

## ThreatGuard

- ∞ Nevíte, **jak čelit nejaktuálnějším bezpečnostním hrozbám?**
- ∞ Nalezení příčin a opatření trvá příliš dlouho a **malware se šíří dál a způsobuje další škody?**
- ∞ **Chybí vám dostupnost preventivních opatření na hrozby zaznamenané v ČR a SR?**
- ∞ **Dokážete určit míru rizika jednotlivých hrozeb pro Vaši společnost?**
- ∞ **Máte problém určit prioritu nápravným opatřením?**

### Potřebné informace na jednom místě

Služba ThreatGuard za vás *sleduje aktuální vývoj IT hrozeb* v prostředí CZ/SK – EU – svět, relevantní hrozby *ohodnotí mírou rizikovosti* a hlavně pro vás *připraví nápravná opatření*, které je vhodné aplikovat. Velkou výhodou služby ThreatGuard je, že *na jednom místě máte přehled všech relevantních hrozeb rozdělených dle zařízení*, na které cílí, rizikovosti a podrobného popisu, jakým způsobem se projevuje. Obsah portálu si můžete vyfiltrovat např. podle vámi využívaných zařízení a získáváte tak jen relevantní informace.

### Unikátní přístup

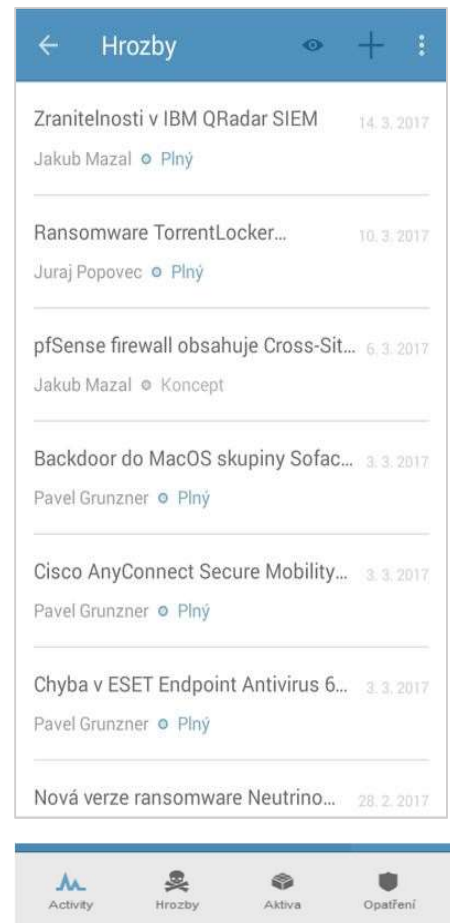
Obsah připravují vybraní specialisté dodavatele na základě vlastních zkušeností, veřejně dostupných informací a simulací. Obsah je uživatelům publikován ve formě ucelených reportů, které mohou být postupně upravovány a obměňovány. Obsah je připravován tak, aby byl **srozumitelný** bezpečnostním manažerům **i správcům konkrétních aktiv**, a aby mohl sloužit jako podklad pro kvalifikované rozhodnutí, zda je nutné a vhodné hrozbu řešit. Pokud se manažer rozhodne hrozbu řešit, má v reportu rovnou k dispozici informace pro administrátory, kterým informace poskytne jako přímočarý návod pro mitigaci hrozby.

### Možnosti ThreatGuard

**TG Portal** – tým expertů pro vás **denne sumarizuje aktuální hrozby a zranitelnosti** z více než 30 ověřených zdrojů a **vyhodnotí jejich relevantnost** pro prostředí organizací v ČR/SR. Vše srozumitelně popsáno, opatřeno doporučeními na úrovni konfigurací nebo workaroundů. Pomůžeme vám jak s preventivními opatřeními, tak v případě napadení výrazně urychlíme vaši akceschopnost.

**TG HelpMe** – nástavba nad TG Portal přináší navíc možnost zadat vlastní problém, tým expertů zanalyzuje prioritně příčinu a vyhodnotí návrhy opatření, které budou publikovány v rámci Portálu.

**ThreatGuard HelpDesk** – nástavba nad TG HelpMe přináší navíc dostupnost individuálních konzultací a podpory a to i v rámci realizace opatření typických pro prostředí zákazníka, analýza příčin a zdrojů.



### Hlavní přínosy ThreatGuard

- ∞ Pouze **relevantní hrozby stručně a přehledně**.
- ∞ Dostupné jako webová a mobilní aplikace pro Android a iOS.
- ∞ Filtrování dle aktiv, která mě zajímají.
- ∞ Omezení šíření hrozby v síti díky okamžitému přístupu do portálu.
- ∞ Snadná akceschopná opatření.
- ∞ Možnost vložit požadavek na rozpracování konkrétní hrozby.
- ∞ Ideální nástroj pro Security Managera.
- ∞ Nutný nástroj pro Operation Managera (provozu).
- ∞ Hrozby rozděleny na kategorie: zranitelnost, malware, phishing, ransomware.

~ 300.. partnerů/resellerů  
~ 3.000.. spokojených klientů  
~ 300.000..... zachráněných dat

**"Scam" balíček s fonty pro Google Chrome**

Malware "Scam" vyzve uživatele při návštěvě nakažené webové stránky k falešné aktualizaci doplňku prohlížeče Google Chrome "Chrome Font Pack". Při potvrzení se malware nainstaluje do systému. "Scam" se využívá pro nakažení počítače ransomwarem "Spora".

Phishing Ransomware

Aktiva: MacOS

Doporučení: Použití pluginov, ktoré blokujú java...

23/02/2017 by Jan Procházka

**Ransomware Osiris - nový přírůstek do rodiny Locky**

Jedná se o nový ransomware, který napadá platformy Windows, Apple i Android. Šíří se prostřednictvím spamu, podvržené reklamy. Je schopen sám se šířit po doménové síti, i pomocí CRM systémů (včetně cloudových). Napadá lokální i síťové složky, i NAS. Je schopen detekovat virtuální prostředí. Šifruje soubory a #444 účinně.

Malware Ransomware

Aktiva: MacOS

Doporučení: Access Protection politika pro McAf...

31/01/2017 by Pavel Grunzner

**F5 BIG-IP SSL Virtual Server - Memory Leak**

Zariadenia F5 BIG-IP obsahujú zraniteľnosť, ktorá umožňuje útočníkovi získat' 31 bytov z pamäti. Ak je na virtuálnom serveri konfigurovaný klientský SSL profil, ktorý má zapnutú voľbu "non-default Session Tickets", môže útočník získat' obsah neinicializovanej pamäti. Tá môže obsahovat' ID iných SSL spojení. Zabrániť tejto zraniteľnosti je možné zmenou firmwaru alebo úpravou

Zraniteľnosť

Aktiva not set

Doporučení: Zmena firmwaru F5 BIG-IP

13/02/2017 by Juraj Popovec

**CVSS link** <https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H>

**Detailní popis**

Pro šíření využívá email se zabaleným XLS souborem s VBA makrem nebo spustitelným JavaScriptem. Po spuštění stáhne DLL soubor, který spouští pomocí Rundll32.exe. V předmětu se vyskytují slova "Invoice" nebo "Order Confirmation".

Druhý způsob šíření je pomocí velkých reklamních sítí (zneužity byly např. BBC, NSN, AOL), kdy kód prošel jejich systémem ověřování. Díky tomu se dokáže šířit s minimální/nulovou interakcí uživatele.

Po spuštění v počítači se snaží šířit po lokální síti s využitím doménových účtů, dále zneužívá různých CRM systémů, kdy je schopen založit nový ticket a přidat se jako příloha. Tak se dostává k účtům s vyššími oprávněními.

V rámci své činnosti je schopen napadat různé zálohovací systémy, na napadených počítačích napadá službu Microsoft Volume Shadow Copy Service, kterou zakáže a následně maže všechny Shadow kopie.

Pro šifrování používá silný šifrovací algoritmus, čili není šance dešifrovat "hrubou silou".

Před odhalením pomocí Sandboxingu, respektive analýzou ve virtuálním prostředí se brání detekci virtuálního prostředí.

Do budoucna lze očekávat řadu kampaní různých variant tohoto malware, které budou v primární fázi schopny projít standardními bezpečnostními systémy.

**Doporučení**

Access Protection politika pro McAfee Endpoint Security

Konfigurace

Idea Opatření třetí strany Otestováno v labu Ověřeno v produkčním prostředí

**Popis**

**Off-line zá** Access Protection politika pro McAfee Endpoint Security modul Threat Prevention obsahující pravidla blokující chování známých typů ransomware.

**Neotvírat p** Nasazení pravidel doporučujeme provést nejdříve pouze v reportovacím módu a po kontrole, zda nedochází k blokování nezávadného softwaru, pravidla přepnout do režimu blokace.

**Files**

**ES-TP-Ransomware.xml** 88.0 kB  
 Attached by Jakub Mazal a month ago

**\* CVSS link**  
<https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H>

**CVE**

**CVE - CVE-2016-9244**  
 Common Vulnerabilities and Exposures  
 CVE.MITRE.ORG

Add another

**Doporučení**

Zmena firmwaru F5 BIG-IP

Aktualizace

Zraniteľnosť CVE-2016-9244 je možné odstrániť zm...

Úprava nastavení F5 BIG-IP

**Workaround**  
 Vypnutím voľby "Session Ticket" sa zraniteľnosť n...

**Garant projektu:**

**COMGUARD**

**Technologický partner:**



~ 300.. partnerů/resellerů  
 ~ 3.000.. spokojených klientů  
 ~ 300.000..... zachráněných dat