Record disku a šifruje disk), Maktub (používající off-line crypter pro šifrování zdrojového kódu samotného ransomwaru), CryptXXX (patrně příbuzný ransomwaru Reveton, zajímavý je detekcí Anti-Sandboxů a schopností monitorovat pohyb myši), ZCryptor (někdy nazývaný kryptočerv – je totiž schopen se šířit na externí zařízení a jiné systémy na síti).

Různé kvalifikované odhady a průzkumy říkají, že momentálně bylo ve světě až neuvěřitelných 80 % firem či soukromých osob nějakým způsobem postiženo ransomwarem. Budoucnost ransomwaru bude samozřejmě v nových, sofistikovanějších variantách. Předpokládáno je zejména využití nových technik šíření, což způsobí infekci ještě většího množství počítačů. Pravděpodobný je také vývoj směrem k šifrování off-line, tj. ransomware nebude využívat komunikaci s infrastrukturou Command and Control za účelem tvorby, udržování a distribuce privátních a veřejných klíčů.

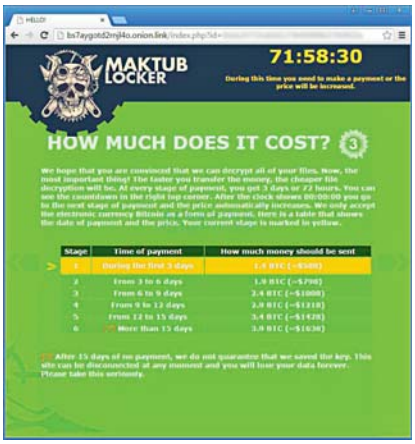
Proč je ransomware tak nebezpečný?

Nedávná studie z června 2016 zjistila, že třetina z 250 dotazovaných IT firem s více než 250 zaměstnanci v Británii střádá bitcoiny, aby je v případě potřeby mohla použít jako výkupné. Na tom je vidět, že firmy berou hrozbu ransomwaru velmi vážně a příliš nespoléhají na opatření, která by mohla infekci zabránit, případně ji odstranit a data odšifrovat. Obrovské nebezpečí hrozí zejména v případě použití ransomwaru proti tzv. kritické infrastruktuře (zdravotnictví, energetika, finance, doprava, apod.). V takových případech můžou kvůli několika bitcoinům vzniknout obrovské škody, včetně ztrát na lidských životech.

Obr. 1: Obrazovka CryptoLockeru – problém s placením

Ransomware jako obchodní model

Vydírání je velmi starý obchodní model. Jeho účinnost a úspěšnost na rozdíl od jiných útoků za účelem obohacení spočívá zejména v tom, že funguje téměř u každého. Při jiných typech útoků si útočník není předem jist, zda se mu útok vůbec vyplatí (např. v případech přímého odcizení cenných dat nebo zneužití bankovních přihlašovacích údajů). Od nakažení počítače k odcizení dat a jejich zpeněžení může vést dlouhá a trnitá cesta. Naproti tomu u vydírání stačí provést infekci a oběť vystrašit okamžitým znefunkčněním počítače a doprovodnými stresujícími efekty, jako jsou varovné obrazovky, odpočítávání času apod. Tím rapidně stoupá ochota oběti zaplatit výkupné. To platí jak pro soukromé osoby, tak pro firmy. Dalším faktorem úspěchu ransomwaru je obrovské množství potenciálních obětí, ačkoliv cílený ransomware (na konkrétní, důležitou osobu) může vydělat na výkupném o řády vyšší sumy.



Obr. 2: Informační obrazovka ransomwaru Maktub – čím později zaplatíte výkupné, tím dražší bude.

Není proto divu, že se už v loňském roce rozběhly služby Ransomware-as-a-Service (RaaS). Tyto obsahují uživatelsky jednoduché soupravy nástrojů, které se dají koupit na ilegálních internetových tržištích. Prodávají se typicky za několik tisíc dolarů (momentálně 1 až 3 tisíce), přičemž obchodní model je založen na tom, že kupující přenechává prodávajícímu 10 až 20 procent svých zisků. První a zřejmě nejvíce rozšířenou sadou typu RaaS je Tox. RaaS používají vysoce sofistikované metody plateb, kterým se říká míchání bitcoinů. Převáděním mikroobnosů tam a zpátky přes desítky tisíc bitcoinových peněženek je znemožněno jejich rychlé vyhledání.

Jak se chránit a jak postupovat v případě útoku?

Primárním způsobem ochrany před ransomwarem je prevence. Technická a organizační opatření, schopná zabránit infekci, by měla být samozřejmostí. Nejlepším způsobem snižování rizika je zálohování mimo dosah ransomwaru, tedy ne např. na nejbližším sdíleném síťovém disku. Ideální jsou způsoby zálohování, kdy proces, který kopíruje data, neběží na počítači, jehož data se zálohují. Tento proces totiž může již být kompromitován ransomwarem. Takový způsob zálohování je však náročný a nepraktický. Proto se doporučuje alespoň namátkově kontrolovat integritu dat na plných zálohách.

K placení výkupného existují různé filozofie, postoje a praktiky. Některé z nich jsou víc ideologické než praktické. Jako perličku je možné uvést informaci, že evropské firmy platí výkupné až dvakrát častěji než americké. Pro placení nebo neplacení výkupného neexistuje jednoznačná odpověď. V případě nakažení je velmi důležité rozmyslet si, zda se vyplatí platit. Místo paniky, která bývá běžnou reakcí, je třeba zvážit, jakou hodnotu znepřístupněná data skutečně mají. Bohužel kyberzločinci jsou obchodně zdatní a běžně nevyžadují vysoké částky, umí využít lidských emocí a vědí, kolik jsou lidé ochotni zaplatit třeba jen za obrázky z nezapomenutelné dovolené... Při zvažování placení nebo neplacení je tedy vždy důležité myslet na výsledek. Pokud jde o skutečně kritická data, je lepší zaplatit. V případě zaplacení kyberzločinci zatím vždy data uvolnili. Jsou si vědomi, že v případě nemožnosti dešifrování dat by jejich obchodní model přestal fungovat.

Na závěr je třeba zdůraznit, že všechna výše uvedené opatření a činnosti je nejlepší zvážit si předem, dokud není člověk nucen jednat pod stresem. Je dobré vědět, jaká data jsou kde uložena, jaká je jejich hodnota a jaká opatření jsou pro jejich zachování prováděna. Rovněž je důležité, aby bezpečnostní technický personál dokázal probíhající útok rozeznat a provést opatření zabraňující šíření útoku. To umožní v případě postižení rychle a správně se rozhodovat. ■

Milan Balážik

Autor článku působí jako Training Arena Manager ve společnosti CyberGym Europe.