#DontNeedtoCry - Dne 12. května WannaCryptor (WannaCry) ransomware napadltisíce počítačů po celém světě. Za pouhých 24 hodin se počet infekcí zvýšil na 185 000 strojů ve více než 100 zemích.

Útok je obzvláště nebezpečný pro firmy. Stačí, aby bylo napadeno jedno zařízení ve firemní síti a virus se šíří dál bez jakékoliv interakce.

Proč k tomu dochází? Ransomware obsahuje červa (worm), který využívá a útočí na operační systémy Windows 7, 7 SP1, Win Server 2008, 2008R2.

WannaCry se automatizoval a využívá zranitelnosti, která se vyskytuje ve většině verzí systému Windows a dovoluje vzdálenému útočníkovi spustit kód na napadeném počítači. Tento kód dokáže spustit ransomware bez jakékoliv lidské asistence nebo zásahu v místní síti.

Nikdy předtím nebyl použit speciální „tool“ k napadení specifických prostředí a infrastruktur se servery se zranitelnou verzí protokolu Server Message Block (protokol SMB).

Zákazníci Bitdefenderu NEJSOU touto útokovou vlnou zasaženi.

Bitdefender GravityZone chrání proti vlnám útoků nultého dne i jejich novým mutacím ransomwaru WannaCry. Detekuje, zachytí a zablokuje pokusy o průnik škodlivého kódu do koncového bodu.
Nejnovější technologie strojového učení využívá samoučící algoritmy, které odhalují nové a neznámé hrozby s dokonalou přesností v reálném čase.

Modely Bitdefender Machine Learning jsou součástí všech edicí platformy Bitdefender GravityZone.

Dokonce nově zavedené řešení Hypervisor Introspection společnosti Bitdefender dokázalo zabránit zneužití chyby EternalBlue nultého bodu dřív než chybu opravila společnost Microsoft.

Bitdefender neustále inovuje své technologie a poskytuje tu nejmodernější ochranu svým zákazníkům. Děkujeme, že nám věříte a propagujete Bitdefender .

Bitdefender Tým