Ransomware: tot ce trebuie să știți

Sunteți ocupat. Sunteți obosit. Vreți doar să jucați Pokémon Go sau să accesați rețeaua intranet a companiei. Indiferent care ar fi motivul, ori de câte ori faceți clic pe „Amintește-mi mai târziu” în caseta de actualizare a unui software, dispozitivul dumneavoastră devine vulnerabil la ransomware.

Acesta este unul dintre numeroasele moduri în care atacurile ransomware pot pătrunde în sistemul dumneavoastră. Publicitatea rău intenționată, e-mailurile de phishing și chiar schemele complexe de tip thumb-drive sunt tactici comune pe care inamicii le utilizează pentru a vă compromite sistemul. Haideți să privim cu mai multă atenție detaliile unui scenariu comun.

Faceți clic pe „Amintește-mi mai târziu”

Niciun software nu este perfect. Dezvoltatorii identifică frecvent erori în programe și lansează corecții pentru a le remedia. Atunci când întârziați actualizarea inserturilor sau a aplicațiilor, inamicii pot exploata cu ușurință aceste vulnerabilități cunoscute. Unul dintre cele mai populare kituri de vulnerabilitate este Flash, care a cumulat peste 80% dintre încercările reușite. Indiferent că este vorba despre Flash, Silverlight sau chiar Google Chrome, utilizați cu regularitate actualizările și corecțiile.

Sunteți infectat

Ransomware controlează acum sistemele vizate de pe dispozitivul dumneavoastră. Apoi utilizează un schimb de chei asimetrice pentru a vă cripta fișierele. În principiu, poate să vă secretizeze datele fără acordul dumneavoastră și numai dezvoltatorul atacului ransomware deține cheia. Anumite forme de ransomware se propagă în rețea. Experții în securitate prevăd că această autopropagare va deveni mult mai semnificativă.

Apare un mesaj de răscumpărare

După finalizarea infecției, va apărea un mesaj pe ecran, în care vi se solicită să plătiți o răscumpărare în bitcoin pentru datele dumneavoastră. O răscumpărare obișnuită poate fi cuprinsă între 850 RON - 42.500 RON, însă anumite instituții au plătit un preț mult mai mare. Un spital din California a plătit 72.000 RON în schimbul datelor. Acest lucru după ce în fiecare zi în care nu au funcționat normal au plătit 425.000 RON.

Experții în securitate vă sfătuiesc să nu plătiți răscumpărarea. Anumite tipuri de ransomware vă pot debloca fișierele sau le pot distruge automat. Cercetătorii Talos în domeniul amenințărilor au descoperit că aceste tipuri de ransomware rău intenționate, care distrug toate datele, devin din ce în ce mai răspândite. Conform Raportului nostru de securitate pentru prima jumătate a anului 2016, cercetătorii în domeniul amenințărilor avertizează că integritatea datelor este o nouă problemă în ceea ce privește atacurile ransomware. Nu puteți avea încredere că inamicii vor păstra integritatea datelor pe care le criptează, iar daunele potențiale în urma modificării dosarelor medicale sau a modelelor de inginerie, de exemplu, pot fi dezastruoase.

În plus, prin plata răscumpărării, susțineți o companie de infractori. Cât pot face bani din aceste scheme, atacatorii vor continua să creeze tipuri și mai puternice de ransomware.

Metode de oprire a atacurilor ransomware

Cea mai bună modalitate să țineți piept unui atac ransomware este implementarea unei abordări stratificate de securitate.

Înainte de un atac

Vă puteți îmbunătăți poziția defensivă în mai multe moduri simple. Ar trebui să luați în calcul un partener care să vă ajute cu recuperarea datelor în caz de dezastre, ca plan de backup, pentru ca afacerea dumneavoastră să funcționeze fără probleme în cazul unui incident. Însă puteți utiliza metode și mai simple. Faceți backup fișierelor cu regularitate pentru a vă proteja datele importante. Instalați programe de blocare a reclamelor și actualizați-vă întotdeauna software-ul atunci când vi se solicită.

Totuși, programele de blocare a reclamelor nu pot detecta și bloca singure toate reclamele rău intenționate și nu pot identifica hyperlinkurile compromise. Utilizați Cisco® Umbrella, care poate fi instalat în mai puțin de 5 minute. Acesta detectează site-urile rău intenționate și blochează solicitările la nivelul gazdei.

În timpul unui atac

Cu „Umbrella”, majoritatea fișierelor ransomware vor fi oprite la nivel DNS, înainte de a ajunge în dispozitivul utilizatorului. În ciuda acestor eforturi de prevenire, nicio metodă nu vă poate oferi protecție completă împotriva ransomware.

Trebuie să vedeți ce se întâmplă în rețea și să puteți identifica atacurile atunci când au loc. Cisco Stealthwatch™ monitorizează traficul din rețea și observă când se întâmplă ceva anormal, cum ar fi infectarea cu ransomware. Acesta emite o alertă care vă anunță că sistemul a fost compromis.

Ransomware: tot ce trebuie să știți

Când fișierul încearcă să ruleze, Cisco deține instrumentele puternice pentru a-l opri:

- „Umbrella” vă protejează sistemul prin blocarea solicitării fișierelor de a accesa infrastructura cu cheie de criptare. Acest lucru înseamnă că atacurile ransomware nu pot obține informațiile necesare pentru a vă cripta datele.
- Atunci când „Umbrella” blochează solicitarea, firewallul de ultimă generație Cisco blochează conexiunea, oferindu-vă protecție suplimentară.
- În cazul în care un fișier trece atât de nivelul DNS, cât și de firewall, „Cisco Advanced Malware Protection (AMP)” pentru terminale poate bloca rularea acestuia și trece la pasul următor. Acesta analizează în mod continuu toate activitățile fișierelor din sistem, oferindu-vă posibilitatea de a găsi și de a elimina toate fișierele rău intenționate.

După atac

Dacă ați fost deja infectat cu ransomware, trebuie să analizați daunele și să împiedicați răspândirea acestora. AMP poate opri rularea fișierelor malware cunoscute și poate elimina fișierul dintr-un terminal.

Pentru a opri răspândirea atacurilor ransomware într-o rețea, segmentarea dinamică ce utilizează tehnologia Cisco TrustSec® poate identifica ce părți ale unei rețele au fost atacate de ransomware și ajuta la oprirea răspândirii.

Doriți să aflați mai multe? cisco.com/go/security.

C11-737870-00 09/16