



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,
- nepooblaščno razkritje informacij,
- krajo opreme,
- krajo informacij,
- poškodovanje opreme,
- sabotžo, 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?

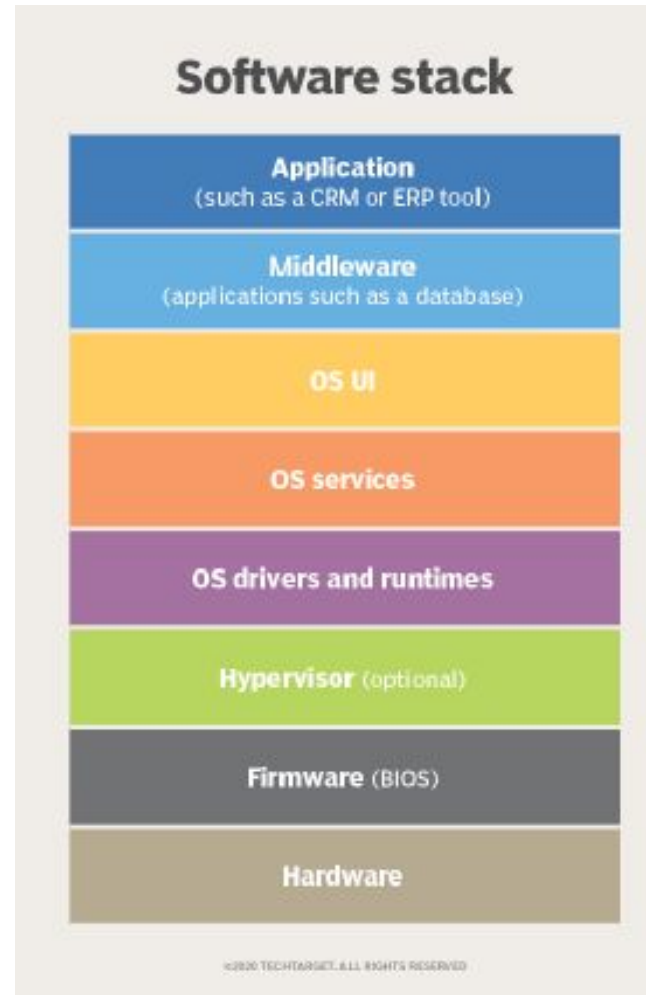
Uporabniška programska oprema

- 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

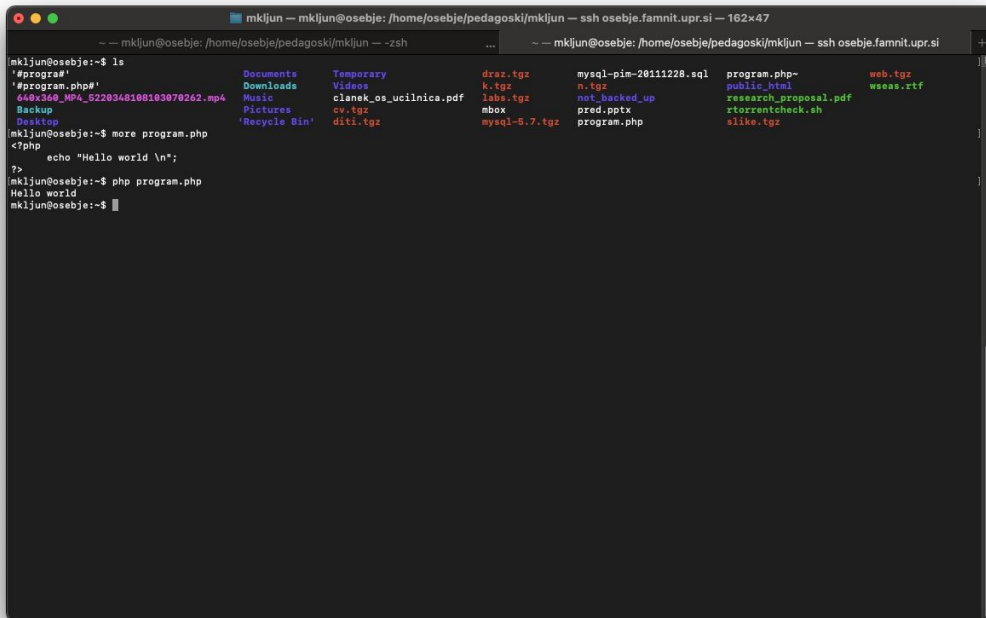
- Operating system service programs
 - Usually run in background

Operating system

Poskusimo dva jezika / Let's try two programming languages

PHP

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

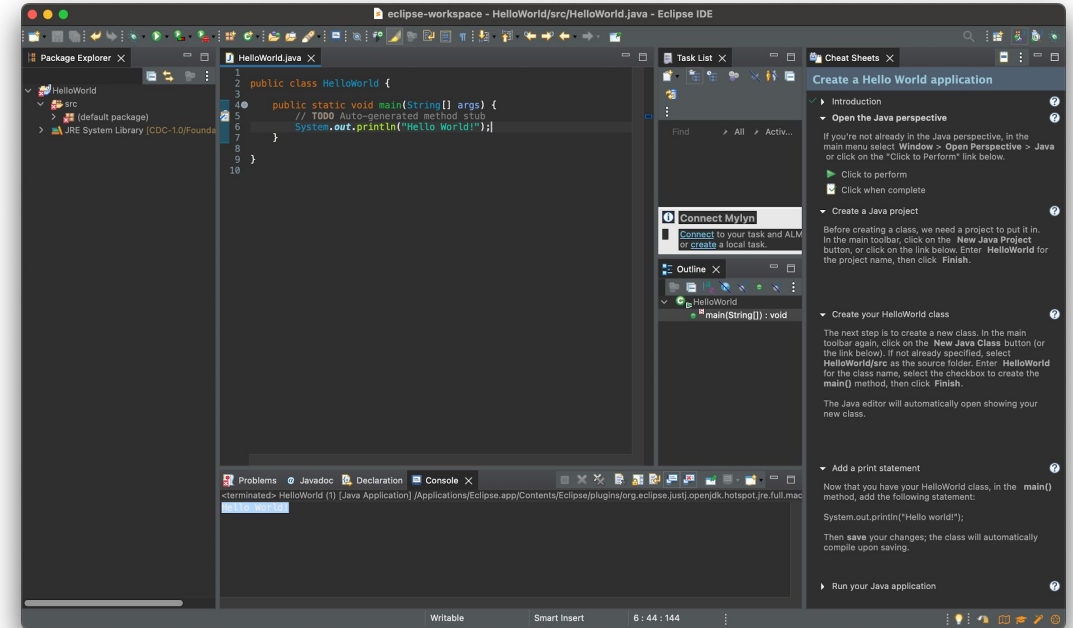


A terminal window showing the execution of a PHP script. The user runs 'ls' to list files, then 'more program.php' to view the code, and finally 'php program.php' to execute it, resulting in the output 'Hello world'.

```
mkijun@osebje:~$ ls
#program#
648x360_MP4_G228348188189078262.mp4
Backup
Desktop
Documents
Downloads
Music
Pictures
Temporary
drax.tgz
k.tgz
mysql-pim-20111228.sql
program.php
web.tgz
#program.php#
648x360_MP4_G228348188189078262.mp4
Backup
Desktop
Documents
Downloads
Music
Pictures
Temporary
drax.tgz
k.tgz
mysql-pim-20111228.sql
program.php
web.tgz
mkijun@osebje:~$ more program.php
<?php
    echo "Hello world \n";
?>
mkijun@osebje:~$ php program.php
Hello world
mkijun@osebje:~$
```

JAVA

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



A screenshot of the Eclipse IDE showing a Java class named 'HelloWorld'. The code is identical to the one shown above. The IDE interface includes a Package Explorer, a Task List, and a Cheat Sheets panel.

```
public class HelloWorld {
    public static void main(String[] args) {
        // TODO Auto-generated method stub
        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 (nekateri zagotavljajo določeno raven zaščite).
- Redno varnostno kopiramo in kopijo shranimo na:
 - nepovezanih nosilcih,
 - nosilcih samo za branje,
 - nosilcin z drugačnim datotečnim sistemom.
- Redno posodabljam 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,

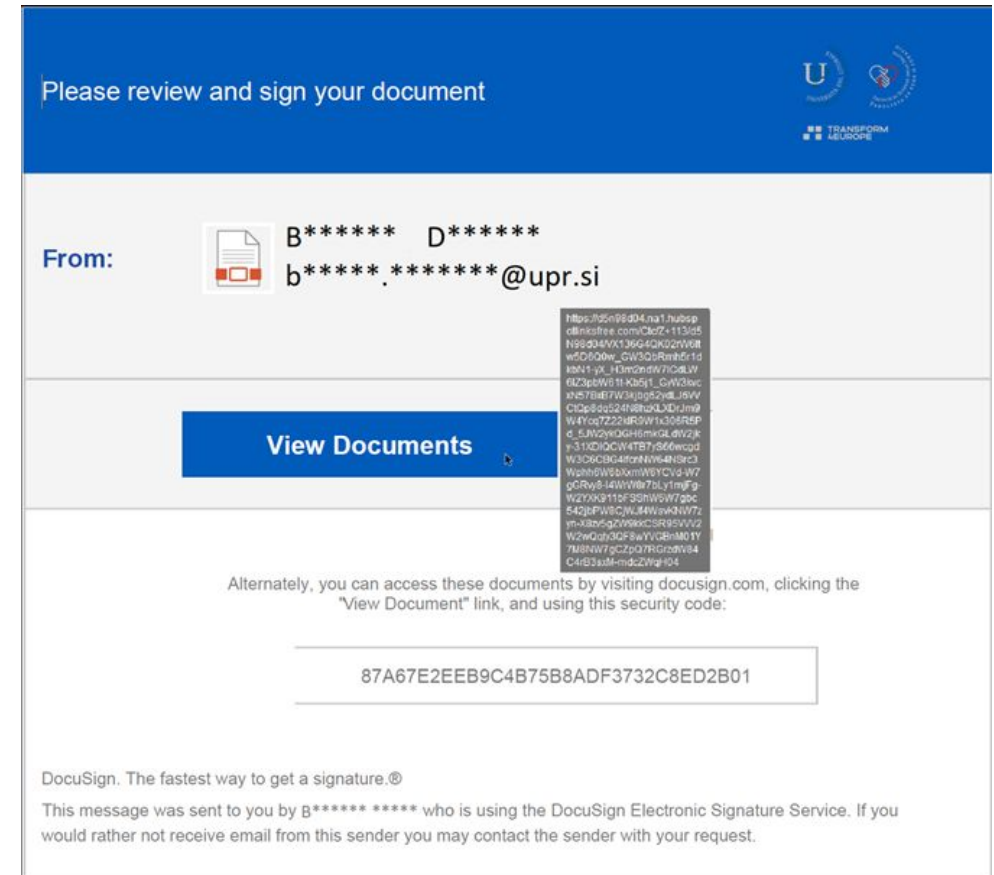
V zadnjem času smo na UP tarča zlonamernih elektronskih sporočil, s katerimi poskušajo vdreti v naš informacijski sistem.
Recently, at UP, we have been the target of malicious e-mails, with which they try to break into our information system.

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 ... kibernetška 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/LKUMRTL49g?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

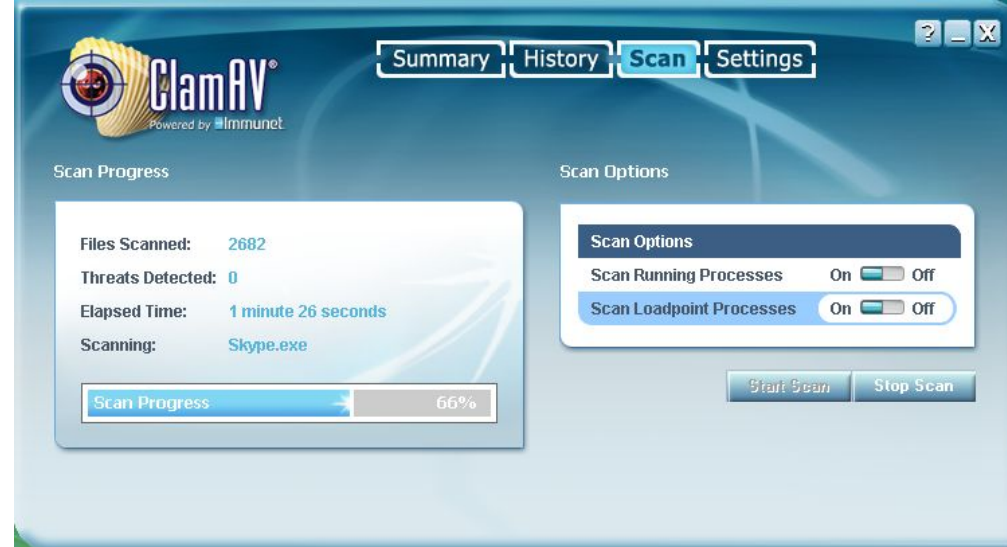
- Sesutje sistema
- Samodejno pošiljaje e-pošte
- Manjkajoče datoteke
- Počasno delovanje
- Pogoste okvare
- Visoka aktivnost na omrežju
- Malo prostora za shranjevanje
- Težave pri izklopu ali ponovnem zagonu
- Težave s programi in datotekami
- Nepravilno delovanje protivirusnih programov
- Sumljiva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

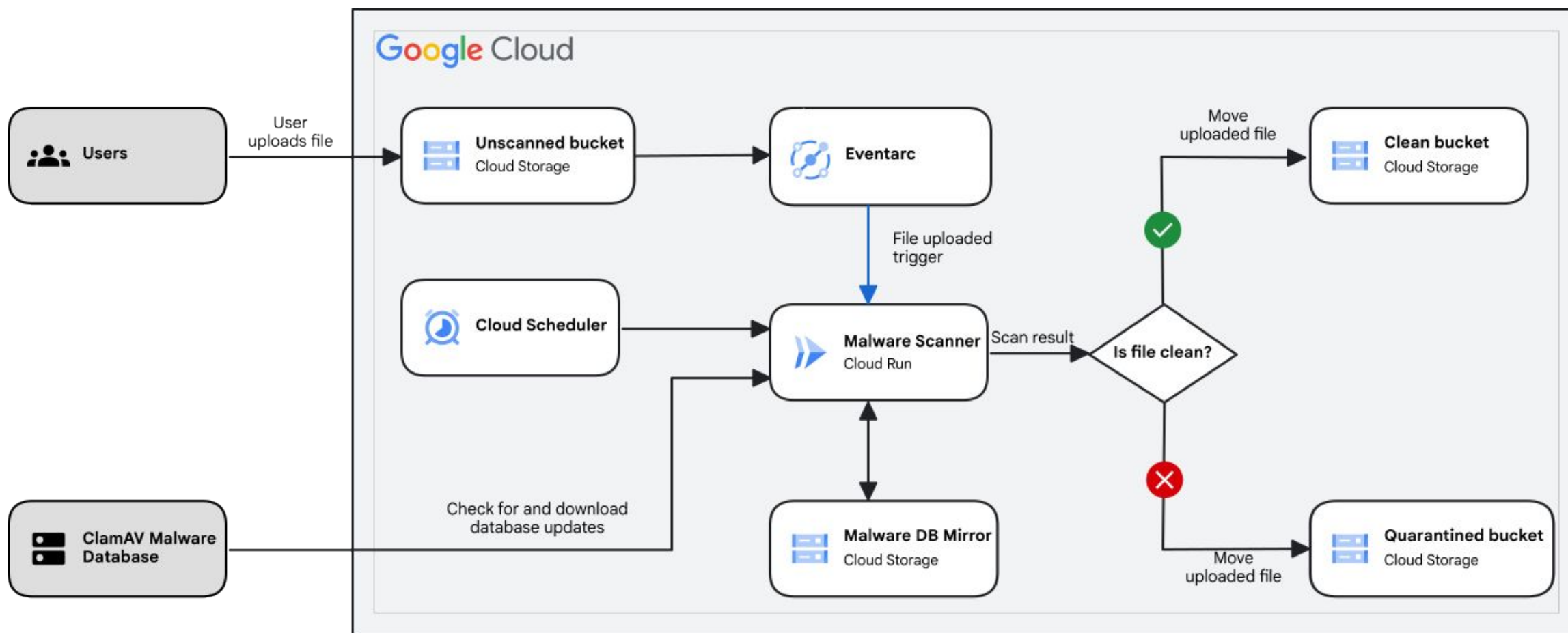
The image shows a Windows Security window with a sidebar on the left and a main content area. The sidebar lists various security features: Home, Virus & threat protection, Account protection, Firewall & network protection, App & browser control, Device security, Device performance & health, Family options, and Protection history. The main content area is titled "Security at a glance" and displays six security features with their status: Virus & threat protection (No action needed), Account protection (No action needed), App & browser control (No action needed), Device security (View status and manage hardware security features), Family options (Manage how your family uses their devices), and Protection history (View latest protection actions and recommendations). A large blue shield icon is visible in the background. A smaller, zoomed-in window of the "Virus & threat protection" settings is overlaid on the right. This window shows the "Virus & threat protection" section with a sub-menu on the left (Home, Virus & threat protection, Account protection, Firewall & network protection, App & browser control, Device security, Device performance & health, Family options, Settings). The main content of this window includes: "Protection for your device against threats.", "Current threats" (No current threats, Last scan: 9/29/2020 7:55 AM (quick scan), 0 threats found, Scan lasted 2 minutes 12 seconds, 41434 files scanned), a "Quick scan" button, "Scan options" (Allowed threats, Protection history - highlighted with a red box), "Virus & threat protection settings" (No action needed, Manage settings), and a "Windows Community videos" section with links for "Learn more about Virus & threat protection", "Have a question? Get help", "Who's protecting me? Manage providers", "Help improve Windows Security Give us feedback", and "Change your privacy settings View and change privacy settings for your Windows 10 device. Privacy settings, Privacy dashboard, Privacy Statement".

ClamAV

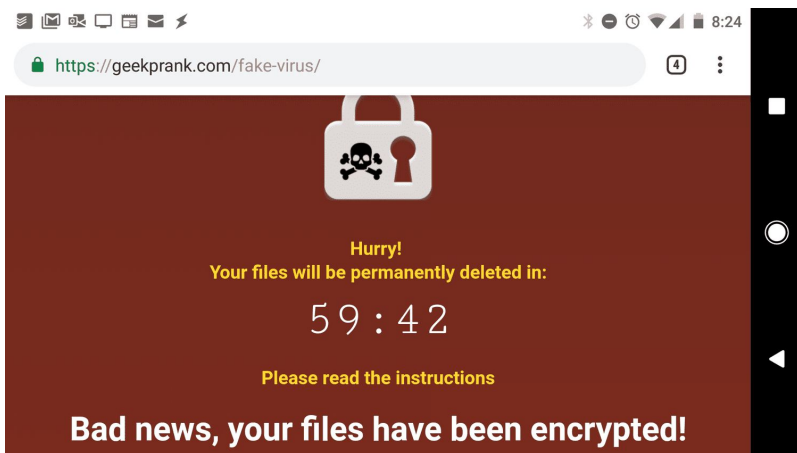
- Odprtokodni protivirusni program
- Različice skupnosti so na voljo za AIX, BSD, HP-UX, Linux, macOS, OpenVMS, OSF (Tru64), Solaris, Haiku in MS Windows.
- Opensource antivirus
- Third party versions available for AIX, BSD, HP-UX, Linux, macOS, OpenVMS, OSF (Tru64), Solaris, Haiku and MS Windows.



Primer v oblaku / An example in the cloud



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 ciljnim 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 veliko 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



- Komprimirana 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.

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 nepooblaščen 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 izsleditev 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.



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

BadBox 2

From: Tehnična pomoč Telekom Slovenije <tehnica.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 <tehnica.pomoc@telekom.si>

Pozdravljeni,

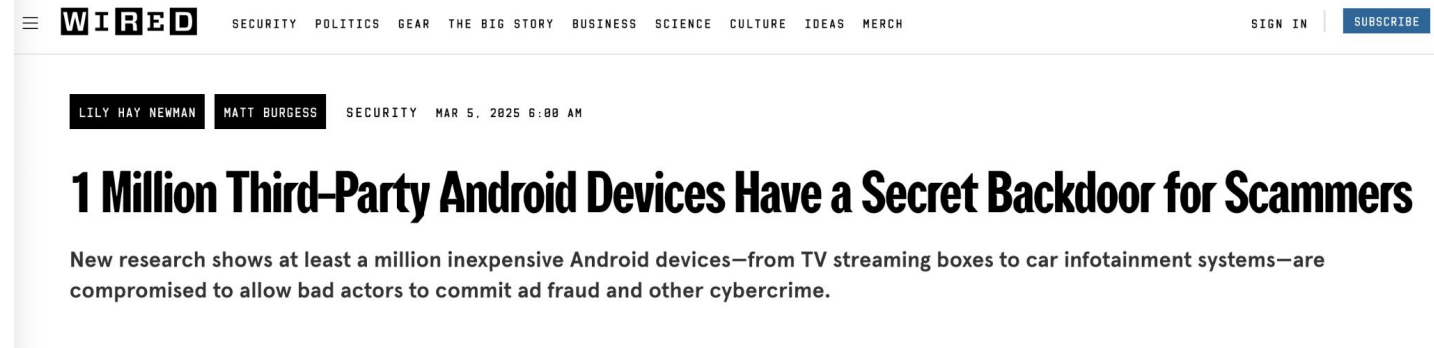
Prejeli smo obvestilo s strani državne obveščevalne službe za kibernetско varnost SI-CERT, da je bil vaš IP naslov prijavljen s strani drugih ponudnikov kot zlonameren oz. je opravljal aktivnosti značilne za okuženo omrežje. Glede na njihovo prijavo se je iz vašega IP naslova "89.142.95.162" kreirala 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](#)

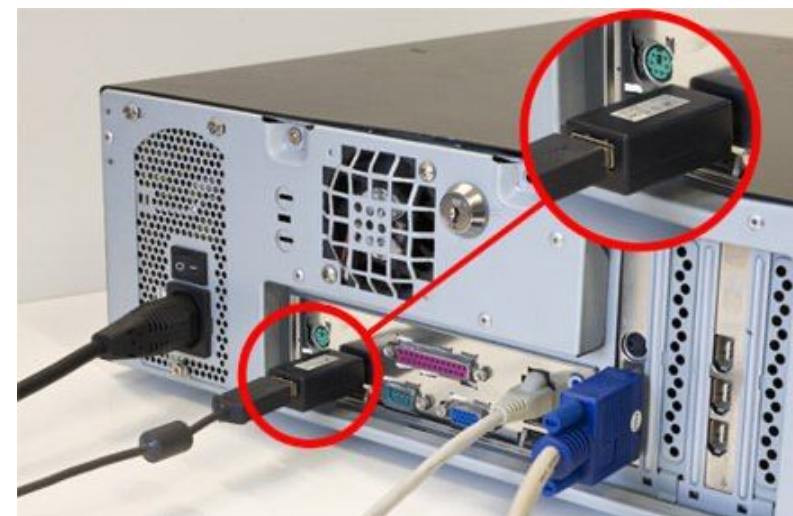


The screenshot shows the top portion of a Wired article. At the top left is the Wired logo. To its right is a navigation menu with categories: SECURITY, POLITICS, GEAR, THE BIG STORY, BUSINESS, SCIENCE, CULTURE, IDEAS, MERCH. On the far right are links for 'SIGN IN' and 'SUBSCRIBE'. Below the navigation is a dark header bar with the authors' names 'LILY HAY NEWMAN' and 'MATT BURGESS', followed by the category 'SECURITY' and the date 'MAR 5, 2025 6:00 AM'. The main headline is '1 Million Third-Party Android Devices Have a Secret Backdoor for Scammers'. Below the headline is a short introductory paragraph: 'New research shows at least a million inexpensive Android devices—from TV streaming boxes to car infotainment systems—are compromised to allow bad actors to commit ad fraud and other cybercrime.'

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.

```
C:\Program Files\PyKeylogger\logs\detailed_log\Keylogger-software-logfile-example.txt - Notepad++
File Edit Search View Encoding Language Settings Macro Run TextFX Plugins Window ?
Keylogger-software-logfile-example.txt
1 20100326|1239|C:\WINDOWS\Explorer.EXE|327786|SoftwareInstall|Run| Commando in run window
2 20100326|1239|C:\WINDOWS\Explorer.EXE|393322|SoftwareInstall|Run|https
://www.gmail.com[KeyName:Return]
3 20100326|1240|C:\Program Files\Mozilla
Firefox\firefox.exe|262710|SoftwareInstall|Private Browsing - Mozilla Firefox (Private
Browsing)|https://www.gmail.com[KeyName:Return]
4 20100326|1240|C:\Program Files\Mozilla Firefox\firefox.exe|262710|SoftwareInstall|Gmail:
Email from Google - Mozilla Firefox (Private Browsing)|accounts Do Not Tell !
5 20100326|1241|C:\Program Files\Mozilla Firefox\firefox.exe|262710|SoftwareInstall|Gmail
- Compose Mail - accounts@gmail.com - Mozilla Firefox (Private Browsing)| Hello John
[KeyName:Home] Dealer Room @wallstreettrade.com Confidential email. Hello,
John, [KeyName:Return] [KeyName:Return] Please use buy 1000 stock shares of our
company. [KeyName:Return] Don't tell anyone, because it will influence the sto
ck price. [KeyName:Return] And ofcourse it is illegal to trade stock with pre
knowledge : 0898989 :- ) [KeyName:Return] Use my credit card number
: [KeyName:Return] 1234 5678 9123 4567 [KeyName:Return] wich
6 20100326|1243|C:\Program Files\Mozilla Firefox\firefox.exe|262710|SoftwareInstall|Gmail
- Compose Mail - accounts@gmail.com - Mozilla Firefox (Private
Browsing)|ck. [KeyName:Return] The card security code on the back is :
123. [KeyName:Return] [KeyName:Return] Thanks, [KeyName:Return] Bob
7 20100326|1243|C:\Program Files\Mozilla
Firefox\firefox.exe|262710|SoftwareInstall|Mozilla Firefox (Private
Browsing)|www.playboy.com[KeyName:Return]
```



Poskusimo / Let's try it

Preprost program,
ki ne potrebuje
namestitve.

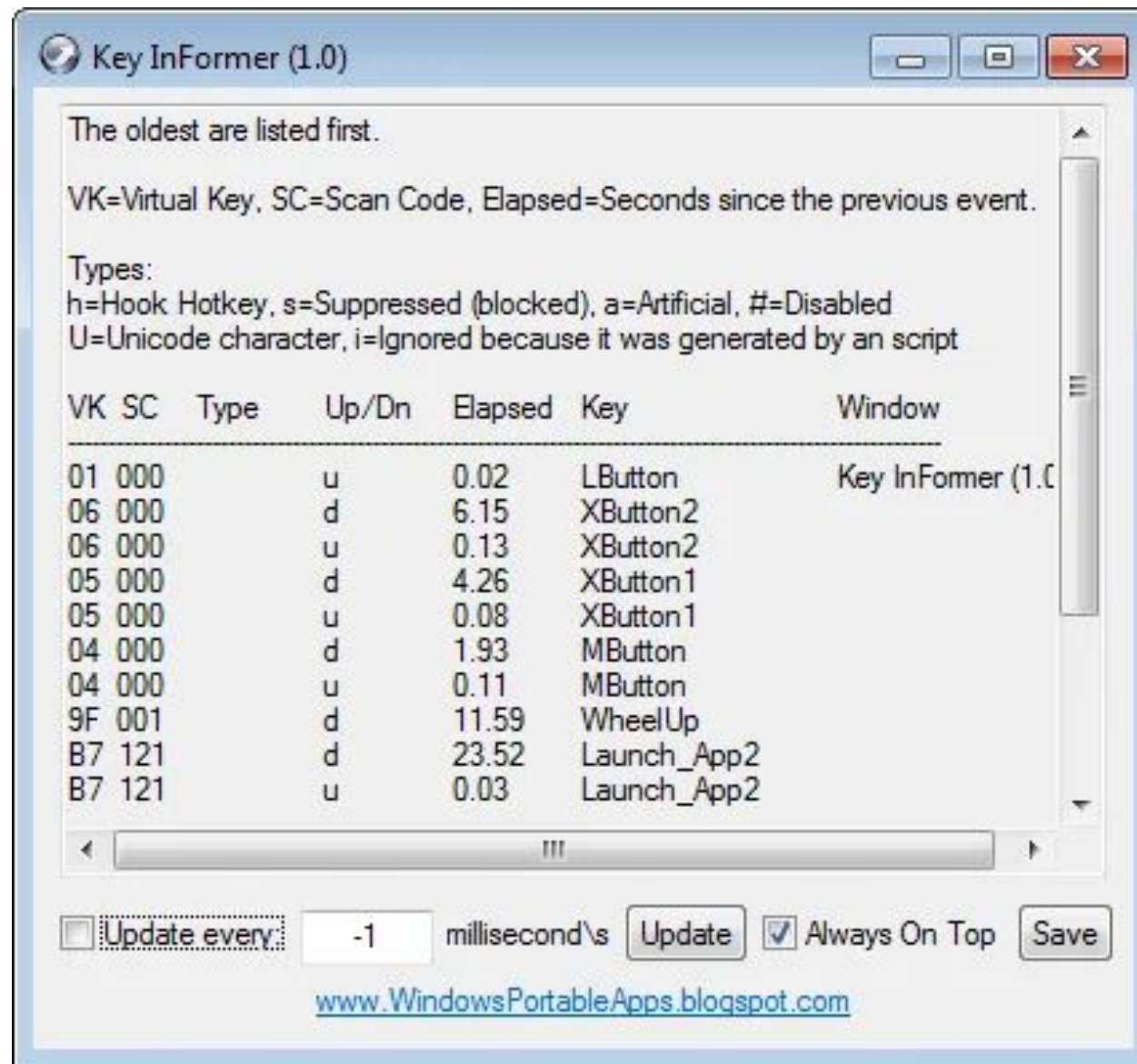
A simple software
that needs no
installation.

Ni skrit v ozadju.

It's not hidden in
the background.

Obstajajo veliko
bolj sofisticirani
programi.

There are much
more
sophisticated
programmes.



Primer strojnega beležnika tipkanja / An example of hw keylogger

AirDrive Forensic Keylogger

Ultra compact and discreet Wi-Fi hardware

Main page Keyloggers ▾ RS-232 & RS-485 ▾ Barcode, Keyboard, Mouse

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

Add to cart

Find out more

\$52.99 / €48.99

Add to cart

Find out more

\$74.99 / €68.99

Add to cart

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](#)



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.

V branje / To Read

forbidden stories | PROTECT YOUR STORIES

GET OUR NEWSLETTER

First Name

Last Name

Your email


OK

DONATE

f t e

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.



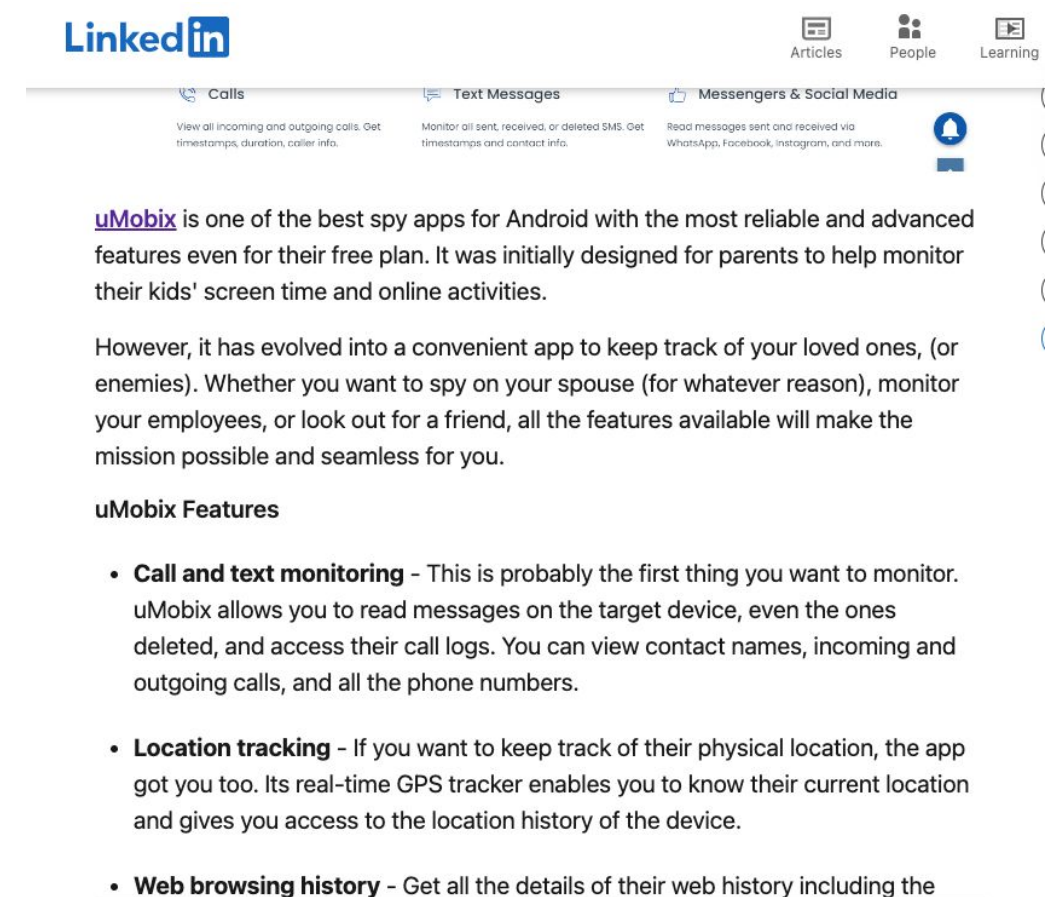
By Phineas Rueckert
Reading time: 21m

THE PEGASUS PROJECT | July 18, 2021

Primeri aplikacij / Examples of apps



The screenshot shows a LinkedIn article. At the top left is the LinkedIn logo. To the right are navigation icons for Articles, People, and Learning. The article title is "Best Spy Apps for Android without Access to Target Phone". Below the title is the author's name, "Diana Moraa", and a "Follow" button. The author's bio reads: "Skilled Content Marketing Copywriter, Editor, and Proofreader for B2B SaaS and Digital Marketing Companies". The article was published on Oct 3, 2023. The main text of the article begins with: "Are you worried about what your partner, child, or employee is up to on their Android phone? Do you want a way to monitor their online activity without having to touch their device? If so, you're in luck. There are a number of spy apps available that allow you to do just that. These apps can be a valuable tool for parents, employers, and anyone else who needs to monitor the online activity of another person. In this article, we take a look at the best spy apps for Android without access to the target phone. We'll discuss the features of each app, as well as its pros and cons. Let's dive right in."



The screenshot shows a LinkedIn article. At the top left is the LinkedIn logo. To the right are navigation icons for Articles, People, and Learning. Below the navigation bar are three tabs: "Calls", "Text Messages", and "Messengers & Social Media". The article text reads: "uMobix is one of the best spy apps for Android with the most reliable and advanced features even for their free plan. It was initially designed for parents to help monitor their kids' screen time and online activities. However, it has evolved into a convenient app to keep track of your loved ones, (or enemies). Whether you want to spy on your spouse (for whatever reason), monitor your employees, or look out for a friend, all the features available will make the mission possible and seamless for you." Below the text is a section titled "uMobix Features" with a bulleted list:

- **Call and text monitoring** - This is probably the first thing you want to monitor. uMobix allows you to read messages on the target device, even the ones deleted, and access their call logs. You can view contact names, incoming and outgoing calls, and all the phone numbers.
- **Location tracking** - If you want to keep track of their physical location, the app got you too. Its real-time GPS tracker enables you to know their current location and gives you access to the location history of the device.
- **Web browsing history** - Get all the details of their web history including the

V branje / To read



The image shows a screenshot of a BBC News article. At the top, the BBC logo is on the left, and navigation links for Home, News, Sport, Earth, Reel, and Worklife are on the right. Below the navigation is a red banner with the word 'NEWS' in white. Underneath the banner is a secondary navigation bar with links for Home, Israel-Gaza war, War in Ukraine, Climate, Video, World, UK, Business, Tech, and Science. The 'Tech' link is underlined. The main headline is 'Stalkerware: The software that spies on your partner'. Below the headline is the date '25 October 2019' and a share icon. A sub-headline reads 'What happened when Joe let his colleague Joanne spy on him for two days?'. The author is 'By Joe Tidy', a cyber-security reporter. A short paragraph of text follows: 'Amy says it all started when her husband seemed to know intimate details about her friends.' Below this is a quote: '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.

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.

Neželená programská oprema

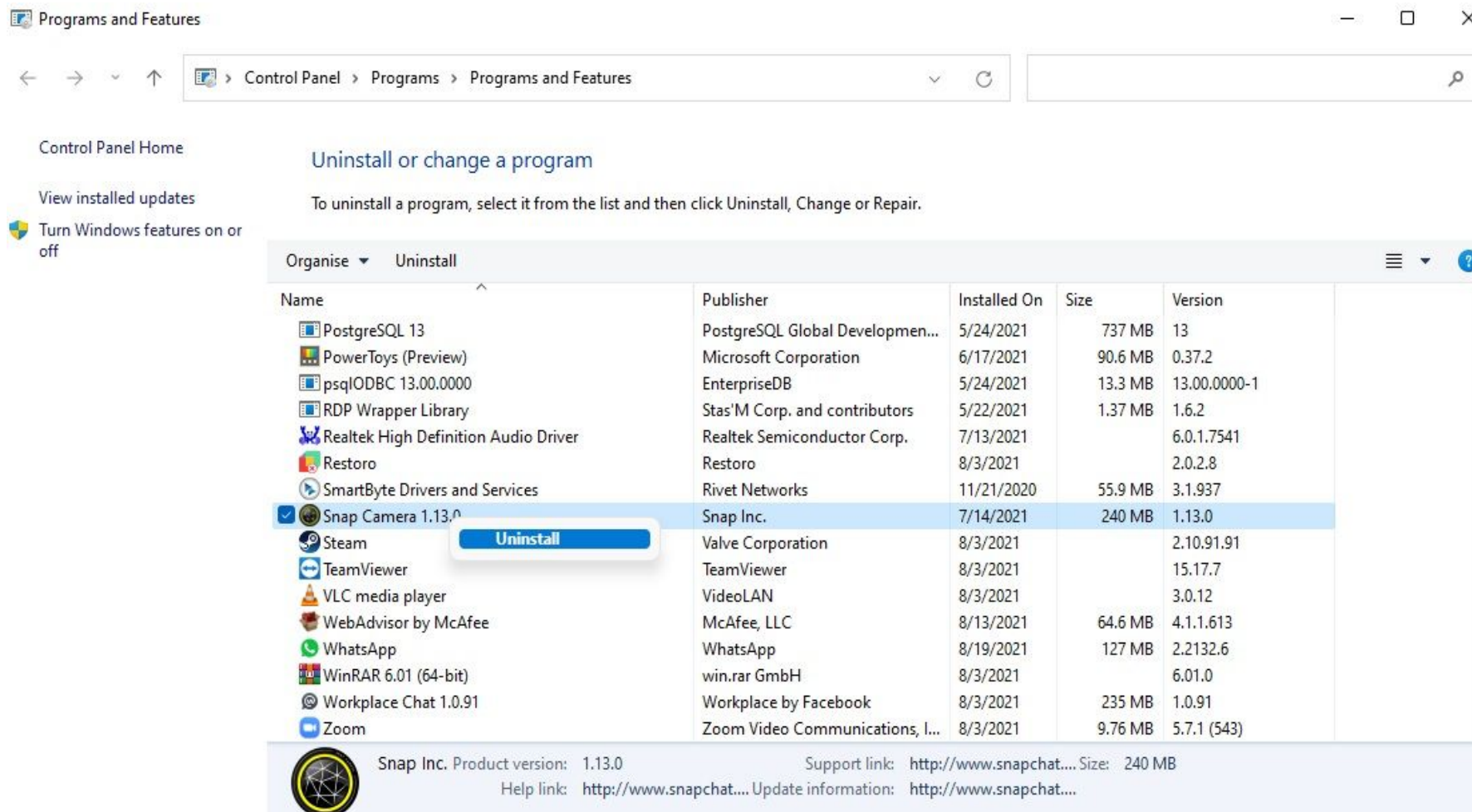
Junkware

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



Programs and Features

Control Panel > Programs > Programs and Features

Control Panel Home

View installed updates

Turn Windows features on or off

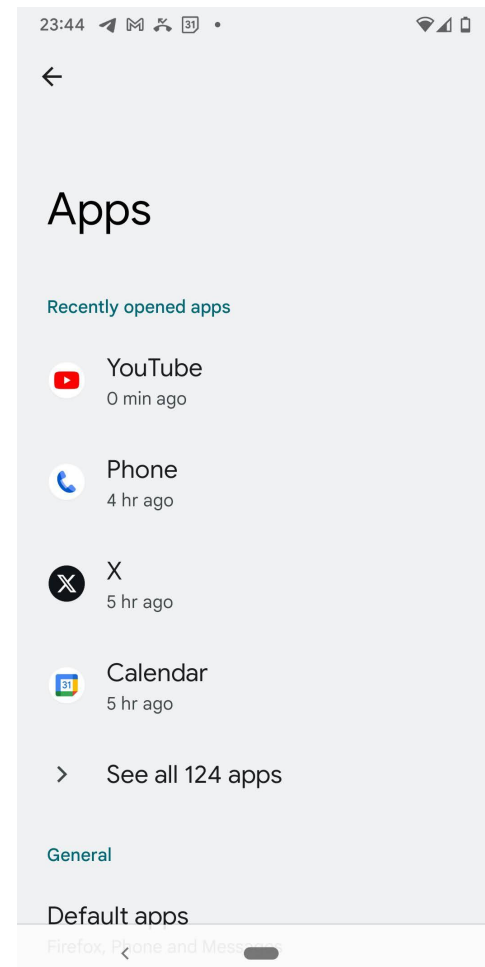
Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change or Repair.

Name	Publisher	Installed On	Size	Version
PostgreSQL 13	PostgreSQL Global Developmen...	5/24/2021	737 MB	13
PowerToys (Preview)	Microsoft Corporation	6/17/2021	90.6 MB	0.37.2
psqlODBC 13.00.0000	EnterpriseDB	5/24/2021	13.3 MB	13.00.0000-1
RDP Wrapper Library	Stas'M Corp. and contributors	5/22/2021	1.37 MB	1.6.2
Realtek High Definition Audio Driver	Realtek Semiconductor Corp.	7/13/2021		6.0.1.7541
Restoro	Restoro	8/3/2021		2.0.2.8
SmartByte Drivers and Services	Rivet Networks	11/21/2020	55.9 MB	3.1.937
Snap Camera 1.13.0	Snap Inc.	7/14/2021	240 MB	1.13.0
Steam	Valve Corporation	8/3/2021		2.10.91.91
TeamViewer	TeamViewer	8/3/2021		15.17.7
VLC media player	VideoLAN	8/3/2021		3.0.12
WebAdvisor by McAfee	McAfee, LLC	8/13/2021	64.6 MB	4.1.1.613
WhatsApp	WhatsApp	8/19/2021	127 MB	2.2132.6
WinRAR 6.01 (64-bit)	win.rar GmbH	8/3/2021		6.01.0
Workplace Chat 1.0.91	Workplace by Facebook	8/3/2021	235 MB	1.0.91
Zoom	Zoom Video Communications, I...	8/3/2021	9.76 MB	5.7.1 (543)

Uninstall

Snap Inc. Product version: 1.13.0 Support link: <http://www.snapchat...> Size: 240 MB
Help link: <http://www.snapchat...> Update information: <http://www.snapchat...>



23:44

Apps

Recently opened apps

- YouTube
0 min ago
- Phone
4 hr ago
- X
5 hr ago
- Calendar
5 hr ago

> See all 124 apps

General

Default apps

Firefox, Phone and Mess...

Konec 1. dela / End of part 1

Matjaž Kljun

matjaz.kljun@upr.si

@_mkljun_

Vprašanja?

Matjaž Kljun

matjaz.kljun@upr.si

@_mkljun_

Questions?

