Battle card

DOTAZY (Q&A)

Otázka: Co je to vlastně ThreatGuard? V čem je lepší?

Odpověď: ***ThreatGuard = Virtuální bezpečnostní analytik = Služba = Webový portál s responzivním designem!***

Vyhodnotíme za vás nejen relevantní hrozby z až několika desítek zdrojů, určíme jejich priority a vektory šíření, připravíme i možná opatření. Pro zákazníky McAfee ePo, McAfee IPS, McAfee WG a EG až na úroveň exportu konfigurací.

Nabízíme Vám buď pomoc pro stávajícího IT Security Managera, nebo tak získáte virtuálního! Jakou pomoc?

- *Za měsíční poplatek získáte tým* ***stálých zaměstnanců*** *- bezpečnostních specialistů, kteří průběžně vybírají a zveřejňují z velkého množství upozornění jen ty relevantní a aktuální hrozby na webovém portálu.*
- *Máte přehled o* ***kritických a nebezpečných zranitelnostech a hrozbách*** *pro Vaše technologie.*
- ***Obdržíte rady a doporučení,*** *jak se správně bránit a jaká máte učinit bezpečnostní opatření.*

ŽE VÁM TO UŽ NĚKDO NABÍDNUL? A umí toto?

- *Poskytujeme konsolidované informace z až* ***několika desítek nezávislých informačních zdrojů****.*
- *ThreatGuard je postaven tak, aby uživatel viděl po přihlášení* ***pouze svoje technologie*** *a případně/volitelně byl na novinky* ***upozorňován mailem*** *pouze pokud nějaká v jeho zájmové oblasti nastane!*
- *ThreatGuard na rozdíl od podobných služeb např. od vendorů má* ***přesně stanovený proces****, jak se informace přidávají a posuzuje se průběžně i kvalita a rychlost = zdroje se přidávají i vyřazují, a to i od renomovaných bezpečnostních firem, protože jejich informace jsou bohužel často týdny až měsíce zastaralé.*
- *Vše určeno pro zákazníky v ČR a SR*

Otázka: Na co potřebuji ThreatGuard, když mám Skener zranitelnosti?

Odpověď: Jsou to dva jiné světy!

"SKENER ZRANITELNOSTÍ" primárně testuje Vaši vnitřní síť a kontroluje, zda byly aplikovány patche na známé zranitelnosti a zda jsou všechny OS a firmware aktuální.

"ThreatGuard" hlídá BEZPEČNOSTNÍ HROZBY:

- *Tedy zranitelnosti jsou podmnožinou jeho zaměření.*
- *O hrozbě skener zranitelnosti ani nemůže vědět a nemůže ani v mnoha případech pomoci! - Reakce na hrozbu není „jen" patchování, ale soubor komplexních opatření od personálních např. neotevírat mail, až po nastavení konkrétních zařízení = to Vám skener nikdy nezajistí!*

"ThreatGuard" je ZDROJ INFORMACÍ o:

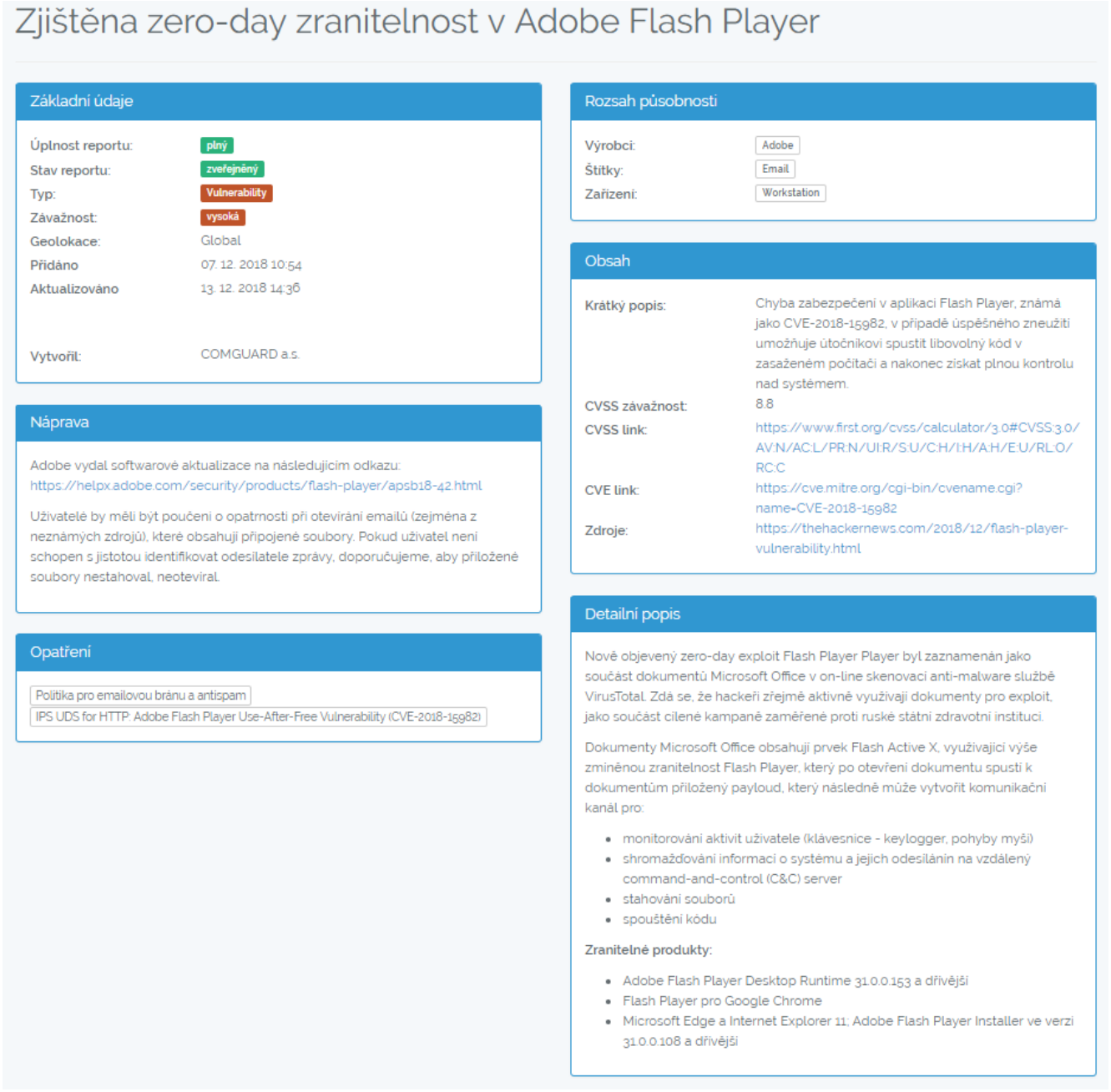
- *Všech hrozbách v ICT, mimo zranitelností systémů také malware, phishing, ransomware, HW i SW vč. různých rozšíření, neopomínaje např. rozšíření webových prohlížečů, atd.*
- *Opatřeních pro reálně uplatnitelné hrozby v ICT, opatření nejen typu instalace patche, ale i úprava konfigurace či designu systému anebo celé sítě.*
- *Proto tuto službu nazýváme také "VIRTUÁLNÍ BEZPEČNOSTNÍ ANALYTIK".*

Otázka: Mám pocit, že vy pod linkem hrozby popisujete zranitelnosti, které odhalím Skenerem zranitelností, nebo se mýlím?

Odpověď: Souhlasíme s Vámi, že některé zranitelnosti lze síťovým skenerem odhalit, je jich však zlomek ve srovnání se všemi hrozbami. Pro Vaši představu o informacích zveřejněných na ThreatGuard, připojujeme několik vybraných hrozeb

(včetně souvisejících opatření, tyto detaily uvidíte v EVAL verzi ZDARMA na 14 dní), na <u>které síťový skener zranitelností</u> ***<u>nedokáže reagovat</u>****:*

- *Nová Zero-Day zranitelnost v Adobe Flash Player*
  - *Objevila se nová chyba zabezpečení v aplikaci Flash Player, známá jako CVE-2018-15982, v případě úspěšného zneužití umožňuje útočníkovi spustit libovolný kód v zasaženém počítači a nakonec získat plnou kontrolu nad systémem..*
  - *Více zde https://portal.threatguard.cz/cs/app/threats/503*



Zjištěna zero-day zranitelnost v Adobe Flash Player

Základní údaje

Úplnost reportu:	plný
Stav reportu:	zveřejněný
Typ:	Vulnerability
Závažnost:	vysoká
Geolokace:	Global
Přidáno	07. 12. 2018 10:54
Aktualizováno	13. 12. 2018 14:36
Vytvořil:	COMGUARD a.s.

Rozsah působnosti

Výrobci:	Adobe
Štítky:	Email
Zařízení:	Workstation

Obsah

Krátký popis:	Chyba zabezpečení v aplikaci Flash Player, známá jako CVE-2018-15982, v případě úspěšného zneužití umožňuje útočníkovi spustit libovolný kód v zasaženém počítači a nakonec získat plnou kontrolu nad systémem.
CVSS závažnost:	8.8
CVSS link:	https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C
CVE link:	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-15982
Zdroje:	https://thehackernews.com/2018/12/flash-player-vulnerability.html

Náprava

Adobe vydal softwarové aktualizace na následujícím odkazu:
https://helpx.adobe.com/security/products/flash-player/apsb18-42.html

Uživatelé by měli být poučeni o opatrnosti při otevírání emailů (zejména z neznámých zdrojů), které obsahují připojené soubory. Pokud uživatel není schopen s jistotou identifikovat odesílatele zprávy, doporučujeme, aby přiložené soubory nestahoval, neoteviral.

Detailní popis

Nově objevený zero-day exploit Flash Player Player byl zaznamenán jako součást dokumentů Microsoft Office v on-line skenovací anti-malware službě VirusTotal. Zdá se, že hackeři zřejmě aktivně využívají dokumenty pro exploit, jako součást cílené kampaně zaměřené proti ruské státní zdravotní instituci.

Dokumenty Microsoft Office obsahují prvek Flash Active X, využívající výše zmíněnou zranitelnost Flash Player, který po otevření dokumentu spustí k dokumentům přiložený payloud, který následně může vytvořit komunikační kanál pro:

- monitorování aktivit uživatele (klávesnice - keylogger, pohyby myši)
- shromažďování informací o systému a jejich odesílánín na vzdálený command-and-control (C&C) server
- stahování souborů
- spouštění kódu

Zranitelné produkty:

- Adobe Flash Player Desktop Runtime 31.0.0.153 a dřívější
- Flash Player pro Google Chrome
- Microsoft Edge a Internet Explorer 11; Adobe Flash Player Installer ve verzi 31.0.0.108 a dřívější

Opatření

Politika pro emailovou bránu a antispam
IPS UDS for HTTP: Adobe Flash Player Use-After-Free Vulnerability (CVE-2018-15982)

- *Go crypto/x509 Package Denial of Service Vulnerability*
  - *Zranitelnost balíčku crypto/x509 Go by mohla umožnit neověřenému vzdálenému útočníkovi způsobit útok Denial of Service na cíleném systému.*
  - *Více zde https://portal.threatguard.cz/cs/app/threats/534*

- *QEMU File Renaming Race Condition Denial of Service Vulnerability*
  - *Zranitelnost v nástroji QEMU by mohla umožnit místnímu útočníkovi, aby způsobil útok Denial of Service na cíleném systému.*
  - *Více zde https://portal.threatguard.cz/cs/app/threats/528*
- *PostgreSQL zranitelnost v pg_user_mappings*
  - *PostgreSQL má zranitelnost v pg_user_mappings, díky které může vzdálený útočník se základními právy získat hesla z user mappingu bez příslušných oprávnění.*
  - *Více zde https://portal.threatguard.cz/cs/app/threats/251*

Otázka: Lze službu ThreatGuard PORTAL používat i v ANGLICKÉM jazyce?

Odpověď: ANO, portál je dostupný, jak v českém, tak i v anglickém jazyce.

Otázka: Je možné službu ThreatGuard provázat na řešení SIEM nebo McAfee ePO?

Odpověď: Služba ThreatGuard PORTAL nabízí opatření proti vybraným hrozbám formou exportu politik pro ePO v ceně služby. Forma předpřipravených konfiguračních exportů pro nastavení doporučených úprav v ePO je velmi efektivní způsob, jak aplikovat doporučení a zkušenosti analytiků ThreatGuard ve vlastní síti.
Napojení do SIEM řešení ThreatGuard aktuálně nenabízí. Kontaktujte obchodního zástupce s popisem vašich požadavků na integraci, služba je stále vyvíjena a zlepšována.

Otázka: Jaká jsou kritéria pro výběr sledovaných hrozeb?

Odpověď: Kritéria jsou interně v týmu analytiků stanovena následovně:

- *Musí se jednat o hrozbu, která je v danou chvíli reálná a ne pouze teoretická*
  - *Existence zranitelnosti, **pro kterou není známá forma aplikovatelného zneužití**, nepovažujeme za podstatnou a zranitelnost do ThreatGuard **nezařadíme**. Šetříme tak Váš čas pouze na podstatné a relevantní hrozby.*
  - *Zveřejnění exploitu nebo zdokumentované pokusy o zneužití určité zranitelnosti je pro nás signál, že je nutné hrozbu do TG zařadit.*
- *Hrozba se musí týkat našeho regionu*
  - *Jakákoliv globální hrozba nebo lokální malwarová/phishingová kampaň je relevantní.*
  - *Phishingová/malwarová kampaň mířící velmi specificky na region mimo CZ/SK je pro ThreatGuard irelevantní*
- *Hrozba se musí týkat aktiv, která jsou relevantní pro firemní použití*
  - *Nezabýváme se např. zranitelnostmi domácích routerů, soukromých blogovacích platforem, herních systémů, apod.*
  - *Velmi vážně bereme hrozby týkající se aplikačních serverů, Active Directory, Linuxových serverů, aktivních prvků apod.*

Ze všech zpracovávaných zdrojů projde našimi filtry cca 10% všech možných zpráv, upozornění, novinek, apod., takže odfiltrujeme zbytečný šum irelevantní pro ochranu infrastruktury.

Otázka: Proč např. zranitelnost NetBackup CVE-2017-885[6-9] není v ThreatGuard uvedena?

Odpověď: Důvodem je, že pro zmíněné zranitelnosti neexistuje zatím (v čase psaní odpovědi) veřejně dostupný exploit ani zmínka o tom, že by zranitelnost byla zneužívána některými útočníky nebo malwarem.

Otázka: S jakým zpožděním se objeví nová hrozba ve službě ThreatGuard?

Odpověď: Jedná se o best-effort aktivitu. Vyhodnocování probíhá v pracovní dny 8:00-17:00 a proces je nastaven tak, aby informace o existenci hrozby byly zveřejněny co nejrychleji po ověření podmínek uvedených výše. Analytik hrozbu zveřejňuje samostatně, abychom eliminovali zpoždění způsobené zavedením schvalovacího procesu. Hrozby jsou kontrolovány zpětně dalším členem týmu, který případně může navrhnout jejich stažení nebo přepracování.

Otázka: Lze službu ThreatGuard přizpůsobit konkrétním požadavkům, tedy budu sledovat pouze technologie, které mám v infrastruktuře nasazeny?

Odpověď: Filtrace je možná již dnes na základě dostupných aktiv.

Otázka: Co přináší ThreatGuard 2.0?

Odpověď: Díky ThreatGuard 2.0 naši zákazníci a partneři budou moct využívat níže uvedené funkcionality:

- *Webová aplikace postavená přímo na míru požadavkům našich zákazníků*
  - *Jednoduchý a přehledný systém (USER friendly)*
  - *Možnost filtrování podle Vámi vybraných aktiv (lze nastavit i více filtrů v rámci jednoho účtu)*
  - *Responzivní design (zobrazení i pro mobilní zařízení)*
- *Obchodní model na míru našim partnerům*
  - *Multitenantnost - Aplikace podporuje členění a oddělení na jednotlivé oblasti podle partnerů či klientů anebo skupin klientů, které mohou sdílet globální informace a nastavení, především pak dokáží obsahovat jen specifické informace a nastavení pro konkrétního klienta či skupinu klientů.*
  - *Rebranding – v rámci Vašeho administrátorského rozhraní budete schopni upravit GUI (změna barev, písma a uvedení Vašeho firemního loga v rámci GUI) dle Vašich představ, tzn. Vaši zákazníci budou vnímat službu ThreatGuard, jako Vaši vlastní.*
  - *News – budete schopni posílat novinky pouze na Vaše zákazníky, díky čemuž budou informováni o aktualitách ve Vaší společnosti, portfoliu a akcích, které připravujete pro Vaše zákazníky.*
  - *Support Vašeho expertního týmu – konkrétní problémy Vašich zákazníků budete schopni řešit skrze Live chat v ThreatGuard 2.0, takže k citlivým informacím a problémům Vašich zákazníků budete mít přístup pouze Vy.*
- *Služba dostupná v ČJ a EN*
- *Support expertního týmu – tým analytiků bude k dispozici pro Vaše požadavky a bude je primárně řešit*
  - *Vaše konkrétní problémy a požadavky bude tým expertů primárně řešit*
  - *Live chat = okamžitá odezva*
  - *Individuální přístup k řešení Vašich požadavků včetně doporučení*
- *Emailová notifikace na aktuální hrozby – na nově evidované hrozby v našem systému budete vždy včas upozorněni prostřednictvím emailu*

Otázka: Jaké funkcionality získá partner v rámci rebrandingu portálu ThreatGuard 2.0?

Odpověď: Partner má díky tomuto možnosti upravit vzhled portálu ThreatGuard 2.0, tzv do „vlastní košilky". Díky rebrandingu je schopný dát na portál ThreatGuard 2.0 vlastní logo, barevně modifikovat vzhled GUI, změnit font písma, a tak prodávat službu, jako vlastní produkt.

Otázka: Co získá partner díky funkcionalitě Editování hrozeb v ThreatGuard 2.0?

Odpověď: Partner je schopný aktivně vytvářet obsah ThreatGuardu 2.0, jako jsou hrozby, opatření a novinky. Společnost má možnost vytvářet vlastní opatření, které vidí pouze zákazníci dané společnosti.

Otázka: Jak funguje Real-time chat/support a co zákazníkovi přinese v rámci licence ThreatGuard HelpDesk?

Odpověď: V případě zakoupení licence ThreatGuard HelpDesk bude mít zákazník k dispozici realtime chat, kdy bude moct v reálném čase řešit své specifické požadavky, dotazy na hrozby s týmem odborníků, kteří za celou službou stojí.

Otázka: Testujete nápravy a opatření k jednotlivým hrozbám uvedeným v ThreatGuard 2.0 před jejich zveřejněním na portálu?

Odpověď: ANO, všechny nápravy a opatření k jednotlivým hrozbám jsou napřed otestovány v rámci našeho labu a až poté, co 100% ověříme jejich funkčnost, tyto ochranné prvky zveřejníme na portále ThreatGuard 2.0.

Otázka: Zabýváte se pouze technologiemi z Vašeho portfolia nebo máte širší záběr, tzn. uvádíte do ThreatGuard 2.0 i hrozby týkající se technologií jiných výrobců?

Odpověď: Chápeme, že abychom byli s touto službou úspěšní, musíme se zajímat i o technologie výrobců, které v ČR a SR nezastupujeme. Proto v ThreatGuard 2.0 naleznete i technologie jiných výrobců (Fortinet, Cisco, Symantec apod.), jen takto jsme schopni efektivně účinně pokrýt různorodé IT infrastruktur našich zákazníků informacemi o aktuálních hrozbách.

