Ransomware: vše, co potřebujete vědět

Máte hodně práce. Jste unavení. Chcete si jen zahrát hru Pokémon Go nebo používat intranet své společnosti. Ať už je důvod jakýkoliv, kdykoliv kliknete u aktualizace softwaru na možnost „Připomenout později“, činíte zařízení zranitelné vůči ransomwaru.

To je jen jeden z mnoha způsobů, jakými může ransomware proniknout do vašeho systému. Škodlivé reklamy, phishingové e-maily a dokonce i sofistikované intriky pomocí přenosných disků představují běžné taktiky, které protivníci používají k narušení bezpečnosti vašeho systému. Pojďme se blíže podívat na jeden běžný scénář.

Kliknete na „Připomenout později“

Žádný software není dokonalý. Vývojáři pravidelně nacházejí chyby ve svých programech a vydávají aktualizace za účelem jejich opravy. Když zpozdíte aktualizaci modulů plug-in nebo aplikací, protivníci mohou tato známá slabá místa snadno zneužít. U jednoho exploit kitu byla aplikace Flash příčinou 80% úspěšnosti pokusů. Ať už jde o Flash, Silverlight nebo dokonce Google Chrome, pravidelně aktualizujte a záplatujte.

Jste nakažení

Ve vašem zařízení teď ransomware přebírá kontrolu nad cílovými systémy. Následně použije asymetrickou výměnu klíčů k zašifrování souborů. V podstatě bude schopen zašifrovat vaše data bez vašeho souhlasu – a pouze vývojář ransomwaru má klíč, který je odemkne. Některé formy ransomwaru se také šíří po síti. Odborníci na zabezpečení předvídají, že toto autonomní šíření bude stále častější.

Zobrazí se poznámka o výkupném

Po infikování se na obrazovce zobrazí zpráva vyžadující, abyste za svá data zaplatili výkupné v bitcoinech. Obvykle může výkupné představovat částku od 5 100 do 255 000 Kč, ale některé instituce zaplatily i mnohem vyšší částku. Jedna nemocnice v Kalifornii zaplatila výměnou za svá data 434 000 Kč. To bylo poté, co přišli o 2,5 milionu Kč za každý den, kdy nemohli normálně fungovat.

Odborníci na zabezpečení radí, abyste výkupné neplatili. Některé typy ransomwaru buď nemohou odemknout vaše soubory, nebo je automaticky zničí. Výzkumníci hrozeb společnosti Talos zjistili, že tyto škodlivé, vše ničící typy ransomwaru jsou stále častější. Podle naší zprávy o zabezpečení z poloviny roku 2016 výzkumníci hrozeb varují, že novým problémem u ransomwaru je integrita dat. Protivníkům nelze důvěřovat, že zachovají integritu dat, která šifrují, a potenciální dopady způsobené manipulací například s lékařskými záznamy nebo konstrukčními návrhy mohou být masivní.

A navíc zaplacením výkupného podporujete zločinecký podnik. Dokud z podobných útoků dokážou získat peníze, budou útočníci pokračovat ve vytváření ještě schopnějších druhů ransomwaru.

Jak zastavit ransomware

Nejlepší způsobem, jak se připravit na ransomware, je použít přístup vícevrstvého zabezpečení.

Před útokem

Můžete posílit své obranné pozice několika jednoduchými způsoby. Velice doporučujeme naplánovat a používat záložní plány pro obnovení činnosti po incidentu a to, jak udržet vaše podnikání v chodu, když dojde na nejhorší. Ale můžete využít i jednodušší opatření. Pravidelně zálohujte své soubory, abyste ochránili důležitá data. Nainstalujte nástroje pro blokování reklamy a vždy po vyzvání svůj software aktualizujte.

Nástroje na blokování reklamy samy o sobě nedokážou zjistit a blokovat všechny škodlivé reklamy nebo identifikovat škodlivé odkazy. Zvažte využití aplikace Cisco® Umbrella, kterou lze nainstalovat za méně než 5 minut. Zjišťuje škodlivé stránky a blokuje žádosti na úrovni hostitele.

Během útoku

Díky aplikaci Umbrella bude velká většina souborů ransomwaru zastavena na úrovni vrstvy DNS, než se dostanou do zařízení koncového uživatele. Navzdory nejlepším snahám o prevenci vám žádná metoda nezajistí naprostou ochranu před ransomwarem.

Musíte vidět, co se děje ve vaší síti, a být schopni identifikovat útoky v jejich průběhu. Detekce hrozeb Cisco Stealthwatch™ sleduje síťový provoz a vidí, když dojde k něčemu neobvyklému – například infekci ransomwarem. Zobrazí upozornění, že systém byl narušen.

Ransomware: vše, co potřebujete vědět

Když se soubor pokusí spustit se, společnost Cisco má účinné nástroje, jak ho zastavit:

- Aplikace Umbrella chrání váš systém blokováním odesílání žádostí souboru do infrastruktury šifrovacích klíčů. To znamená, že ransomware nedokáže odpovědět a získat informace potřebné k zašifrování vašich dat.
- Jelikož aplikace Umbrella blokuje žádosti, brána firewall nové generace společnosti Cisco zablokuje připojení a poskytne vám dodatečnou ochranu.
- Pokud se soubor dostane za vrstvu DNS a bránu firewall, aplikace Cisco Advanced Malware Protection (AMP) pro koncové body dokáže zablokovat spuštění souboru a pak jde ještě o krok dále. Neustále analyzuje veškerou aktivitu souboru v systému a poskytuje vám schopnost najít a odstranit všechny škodlivé soubory.

Po útoku

Pokud jste již byli infikováni ransomwarem, musíte lokalizovat škody a zastavit jeho šíření. Aplikace AMP dokáže zabránit spuštění známých souborů malwaru a odstranit soubor v koncovém bodě.

K zastavení šíření ransomwaru v síti lze využít dynamickou segmentaci pomocí technologie Cisco TrustSec®, která dokáže identifikovat, do kterých částí sítě ransomware pronikl, a pomůže zastavit jeho šíření.

Chcete vědět víc? Podívejte se na web cisco.com/go/security.

C11-737870-00 09/16