STRUČNÝ POPIS TECHNICKÉHO ŘEŠENÍ

Bitdefender

Security

Ransomware

Prevence a zmírnění škod pomocí Bitdefender GravityZone

Obsah

Přehled Ransomware

Co je to Ransomware?

Ransomware je škodlivý software, který se snaží zašifrovat soubory a požadovat za ně výkupné. Oběti ransomwaru musí útočníkům zaplatit, aby znovu získaly přístup ke zdrojům, obvykle v nedohledatelné kryptoměně, výměnou za dešifrovací klíč, který může, ale nemusí přijít po provedení platby. Jednotlivcům mohou v případě ohrožení způsobit starosti soubory, jako jsou obrázky, videa nebo důležité dokumenty, ale u podnikatelských subjektů může vykoupený obsah snadno zahrnovat informace o vlastnictví, osobní údaje zákazníků, údaje o účtech a platebních kartách nebo jiná cenná data.

Ransomware je téměř vždy motivován ziskem, nicméně pokročilé útoky ransomwaru mohou mít širší cíle a způsobit organizacím obrovské škody, včetně existenčních obav, pokud by útok ransomwaru způsobil, že subjekt nebude moci pokračovat v běžném podnikání. V extrémních případech mohou být ohroženy i lidské životy.

Příklady nedávných známých ransomwarových útoků s nadměrnými finančními ztrátami a negativním společenským dopadem:

- Nemocnice British National Health Service (odhadované náklady 92 milionů liber na přímé náklady a ztrátu produktivity)
- Státní správa/místní samospráva:: State of Louisiana (vyhlášení výjimečného stavu), 2 Florida cities ($1.1 million zaplaceno)
- Vzdělávání: University of Utah ($457,000 zaplaceno), University of California San Francisco ($1.14 million zaplaceno)

Ransomware se může na infikovaném notebooku, stolním počítači nebo serveru projevit různými způsoby a obvykle znemožní uživateli přístup k systému, dokud nezaplatí výkupné:

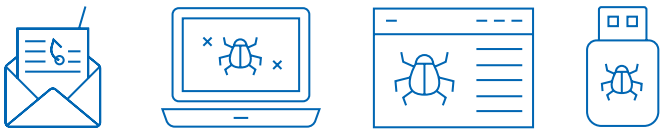
- Šifruje citlivé a osobní soubory bez možnosti dešifrování
- Vyhrožuje zveřejněním citlivých a osobních souborů
- Uzamkne obrazovku počítače a znemožní úplný přístup do systému
- Blokuje spouštění některých aplikací, což snižuje produktivitu uživatele.

Ransomware je velmi přizpůsobivý a pečlivě navržený tak, aby se vyhnul detekci bezpečnostním softwarem. I malé zpoždění při detekci může poskytnout dostatek času k potenciálně nevratnému zašifrování souborů.

Jak Ransomware proniká do organizace?

Ransomware má spoustu možností, jak se dostat do organizace, a kyberzločinci jsou velmi kreativní ve využívání technologických i lidských zranitelností. Navzdory mnohaletým školením o bezpečnostním povědomí, přetrvává riskantní chování uživatelů, které je vytrvale vysoké a vede k riskantnímu klikání na pochybné odkazy a neuváženému stahování aplikací/souborů.

- Cílený phishingový e-mail se škodlivými odkazy a soubory v příloze
- Škodlivé stahování dokumentů, ať už z podnětu uživatele, nebo prostřednictvím stahování z disků
- Stahování škodlivých aplikací/spustitelných souborů, včetně falešného softwaru, a falešných aktualizací produktů.
- Útoky bez souborů v paměťovém prostoru iniciované z prohlížeče, aniž by se dotkly diskové jednotky
- Infikované dokumenty a soubory médií ze sdílených síťových souborů a přenosných médií



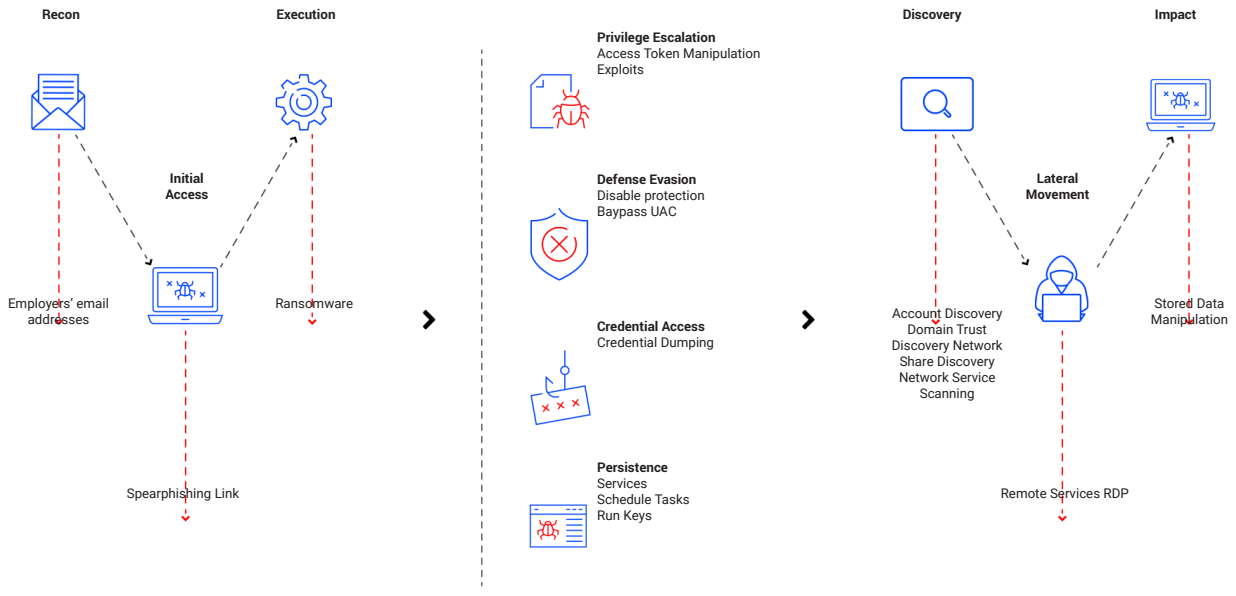
Obrázek 1: Běžné vektory útoku ransomwaru

Co zahrnuje ochrana proti ransomwaru?

Komplexní zmírnění ransomwaru vyžaduje proaktivní ostražitost na několika frontách současně, z nichž každá musí být pokryta bezpečnostním řešením.

- **Preventivní ochrana** - vytváření záložních kopií uživatelských souborů, které jsou pro ransomware nedostupné.
- **Blokování a prevence** - nasazení adaptivní obrany, která není závislá na detekčních technikách založených na signaturách
- **Monitorování a včasná detekce** - sledování podezřelých procesů a síťové aktivity, korelace indikátorů útoků.
- **EDR a reakce na incidenty** - žádná prevence není vždy stoprocentně účinná, proto EDR hledá podezřelé indikátory na koncovém zařízení a v síťovém provozu, aby je mohl přiřadit ke konkrétním incidentům a reagovat na ně
- **Záplatování zranitelností** - aktualizace zranitelných aplikací a operačních systémů pomocí nejnovějších záplat dodaných výrobcem, které se aplikují automaticky
- **Správa rizikové konfigurace** - Identifikace a uzavření všech snadno dostupných zdrojů vstupu ransomwaru pomocí identifikace a opravy chybných konfigurací systému, z nichž mnohé lze opravit automaticky
- **Monitorování rizik chování uživatelů** - identifikace a náprava chování uživatelů, které zvyšuje riziko pro organizaci, jako je opakované používání hesel, klikání na phishingové nástrahy, riskantní klikání, stahování a přihlašování na nešifrované webové stránky
- **Kontrola aplikací a zařízení** - sledujte využívání a povolte spouštění pouze potřebných aplikací, a přístup k systému pouze nezbytným externím zařízením

Aby bylo možné ransomware porazit, je třeba pochopit celý řetězec kybernetického útoku a zmapovat obranu pro každou fázi útoku.



Obrázek 2: Taktika útoku ransomwaru a typický řetězec kybernetického útoku

Zabezpečení vektorů útoku ransomwaru

Ochrana před ransomwarem se všemi jeho ničivými účinky, vyžaduje také pokrytí všech běžných vektorů útoku:

- Phishingové nebo nevyžádané e-mailové odkazy a škodlivé přílohy souborů
- Stahování škodlivých souborů, a to jak z podnětu uživatele, tak i z důvodu stahování prostřednictvím jednotek drive-by
- Stažení škodlivé aplikace nebo spustitelného souboru
- Útoky bez souborů v paměťovém prostoru iniciované z prohlížeče, aniž by se dotkly pevného disku.
- Přenosné jednotky médií a síťové nebo sdílené vzdálené soubory

Jak funguje Bitdefender Ransomware Mitigation

Zálohy odolné proti neoprávněné manipulaci

Bitdefender vytváří automatické, aktuální záložní kopie uživatelských souborů odolné proti neoprávněné manipulaci bez použití stínových kopií, které jak bylo opakovaně prokázáno, lze snadno odstranit ransomwarem. Jedná se o ochranu "bez nutnosti použití rukou", protože uživatel nemusí nic dělat. Ransomware nemá k chráněným záložním souborům přístup a uživatel o jejich přítomnosti neví. Ransomware Mitigation identifikuje, kdykoli se případný nový ransomware pokusí zašifrovat soubory, a automaticky vytvoří zálohu cílových souborů, které budou po zablokování malwaru obnoveny. Bitdefender zablokuje všechny procesy zapojené do útoku a zahájí nápravu, přičemž zároveň informuje uživatele.

Blokování a prevence

Obrana před útoky bez souborů (fileless attack) a funkce Hyper Detect

Po aktivaci aplikace Bitdefender automaticky odhalí a zablokuje útoky bez souborů ve fázi před spuštěním, čímž zabrání šifrování souborů a zachová plný přístup k systému. HyperDetect dokáže odhalit a zablokovat bezsouborové útoky v fázi před spuštěním pomocí vysoce vyladěných modelů strojového učení, které s vysokou přesností odhalují nový a neznámý malware, aby bylo možné úspěšně porazit bezsouborový ransomware během několika fází řetězce zničení útoku analýzou chování na úrovni kódu.

Strojové učení proti malwaru

Bezpečnostní řešení Bitdefender automaticky a nepřetržitě trénuje a zlepšuje své schopnosti rozpoznávání škodlivého softwaru pomocí jednoho z největších skladů vzorků v oboru, shromážděných v reálném prostředí z rozsáhlé sítě globálních senzorů. Vzhledem k tomu, že se ransomware neustále vyvíjí, Bitdefender přesně detekuje nové vzory před spuštěním a za běhu.

Pokročilý nástroj Anti-Exploit

Autoři ransomwaru používají k získání přístupu k systému sady využívající zranitelnosti zero-day nebo neopravené bezpečnostní chyby. Bitdefender se zaměřuje na techniky útoků, které chrání systémy a zabraňují šíření ransomwaru. Pokročilé technologie proti zneužití dokáží rychle identifikovat a automaticky ukončit škodlivé procesy.

Ochrana sítě

Služba Network Attack Defense využívá behaviorální heuristiku k analýze síťové aktivity hostitele v reálném čase, a k posílení kontroly proti technikám zneužití, které mohou exfiltrovat osobní informace ze sítě. Využívá strojové učení k blokování exploitů ransomwaru, které přicházejí přes vstupní body sítě, jako je například BlueKeep. Ochrana sítě slouží také k zastavení škodlivé aktivity ve fázích počátečního přístupu, přístupu k pověření, objevení a útoku pomocí laterálního pohybu.

Monitorování a včasná detekce (Pokročilá kontrola hrozeb)

GravityZone monitoruje spuštěné procesy v reálném čase - modifikace klíčů registru, čtení/zápisy souborů, šifrovací akce - a identifikuje podezřelé nebo škodlivé procesy, které mohou bezpečnostní týmy automaticky nebo ručně ukončit.

EDR a řešení incidentů

Ne všechny útoky lze zablokovat nebo jim zabránit, a některé fáze útoku se projevují pomalu v průběhu času. EDR bude vždy hrát roli při zmírňování ransomwaru. GravityZone EDR automaticky koreluje několik indikátorů útoku a kompromitace (IOA/IOC) se škodlivou aktivitou pozorovanou v systému a v síti, což usnadňuje rychlou a přesnou reakci na incident, která zkracuje dobu přítomnosti útočníka, a usnadňuje rychlé obnovení souborů po útoku ransomwaru.

Omezování uživatelských a systémových rizik

Záplatování zranitelností

Nezáplatované systémy činí organizace náchylnými k útokům ransomwaru. Modul GravityZone Patch Management pomáhá organizacím udržovat operační systémy a aplikace aktuální v celé instalační základně systému Windows, včetně stolních a přenosných pracovních stanic, fyzických serverů a virtuálních serverů.

Chybná konfigurace systému

Nesprávně nakonfigurované systémy ponechávají dveře otevřené útokům ransomwaru, včetně nastavení zabezpečení prohlížeče, nastavení sítě a pověření, nastavení zabezpečení operačního systému, jako jsou otevřené porty, nedůležité služby a povolené nástroje pro správu skriptů (např. PowerShell). GravityZone vyhledává chybné konfigurace systému a dokáže automaticky vzdáleně aktualizovat mnoho nastavení chybně nakonfigurovaných počítačů, a zároveň upozornit správce, aby obnovil ostatní nastavení.

Zranitelnosti aplikací

Zastaralé aplikace se známými zranitelnostmi (CVE) mohou autoři ransomwaru využít ke zneužití funkcí programu nebo ke stažení škodlivého obsahu z internetu. Rizikové aplikace lze buď aktualizovat na novější, bezpečnější verzi, nebo je lze ze systému odstranit, pokud je uživatel nepotřebuje. GravityZone skenuje zranitelnosti CVE a řadí zranitelnosti aplikací podle závažnosti, takže správci mohou okamžitě přijmout nápravná opatření.

Rizikové chování uživatelů

Uživatelé se vystavují riziku nákazy ransomwarem pokaždé, když otevřou e-mail, kliknou na odkaz nebo stáhnou soubor. Služba GravityZone Human Risk Analytics sleduje, kde uživatelé brouzdají, jaké soubory otevírají, k jakým umístěním souborů přistupují, jak a kde se přihlašují na rizikové webové stránky, a sleduje hygienu hesel a jejich opakované používání, aby bylo možné rizikové chování napravit.

Proč potřebujete Bitdefender Ransomware Mitigation

Komplexní ochrana koncových bodů proti ransomwaru je velmi důležitá, protože koncové body jsou branami k serverům a dalším cílům s vysokou hodnotou, na kterých jsou umístěny chráněné informace, údaje o zákaznících, platební údaje a další cenné duševní vlastnictví. Mezi výhody Bitdefender Ransomware Mitigation patří:

- Bezproblémové zajištění kontinuity provozu proti všem běžným vektorům útoku ransomwaru
- Jistota, že vaše bezpečnostní řešení je přizpůsobivé a dokáže čelit novým a objevujícím se technikám ransomwaru.
- Osvobození od výhradního spoléhání se na problematické zálohování na serverech nebo dlouhé doby obnovy z cloudových záloh.
- Místní, síťové a incidentové možnosti obnovy souborů a zmírnění narušení pro obnovu po útocích
- Chyby se stávají! Bitdefender posouvá vyvažování restriktivního poměru mezi bezpečností a produktivitou uživatele ve prospěch uživatele

Případy použití Bitdefender Ransomware Mitigation

Bitdefender pokrývá více případů použití pro zmírnění ransomwaru než konkurenční řešení, a nabízí uživatelům a správcům zabezpečení nástroje na různých úrovních, které ransomware udrží na uzdě. Důkladná prevence a náprava probíhá na úrovni koncového bodu, sítě a administrace konzole GravityZone, ať už byl původní útok úspěšný, nebo ne.

Místní potlačení ransomwaru

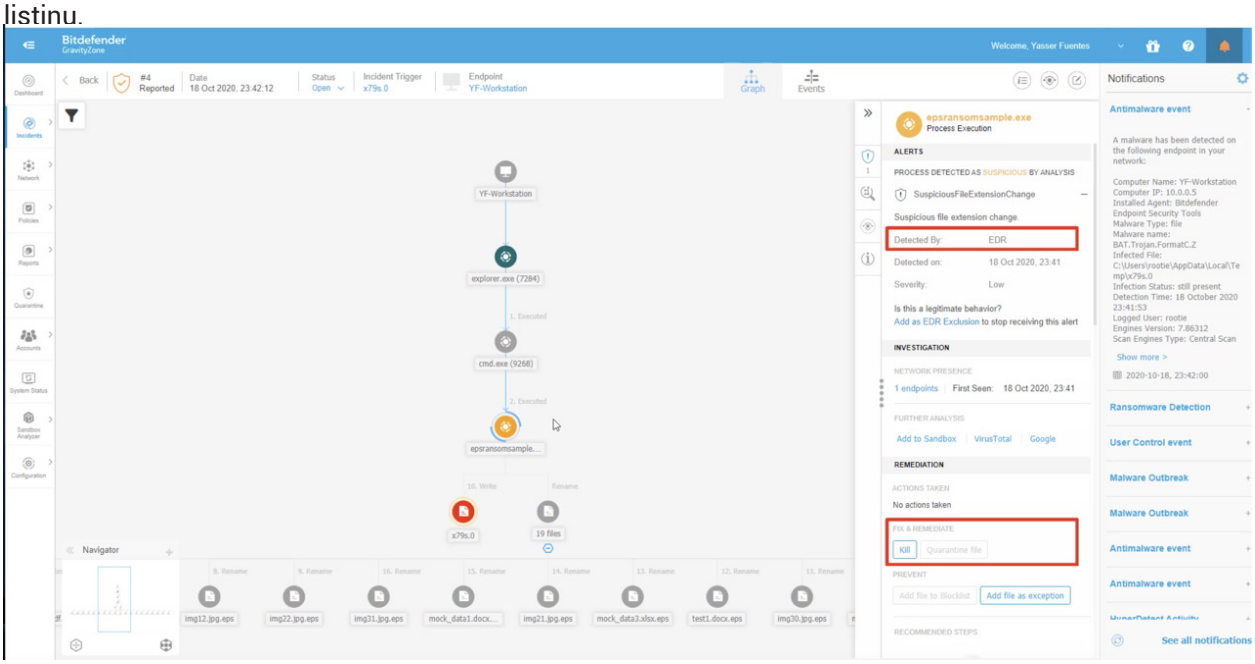
V případě lokálního potlačení ransomwaru mohou správci nakonfigurovat zásady zabezpečení Bitdefender tak, aby monitorovaly procesy koncového bodu a obnovily zašifrované soubory, jakmile adaptivní technologie útok zjistí a zablokuje. I na webové stránce se ransomwaru podaří zašifrovat místní soubory, technologie zmírnění okamžitě naskočí a tyto soubory obnoví, a to buď automaticky, nebo na vyžádání, kdy správce řídí harmonogram obnovy zašifrovaných souborů.

Vzdálené potlačení ransomwaru

V případě technologie Remote Ransomware Mitigation může správce zabezpečení povolit sledování cest ke sdílení v síti, ke kterým lze přistupovat vzdáleně, a zabránit zašifrování souborů. Na vzdáleném koncovém zařízení uživatelský agent potvrdí, že nástroj Ransomware Mitigation zachytil chování vzdáleného škodlivého procesu a ochránil soubory. Správci produktu Bitdefender mohou rychle spustit auditní zprávy a zjistit další informace o IP adrese, ze které byl vzdálený ransomwarový útok spuštěn, a o bezpečnostním modulu, který chránil koncový bod, a mohou také obdržet e-mailové oznámení, když je útok zablokován, obsahující informace o IP adrese útočníka.

Správa incidentů z GravityZone

V systému GravityZone mají bezpečnostní týmy úplný přehled o řetězci útoku a o souborech zasažených útokem ransomwaru. Bitdefender EDR detekuje aktivitu ransomwaru a správci zabezpečení mohou buď ukončit aktivní škodlivý proces, nebo dát infikované soubory do karantény. Mohou také trvale zařadit IP adresu útočníka na černou listinu.



Obrázek 3: Reakce GravityZone EDR na incident ukazuje celý řetězec útoku ransomwaru.

Odlišnosti GravityZone

Prevence a zmírňování ransomwaru jsou integrovány do konzoly GravityZone Management Console a klienta Bitdefender Endpoint Security Tools (BEST) na několika úrovních, což dalece převyšuje konkurenční bezpečnostní řešení.

Bezkonkurenční kombinace obrany proti ransomwaru od společnosti GravityZone	
Více vrstev blokování	Koncový bod a síť, před spuštěním a při přístupu, na bázi souborů a bez souborů
Více detekčních vrstev	Kontrola procesů, monitorování registrů, kontrola kódu, Hyper Detect
Více vrstev obnovy	Účinný rollback z lokálního počítače, vzdáleného systému nebo incidentu EDR
Adaptivní obrana	Pokročilá ochrana proti zneužití, adaptivní heuristika, laditelné strojové učení
Technologie pro zmírnění rizik	Automatické opravování zranitelností, chybná konfigurace systému, chování uživatelů
Zálohy odolné proti manipulaci	Žádné použití zranitelných stínových kopií, ransomware nemůže odstranit zálohy
Vzdálené blokování ransomwaru	Blokuje ransomwarové útoky na dálku a v síti, a zařazuje IP adresy útočníků na černou listinu.
Celopodnikové čištění	Vzdálené ukončování procesů, snadná globální karanténa a odstraňování souborů

Bezkonkurenční kombinace ochrany GravityZone proti ransomwaru

Nejvíce oceňovaný dodavatel zabezpečení koncových bodů

Bitdefender se v nezávislých testech a hodnoceních třetích stran trvale umisťuje na předních místech:

- Umístění na 1. místě a volba PC Editors' Choice pro "Best Hosted Endpoint Protection and Security Software for 2020"
- Umístění na 1. místě a volba PC Editors' Choice pro "Best Mac Antivirus Protection for 2020"
- "The biggest EDR vendor you haven't considered but should have" – Forrester Research
- 100% detection vs. real world threats, AV-Test (Jan-Aug 2020)

Podívejte se na Bitdefender GravityZone v akci

- Přesvědčte se sami: Podívejte se na ukázkové video, které ukazuje mnoho způsobů, jakými Bitdefender čelí ransomwaru.

Chraňte se před ransomwarem

Kontaktujte nás pro více informací a demo verzi

Chcete-li získat další informace, kontaktujte nás a domluvte si podrobnou ukázku produktu a podrobnou diskusi o produktu Bitdefender GravityZone a o tom, jak funguje při prevenci a zmírňování útoků ransomwaru.

Společnost Bitdefender je nejoblíbenějším dodavatelem technologií - 38 % dodavatelů kybernetické bezpečnosti na celém světě používá jednu nebo více technologií Bitdefender, což potvrzuje kvalitu našich produktů a nejvyšší přesnost detekce. Jsme odhodláni vyvíjet vlastní technologie a udržovat více než 50 % našich zaměstnanců na pozicích výzkumu a vývoje.

Proč Bitdefender

Hrdě sloužíme našim zákazníkům

Společnost Bitdefender poskytuje řešení a služby pro malé a střední podniky, poskytovatele služeb a technologické integrátory. Jsme hrdí na důvěru, kterou nám projevují podniky jako např. **Mentor, Honeywell, Yamaha, Speedway, Esurance or Safe Systems**

Vedoucí pozice v inauguračním žebříčku Forrester Wave™ pro zabezpečení cloudové pracovní zátěže

Hodnocení NSS Labs "Doporučeno" ve skupinovém testu NSS Labs AEP Ocenění SC Media Industry Innovator Award za introspekci hypervizoru, 2. rok v řadě

Reprezentativní prodejce platforem pro ochranu cloudového pracovního zatížení společnosti Gartner®

Věnováno našim +20 000 partnerům po celém světě

Společnost Bitdefender je exkluzivním prodejcem a je hrdá na to, že může sdílet úspěch s desítkami tisíc prodejců a distributorů po celém světě.

Pětihvězdičkový partner CRN, 4. rok v řadě. Uznáván na seznamu CRN Security 100. CRN Cloud Partner, 2. rok v řadě

Důvěryhodná bezpečnostní autorita

Společnost Bitdefender je hrdým technologickým aliančním partnerem hlavních dodavatelů virtualizace, který přímo přispívá k rozvoji bezpečných ekosystémů. **VMware, Nutanix, Citrix, Linux Foundation, Microsoft, AWS, and Pivotal.**

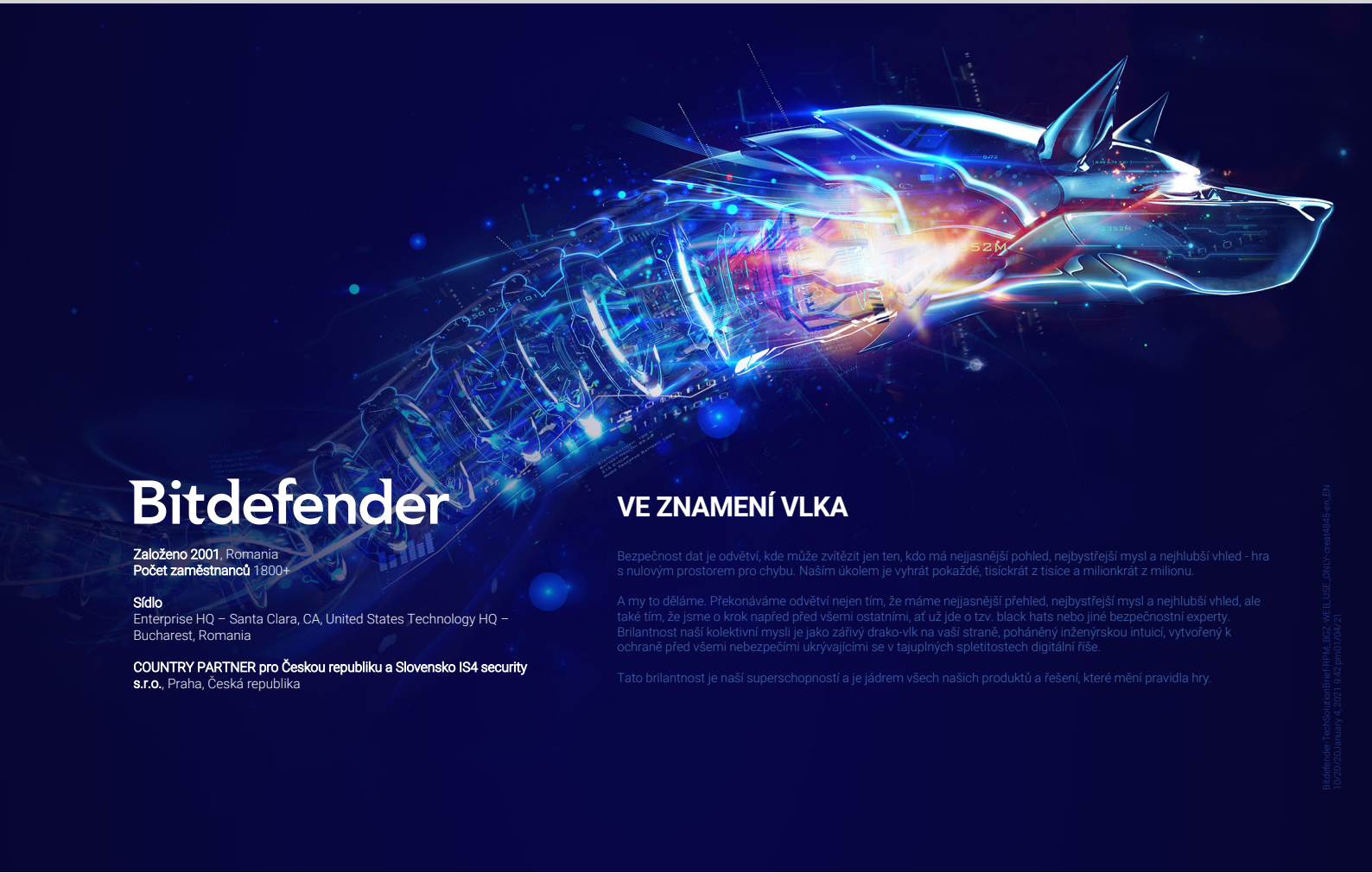
Prostřednictvím svého špičkového forenzního týmu se Bitdefender také aktivně zapojuje do boje proti mezinárodní počítačové kriminalitě společně s významnými orgány činnými v trestním řízení, jako jsou FBI a Europol, v rámci iniciativ, jako jsou NoMoreRansom a TechAccord, a také do likvidace černých trhů, jako je Hansa. Od roku 2019 je společnost Bitdefender také hrdě jmenovanou autoritou pro číslování CVE v rámci partnerství MITRE.

UZNÁVANÉ PŘEDNÍMI ANALYTIKY A NEZÁVISLÝMI TESTOVACÍMI ORGANIZACEMI.

CRN AV-TEST AV Gartner 451 Research FORRESTER IDC GLOBAL

TECHNOLOGICKÉ ALIANCE

Microsoft NUTANIX aws Pivotal Cloud Foundry CITRIX



Bitdefender

Založeno 2001, Romania
Počet zaměstnanců 1800+

Sídlo
Enterprise HQ – Santa Clara, CA, United States Technology HQ – Bucharest, Romania

COUNTRY PARTNER pro Českou republiku a Slovensko IS4 security s.r.o., Praha, Česká republika

VE ZNAMENÍ VLKA

Bezpečnost dat je odvětví, kde může zvítězit jen ten, kdo má nejjasnější pohled, nejbystřejší mysl a nejhlubší vhled - hra s nulovým prostorem pro chybu. Naším úkolem je vyhrát pokaždé, tisíckrát z tisíce a milionkrát z milionu.

A my to děláme. Překonáváme odvětví nejen tím, že máme nejjasnější přehled, nejbystřejší mysl a nejhlubší vhled, ale také tím, že jsme o krok napřed před všemi ostatními, ať už jde o tzv. black hats nebo jiné bezpečnostní experty. Brilantnost naší kolektivní mysli je jako zářivý drako-vlk na vaší straně, poháněný inženýrskou intuicí, vytvořený k ochraně před všemi nebezpečími ukrývajícími se v tajuplných spletitostech digitální říše.

Tato brilantnost je naší superschopností a je jádrem všech našich produktů a řešení, které mění pravidla hry.

Bitdefender-TechSolutionBrief-FPPM_LBZ-WEB_USE_ONLY-creat4845-en_EN 10/20/20January 4, 2021 9:42 pm01.04.21