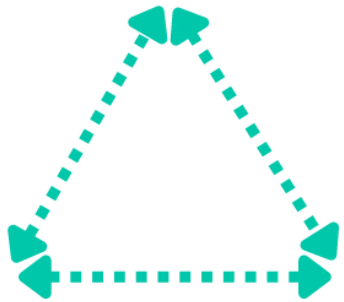
COMGUARD
communication security

COMGUARD - Ohlédnutí za rokem 2021 optikou služby ThreatGuard a PhishTest

Roman Jiráček, Account & Vendor Manager

Stolička bezpečnosti

Informace



Technologie

Uživatelé

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.

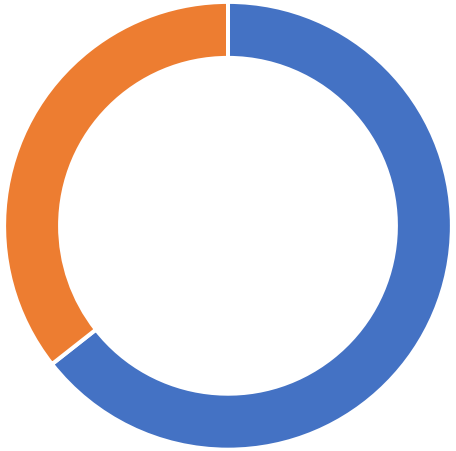
Přepravní náklady: 40,20 CZK

Zákaznický servis Česká pošta

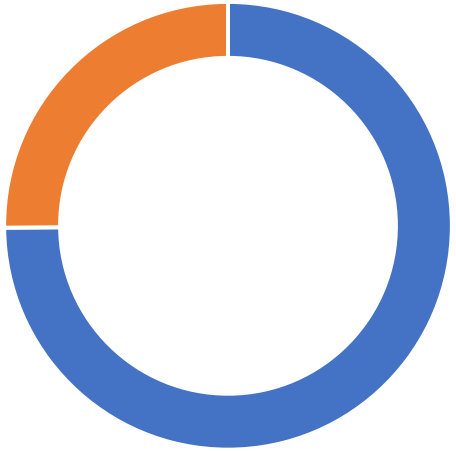
PhishTest – statistiky

- Výsledky phishingových kampaní testování v regionu

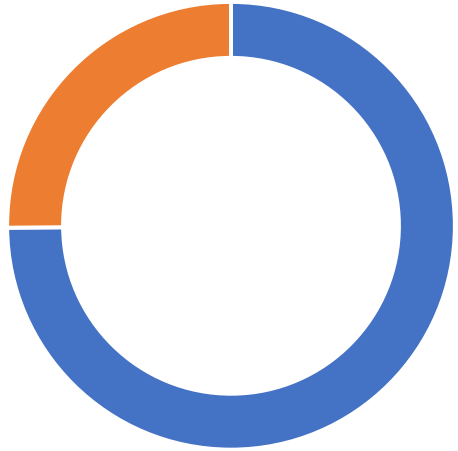
Otevření emailu 35,60%



Kliknutí na odkaz 25,14%

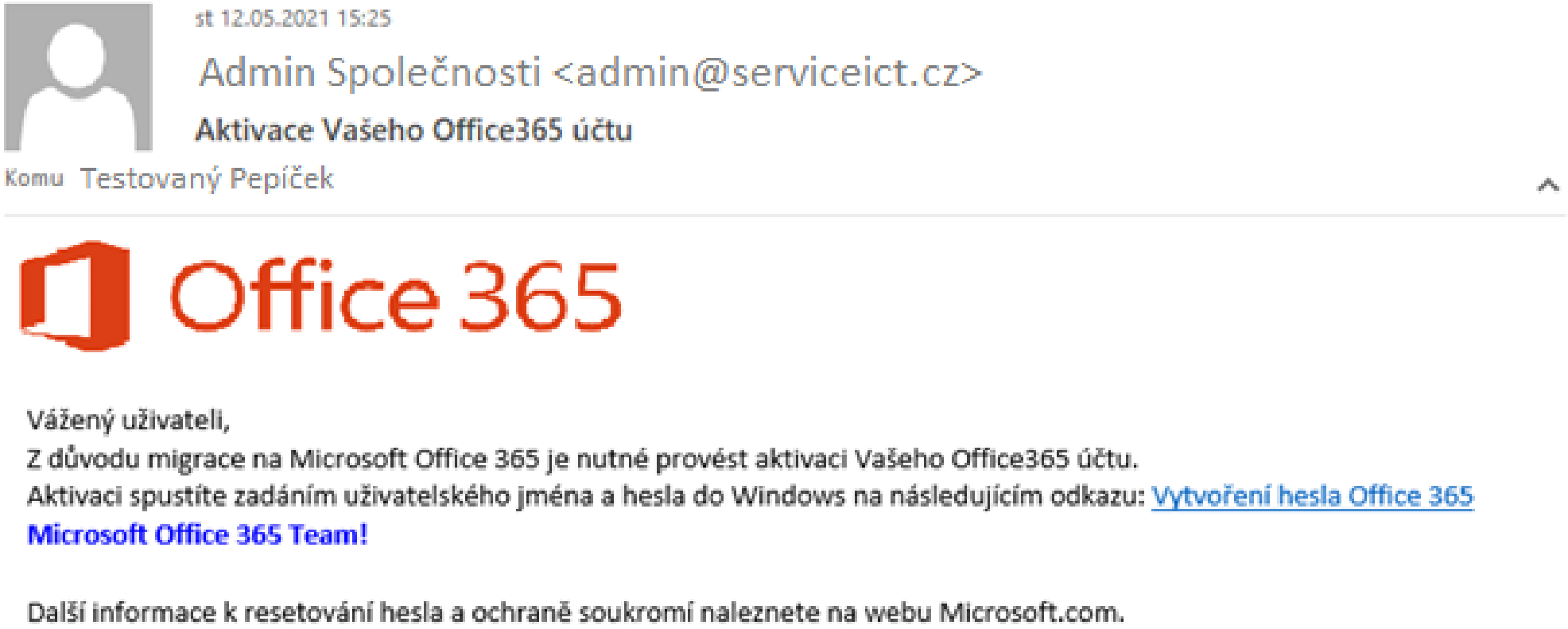


Zadaná data 16,78%



- Zdroj: COMGUARD PhishTest

PhishTest - ukázka



st 12.05.2021 15:25

Admin Společnosti <admin@serviceict.cz>

Aktivace Vašeho Office365 účtu

Komu Testovaný Pepíček

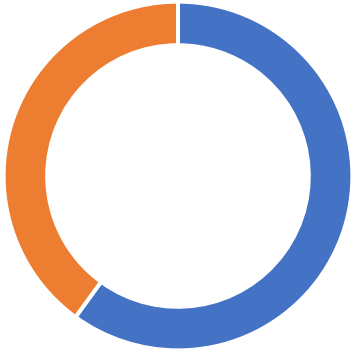
Office 365

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!

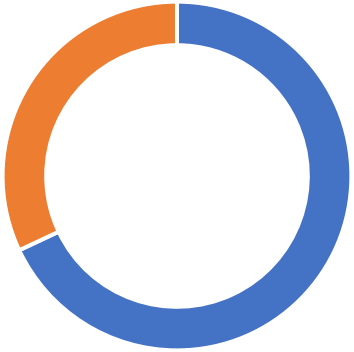
Další informace k resetování hesla a ochraně soukromí naleznete na webu Microsoft.com.

- Porovnání dvou phishingových kampaní u vybraného klienta

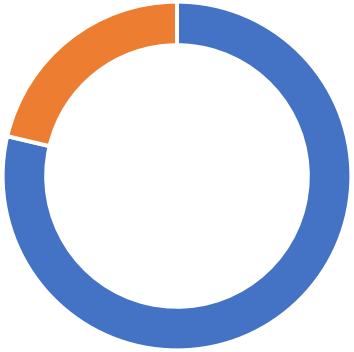
Otevření emailu 40,00%



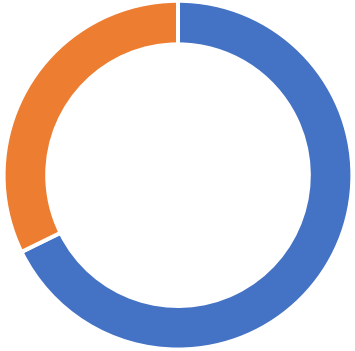
Kliknutí na odkaz 32,00%



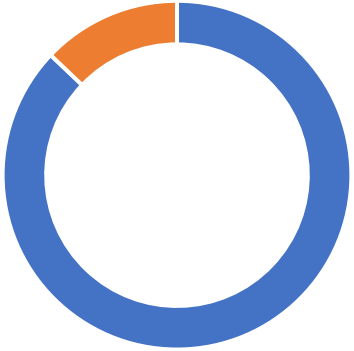
Zadaná data 21,33%



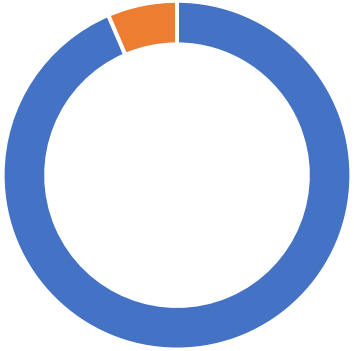
Otevření emailu 32,26%



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

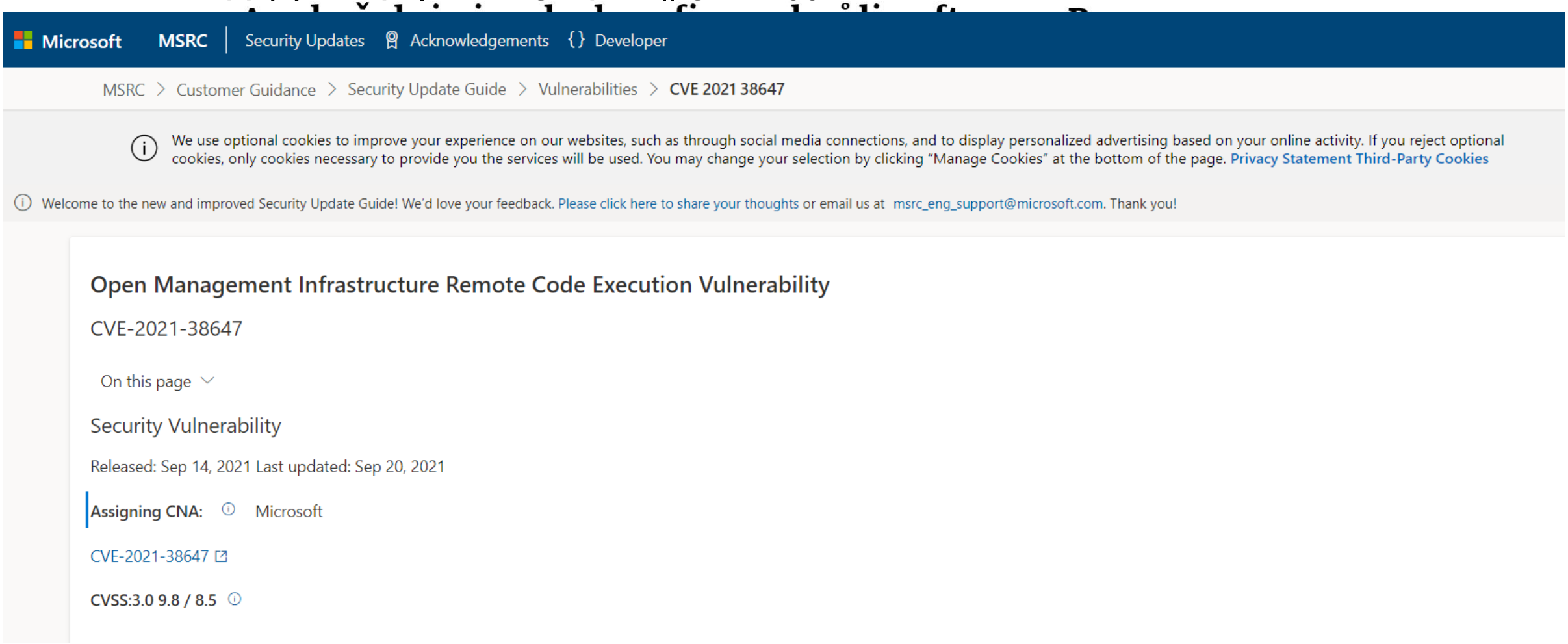
Úroveň 4

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:

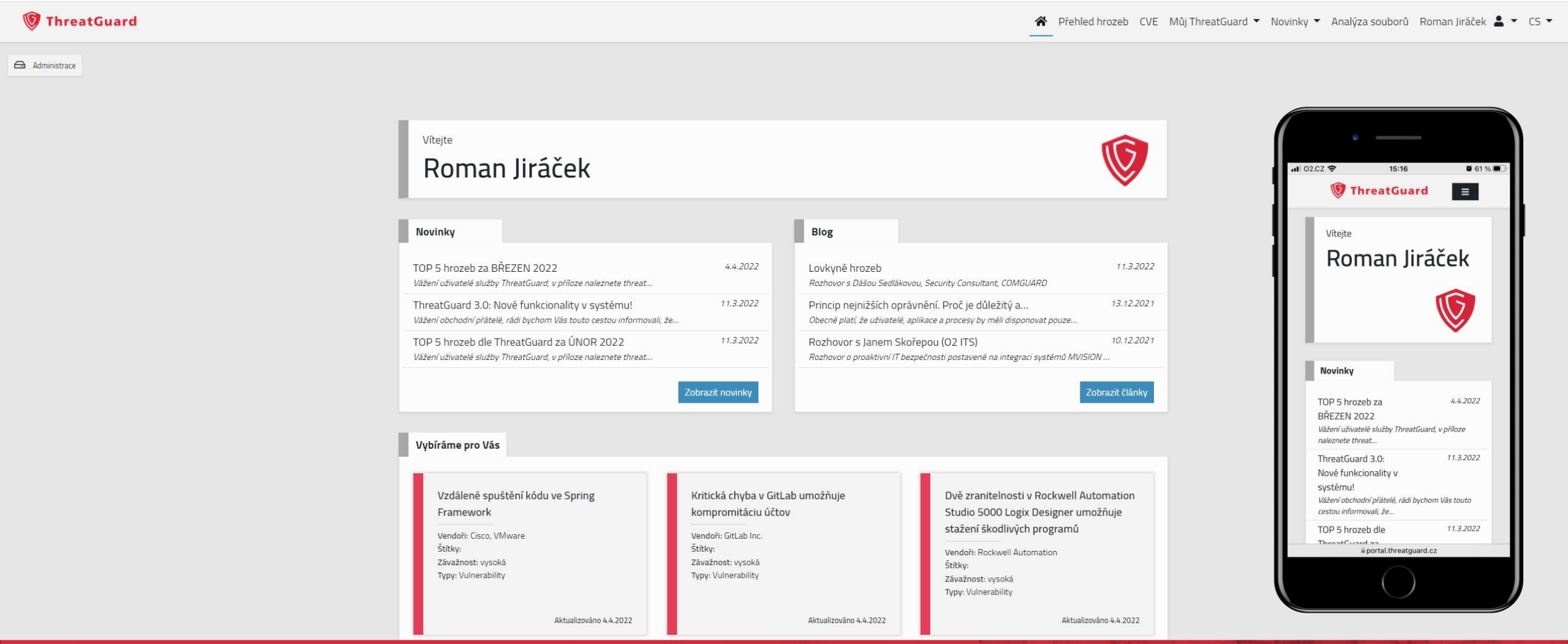
- Vzdálené převzetí kontroly v Apache Server



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.) – ELISA
- **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 Trellix ATD** – nahrajete neznámý soubor nebo URL adresu skrze ThreatGuard do McAfee, kde se otestuje a řekne Vám, jestli je v pořádku nebo kritický
- **Integrace s Whalebone Immunity** – zjistěte reputaci domény prostřednictvím portálu ThreatGuard

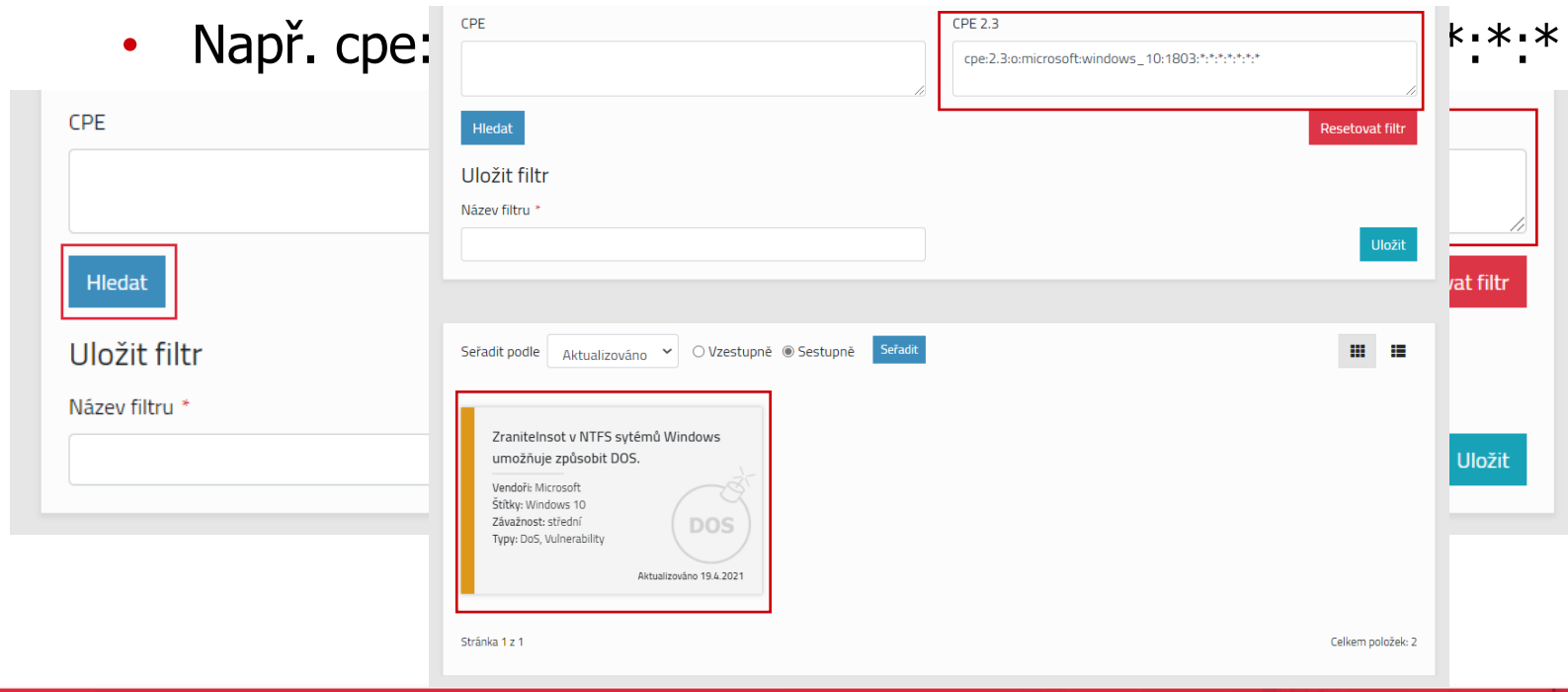
CPE string je název software, aplikace a její konkrétní verze ve formátu, který je standardizovaný

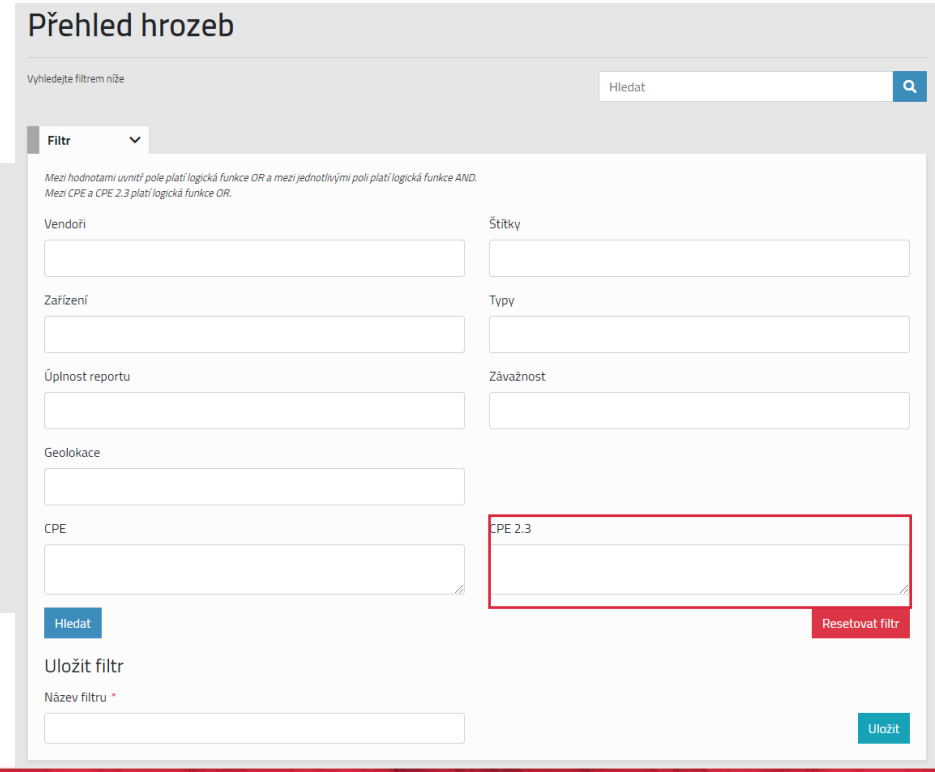
- CPE slovník: [NVD - CPE (nist.gov)]

Jak CPE string dohromady?

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

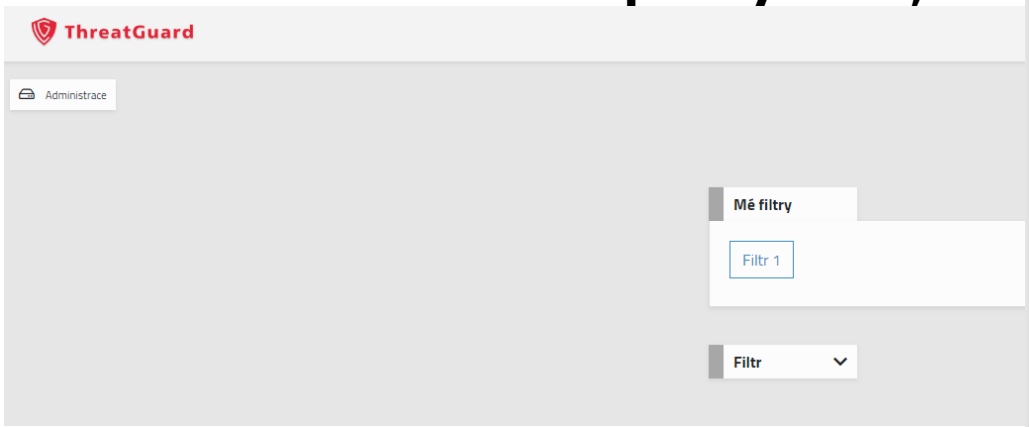
- Např. cpe:





CVE katalog

- Zrcadlení celého CVE katalogu d
- **Možnosti filtrování v CVE dat**
  - Dle ID u dané CVE
  - Poslední aktualizace
  - Publikováno
  - **Aktivní filtr per Výrobce, Zaří**



ID	CVSS	Shrnutí
	10 -	
CVE-2020-29659	10	A buffer overflow in the web server of Flexense DupScout Enterprise 10.0.18 allows a remote anonym
CVE-2021-42392	10	The org.h2.util.JdbcUtils.getConnection method of the H2 database takes as parameters the class nam various attack...
CVE-2020-29552	10	An issue was discovered in URVE Build 24.03.2020. By using the _internal/pc/vpro.php?mac=0&ip=0&

CVE-2020-29659

ID	CVE-2020-29659
Shrnutí	A buffer overflow in the web server of Flexense DupScout Enterprise 10.0.18 allows a remote anonymous attacker to execute code as SYSTEM by overflowing the sid
Reference	https://www.dupscout.com
Zranitelné konfigurace	cpe:2.3:a:flexense:dupscout:10.0.18:*:*:*:enterprise:*:*:*
CVSS	10
CWE	CWE-120

Přístupnost

Authentication	Complexity	Vector
NONE	LOW	NETWORK

Dopad

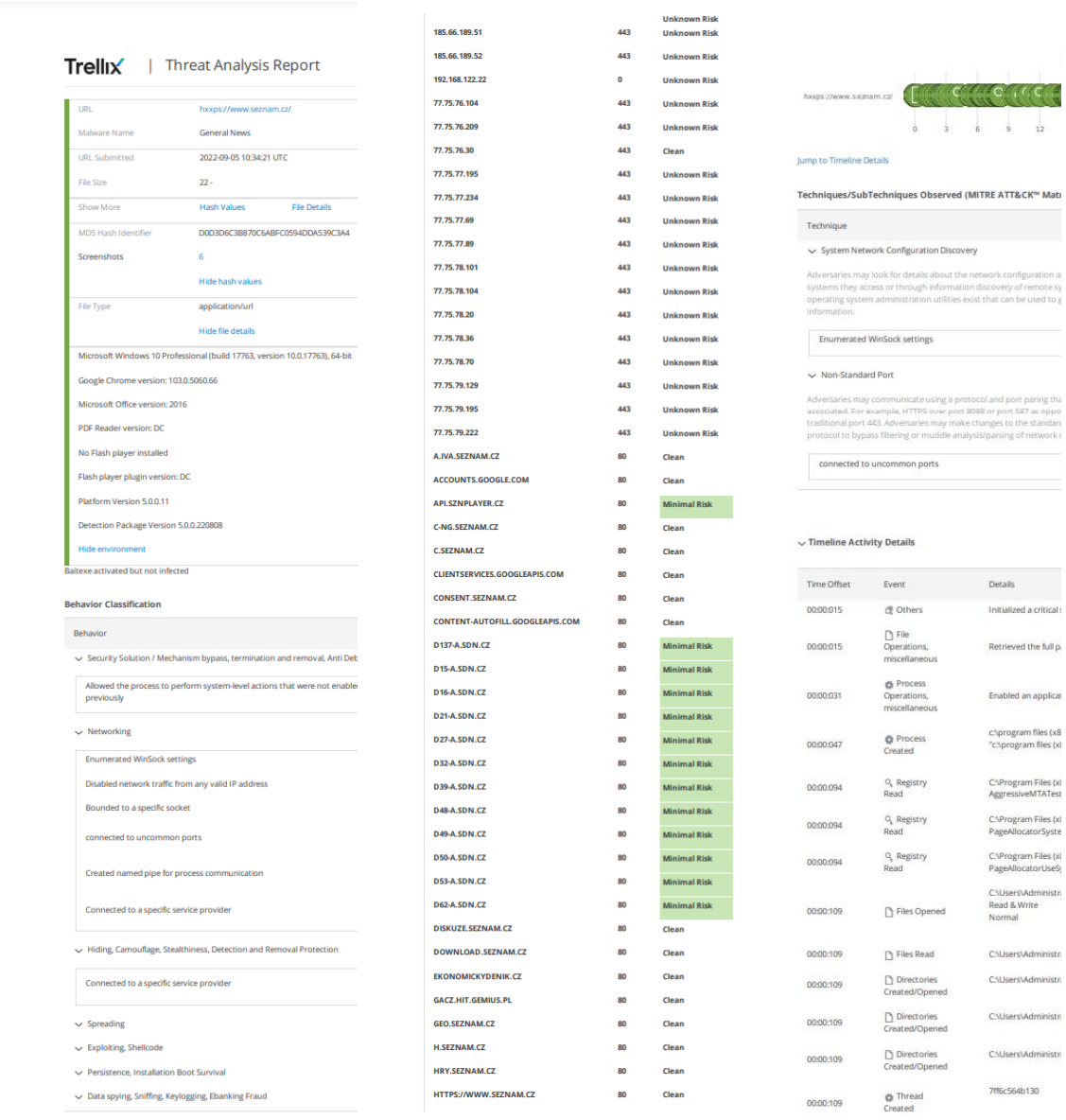
Availability	Confidentiality	Integrity
COMPLETE	COMPLETE	COMPLETE

CVSS vektor	AV:N/AC:L/Au:N/C:C/I:C/A:C
Poslední velká aktualizace	3.9.2022 - 03:58
Publikováno	9.12.2020 - 17:15
Poslední úpravy	3.9.2022 - 03:58

Vendoři

Zařízení

Štítky



Trellix | Threat Analysis Report

URL	hxxps://www.seznam.cz/
Malware Name	General News
URL Submitted	2022-09-05 10:34:21 UTC
File Size	22 -
Show More	Hash Values File Details
MD5 Hash Identifier	D0D3D6C3B870C6ABFC0594DDA539C3A4
Screenshots	6
	Hide hash values
File Type	application/url
	Hide file details

Microsoft Windows 10 Professional (build 17763, version 10.0.17763), 64-bit
Google Chrome version: 103.0.5060.66
Microsoft Office version: 2016
PDF Reader version: DC
No Flash player installed
Flash player plugin version: DC
Platform Version 5.0.0.11
Detection Package Version 5.0.0.220808
Hide environment

Baitexe activated but not infected

Behavior Classification

Behavior

- Security Solution / Mechanism bypass, termination and removal, Anti Deb
  - Allowed the process to perform system-level actions that were not enable previously
- Networking
  - Enumerated WinSock settings
  - Disabled network traffic from any valid IP address
  - Bounded to a specific socket
  - connected to uncommon ports
  - Created named pipe for process communication
  - Connected to a specific service provider
- Hiding, Camouflage, Stealthiness, Detection and Removal Protection
  - Connected to a specific service provider
- Spreading
- Exploiting, Shellcode
- Persistence, Installation Boot Survival
- Data spying, Sniffing, Keylogging, Ebanking Fraud

		Unknown Risk
185.66.189.51	443	Unknown Risk
185.66.189.52	443	Unknown Risk
192.168.122.22	0	Unknown Risk
77.75.76.104	443	Unknown Risk
77.75.76.209	443	Unknown Risk
77.75.76.30	443	Clean
77.75.77.195	443	Unknown Risk
77.75.77.234	443	Unknown Risk
77.75.77.69	443	Unknown Risk
77.75.77.89	443	Unknown Risk
77.75.78.101	443	Unknown Risk
77.75.78.104	443	Unknown Risk
77.75.78.20	443	Unknown Risk
77.75.78.36	443	Unknown Risk
77.75.78.70	443	Unknown Risk
77.75.79.129	443	Unknown Risk
77.75.79.195	443	Unknown Risk
77.75.79.222	443	Unknown Risk
A.IVA.SEZNAM.CZ	80	Clean
ACCOUNTS.GOOGLE.COM	80	Clean
API.SZNPLAYER.CZ	80	Minimal Risk
C-NG.SEZNAM.CZ	80	Clean
C.SEZNAM.CZ	80	Clean
CLIENTSERVICES.GOOGLEAPIS.COM	80	Clean
CONSENT.SEZNAM.CZ	80	Clean
CONTENT-AUTOFILL.GOOGLEAPIS.COM	80	Clean
D137-A.SDN.CZ	80	Minimal Risk
D15-A.SDN.CZ	80	Minimal Risk
D16-A.SDN.CZ	80	Minimal Risk
D21-A.SDN.CZ	80	Minimal Risk
D27-A.SDN.CZ	80	Minimal Risk
D32-A.SDN.CZ	80	Minimal Risk
D39-A.SDN.CZ	80	Minimal Risk
D48-A.SDN.CZ	80	Minimal Risk
D49-A.SDN.CZ	80	Minimal Risk
D50-A.SDN.CZ	80	Minimal Risk
D53-A.SDN.CZ	80	Minimal Risk
D62-A.SDN.CZ	80	Minimal Risk
DISKUZE.SEZNAM.CZ	80	Clean
DOWNLOAD.SEZNAM.CZ	80	Clean
EKONOMICKYDENIK.CZ	80	Clean
GACZ.HIT.GEMIUS.PL	80	Clean
GEO.SEZNAM.CZ	80	Clean
H.SEZNAM.CZ	80	Clean
HRY.SEZNAM.CZ	80	Clean
HTTPS://WWW.SEZNAM.CZ	80	Clean

Jump to Timeline Details

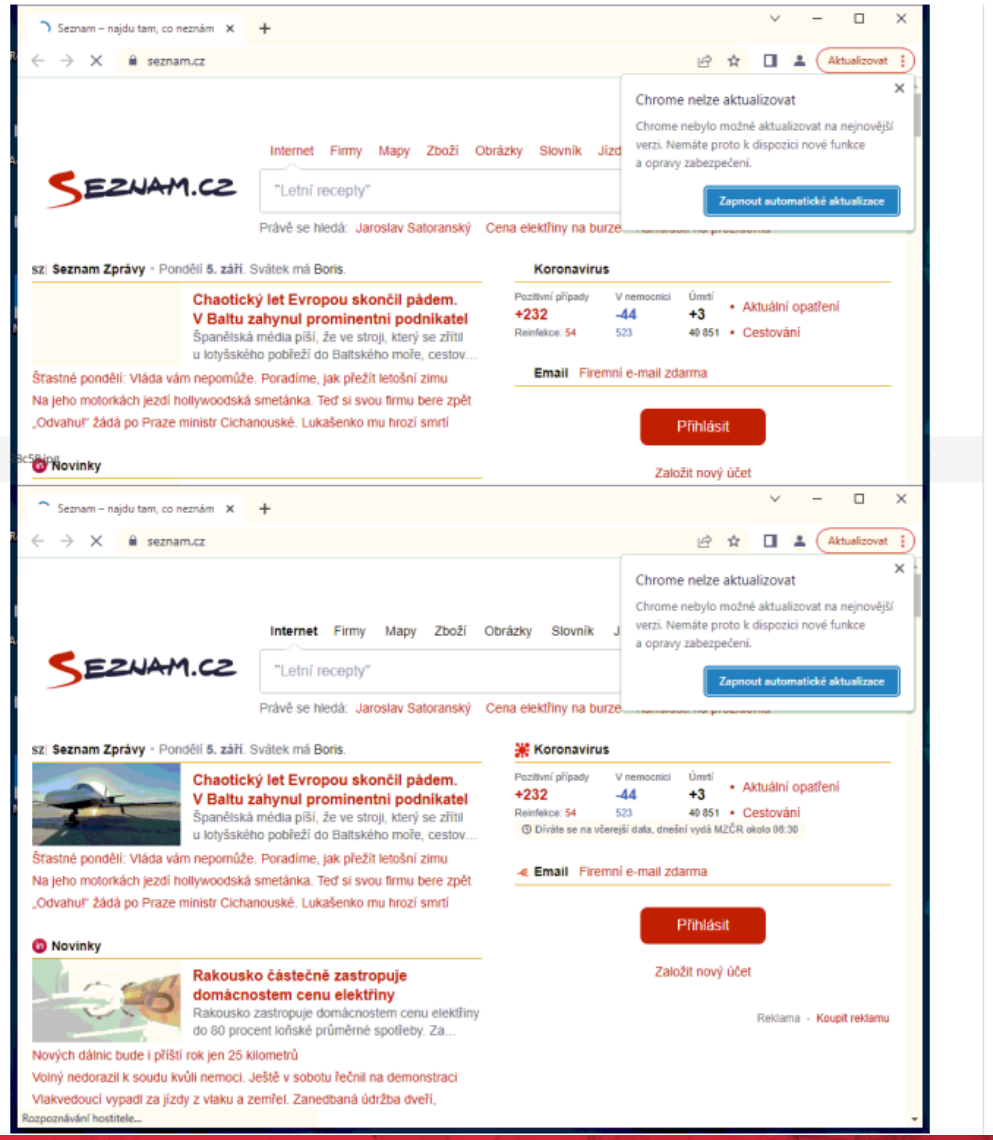
Techniques/SubTechniques Observed (MITRE ATT&CK™ Mat

Technique

- System Network Configuration Discovery
  - Enumerated WinSock settings
- Non-Standard Port
  - connected to uncommon ports

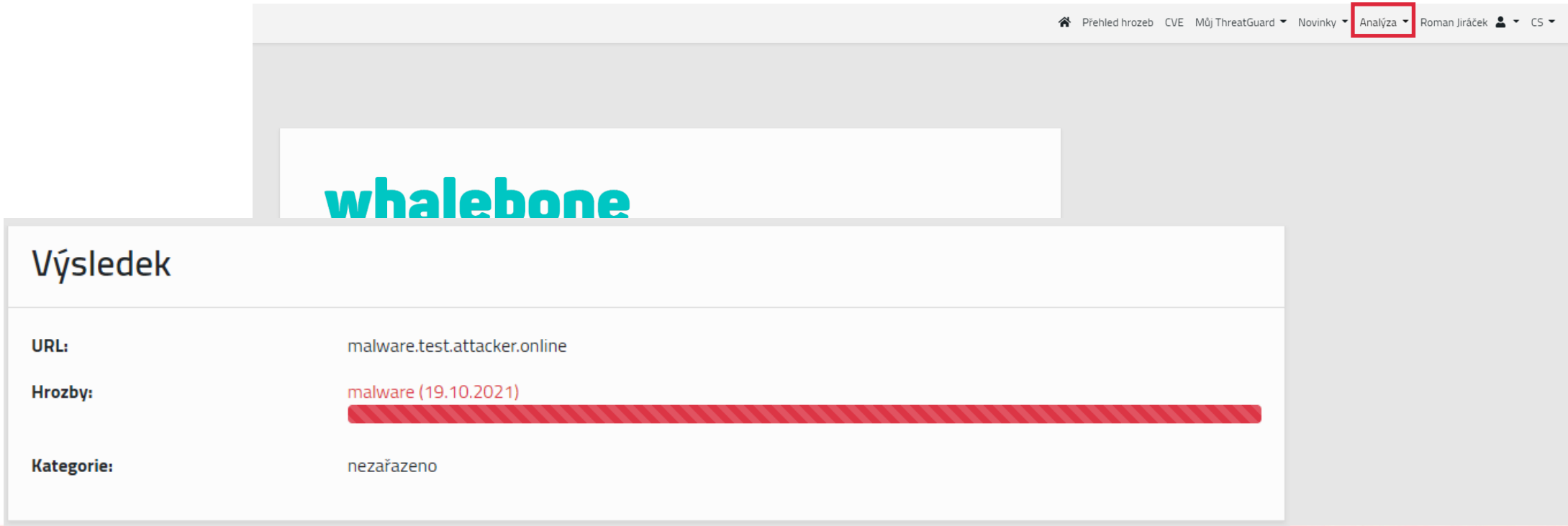
Timeline Activity Details

Time Offset	Event	Details
00:00:015	Others	Initialized a critical
00:00:015	File Operations, miscellaneous	Retrieved the full p
00:00:031	Process Operations, miscellaneous	Enabled an applica
00:00:047	Process Created	c:\program files (x8 "c:\program files (x
00:00:094	Registry Read	C:\Program Files (x AggressiveMTATest
00:00:094	Registry Read	C:\Program Files (x PageAllocatorSyste
00:00:094	Registry Read	C:\Program Files (x PageAllocatorUseS
00:00:109	Files Opened	C:\Users\Administr Read & Write Normal
00:00:109	Files Read	C:\Users\Administr
00:00:109	Directories Created/Opened	C:\Users\Administr
00:00:109	Directories Created/Opened	C:\Users\Administr
00:00:109	Directories Created/Opened	C:\Users\Administr
00:00:109	Thread Created	7ff6c564b130



Integrace s Whalebone Immunity

- **Jednoduchý přístup k reputaci domény –** uživatel zadá doménu, např. www.portal.threatguard.cz (FQDN) a ThreatGuard zobrazí zdali je doména:
  - **Doména je v pořádku** – zobrazí kategorii domény (gambling, audio-video, advertisement apod.)
  - **Doména NENÍ v pořádku** – zobrazí informaci, o jakou doménu se jedná (C&C apod.)



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

Děkujeme za pozornost!

Přednášková část je nyní u konce.

Dotazy?

COMGUARD
communication security

TOMBOLA

Hodně štěstí!