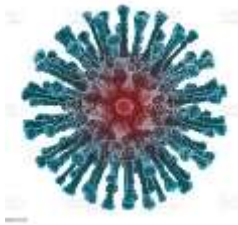
Sigurnosni aspekti rada od kuće

DOC.DOR.SC. IGOR TOMIČIĆ

FAKULTET ORGANIZACIJE I INFORMATIKE VARAŽDIN

Uvod: COVID-19 brojevi



3/2020 **phishing** 600%

4/2020 Google: blokiravao 18 000 000 **malware/phishing** covid-related emaila dnevno

3/2020 NordVPN: globalna upotreba njihovih **VPN** tehnologija povećana 165%

3/2020 Nizozemska: porast broja poslovnih **VPN** korisnika 240%

03-04/2020 broj **brute-force** napada povećan 400%

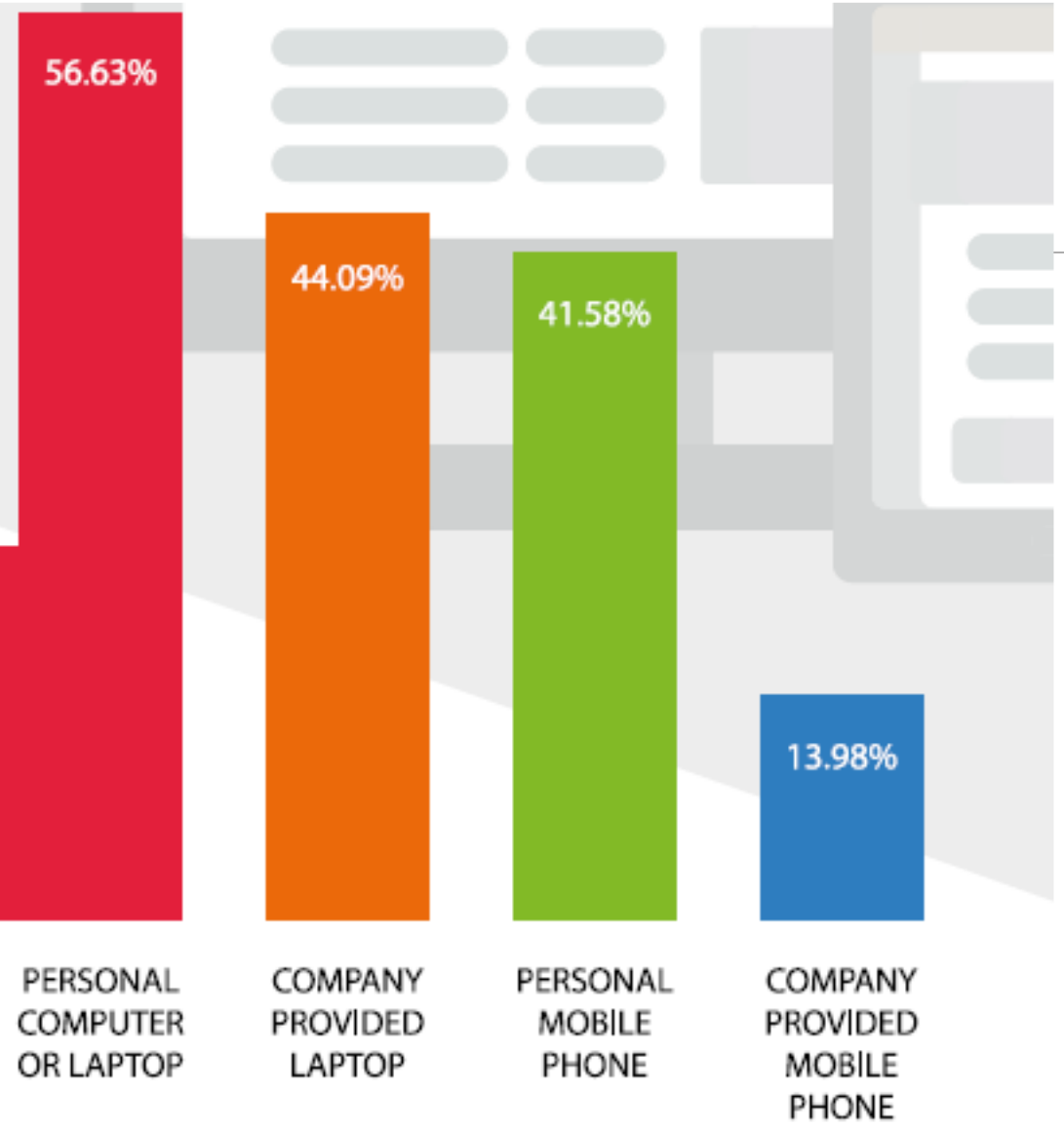
03/2020 vjerojatnost da korisnik klikne na **phishing link** i unese svoje login podatke
3 puta su veće nego prije COVID-19

03/2020 Broj upita za izraz "**how to remove a virus**" povećan je na tražilicama za 42%

03/2020 porast broj RDP portova otvorenih prema Internetu +1500000 od 01/2020

Q What devices are you using for working remotely during this period?

56% Use Their Personal Laptop or Computer for Working Remotely



https://www.morphisec.com/hubfs/eBooks_and_Whitepapers/Morphisec-2020-WFH-Employee-Cybersecurity-Threat-Index-FINAL.pdf

Uvod: COVID-19 brojevi

47% zaposlenika pali su na phishing prijevaru radi **distrakcija kod kuće**

Rast broja **ransomware-a** za 72% - 105%

IBM: više od 80% ispitanika rijetko je ili **nikada nije radilo od kuće** prije pandemije

Rad od kuće povećao je **prosječni data breach trošak** za $137 000

Broj nesigurnih RDP računala povećan više od 40%

- Povećanje broja brute force napada na **MS RDP**

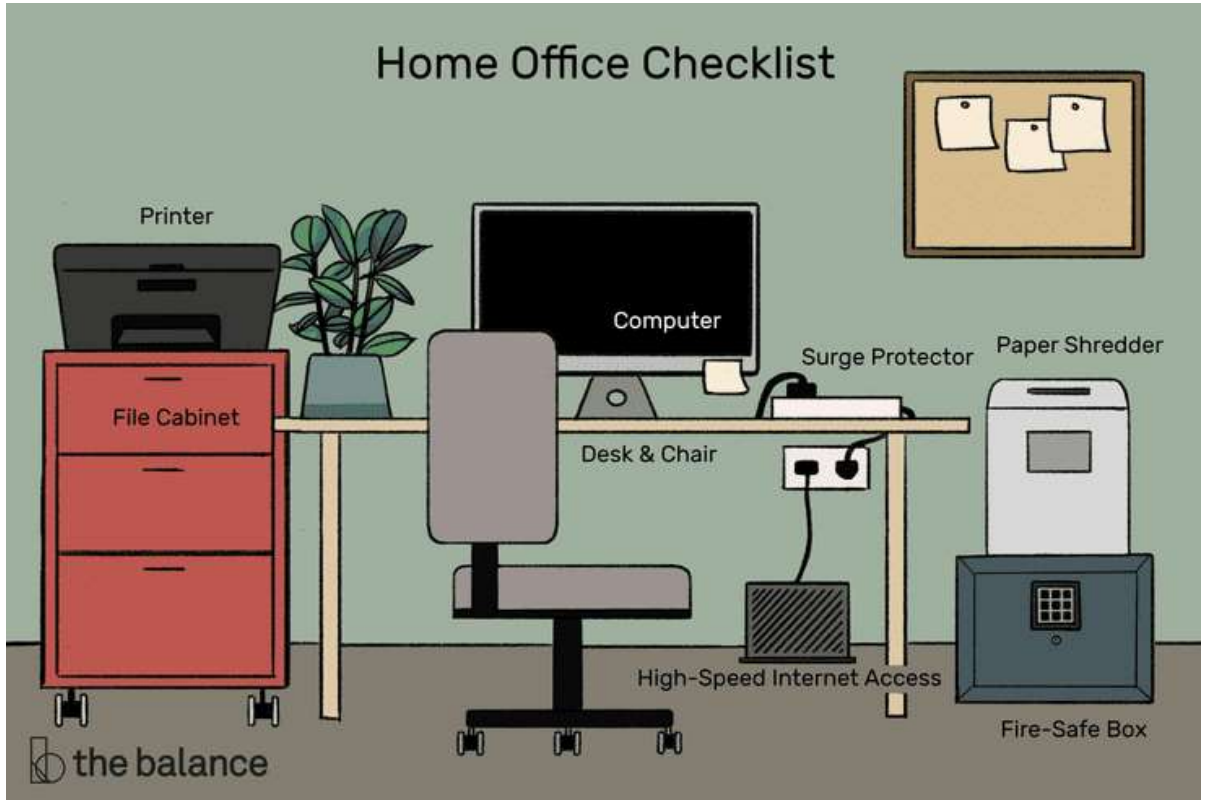
500 000 **Zoom korisničkih računa** je kompromitirano i prodavano na dark web forumu

- Cijena računa od $0.0020 … == **0.013 HRK**

Porast od 2000% malicioznih datoteka koje sadrže string "**zoom**"

Microsoft cloud servisi: 300 milijuna pokušaja lažnih logina svaki dan

Home Office: teorija



Home Office: stvarnost

Remote: generalni problemi

Rasuti IT sustavi, nedostatak centralne sigurnosti

Tehnička nepripremljenost kućnih ureda

Nepostojanje **sigurnosnih politika**

Ranjivosti **kućne mreže** i uređaja

privatno računalo (admin) == dijeljeno računalo == poslovno računalo

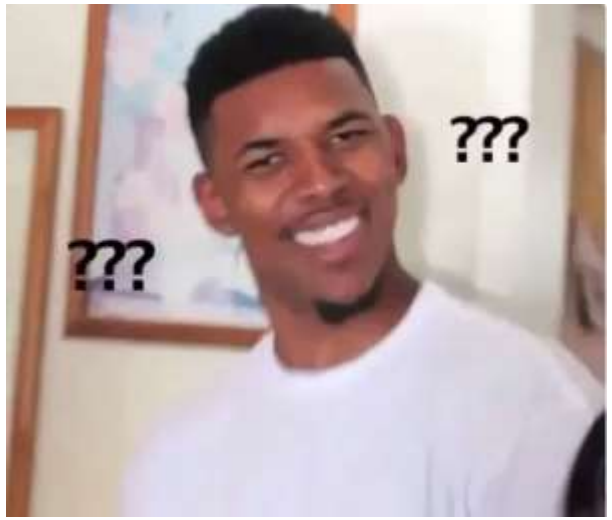
Needuciranost iz područja kibernetičke sigurnosti

Distrakcije

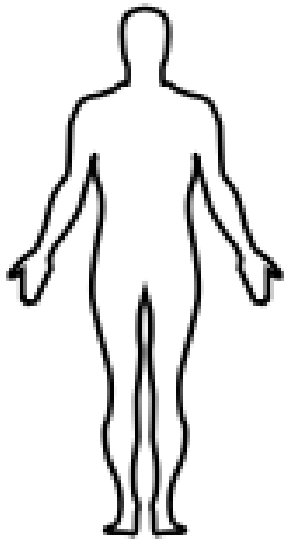
Umanjeni psihološki **obrambeni mehanizmi**

Remote: UBA?

User Behavior Analytics be like:



Ljudske ranjivosti u COVID doba



povećana razina stresa

anksioznost, panika

distrakcije

vremenska ograničenja

potreba za informacijama

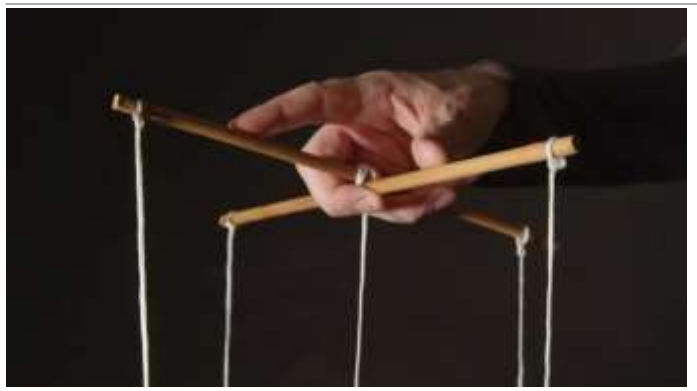
osobne promjene, zdravstvene poteškoće, poslovni pritisci

Ovisnosti (kockanje, igrice, pornografija, …)

masovni traumatični događaji na svjetskoj razini

…

Socijalni inžinjering



Principi utjecaja

(Robert B. Cialdini)

Uzajamnost

Obveza i dosljednost

Socijalna potvrda

Sviđanje

Autoritet

Oskudica

Socijalni inžinjering

komunikacijski modeli

Neverbalna komunikacija

profiliranje

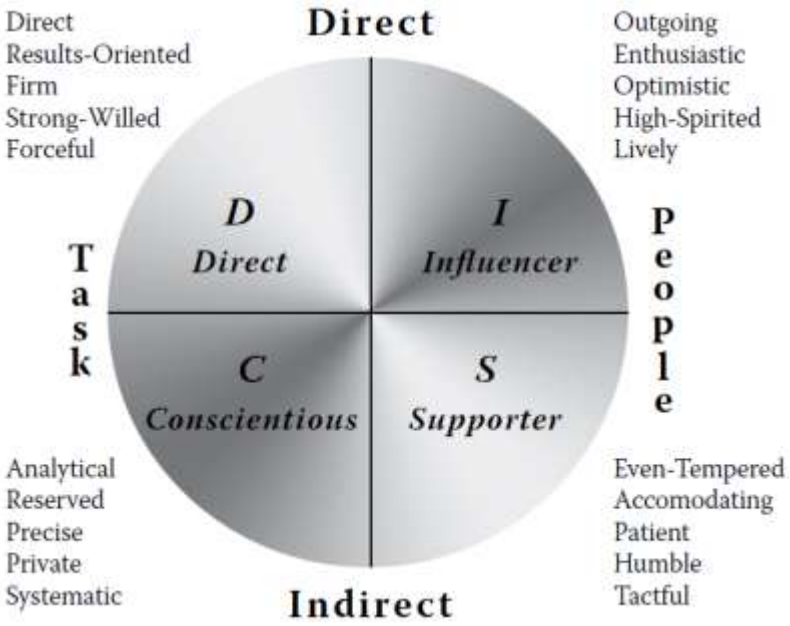
lažiranje identiteta

OSINT (*open source intelligence*)

stvaranje umjetnog konteksta (pretexting)

Manipulacija

- amigdala, procesiranje informacija, utjecaj emocija
- oxytocin, dopamin



Phishing

Naglasak na **proizvodima visoke potražnje**

- jeftine maske, cjepiva, testovi, dezinficijensi

Impersoniranje javnih autoriteta i organizacija

Korištenje ukradenih lozinki starih accountova

- Sextorsion

Hi, I know one of your passwords is: [redacted]

Your computer was infected with my private malware, your browser wasn't updated / patched, in such case it's enough to just visit some website where my iframe is placed to get automatically infected, if you want to find out more - Google: "Drive-by exploit".
My malware gave me full access to all your accounts (see password above), full control over your computer and it also was possible to spy on you over your webcam.

I collected all your private data and I RECORDED YOU (through your webcam) SATISFYING YOURSELF!

After that I removed my malware to not leave any traces and this email(s) was sent from some hacked server.

Phishing

Pogodni faktori za oportunističke napadače:

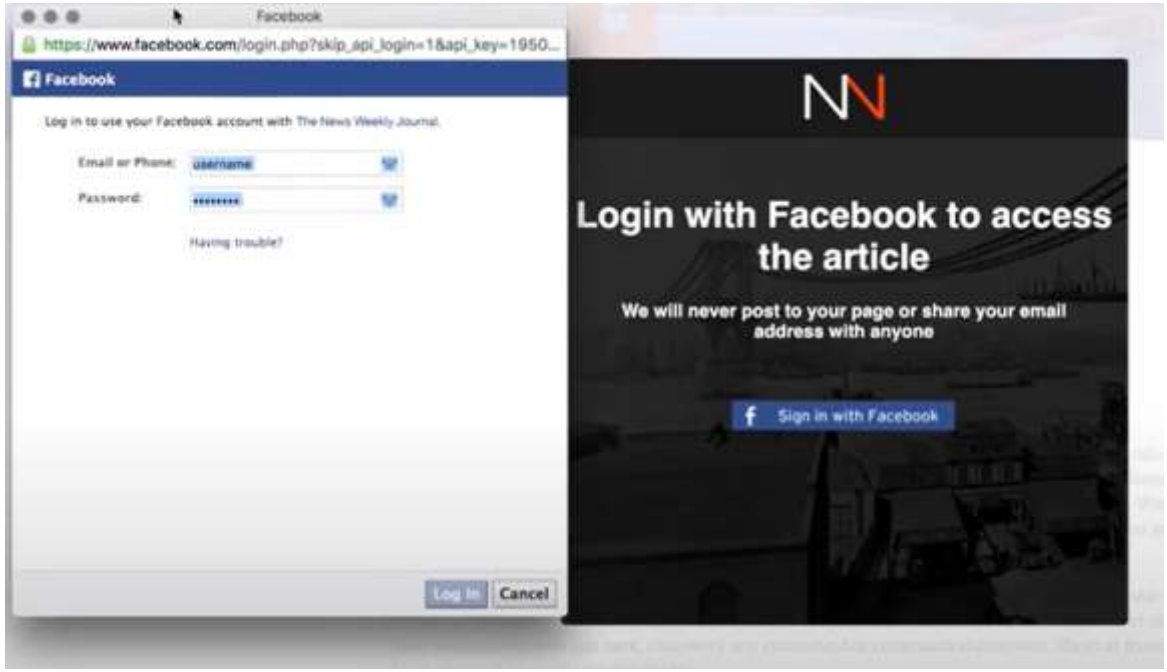
prirodne nepogode, krize ili značajni javni događaji

- 2005 (**uragan Katrina**): tisuće lažnih web sajtova za humanitarne donacije; email prijevare traže osobne podatke za isplate subvencija, …
- 2016 (**potresi u Japanu i Ekvadoru**)
- 2017 (**uragan Harvey**)
- 2020 (**požari u Australiji**)
- 2020 (**COVID-19)**
- …

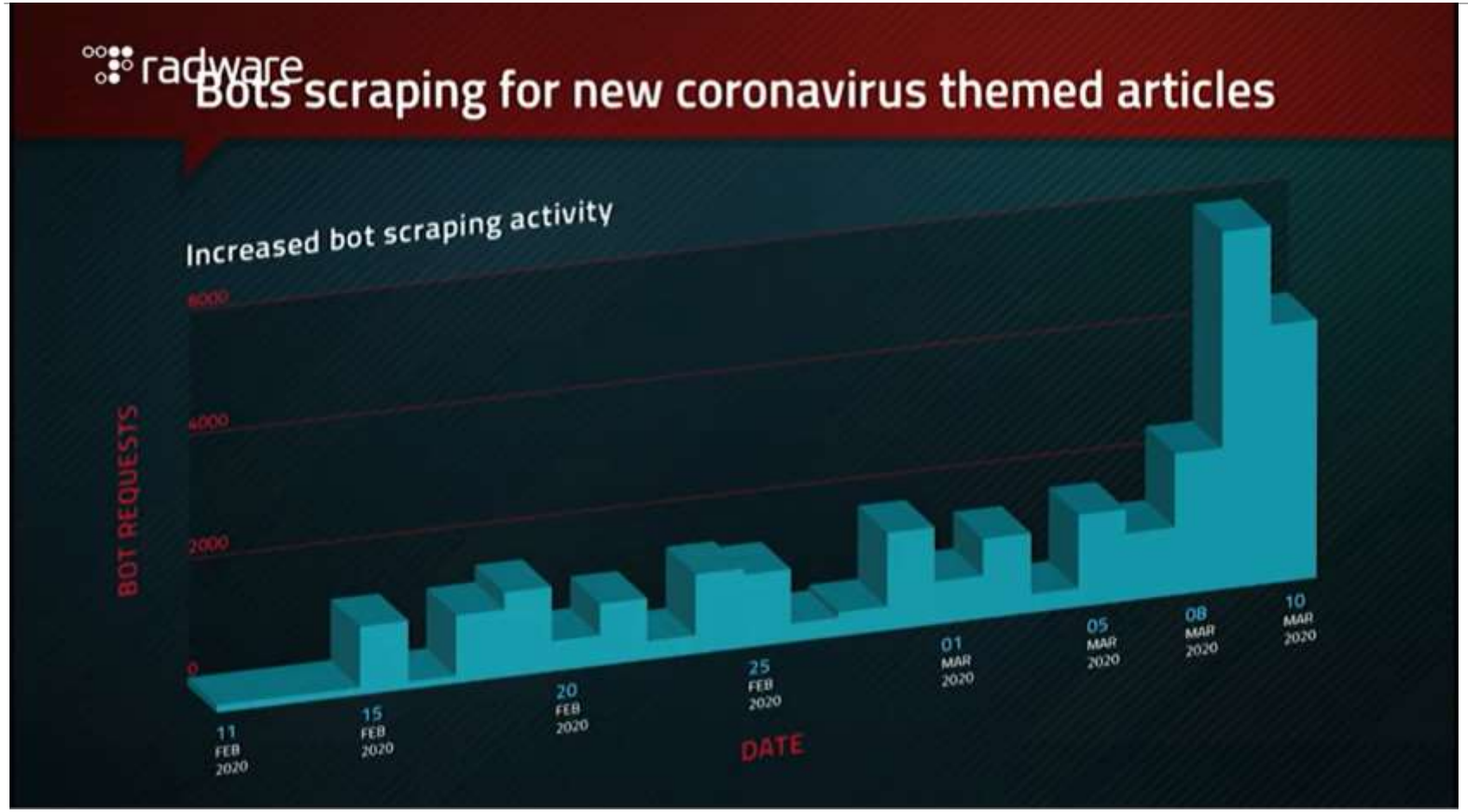
Phishing: samo za “naivne”?

SSO

https://youtu.be/nq1gnvYC144



Scraping


radware
Bots scraping for new coronavirus themed articles
Increased bot scraping activity
BOT REQUESTS
8000
4000
2000
0
11 FEB 2020
15 FEB 2020
20 FEB 2020
25 FEB 2020
01 MAR 2020
05 MAR 2020
08 MAR 2020
10 MAR 2020
DATE

How Secure Is Skype and Other Video Conferencing Tools?

Think your video conferencing software is secure? Here's how Skype, Zoom, Webex, and others have been hit by vulnerabilities.

BY GEORGINA TORBET

Vulnerabilities in Conferencing Tools: Much Ado about Something or g?

remote access | video conferencing security | 10,942 people reacted

king to family members who live far

of the software used for

A Discussion of Videoconferencing Security Vulnerabilities

Technical Services Reference

Abstract

This reference discusses the reasons why an organization should use encryption to protect their

Video Conferencing Vulnerabilities

While software has become extremely popular, business owners should be aware of the dangers and develop best practices for security

Zoom CVEs

HOME » CVE » SEARCH RESULTS

Search Results

There are **60** CVE entries that match your search.

Name	Description
CVE-2020-6767	A vulnerability related to Dynamic-link Library ('DLL') loading in the Zoom Sharing Service would allow an attacker who had local access to a machine on which the service was running with elevated privileges to elevate their system privileges as well through use of a malicious DLL. Zoom addressed this issue, which only applies to Windows users, in the 5.0.4 client release.
CVE-2020-6110	An exploitable partial path traversal vulnerability exists in the way Zoom Client version 4.6.10 processes messages including shared code snippets. A specially crafted chat message can cause an arbitrary binary planting which could be abused to achieve arbitrary code execution. An attacker needs to send a specially crafted message to a target user or a group to trigger the vulnerability. For the most severe effect, target user interaction is requ
CVE-2020-6109	An exploitable path traversal vulnerability exists in the Zoom client, version 4.6.10 processes messages including animated GIFs. A specially crafted chat message can cause an arbitrary file write, which could potentially be abused to achieve arbitrary code execution. An attacker needs to send a specially crafted message to a target user or a group to exploit this vulnerability.
CVE-2020-11877	** DISPUTED ** aomsat.exe in Zoom Client for Meetings 4.6.11 uses 34334234232232349 as the Initialization Vector (IV) for AES-256 CBC encryption. NOTE: the vendor states that this IV is used only within unreachable code.
CVE-2020-11878	** DISPUTED ** aomsat.exe in Zoom Client for Meetings 4.6.11 uses the SHA-256 hash of 0133433234334fdsfdsf3242 for initialization of an OpenSSL EVP AES-256 CBC context. NOTE: the vendor states that this initialization only occurs within unreachable code.
CVE-2020-11308	Zoom Client for Meetings through 4.6.9 uses the ECB mode of AES for video and audio encryption. Within a meeting, all participants use a single 128-bit key.
CVE-2020-11478	Zoom Client for Meetings through 4.6.8 on macOS has the disable-library-validation entitlement, which allows a local process (with the user's privileges) to obtain unprompted microphone and camera access by loading a crafted library and thereby inheriting Zoom Client's microphone and camera access.
CVE-2020-11469	Zoom Client for Meetings through 4.6.8 on macOS copies runwithroot to a user-writable temporary directory during installation, which allows a local process (with the user's privileges) to obtain root access by replacing runwithroot.
CVE-2020-11442	The Zoom IT installer for Windows (ZoomInstallerFull.msi) prior to version 4.6.10 deletes files located in %APPDATA%\Zoom before installing an updated version of the client. Standard users are able to write to this directory, and can write links to other directories on the machine. As the installer runs with SYSTEM privileges and follows these links, a user can cause the installer to delete files that otherwise cannot be deleted by the user.
CVE-2019-18632	A privilege escalation vulnerability in ZOOM Call Recording 6.3.1 allows an user account (i.e., the account under which the program runs - by default, the callrec account) to elevate privileges to root by abusing the callrec-re@.service. The callrec-re@.service starts the /opt/callrec/bin/re binary with root privileges, and this binary is owned by callrec. It can be replaced by a Trojan horse.
CVE-2019-18233	ZOOM International Call Recording 6.3.1 suffers from multiple authenticated stored XSS vulnerabilities via the phoneNumber field in the (1) User Edit or (2) User Add form, (3) name field in the Role Add form, (4) name or number field in the Edit Group form, (5) tagKey or tagValue field in the Recording Rules Configuration, or (6) txt_69735::/VernalAddress/value or txt_75767::/VernalFrom/value field in callrec/config.
CVE-2019-16272	DTEN D5 and D7 before 1.3.4 devices allow unauthenticated root shell access through Android Debug Bridge (adb), leading to arbitrary code execution and system administration. Also, this provides a covert ability to capture screen data from the Zoom Client on Windows by executing commands on the Android OS.
CVE-2019-13567	The Zoom Client before 4.4.53932.0709 on macOS allows remote code execution, a different vulnerability than CVE-2019-13450. If the ZoomOpener daemon (aka the hidden web server) is running, but the Zoom Client is not installed or can't be opened, an attacker can remotely execute code with a maliciously crafted launch URL. NOTE: ZoomOpener is removed by the Apple Malware Removal Tool (MRT) if this tool is enabled and has the 2019
CVE-2019-13452	In the Zoom Client through 4.4.4 and RingCentral 7.0.136386.0112 on macOS, remote attackers can force a user to join a video call with the video camera active. This occurs because any web site can interact with the Zoom web server on localhost port (9421 or (9424. NOTE: a machine remains vulnerable if the Zoom Client was installed in the past and then uninstalled. Blocking exploitation requires additional steps, such as the ZDisableVide
CVE-2019-13449	In the Zoom Client before 4.4.2 on macOS, remote attackers can cause a denial of service (continual focus grabs) via a sequence of invalid launchAction: joinAconfno requests to localhost port (9421.
CVE-2019-2040	Zoom 5352 v5.0.0.EV devices allow remote attackers to discover credentials via iso.3.6.1.4.1.4491.2.4.1.1.8.1.1.0 and iso.3.6.1.4.1.4491.2.4.1.1.8.1.2.0 SNMP requests.
CVE-2018-15713	Zoom clients on Windows (before version 4.1.34814.1119), Mac OS (before version 4.1.34801.1116), and Linux (3.4.129706.0913 and below) are vulnerable to unauthorized message processing. A remote unauthenticated attacker can spoof UDP messages from a meeting attendee or Zoom server in order to invoke functionality in the target client. This allows the attacker to remove attendees from meetings, spoof messages from users, or hija
CVE-2018-1000518	wBF Image Zoom version 1.32 contains a Incorrect Access Control vulnerability in AJAX settings that can result in allows anybody to cause denial of service. This attack appears to be exploitable via Can be triggered intentionally (or unintentionally via CSRF) by any logged in user. This vulnerability appears to have been fixed in 1.34.
CVE-2017-15048	The ZoomLauncher binary in the Zoom client for Linux before 2.0.111900.1201 does not properly sanitize user input when constructing a shell command, which allows remote attackers to execute arbitrary code by leveraging the zoommtg:// scheme handler.
CVE-2017-15048	Stack-based buffer overflow in the ZoomLauncher binary in the Zoom client for Linux before 2.0.111900.1201 allows remote attackers to execute arbitrary code by leveraging the zoommtg:// scheme handler.
CVE-2017-14814	Boston Scientific ZOOM LATITUDE PRM Model 3130 uses a hard-coded cryptographic key to encrypt PHI prior to having it transferred to removable media. CVSS v3 base score: 4.6; CVSS vector string: AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N.
CVE-2017-14812	Boston Scientific ZOOM LATITUDE PRM Model 3120 does not encrypt PHI at rest. CVSS v3 base score: 4.6; CVSS vector string: AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N.
CVE-2016-6667	XSS issues were discovered in phpMyAdmin. This affects Zoom search (especially crafted column content can be used to trigger an XSS attack); GIS editor (certain fields in the graphical GIS editor are not properly escaped and can be used to trigger an XSS attack); Relation view; the following Transformations: Formatted, Imagelink, JPEG: Upload, RegexValidation, JPEG inline, PNG inline, and transformation wrapper; XML export; Modularized exp and 4.0.x versions (prior to 4.0.10.17) are affected.
CVE-2016-5703	Multiple cross-site scripting (XSS) vulnerabilities in phpMyAdmin 4.0.x before 4.0.10.16, 4.4.x before 4.4.15.7, and 4.5.x before 4.5.3 allow remote attackers to inject arbitrary web script or HTML via vectors involving (1) a crafted table name that is mishandled during privilege checking in table_row.phtml, (2) a crafted mysqli log_bin directive that is mishandled in log_selector.phtml, (3) the Transformation implementation, (4) AJAX error hand
CVE-2016-5260	Multiple cross-site scripting (XSS) vulnerabilities in phpMyAdmin 4.0.x before 4.0.10.15, 4.4.x before 4.4.15.5, and 4.5.x before 4.5.1.1 allow remote attackers to inject arbitrary web script or HTML via (1) a crafted Host HTTP header, related to libraries/Config.class.php; (2) crafted JSON data, related to file_echo.php; (3) a crafted SQL query, related to js/functions.js; (4) the initial parameter to libraries/server_privileges.lib.php in the user acc
CVE-2016-10094	uhttpd through 2.10 does not block multitouch events. Consequently, an attacker at a locked screen can send input to (and thus control) various programs such as Chromium via events such as pan scrolling, "pinch and zoom" gestures, or even regular mouse clicks (by depressing the touchpad once and then clicking with a different finger).
CVE-2016-2069	Summer Baby Zoom Wifi Monitor & Internet Viewing System allows remote attackers to gain privileges via manual entry of a Settings URL.
CVE-2016-2068	Summer Baby Zoom Wifi Monitor & Internet Viewing System allows remote attackers to bypass authentication, related to the MyStrapCam web service.
CVE-2015-2755	Multiple cross-site request forgery (CSRF) vulnerabilities in the AB Google Map Travel (AB-MAP) plugin before 4.0 for WordPress allow remote attackers to hijack the authentication of administrators for requests that conduct cross-site scripting (XSS) attacks via the (1) lat (Latitude), (2) long (Longitude), (3) map_width, (4) map_height, or (5) zoom (Map Zoom) parameter in the ab_map_options page to wp-admin/admin.php.
CVE-2014-9084	Multiple cross-site scripting (XSS) vulnerabilities in deploy/designer/preview.php in the Digital Zoom Studio (DZS) Video Gallery plugin for WordPress allow remote attackers to inject arbitrary web script or HTML via the (1) swfloc or (2) designmd parameter.
CVE-2014-8958	Multiple cross-site scripting (XSS) vulnerabilities in phpMyAdmin 4.0.x before 4.0.10.6, 4.1.x before 4.1.14.7, and 4.2.x before 4.2.12 allow remote authenticated users to inject arbitrary web script or HTML via a crafted (1) database, (2) table, or (3) column name that is improperly handled during rendering of the table browse page; a crafted ENUM value that is improperly handled during rendering of the (4) table print view or (5) zoom searc
CVE-2014-7936	Use-after-free vulnerability in the ZoomBubbleView::Close function in browser/ui/views/location_bar/zoom_bubble_view.cc in the Views implementation in Google Chrome before 40.0.2214.91 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted document that triggers improper maintenance of a zoom bubble.
CVE-2014-5811	The ZOOM Cloud Meetings (aka us.zoom.videomeetings) application @7f3602038 for Android does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.
CVE-2014-3922	Multiple cross-site scripting (XSS) vulnerabilities in the Digital Zoom Studio (DZS) Video Gallery plugin for WordPress allow remote attackers to inject arbitrary web script or HTML via the logoLink parameter to (1) preview.swf, (2) preview_skin_rouge.swf, (3) preview_aldnars.swf, or (4) preview_skin_overlay.swf in deploy/.
CVE-2013-3260	Heap-based buffer overflow in INMATRIX Zoom Player before 8.7 beta 11 allows remote attackers to execute arbitrary code via a large biChUsed value in a BMP file.
CVE-2013-3258	Stack-based buffer overflow in INMATRIX Zoom Player before 8.7 beta 11 allows remote attackers to execute arbitrary code via a large biClrUsed value in a BMP file.
CVE-2011-4279	Moodle 2.0.x before 2.0.2 does not use the forcelogin/forceprofiles setting for course-profiles access control, which makes it easier for remote attackers to obtain potentially sensitive information via vectors involving use of a search engine, as demonstrated by the search functionality of Google, Yahoo!, Wikiseft Zoom, MSN, Yandex, and AltaVista.
CVE-2009-4474	SQL injection vulnerability in the Mike do Boer zoom (zom_zoom) component 2.0 for Mambo allows remote attackers to execute arbitrary SQL commands via the catid parameter to index.php.
CVE-2009-0670	Microsoft Internet Explorer 7, when XHTML strict mode is used, allows remote attackers to execute arbitrary code via the zoom style directive in conjunction with unspecified other directives in a malformed Cascading Style Sheets (CSS) stylesheet in a crafted HTML document, aka "CSS Memory Corruption Vulnerability."
CVE-2006-4833	Buffer overflow in the DjVu Activex Control 3.0 for Microsoft Office (DjVu_Activex_MSOffice.dll) allows remote attackers to execute arbitrary code via a long (1) ImageURL property, and possibly the (2) Mode, (3) Page, or (4) Zoom properties.
CVE-2007-6033	Buffer overflow in Zoom Player 6.50 beta 2 and earlier allows user-assisted remote attackers to execute arbitrary code via an HTTP link to a PLS file in a crafted ZPL file, which causes an overflow in Unicode handling when generating an error message.
CVE-2007-3568	SQL injection vulnerability in reply.php in VBZoom 1.12 allows remote attackers to execute arbitrary SQL commands via the UserID parameter to sub-join.php. NOTE: this may be the same as CVE-2006-3691.4.
CVE-2007-1982	Multiple PHP remote file inclusion vulnerabilities in the com_zoom 2.5 beta 2 and earlier module for Mambo allow remote attackers to execute arbitrary PHP code via a URL in the mosConfig_absolute_path parameter to (1) EXIF_Makernote.php or (2) EXIFinfo in classes/pbc/.
CVE-2007-1930	SQL injection vulnerability in index.php in the aktualnosci module in GrooBIF 1.00 and earlier allows remote attackers to execute arbitrary SQL commands via the zoom parameter, possibly related to home.php.
CVE-2006-5063	PHP remote file inclusion vulnerability in libs/phpmyvisites.php in ZoomStats 1.0.2 and earlier, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a URL in the GLOBALS[lib][dir][path] parameter.
CVE-2006-4854	Cross-site scripting (XSS) vulnerability in index.php in VBZoom allows remote attackers to inject arbitrary web script or HTML via the UserID parameter, a different vector than CVE-2006-1133 and CVE-2005-2441.
CVE-2006-3691	Multiple SQL injection vulnerabilities in VBZoom 1.11 and earlier allow remote attackers to execute arbitrary SQL commands via the UserID parameter to (1) ignore-om.php, (2) sendmail.php, (3) reply.php or (4) sub-join.php.
CVE-2006-3256	SQL injection vulnerability in message.php in VBZoom 1.11 and earlier allows remote attackers to execute arbitrary SQL commands via the UserID parameter.
CVE-2006-3238	Multiple SQL injection vulnerabilities in VBZoom 1.00 and earlier allow remote attackers to execute arbitrary SQL commands via the (1) MemberID parameter to rank.php, and the (2) QuranID parameter to ing.php.
CVE-2006-3142	SQL injection vulnerability in forum.php in VBZoom 1.11 allows remote attackers to execute arbitrary SQL commands via the MainID parameter.
CVE-2006-3006	SQL injection vulnerability in language.php in VBZoom 1.01 allows remote attackers to execute arbitrary SQL commands via the Action parameter.
CVE-2006-3021	Multiple SQL injection vulnerabilities in VBZoom 1.00 allow remote attackers to execute arbitrary SQL commands via the (1) QuranID, (2) ShowByQuranID, or (3) Action parameters to meaning.php.
CVE-2006-3004	Multiple SQL injection vulnerabilities in VBZoom 1.11 allow remote attackers to execute arbitrary SQL commands via the (1) subjectID or (2) MAINID parameters to (a) show.php or (3) MainID parameter to (b) subject.php.
CVE-2006-1133	Multiple cross-site scripting (XSS) vulnerabilities in vbzoom 1.11 allow remote attackers to inject arbitrary web script or HTML via the UserID parameter to (1) comment.php or (2) contact.php. NOTE: the profile.php/Username vector is already covered by CVE-2005-2441.
CVE-2006-1132	SQL injection vulnerability in show.php in vbzoom 1.11 allow remote attackers to execute arbitrary SQL commands via the MainID parameter. NOTE: the SubjectID vector is already covered by CVE-2005-4729.
CVE-2005-4729	SQL injection vulnerability in show.php in VBZoom Forum allows remote attackers to execute arbitrary SQL commands via the SubjectID parameter.
CVE-2005-3178	Buffer overflow in cloudimage 4.1 and earlier, and xli, might allow user-assisted attackers to execute arbitrary code via a long title name in a NIFF file, which triggers the overflow during (1) zoom, (2) reduce, or (3) rotate operations.
CVE-2005-1879	SQL injection vulnerability in index.php for zOOm Media Gallery 2.1.2 allows remote attackers to execute arbitrary SQL commands via the catid parameter.
CVE-2004-0809	Zoom X3 ADSL modem has a terminal running on port 334 that can be accessed using the default HTML management password, even if the password has been changed for the HTTP interface, which could allow remote attackers to gain unauthorized access.
CVE-2003-1488	Cross-site scripting (XSS) vulnerability in search.php for WEBSOFT Zoom Search Engine 2.0 Build 1018 and earlier allows remote attackers to inject arbitrary web script or HTML via the zoom_query parameter.

NSA vodič za odabir sigurnih konferencijskih i kolaboracijskih alata

Da li servis implementira **E2E enkripciju**?

Da li E2E enkripcija koristi snažne, poznate, i testabilne **enkripcijske primitive/standarde**?

Da li postoji podrška za **MFA**?

Da li korisnici mogu vidjeti i kontrolirati **tko se spaja** na sesije?

Da li proizvođač alata **dijeli podatke** sa trećim strankama ili partnerima?

Imaju li korisnici mogućnost **sigurnog brisanja podataka** iz servisa i repozitorija po potrebi (i sa klijentske i poslužiteljske strane)?

Je li **izvorni kod alata javno dostupan** (open source)?

Je li servis **FedRAMP**-approvan za službeno korištenje od strane vlade US?

Service	Basic Functionality	1 – E2E Encryption	2 – Testable Encryption	3 – MFA	4 – Invitation Controls	5 – Minimal 3rd Party Sharing	6 – Secure Deletion	7 – Public Source Code Shared	8 – Certified Service (FedRAMP / NIAP)
Cisco Webex®	a, b, c, d, e	Y[1]	Y	Y[12]	Y[1]	Y	Client – Y Server – N[3]	N	FedRAMP
Dust	a	Y	N[3]	N	Y	N	Client – Y Server – Y	N	None
Google G Suite™	a, b, c, d	N	Y	Y[1]	Y[1]	Y	Client – Y Server – Y[2]	N	FedRAMP
GoToMeeting®	a, b, c	Y[1]	Y	N	Y[1]	Y	Client – Y Server – N[3]	N	None
Mattermost™	a, b, c, e	Y	Y	Y[2]	Y	N	Client – Y Server – N	Y	FedRAMP
Microsoft Teams®	a, c, d, e	N	Y	Y	Y	Y	Client – Y[1] Server – Y[1]	N	FedRAMP
Signal®	a, b, d	Y	Y	Y	Y	Y	Client – Y Server – Y	Y	None
Skype for Business™	a, c, d, e	Y[4]	Y[4]	Y	Y	N	Client – Y Server – N[3]	N	None
Slack®	a, c, d, e	N	Y	Y	Y	N[3]	Client – N Server – N	N	FedRAMP
SMS Text	a, d	N	N	N	N	N	Client – Y Server – N	N	None
WhatsApp®	a, c, d	Y	Y	Y	Y	Y	Client – Y Server – Y	N	None
Wickr®	a, c, d, e	Y	Y	Y	Y	Y	Client – Y Server – Y	Y	None
Zoom®	a, b, c, e	Y[14]	Y	N	Y	Y	Client – Y Server – N[3]	N	FedRAMP

Legend: Y = Yes, N = No; (a) text chat, (b) voice conferencing, (c) video conferencing, (d) file sharing, (e) screen sharing.

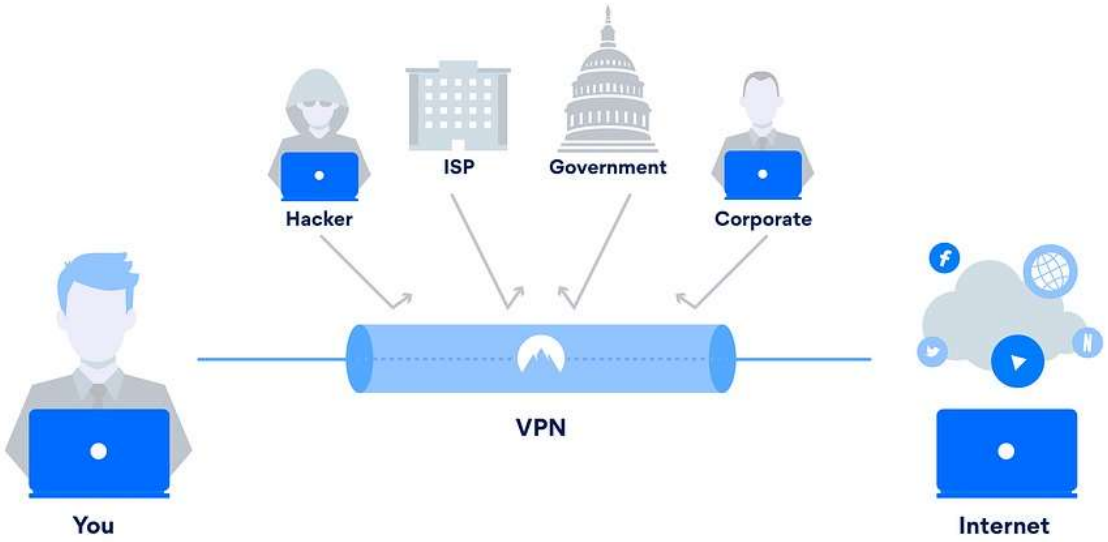
Virtualne privatne mreže

Osobni (personal) VPN

- Pristup geo-restricted servisima
- Sigurnosni sloj za nesigurne (wifi) mreže
- “Zasljepljivanje” ISPova

Poslovni (business, corporate) VPN

- Pristup resursima organizacije
- Isključivo za poslovnu upotrebu



Background check VPN servisa

- *Provjeriti ‘neutralna’ recenzijska web mjesta (CNET? Wirecutter?)*
- *Provjeriti neutralne grupe, forume (reddit)*

Information

Product Affected	Pulse Connect Secure, Pulse Policy Secure
Problem	Multiple vulnerabilities were discovered and have been resolved in Pulse Connect Secure (PCS) and Pulse Policy Secure (PPS). This includes an authentication by-pass vulnerability that can allow an unauthenticated user to perform a remote arbitrary file access on the Pulse Connect Secure gateway. This advisory also includes a remote code execution vulnerability that can allow an authenticated administrator to perform remote code execution on Pulse Connect Secure and Pulse Policy Secure gateways. Many of these vulnerabilities have a critical CVSS score and pose significant risk to your deployment. We strongly recommend to upgrade to the corresponding version with the fix as soon as possible. CVE have been requested and will be updated in the future.

Pulse Connect Secure

Zero Trust Secure Access from Any Device to Apps & Services in the Cloud and Data Center

DATASHEET

SSL VPN vs IPSEC VPN

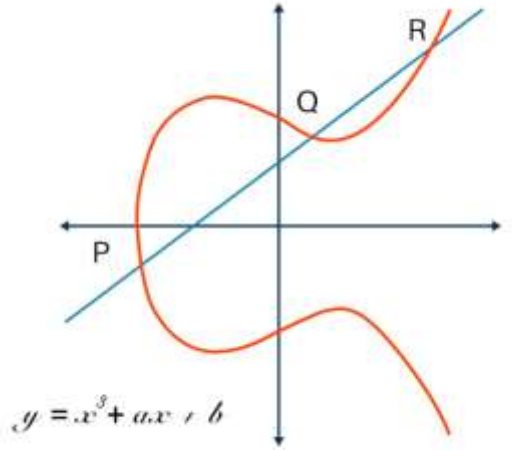
SSL VPN:

- Layer ~6 OSI (TLS)
- Jednostavniji za korištenje;
  jednostavniji client management
- Dostupan bez posebnog klijenta (web portal)
- Moguće koristiti samo web-based aplikacije out-of-the-box
  - Tuneliranje na određene aplikacije
    (ne mora biti network-wide pristup)
- Veća podložnost malware napadima
  (otvoreni TLS port)
- Bolje kretanje kroz firewallove (443)
- Bolja integracija za cloud-based organizacije

IPSEC VPN:

- Layer 3 OSI
- Robustan, dokazan, testiran
- Potreban konfigurirani klijent
- Lošije kretanje kroz firewallove
- Nakon logiranja, korisnik je punopravni član mreže (manje restrikcije)
  - Network user permissions za restrikcije
    / višestruke konekcije

VPN kripto



Na tržištu još uvijek zastarjeli kripto algoritmi poput
DES, 3DES, SHA-1 ili RSA sa malim ključevima

Ili vlastito razvijena *ultra-mega-ninja-bomba kripto rješenja*, koja se ne mogu testirati

Kripto algoritmi koji dolaze u obzir:

- Simetrična enkripcija: **AES**, Twofish, Camellia, ..
- Razmjena/generiranje ključeva: **ECDH**, RSA 2048, RSA 4096
- Hash: **SHA256**(+), SHA-3
- Perfect Forward Secrecy (ECDH**E**)

*NOTE: I jaki kripto algoritmi mogu se upropastiti **lošom implementacijom***

- *npr. generatori slučajnih brojeva*

VPN protokoli


PPTP (Point-to-Point Tunneling Protocol): 90te, brz, zastario, nesiguran

L2TP/IPSec (Layer Two Tunneling Protocol): star, ne nudi enkripciju out-of-the-box (potrebno upariti sa kripto protokolom - IPSec)

IKEv2/IPSec (Internet Key Exchange 2): obično korišten uz IPSec, noviji, razvijen od Cisco i Microsoft, često korišten u mobilnoj komunikaciji

- Snowden procurio info kojim se indicira da je NSA uspjela probiti/oslabjeti enkripciju

SSTP (Secure Socket Tunneling Protocol): koristi SSL/TLS, autor Microsoft, siguran, dobar za Win korisnike, nije transparentan

OpenVPN: dobra reputacija, siguran, open source, ali već pomalo star i kilav

Wireguard: novi, open source, GPLv2, bolje performance od IPsec i OpenVPN, UDP only

- Linus Torvalds: "work of art"

Besplatni VPN?

"If you don't pay for the product, then ***you are*** the product."

Betternet is a VPN for Windows, Mac, iOS and Android

ONLINE PRIVACY AND SECURITY TRUSTED BY MILLIONS

#	App ID	Class	Rating	# Installs	AV-rank
1	OkVpn [35]	Prem.	4.2	1K	24
2	EasyVpn [15]	Prem.	4.0	50K	22
3	SuperVPN [52]	Free	3.9	10K	13
4	Betternet [19]	Free	4.3	5M	13
5	CrossVpn [7]	Free	4.2	100K	11
6	Archie VPN [4]	Free	4.3	10K	10
7	HatVPN [22]	Free	4.0	5K	10
8	sFly Network Booster [48]	Prem.	4.3	1K	10
9	One Click VPN [36]	Free	4.3	1M	6
10	Fast Secure Payment [17]	Prem.	4.1	5K	5

Table 5: VPN Apps with a VirusTotal AV-rank ≥ 5.

Besplatni VPN: “privatnost”

# Trackers	VPN Apps			Free non-VPN Apps
	Premium	Free	All	
0	65%	28%	33%	19%
1	13%	10%		
2	10%	10%		
3	12%	25%	13%	23%
4	2%	8%	4%	16%
≥5	5%	18%	8%	17%

72% ima trackere?

Table 4: Distribution of third party trackers embedded in VPN apps.

PSIPHON

*"We **sometimes** use advertisements to support our service, which may **use technology** such as **cookies** and **web beacons**. Our **advertising partners** use of cookies enable them and their partners to serve ads based on **your usage data**."*

Napadi na VPN servere

- **Palo Alto Network** Security Advisory PAN-SA-2019-0020, in relation to CVE-2019-1579
- **FortiGuard** Security Advisories FG-IR-18-389, in relation to CVE-2018-13382; FG-IR-18-388 in relation to CVE-2018-13383; FG-IR-18-384, in relation to CVE-2018-13379
- **Pulse Secure** Security Advisory SA44101, in relation to CVE-2019-11510, CVE-2019-11508, CVE-2019-11540, CVE-2019-11543, CVE-2019-11541, CVE-2019-11542, CVE-2019-11539, CVE-2019-11538, CVE-2019-11509, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11507CVE-2019-11507
- **Citrix** Security Advisory CTX267027, in relation to CVE-2019-19781

VPN DDoS

Izgaranje resursa; rušenje VPN servera

VPN server == gateway od remote zaposlenika prema poduzeću

Cutoff regularnih zaposlenika, ali i IT osoblja

Report o iscrpljivanju resursa sa samo 1 Mbps na VPN ili firewallu

- Kombinacija TCP paketa sa SYN, ACK i URG flagovima

SSL-based VPNovi ranjivi na **SSL flood**

Ranjivost na UDP flood

VPN preporuke za autentikaciju
(in a nutshell)

1. MFA
2. Certifikati

MFA

Microsoft: *"enabling a MFA solution for online accounts usually blocks 99.9% of all account takeover (ATO) attacks, even if the attacker has valid credentials for the victim's account."*

Google: "*Our research shows that simply adding a recovery phone number to your Google Account can block up to 100% of automated bots, 99% of bulk phishing attacks, and 66% of targeted attacks that occurred during our investigation" (…)*

Kućni LAN/WiFi

Gateway: default username/password

Firmware upgrade?

Network Firewall? IDS/IPS?

WPS ranjivosti

Remote management

Ranjivi IoT uređaji

Loša Internet veza

Loša strujna mreža

Ranjiva privatna računala i rootani uređaji

Nekontrolirano spajanje xy uređaja

WEP??

...

Kućni LAN/WiFi

Otprilike 5 od svakih 6 kućnih WiFi rutera nije adekvatno ažurirano protiv poznatih sigurnosnih ranjivosti (*The American Consumer Institute Center for Citizen Research, ACI*)

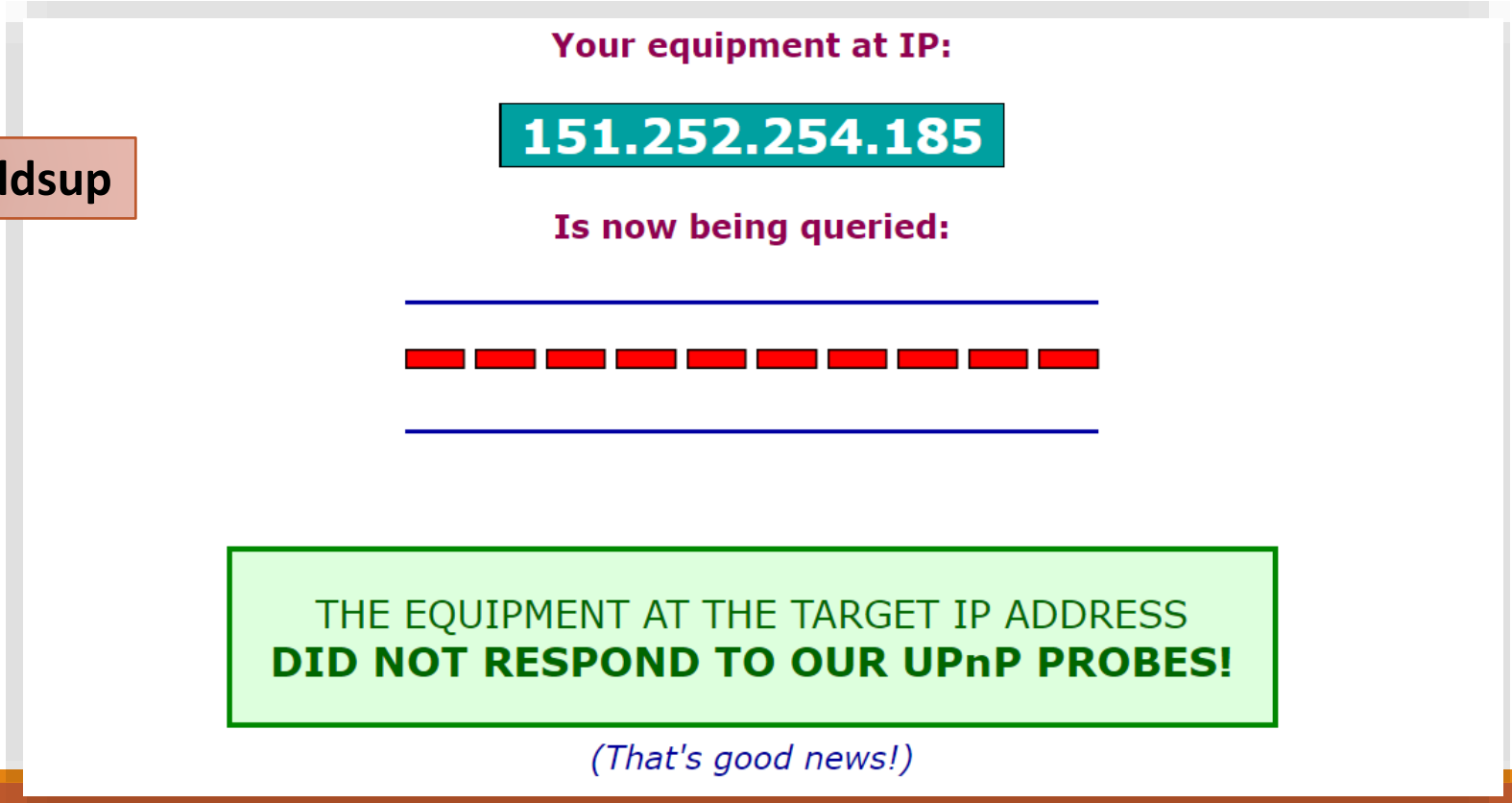
Ključni nalazi ACI studije o 186 WiFi rutera 14 različitih proizvođača:

- 32003 poznatih sigurnosnih ranjivosti
- 83% rutera ima ranjivosti za potencijalne napade
- 28% ranjivosti su u kategoriji "visoko-rizične i kritične"
- Najčešće ranjivosti: "srednje rizične", s prosječno 103 ranjivosti po ruteru
- Nepostojanje user-friendly firmware update ("nepotrebni trošak")
- **Samostalni update**: opasnost od skidanja zastarjelog koda ili malicioznog koda

Kućna mreža: provjera otvorenih portova

Resursi: routersecurity.org/testrouter.php

grc.com/shieldsup



ipvoid.com/port-scan

Enter IPv4 or IPv6 address to scan:

151.252.254.185

Scan all common ports

Scan a custom port

80

I agree to the terms of use

I'm not a robot

reCAPTCHA
Privacy - Terms

Scan Now

Port Scanning Results

Port	Type	Status	Service
21	TCP	Filtered	ftp
22	TCP	Filtered	ssh
23	TCP	Filtered	telnet
25	TCP	Filtered	smtp
53	TCP	Filtered	domain
80	TCP	Filtered	http
110	TCP	Filtered	pop3
111	TCP	Filtered	rpcbind
135	TCP	Filtered	msrpc
139	TCP	Filtered	netbios-ssn
143	TCP	Filtered	imap
389	TCP	Filtered	ldap

FBI: IoT uređaji na kućnoj mreži

→ Izolirati IoT uređaje na zasebnu WiFi mrežu
- Micro-segmentation: VLAN-ovi (firmware rutera)
- Fizička segmentacija: 2+ rutera

→ Paziti na zahtjeve za privilegije od strane mobilnih appova

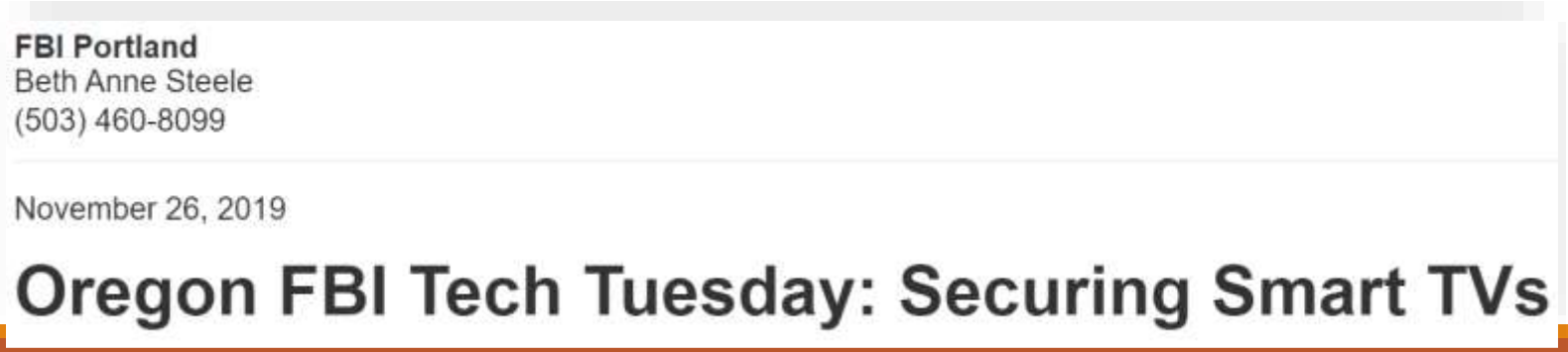
→ Paziti na higijenu passworda, ažuriranje firmwarea, ..

→ Sakriti kamere na smart TV-ovima

Security Holes Opened Back Door To TCL Android Smart TVs

Paul Roberts 2 days ago

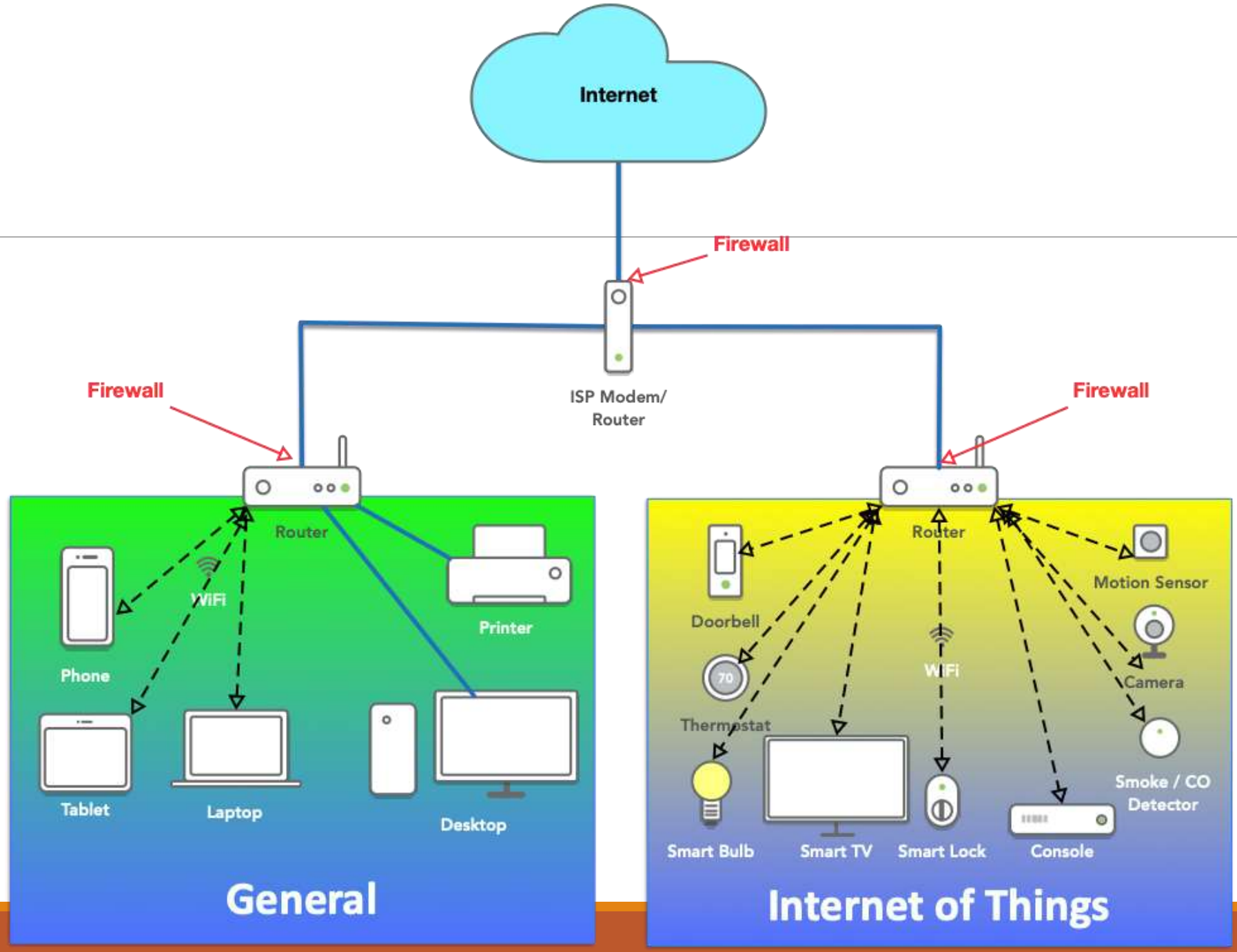
Millions of Android smart television sets from the Chinese vendor TCL Technology Group Corporation contained gaping software security holes that researchers say could have allowed remote attackers to take control of the devices, steal data or



FBI Portland
Beth Anne Steele
(503) 460-8099

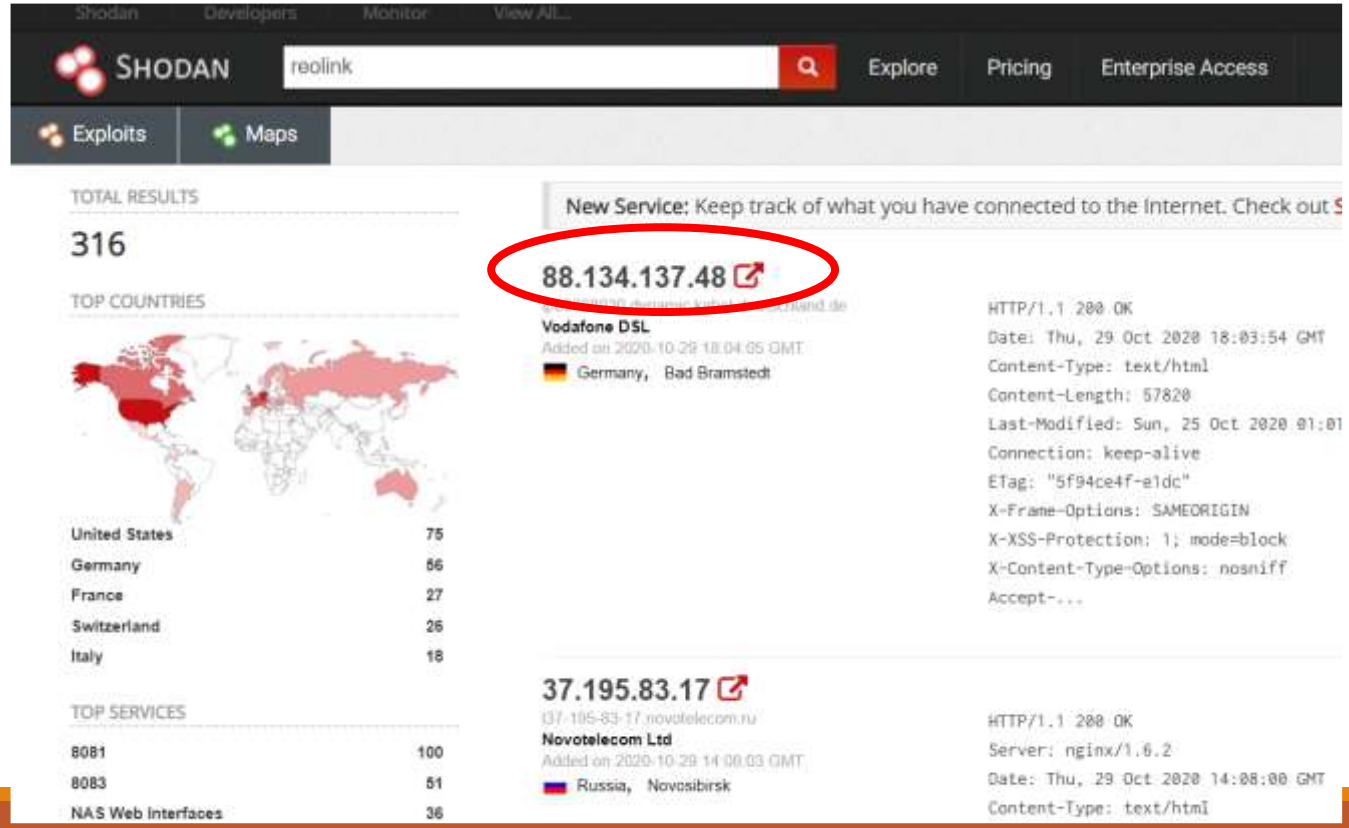
November 26, 2019

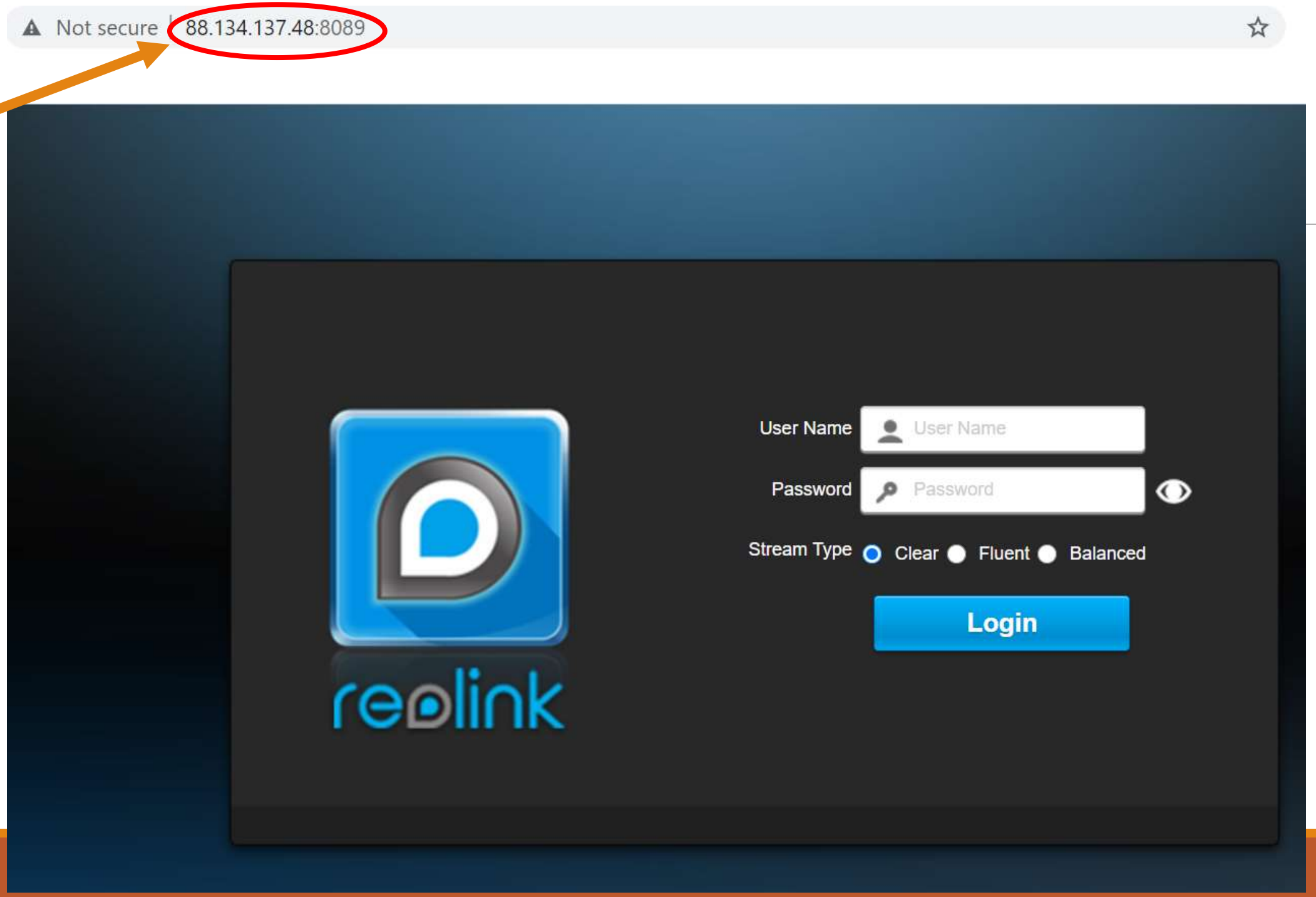
Oregon FBI Tech Tuesday: Securing Smart TVs


Internet
Firewall
ISP Modem/
Router
Firewall
Firewall
Router
Router
WiFi
Phone
Printer
Tablet
Laptop
Desktop
General
Doorbell
Motion Sensor
70
Thermostat
WiFi
Camera
Smoke / CO
Detector
Smart Bulb
Smart TV
Smart Lock
Console
Internet of Things

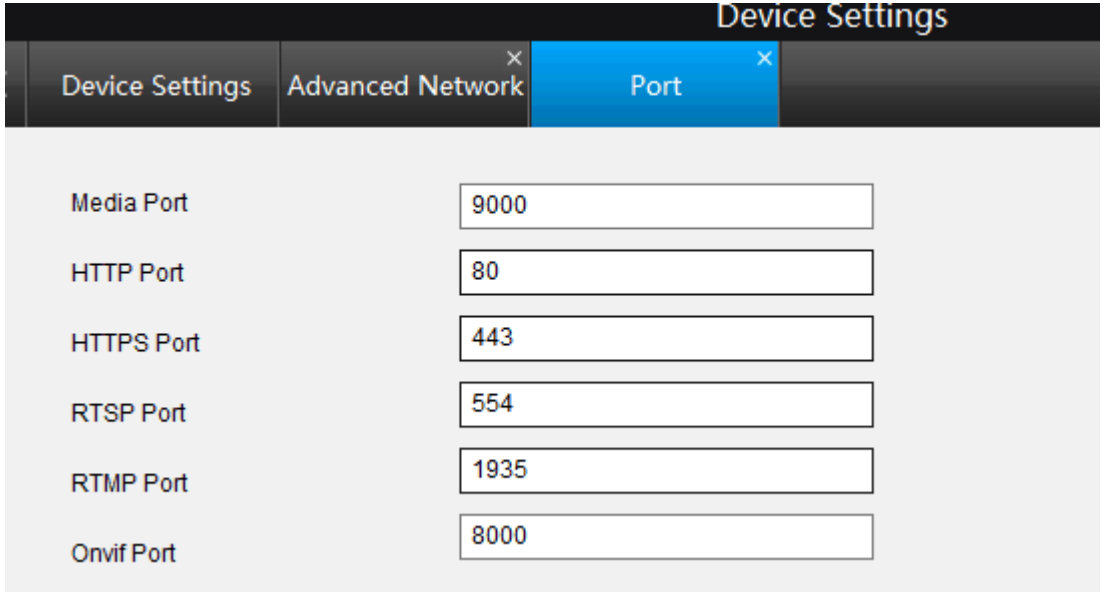
Kamere u kućnom uredu?

https://www.shodan.io/search?query=reolink



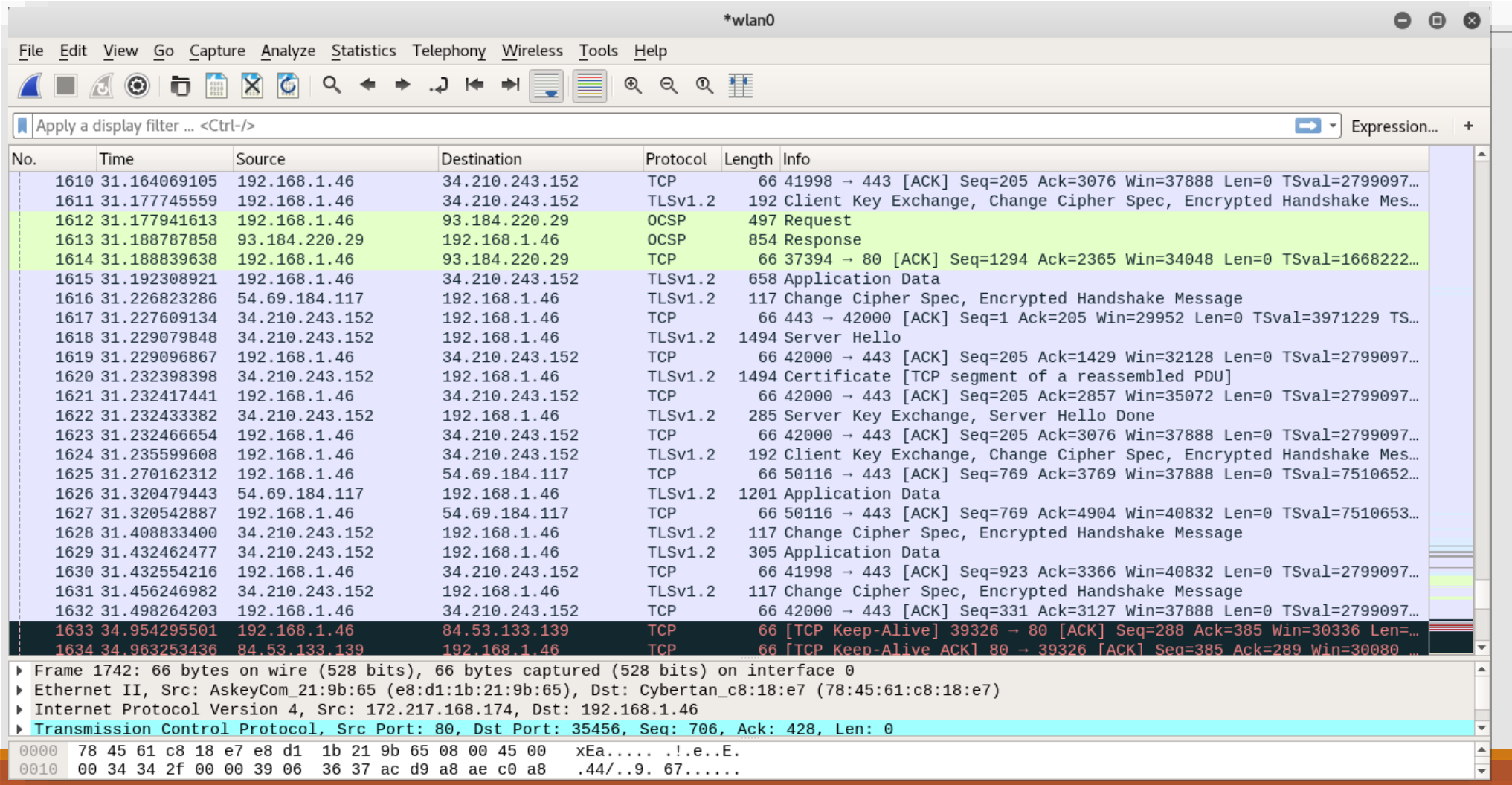

Not secure
88.134.137.48:8089
User Name
User Name
Password
Password
Stream Type
Clear
Fluent
Balanced
Login
reolink

Pristup kamerama



1. **IP** pristup
   - Forward portova na ruteru
2. **UID** pristup
   - Nema određenih portova (random UDP)
   - Nema forwardiranja

Praćenje prometa sumnjivih uređaja



Javni WiFi hotspotovi za remote?

Otvoreni, nekriptirani hotspotovi?

Hvatanje paketa, krađa nekriptiranih kritičnih informacija

Sidejacking (session hijacking)

Maliciozni **captive portal**

Sigurnosne postavke na OS-u (file sharing, firewall, …)

MitM, maliciozni hotspotovi

Evil twin hotspotovi

DNS Spoofing: lažirani DNS odgovori, redirekcije po volji napadača

Shoulder Surfing

…

UK's **N**ational **C**yber **S**ecurity **C**entre (NCSC)

- Napisati pisane **vodiče i dokumente s uputama** za korištenje softvera.
- Paziti da uređaji ispravno **kriptiraju podatke** u stanju mirovanja, kako bi zaštitili podatke na uređaju u slučaju gubitka ili krađe.
- Koristiti **mobile device management** alate (**MDM**) za konfiguraciju, daljinsko zaključavanje, brisanje podataka ili preuzimanje sigurnosne kopije kod mobilnih uređaja.
- Provjeriti jesu li **VPN**-ovi ažurirani; imati na umu potencijalno potrebne dodatne licence, kapacitet ili bandwidth.
- Zaposlenici moraju znati što učiniti **ako se njihov uređaj izgubi ili ukrade**, kome prijaviti, i osigurati da je process *blame-free*.
- **Onemogućiti prijenosne medije** pomoću MDM postavki.
- Koristiti **antivirusne alate.**
- Dopustiti upotrebu samo onih proizvoda **koje opskrbljuje organizacija**.
- **Kriptirati podatke** na prijenosnim medijima.

…

European Cybersecurity Agency ENISA

→ Osiguran WiFi

→ U potpunosti ažuriran antivirusni sustav

→ Ažurirani sigurnosni softver

→ Sigurnosne kopije (backup)

→Lock screen u slučaju rada u zajedničkom prostoru

→Sigurna konekcija na radno okruženje

→ Instalirani alati za enkripciju

European Cybersecurity Agency ENISA

Što mogu učiniti poslodavci?

→ Pružiti zaposlenicima **upute o tome kako reagirati** u slučaju problema
- kontakti, radno vrijeme službi, hitne procedure

→ Definirati **jasne operativne procedure** u slučaju sigurnosnog incidenta

Moderni SOC hibridnog doba

Istraživanje Exabeama nad **1000+ cybersecurity profesionalaca** unutar SOC-ova:

- 34% prijavilo **poteškoće u istraživanju** sigurnosnih incidenata
- 30% identificiralo **manjak vidljivosti u individualne mreže** kao problem
- 47% prijavilo **probleme sa novim alatima**, uključujući SaaS aplikacije

→ Implementirati arhitekture opremljene za rad u hibridnom okružju, gdje veliki dio zaposlenika radi na daljinu

Novo okruženje ubrzati će prelazak na cloud-based, SaaS SIEM-ove

- ugrađen UBA
- data input: xyz cloud, lokalni podaci

Moderna sigurnosna strategija hibridnog doba

Holistički pogled na security strategiju: HR + IT

HR

- Alati za psihometrijska testiranja i samosvjesnost
- Profiliranje timova
- Identifikacija ranjivosti

IT

- Korištenje rezutata HR istraživanja
- Izgradnja sigurnosnih protokola
- Izgradnja proaktivne sigurnosne strategije

Remote: zaključne preporuke

Snažne **lozinke/fraze**:
3ZelenaKuglofaUjela5Ruku!

MFA, barem 2FA
(izbjegavati mobilne MFA?)

Backup (offsite)

Higijena **rutera** (gatewaya)

Updateovi (security patcheovi)

Oprezno sa **"free" softverom**

Razdvojiti **osobni i poslovni hardver**;
Izdavati korporativne uređaje za rad od kuće

Korištenje **VPN**a

Izbjegavati **javne WiFi** hotspotove

Mobile malware u porastu
(izbjegavati shady firmwareove)

Guest Network, VLAN ili
segmentacija networka za IoT i sl.

UPS + baterija

Provjeriti **otvorene portove/ulazne vektore**

Antivirus (EPP) + **EDR**

Comodo open-sources its EDR solution

OpenEDR, announced in September, is available on GitHub starting this week.

Hvala na pažnji!

Sigurnosni aspekti rada od kuće

Doc.dr.sc. Igor Tomičić

Fakultet organizacije i informatike Varaždin