ZÁPADOČESKÁ
UNIVERZITA
V PLZNI

Řešení bezpečnostních incidentů na ZČU

Viktor Ferus / 2023

Úvod

- Síť WEBnet
  - Bezdrátová síť - eduroam, zcu-mobile
  - Pevná síť - učebny, katedry, koleje
- Západočeská univerzita v Plzni
  - Odpovědnost za svou síť
    - Funkční pro uživatele
    - Bezproblémová pro zbytek internetu
  - Pravidla používání sítě WEBnet (10R/2008)
    - Základní návod co (ne)dělat

Ideální stav

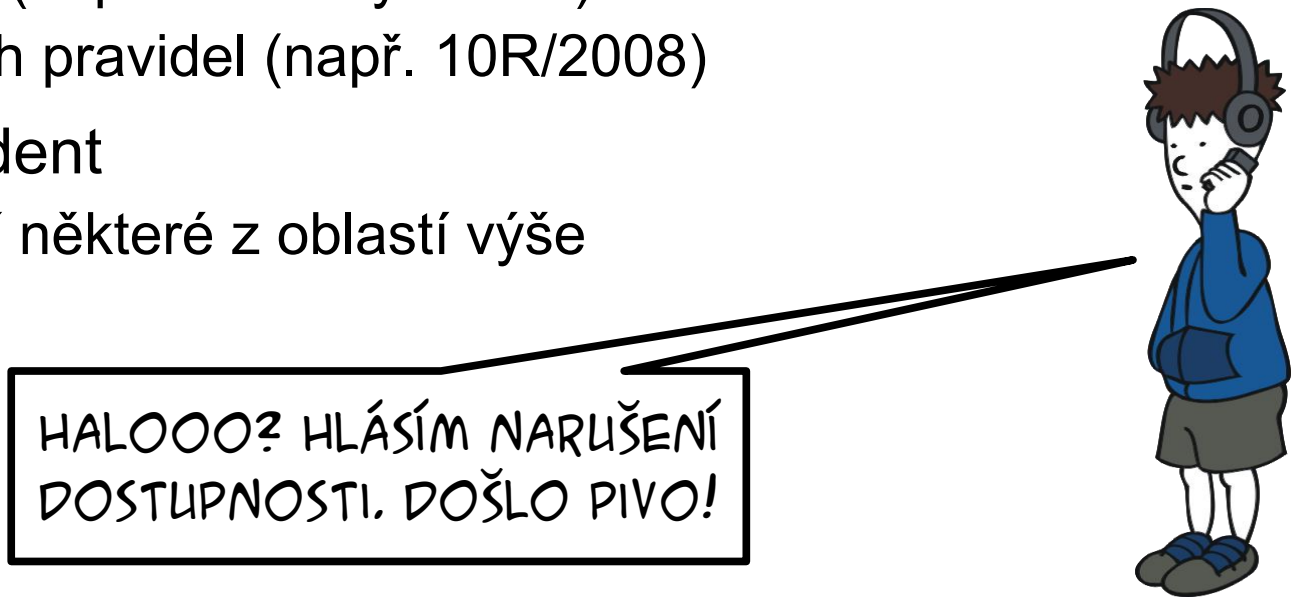
Ideální stav

- Všichni uživatelé dodržují pravidla
  - Zákony platné v ČR
  - Licenční a jiná ujednání
  - Univerzitní směrnice
  - Pravidlo „zdravého rozumu“
- Připojená zařízení jsou
  - Pečlivě udržovaná
  - Zabezpečená
  - Používající legální SW
- Nikdo nemá zlé úmysly

Reálný stav
opak ideálního

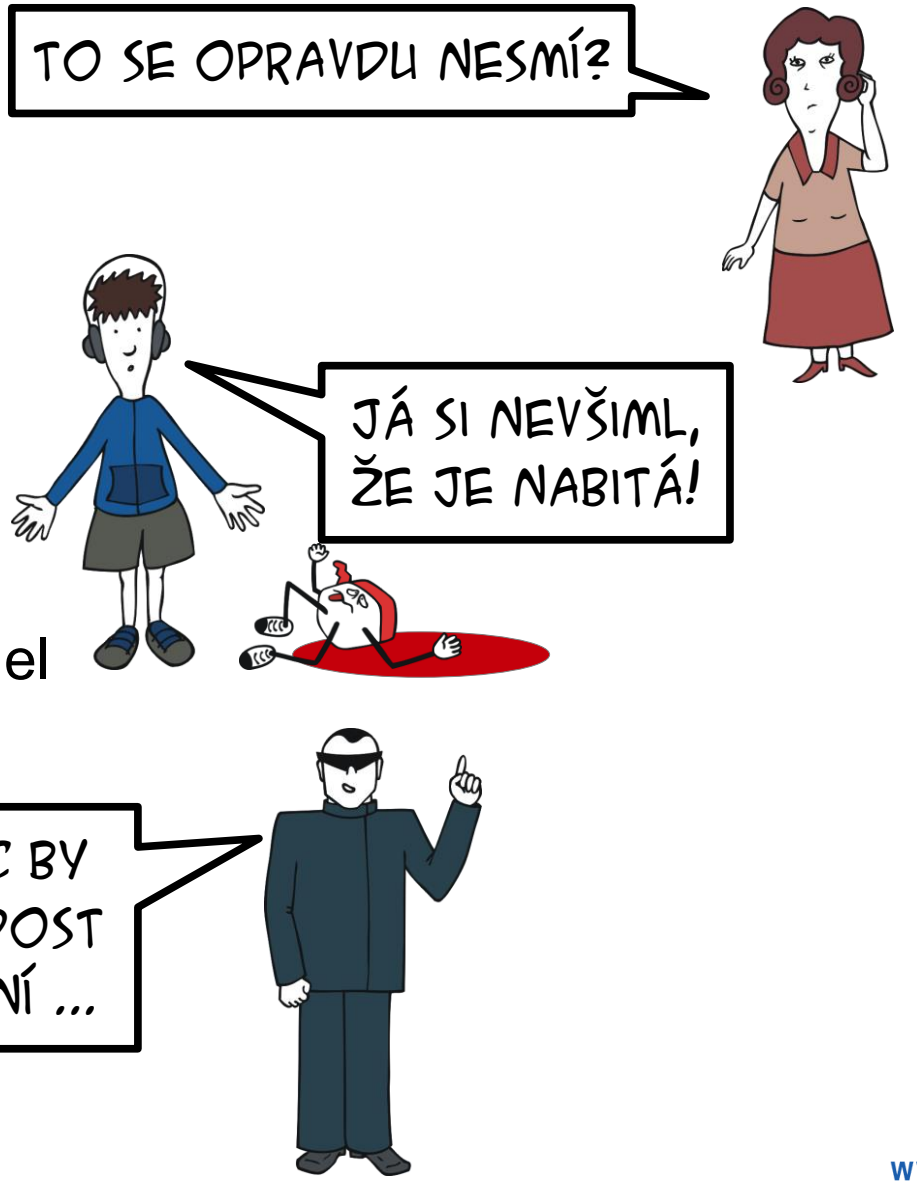
Co se může pokazit

- Oblasti možných problémů
  - Dostupnost (např. DoS/DDoS útok)
  - Integrita (např. zavirování počítače)
  - Důvěrnost (např. neoprávněný přístup)
  - Porušení zákonů (např. autorský zákon)
  - Porušení vnitřních pravidel (např. 10R/2008)
- Bezpečnostní incident
  - Obecně narušení některé z oblastí výše

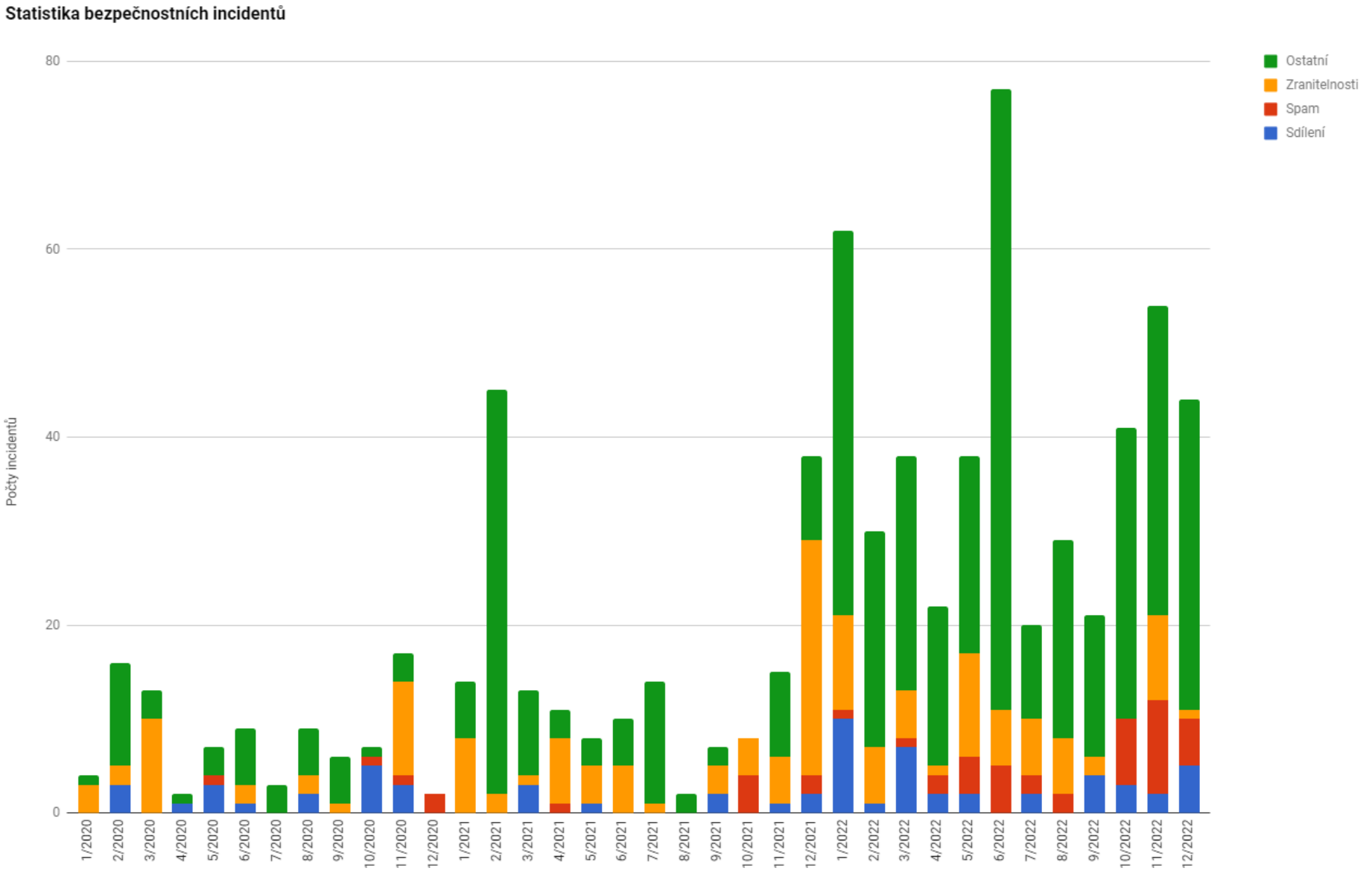


Z čeho pramení vznik incidentu

- Neznalost
  - Nemám ponětí, co dělám
  - Neznám důsledky
- Nedbalost
  - Opomenutí
- Úmysl
  - Záměrná aktivita
  - Záměrné ignorování pravidel



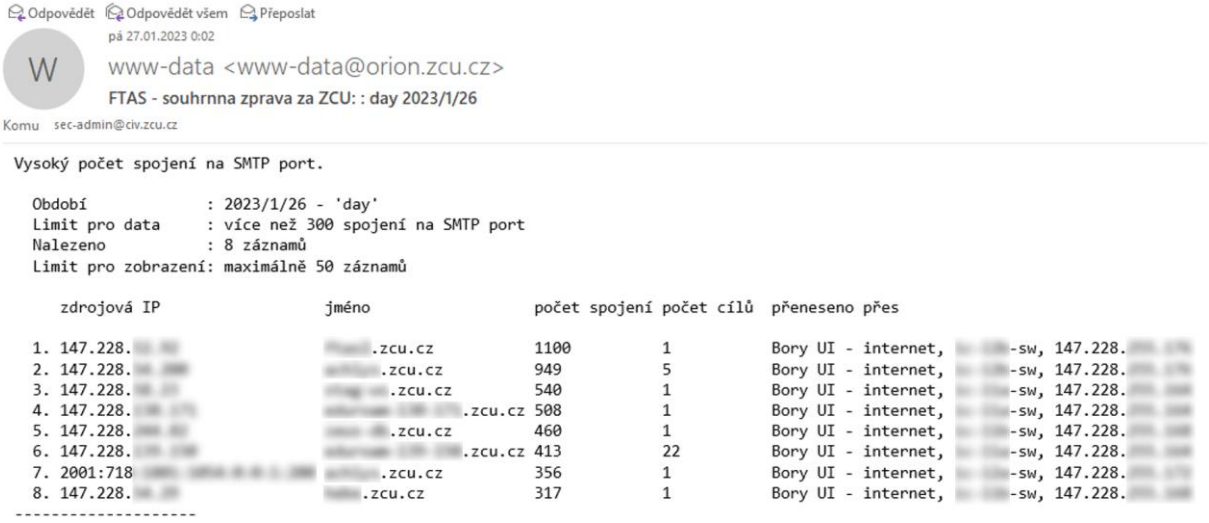
Statistika 2020 - 2022



Řešení incidentu

Zjištění

- Interní detekční systémy
- Sledujeme L3 a L4
- L7 inspekci neprovádíme



Odpovědět Odpovědět všem Přeposlat

pá 27.01.2023 0:02

W www-data <www-data@orion.zcu.cz>

FTAS - souhrnna zprava za ZCU: : day 2023/1/26

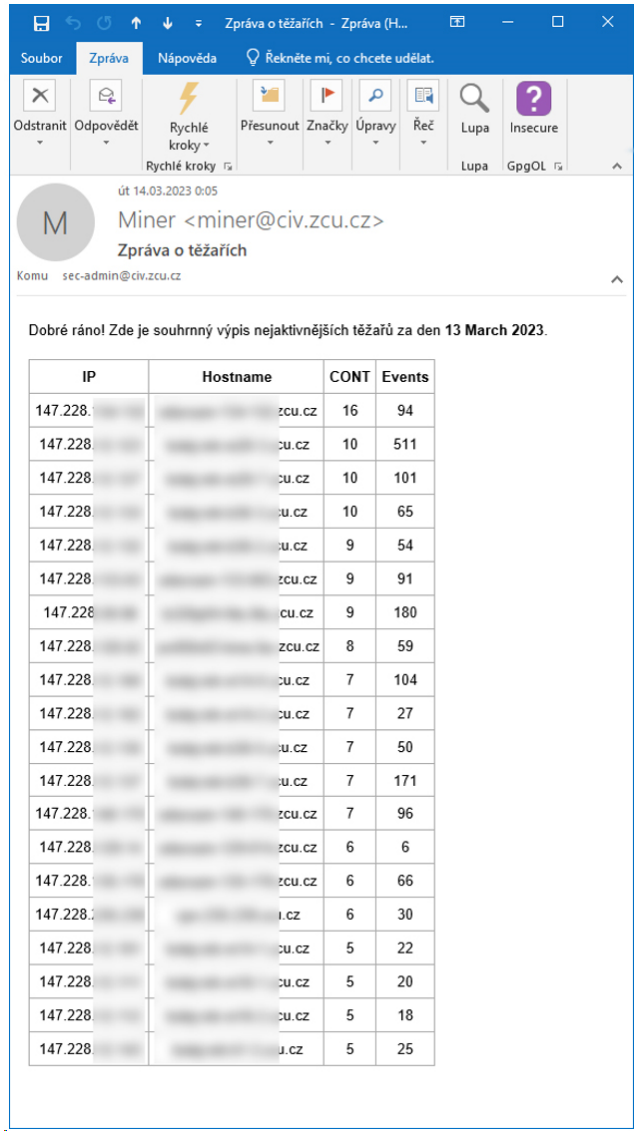
Komu sec-admin@civ.zcu.cz

Vysoký počet spojení na SMTP port.

```
  Období             : 2023/1/26 - 'day'
  Limit pro data     : více než 300 spojení na SMTP port
  Nalezeno           : 8 záznamů
  Limit pro zobrazení: maximálně 50 záznamů

     zdrojová IP                jméno                 počet spojení počet cílů  přeneseno přes

  1. 147.228.                   .zcu.cz               1100          1           Bory UI - internet,  -sw, 147.228.
  2. 147.228.                   .zcu.cz               949           5           Bory UI - internet,  -sw, 147.228.
  3. 147.228.                   .zcu.cz               540           1           Bory UI - internet,  -sw, 147.228.
  4. 147.228.                   .zcu.cz               508           1           Bory UI - internet,  -sw, 147.228.
  5. 147.228.                   .zcu.cz               460           1           Bory UI - internet,  -sw, 147.228.
  6. 147.228.                   .zcu.cz               413           22          Bory UI - internet,  -sw, 147.228.
  7. 2001:718                   .zcu.cz               356           1           Bory UI - internet,  -sw, 147.228.
  8. 147.228.                   .zcu.cz               317           1           Bory UI - internet,  -sw, 147.228.
--------------------
```



Zpráva o těžařích - Zpráva (H...

Soubor Zpráva Nápověda Řekněte mi, co chcete udělat.

Odstranit Odpovědět Rychlé kroky Přesunout Značky Úpravy Řeč Lupa Insecure

Rychlé kroky Lupa GpgOL

M

út 14.03.2023 0:05

Miner <miner@civ.zcu.cz>

Zpráva o těžařích

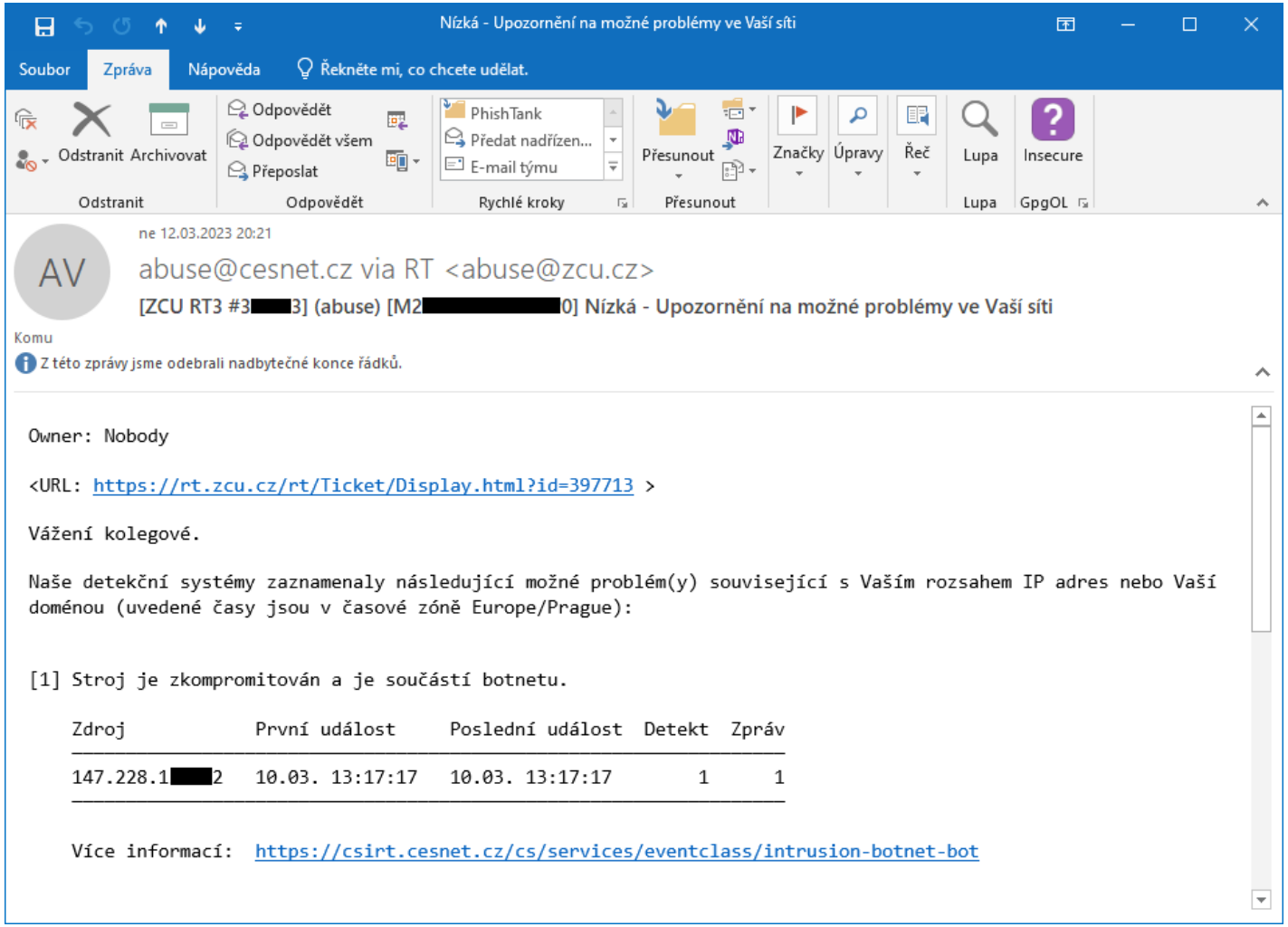
Komu sec-admin@civ.zcu.cz

Dobré ráno! Zde je souhrnný výpis nejaktivnějších těžařů za den **13 March 2023**.

IP	Hostname	CONT	Events
147.228.	zcu.cz	16	94
147.228.	cu.cz	10	511
147.228.	cu.cz	10	101
147.228.	u.cz	10	65
147.228.	u.cz	9	54
147.228.	zcu.cz	9	91
147.228.	cu.cz	9	180
147.228.	zcu.cz	8	59
147.228.	cu.cz	7	104
147.228.	cu.cz	7	27
147.228.	u.cz	7	50
147.228.	u.cz	7	171
147.228.	zcu.cz	7	96
147.228.	zcu.cz	6	6
147.228.	zcu.cz	6	66
147.228.	.cz	6	30
147.228.	cu.cz	5	22
147.228.	cu.cz	5	20
147.228.	cu.cz	5	18
147.228.	u.cz	5	25

Zjištění

- Externí detekční systémy



Nízká - Upozornění na možné problémy ve Vaší síti

Soubor | Zpráva | Nápověda | Řekněte mi, co chcete udělat.

Odstranit | Archivovat | Odpovědět | Odpovědět všem | Přeposlat | PhishTank | Předat nadřízen... | E-mail týmu | Přesunout | Značky | Úpravy | Řeč | Lupa | Insecure

Odstranit | Odpovědět | Rychlé kroky | Přesunout | Lupa | GpgOL

ne 12.03.2023 20:21

AV

abuse@cesnet.cz via RT <abuse@zcu.cz>

[ZCU RT3 #3[redacted]3] (abuse) [M2[redacted]0] Nízká - Upozornění na možné problémy ve Vaší síti

Komu

Z této zprávy jsme odebrali nadbytečné konce řádků.

Owner: Nobody

<URL: https://rt.zcu.cz/rt/Ticket/Display.html?id=397713 >

Vážení kolegové.

Naše detekční systémy zaznamenaly následující možné problém(y) související s Vaším rozsahem IP adres nebo Vaší doménou (uvedené časy jsou v časové zóně Europe/Prague):

[1] Stroj je zkompromitován a je součástí botnetu.

Zdroj	První událost	Poslední událost	Detekt	Zpráv
147.228.1[redacted]2	10.03. 13:17:17	10.03. 13:17:17	1	1

Více informací: https://csirt.cesnet.cz/cs/services/eventclass/intrusion-botnet-bot

Zjištění

Externí hlášení

Odpovědět Odpovědět všem Přeposlat

so 25.02.2023 15:05

ND NFOservers.com DDoS notifier via RT <abuse@zcu.cz>

[ZCU RT3 #[redacted]] (abuse) Compromised host used for an attack: 147.228.[redacted] [~423 Mbps]

Komu

Owner: Nobody

<URL: https://rt.zcu.cz/rt/Ticket/Display.html?id=396698 >

An IP address (147.228.[redacted]) under your control appears to have attacked one of our customers as part of a coordinated DDoS botnet. We manually reviewed the captures from this attack and do not believe that your IP address was spoofed, based on the limited number of distinct hosts attacking us, the identicality of many attacking IP addresses to ones we've seen in the past, and the non-random distribution of IP addresses.

It is possible that this host is one of the following, from the responses that others have sent us:

- A compromised router, such as a D-Link that is running with WAN access enabled; a China Telecom which still allows a default admin username and password; a Netis, with a built-in internet-accessible backdoor (http://blog.trendmicro.com/trendlabs-security-intelligence/netis-routers-leave-wide-open-backdoor/); or one running an old AirOS version with a vulnerable and exposed administrative interface
- An IPTV device that is vulnerable to compromise (such as HTV), either directly through the default firmware or through a trojan downloaded app
- A compromised webhost, such as one running a vulnerable version of Drupal (for instance, using the vulnerability discussed at https://groups.drupal.org/security/faq-2018-002), WordPress, phpMyAdmin, or zPanel
- A compromised DVR, such as a "Hikvision" brand device (ref: https://www.hikvision.com/en/support/cybersecurity/security-advisory/security-notification-command-injection-vulnerability-in-some-hikvision-products/security-notification-command-injection-vulnerability-in-some-hikvision-products/)
- A compromised IPMI device, such as one made by Supermicro (possibly because it uses the default U/P of ADMIN/ADMIN or because its password was found through an exploit described at http://arstechnica.com/security/2014/06/at-least-32000-servers-broadcast-admin-passwords-in-the-clear-advisory-warns/)
- A compromised Xerox-branded device
- Some other compromised standalone device
- A server with an insecure password that was brute-forced, such as through SSH or RDP
- A server running an improperly secured Hadoop installation
- A server running a pre-13.10.3 GitLab instance that is vulnerable to CVE-2021-22205
- A compromised Microsoft DNS server (through the July 2020 critical vulnerability)

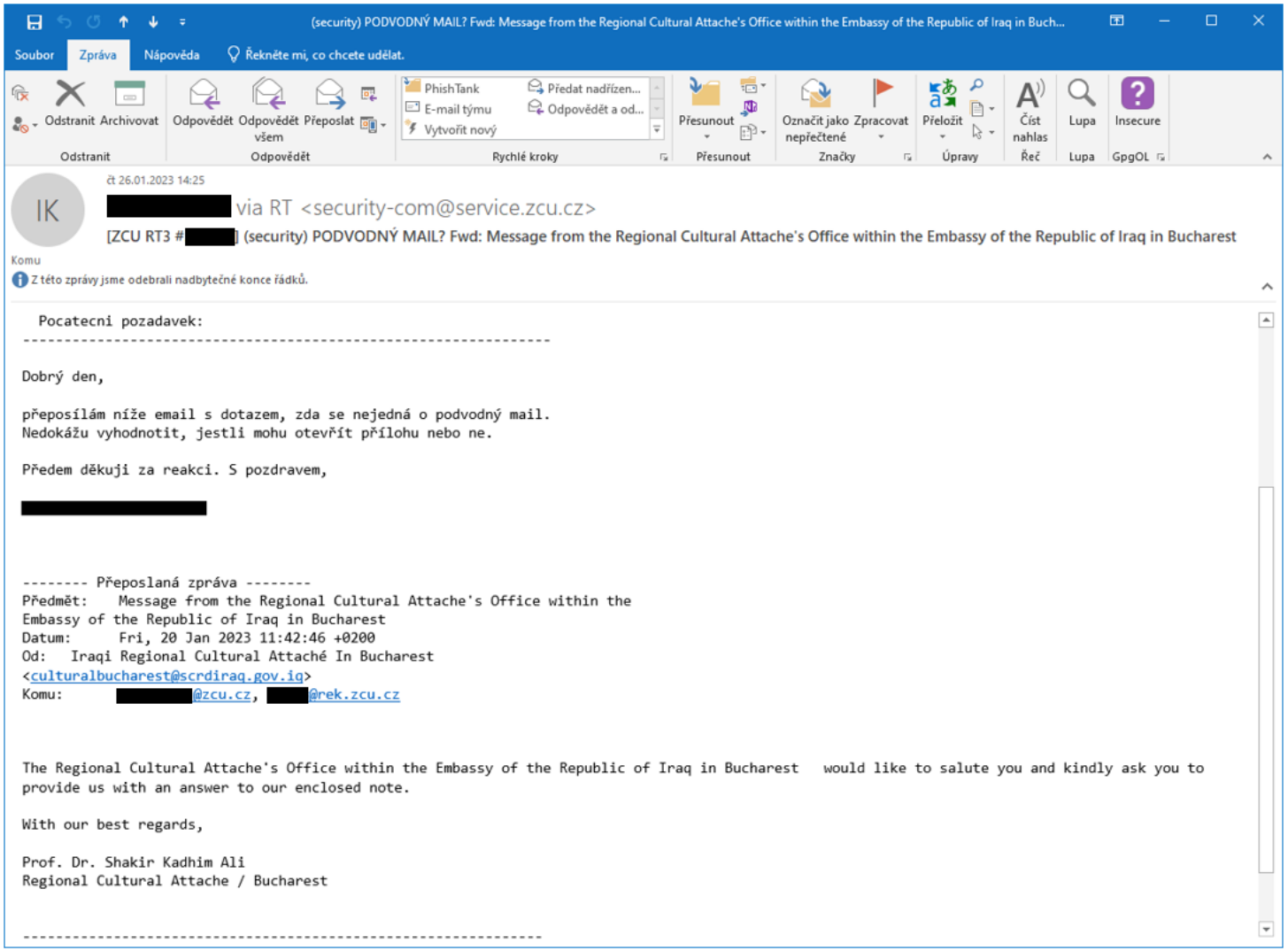
The overall botnet attack was Nx10Gbps in size (with traffic from your host as well as some others) and caused significant packet loss for our clients due to external link saturation. It required an emergency null-route operation on our side to mitigate.

Attacks like this are usually made very short, intentionally, so that they are not as noticeable and slip past certain automatic mitigation systems. From your side, you would be able to observe the attack as a burst of traffic that likely saturated the network adapter of the source device for perhaps 30 seconds. Since the source device is a member of a botnet that is being used for many attacks, you will see many other mysterious bursts of outbound traffic, as well.

This is example traffic from the IP address, as interpreted by the "tcpdump" utility and captured by our router during the attack. Source and destination IP addresses, protocols, and ports are included.

Zjištění

- Interní hlášení



(security) PODVODNÝ MAIL? Fwd: Message from the Regional Cultural Attache's Office within the Embassy of the Republic of Iraq in Buch...

Soubor | Zpráva | Nápověda | Řekněte mi, co chcete udělat.

Odstranit | Archivovat | Odpovědět | Odpovědět všem | Přeposlat | PhishTank | E-mail týmu | Vytvořit nový | Předat nadřízen... | Odpovědět a od... | Přesunout | Označit jako nepřečtené | Zpracovat | Přeložit | Číst nahlas | Lupa | Insecure

Odstranit | Odpovědět | Rychlé kroky | Přesunout | Značky | Úpravy | Řeč | Lupa | GpgOL

IK

čt 26.01.2023 14:25

[redacted] via RT <security-com@service.zcu.cz>

[ZCU RT3 #[redacted]] (security) PODVODNÝ MAIL? Fwd: Message from the Regional Cultural Attache's Office within the Embassy of the Republic of Iraq in Bucharest

Komu

Z této zprávy jsme odebrali nadbytečné konce řádků.

```
  Pocatecni pozadavek:
----------------------------------------------------------------

Dobrý den,

přeposílám níže email s dotazem, zda se nejedná o podvodný mail.
Nedokážu vyhodnotit, jestli mohu otevřít přílohu nebo ne.

Předem děkuji za reakci. S pozdravem,

[redacted]



-------- Přeposlaná zpráva --------
Předmět:    Message from the Regional Cultural Attache's Office within the
Embassy of the Republic of Iraq in Bucharest
Datum:      Fri, 20 Jan 2023 11:42:46 +0200
Od:   Iraqi Regional Cultural Attaché In Bucharest
<culturalbucharest@scrdiraq.gov.iq>
Komu:       [redacted]@zcu.cz, [redacted]@rek.zcu.cz


The Regional Cultural Attache's Office within the Embassy of the Republic of Iraq in Bucharest   would like to salute you and kindly ask you to
provide us with an answer to our enclosed note.

With our best regards,

Prof. Dr. Shakir Kadhim Ali
Regional Cultural Attache / Bucharest


----------------------------------------------------------------
```

Řešení incidentu

- ZČU má zodpovědný přístup
  - Bezpečnostní tým WIRT (WEBnet Incident Response Team)
  - Reakce na bezpečnostní incidenty
- Cílem je chránit
  - Vlastní uživatele
  - Okolní internet
  - Pověst sítě WEBnet (resp. ZČU)

Nejčastější typy incidentů

- Phishing
- Těžba kryptoměn
- Napadené stroje v botnetech
- Rozesílání SPAMu
- Sdílení autorsky chráněných dat

Postup řešení incidentu

1) Zjištění (detekce)
   - Zjištění vlastními silami (IDS, McAfee, logy, …)

   - Ohlášení třetí stranou
     - CESNET NetFlow, IDS, honeypoty, Mentat, …
     - Bezpečnostní tým jiné organizace
     - Dotčená fyzická/právnická osoba
     - Zástupci držitelů autorských práv

Příklad stížnosti zástupce vlastníka autorských práv

Dear Sir or Madam:

We are contacting you on behalf of Paramount Pictures Corporation (Paramount). Under penalty of perjury, I assert that IP-Echelon Pty. Ltd., (IP-Echelon) is authorized to act on behalf of the owner of the exclusive copyrights that are alleged to be infringed herein.

IP-Echelon has become aware that the below IP addresses have been using your service for distributing video files, which contain infringing video content that is exclusively owned by Paramount.

IP-Echelon has a good faith belief that the Paramount video content that is described in the below report has not been authorized for sharing or distribution by the copyright owner, its agent, or the law. I also assert that the information contained in this notice is accurate to the best of our knowledge.

We are requesting your immediate assistance in removing and disabling access to the infringing material from your network. We also ask that you ensure the user and/or IP address owner refrains from future use and sharing of Paramount materials and property.

In complying with this notice, Zapadoceska univerzita v Plzni should not destroy any evidence, which may be relevant in a lawsuit, relating to the infringement alleged, including all associated electronic documents and data relating to the presence of infringing items on your network, which shall be preserved while disabling public access, irrespective of any document retention or corporate policy to the contrary.

Please note that this letter is not intended as a full statement of the facts; and does not constitute a waiver of any rights to recover damages, incurred by virtue of any unauthorized or infringing activities, occurring on your network. All such rights, as well as claims for other relief, are expressly reserved.

Should you need to contact me, I may be reached at the following address:

Adrian Leatherland
On behalf of IP-Echelon as an agent for Paramount
Address: 7083 Hollywood Blvd., Los Angeles, CA 90028, United States
Email: p2p@copyright.ip-echelon.com

Evidentiary Information:
Protocol: BITTORRENT
Infringed Work: Baywatch
Infringing FileName: Baywatch (2017) [YTS.AG]
Infringing FileSize: 940417015
Infringer's IP Address: 147.228.XXX.XXX
Infringer's Port: 13769
Initial Infringement Timestamp: 2017-10-14T21:38:06Z

Postup řešení incidentu

2) Ověření

- Informaci může poslat každý
  - Řešíme jen skutečné události
- Naše záznamy
  - Potvrdí výskyt incidentu
  - Doplní podrobnosti

3) Minimalizace dopadů

- Cílem je zastavit zhoršování situace
  - Odpojení napadeného počítače
  - Zablokování služby
  - Zablokování zneužitého konta
  - Odebrání přístupových práv
  - …
- Dočasné řešení do provedení nápravy

Postup řešení incidentu

4) Provedení nápravy

- Technická opatření
  - Odvirování, reinstalace, rekonfigurace, …
  - Změna hesla, revokace certifikátů, …
- Interakce s uživateli
  - Informace o incidentu
  - Instrukce k (vy)řešení incidentu
  - Osobní návštěva WIRT

Osobní návštěva

- Pohovor s uživateli
  - U závažných incidentů
  - U opakovaných incidentů
  - Na žádost uživatele
- Standardní postup
  - Vysvětlení problému
  - Vysvětlení správného chování
  - Upozornění na následky

Následky

- Dopady vlastního incidentu
  - Napadený počítač – zneužití dat, přístupů, …
  - Odpojení od sítě
- Vymáhání dodržování univerzitních směrnic
  - Disciplinární komise / porušení pracovní kázně
  - Omezení „nenárokových“ služeb
- Vymáhání dodržování zákonů platných v ČR
  - Trestněprávní řízení
  - Občanskoprávní řízení

Pohovor s uživateli

- Čeho se při pohovoru rozhodně vyvarovat
  - Zapírat
    - Víme víc, než si myslíte
  - Vymýšlet si historky
    - DLP (Dojemný Lidský Příběh)
    - Známe všechny
  - Nabízet úplatky a žádat výjimky
    - Mimo vaše možnosti
    - Máme standardní postupy
    - Průběh incidentu je zaznamenán v interních systémech

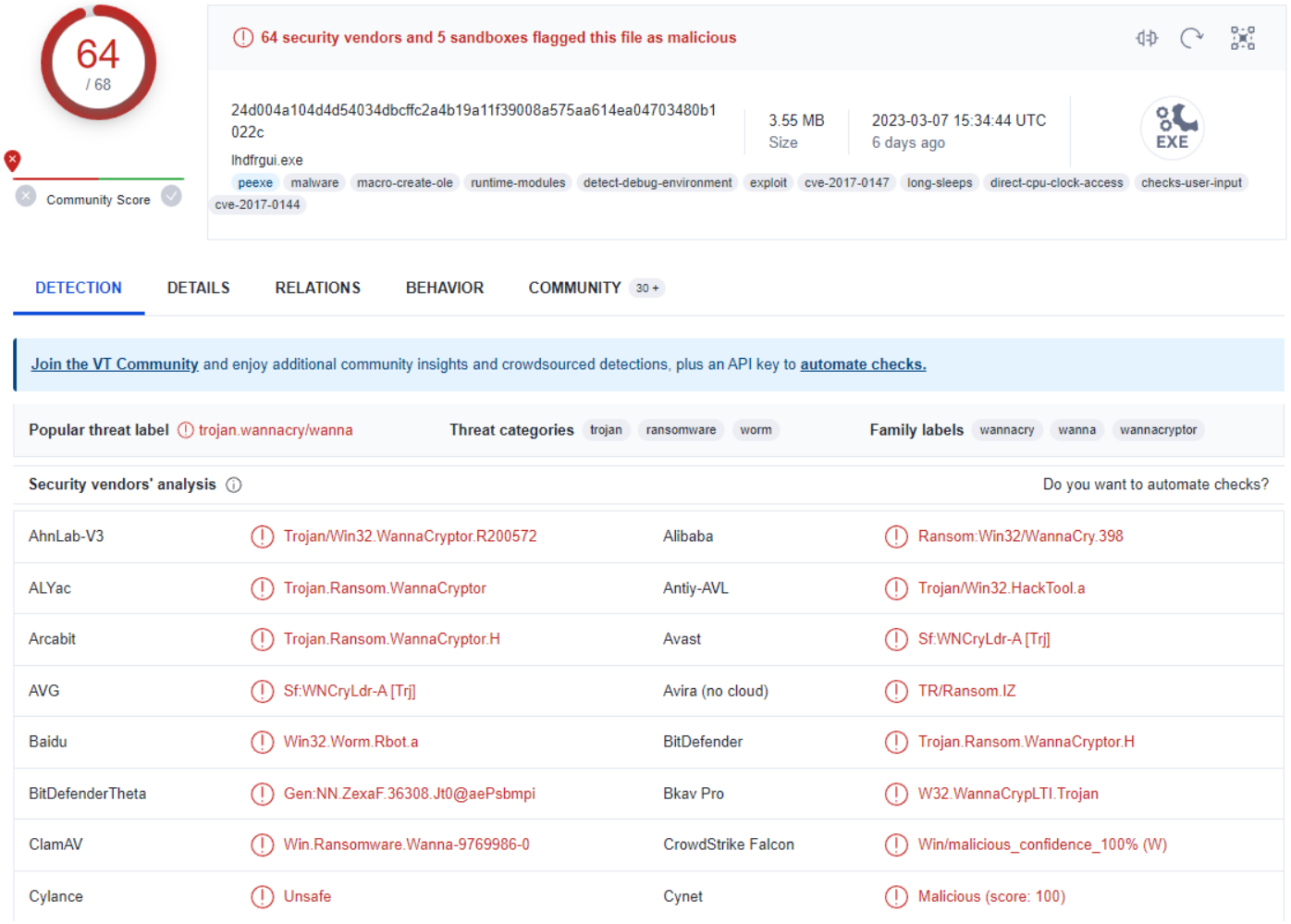
Shrnutí

- Svět není ideální
  - bezpečnostní incidenty
- ZČU
  - Odpovědnost za univerzitní síť WEBnet
  - WEBnet Incident Response Team
  - Reakce na bezpečnostní incidenty
- Doporučení
  - Dodržujte 10R/2008 a řiďte se zdravým rozumem
  - Spolupracujte (když už jste účastníkem bezpečnostního incidentu)

Na závěr – nástroje, které se mohou hodit i vám

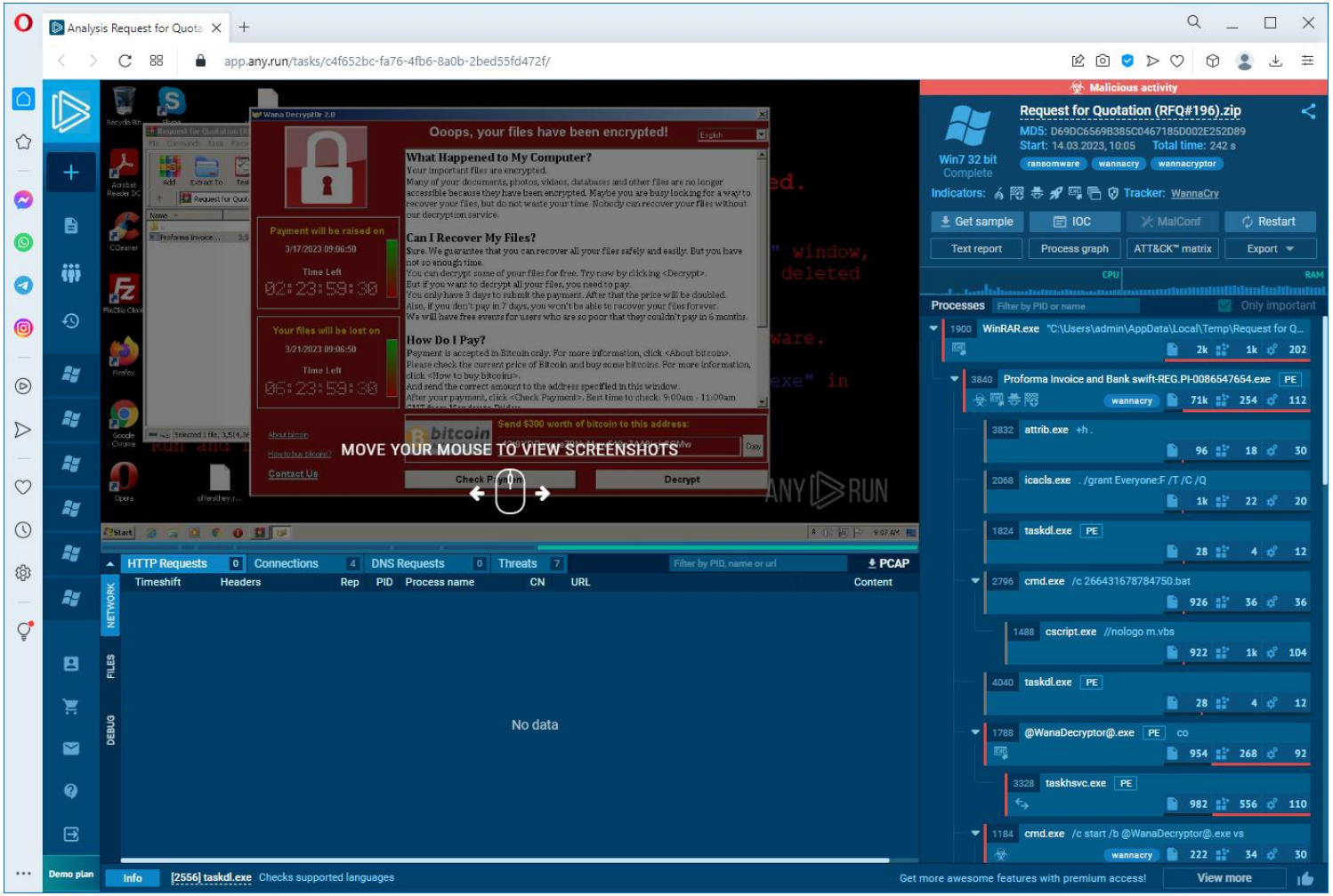
Nástroje používané při práci týmu WIRT

- VirusTotal



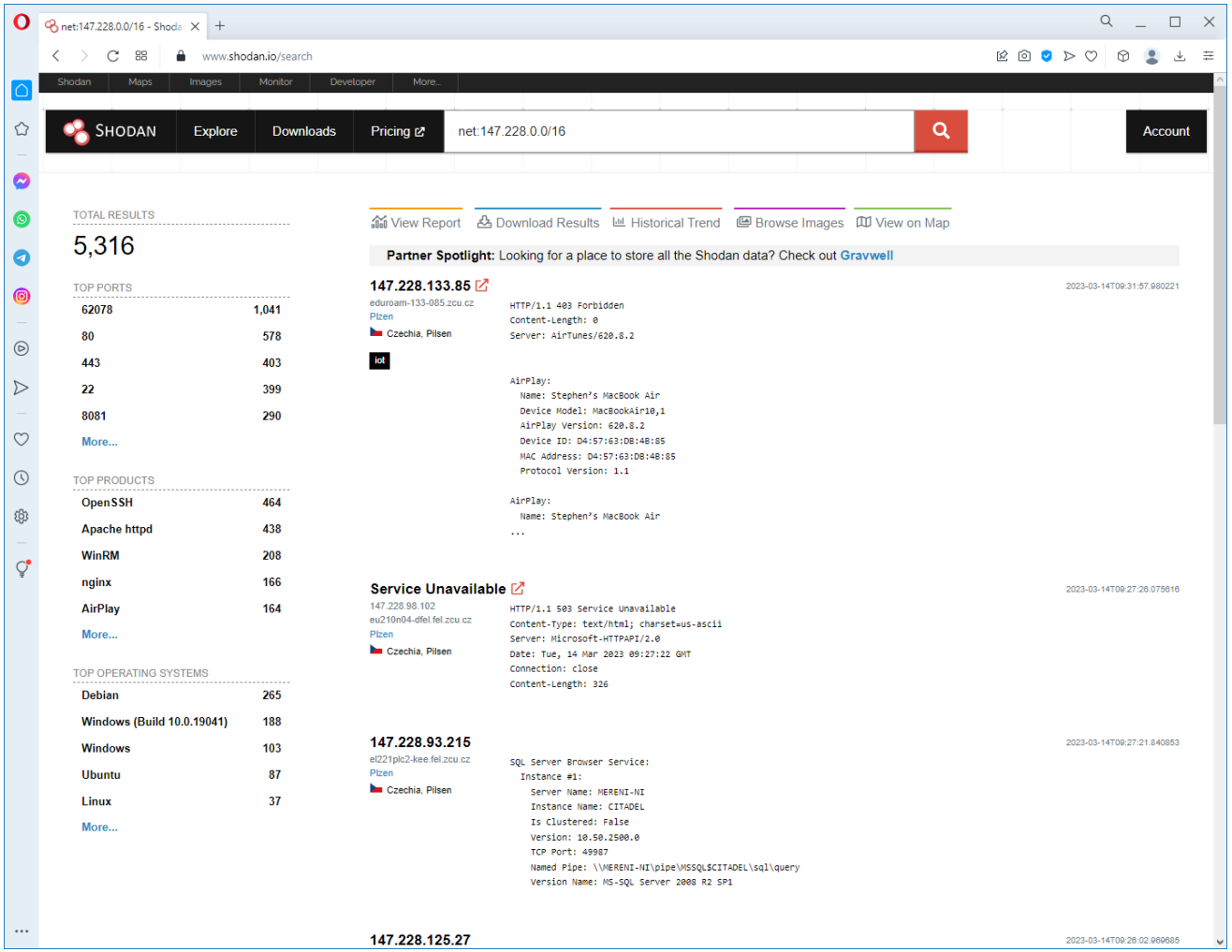
Nástroje používané při práci týmu WIRT

- Sandbox ANY.RUN



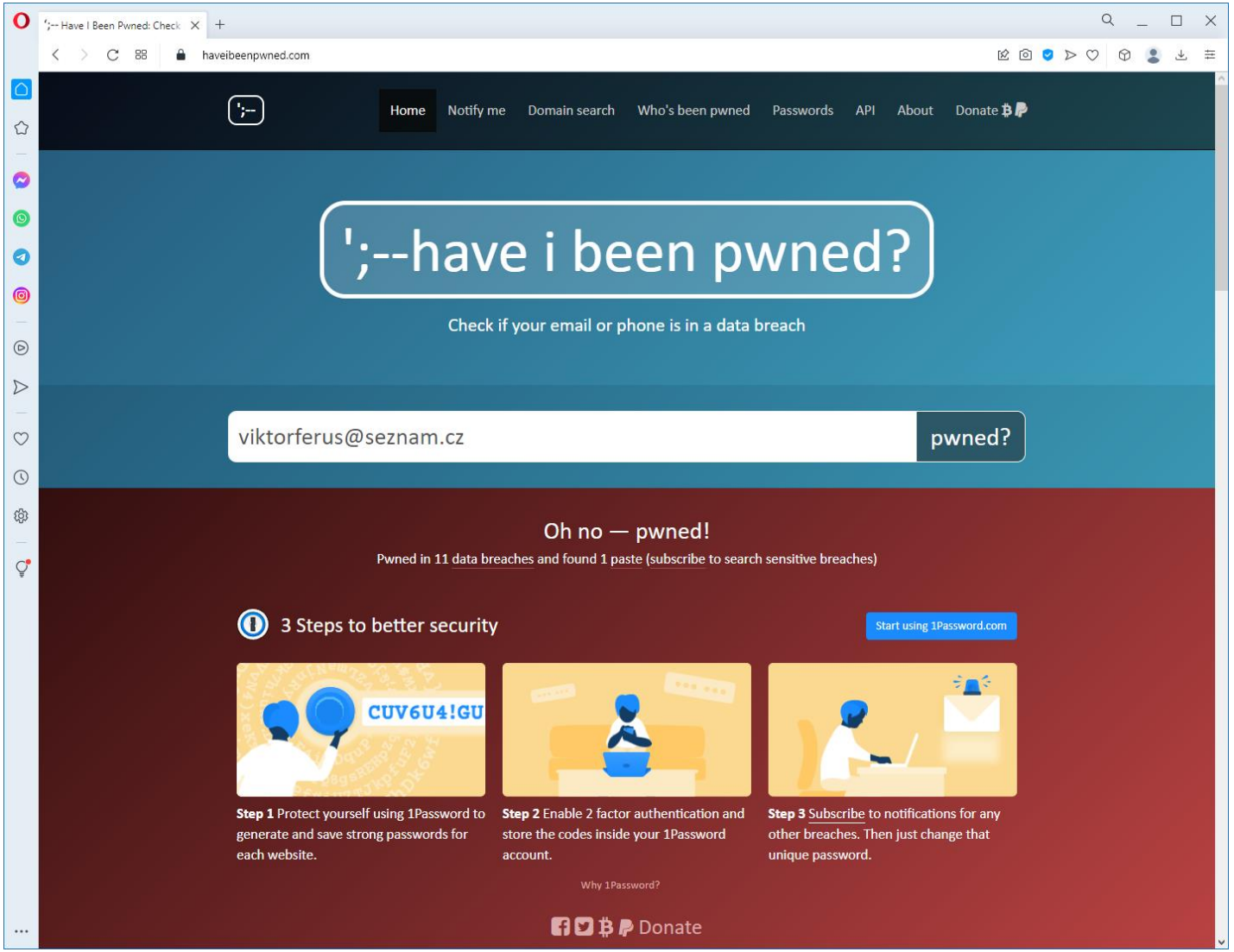
Nástroje používané při práci týmu WIRT

- Shodan.io – **free academic membership!**



Nástroje používané při práci týmu WIRT

- Have I Been pwned



ZÁPADOČESKÁ
UNIVERZITA
V PLZNI

Dotazy?

Viktor Ferus / ferusvi@civ.zcu.cz