Ransomware

Historie hrozby, aktuální vyhlídky a možnosti ochrany

Milan Balážik

Ransomware je aktuálně asi nejsledovanějším typem kybernetické hrozby. Vzhledem k laicky srozumitelnému, destruktivnímu a vyděračskému projevu totiž vzbuzuje velkou pozornost v médiích. Mohli bychom podlehnout zdání, že jde jen o další efektní téma, které zmizí, jakmile se objeví nový druh škodlivého softwaru. Bohužel to tak zatím nevypadá. Ransomware se šíří jako epidemie a je pravděpodobné, že jen tak rychle nevymizí. Všechny statistiky ukazují, že jeho rozšíření strmě stoupá a že se jedná o velmi vážné nebezpečí. Je třeba si uvědomit, že ransomware neohrožuje pouze koncové stanice, ale i firemní servery a kromě ztrát v případném zaplacení výkupného je ohrožen i běh organizace a její reputace.

Co je ransomware?

Obecně je ransomware škodlivým softwarem typu trojského koně, který zabraňuje legitimnímu přístupu k výpočetním prostředkům a jejich používání. Název ransomware je odvozen z anglických slov „ransom“ (výkupné) a „malware“ (škodlivý software). Laicky řečeno ransomware uzamkne počítač, blokuje přístup nebo šifruje data. Ransomware je dnes velmi rozšířený a efektivní škodlivý software. Kybernetičtí zločinci pomocí něho nekradou informace a nesnaží se zničit data, ale snaží se oběť přímo finančně vydírat.

Minulost ransomware

Prvním dokumentovaným případem ransomware se zdá být trojan AIDS z roku 1989, kterému říkali také PC Cyborg. Harvardský evoluční biolog Joseph L. Popp rozeslal kolem 20 tisíc disket nadepsaných jako „informace k AIDS“ účastníkům světové konference WHO o AIDS. Po devadesátém startu začal trojan skrývat adresáře a zašifroval soubory. Za dešifrování souborů byla požadována platba 189 dolarů na poštovní účet v Panamě. Dr. Popp byl chycen, ale povedlo se mu předstírat psychickou nemoc, takže nebyl nikdy souzen.

První byly blokátory

Historii ransomwaru je možné rozdělit na dobu před šifrováním a po něm. Blokátory byly předchůdci modernějších šifrátorů. Tento typ malwaru jednoduše blokoval start operačního systému nebo některých aplikací (např. prohlížeče), dokud uživatel nezaplatil „mírný poplatek“. Platba se často prováděla přes placenou SMS nebo převodem na účet či nějaký druh elektronické peněženky. Převody na účty (i některé jiné platební metody, jako např. PayPal) přestaly být efektivní, jakmile policie ve spolupráci s bankami provedla změny v platebních systémech a byly zavedeny lepší korelační metody plateb.

Nastupují šifrátory

Před několika léty se vše změnilo s nástupem tzv. kryptoměn. Mezi kyberzločinci (a zločinci obecně) se rychle rozšířila obliba bitcoinů. Tato virtuální digitální kryptoměna je totiž velmi likvidní (umožňuje převod na reálnou měnu) a ve spolupráci s anonymizační sítí Tor zároveň ze své podstaty jen těžko umožňuje regulaci nebo zpětné dohledávání plateb, čímž zaručuje dostatečnou anonymitu.

Zároveň se také změnil přístup ke způsobu blokování počítačů, když zločinci začali šifrovat soubory na počítači nebo i celé oddíly disků oběti. Opětovnou instalací operačního systému tedy již nebylo možné malware odstranit – uživatelé by tak přišli o svá data. Za dešifrování dat (pomocí zaslaného klíče nebo i přímo nástroje pro dešifrování) mohli kyberzločinci náhle začít žádat enormní sumy – stovky dolarů od soukromých osob až po statisíce od firem.

Současnost a budoucnost ransomwaru

Starý trojan AIDS používal symetrické šifrování a klíč byl uložen v jeho kódu. Přibližně v roce 2006 začali kyberzločinci používat efektivnější asymetrické šifrování RSA. Od roku 2011 se ransomware opravdu „rozjel“. V posledním čtvrtletí 2011 bylo objeveno 60 tisíc nových variant ransomwaru, ve 3. čtvrtletí 2012 jich bylo už 200 tisíc. Konec roku 2015 byl v rozšíření ransomwaru zlomový, když počet nových variant přesáhl hranici 700 tisíc.

Nejslavnější ransomware Cryptolocker se poprvé objevil v září 2013 a postupně přišel s mnohými klony. CryptoLocker 2.0 v prosinci 2013, pak CryptoDefense s vylepšenou verzí CryptoWall.

V roce 2014 přišel CTB-Locker, pak první šifrující ransomware pro Android. První ransomware, který uměl resetovat PIN v mobilech s Androidem, přišel v roce 2015 pod jménem LockerPin. Jeho odblokování pro zajímavost stálo 500 dolarů. Výčet nejrozšířenějších ransomwarů by nebyl úplný bez TeslaCrypt, LowLevel04 a Chimera, který vyhrožoval publikováním citlivých dat uživatele.

Z nejzajímavějších ransomwarů tohoto roku připomeňme Ransom32 (první ransomware v JavaScriptu), 7ev3n (zatím nejdražší výkupné 13 Bitcoinů), LOcky (tzv. nemocniční ransomware, jehož zdrojový kód byl publikován), SamSam (infikuje zranitelné JBoss servery a napřímo komunikuje s obětí), KeRanger (první oficiální ransomware pro Mac OSX, šířený přes bittorrentového klienta a podepsaný vývojářským certifikátem), Petya (šířený přes DropBox, přepisuje Master Boot