# Ransomvér: Všetko, čo potrebujete vedieť

**Ste zaneprázdnení. Ste unavení. Chcete si len zahrať Pokémon Go alebo zájsť na firemný intranet. Nech už je dôvod akýkoľvek, zakaždým, keď v prípade aktualizácie softvéru kliknete na „Pripomenúť neskôr“, vaše zariadenie je nechránené voči ransomvéru.**

**Ide len o jeden z možných spôsobov, ako sa ransomvér môže dostať do vášho systému. Škodlivé reklamy, e-maily zamerané na neoprávnené získavanie údajov a dokonca aj sofistikované schémy s použitím USB kľúčov predstavujú bežné taktiky, ktoré protivníci používajú na napadnutie vášho systému. Poďme sa bližšie pozrieť na jeden spoločný scenár.**

## Kliknete na „Pripomenúť neskôr“

Žiadny softvér nie je dokonalý. Vývojoví pracovníci pravidelne identifikujú vo svojich programoch chyby a uvádzajú na trh záplaty na ich opravu. Keď odkladáte aktualizáciu vašich doplnkov alebo aplikácií, protivníci môžu ľahko zneužiť tieto známe aspekty zraniteľnosti. Pokiaľ ide o obľúbený spôsob šírenia ransomvéru, technológia Flash je zodpovedná až za 80 % úspešných pokusov. Či už ide o Flash, Silverlight alebo dokonca Google Chrome, pravidelne aktualizujte a využívajte funkciu bezpečnostných záplat.

## Ste infikovaní

Ransomvér teraz prevezme kontrolu nad cielenými systémami vo vašom zariadení. Potom použije asymetrickú výmenu kľúčov na zašifrovanie vašich súborov. V podstate je schopný zakódovať vaše údaje bez vášho súhlasu – a kľúč na riešenie má len vývojár ransomvéru. Niektoré formy ransomvéru sa šíria aj po sieti. Niektorí experti predpovedajú, že toto samošírenie bude bežné.

## Zobrazí sa správa týkajúca sa výkupného

Po dokončení infikovania sa na obrazovke zobrazí správa, aby ste zaplatili výkupné za svoje údaje v bitcoinoch. Výška bežného výkupného sa môže pohybovať od 188 Euros – 9,400 Euros, niektoré inštitúcie však už zaplatili aj oveľa vyššiu cenu. Jedna nemocnica v Kalifornii zaplatila za opätovný prístup k svojim údajom 16,000 Euros. Došlo k tomu potom, ako každý deň prišla o 94,000 Euros, pretože nemohla normálne fungovať.

Bezpečnostní experti odporúčajú neplatiť výkupné. Niektoré typy ransomvéru buď nedokážu odomknúť vaše súbory, alebo ich automaticky zničia. Členovia tímu Talos, ktorí sa zaoberajú výskumom hrozieb, zistili, že tieto škodlivé, deštruktívne typy ransomvéru sa vyskytujú stále častejšie. Podľa našej polročnej správy týkajúcej sa bezpečnosti za rok 2016 pracovníci zaoberajúci sa výskumom hrozieb varujú, že integrita dát predstavuje pri ransomvéri nový problém. Protivníkom nemožno dôverovať v tom, že zachovajú integritu dát, ktoré šifrujú, a potenciálny dôsledok napríklad zmanipulovaných lekárskych záznamov alebo konštrukčných návrhov môže byť obrovský.

Navyše tým, že zaplatíte výkupné, podporíte podnikavosť zločincov. Kým útočníci budú zarábať z týchto programov, budú aj naďalej vytvárať ešte silnejšie kmene ransomvéru.

## Ako zastaviť ransomvér

Najlepším spôsobom, ako sa pripraviť na ransomvér, je nasadiť vrstvený bezpečnostný prístup.

### Pred útokom

Niekoľkými jednoduchými spôsobmi môžete posilniť svoju obrannú pozíciu. Pokiaľ ide o záložný plán, mali by ste vážne uvažovať o použití partnera na zotavenie po havárii, ktorý by udržal hladký chod vašej firmy v prípade, že nastane to najhoršie. Môžete však prijať aj jednoduchšie opatrenia. Pravidelne zálohujte svoje súbory a tým ochránite svoje dôležité údaje. Nainštalujte blokátory zobrazovania reklám a vždy po výzve aktualizujte softvér.

Samotné blokátory zobrazovania reklám však nedokážu detegovať a zablokovať všetky škodlivé reklamy alebo identifikovať všetky škodlivé hypertextové prepojenia. Zvážte používanie riešenia Cisco® Umbrella, ktoré možno nainštalovať do 5 minút. Slúži na detegovanie škodlivých webových lokalít a zablokovanie žiadostí na úrovni hostiteľa.

### V priebehu útoku

Pomocou riešenia Umbrella sa drvivá väčšina ransomvérových súborov zastaví vo vrstve DNS ešte skôr než sa vôbec dostane do zariadenia koncového používateľa. Aj napriek všetkým snahám zameraným na prevenciu vám žiadna metóda neposkytne úplnú ochranu pred ransomvérom.

Musíte vidieť, čo sa deje vo vašej sieti a dokázať identifikovať útoky, keď k nim dochádza. Nástroj na detekciu hrozieb Cisco Stealthwatch™ monitoruje sieťovú prevádzku a vidí, keď dôjde k niečomu neobvyklému – napr. infikovaniu ransomvérom. Vydá upozornenie, že došlo k napadnutiu systému.

# Ransomvér: Všetko, čo potrebujete vedieť

Keď sa súbor pokúsi spustiť, Cisco má výkonné nástroje na to, aby ho zastavil.

- Umbrella chráni váš systém tým, že blokuje požiadavku súboru na zašifrovanie kľúčovej infraštruktúry. To znamená, že ransomvér nedokáže spätne komunikovať a získať informácie potrebné na šifrovanie údajov.
- Keď Umbrella blokuje požiadavku, firewall budúcej generácie od spoločnosti Cisco zablokuje pripojenie a poskytne vám tak osobitnú ochranu.
- V prípade, že súbor prekoná vrstvu DNS a firewallu, riešenie Cisco Advanced Malware Protection (AMP) for Endpoints dokáže zablokovať postup súboru a následne prejde na ďalší krok. Neustále analyzuje všetky aktivity súborov v rámci celého systému, takže máte možnosť nájsť a odstrániť všetky škodlivé súbory.

## Po útoku

Ak ste už boli napadnutí ransomvérom, je potrebné zistiť rozsah poškodenia a zastaviť jeho šírenie. AMP dokáže zastaviť postup známych malvérových súborov a odstrániť súbor v koncovom bode.

Ak chcete zastaviť šírenie ransomvéru po celej sieti, dynamická segmentácia s technológiou Cisco TrustSec® dokáže identifikovať, do akých častí siete ransomvér prenikol, a pomôže zastaviť jeho šírenie.

Chcete sa dozvedieť viac? Vyskúšajte cisco.com/go/security.



C11-737870-00 09/16