COMGUARD
security & networking

ThreatGuard
Dostaňte IT hrozby pod kontrolu

Martin Votava
COMGUARD a.s.

Zastupujeme výrobce pro český a slovenský trh

1) Specializace na bezpečnost IT
   - ✓ Stabilní síť prodejních partnerů
   - ✓ Dlouhodobé partnerství s výrobci

2) Expertní služby
   - ✓ Nové řešení a služby
   - ✓ Školící středisko
   - ✓ Security Operation Services (SOS), identifikace a analýza událostí
   - ✓ Support centrum – podpora pro distribuovaná řešení
   - ✓ Audity, penetrační testy, poradenství
   - ✓ Kompetenční centrum

COMGUARD

Máme odborné znalosti

Odborné znalosti technického týmu:

- SOPHOS
  - **Autorizované školicí středisko**
  - **MSP distributor pro ČR a SR!**
- McAfee
  - „**Service Delivery Provider**" – professional services (SIEM, DLP, ePO, IPS…)
- Rapid7
  - **Autorizovaný školicí program** (2018)

- Certifikovaný/školený tým
  - CISSP, CompTIA Security+, PRINCE2

Aktuální školení (ATC):

- SOPHOS
  - Sophos XG FW Engineer
  - Sophos XG FW Architect
- McAfee
  - McAfee ePolicy Orchestrator, endpoint
  - McAfee IPS (Network Security Platform)
  - McAfee Web Gateway

Webinář – virtuální technik:

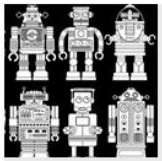
- Sophos
  - **Webinář Sophos - Odborný technický webinář - Intercept X Advanced s EDR**

COMGUARD

Přehled portfolia

COMGUARD

Aktuální informace o hrozbách v IT



14 MAY 2018 OPINION
Whose Team Is Artificial

11 MAY 2018 NEWS
EE Fix Portal Which Was

Microsoft Patches Two Zero-Day Flaws Under Active Attack

Tuesday, May 08, 2018 Swati Khandelwal

Share 1.69k Share Tweet Share

Safe Links

Learn Ethical Hacking Online: A to

11 MAY 2018 NEW
Chrome E
Malware

A new malware
links on Faceboc

Online IT Securi

Friday, April 20, 2018 Exclusiv

Share 997 Share

Hackers Found U
365 Safe Links

Tuesday, May 08, 2018 Mohit

Share 1.94k Share

11 MAY 2018 NEW
Bolton's P
Security I

Slashdot Stories Firehose All Popular Polls Deals Submit

Topics: Devices Build Entertainment Technology Open Source Science YRO

Please create an account to participate in the Slashdot moderation system

20 let narozeninový speciál

LUPA.cz
Server o českém internetu

active24 Generální partner

Google Hasn'

Posted by msr

An anonymous rea

If you're a Gma
email chains ar
whole host of o

Though Google
included in its
that Google als
within the Goo
a practice the

AKTUALITY

PGP a S/MIME obsahují
možné číst zašifrované

Pokud pro šifrování svých e-m
Good Privacy) a standard S/M
chráněné tak dobře, jak si... v

11:07 | 1

Jak bude svět vypadat z
obrázku do soutěže maj

Ještě do úterý 15. května se m
zúčastnit soutěže, kterou jsm
k 20. výročí založení serveru..

9:53

Nová verze aplikace Sky
televizory kombinuje sa

Hlavní předností nové verze a
kombinace výhod satelitní a i
ji operátor nabízí. Aplikaci si..

6:00

California Hig

Posted by msr

Police in Concord,
campaign directed

The 16-year-olc
enforcement, w
trickle into polic
turns out, they were part of a phishing at
constructed by the student to look like t
their username and password. The site v

seduo.cz

ROOT.CZ Články Zprávičky Fórum Podpořte Root Blogy Galerie Kalendář Root do mailu RSS Práce v IT Školení Knihy

reklama

ZPRÁVIČKY

Cloudflare – DNS, CDN a DD
jednom (školení)

Není vám lhostejná rychlost vašich
řešit DDoS útoky ani TLS certifikáty
kupovat drahé fyzické firewally, DDc

11:38

Gmail nepřestal číst obsah
e-mailů

Loni Gmail od Google prohlásil, že u
automatické skenování obsahu e-m
cílení reklamy. Důvodem byly obavy

11:01 | 3

Spor System76 a Fwupd

Mezi známým výrobcem linuxových
System76 a Richard Hughesem z R
rozhořel spor o to, jak aktualizovat f
je... více

10:10 | 4

jobs.cz Práce

- Programátor PLC
- Idea maker (a taky tak trochu analyti
- HW designér, vývoj elektroniky

PC REVUE

Správy Magazín Recenzie AkoNaTo ITPro Video Startupy Archív

Lenovo chce dať konvertibilným počítačom ohybný displej s notifikáciami na boku à la Edge

Technológie
15. 05. 2018

Steam Link prichádza na mobilné platformy. PC hry si zahráte už aj na smartfóne

Technológie
15. 05. 2018

Talianski vedci vyvinuli ľahšiu a lacnejšiu robotickú ruku. Dokáže pracovať s ceruzkou či používať príborový nôž

Výskum
15. 05. 2018

VYHĽADÁVANIE

Hľadať v článkoch Hľadať

Roboty Boston Dynamics sa učia behať po vonku. Vyzerajú stále prirodzenejšie

Technológie
15. 05. 2018

Univerzity otvárajú špeciálne študijné programy zamerané na umelú inteligenciu. Cieľom je používať ju na sociálne dobro

Informatizácia
15. 05. 2018

Aplikácia Tatrabanky vás už spozná podľa tváre

Produkty
14. 05. 2018

24 Hodín Týždeň Mesiac

Roboty Boston Dynamics sa učia behať po vonku. Vyzerajú stále prirodzenejšie (199)

Steam Link prichádza na mobilné platformy. PC hry si zahráte už aj na smartfóne (124)

Aplikácia Tatrabanky vás už spozná podľa tváre (124)

Lenovo chce dať konvertibilným počítačom ohybný displej s notifikáciami na boku à la Edge (103)

COMGUARD

Množství informací o hrozbách v IT

- Velkém množství zpráv
- Nestrukturované informace
- Všemožný charakter

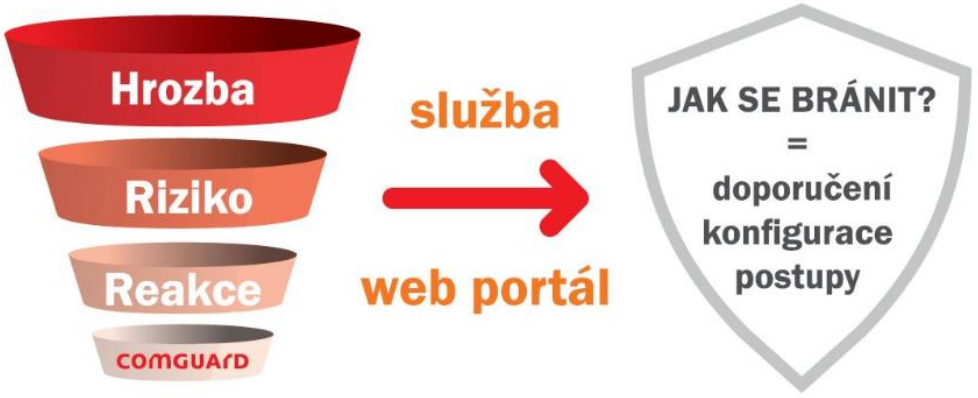
- [webapps] Monstra CMS 3.0.4 - Arbitrary Folder Deletion Monstra CMS 3.0.4 - Arbitrary Folder Deletion
- [webapps] Open-AudIT 2.1 - CSV Macro Injection Open-AudIT 2.1 - CSV Macro Injection
- [shellcode] Linux/x86 - execve(cp /bin/sh /tmp/sh; chmod +s /tmp/sh) + Null-Free Shellcode (74 bytes) Linux/x86 - execve(cp /bin/sh
- [shellcode] Linux/x86 - chmod 4755 /bin/dash Shellcode (33 bytes) Linux/x86 - chmod 4755 /bin/dash Shellcode (33 bytes)
- [shellcode] Linux/x86 - Reverse TCP (127.1.1.1:5555/TCP) Shell Shellcode (73 Bytes) Linux/x86 - Reverse TCP (127.1.1.1:5555/TCP)
- [shellcode] Linux/x86 - Edit /etc/sudoers (ALL ALL=(ALL) NOPASSWD: ALL) For Full Access + Null-Free Shellcode (79 bytes) Linux/
- [papers] Building a Proxy Fuzzer for MQTT with Polymorph Framework Building a Proxy Fuzzer for MQTT with Polymorph Framework
- Securing financial data of the future: behavioral biometrics explained Some of us would be pretty excited about a brave, new passwordl
- [shellcode] Linux/x86 - Bind TCP (1337/TCP) Shell + Null-Free Shellcode (92 bytes) Linux/x86 - Bind TCP (1337/TCP) Shell + Null-Fre
- Glusterfs Snapshot Scheduler Privilege Escalation Vulnerability A vulnerability in the snapshot scheduler of glusterfs could allow an un
- Linux Kernel arch_timer_reg_read_stable Macro Denial of Service Vulnerability A vulnerability in the Linux Kernel could allow a local at
- Fifth Generation Phishing Kits Have Arrived US Security Data Part " Give a man a fish and you feed him for a day. Teach a man tc
- 5 great talks you may have missed at RSA 2018 We value every opportunity to get face time with our customers and partners, and to
- Nintendo Switches Hacked to Run Linux—Unpatchable Exploit Released Two separate teams of security researchers have published
- [webapps] WUZHI CMS 4.1.0 - Cross-Site Request Forgery WUZHI CMS 4.1.0 - Cross-Site Request Forgery
- [webapps] UK Cookie Consent - Persistent Cross-Site Scripting UK Cookie Consent - Persistent Cross-Site Scripting
- How to Steal Bitcoin Wallet Keys (Cold Storage) from Air-Gapped PCs Dr. Mordechai Guri, the head of R&D team at Israel's Ben Guri

COMGUARD

Co to je ThreatGuard?

- ThreatGuard je zdroj informací!
  - Stále dostupná, aktuální a strukturovaná databáze hrozeb a opatření.
  - Přehled kritických a nebezpečných hrozeb pro Vaše technologie, vč. rad a doporučení, jak se správně bránit.

- **Virtuální bezpečnostní analytik**



ThreatGuard

security & networking

COMGUARD

Zdroje informací

- Tým vyhodnocuje informace z různých zdrojů:
  - Webové stránky
  - Databáze exploitů
  - Sociální sítě
  - Newsfeedy vendorů
  - CSIRT týmy
  - další veřejná i neveřejná média a aktuálně řešené incidenty v našem regionu.
- Seznam desítek pečlivě vybraných zdrojů s ověřenými informacemi je sledován.
- Seznam zdrojů informací se průběžně upravuje.
- Nikdy nekončící proces vyhledávání relevantních zdrojů informací.

Zpracování hrozeb

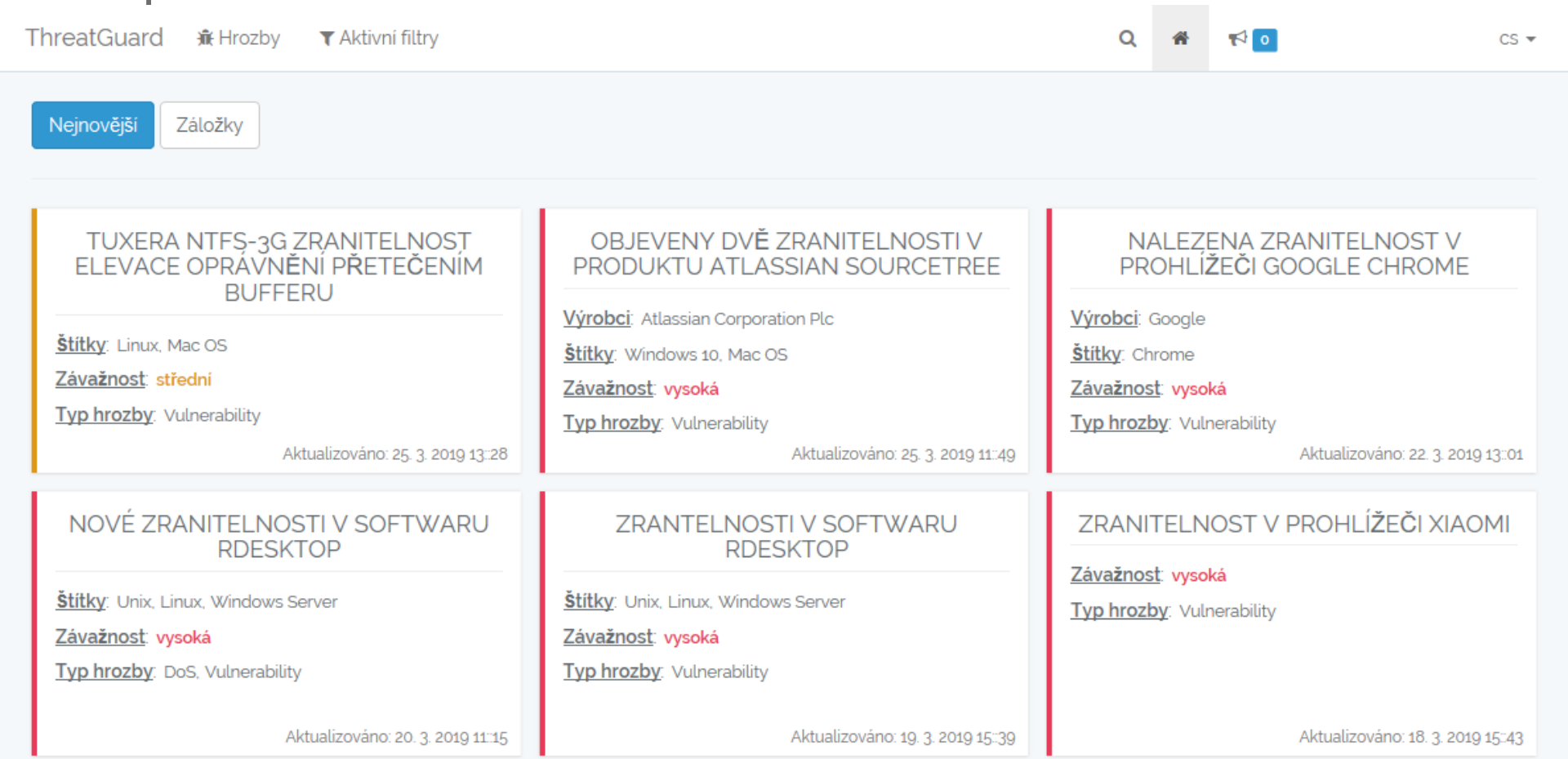
- Tým několikrát denně vyhodnocuje zdroje informací
  - Vstupní otázky:
    - Týkají se nějak firemní a enterprise infrastruktury?
    - Mohou postihnout náš region?
    - Jedná se o existující hrozbu nebo jde jen o teoretický koncept?
    - Jde o upřesnění již dříve uveřejněné hrozby či opatření?

- Zveřejnění hrozeb a opatření
  - Analytik ihned informuje o relevantní hrozbě v podobě konceptu a alespoň jednoduché nápravy.
  - Detailní popis hrozby a opatření jsou dalšími úkoly v procesu zveřejnění reportu.
  - Následuje upřesnění či doplnění míry detailu popisu i opatření plného či rozšířeného reportu dle dostupných informací.
  - Hrozby i opatření jsou zpětně kontrolovány dalšími členy týmu.

COMGUARD

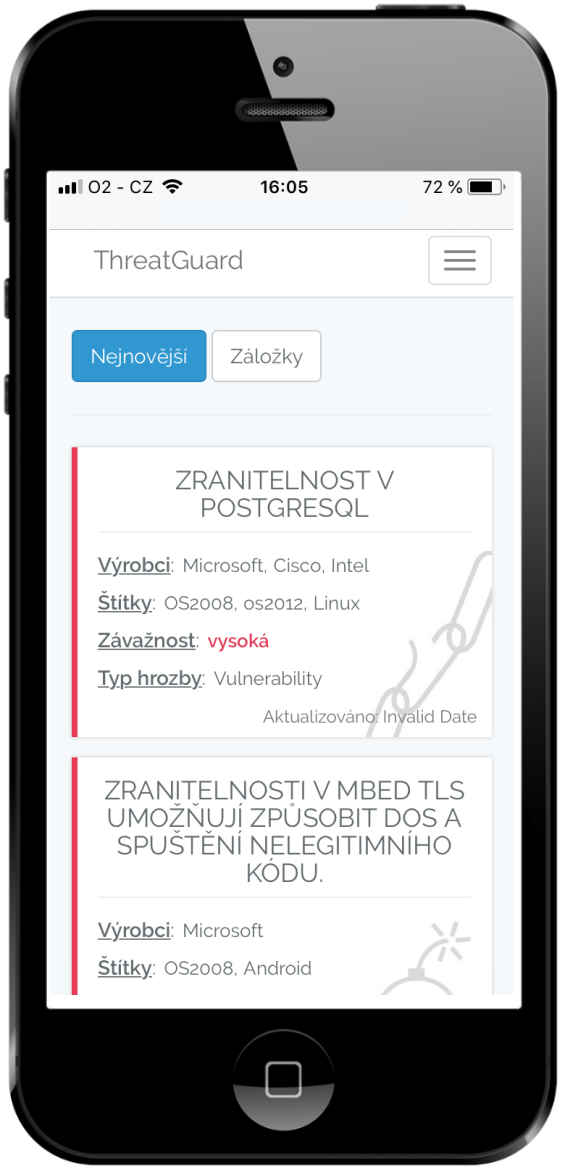
Webové rozhraní

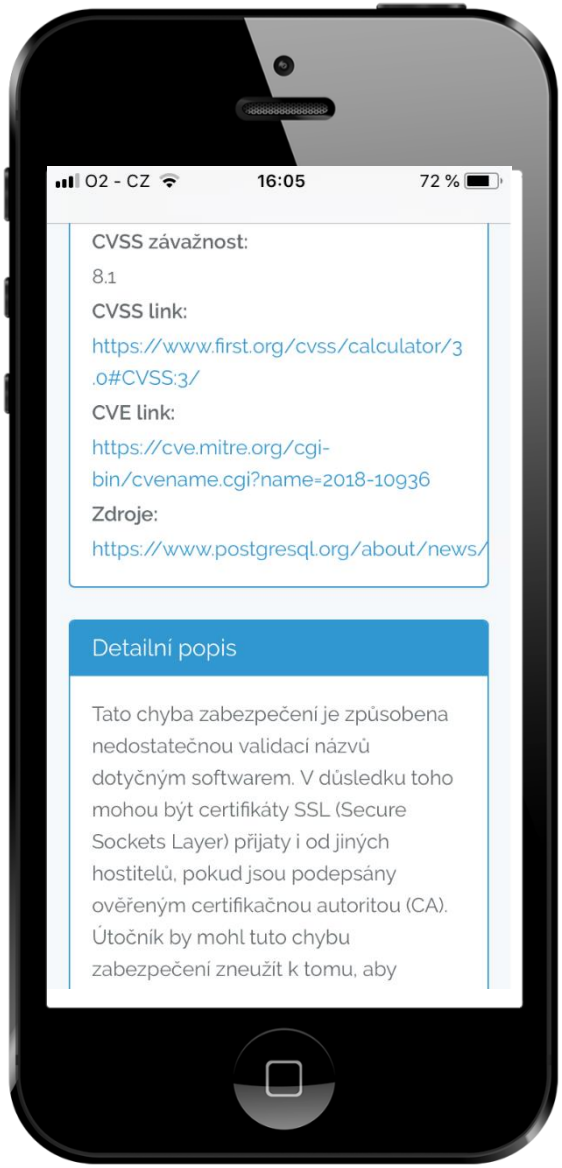
- Stále dostupná, aktuální a strukturovaná databáze hrozeb a opatření



COMGUARD

Mobilní přístup





Hrozba

- Každá hrozba má svůj strukturovaný záznam

Těžba kryptoměn v kontejnerovém systému Docker

Základní údaje

Úplnost reportu:	koncept
Stav reportu:	zveřejněný
Typ:	Malware
Závažnost:	střední
Geolokace:	EU
Přidáno	06. 03. 2019 15:35
Aktualizováno	06. 03. 2019 15:38
Vytvořil:	ThreatGuard

Náprava

Striktně oddělit Docker API jen pro lokální systémy určené k jeho administraci popřípadě vývoji.

Opatření

Omezení přístupu k systému

Rozsah působnosti

Štítky:	Linux, Windows Server
Zařízení:	Server

Obsah

Krátký popis:	V poslední době bylo zaznamenáno zvýšené množství zneužití systémů s nezabezpečeným Docker API pro těžbu kryptoměn.
CVSS závažnost:	7.5
CVSS link:	https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H
CVE link:	
Zdroje:	https://blog.trendmicro.com/trendlabs-security-intelligence/exposed-docker-control-api-and-community-image-abused-to-deliver-cryptocurrency-mining-malware/ https://blog.trendmicro.com/trendlabs-security-intelligence/misconfigured-container-abused-to-deliver-cryptocurrency-mining-malware/

Detailní popis

Útočník nejprve vyhledá dostupné nezabezpečené Docker API. Následně instaluje nový kontejner a spustí skripty pro modifikaci a následnou těžbu kryptoměny. Současně se před odhalením poměrně úspěšně skrývá za běžné procesy běžící na standardním systému.

Verze Dockeru jsou relativně nové, cca polovina byla identifikovaná jako 18.06.1-ce a běží především na Linuxovém, ale i Windows systému.

Modifikované systémy byly nalezeny celosvětově především v USA, Singapuru a Číně, ale i v Evropě ve Francii, Nizozemí, Švicarsku, Německu či Velké Británii a Irsku.

COMGUARD

Opatření

- Opatření jsou přiřazována hrozbám a udržována a aktuální

Omezení přístupu do C:\Windows\Tasks

Základní údaje

Ověřenost:	Testováno
Přidáno	06. 09. 2018 14:31
Naposledy upraveno	06. 09. 2018 14:31
Přidal:	ThreatGuard

Přílohy

- Příloha 1

Zdroje

https://www.kb.cert.org/vuls/id/906424

Popis

Opatření třetí strany:

Úprava ACL k zložke C:\Windows\Task

Táto zmena nie je ofciálne podporovaná spoločnosťou Microsoft. Po zmene ACL fungujú plánované úlohy a uživatelia môžu vytvárať nové. Prestanú však fungovať úlohy vytvorené legacy rozhraním plánovača úloh.

V príkazovom riadku s navýšenými právami spustite nasledovné príkazy:

icacls c:\windows\tasks /remove:g "Authenticated Users"
icacls c:\windows\tasks /deny system:(OI)(CI)(WD,WDAC)

Zmeny ACL vrátite do pôvodného stavu nasledujúcimi príkazmi:

icacls c:\windows\tasks /remove:d system
icacls c:\windows\tasks /grant:r "Authenticated Users":(RX,WD)

Opatření McAfee Endpoint Security - Idea (v testování)

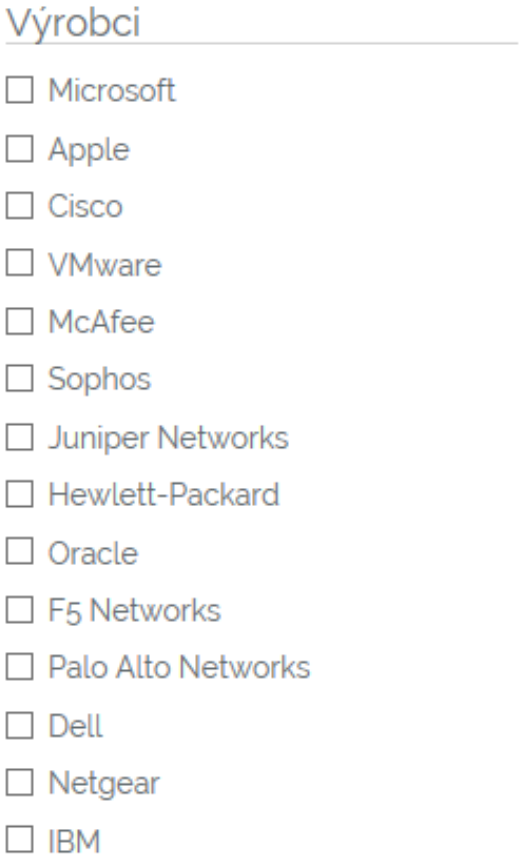
Access Protection politika

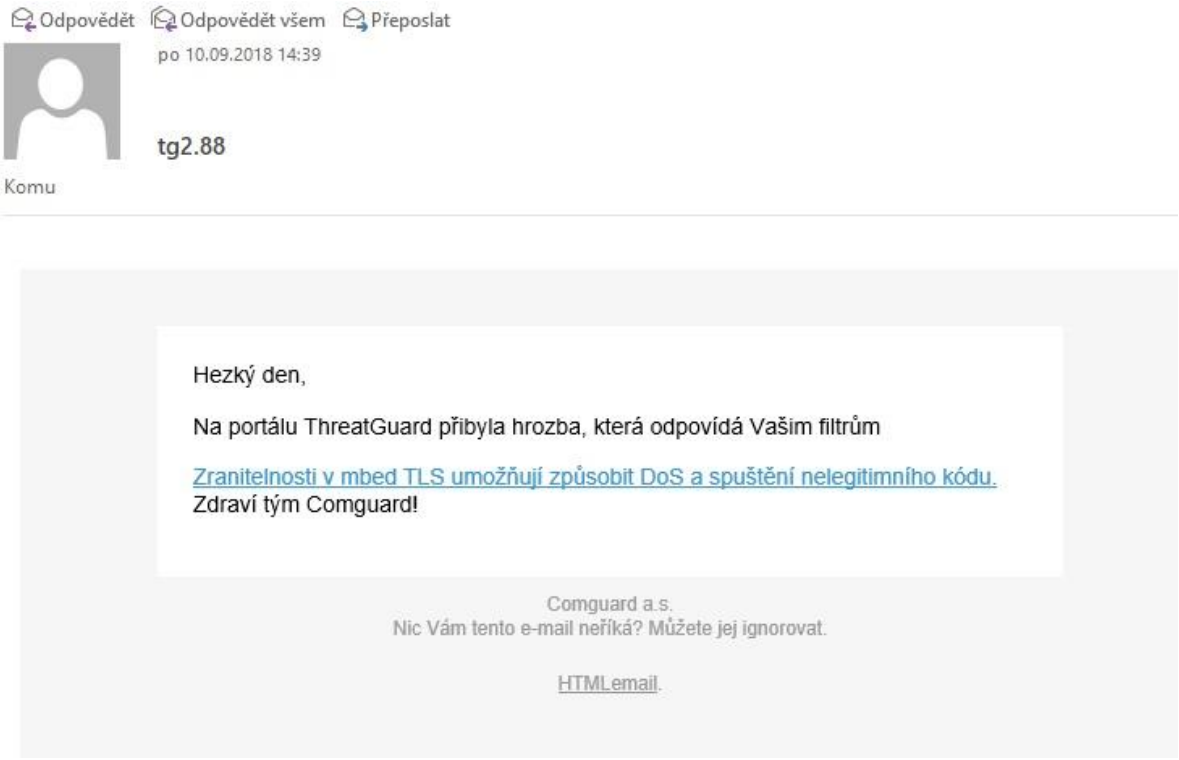
- ALPC_privilege_escalation.xml

Politika zakazuje všem uživatelům mimo Local\System vytvářet a modifikovat soubory v umístění C:\Windows\Task. Politika je pouze v logovacím režimu, pro blakaci je nutné přepnout Action na"Block".

Filtry a notifikace

- Filtrace podle všech atributů (typ hrozby, dotčená aktiva, typ opatření, atd.)
- Customizované notifikace na hrozby a opatření

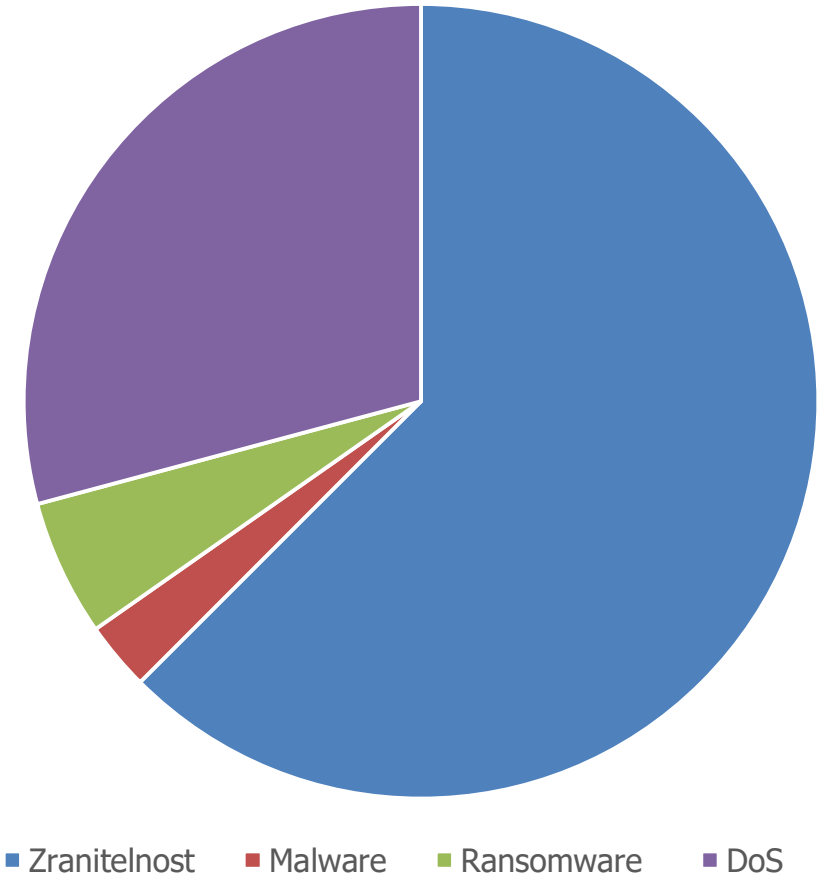




COMGUARD

Sledování aktuálních trendů ve světě hrozeb

- Za poslední dva měsíce ThreatGuard upozornil na
  - celkem 72 hrozeb



COMGUARD

Co přináší ThreatGuard 2.0

- **Webová aplikace postavená přímo na míru požadavkům koncových zákazníků –** jednoduchá a přehledný systém
- **News –** aktuální informace pro uživatele (workshopy, konference, PROMO akce apod.)
- **Support expertního týmu** – tým analytiků bude k dispozici pro Vaše požadavky a bude je primárně řešit prostřednictím realtime chatu
- **Emailová notifikace na aktuální hrozby –** efektivní a rychlá informovanost o nejnovějších IT hrozbách
- **Služba dostupná v ČJ a EN**

Novinky v ThreatGuard 2.0

- **Novinky v ThreatGuard 2.0**
  - TOP 5 hrozeb dle ThreatGuard za MĚSÍC
    - Výběr TOP 5 aktuálních hrozeb každý měsíc = **VAŠE MAXIMÁLNÍ INFORMOVANOST**
  - Aplikace postavená na míru požadavkům koncových uživatelů
    - Zapracování požadovaných funkcionalit od zákazníků = **MAXIMÁLNÍ UŽIVATELSKÁ PŘÍVĚTIVOST**

- ThreatGuard 2.0 - Evidované chyby:
  - Prosinec 2018:
    - [illegible]vní pozvánky (tenantní větev)
    - [illegible]vání [illegible]ozeb (platnost stránky)
    - Vy[illegible]ení hrozeb současné vytváření 2 editorů)
    - Upozornění na [illegible]by (draft)
    - Přetékaní odkazů
    - Prodloužení SSL certifikátu
    - Tlačítko „ZPĚT"
    - Optimalizace TG 2.0 pro prohlížeče MS Edge, IE, Firefox, Chrome
    - Hlídka v administrátorském rozhraní
    - Zobrazení tenantního GUI

ZAPRACOVÁNO!

- ThreatGuard 2.0 – Nové funkcionality:
  - Prosinec 2018:
    - Zobrazení emailů
    - Historie v rámci Realtime chatu (admin i user rozhraní)

TOP 5 hrozeb dle ThreatGuard

Nově v rámci naší expertní služby ThreatGuard – virtuální bezpečnostní analytik přicházíme s TOP 5 hrozbami uvedenými na našem portálu, protože chceme, abyste byli informováni o tom nejrizikovějším, co jsme za únor 2019 zachytili.

Top 5 hrozeb za ÚNOR 2019:

- Malware LoJax – AKTUALIZACE
- Zranitelnost Microsoft Windows Server 2008 R2
- Zranitelnost v OS GoogleAndroid
- Zranitelnost Dirty Sock – OHROŽENY LINUXOVÉ DISTRIBUCE
- Zranitelnost GNU Bash Remote Code Execution

COMGUARD

ThreatGuard 2.0 - zákazníci

- **Zákazníci si nejvíce cení:**
  - **Jednoduchého přístupu k aktuálním informacím o IT hrozbách**
  - **Proaktivního přístupu k vývoji aplikace ThreatGuard** – zapracování požadavků a funkcionalit od zákazníků
  - **Aktivní filtry** – zobrazení pouze aktiv, které máte nasazeny ve Vaší IT infrastruktuře
  - **Customizované notifikace** – jednoduché a efektivní získání potřebných informací o aktuálních IT hrozbách
  - **Support expertního týmu** – tým analytiků je k dispozici pro Vaše požadavky a bude je primárně řešit prostřednictvím realtime chatu
  - **Služba dostupná v ČJ a AJ**

COMGUARD

Proč ThreatGuard?

- Ideální pomocník pro Security či Operation Managera.
  - ThreatGuard poskytuje relevantní informace.
  - ThreatGuard odfiltruje zbytečný šum.
  - ThreatGuard popíše problém.
  - ThreatGuard identifikuje nápravu.
  - ThreatGuard zpracuje a případně i otestuje opatření.
  - ThreatGuard umožňuje konzultace.

- ThreatGuard šetří čas a peníze!

COMGUARD

Děkuji za pozornost

Otázky?

Martin Votava| martin.votava@comguard.cz | www.comguard.cz