ALISON

Evolúcia malvéru: od oštepu k dynamitu

- **Emotet vstáva z popola**
- **Prečo veríme mailom**
- **Ciele sú veľké, citlivé a drahé**
- **Nie sme úplne bezbranní**

Malvér Emotet sa šíri internetom od roku 2014 a stihol už napáchať škody za milióny eur. Emotet patrí do skupiny trójskych koní, ktorá sa vyznačuje vysokou mierou automatizácie, modulárnosti a mimoriadnou prispôsobivosťou. Možno povedať, že ide o inteligentný malvér. Mozgom je riadiaci server, z ktorého si Emotet sťahuje rôzne funkčné moduly. Malvér sa zameriava na veľké spoločnosti a verejné organizácie. Dobrá správa je, že sa organizácie proti takémuto kybernetickému útoku dokážu brániť.

Veľmi obvyklé nebezpečenstvo na internete: útočníci zachytávajú dôverné informácie používateľov, napríklad používateľské mená a heslá pre firemné účty alebo online bankovníctvo. Ide o „phishing“ – používateľ dostáva falošné e-maily, ktoré zdanlivo prichádzajú od dôveryhodných odosielateľov a navádzajú príjemcu, aby zadal svoje prihlasovacie údaje na webových stránkach, predstierajúcich pravosť. Autori phishingových e-mailov lovia cenné prihlasovacie údaje a používajú ich na svoje nekalé ciele.

Povedomie medzi spoločnosťami a používateľmi však narastá a takéto, často štylistický chybné a strojovo pôsobiace e-maily oklamú čoraz menší počet príjemcov. Ak zostaneme v metaforickom svete rybolovu – sieť má také veľké diery, že väčšina rýb z nej unikne.

V sieti útočníka: prihlasovacie údaje a heslá

Útočníci nespia na vavrínoch a phishing sa vyvinul do tzv. lovu oštepom (spear phishing). Phishingové maily sa pri tejto metóde už neposielajú hromadne, ale sú zacielené na konkrétnych, dôkladne vybraných príjemcov. Ich obsah vychádza z prieskumu a je relevantnejší pre príjemcu než pri bežnom phishingu. Maily sa pri spear phishingu týkajú témy, ktorou sa príjemca práve aktívne zaoberá. Ich cieľom je presvedčiť ho, že dostal legitímny, pravý e-mail napríklad preto, že vedome či podvedome očakáva správu na danú tému.

Takýto prístup prirodzene vedie k tomu, že inštrukciami zaslanými vo falošnom maile sa riadi vyšší počet príjemcov než pri bežných phishingových mailoch. Nevýhodou je vyššia náročnosť na strane útočníka, ktorý musí pred rozbehnutím úspešného útoku zhromaždiť veľké množstvo informácií o cieľovej osobe buď prostredníctvom sociálneho inžinierstva, alebo infiltráciou spriazneného človeka do spoločnosti. Spear phishing sa v minulosti využíval najmä tam, kde cieľová osoba bola taká cenná, že aj vysoká vstupná investícia útočníkov priniesla dobrú návratnosť. Útočníci často pracovali priamo pre vlády alebo štátne organizácie.

Evolúcia malvéru: od spear phishingu (lovu oštepom) k lovu dynamitom

Emotet predstavuje ďalšiu fázu vo vývoji phishingu: dôsledná personalizácia, ktorou sa vyznačoval spear phishing, je teraz automatizovaná. Emotet na tento účel používa adresár a mailové kontakty obete, vďaka čomu dokáže rekonštruovať jej sieť sociálnych kontaktov. Okrem toho malvér automaticky čerpá z obsahu

ostatných, skutočných mailových konverzácií obete. Vďaka tomu Emotet môže posielať phishingové maily, ktoré takmer dokonale zapadnú do kontextu reálnych pracovných vzťahov a mailových konverzácií obete – a navyše to robí vo veľkom rozsahu. Pre takýto prístup sa vžilo označenie „dynamite phishing“ (lov dynamitom). Dokáže totiž pôsobiť vo veľkej mierke a „uloviť“ enormne vysoké percento obetí.

Emotet: infekcia pomocou makier

Počiatočná infekcia vírusom Emotet sa zvyčajne začína inteligentne sfalšovaným, zdanlivo dôveryhodným e-mailom, ktorý obsahuje ako prílohu dokument balíka Office. Keď používateľ dokument otvorí a na výzvu aktivuje makrá, infekcia naberie obrátky. Len čo Emotet prenikne do svojho cieľa, spojí sa so svojím riadiacim serverom; ten na diaľku určí, ako sa malvér bude ďalej správať. Toto správanie sa môže v závislosti od prijatých pokynov značne líšiť.

Jednou z hlavných funkcií malvéru Emotet je vlastné šírenie zasielaním phishingových e-mailov z kontaktov získaných v infikovanom zariadení. Emotet používa na čítanie e-mailových kontaktov obete rozhranie Windows MAPI (Messaging Application Programming Interface).

Načítanie modulov, reprodukcia ako červ

Len čo sa Emotet dostane do pracovného počítača, môže načítať ďalšie moduly do pracovnej pamäte bez toho, aby sa ukladali ako súbory. Nazýva sa preto aj „fileless malware“ (malvér bez súborov), čo značne sťažuje jeho identifikáciu.

Emotet zároveň funguje ako červ a dokáže sa šíriť z jedného infikovaného počítača na ďalšie v rovnakej sieti bez aktívneho zásahu ich používateľov. Využíva na to protokol SMB (Server Message Block) spoločnosti Microsoft a číta prihlasovacie tokeny z miestneho úložiska systému Windows. Tiež vykonáva útoky hrubou silou na používateľské účty pomocou zoznamov hesiel.

Na najvyššej úrovni infekcie Emotetom útočníci manuálne preskúmajú infikovaný systém a vyhľadávajú obzvlášť dôležité údaje, ktoré následne napríklad odstránia a požadujú výkupné za ich vrátenie. Podobne funguje vydieranie: útočníci objavené citlivé informácie zašifrujú priamo na počítači obete a stiahnu si ich kópiu. Ak obeť nezaplatí požadované výkupné, vydierači zverejnia údaje na internete.

Za určitých okolností trvá odhalenie infekcie systému aj celé mesiace. Objavili sa prípady, v ktorých Emotet a jeho moduly fungovali v systéme viac než šesť mesiacov, prípadne až 18 mesiacov. Celý čas menili nepozorovane dáta. Zákerné je, že údaje zo systému nezmiznú, len sa nebadane mení ich obsah, takže zálohy sú zbytočné. Pozmenené dáta sa premietnu aj do zálohy.

Rozhodujúca je prevencia

Existuje však celý rad opatrení, ktoré sľubujú úspech v boji proti tomuto typu útoku. Rovnako ako pri všetkých phishingových útokoch aj pri prevencii infekcií Emotetom má veľký význam vzdelávanie zamestnancov spoločnosti. Ich povedomie je vhodné zvyšovať koordinovanými opatreniami, napr. internými e-mailmi a informačnými výveskami. Potrebné odborné znalosti, napr. v oblasti e-mailovej bezpečnosti, môžu zasa zamestnancom poskytnúť špecializované školenia. Z toľko diskutovaného „bezpečnostného rizika ľudského faktora“ sa tak stane ľudský faktor bezpečnosti, ktorý aktívne pomáha brániť sa proti kybernetickým útokom, ako je Emotet.

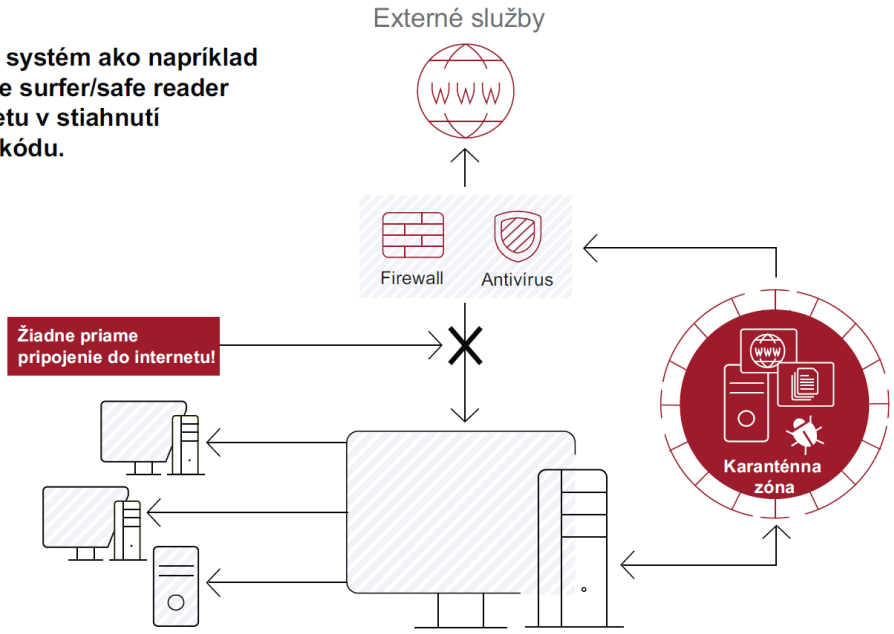
Ak sa má IT infraštruktúra technicky vyzbrojiť proti malvéru Emotet, je potrebné najskôr zistiť mieru jej zabezpečenia. Počiatočné zhodnotenie situácie možno vykonať rýchlym auditom informačnej bezpečnosti. Vykonávajú ho odborníci na bezpečnosť IT a vychádza okrem iného z koncepcie informačnej bezpečnosti „IT-Grundschutz“ Nemeckého spolkového úradu pre informačnú bezpečnosť (BSI). Odborníci vypracujú správu z auditu s manažérskym zhrnutím a znázornením zistených nedostatkov. Tá sa stáva základom pre ďalšie opatrenia.

Z technického pohľadu je počiatočným opatrením test prieniku. Pri ňom odborníci na IT bezpečnosť simulujú prienik malvéru a snažia sa nájsť odpovede na nasledovné otázky: Akú účinnosť majú nasadené ochranné opatrenia? Existujú slabé stránky, ktoré treba urýchlene odstrániť? Sú v sieti oprávnenia, ktoré by mohol útočník zneužiť? Počas testu odborníci hľadajú aj známky infekcie, ktorá systém postihla, no nebola zatiaľ odhalená.

Ak organizácia chce zabrániť šíreniu malvéru Emotet, mala by v prvom rade preveriť správu oprávnení – používatelia by mali mať len takú úroveň oprávnení, aká postačuje na vykonávanie ich povinností. Treba sa vyvarovať zavádzaniu všeobecných administrátorských oprávnení.

ALISON

Karanténny systém ako napríklad secunet safe surfer/safe reader bráni Emotetu v stiahnutí škodlivého kódu.



Odhaľovanie Emotetu a boj proti nemu

Tradičné strážne (gateway) a analytické systémy, ako sú firewally a antivírusový softvér, nemajú proti útokom Emotetu šancu. Namiesto toho jestvuje dopyt po opatreniach, ktoré idú hlbšie – ako napríklad karanténny systém secunet safe surfer. Ten zabráni, aby Emotet získal prístup k počítaču a k sieti, do ktorej je počítač pripojený, len na základe bezmyšlienkovitého kliknutia na infikovaný odkaz. Pri použití technológie secunet safe surfer sa napadnutá webová stránka neotvára v bežnom pracovnom prostredí používateľa, ale v izolovanom prehliadači na karanténnom systéme, ktorý používateľ ovláda „na diaľku“. Emotet nemôže spôsobiť žiadne škody, pretože sa nedostane mimo karanténneho systému. Doplnková funkcia „bezpečná čítačka“ navyše účinne blokuje infikovanú prílohu e-mailu, a ak používateľ otvorí napadnutú prílohu pomocou bezpečnej čítačky, Emotet nedokáže načítať škodlivý kód, pretože nemá priame pripojenie do internetu.

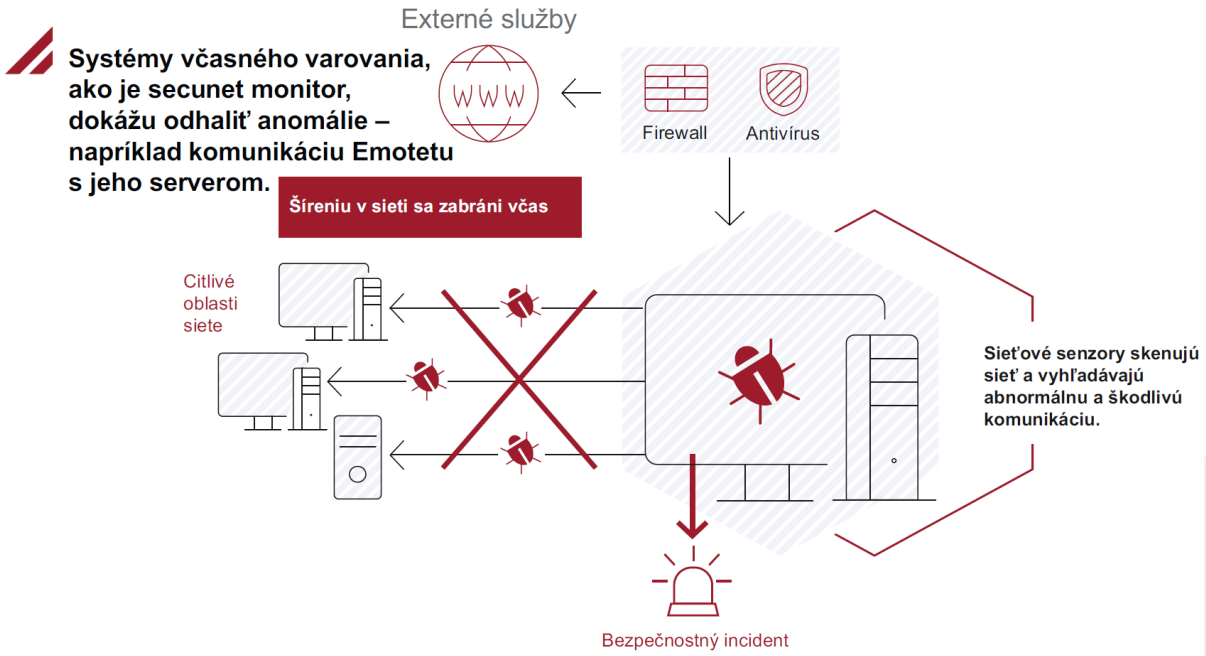
Prevádzkovatelia IT infraštruktúry by navyše mali byť vždy informovaní o dianí v ich sieti a o tom, či nevykazuje príznaky napadnutia malvérom. Systémy včasného varovania nepretržite vyhodnocujú komunikáciu v sieti a hľadajú anomálie ako podozrivé dátové toky. Dokážu napríklad odhaliť, kedy Emotet komunikuje so svojím riadiacim serverom a nahráva malvér. Po rozpoznaní infekcie možno zabrániť jej ďalšiemu šíreniu v sieti.

Verejné orgány a spoločnosti, ktoré používajú architektúru SINA (Secure Inter-Network Architecture) na digitálne spracovanie citlivých alebo dokonca utajovaných údajov, majú v boji proti Emotetu ďalšiu výhodu. Pracovná stanica SINA, ktorá v systéme funguje ako klient, vytvára pomocou virtualizačnej technológie množstvo hosťovských systémov, ktoré sú vzájomne dôkladne izolované. Tieto hosťovské systémy dokážu fungovať súčasne, aj keď majú pridelené rôzne úrovne zabezpečenia. Používatelia tak môžu napríklad pracovať s dôvernými údajmi a zároveň surfovať po internete. Malvér nedokáže prekonať bariéry medzi hosťovskými systémami a jeho pokusy pripojiť sa k sieti vychádzajú naprázdno.

Zabezpečenie pomocou SINA spočíva v množstve ďalších vzájomne prepojených bezpečnostných opatrení: siete SINA sú postavené z pripojení VPN zabezpečených pomocou IPsec a podľa požiadaviek ponúkajú silné až veľmi silné šifrovanie. Rozhrania pracovných staníc SINA sú nastavené tak, aby zabránili prenikaniu škodlivého softvéru do systému touto cestou. Šifrovanie pevného disku a dvojstupňové overenie zabezpečujú, aby sa údaje spoločnosti alebo úradu nedostali do nesprávnych rúk.

Návrh ochranných opatrení

Vývoj bezpečnostných opatrení IT našťastie drží krok s novými typmi útokov. Verejné orgány a súkromné spoločnosti tak nie sú proti Emotetu úplne bezbranné. Úspech v boji proti tomuto typu útoku majú zvyčajne skôr opatrenia, ktoré pôsobia na hlbšej úrovni. Nastavené opatrenia musia, ako obvykle, zohľadňovať jestvujúce okolnosti a požiadavky na ochranu príslušnej siete.



Certifikovaným partnerom pre produkty secunet na Slovensku je spoločnosť ALISON Slovakia. Krypto produkty SINA sú certifikované na ochranu utajovaných skutočností EÚ aj NATO. V podmienkach Slovenskej republiky pravidlá pre používanie a prevádzku vyplývajú z legislatívy Slovenskej republiky a požiadaviek národných autorít pre túto oblasť.