Računalniška/Informacijska/Kibernetska/Digitalna varnost
Computer/Information/Cyber/Digital security

Matjaž Kljun matjaz.kljun@upr.si

Oblika delavnice / Workshop format

- 8 urna delavnica (8x45 min)
  - 7. 4. 2025 - 4 ure
  - 14. 4. 2025 - 4 ure
- Kraj izvedbe: UP PEF

Vsebina:

- Programski napadi
- Varovanje pred napadi
- Socialni inženiring
- Varnost na spletu
- Brezžična omrežja
- …

- 8 hour workshop (8x45 min)
  - 7 April 2025 - 4 hours
  - 14 April 2025 - 4 hours
- Venue: UP PEF

Content:

- Software attacks
- Protection against attacks
- Social engineering
- Online security
- Wireless networks
- ...

1. del / Part 1

- Računalniška varnost
- Grožnje programske opreme
- Računalniška programska oprema
- Zlonamerna programska oprema
- Zaščita pred zlonamernim programjem
- Človeški vidiki groženj
- Primeri programskih groženj

- Computer security
- Software threats
- Computer software
- Malware
- Protection from malware
- Human aspects to threats
- Examples of software threats

Kaj je ta varnost? / What is this security about?

Kaj je ta varnost? / What is this security about?

Zaščita računalniških sistemov in omrežij pred napadi zlonamernih akterjev, ki lahko med drugim izvedejo:

- napad s programsko opremo,
- krajo intelektualne lastnine,
- krajo identitete,
- nepooblaščeno razkritje informacij,
- krajo opreme,
- krajo informacij,
- poškodovanje opreme,
- sabotažo, motnje in napačno usmeritev storitev ter
- Izsiljevanje s pridobljenimi informacijami.

The protection of computer systems and networks from attacks by malicious actors that may result, among other, in:

- software attacks,
- theft of intellectual property,
- theft of identity,
- unauthorized information disclosure,
- theft of equipment,
- theft of information,
- damage of equipment,
- sabotage, disruption misdirection of services, and
- information extortion.

Programski napadi / Software attacks

Škodljiva (zlonamerna) **programska oprema**:

- Virusi,
- Črvi,
- Trojanski konji,
- Izsiljevalska programska oprema,
- Stranska vrata,
- Botneti,
- Beležniki tipkanja,
- Vohunsko programje,
- Korenski kompleti,
- Strašilna programska oprema,
- …

Malware **software**:

- Viruses,
- Worms,
- Trojan horses,
- Ransomware,
- Backdoors,
- Botnets,
- Keyloggers (keystroke logging, recorder, keyboard capturing),
- Spyware,
- Rootkits,
- Scareware,
- …

Kaj je računalniški program? / What is a computer program?

Uporabniška programska oprema

- Grafični uporabniški vmesniki
- Uporabniški vmesniki z ukazno vrstico

Programska oprema brez vmesnika

- Servisni programi operacijskega sistema
  - Običajno se izvajajo v ozadju

Operacijski sistem

User software

- Graphic user interfaces
- Command line user interfaces

Software without interface

- Operating system service programs
  - Usually run in background

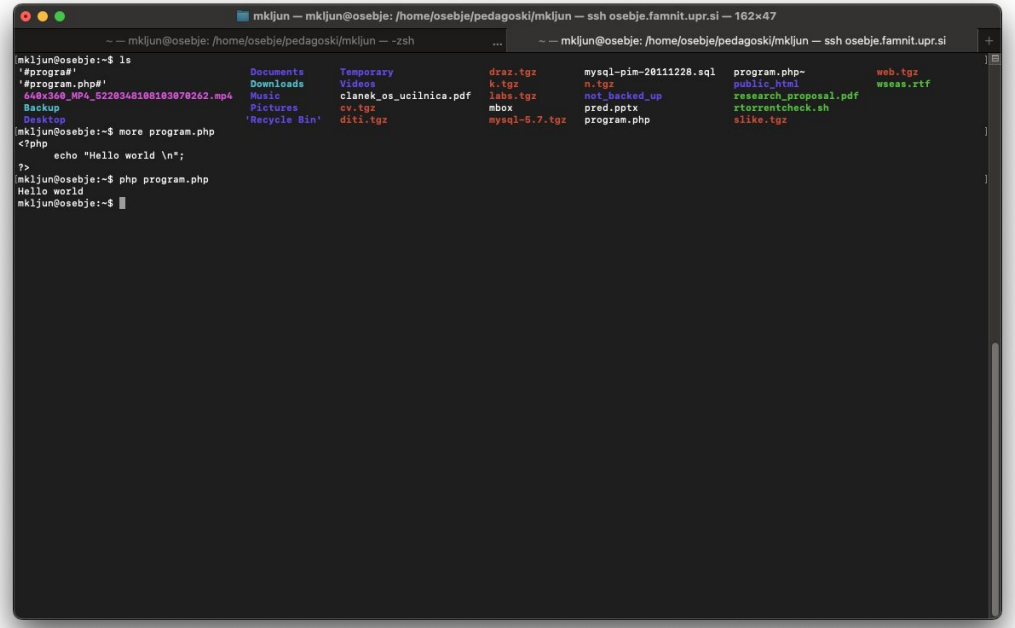
Operating system

https://www.techtarget.com/searchapparchitecture/definition/software-stack

Poskusimo dva jezika / Let’s try two programming languages

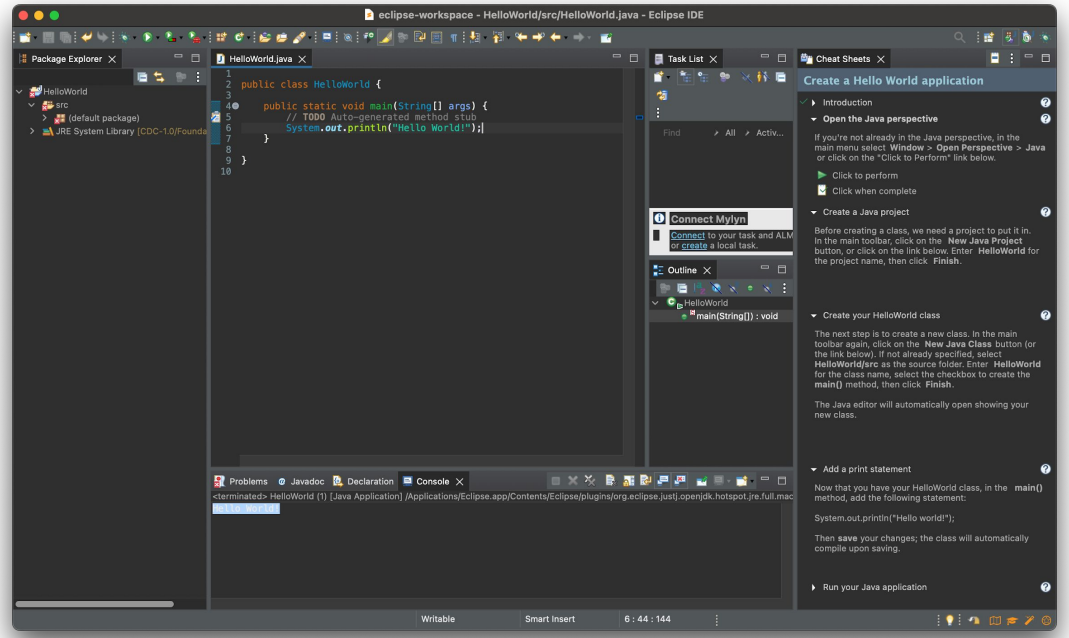
PHP

```
<?php
    echo "Hello, World!";
?>
```



JAVA

```
public class HelloWorld {
    public static void main(String[] args) {
        System.out.println("Hello World!");
    }
}
```



Zaščita / Protection

- Uporabimo protivirusno programsko opremo.
- Uporabimo programje proti zlonamerni programski opremi.

- Samodejno varnostno kopiramo v storitvah shranjevanja v oblaku (nekatere zagotavljajo določeno raven zaščite).
- Redno varnostno kopiramo in kopijo shranimo na:
  - nepovezanih nosilcih,
  - nosilcih samo za branje,
  - nosilcin z drugačnim datotečnim sistemom.
- Redno posodabljamo operacijski sistem in programsko opremo (iz zanesljivih virov, ne klikamo na neznane povezave).
- Odstranimo nepotrebno programsko opremo.
- Uporabimo dvo ali več faktorsko preverjanje pristnosti (2FA, MFA), če je na voljo.
- Še bolje, uporabimo Passkey, če je na voljo.

- Use antivirus software.
- Use anti malware software.

- Set up automatic backup on cloud storage services (some provide a level of protection).

- Perform regular backups kept on:
  - unconnected mediums,
  - read only mediums,
  - mediums with a different file system.
- Ensure operating system and software are always up to date (from reputable sources, do not click on unknown links).
- Uninstall unneeded software.
- Set up two- or multi-factor authentication (2FA, MFA) where this option is available.
- Even better, use Passkey if available

Bodimo pozorni / Be vigilant

- Ne delimo svojih osebnih podatkov z ljudmi, ki jih ne poznamo.
- Ne nakažemo denarja, ne da bi potrdili pristnost zahtevka. Če nam nekdo pošlje sporočilo s prošnjo za denar, ga pokličemo in preverimo, da je prošnjo poslal on.
- Nikoli z nikomer ne delimo gesel, kod.
- Ne klikamo na naključne povezave in ne odpiramo naključnih priponk. Če je videti, kot da nam je prijatelj nekaj poslal, ga prek drugih kanalov vprašamo, ali je bilo sporočilo res namenjeno nam. Bodimo pozorni tudi na slovnične napake ali čudne povezave (povezava na primer vodi na naslov URL, ki se ne ujema z imenom podjetja).
- Banke nam ne pošiljajo sporočil, z vprašanji. Nikoli ne razkrijemo svojih osebnih podatkov in prijavnih podatkov. Obiščemo uradno spletno stran banke, najbolje tako, da v spletni brskalnik vtipkamo njen naslov URL.

- Avoid sharing your personal information with people you don’t know.
- Do not transfer money without confirming the authenticity of the request. For example, if someone sends you a text asking for money, call them to make sure the request came from them.
- Never share verification passwords, codes with anyone.
- Don’t click on random links or open random attachments. If it looks like a friend sent you something, ask them via other channels if the message was really intended for you. Make sure to also look out for grammar mistakes or weird links (for example, the link goes to a URL that doesn’t match the company name).
- Banks don’t message you to ask questions. Never give away your personal information and login credentials. Visit the bank's official website, ideally by typing its URL address into the web browser.

To je to!

This is it!

Hvala za pozornost / Thank you for your attention

Matjaž Kljun
matjaz.kljun@upr.si
@_mkljun_

Vprašanja?

Matjaž Kljun
matjaz.kljun@upr.si
@_mkljun_

Questions?

A vendar … smo ljudje … / But nevertheless … we are human …

Strah, ljubezen, pohlep, stres, radovednost in druga stanja vplivajo na

- našo sposobnost kritičnega razmišljanja in
- naši reptilski možgani prevzamejo oblast.

Socialni inženiring igra na karto:

- Čustev
- Nujnosti
- Poziva k ukrepanju

- Lahko smo zavedeni v klik priponke v e-pošti, ki je zamaskirana tako, da se zdi nedolžna (npr. rutinski obrazec, ki ga je treba izpolniti).
- Lahko smo zavedeni v klik na lažni oglas v družabnih medijih ali kjer koli drugje.
- Lahko po telefonu povemo podatke plačilne kartice.
- Lahko "najdemo" USB ključek in preverimo, kaj je gor.
- …

Fear, love, stress, greed, curiosity and other states can affect

- our critical thinking capabilities are affected and
- our reptilian brain takes over.

Social engineering is counting on:

- Emotions
- Emergency
- Call to actions

- We can be duped into executing an email attachment disguised to appear innocuous (e.g., a routine form to be filled in),
- When can be duped into clicking on a fake advertisement on social media or anywhere else.
- We can tell paycard data over the phone.
- We can "find" a thumbdrive and check what’s on it.
- …

21. 1. 2025

Spoštovani,
Dear colleagues,

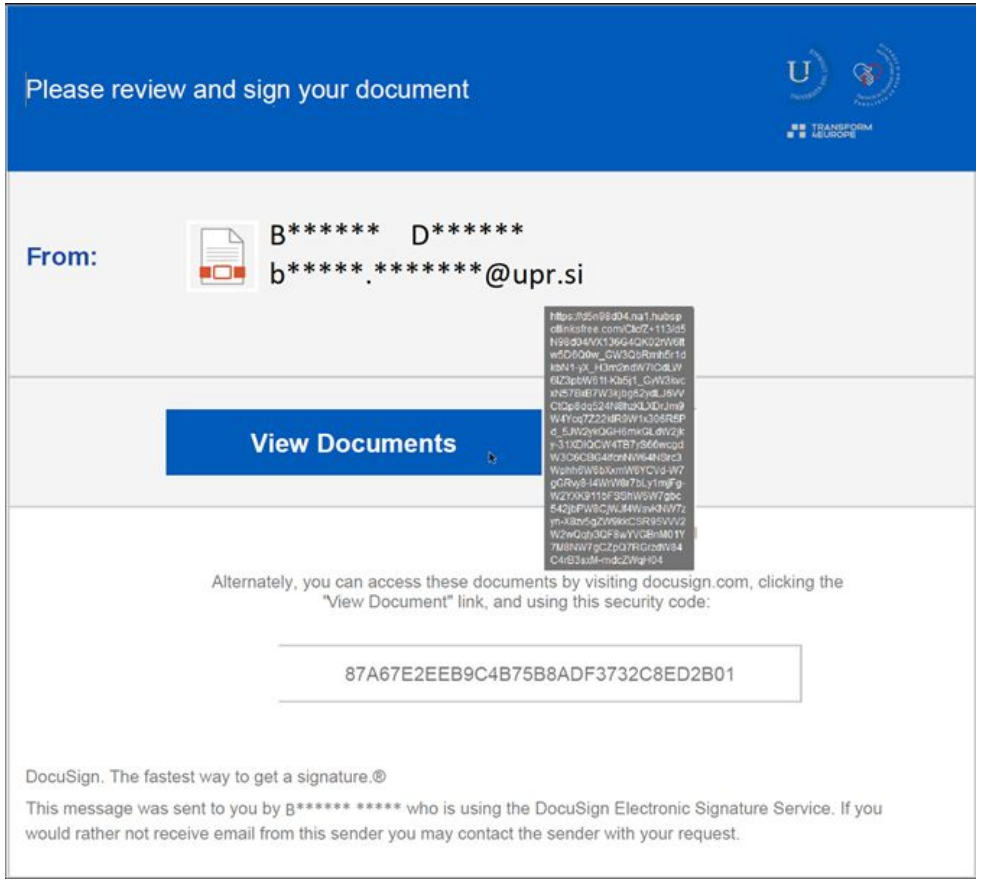
V zadnjem času smo na UP tarča zlonamernih elektronskih sporočil, s katerimi poskušajo vdreti v naš informacijski sistem.
Recently, at UP, we have been the target of malicious e-mails, with which they try to break into our information system.

Zlonamerneži vdrejo v račun uporabnika in iz računa pošiljajo elektronska sporočila. Ta sporočila vsebujejo povezavo do OneDrive osebe, od katere ste prejeli sporočilo in/ali dokumenta (pdf ali drugega formata). V tem dokumentu je nato še ena povezava, ki pa vas preusmeri na stran zlonamernežev.
Malicious people hack into a user's account and send emails from the account. These messages contain a link to the OneDrive of the person from whom you received the message and/or document (pdf or other format). There is another link in this document, but it redirects you to the malicious site.

Ko kliknete na to povezavo, se pojavi zahteva za vnos uporabniškega imena in gesla, ki je vizualno enaka kot od MS Office 365. Če vnesete podatke, zlonamerneži pridobijo vaše uporabniško ime, geslo in celo dvofaktorsko kodo ter dostopajo do sistema.
When you click on this link, you will be prompted to enter a username and password, which is visually identical to that of MS Office 365. If you enter the information, the attackers will obtain your username, password and even a two-factor code and gain access to the system.

Sporočila so zelo dobro pripravljena in vizualno enaka kot Office 365!
The messages are very well prepared and visually identical to Office 365!

Iz primera se vidi slab UP logo in povezavo, ki vodi na tujo spletno stran.
From the example, you can see a bad UP logo and a link that leads to a foreign website.



Poučna zgodba / An educational story

Eva Wolfangel

... novinarka, govornica in moderatorka, ki se osredotoča na tehnologije prihodnosti, kot so ... kibernetska varnost ...

Eva Wolfangel

... a **journalist, speaker and moderator**, focusing on future technologies such as … cyber security ...

CHI 2023 Opening Keynote – Eva Wolfangel "The Human Element in Cybercrime and Cybersecurity"

https://www.youtube.com/live/LKUMRTLV49g?t=2111

Napadi s programsko opremo

Software attacks

Virusi / Viruses

- Računalniški virus je računalniški program, ki se ob izvajanju razmnožuje tako, da spreminja druge računalniške programe (gostiteljske programe) in vanje vstavlja svojo kodo.
- Če to razmnoževanje uspe, se za prizadeta območja reče, da so "okužena" z računalniškim virusom, kar je metafora, izpeljana iz bioloških virusov.

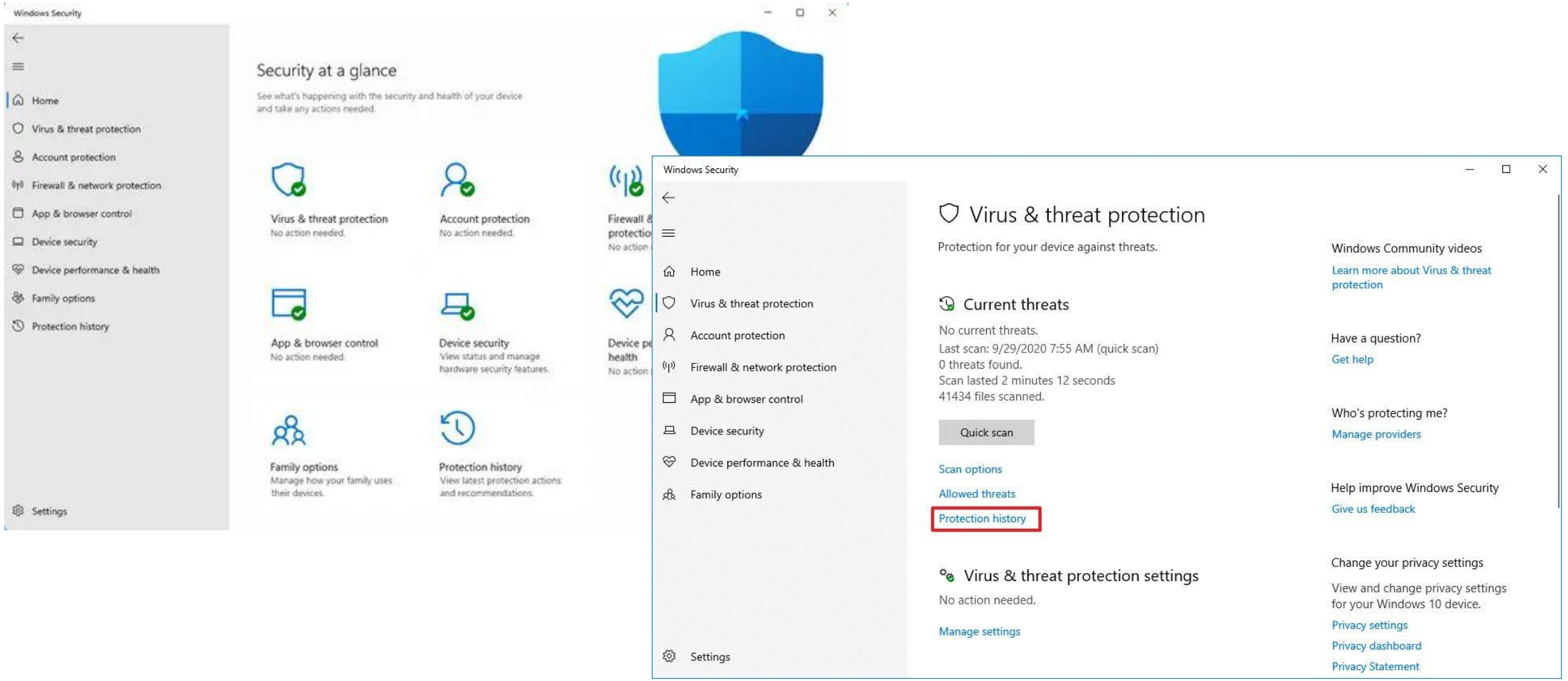
- A computer virus is a computer program that, when executed, replicates itself by modifying other computer programs (host program) and inserting its own code into those programs.
- If this replication succeeds, the affected areas are then said to be "infected" with a computer virus, a metaphor derived from biological viruses.

Učinki računalniških virusov / Effects of a computer viruses

- Sesutje sistema
- Samodejno pošiljaje e-pošte
- Manjkajoče datoteke
- Počasno delovanje
- Pogoste okvare
- Visoka aktivnost na omrežju
- Malo prostora za shranjevanje
- Težave pri izklopu ali ponovnem zagonu
- Težave s programi in datotekami
- Nepravilno delovanje protivirusnih programov
- Sumljiva dejavnost trdega diska

- System crashes
- Emails sent autonomously
- Missing files
- Slow performance
- Frequent crashes
- High network activity
- Low storage
- Issues shutting down or restarting
- Issues with programs and files
- Malfunctioning antivirus programmes
- Suspicious hard drive activity

Preverimo protivirusni program / Check antivirus software

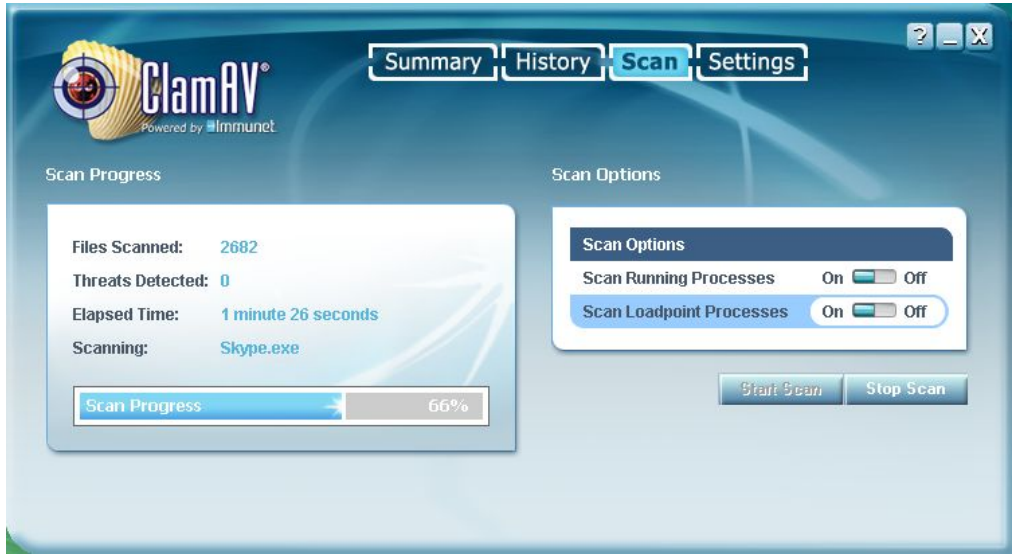


https://en.wikipedia.org/wiki/Microsoft_Defender_Antivirus

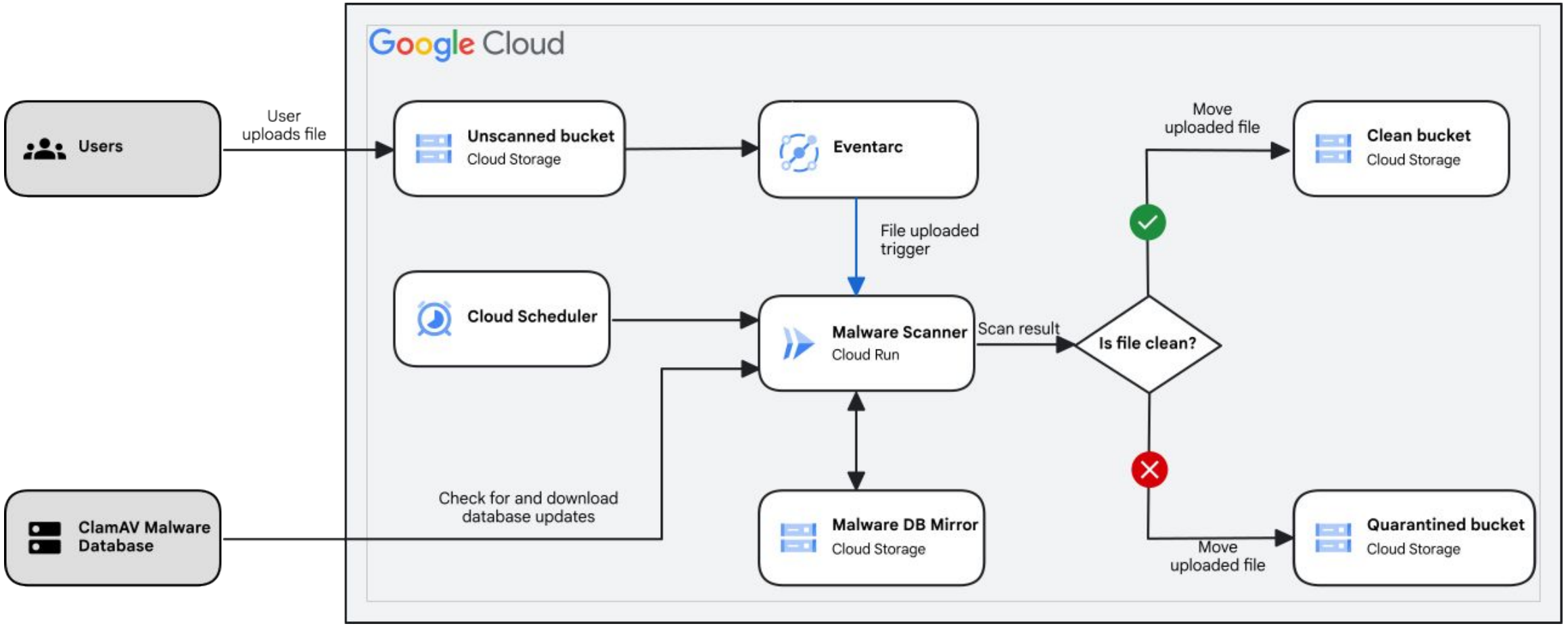
ClamAV

- Odprtokodni protivirusni program
- Različice skupnosti so na voljo za AIX, BSD, HP-UX, Linux, macOS, OpenVMS, OSF (Tru64), Solaris, Haiku in MS Windows.

- Opensource antivirus
- Third party versions available for AIX, BSD, HP-UX, Linux, macOS, OpenVMS, OSF (Tru64), Solaris, Haiku and MS Windows.

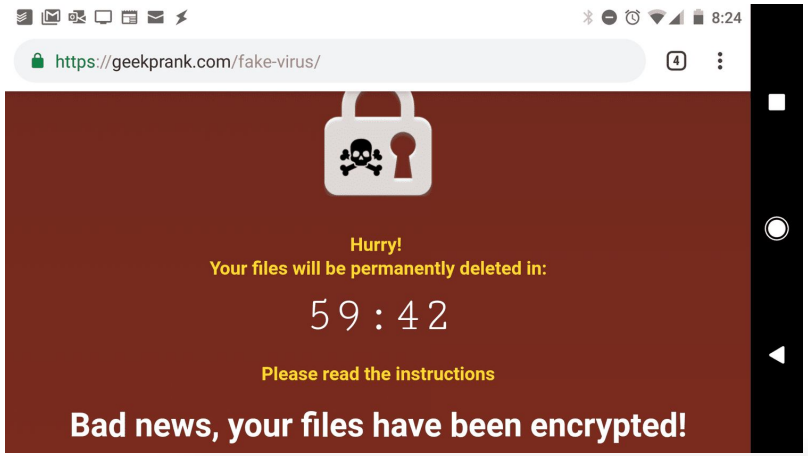


Primer v oblaku / An example in the cloud



https://cloud.google.com/architecture/automate-malware-scanning-for-documents-uploaded-to-cloud-storage

Lažna opozorila / Fake alerts



- Čustva
- Nujnost
- Poziv k ukrepanju

- Emotions
- Emergency
- Call to actions

Črv / Worm

- Računalniški črv je samostojen zlonamerni računalniški program, ki se razmnožuje in se širi na druge računalnike prek omrežja.
- Za napad izrablja varnostne napake v ciljnem računalniku. Okužen računalnik nato uporabi kot gostitelja za pregledovanje in okužbo drugih računalnikov, ki jih nato uporabi kot gostitelje, in tako nadaljuje napad.
- Računalniški črvi uporabljajo rekurzivne metode za kopiranje brez gostiteljskih programov (kot to rabijo virusi) in se širijo na podlagi izkoriščanja hitre eksponentne rasti ter tako v kratkem času lahko nadzorujejo in okužijo veeliko število računalnikov.

- A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers over a network
- It relies on security failures on the target computer to access it. It will use this machine as a host to scan and infect other computers to use as hosts and this behaviour continues.

- Computer worms use recursive methods to copy themselves without host programs (like viruses) and distribute themselves based on exploiting the advantages of exponential growth, thus controlling and infecting more and more computers in a short time.

V branje / To read - NoPetya

- Komprimitirana oprema skupine Linkos, majhnega podjetja, ki trži računovodski programski imenovan M.E.Doc.
- Orodje, imenovano EternalBlue, ki ga je razvila Agencija za nacionalno varnost (NSA) leta 2017.
- Mimikatz, programska aplikacija, ki je lahko iz pomnilnika RAM izvlekla uporabniška gesla in jih ponovno uporabila za kompromitiranje ciljnih računalnikov.

- The compromise of the Linkos Group, a small software firm that markets an accounting software package called M.E.Doc.
- A tool called EternalBlue, created by the National Security Agency (NSA), leaked in early 2017.
- Mimikatz, a software application that had the ability to pull user passwords out of RAM and reuse them to compromise targeted machines.

https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Trojanski konj / Trojan horse

Zlonameren program, ki uporabnike zavaja glede svojega pravega namena tako, da se predstavlja kot poznani program.

“Tovor” trojanskega konja je lahko karkoli, vendar danes pogosto:

- odpre stranska vrata in vzpostavi stik z napadalcem, ki lahko nato nepooblaščeno dostopa do prizadetega računalnika,
- izvaja napade z izsiljevalsko programsko opremo, ki šifrira disk računalnika.

Any malware that misleads users of its true intent by disguising itself as a standard program.

The “payload” can be anything, but many modern forms:

- act as a backdoor, contacting a controller who can then have unauthorized access to the affected computer,
- carry ransomware attacks encrypting computer’s disk.

Izsiljevalska programska oprema / Ransomware

Zlonamerno programje, ki trajno onemogoči dostop do osebnih podatkov, če žrtev ne plača odkupnine. Dostop lahko onemogoči z:

- zaklepom sistema, ne da bi poškodovala datoteke,
- šifriranjem datotek, zaradi česar postanejo le te nedostopne (kriptovirusno izsiljevanje).

Odkupnina se ponavadi zahteva v

- prednaloženih plačilnih karticah ali
- kriptovalutah,

kar otežuje izsledite in pregon storilcev.

NE PLAČAMO!

Malware that permanently block access to the victim's personal data unless a ransom is paid. The access is blocked either by:

- locking the system without damaging any files,
- encrypting the victim's files, making them inaccessible (cryptoviral extortion).

The ransom is usually demanded in

- paysafecards or
- cryptocurrencies

making tracing and prosecuting the perpetrators difficult.

V branje / To read - WannaCry

- Se je širil s pomočjo EternalBlue DoublePulsar backdoor implant tool.
- Okuženih 300.000 računalnikov v 150 državah

- Propagated by using EternalBlue in DoublePulsar backdoor implant tool.
- 300,000 computers affected across 150 countries.

https://blog.checkpoint.com/security/how-the-evolution-of-ransomware-changed-the-threat-landscape/

Programski napadi / Software attacks

- Stranska vrata
  - Prikrit način izogibanja običajnemu preverjanju pristnosti ali šifriranju v računalniku, izdelku ali vgrajeni napravi (npr. domačem usmerjevalniku).
- Botnet
  - Skupina naprav, povezanih v internet, ki se uporablja za izvajanje napadov DDoS, krajo podatkov, pošiljanje neželene pošte in omogoča napadalcu dostop do naprave in njene povezave.
- Rootkit
  - Zbirka programske opreme, namenjena omogočanju dostopa do računalnika ali dela njegove programske opreme, ki sicer ni dovoljen (na primer nepooblaščenemu uporabniku), in pogosto prikriva svoj obstoj ali obstoj druge programske opreme.
- Scareware
  - Zlonamerna programska oprema, ki uporablja socialni inženiring za povzročanje šoka, tesnobe ali grožnje, da bi uporabnike prepričala v nakup neželene programske opreme.

- Backdoor
  - A covert method of bypassing normal authentication or encryption in a computer, product, embedded device (e.g. a home router),
- Botnet
  - A group of Internet-connected devices used to perform DDoS attacks, steal data, send spam, and allow the attacker to access the device and its connection.
- Rootkit
  - A collection of software, designed to enable access to a computer or an area of its software that is not otherwise allowed (for example, to an unauthorised user) and often masks its existence or the existence of other software.
- Scareware
  - malware which uses social engineering to cause shock, anxiety, or the perception of a threat in order to manipulate users into buying unwanted software

https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/

BadBox 2

From: Tehnična pomoč Telekom Slovenije <tehnicna.pomoc@telekom.si>
Date: 18 March 2025 at 13:15:28 CET
To:
Subject: RE: INC000102375569 Screenshot 2025-03-18 at 11.07.27
Reply-To: Tehnična pomoč Telekom Slovenije <tehnicna.pomoc@telekom.si>

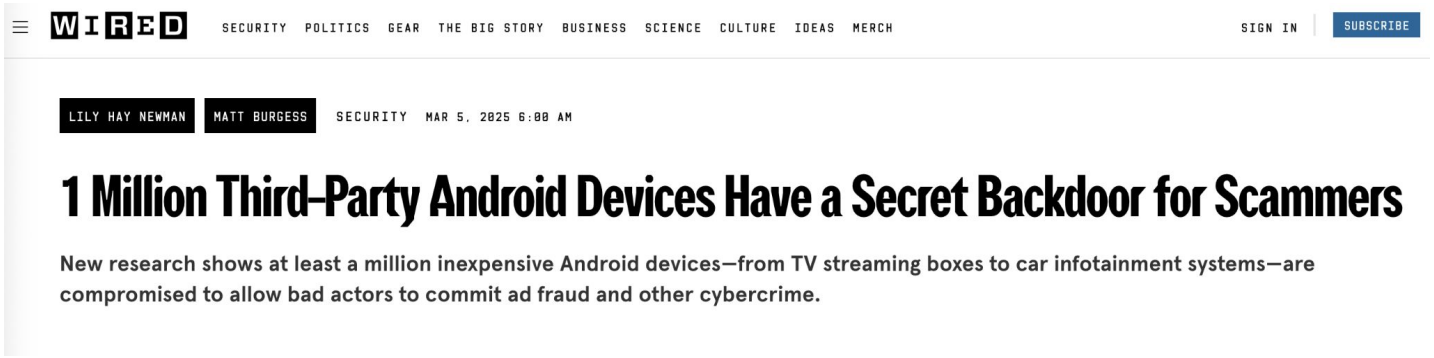
Pozdravljeni,

Prejeli smo obvestilo s strani državne obveščevalne službe za kibernetsko varnost SI-CERT, da je bil vaš IP naslov prijavljen s strani drugih ponudnikov kot zlonameren oz. je opravljal aktivnosti značilne za okuženo omrežje. Glede na njihovo prijavo se je iz vašega IP naslova "89.142.95.162" kreirala povezava proti domeni "dcylog.com", pri katerem je tuji ponudnik v povezavi zaznal značilnosti okužbe "android.badbox2" (**Android.BadBox2** je različica zlonamerne programske opreme, ki okuži naprave z operacijskim sistemom Android. Gre za botnet, ki okuži naprave in jih uporablja za različne zlonamerne dejavnosti). Predlagam vam preverbo vseh domačih in android naprav z protivirusnim programom.

Vabimo vas, da s klikom na anketo ocenite svojo izkušnjo z reševanjem primera.

Prijazen pozdrav,

Jure Brenčič
Tehnična podpora - Storitve uporabnikov / Customer Technical Support
Operativno storitveni center / Service Operations Center

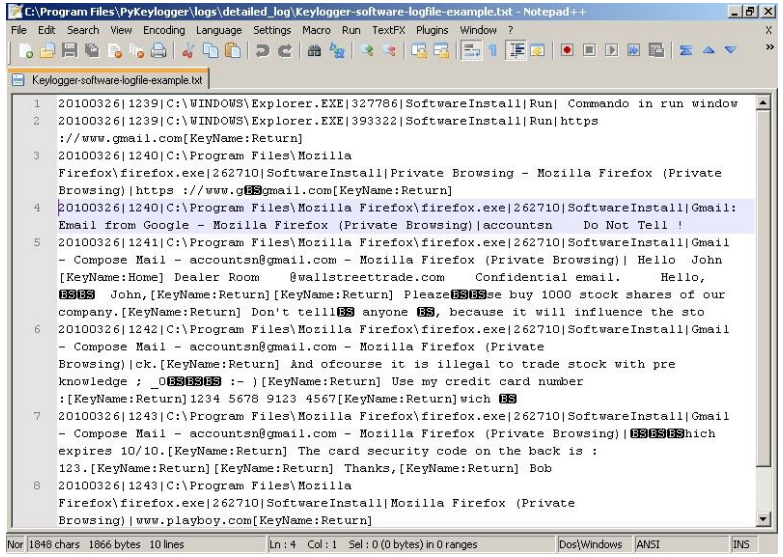


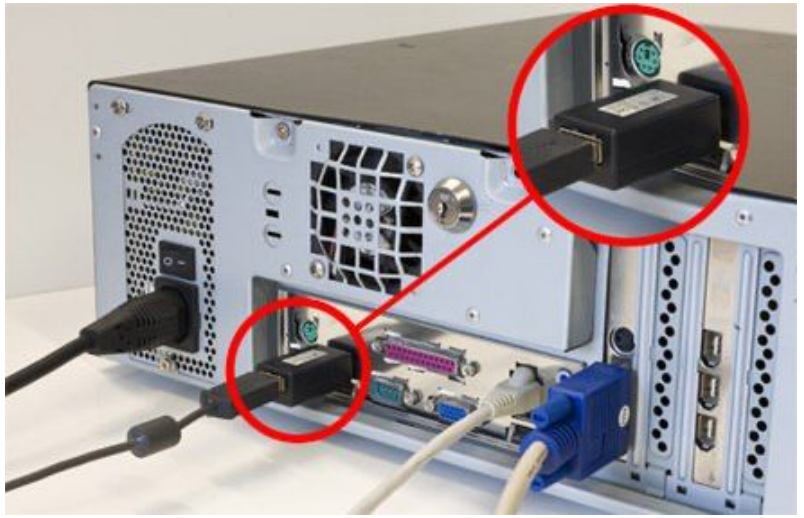
https://www.wired.com/story/1-million-third-party-android-devices-badbox-2/

Beležnik tipkanja / Keylogger

- Snemanje (beleženje) pritisnjenih tipk na tipkovnici, običajno prikrito, tako da se oseba, ki uporablja tipkovnico, ne zaveda, da se tipkanje beleži.
- Programska ali strojna oprema.

- Recording (logging) the keys struck on a keyboard, typically covertly, so that a person using the keyboard is unaware that their actions are being monitored.
- Software or hardware.





Poskusimo / Let’s try it

Preprost program, ki ne potrebuje namestitve.

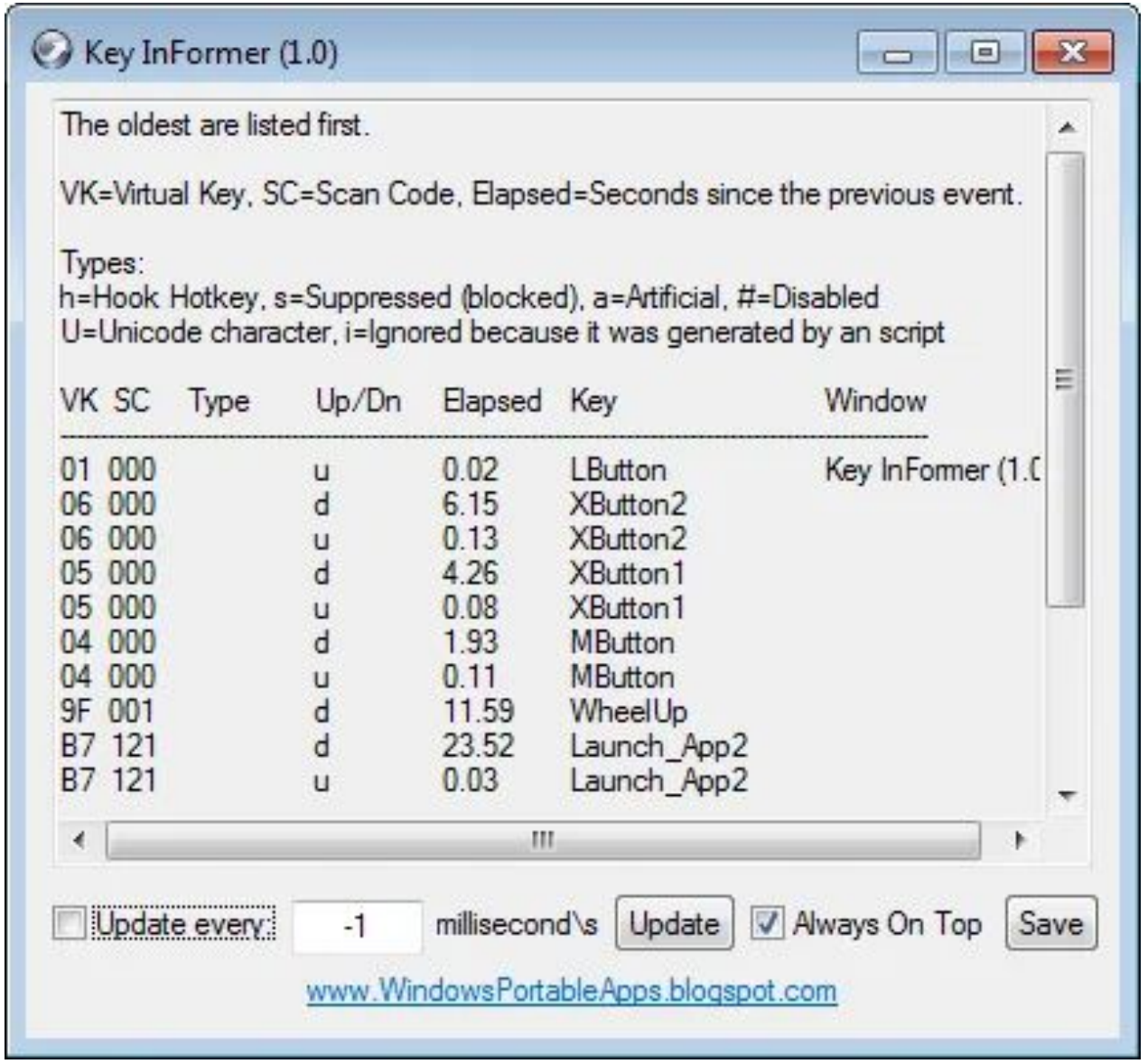
A simple software that needs no installation.

Ni skrit v ozadju.

It’s not hidden in the background.

Obstajajo veliko bolj sofisticirani programi.

There are much more sophisticated programmes.



https://alternativeto.net/software/key-informer/about/

Primer strojnega beležnika tipkanja / An example of hw keylogger

AirDrive Forensic Keylogger

Ultra compact and discreet Wi-Fi hardwa

Main page Keyloggers RS-232 & RS-485 Barcode, Keyboard, Mous

KeyGrabber Forensic Keylogger

Setting a new standard

The **KeyGrabber Forensic Keylogger** is a record-breaking USB hardware keylogger in terms of size, keyboard compatibility, and price. It measures only **0.4" (10 mm)** in length, and can be accessed as a **USB flash drive** for instant data retrieval. It's by far the most miniaturized and discreet hardware keylogger available on the market. Completely transparent for computer operation, cannot be detected by computer software. The KeyGrabber Forensic hardware keylogger features a sophisticated FPGA chip with a 32X oversampling algorithm, making it compatible with all types of USB keyboards and barcode readers. It's also an **advanced penetration testing tool**, with a **built-in scripting language**.

$44.99 / €40.99 | $52.99 / €48.99 | $74.99 / €68.99

Add to cart | Add to cart | Add to cart

Find out more | Find out more | Find out more

Interested in B2B or wholesale? Check our B2B prices and wholesale prices.

Applications

- Observe WWW, E-mail & chat usage by children and employees
- Monitor employee productivity
- Protect your child from on-line hazards and predators
- Save a copy of typed text
- Penetration testing
- Keystroke generation macros & scripts
- ...and several more, see keystroke recorder benefits

https://www.keelog.com/keygrabber-keylogger/

Vohunska programska oprema / Spyware

Programska oprema, katere namen je zbiranje informacij o osebi (organizaciji) in njihovo pošiljanje drugi osebi na način, ki škoduje uporabniku (organizaciji) s kršenjem njegove (njene) zasebnosti, ogrožanjem varnosti (njene) naprave (naprav) ali na druge načine.

Software that aims to gather information about a person or organization and send it to another entity in a way that harms the user (organisation) by violating their privacy, endangering their device's security, or other means.

https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/

V branje / To Read

forbidden stories

PROTECT YOUR STORIES

GET OUR NEWSLETTER

First Name

Last Name

Your email

OK

DONATE

PEGASUS: THE NEW GLOBAL WEAPON FOR SILENCING JOURNALISTS

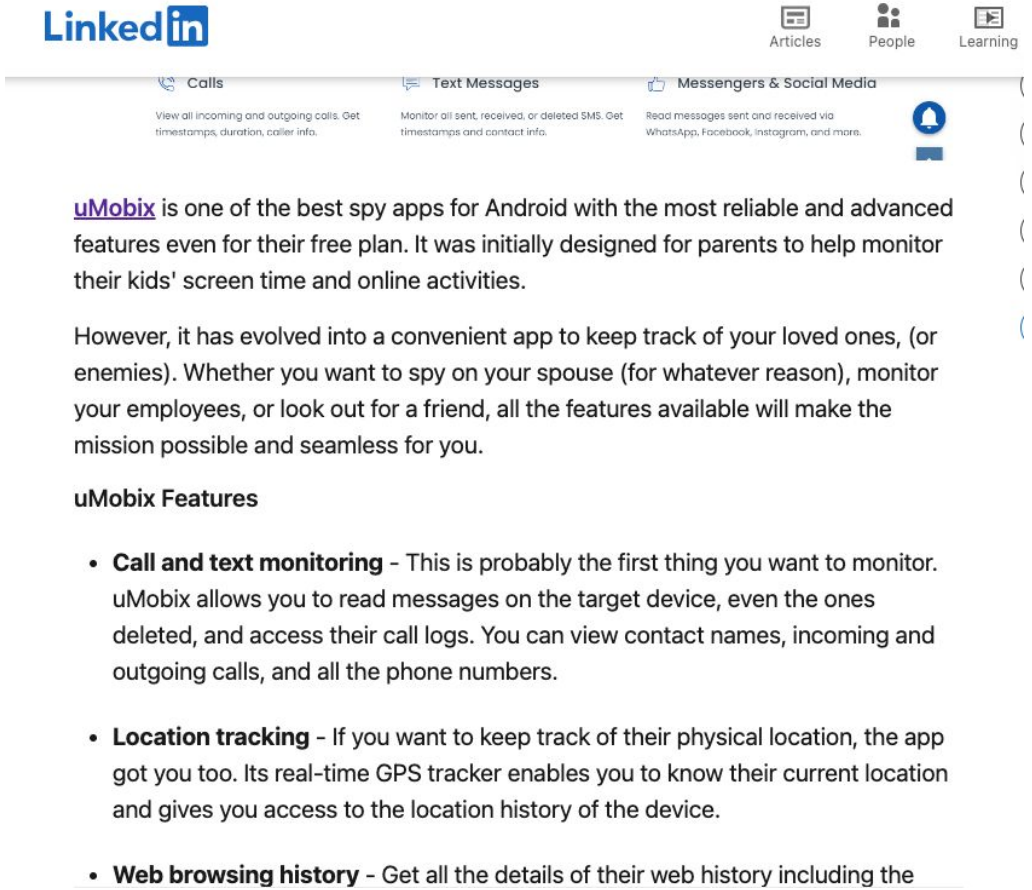
At least 180 journalists around the world have been selected as targets by clients of the cybersurveillance company NSO Group, according to a new Forbidden Stories investigation, published today.

By Phineas Rueckert
Reading time: 21m

THE PEGASUS PROJECT | July 18, 2021

https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/

Primeri aplikacij / Examples of apps



https://www.linkedin.com/pulse/best-spy-apps-android-without-access-target-phone-diana-moraa

V branje / To read

BBC Sign in Home News Sport Earth Reel Worklife

NEWS

Home | Israel-Gaza war | War in Ukraine | Climate | Video | World | UK | Business | Tech | Science

Tech

Stalkerware: The software that spies on your partner

25 October 2019

What happened when Joe let his colleague Joanne spy on him for two days?

By Joe Tidy
Cyber-security reporter

Amy says it all started when her husband seemed to know intimate details about her friends.

"He would drop snippets into conversations, such as knowing about Sarah's baby. Really private things that he shouldn't have known about. If I asked how he knew these things, he'd say I'd told him and accuse me of losing it," she says.

https://www.bbc.com/news/technology-50166147

Neželena programska oprema

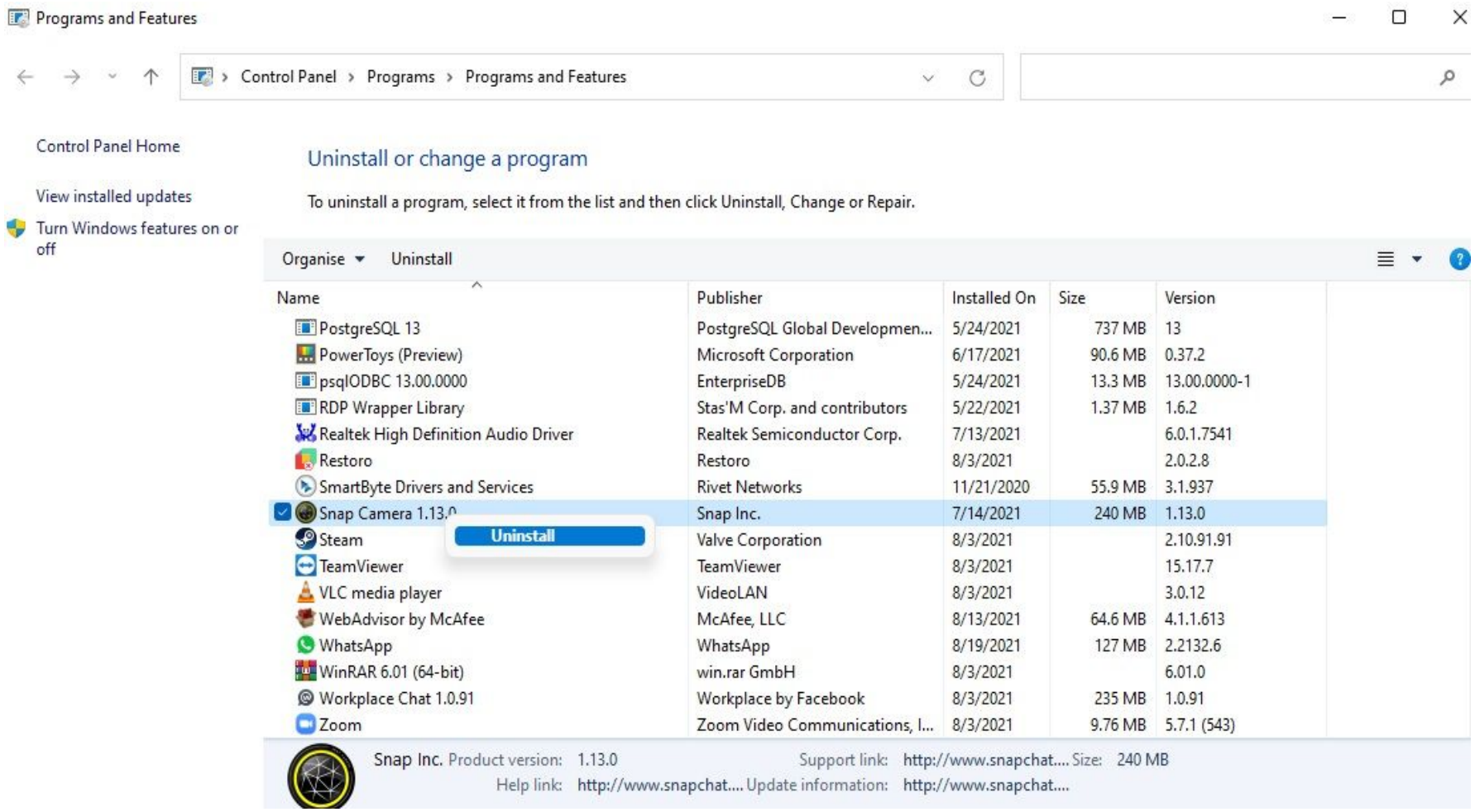
Junkware

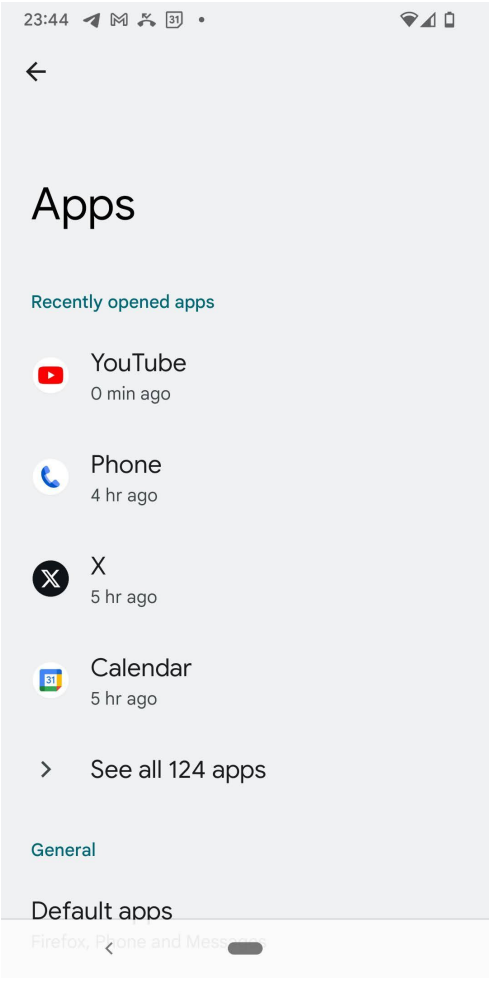
Naželena programska oprema / Junkware:

- Napihnjena programska oprema
- Prednaložena programska oprema
- Nepotrebna programska oprema
- Oglaševalni programi
- …
- Bloatware
- Bundled software
- Crapware
- Adware
- …

Preverimo naše računalnike in telefone

Check our computers and phones





Konec 1. dela / End of part 1

Matjaž Kljun
matjaz.kljun@upr.si
@_mkljun_

Vprašanja?

Matjaž Kljun
matjaz.kljun@upr.si
@_mkljun_

Questions?