Cisco Ransomware Defense: držte si ransomware od těla

Co kdybyste se mohli bránit proti ransomwaru bez ohledu na způsoby, jakými se k vám snaží proniknout? Pouze společnost Cisco vám poskytuje produkty pro zabezpečení a architekturu, které toto umí.

Přehled

Soubory a informace jsou životodárnou tekutinou společnosti. Ochrana a neporušenost těchto informací, a tím i zajištění produktivity vaší společnosti, jsou nutností.

Do toho však vstupuje ransomware, škodlivý software, neboli malware, který uzamkne informace v soukromém nebo firemním počítači, například dokumenty, fotografie a hudbu. Tyto soubory nevydá, dokud uživatel nezaplatí poplatek, neboli výkupné, aby tyto soubory odemkl a získal je zpět. Bez vhodné obrany může ransomware způsobit dostatečně velké škody, aby donutil společnost pracovat pouze s perem a papírem.

Ransomware je obvykle doručen prostřednictvím exploit kitů, nakažených reklam (na webových stránkách, které mohou doručit malware), phishingu (podvodných e-mailů maskujících se jako důvěryhodné) nebo spamových kampaní. Skutečná infekce může začít, když někdo klikne na odkaz nebo přílohu ve phishingových e-mailech. K infekci může také dojít, když uživatelé prohlíží stránky s nakaženými reklamami, které počítače automaticky infikují.

Vstupte do světa Cisco® Ransomware Defense. Toto řešení omezuje riziko infekcí ransomwarem díky vícevrstvému přístupu, od vrstvy DNS po koncový bod a sítě, e-maily a web. Poskytujeme integrovanou obranu s architektonickým přístupem, který kombinuje vynikající viditelnost hrozeb s jedinečnou reaktivitou vůči ransomwaru.

Výhody

- **Snížení rizika ransomwaru**, abyste se mohli soustředit na chod vaší společnosti
- **Získání okamžité ochrany** díky zabezpečení, které dokáže zablokovat hrozby dříve, než se pokusí zapustit kořeny
- **Získání výborné viditelnosti hrozeb a reaktivity** z architektonického přístupu, od vrstvy DNS po síť a koncové body
- **Předcházení laterálnímu šíření malwaru** díky silné segmentaci sítě
- **Získání poznatků a informací o ransomwaru** z předního výzkumného týmu v oboru hrozeb – od společnosti Talos

Rychle rostoucí a mocná hrozba

Toto je rok ransomwaru. A ukazuje se jako skutečně ziskový. Ransomware se rychle stal nejlukrativnějším typem malwaru, který jsme kdy viděli.

FBI tvrdí, že ransomware je na cestě k dosažení ročního obratu 1 miliardy USD. Výzkum společnosti Cisco Talos ukazuje, že jediná kampaň ransomwaru může vygenerovat ročně až 60 milionů USD. Ransomware získává tolik pozornosti, že se již vyskytl v televizních pořadech.

Útočníci mají prostředky a touhu pokračovat v inovacích ransomwaru, aby se stal mnohem nakažlivějším. Myslíme si, že ransomware se stane mnohem schopnější v autopropagaci s cílem uzamčení rozsáhlých částí podnikové sítě. Takový krok by v podstatě srazil fungování IT společnosti zpět do roku 1970.

Aktuální reakce na ransomware mají tendenci se zaměřovat na jednotlivé produkty. Musíme zvážit zavedení vícevrstvého architektonického přístupu vzhledem k různým směrům, na které se ransomware zaměřuje, aby dosáhl infekce.

Tento přehled řešení se zaměřuje na různé směry a metody, které útočníci používají. Obránci musí zabezpečit jak e-mail, tak i web, blokovat přístup ke škodlivé infrastruktuře na internetu, zastavit všechny soubory ransomwaru, které se dostanou až k cíli, zablokovat používaná zpětná volání typu command-and-control a zabránit snadnému laterálnímu pohybu ransomwaru, pokud dojde k infekci.

Co kupujete

Řešení Cisco Ransomware Defense spojuje dohromady všechny nezbytné součásti architektury zabezpečení společnosti Cisco pro řešení problémů s ransomwarem. Můžete si vybrat všechny součásti nebo pouze ty, které splní vaše okamžité potřeby zabezpečení.

Řešení Ransomware Defense zahrnuje:

- nástroj Cisco Umbrella, který blokuje hrozby ve vrstvě DNS, daleko od vaší sítě;
- nástroj Cisco Advanced Malware Protection (AMP) pro koncové body, který blokuje spouštění škodlivých souborů ransomwaru na koncových bodech;

- nástroj Cisco Email Security v cloudu i lokálně zastavuje phishingové a spamové zprávy, které se snaží doručit ransomware;
- nástroj Advanced Malware Protection můžete okamžitě přidat do produktů zabezpečení e-mailů pomocí snadné licence pro statickou a dynamickou analýzu (sandboxing) neznámých příloh, které překročí bránu zabezpečení e-mailu společnosti Cisco;
- firewall nové generace Cisco Firepower™ (NGFW), který blokuje přenosy typu command-and-control a všechny škodlivé soubory procházející sítí;
- nástroj Cisco ISE prostřednictvím sítě Cisco dynamicky segmentuje vaši síť, aby se ransomware nemohl šířit laterálně.

Díky produktu Ransomware Defense mohou společnosti využívat své sítě pro zastavení šíření ransomwaru. Ten se nebude moci v případě infekce šířit po síti tak snadno.

Služba Cisco Security Services může okamžitě stanovit priority podle naléhavosti v reakci na incident v případě propuknutí infekce. Také usnadňuje nasazování nástrojů AMP, NGFW a dalších produktů.

Klíčové funkce

- Blokuje ransomware a znemožňuje jeho vniknutí do sítě nebo stažení do přenosných počítačů.
- Zastavuje ransomware v případech, kdy už vstoupil do sítě.

Security Services pomáhají bojovat s ransomwarem

Cisco Security Services Incident Response tým dokáže zajistit jak služby připravenosti reakce na incidenty, tak i okamžité reakce na incidenty v případě infekce ransomwarem.

A konečně Cisco Security Integration Services řeší problémy a výzvy při řešení bezpečnostní architektury. Zjednodušují nasazení technologií řešení jako AMP pro koncové body a Cisco Firepower NGFW. Náš tým má hluboké znalosti ohledně poskytování integrovaných řešení zabezpečení k urychlení přijímání potřebných bezpečnostních technologií, a to s minimálním narušením.

A co více, společnosti musí také zajistit, že mají vhodné technologie a zásady pro zálohování dat jako pojistku proti dopadům nákazou ransomwaru.

„Pokryli jsme velká rizika v případech útoků ransomwaru z webu a významně jsme vylepšili zkušenosti uživatelů týkající se internetové konektivity.“

– Octapharma

Cisco Capital

Financování, které vám pomůže dosáhnout vašich cílů

Financování Cisco Capital® vám může pomoci získat technologie, které potřebujete k dosažení svých cílů, abyste zůstali konkurenceschopní. Můžeme vám pomoci snížit investiční výdaje. Zrychlit váš růst. Optimalizovat investované peníze a návratnost investic. Financování Cisco Capital vám poskytuje flexibilitu při pořizování hardwaru, softwaru, služeb a doplňkového vybavení třetích stran. A je účtována pouze jedna předvídatelná platba. Financování Cisco Capital je dostupné ve více než 100 zemích. Další informace.

Výhody řešení Cisco

Ransomware si najde cestu do vaší společnosti všemi možnými prostředky. Phishingové e-maily, infikované webové bannery, spam – mnoho směrů, které je třeba chránit. Pouze společnost Cisco přináší architekturu zabezpečení, která je schopna čelit výzvám ransomwaru. Samostatné produkty nebudou dostačovat. Naše řešení je založeno na základech přední společnosti v oboru výzkumu hrozeb, Talos Research Group, která provedla rozsáhlý výzkum hrozeb týkajících se ransomwaru. Tento výzkum je základem naší efektivní vícevrstvé ochrany. Blokujeme ransomware a bojujeme s ním, i když proklouzne trhlinami a dostane se do vaší sítě – což se může stát nemilou realitou.

C22-737492-01 08/16