



Co je ThreatGuard?

- **Webový portál** s databází seříděných reálných hrozeb
- Obsahuje **aktivní filtry** a **notifikuje hrozby** emailem
- **Tým IT expertů**, který analyzuje kybernetické hrozby
- **Navrhuje konkrétní a účinná nápravná opatření**



RADAR IT HROZEB



Tým expertů s více jak 10 letou praxí denně vyhledává reálné IT hrozby a zranitelnosti z ověřených zdrojů a sbírá informace od světových bezpečnostních výrobců a vydává **návrhy nápravných opatření** pro každou hrozbu. **Analyzuje a klasifikuje hrozby podle stupně závažnosti.**

ThreatGuard obsahuje **ucelené reporty** a je připravován tak, aby byl srozumitelný nejen IT odborníkům a bezpečnostním manažerům. Slouží také jako **podklad pro rychlá a kvalifikovaná rozhodnutí.**

Uživatel má v reportu k dispozici také návrhy **nápravných opatření**, které může rovnou přeposlat kompetentním osobám jako **přímočarý návod** za účelem eliminace hrozby.

Hrozba vyzrazení citlivých informací v VMware vCenter

Vendoři: VMware
Štítky:
Závažnost: vysoká
Typy: Vulnerability

Aktualizováno 14.4.2020

Základní údaje

ID	1059	Přidáno	14.4.2020 11:57
Úplnost reportu	plný	Aktualizováno	14.4.2020 11:57
Typy	Malware	Geolokace	Global
Závažnost	vysoká		

CVSS závažnost	0.00
CVSS link	
CVE link	
Zdroje	https://blog.malwarebytes.com/android/2020/02/new-variant-of-android-trojan-xhelper-reinfects-with-help-from-google-play/ https://thehackernews.com/2020/04/how-to-remove-xhelper-malware.html

Vendoři	Google
Štítky	Android
Zařízení	Mobile

Náprava

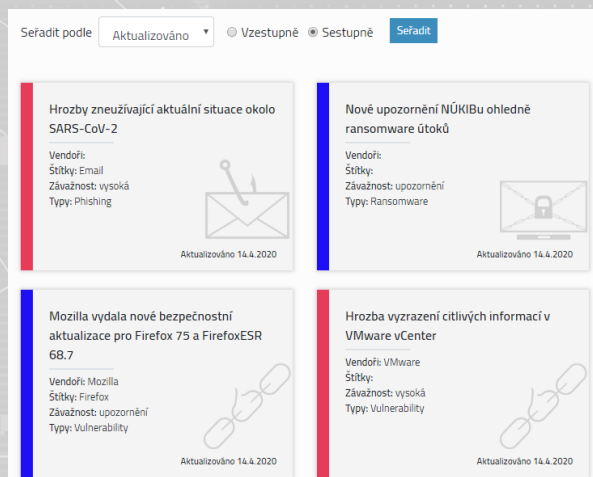
Uživatelům zmíněných mobilních zařízení, zvláště těch, co již výše popsanou situaci zažili, doporučujeme postupovat následovně:

- Nainstalovat antimalwarovou aplikaci (např. aplikaci **Malwarebytes for Android**, která je k dispozici zdarma)
- Nainstalovat Správce souborů z GooglePLAY, který má schopnost vyhledávat soubory a adresáře (např.: správce souborů **ASTRO**)
- Dočasně zakázat GooglePLAY pro zabránění neustálé a opětovné infekce zařízení malwarem (cesta **Settings > Apps > Google Play Store** a následně stisknout tlačítko **Disable**)
- Spustit scan antimalwaru k odstranění **xHelperu** a ostatního malware (manuálně)



ThreatGuard vám šetří čas, peníze a personální zatížení

ThreatGuard analyzuje hrozby za vás a vy tak můžete věnovat čas jiným úkolům. IT hrozby již nechte na nás.



Reference

AirBank: „Díky ThreatGuard má náš bezpečnostní tým přesnější informace o relevantních hrozbách a je na ně schopnější efektivněji reagovat. V důsledku se nám také uvolnily kapacity pro další aktivity v oblasti IT bezpečnosti.“

Meopta: „Osobně jsem neměl moc velké očekávání, nicméně mě služba příjemně překvapila. Hlavně, když jsem přišel na to, jak fungují filtry. Po jejich nastavení se přidaná hodnota služby posunula ještě dál.“



Co získáte díky ThreatGuard?

- Přehled kritických zranitelností a hrozeb pro vaše technologie
- Obdržíte **setříděné informace** z ověřených informačních zdrojů
- **Kvalifikovaná doporučení** o účinných bezpečnostních opatřeních
- **Návody na ověřenou a vyzkoušenou obranu** při napadení
- **Stanovení míry rizika hrozby pro** vaše konkrétní IT prostředí
- Přístup k **návodům pro nápravná a preventivní opatření**

Co přináší ThreatGuard 3.0?

- **Rozhraní pro integraci do dalších systémů** (SIEM, SOC, SOAR, apod.)
- **Rozšířené možnosti filtrování** – fulltextové vyhledávání nad celou databází hrozeb
- Rozšíření datových zdrojů hrozeb
- **HTML5 notifikace** – jednoduché upozornění na vašem mobilním telefonu, tabletu, notebooku apod.
- Komplettní úprava GUI, zobrazování hrozeb a filtrování
- Verzování hrozeb a opatření