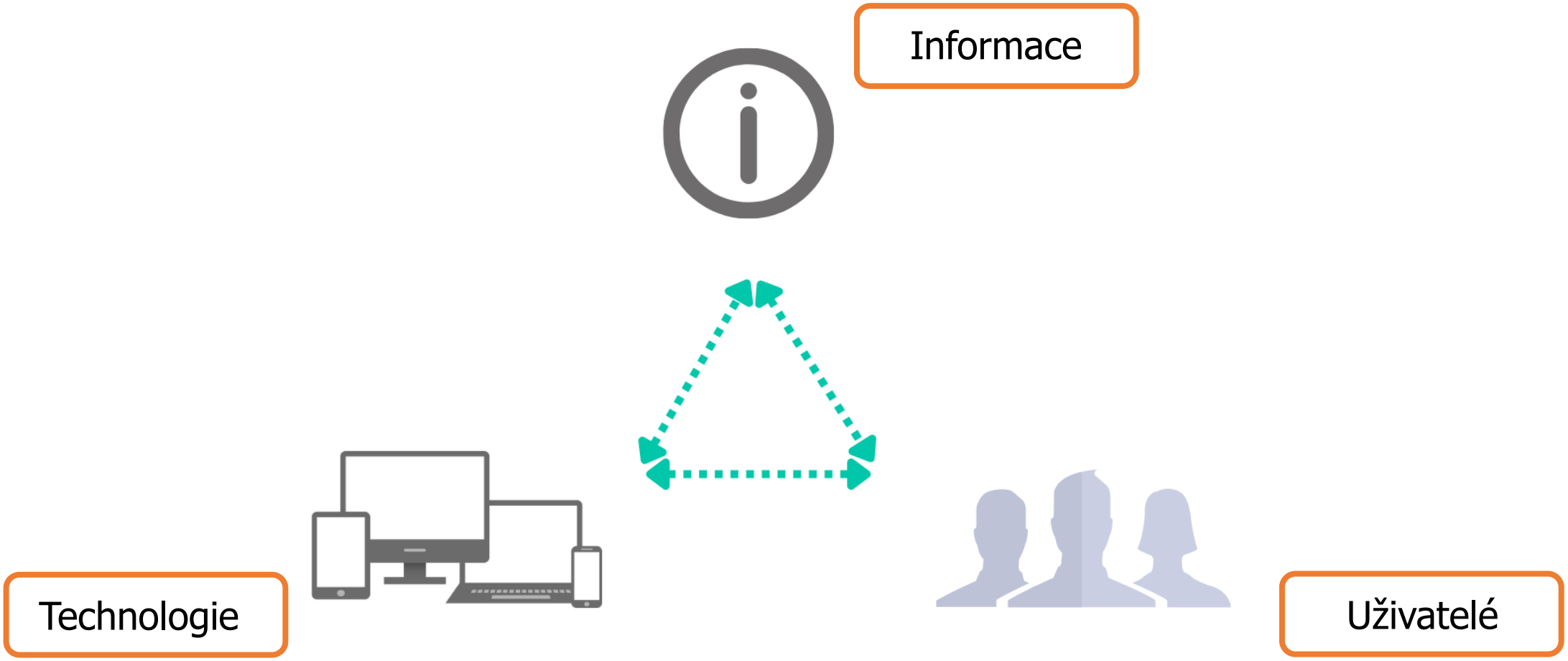
COMGUARD
communication security

COMGUARD - Ohlédnutí za rokem 2021 optikou služby ThreatGuard a PhishTest

Roman Jiráček, Account & Vendor Manager

Stolička bezpečnosti



PhishTest – simulované phishingové kampaně

[O365-SPAM] Váš balík nebyl doručen.

ČP Česká pošta <notificaciones.sgjp@tsjcdmx.g
Komu **Sales**

Odpovědět | Odpovědět všem | Přeposlat | ...

po 21.03.2022 6:15

V této zprávě byly zakázané odkazy a jiné funkce. Pokud chcete tyto funkce povolit, přesuňte zprávu do složky Doručená pošta.
Tato zpráva byla převedená do formátu prostého textu.

<https://www.ceskaposta.cz/CeskaPosta-theme/images/cp/logo.png>

Vážený zákazník,

Všimli jsme si, že vaše objednávka DKRMH60562763, sledovací číslo L938478764, čeká na odeslání kvůli chybějící adrese. Vyplňte svou adresu kliknutím na následující odkaz:

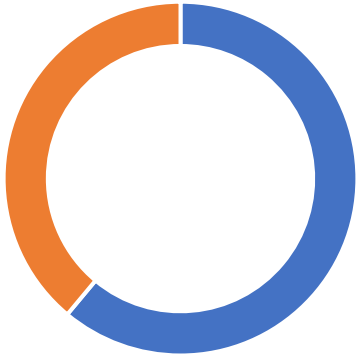
Sledujte svou objednávku <https://shor.at/U5G9seEQ>

Stačí vyplnit všechny údaje o vaší poštovní adrese; Balíček bude doručen 48 hodin po zákroku.
Další informace vám zůstáváme k dispozici.

Přepravní náklady: 40,20 CZK

Zákaznický servis Česká pošta

Otevření emailu 38,94%

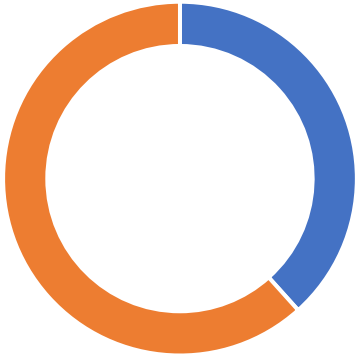


Neotevření emailu
Otevření emailu

Kliknutí na odkaz 50,55%

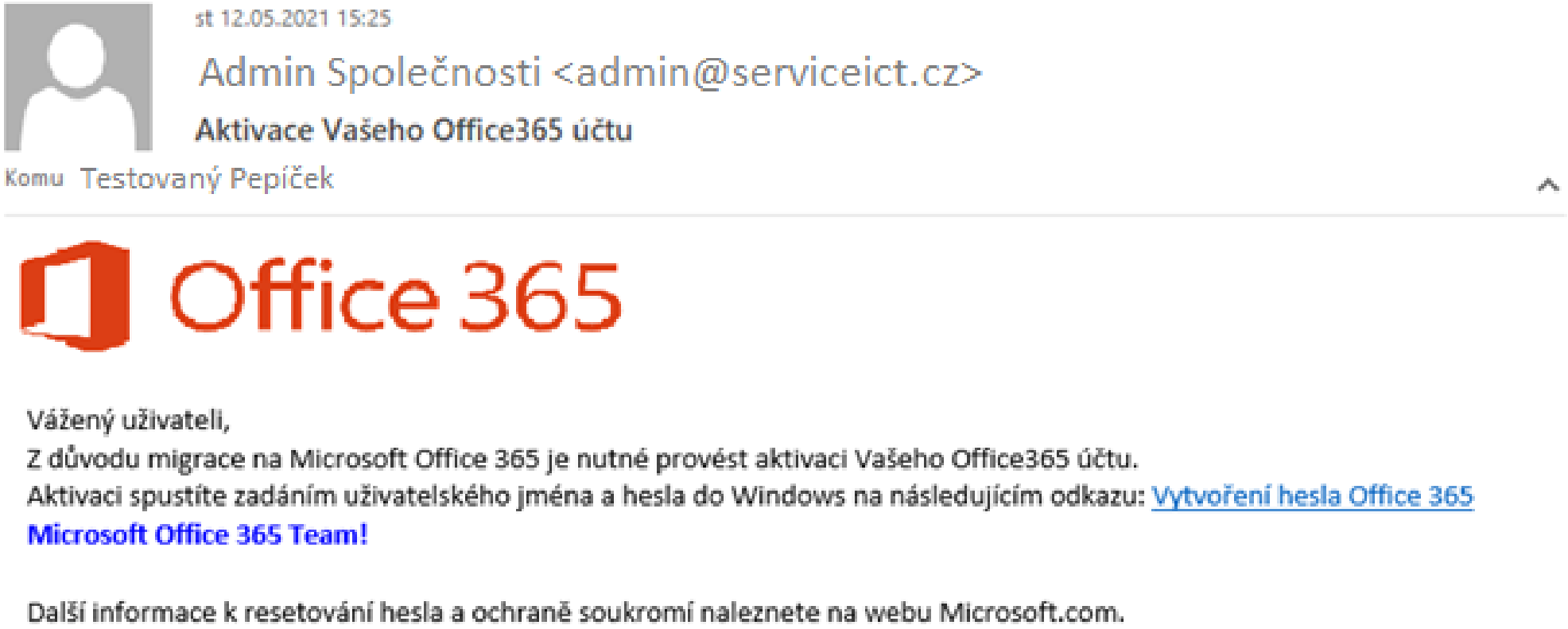
Nekliknutí na odkaz
Kliknutí na odkaz

Zadaná data 61,65%



Nezadaná data
Zadaná data

PhishTest - ukázka



st 12.05.2021 15:25

Admin Společnosti <admin@serviceict.cz>

Aktivace Vašeho Office365 účtu

Komu Testovaný Pepíček

Office 365

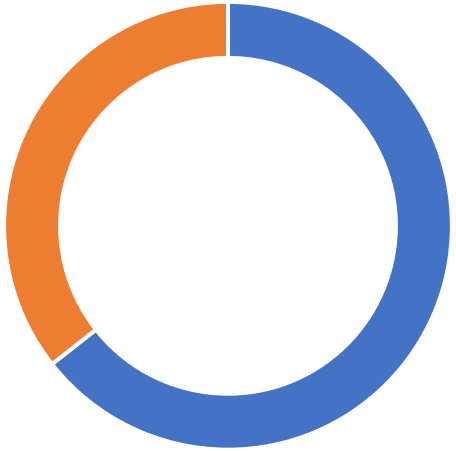
Vážený uživateli,
Z důvodu migrace na Microsoft Office 365 je nutné provést aktivaci Vašeho Office365 účtu.
Aktivaci spustíte zadáním uživatelského jména a hesla do Windows na následujícím odkazu: Vytvoření hesla Office 365
Microsoft Office 365 Team!

Další informace k resetování hesla a ochraně soukromí naleznete na webu Microsoft.com.

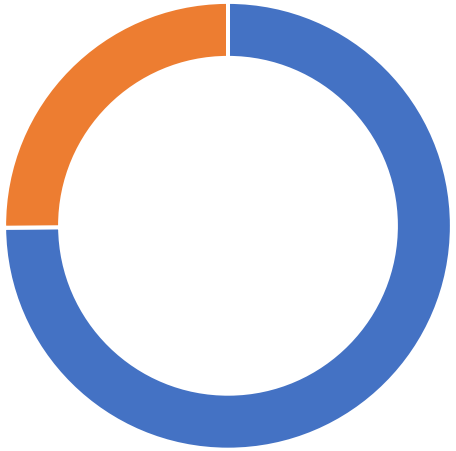
PhishTest – statistiky

- Výsledky phishingových kampaní testování v regionu

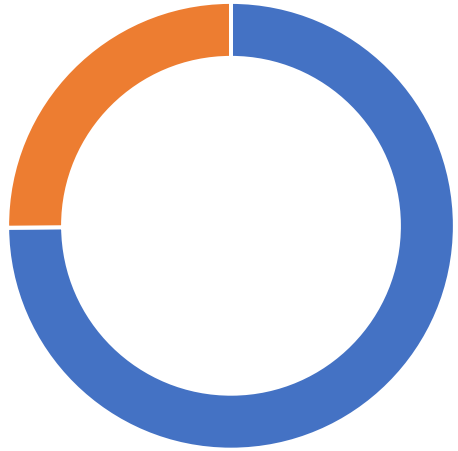
Otevření emailu 35,60%



Kliknutí na odkaz 25,14%



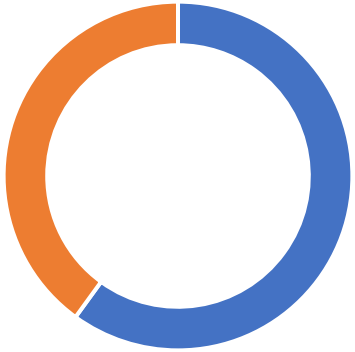
Zadaná data 16,78%



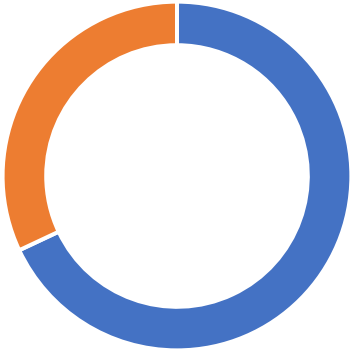
- Zdroj: COMGUARD PhishTest

- Porovnání dvou phishingových kampaní u vybraného klienta

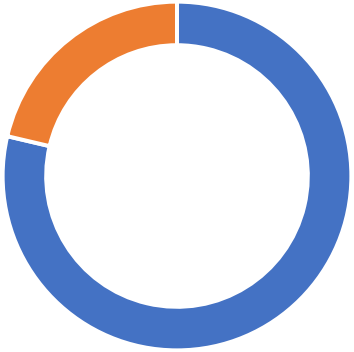
Otevření emailu 40,00%



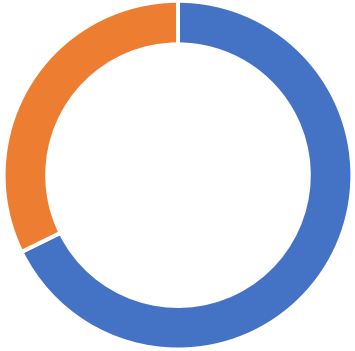
Kliknutí na odkaz 32,00%



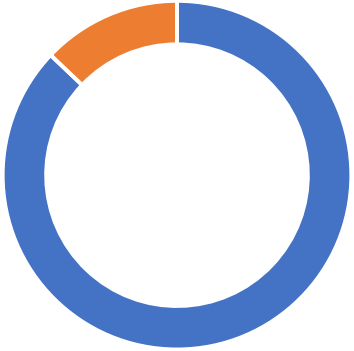
Zadaná data 21,33%



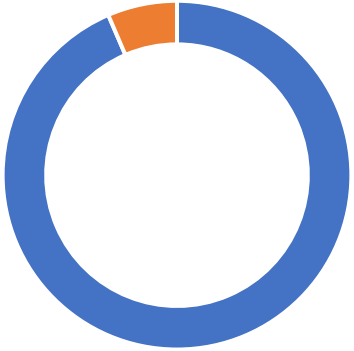
Otevření emailu 32,26%



Kliknutí na odkaz 12,90%



Zadaná data 6,45%



- Zdroj: COMGUARD PhishTest

Jak služba funguje?

- Testování je prováděno pomocí e-mailů, které simulují V
- Vytvoření scénáře útoku - vizuálu podvodného e-mailu a
- Spuštění kampaně rozesláním vybraných podvodných e
- Sledování průběhu kampaně po smluvenou dobu.
- Sběr dat a jejich vyhodnocení.
- Závěrečná zpráva obsahující podrobné zhodnocení kamp bezpečnosti.

Běžné služby

Otestování uživatelů pomocí phishingového **emailu na běžné služby např. Office365** nesoucí link a odkazující na podvrženou stránku.

Úroveň 1

Custom služby

Otestování uživatelů pomocí phishingového emailu na **Vámi definované služby** nesoucí link a odkazující na podvrženou stránku.

Úroveň 2

Malware příloha

Otestování uživatelů pomocí phisingového **emailu obsahujícího malware přílohu.**

Úroveň 3

Na míru

Otestování uživatelů dle Vašich specifických požadavků a přání.

Kontaktujte nás

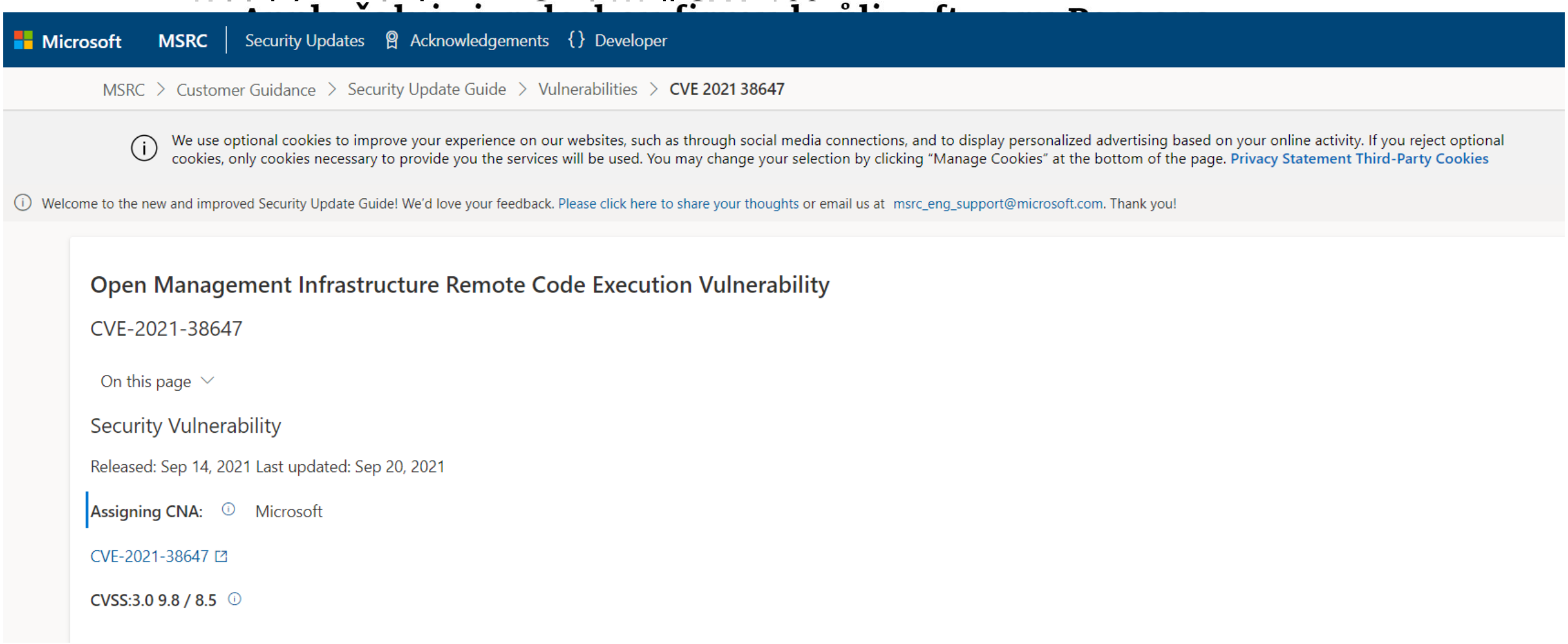
Úroveň 4

Hlavní přínosy PhishTestu pro Vás

- Posílíte povědomí zaměstnanců o IT bezpečnosti.
- Zvýšíte odolnost zaměstnanců před phishingovými útoky.
- Zavedete další formu ochrany v rámci kybernetické bezpečnosti - prevenci.
- Ošetříte jeden z nejčastějších vektorů útoku.
- Získáte přehled o úrovni odolnosti Vaší společnosti před cílenými útoky.
- Snížíte pravděpodobnost bezpečnostního incidentu.

Kritické hrozby roku 2021:

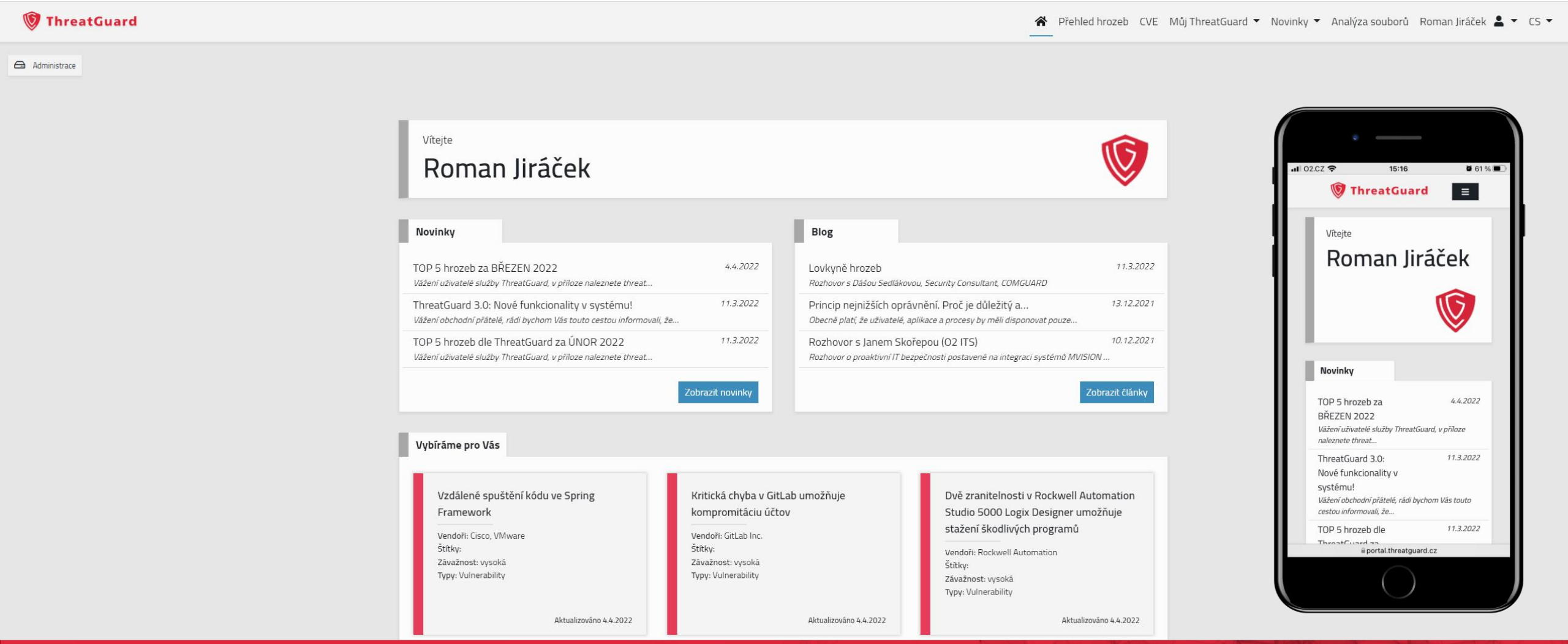
- Vzdálené převzetí kontroly v Apache Server



Virtuální bezpečnostní analytik

- Výsledek nepřetržité práce teamu bezpečnostních analytiků
  - Databáze aktuálních hrozeb pro Vaše IT
  - Prověřené návrhy nápravných opatření
- Možnost filtrace hrozeb dle Vašich aktiv
- Dostupné formou webového portálu s notifikacemi
  - Chat s podporou expertního teamu

Stále dostupná, aktuální, strukturovaná databáze hrozeb a opatření



Zpět

Vzdialené prevzatie kor

Základní údaje

ID	1946	Přidáno	
Úplnost reportu	plný	Aktualiz	
Typy	Vulnerability	Geoloka	
Závažnost	vysoká	Autor	

Náprava

Administrátorom odporúčame čo najskor upgradovať na verziu Log4j 2.15.0, ktorá zraniteľnosť opravuje:

https://logging.apache.org/log4j/2.x/security.html#Fixed_in_Log4j_2.15.0

Aktualizace: CVE-2021-45046

Log4j 1.x není touto zranitelností ovlivněn. Pokud v rámci Log4j2 nevyužíváte defalní konfiguraci, doporučujeme co nejdříve update na verzi Log4j 2.16.0.

Opatření

Aktualizace | "Log4Shell" (CVE-2021-44228) - LogRhythm | "Log4Shell" (CVE-2021-44228) - Sophos | "Log4Shell" (CVE-2021-44228) - Rapid7 | "Log4Shell" (CVE-2021-44228) - Forcepoint SMC | Mitigácia Log4Shell | "Log4Shell" (CVE-2021-44228) - McAfee

Mitigácia Log4Shell

Zpět

Základní údaje

Ověřenost	Opatření třetí strany	Přidáno	13.12.2021 14:58
		Aktualizováno	27.12.2021 14:57
Úplnost reportu	plný		
Vytvořil	Dáša Sedláková		

Přílohy

Zdroje

https://logging.apache.org/log4j/2.x/security.html
https://www.marketscreener.com/quote/stock/RAPID7-INC-23055722/news/Rapid7-Widespread-Exploitation-of-Critical-Remote-Code-Execution-in-Apache-Log4j-37284964/
https://www.cisa.gov/uscert/ncas/alerts/aa21-356a

Popis

Priama oprava

Kritická zraniteľnosť CVE-2021-44228 v Apache Log4j bola opravená vo verzii 2.15. Nadväzujúca menej závažná zraniteľnosť (CVE-2021-45046 s CVSS 3.7) v Apache Log4j bola opravená vo verzii 2.16. A ďalšia závažná zraniteľnosť CVE-2021-45046 je opravená vo verzii 2.17.

Čo najskôr identifikujte, zmiernite a aktualizujte ovplyvnené produkty, ktoré používajú Log4j, na najnovšiu opravenú verziu:

- Pre prostredia používajúce Javu 8 alebo novšiu inovujte na Log4j verziu 2.17.0 (vydaná 17. decembra 2021) alebo novšiu.
- Pre prostredia používajúce Java 7 inovujte na Log4j verziu 2.12.3 (vydaná 21. decembra 2021). Poznámka: Java 7 je momentálne na konci životnosti a organizácie by mali upgradovať na Java 8.

Manuálna oprava

Pokiaľ z akéhokoľvek dôvodu nemôžete aktualizovať, vo vydaniach novších(alebo rovnakých) ako verzia 2.10 možno zraniteľnosť zmierniť nastavením systémovej vlastnosti `log4j2.formatMsgNoLookups` alebo premennej prostredia `LOG4J_FORMAT_MSG_NO_LOOKUPS` na hodnotu **true**.

Aplikujte preto parameter **-Dlog4j2.formatMsgNoLookups=True** do príkazu JVM na spustenie aplikácie.

Pre vydania novšie(alebo rovnaké) ako verzia 2.7 a staršie(alebo rovnaké) ako 2.14.1, všetky vzory **PatternLayout** môžu byť upravené tak, aby špecifikovali konvertor správ ako %m{nolookups} namiesto pôvodného iba %m.

Pre vydania novšie(alebo rovnaké) ako verzia 2.0-beta9 a staršie(alebo rovnaké) ako 2.10.0 je zmiernením odstránenie triedy JndiLookup z cesty k triede: **zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class**.

Ďalšie opatrenia

Navyše, Verzie JDK väčšie ako 6u211, 7u201, 8u191 a 11.0.1 nie sú ovplyvnené vektorom útoku LDAP. com.sun.jndi.ldap.object.trustURLCodebase je nastavený na false, čo znamená, že JNDI nemôže načítať vzdialenú kódovú základňu pomocou LDAP.

Ďalším odporúčaním je kontrola prichádzajúcich sieťových požiadavok obsahujúcich string "${jndi:".

- **Rozhraní pro integraci do dalších systémů** (SIEM, SOC, SOAR, apod.)
- **Rozšířené možnosti filtrování** - fulltextové vyhledávání, Multiselect vyhledávání s možností našeptávání a CPE
- **Rozšíření datových zdrojů hrozeb** - CSIRT ČR a SK
- **HTML notifikace**
- **Zrcadlení celého CVE katalogu do ThreatGuard v AJ** - nová položka v menu
- **Integrace s McAfee ATD** – nahrajete neznámý soubor nebo URL adresu skrze ThreatGuard do McAfee, kde se otestuje a řekne Vám, jestli je v pořádku nebo kritický

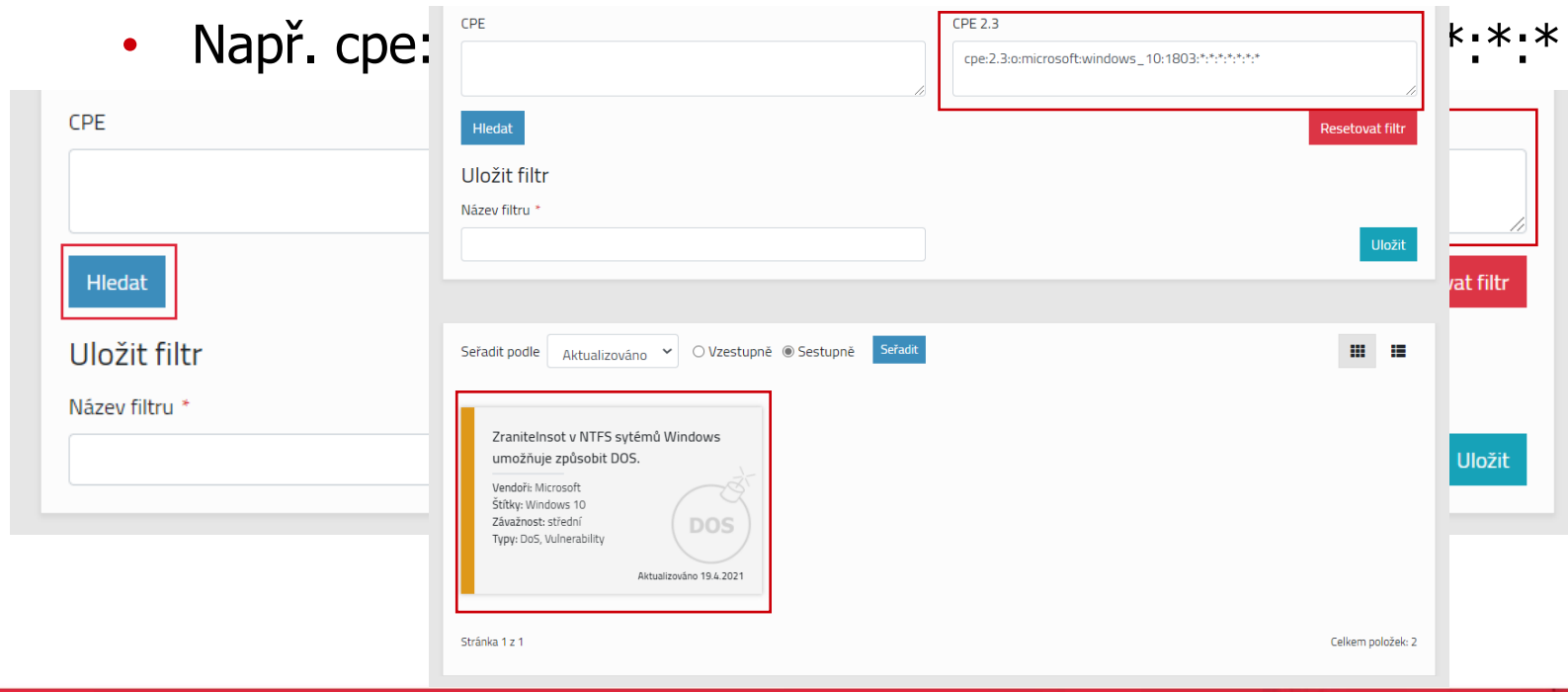
CPE string je název software, aplikace a její konkrétní verze ve formátu, který je standardizovaný

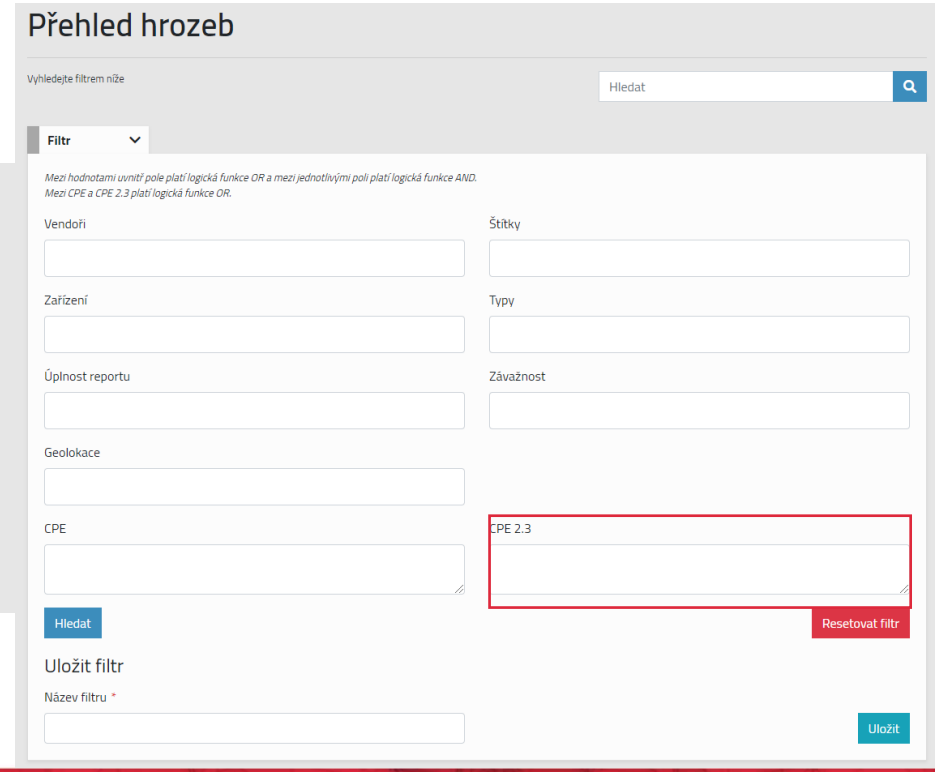
- CPE slovník: [NVD - CPE (nist.gov)]

Jak CPE string dohromady?

cpe:<verze – 2.3>:<a,o,h – a=aplikace, o=operační system, h=hardware device >:<vendor>:<produkt>

- Např. cpe:

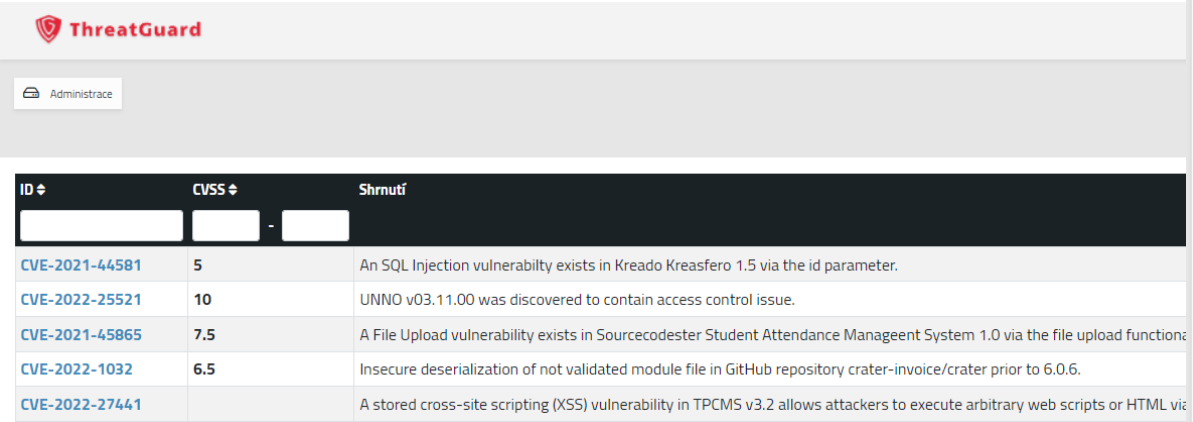


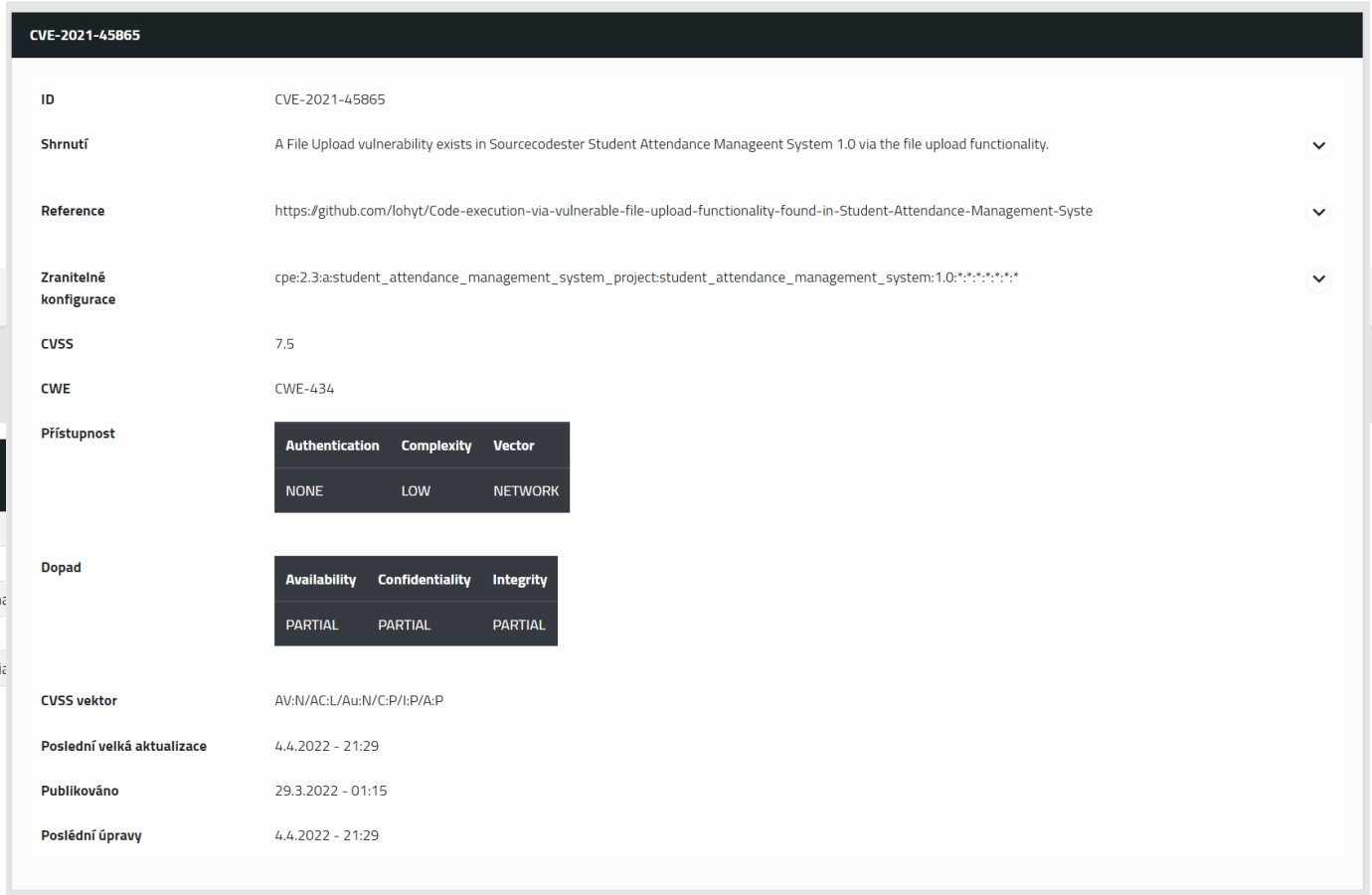


CVE katalog

- Zrcadlení celého CVE katalogu do ThreatGuard v angličtině – nová položka v menu

- **Možnosti filtrování v CVE databázi – aktuálně:**
  - Dle ID u dané CVE
  - Dle CVSS
  - Poslední aktualizace
  - Publikováno





Integrace s McAfee Advanced Threat Defense

McAfee | Threat Analysis Report

URL	hxxps://www.seznam.cz/
Malware Name	Analysis.Dynamic
URL Submitted	2022-03-11 09:06:00 UTC
File Size	22 -
Show More	Hash Values File Details
MD5 Hash Identifier	D0D3D6C3B870C6ABFC0594DDA539C3
Screenshots	2
	Hide hash values
File Type	application/url
	Hide file details

Microsoft Windows 7 Professional Service Pack 1 (build 7601, version 6.1

Windows® Internet Explorer version: 8.0.7601.17514

Microsoft Office version: 2010

PDF Reader version: DC

No Flash player installed

Flash player plugin version: 32.0.0.387

Platform Version 4.14.0.7

Detection Package Version 4.14.0.220107

Hide environment

Baitexe activated but not infected

Name	Reason
hxxps://www.seznam.cz/	loaded by MATD Analyzer

Timeline Activity

Processes Files Registry Operations Network Operations Multiple

Select Any Area to Zoom In

hxxps://www.seznam.cz/

0 3 6 9 12 15 18

Offset in s

Jump to Timeline Details

Techniques/SubTechniques Observed (MITRE ATT&CK™ Matrix)

Technique

System Services

Service Execution

Adversaries may abuse the Windows service control manager to execute malicious commands or payloads. The Windows service control manager (services.exe) is an interface to manage and manipulate services. The service control manager is accessible to users via GUI components as well as system utilities such as sc.exe and [Net].

Attempted to execute service — 2 - Low

Hide Artifacts

Hidden Files and Directories

Adversaries may set files and directories to be hidden to evade detection mechanisms. To prevent normal users from accidentally changing special files on a system, most operating systems have the concept of a hidden file. These files don't show up when a user browses the file system with a GUI or when using normal commands on the command line. Users must explicitly ask to show the hidden files either via a series of Graphical User Interface (GUI) prompts or with command line switches (dir /a for Windows and ls -a for Linux and macOS).

Hid content by modifying its attributes — 2 - Low

System Network Configuration Discovery

Adversaries may look for details about the network configuration and settings of systems they access or through information discovery of remote systems. Several operating system administration utilities exist that can be used to gather this information.

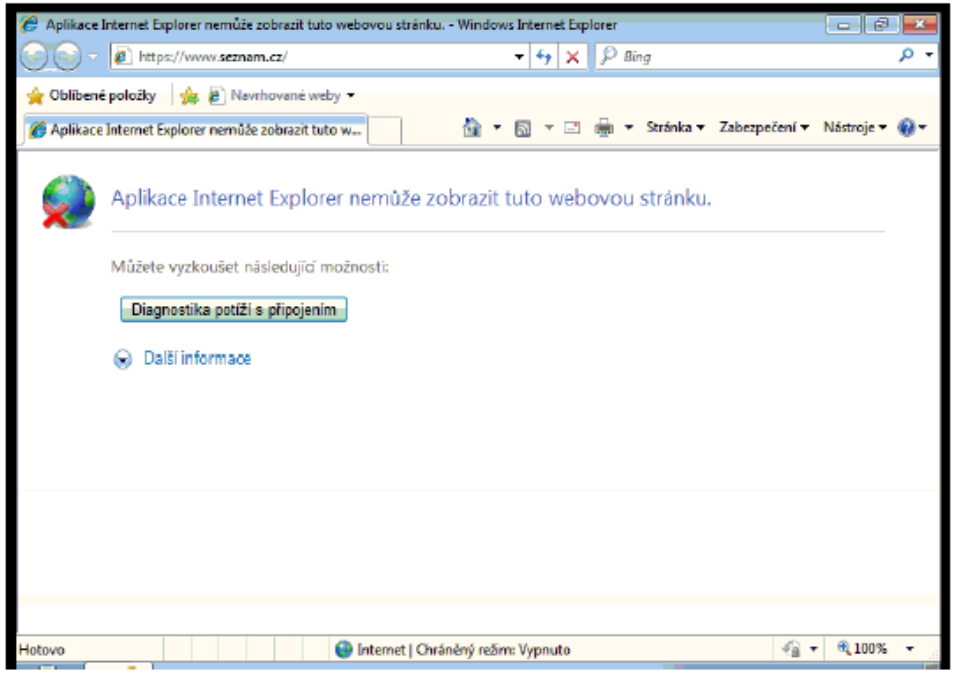
Queried for system network configuration information — 2 - Low

Screenshots

Note: a pop-up window was detected during dynamic analysis so user interaction may be required in order to fully analyze this sample

Images: 2

3e8fa.jpg



36bcb.jpg

o souboru nebo URL může trvat i

Detail

Hlavní přínosy ThreatGuard pro Vás

- Rychlý přehled o nejnovějších hrozbách pro vaše IT
- Přehlednou aktuální databázi hrozeb včetně návrhů nápravných opatření
- Pouze informace, které potřebujete - filtrace IT hrozeb dle vašich preferencí a potřeb
- Detailní filtrování na úrovni verze operačního systému nebo aplikace
- Emailová notifikace pro vaši pružnou reakci
- Dostupnost na všech rozšířených platformách Windows, Android, iOS
- Online chat s podporou IT expertů

COMGUARD
communication security

Děkuji za pozornost!