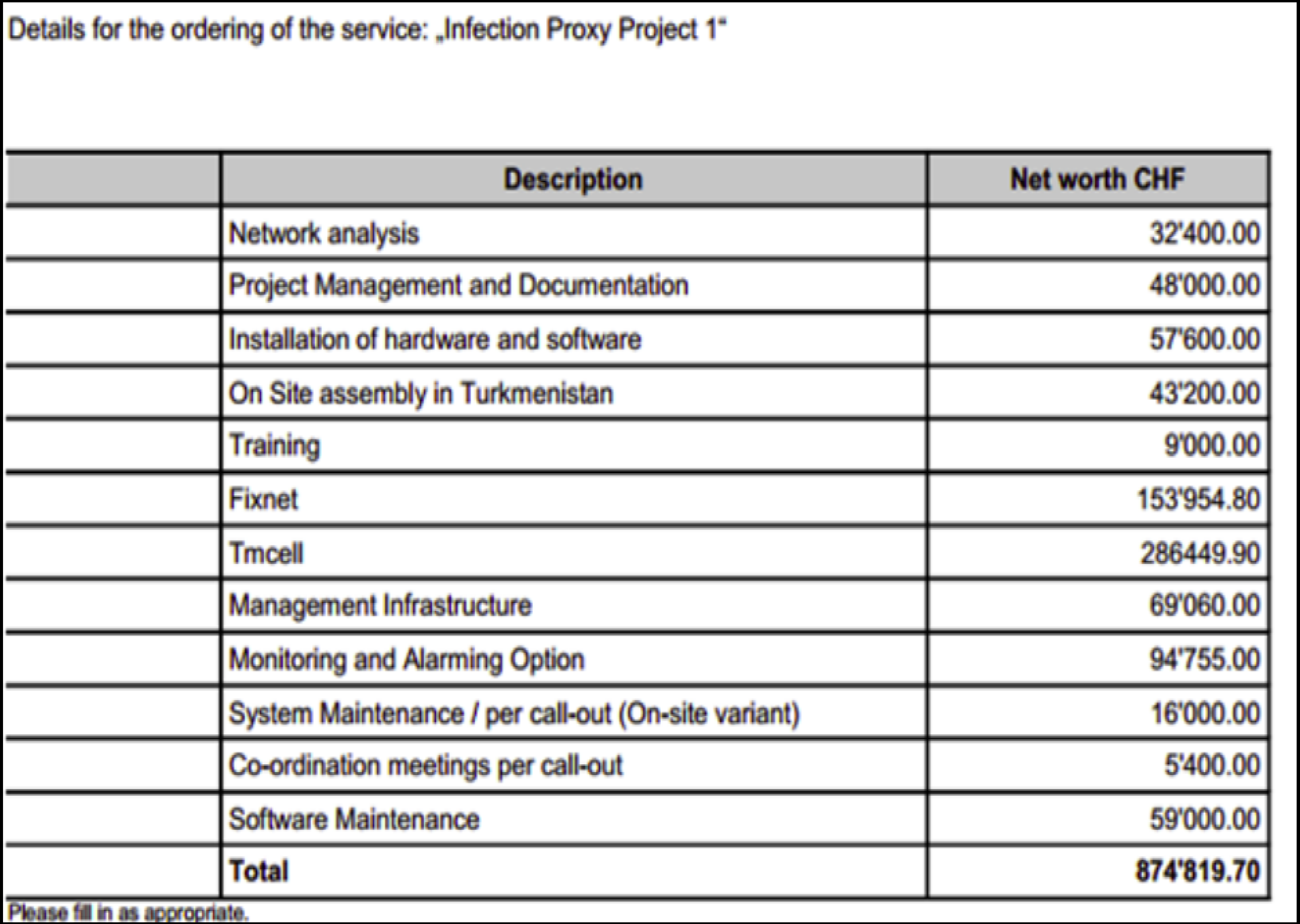
https://docs.google.com/spreadsheets/d/1H9_xaxQHpWaa4O_Son4Gx0YOIzlcBWMsdvePFX68EKU/edit

„Gamma Group was [broken into] and a 40 Gb dump of information was released detailing Gamma's client lists, price lists, source code, (…) and much more.”

https://en.wikipedia.org/wiki/Gamma_Group

„[T]he Twitter account of the company was compromised (...) and provided links to over 400 gigabytes of data, including alleged internal e-mails, invoices, and source code”

https://en.wikipedia.org/wiki/Hacking_Team#2015_data_breach



Details for the ordering of the service: „Infection Proxy Project 1"

	Description	Net worth CHF
	Network analysis	32'400.00
	Project Management and Documentation	48'000.00
	Installation of hardware and software	57'600.00
	On Site assembly in Turkmenistan	43'200.00
	Training	9'000.00
	Fixnet	153'954.80
	Tmcell	286449.90
	Management Infrastructure	69'060.00
	Monitoring and Alarming Option	94'755.00
	System Maintenance / per call-out (On-site variant)	16'000.00
	Co-ordination meetings per call-out	5'400.00
	Software Maintenance	59'000.00
	Total	**874'819.70**

Please fill in as appropriate.

„Meltdown and Spectre: Every modern processor has unfixable security flaws”

https://arstechnica.com/gadgets/2018/01/meltdown-and-spectre-every-modern-processor-has-unfixable-security-flaws/

„Meltdown and Spectre: Every modern processor has unfixable security flaws”

https://arstechnica.com/gadgets/2018/01/meltdown-and-spectre-every-modern-processor-has-unfixable-security-flaws/

„Meltdown, Spectre Can Be Exploited Through Your Browser”

http://www.tomshardware.com/news/meltdown-spectre-exploit-browser-javascript,36221.html

„Listen, when you get home tonight you're going to be confronted by the instinct to drink alone.

Trust that instinct.
Manage the pain.
Don't try to be a hero."

– Toby Ziegler, „The West Wing"

There is barely any engineering
in „software engineering”.

How to fix it?

- Fix the development process
- Dismantle vendor lock-in
- It's the Education, Stupid!
- Incentives!

Fix the development process

- Reproducible builds
- LANGSEC
- Coordinated Disclosure
- Etc, etc

Fight vendor lock-in

- Open Standards
- Open Protocols

Insecurity as a Business Model

- Companies focus on features, not security
- Because that's what brings users, and locks them to a platform
- Making it harder for them to switch to more secure alternatives
- Rinse, repeat

Insecurity as a Business Model

- Microsoft introduces non-standard „features”, which turn out to be exploitable
- For decades people are being exploited, but can't move
- Microsoft sells more software
- Rinse, repeat

Insecurity as a Business Model

- Intel introduces speculative execution, which turns out to be exploitable
- Software fix creates 20-30% performance drop
- Intel sells more CPUs
- Rinse, repeat

Insecurity as a Business Model

- Facebook creates a walled-garden social network, which turns out to be exploitable
- Millions of users' data is siphoned out, but people can't move
- Facebook sells more ads
- Rinse, repeat

Fight vendor lock-in

- Mozilla Filrefox breaks Internet Explorer's monopoly
- Actual standards are adopted across the web, competition becomes possible
- Huge step-up in security across all browsers
- Rinse, repeat, please!

It's the Education, Stupid!

- Teach more than one OS, more than one office suite
- InfoSec, OpSec in schools!
- Media Education instead of Computer Science

We need to change the whole incentive structure in software and hardware engineering.

Incentives!

- Regulate the Tech Industry
- Fix „cybersecurity agencies” and the surveillance industry

Regulate the Tech Industry

- Open standards, open protocols!
- Warranty, Liability
- „Best before” date on hardware
- Labels akin to food safety labels?
- Mandatory update support
- Release code, or remain liable

Fix „cybersecurity agencies"

- Focus on defence
- Help fix bugs, not hoard exploits!
- Liability

Fix the surveillance industry

- Control export and sales as weapons
- Explicit regulation about deployment
- Effective enforcement

Do not, under any circumstances:

- Ban or back-door encryption
  https://cointelegraph.com/news/france-and-germany-want-eu-to-ban-end-to-end-encryption
- Censor the Internet
  https://en.wikipedia.org/wiki/Internet_censorship_in_the_United_Kingdom
- Prosecute security researchers
  https://en.wikipedia.org/wiki/Weev#AT&T_data_breach
- Cripple security research to protect copyright
  https://www.eff.org/deeplinks/2015/07/jeep-hack-shows-why-dmca-must-get-out-way-vehicle-security-research

"EU seeks to outlaw 'backdoors' in new data privacy proposals"

https://www.theguardian.com/technology/2017/jun/19/eu-outlaw-backdoors-new-data-privacy-proposals-uk-government-encrypted-communications-whatsapp

Thank you!

rysiek@occrp.org