Průvodce aplikací

Vodafone Business CyberWall pro Android a iOS

CyberWall



Průvodce aplikací Vodafone Business CyberWall pro Android a iOS



Obsah

And	Iroid
1.	Instalace a aktivace
2.	Princip ochrany – sledování 3 vektorů
3.	Hlavní stránka aplikace – status hrozeb dle barev4
4.	Hlavní stránka
5.	Správa hrozeb4
6.	Nastavení aplikace CyberWall
7.	Historie
iOS	
8.	Instalace a aktivace
9.	SMS phishing – nastavení
10.	Hlavní stránka aplikace – status hrozeb dle barev
11.	Nastavení7

12	istorie	7
12.		'

Android

Instalace a aktivace

- » V zařízení s **OS Android** klikněte na odkaz s licenčním klíčem, který jste obdrželi v SMS hned po aktivaci služby u Vodafonu
- » Budete přesměrováni na Google Play store a vyzváni ke stažení aplikace CyberWall
- » Po stažení se aplikace automaticky aktivuje, pokud byly splněny předchozí 2 body
- » Pokud byla zakoupena licence typu MULTI, tento postup lze opakovat ještě 4× (licence je platná pro 5 zařízení)



Princip ochrany – sledování 3 vektorů

- » Bezpečnost zařízení
 - USB debug
 - > Neznámé zdroje
 - Zranitelnosti
 - > SMS phishing
- » Nebezpečné aplikace
 - > Instalované aplikace
 - > Aplikační soubory uložené v zařízení
- » Útoky z internetové sítě
 - Reputace sítě
 - MITM útoky
 - > Nešifrované (veřejné) Wi-Fi



Hlavní stránka aplikace – status hrozeb dle barev

	ČERVENÁ	ŽLUTÁ
Aplikace	Škodlivá nainstalovaná aplikace	Škodlivý APK soubor v zařízení
Síť	MITM* útok, nebezpečná síť	Veřejná Wi-Fi
Zařízení	Aktualizace OS	Zranitelnost OS
	Rootovaný device	Nebezpečné nastavení OS

*MITM – Man In The Middle – podstatou tohoto útoku je snaha útočníka odposlouchávat komunikaci mezi účastníky tak, že se stane aktivním prostředníkem

Hlavní stránka

- » Celkový status
 - > Zobrazuje barvu kruhu podle důležitosti nalezených zranitelností
- » Dílčí status pro jednotlivé vektory
 - Zařízení
 - > Aplikace
 - > Síť



Správa hrozeb



- › Název
- > Důležitost
- > Popis

> Doporučení

- > Akce
- > Ignorování

	9% 📃 16:56
CyberWall	:
ZJIŠTĚNÁ RIZIKA!	
MOJE ZAŘÍZENÍ	×
Samsung SM-A500FL	J
CyberWali je aktuální	~
Aplikace z neznámých zdrojů jsou povoleny	^
BEZPEČNOSTNÍ ANALÝZA	
Instalování aplikací z neznámých zdrojů mí ohrozit bezpečnost a soukromí vašeho zaří Doporučujeme instalovat aplikace pouze z důvěryhodných zdrojů.	ùže izeni.
DOPORUČENÉ KROKY	
Zakázat aplikace z neznámých zdrojů. Vypnout × Ztišit	

- » Prohlížení webu detekce nebezpečné stránky
 - > Blokovaná stránka
 - Adresa stránky (webu)
 - > Zablokovaná kategorie



Nastavení aplikace CyberWall

- » Bezpečnostní nastavení
 - Notifikace
 - > Kontroly na pozadí
 - > Přístup k polohovým službám
 - Přístup k úložišti
- » Podpora
- » Návod

\leftarrow Nastavení Bezpečnostní nastavení Upozornění Zapnout doručování bezpečnostních upozornění Kontroly na pozadí Zapnout provádění kontrol bezpečnosti vašeho zařízení na pozadí Přístup k polohovým službám Získejte bezpečnostní analýzu podle své současné pozice. Přístup k úložišti Umožněte přístup k úložišti, aby bylo možné kontrolovat lokální soubory PODPORA Your device name: Samsung SM-A500FU (f102) Odeslat hlášení problému emailem Návod

Historie

- » Posledních 30 dní
- » Kontrola sítí
- » Skeny zařízení
- » Nové aplikace



Instalace a aktivace

- » V zařízení s **iOS** klikněte na odkaz s licenčním klíčem, který jste obdrželi v SMS hned po aktivaci služby u Vodafonu
- » Po stažení klikněte znovu na odkaz v SMS anebo zadejte licenční klíč z SMS do pole Aktivovat na úvodní stránce aplikace CyberWall
- » Pokud byla zakoupena licence typu MULTI, tento postup lze opakovat ještě 4× (licence je platná pro 5 zařízení)



SMS phishing – nastavení

11:38 7	, all LTE 🗨	 ◄ CyberWallII Zprávy 	LTE 15:58 Neznámé a spam	0 95 % 🛤
	N	FILTROVÁNÍ IM	IESSAGE	
DETEROVANO MOZNE RIZIRO		Filtrovat nez	známé odesilatele	
	×	Bude vypnuto nejsou ve vašić uloženy do san FILTROVÁNÍ SP	oznamování zpráv iMessage ch kontaktech. Jejich zprávy nostatného seznamu. MS	od lidí, kteří budou
		CyberWall		
CyberWall je aktuální	~	Vyberte filtr pr a jejich řazení (O Eiltrování SM	o vypnutí oznamování nevyž do samostatném seznamu. AS a soukromí	ádaných SMS
K dispozici je nová verze iOS	\sim	o rinto din on		
SMS Phishing	~			

Hlavní stránka aplikace – status hrozeb dle barev

	ČERVENÁ	ŽLUTÁ
Síť	MITM* útok, nebezpečná síť	Veřejná Wi-Fi
Zařízení	Aktualizace OS	Zranitelnost OS

*MITM – Man In The Middle – podstatou tohoto útoku je snaha útočníka odposlouchávat komunikaci mezi účastníky tak, že se stane aktivním prostředníkem

Nastavení

- » Monitorovat na pozadí kontroluje veškeré podezřelé aktivity, nepřetržitě
- » Wi-Fi poradce v případě podezřelé sítě doporučí se k ní nepřipojovat
- » Podpora
- » Historie



Historie

- » Nachází se na hlavní stránce
- » Posledních 30 dní
- » Kontrola sítí
- » Skeny zařízení
- » Ověření CyberWall verze



PK8120