Malware

Více informací na Sec.eff.org
Projekt zpracovala organizace Electronic Frontier Foundation

Škodlivý software, zkráceně malware, je jakýkoli program, který je navržený tak, aby způsoboval nevyžádané akce na vašem zařízení

Příklady malwarů:

- Počítačové viry
- Programy pro krádež hesel
- Programy, které vás potají nahrávají
- Programy, které skrytě mažou vaše data

MALWARE NA ZÁKLADĚ PHISHINGU

Phishingem nazýváme situaci, kdy vám útočník zašle zprávu, e-mail nebo odkaz, který vypadá neškodně, ale ve skutečnosti je škodlivý. Phishing zneužívá identitu někoho, koho znáte, nebo platformu, které důvěřujete (např. bankovnictví).

Poznámka: Ne každý phishing obsahuje škodlivý malware. Cílem útočníka může být také ukrást vaše heslo k nějaké digitální službě. Toho se snaží dosáhnout tak, že se vydává za danou webovou stránku, a to bez instalace malwaru do vašeho zařízení.

NEJČASTĚJŠÍ ZPŮSOBY, JAK SE MALWARE DOSTANE DO VAŠEHO ZAŘÍZENÍ

Otevřením škodlivého souboru či přílohy	Škodlivé přílohy jsou obvykle obsaženy v phishingových zprávách.
Kliknutím na škodlivý odkaz	Škodlivý odkaz je také často obsahem phishingových zpráv.
Stažením nelicencovaných softwarů	Software, u kterého nemůžete provést bezpečnostní aktualizaci může být rizikový (to se netýká například softwarů stažených z obchodů s aplikacemi, jako je App Store od Apple nebo Google Play).

Návštěvou pochybných webů	Webové stránky jsou někdy zneužity a obsahují škodlivý obsah.

TYPY MALWARŮ

Adware	Reklamy jsou všude Tento škodlivý software se obvykle uživateli internetu snaží vnutit reklamu na základě velkého množství vyskakovacích oken či jinými metodami. Některé adwary mapují informace o uživateli nebo kradou jejich osobní informace. Adwary, stejně jako jiné malwary, mohou být součástí jiných softwarů, které jsou stažené na pochybných zdrojích, jako například z neoficiálních obchodů s aplikacemi nebo odjinud než od softwarových vývojářů.
Stalkerware	Když vás vaše zařízení pomáhá sledovat Stalkware dává útočníkovi plnou a nepozorovanou kontrolu nad zařízením. Stalkware se do vašeho zařízení může dostat, když má někdo, například člen rodiny nebo partner („Můžeš mi na chvíli dát svůj telefon?“) fyzický přístup k vašemu zařízení a nainstaluje vám ho tam. Případně si ho uživatel může stáhnout sám, když je donucen ke stažení škodlivé aplikace.
Trojský Kůň	Dárek, který je útokem v převleku Trojský kůň se po stažení jeví jako běžná legitimní aplikace, nicméně na pozadí provádí drobné zlomyslné úkony. Je často nalezen v načerno pořízeném či staženém softwaru nebo falešném antiviru.
Ransomware	Software, který z vás udělá rukojmí

	Po stažení tento škodlivý software drží data firem nebo lidí jako rukojmí. V poslední dekádě je velmi populární, stal se z něj miliardový byznys pro útočníky z celého světa.
APT útok	Pokročila trvalá hrozba (tzv. APT útok) APT útok je malware od útočníka, který má velmi sofistikované schopnosti a zdroje pro dosažení jeho cílů: narušení vašeho systému. APT útoky jsou hojně využívány také příslušníky státních složek k udržení dlouhodobého přístupu k systému, na který se zaměřují.

5 RAD, JAK SE BRÁNIT PROTI MALWARU

RADA #1: AKTUALIZUJTE SVŮJ SOFTWARE

(A PRAVIDELNĚ KONTROLUJTE, ZDA VYUŽÍVATE LICENCOVANÝ SOFTWARE)

Většina malwarů využívá známé zranitelnosti. Softwarové společnosti často opraví uživatelům zranitelnosti skrze aktualizace samotného softwaru.

Softwarové aktualizace jsou proto kritické pro uživatelskou bezpečnost, protože představují nejlepší způsob, jak udržet aktuální informace o známých zranitelnostech, které mohou útočníci využít.

*Pokud si nejste jisti tím, jak využít licencovaný software, zeptejte se svého experta na kybernetickou bezpečnost pro dostupné rady a zdroje.

RADA #2: ZÁLOHY PRO BUDOUCNOST

Zálohujte svá data dnes a vaše budoucí já vám poděkuje. Pokud ztratíte své zařízení (ať už z důvodu zneužití malwarem, krádeží nebo zařízení prostě přestane fungovat) vše bude ztraceno, nicméně vaše soubory budou uloženy v záloze. Zálohy chraňte silným heslem a šifrováním.

RADA #3: PŘED KLIKNUTÍM SE ZAMYSLETE

Sdílení odkazů a souborů je běžná praxe, buďte ale opatrní při práci se sdílením odkazů. Než kliknete, zastate se a zamyslete se – není to podezřelé?

POZOR NA … ZKRÁCENÉ A USEKLÉ LINKY

Odkazy a e-maily mohou vypadat kratší, pokud je zobrazíte na telefonu oproti těm na počítači. Zkracovače URL adres jako bit.ly mohou odkazovat na škodlivé stránky.

Tip: zkuste službu jako https://unshorten.it – ukáže vám plnou URL adresu!

IMITACE: NEJLEPŠÍ FORMA PODVODU

Překlepy, podobné znaky a kopie grafiky vás mohou velmi často oklamat. Ověřte si, že skutečně používáte danou službu.

Tip: Udělejte si záložku ověřené služby: toto může být jednodušší pro váš počítač si uložit skutečnou adresu.

Tip: Uložte si správný link do správce hesel. Správce hesel si pamatuje konkrétní stránky a předvyplní vaše hesla.

Pozor na podvod typu sociální inženýrství, jako zprávy od někoho, kdo předstírá že je váš kamarád.

Tip: ozvěte se kamarádovi přes jiný komunikační kanál a ověřte si, že je to opravdu ta správná osoba.

KLIKNUTÍ OMYLEM

Když zkoumáte link, pozor ať na něj náhodou nekliknete.

Tip: pokud používáte myš, najeďte na odkaz kurzorem, aby se zobrazila jeho celá adresa.

RADA #4: POZOR NA FYZICKÝ PŘÍSTUP

Občas může být útočníkem někdo, koho znáte nebo kdo má přístup k vašemu zařízení, když nedáváte pozor. Využití plného šifrování disku a silných hesel může zamezit nedovolenému přístupu. Buďte opatrní, když odemčené zařízení někomu půjčujete. Pro více informací se podívejte na ssd.eff.org.

RADA #5: POUŽÍVEJTE ANTIVIRUS

Ne všechny antiviry jsou si rovny, některý software prezentovaný jako antivirus může být převlečený malware. Možná můžete využít antivirus ve vašem operačním systémů. Pokud preferujete externí antivirus, zkontrolujte:

- Nezávislé recenze softwaru
- Zda má výrobce aktualizovaný seznam malware* a útoků kterých se obáváte

*Publikování výzkumu hrozeb může znamenat, že výrobce má aktivní tým pro obranu proti tomuto typu malware.

OBÁVÁM SE, ŽE MÁM MALWARE. CO MÁM DĚLAT?

Děje se s vaším zařízením něco divného? Jde o konkrétní účet (sociální sítě, atp). Nebo celé zařízení? Pokud to vypadá na malware, buďte opatrní jak s infikovaným zařízením zacházíte. Následně kontaktujte odborníka, aby vám pomohl, případně využijte jiné zařízení.

*Oddělené zařízení, které není připojeno k zařízení napadaného malwarem. Např. počítač v knihovně nebo kamarádův telefon.

KONTAKTUJTE DŮVĚRYHODNÉHO TECHNIKA

Dělejte si záznamy, např. podezřelé zprávy v jejich původní podobě (např. e-mail i s metadaty, nikoliv pouze jeho screenshot). Přidejte detaily: datum, čas, popis. Pošlete informace důvěryhodnému technikovi.

VYHODNOŤTE ŠKODY

Jaké citlivé informace mohly být zneužity? Měli byste si změnit hesla nebo vytvořit nové účty? Naplánujte další kroky, vyhodnoťte rizika (neboli modelování hrozeb).

Proč jsou metadata důležitá?

Poslední aktualizace: 11. března 2019

Za metadata je často považováno všechno, krom obsahu dané komunikace. Pro přirovnání si můžete představit papírovou obálku. Ta obsahuje informace o odesílateli, příjemci a místě doručení, a stejně tak fungují i metadata. Jde o informaci o digitální komunikaci, které jste součástí. Zde jsou některé příklady metadat:

- předmět vašich e-mailů
- délka vašich konverzací
- časové okno ve kterém konverzace proběhla
- vaše lokace odkud komunikujete (a také s kým)

Zákony řady zemí, včetně USA, historicky nevěnují tolik pozornost ochraně soukromí v případě metadat, jako v případě obsahu komunikace. V mnoha zemích může policie snadno získat záznamy o tom, s kým jste v posledním měsíci volali, ale je pro ně těžší zajistit odposlech vaší telefonní komunikace, aby zjistila, o čem jste mluvili.

Ti, kdo sbírají metadata, nebo k nim vyžadují přístup, jako vlády nebo telekomunikační firmy, tvrdí, že zveřejnění (a sběr) metadat není žádný velký problém. Bohužel ale nemají pravdu. Jen malý vzorek metadat může poskytnout intimní vhled do osobního života. Podívejte se, jak odhalená metadata mohou být pro vlády nebo firmy, které je sbírají, užitečná:

- Vědí, že jste ve 2:24 ráno volali na erotickou linku a mluvili 18 minut. Ale neví, o čem jste mluvili.

- Vědí, že jste zavolali na linku pro prevenci sebevražd z mostu Golden Gate. Ale téma hovoru zůstává utajeno.
- Vědí, že jste dostali e-mail ohledně HIV testování, pak zavolali svému doktorovi a pak navštívili stránku podpůrné skupiny pro HIV v tu samou hodinu. Ale neví, co bylo v e-mailu nebo o čem jste mluvili do telefonu.
- Vědí, že jste dostali e-mail od aktivistické skupiny pro digitální práva s předmětem “Stop Americkým radarům v Česku” a hned poté zavolali vašemu zastupiteli. Ale obsah obou komunikací zůstává zabezpečený před vládním narušením.
- Vědí, že jste volali gynekologovi, mluvili spolu půl hodiny a pak zavolali na číslo místní potratové kliniky.

Může být těžké ochránit vaše metadata před sběrem, protože třetí strany často potřebují metadata k tomu, aby úspěšně propojili vaši komunikaci. Tak jako pošťák potřebuje přečíst adresu na obálce, aby dopis doručil, digitální komunikace zase musí být většinou označena zdrojem a destinací. Mobilní operátoři potřebují vědět, kde zhruba se váš telefon nachází, aby na něj mohli připojit příchozí hovory.

Služby jako Tor se snaží omezit objem metadat, která vznikají při online komunikaci. Dokud nebudou aktualizovány zákony, aby šly lépe aplikovat na metadata, a nástroje, které metadata minimalizují, nebudou rozšířené, to nejlepší, co můžete udělat, je si uvědomit, jaká metadata můžete při komunikaci šířit, kdo k nim může mít přístup a jak mohou být použita.

Tvůj bezpečnostní plán

Poslední úprava: 2. února 2021

Snažit se neustále ochraňovat svá data před všemi je nepraktické a často neefektivní. Nemějte ale obavy, bezpečnost je proces a pokud se zamyslíte nad vašimi potřebami, můžete si vytvořit bezpečnostní plán, který pro vás bude dávat smysl. Bezpečnost není jen o nástrojích, které používáte nebo o softwarech, které si stáhnete. Nejdříve je potřeba pochopit rizika, kterým čelíte a způsobům, jak se konkrétně těmto hrozbám bránit.

V počítačové bezpečnosti je hrozba potenciální událost, která může narušit vaši snahu chránit osobní data. Když si ujasníte, co a před kým potřebujete chránit, můžete tyto hrozby zvrátit. Jde o proces bezpečnostního plánování, kterému se často říká „modelování hrozeb“.

Tento průvodce vás naučí, jak vytvořit bezpečnostní plán pro ochranu svých digitálních dat a jak se rozhodnout, která řešení jsou pro vás nejvhodnější.

Jak takový bezpečnostní plán vypadá? Dejme tomu, že potřebujete zabezpečit svůj domov a majetek. V takovém případě si můžete položit následující otázky:

Co z toho, co mám doma, potřebuji ochránit?

Předmětem ochrany mohou být šperky, elektronika, účetní dokumenty, pasy nebo třeba fotografie

Před kým potřebuji předměty zabezpečit?

Útočníka může představovat zloděj, ale i váš spolubydlící či návštěva

Jak moc je pravděpodobné, že se někdo pokusí narušit vaše zabezpečení?

Došlo v mém sousedství v minulosti k nějakým krádežím? Jak důvěryhodní jsou mí spolubydlící či hosté? Jaké jsou možnosti mých protivníků? Jaká rizika bych neměl přehlédnout?

Jaké negativní následky může mít vaše nedostatečná ochrana?

Mám doma něco nepostradatelného? Mám dostatek peněz a času, abych to případně nahradil? Mám pojištění proti krádežím?

Co je možné udělat, aby bylo zabráněno daným následkům?

Je možné si pořídit trezor pro citlivé dokumenty? Mohu si dovolit zaplatit za kvalitní zámek? Mám dostatek času zajít do banky a zařídit si tam bezpečnostní schránku, do které si uložím své cennosti?

Když se na tyto otázky zeptáte, pomůže vám to ujasnit, jaká opatření zvolit. Pokud je váš majetek cenný, ale je malá pravděpodobnost, že by se ho někdo snažil získat, pak například nebudete chtít investovat tolik peněz do bezpečnostního zámku. V případě, že je velká šance se k vám vloupat, je lepší si pořídit nejlepší zámek na trhu a ještě k tomu zvážit pořízení bezpečnostního systému.

Vytvoření bezpečnostního plánu vám pomůže pochopit hrozby které jsou jedinečné pro vás a pro ochranu vašich zdrojů, schopnosti vašich útočníků a stejně tak i rizika, kterým čelíte.

Jak si nastavit bezpečnostní plán?

Bezpečnostní plánování vám pomůže identifikovat, co by se mohlo stát s věcmi, na kterých vám záleží a stanovit si, před kým je třeba se chránit. Když tvoříte bezpečnostní plán, zodpovězte si těchto pět otázek:

- Jaké věci chci ochránit?
- Před kým chci věci ochránit?
- Jak zlé budou následky selhání?
- Jak je pravděpodobné, že tyto věci bude potřeba ochránit?
- Kolika problémům mám ochotu čelit, aby nedošlo k žádným následkům?

Pojďme se podívat blíže na tyto otázky.

Co chci ochránit?

“Předmět ochrany” je něco, čeho si vážíte a chcete ochránit. V kontextu digitální bezpečnosti, je zpravidla předmětem ochrany nějaká forma informace. Např. vaše e-maily, seznam kontaktů, zprávy, lokalita, soubory, atp. Vaše zařízení může být také předmětem ochrany společně s vaší identitou.

Udělejte si seznam předmětů ochrany: data, která máte, kde jsou uložena, kdo k nim má přístup a jakým způsobem můžete zamezit takovému přístupu v případě potřeby.

Před kým je chci chránit?

Abyste si odpověděli na tuto otázku, je důležité identifikovat, kdo může cílit na vás či vaše informace. Osoba nebo subjekt která nese hrozbu vašim zdrojům je útočník. Příklady potenciálních útočníků jsou váš šéf, ex partner, obchodní konkurence, vláda nebo hacker na veřejné síti.

Udělejte si seznam útočníků, kteří by mohli chtít získat vaše předměty ochrany. To mohou být jednotlivci, vládní úřady nebo korporace.

V závislosti na tom, kdo jsou vaši útočníci, můžete za některých okolností seznam zničit poté, co jste dokončili vaše bezpečnostní plánování.

Jak zlé jsou důsledky selhání, pokud nastane?

Je mnoho způsobu jak může útočník získat přístup k vašim datům. Např. může číst vaši soukromou komunikaci nebo smazat či zničit vaše data.

Motivy útočníků se velmi liší a stejně tak i jejich taktiky. Vláda která se snaží zamezit sdílení videa obsahujícího policejní násilí může vyžadovat jeho smazání nebo snížit jeho dostupnost. Oproti tomu, politický oponent může usilovat o přístup k tajnému obsahu bez vašeho vědomí.

Bezpečnostní plánování zahrnuje porozumění tomu, jak velké následky může mít neoprávněný přístup k vašim zdrojům. Abyste toto zhodnotili, potřebujete zvážit schopnosti útočníka. Např. váš mobilní operátor má přístup k vašemu výpisu hovorů. Hacker na veřejné WiFi může číst vaši nešifrovanou komunikaci. Vaše vláda může mít silnější nástroje.

Napište si, co by váš útočník mohl chtít udělat, aby získal přístup k vašim datům.

Jak je pravděpodobné, že to budu muset chránit?

Riziko je pravděpodobnost, že se určitá hrozba vůči určitému předmětu ochrany skutečně stane. Zatímco váš mobilní operátor má přístup k veškerým vašim soukromým datům, riziko, že vaše data zveřejní, aby vás poškodil, je nízké.

Je důležité rozlišit mezitím, co by se mohlo stát a pravděpodobností, že k domu dojde. Např. existuje hrozba, že se vaše budova zřítí je mnohem větší v San Francisku (kde jsou běžné zemětřesení) než ve Stockholmu (kde nebývají).

Hodnocení rizik je osobní a subjektivní proces. Hodně lidí považuje některé hrozby za nepřijatelné nezávisle na jejich pravděpodobnosti, už jen proto, že pouhá přítomnost hrozby, nehledě na pravděpodobnost, nestojí za její cenu. V jiných případech lidé nedbají na vysoká rizika, protože je nevidí jako problém.

Sepište si, které hrozby budete brát vážně a které jsou příliš vzácné nebo neškodné (nebo jim lze jen těžko předejít), abyste se jimi zabývali.

Jak moc toho chci udělat abychom předešli potenciálním následkům?

Neexistuje žádná perfektní verze zabezpečení. Ne každý má stejné priority, zájmy nebo přístup ke zdrojům. Vaše vyhodnocení rizik vám umožní naplánovat tu pravou strategii pro vás, vyvážit pohodlnost, náklady a soukromí.

Např. advokát zastupující klienta v případu národní bezpečnosti může nastavit přísnější opatření jako používání šifrovaného e-mailu než člen rodiny sdílející srandovní videa koček.

Napište si jaké možnosti máte k dispozici pro snížení unikátních hrozeb. Poznamenejte si případné finanční nebo sociální omezení.

Bezpečnostní plánování jako pravidelná aktivita

Počítejte s tím, že bezpečnostní plán se může měnit podle situace. Je tedy dobré jej pravidelně revidovat.

Vytvořte si vlastní bezpečnostní plán pro vaši konkrétní situaci. Pak si v kalendáři poznačte datum někdy v budoucnosti a až přijde, vraťte se ke svému plánu a zrevidujte, jestli pořád odpovídá aktuální situaci.

Credit for translation and localization goes to Journalist Security Fellowship fellows in partnership with Localization Lab.

In partnership with

LOCALIZATION LAB