Technet.cz

V Benešově udeřil virus, který vydírá nemocnice i města po celém světě

11. prosince 2019 10:46, aktualizováno 11:35

V benešovské nemocnici pravděpodobně zaútočil typ počítačového viru, který dokáže z provozu vyřadit policii, úřady i celá města. V Česku novinka, jinde už běžná praxe.

ilustrační snímek | foto: @k3r3n3, Jan Kužník, Technet.cz

Provoz benešovské nemocnice zcela narušil počítačový virus, který v noci napadl nemocniční počítačový systém. Nelze spustit žádný přístroj včetně počítačové sítě. Nemocnice musí rušit i plánované operace. Lékaři odbavují pacienty postaru, jako „před příchodem počítačů“.

Podrobnosti o viru zatím nejsou známé, ale oslovení odborníci se shodují na tom, že došlo k nakažení takzvaným kryptovirem neboli ransomwarem. Tento typ viru zjednodušeně řečeno zašifruje data v počítači tak, že jej nejde používat. Útočník většinou žádá za rozšifrování výkupné. Zda je tomu tak i v případě benešovské nemocnice, zatím není známo.

Týdny plné potíží

Provoz v Benešově se nepodaří rychle obnovit, technici musí vyčistit na 300 počítačů

Benešovská nemocnice není zdaleka prvním případem. Loni útočníci ransomwarem zaútočili na systém léčebny v Janově na Rokycansku. Před několika týdny udeřili ransomwarem na tři velké nemocnice ve státě Alabama. Lékaři museli všem neakutním pacientům zrušit schůzky a výkony. Problémy s obnovou IT systému byly takového rázu, že se majitel nemocnic rozhodl v úterý 8. října vyděračům zaplatit, aby obdržel klíč k dešifrování svých vlastních dat. Kolik přesně zločinci obdrželi, zatím nebylo zveřejněno.

Fotogalerie

Úspěšné útoky vyděračů na nemocnice jsou za poslední dny hlášeny také z Austrálie. Během srpna byla napadena zdravotnická zařízení ve Filadelfii a

Zobrazit fotogalerii

Wyomingu. A to nejsou zdaleka všechny případy posledních měsíců.

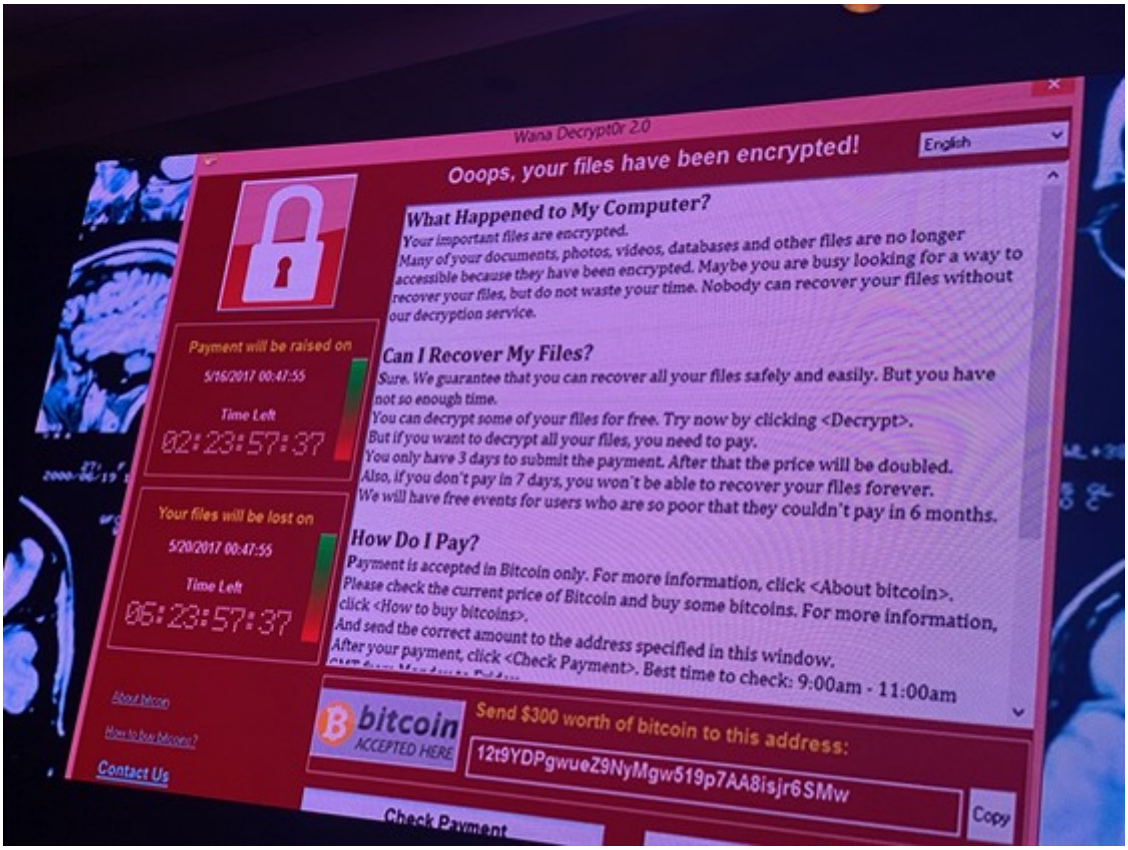
FBI vydala počátkem října speciální varování před ransomwarem a pro postižená města zřídila poradenskou linku.

Jen během dvou letních měsíců bylo letos v USA napadeno vyděračským softwarem přes 22 obcí. Takzvaný ransomware paralyzoval policii v třicetitisícovém městě, ale třeba i malou knihovnu v Texasu.

Co odstavilo nemocnici a dokáže ochromit i celé město?

Ransomware se šíří obvykle e-mailem, ale do počítače se může dostat i na USB disku, stažením nakaženého souboru z cloudového úložiště atd. Aby došlo k infikování, vyžaduje interakci oběti. Většinou ji dosáhne tím, že nabídne nahé fotografie Brada Pitta, aktuální filmový kinohit ke stažení nebo podvrhne dokument, který se tváří jako nezplacená faktura pro danou firmu.

Následně stačí, aby nepozorný uživatel soubor otevřel (většinou má příponu ZIP nebo jinou podobnou, která evokuje zkomprimovaný soubor). Otevřením souboru se spustí instalace viru. V lokální síti se šíří skrze nezáplatované systémy. Zároveň si některé viry vytvoří i vlastní botnetovou síť, pomocí které skenují dostupné IP adresy a hledají další zranitelné počítače.



Takto může vypadat to jediné, co se vám na počítači napadeném ransomwarem zobrazí: pokyn k zaplacení výkupného.

Některé ransomwary šifrují jen vybrané soubory (jako například „populární“ WannaCry), jiné, jako v případě benešovské nemocnice, zašifrují počítač tak, že jediná operace, kterou může uživatel provést, je zaplatit výkupné nebo stroj vypnout.

Existují však i mnohem zákeřnější a velmi těžko odhalitelné způsoby útoku. „Skrze takzvaný spear phishing je útok veden například na konkrétního člověka z vedení firmy. Právě ten může disponovat administrátorskými právy a je klíčem k celé firemní síti. Útočníci znají charakter společnosti i chování dané oběti a podle toho podvrhnou například e-mailovou komunikaci. Oběť si tak může několik dní dopisovat s obchodním partnerem, kterým je ve skutečnosti útočník chystající si půdu pro úder. Takto podvržené e-maily samozřejmě neobsahují žádnou přílohu, kterou by dokázal běžný antivirus odhalit,“ vysvětluje odborník přes zabezpečení a zálohování systému Aleš Hok ze společnosti Zebra Systems zastupující společnost Acronis v ČR .

Postupně, ale někdy i jen v jediném e-mailu, donutí oběť kliknout na odkaz, který se tváří například jako stránky s ceníkem partnerské firmy. „Stránky jsou pak už rovnou infikované nebo přinutí návštěvníka, aby si nainstaloval domněle chybějící doplněk, který je k prohlížení webu nutný. Například podvrhnou hlášení o zastaralém Java scriptu. Instalací doplňku/viru dojde k infikování počítače,“ dodává Hok.

Útočníci si díky administrátorskému pověření získanému od oběti mohou v síti napadané firmy dělat, co se jim zamane. Někdy rovnou zašifrují celou síť, nebo pomalu infikují systém a začnou škodit v pozadí. Nejprve například vyřadí antivirus a zálohovací systémy a vyčkávají.

Pokud je napadený systém zranitelný (například nezáplatované nebo staré Windows), dokáže se virus rozšířit i na další stroje a začne šifrovat i z nich. Zastavit takový útok je mnohem obtížnější, než když se nákaza šíří jen z jednoho stroje.

Právě nedostatečné zabezpečení systémů, špatně řešené nebo dokonce žádné zálohování a obnovení dat jsou podle odborníků jedny z hlavních důvodů, proč se v poslední době masivně daří útokům vedeným pomocí vyděračského softwaru, takzvaného ransomwaru. Dosud používané způsoby zabezpečení, zálohy a obnovy dat přestávají stačit. Útoky ransomwarem se však České republice dosud z velké části vyhýbaly.

Virus budoucnosti
Přečtěte si článek z roku 2016, který bohužel stále platí.

Jak se bránit?

Název viru ransomware je odvozen z anglického slova ransom, což česky znamená výkupné. „Útočník zpravidla požaduje za opětovné zpřístupnění zašifrovaných dat výkupné. Částka, kterou je oběť nucena zaplatit, přitom může být od zlomků bitcoinu, při plošném útoku, po statisícové i vyšší částky při cílené aktivitě útočníka,“ vysvětluje Ondřej Šafář ze společnosti ESET.

„Hlavním způsobem ochrany je využití spolehlivých kyberbezpečnostních produktů a zároveň správně implementované bezpečnostní politiky včetně zálohování,“ dodává Šafář.

Při zálohování dat platí jednoduché, ale ne vždy dodržované pravidlo, které lze shrnout do „šifry“: 3 - 2 - 1. Do češtiny přeloženo to znamená: Pořiďte si tři kopie dat, uložte je na dvě místa, z nichž jedno by mělo být uloženo mimo budovu, kde se nachází první kopie. To samozřejmě platí nejen pro firmy, ale pro kohokoliv, kdo chce například své digitálně uložené fotografie ukazovat i vnoučatům za dvacet let.

Podmínka, že druhá kopie by měla být mimo budovu, je důležitá a často opomíjená. „Není neobvyklé, že klient si druhé diskové pole uloží jen do jiné místnosti téhož podzemí,“ podotýká Martin Beran, systémový inženýr společnosti Veeam. „Pak samozřejmě stačí jedna živelná pohroma nebo cílený útok a vše je ztraceno.“

Nemocnice jsou ve vztahu k útočníkům ve velmi nevýhodné pozici. „Při takovém incidentu jde doslova o životy. Proto bývá u cílených útoků i vyšší tlak na částku, kterou útočník za opětovně zpřístupnění dat požaduje. U ransomwaru je faktor tlaku na oběť pro útočníky obecně klíčový, protože v takovém případě jde o snadněji monetizovatelnou oběť,“ varuje Šafář.

Autor: Jan Kužník