Co je počítačový virus + Druhy virů | ESET

Počítačový vir je škodlivý program, který se sám šíří bez vědomí uživatele kopírováním do jiného spustitelného programu nebo dokumentu. Účelem viru je infikovat zranitelné systémy, získat kontrolu nad zařízením a ukrást citlivá data uživatelů. Hackeři vytvářejí počítačové viry s úmyslem oklamat uživatele.

Má vlastnosti živého organismu – dovede se množit, dovede cestovat, je inteligentní – dovede se učit. Nepotřebuje však potravu, nemusí spát.

Podle statistik společnosti ESET je každý den detekováno na 300 tisíc nových variant škodlivých kódů, které označujeme jako malware.

Virus Brain (1986) = první virus

Snad úplně první počítačovou hrozbou, se kterou se uživatelé setkali, byl virus Brain. V roce 1986 jej naprogramovali dva bratři z Pákistánu. V tomto případě je původ viru snadno prokazatelný, neboť se do něj oba sami podepsali a to včetně názvu své společnosti a telefonního čísla. Bootovací virus, který se šířil po disketách, měl původně zabránit nelegální distribuci lékařského softwaru, který bratři Alviové naprogramovali. Škodlivý kód zpomaloval čtení disket, ale pevné disky nenapadal.

Stuxnet (2010) = virus zaměřený na průmyslové systémy

Od konce osmdesátých let se různé internetové hrozby šířily v naprosté většině neadresně, poměrně málo vzorků škodlivého kódu mělo konkrétní cíl v podobě konkrétní společnosti či fyzické osoby. S malware jako zbraní v mezinárodním konfliktu jsme se ale – s největší pravděpodobností, oficiální potvrzení nezaznělo – setkali v podobě počítačového červa Stuxnet v roce 2010. Z jeho analýzy vyplynulo, že byl zaměřen na kontrolu průmyslových systémů, konkrétně monitorovacího systému SCADA. Infikování proběhlo skrze přenosné USB zařízení a pravděpodobným primárním cílem tohoto úspěšného útoku byla íránská jaderná elektrárna, konkrétně centrifugy na obohacování uranu. V tomto případě nepomohl ani fakt, že je systém zcela izolován od internetové sítě.

Jak se virus šíří?

Jeden z nejčastějších způsobů šíření virů představuje e-mail. Otevřeme nakaženou přílohu e-mailu. Klikneme na odkaz vedoucí na infikovanou webovou stránku. Stáhneme a spustíme zavirovaný soubor. To vše může způsobit rozšíření viru do systému.Virová infekce se šíří také při připojení infikovaných vyměnitelných paměťových médií, jako jsou například USB disky. Virus se z nich přenáší kopírováním zavirovaných souborů do PC.Pokud je náš počítač připojený k zavirované síti, může se vir přenést i po síti.

Proč uživatel virus neodhalí?

Pokud spustíme program obsahující virus, převezme škodlivý kód skrytý ve zdrojovém kódu kontrolu nad počítačem nenápadně. Vir začne na pozadí provádět škodlivou činnost a když má hotovo, předá kontrolu zpět originálnímu programu. Uživatel si ani nevšimne, že se něco děje. Vir se šíří dál bez jeho vědomí. Že máme na počítači vir poznáme, až když je pozdě.

Co je phishing?

Phishing je typ kybernetického útoku pomocí technik sociálního inženýrství, kdy se útočník snaží získat důvěrná data oběti nebo spustit na zařízení oběti škodlivý kód. Nejčastěji probíhá phishingový útok pomocí podvodného e-mailu s žádostí o informace k naší platební kartě nebo přihlašovací údaje do našeho internetového bankovnictví. Výjimkou ale není ani v chatovacích aplikacích a na sociálních sítích.

Typy phishingu

E-mail phishing

Většina phishingových zpráv je zasílána **e-mailem, který není adresovaný specifické osobě nebo organizaci** a je posílán hromadně na velké množství cílů, proto tento typ phishingu označujeme také jako bulk phishing.

Spear phishing

Jde o cílený phishingový útok, kdy si **útočník dopředu získá veškeré dostupné informace** o cílové skupině či jednotlivci a **vytvoří phishingovou zprávu přesně na míru**.

Whaling

Whaling je typem spear phishingového útoku, který cílí tzv. na velké ryby čili na **vrcholové manažery a majitele firem**.

CEO fraud

Faktickým opakem whalingu je CEO fraud, kdy se phishingové zprávy tváří jako by pocházely právě od vysoce postavených manažerů a cílí na ostatní zaměstnance v podniku.

Vishing

V případě phishingového útoku **přes telefonní hovor** mluvíme o tzv. voice phishingu nebo zkráceně vishingu, česky také **podvodném volání**. Útočníci pro tyto útoky mohou využívat předem namluvené a automaticky přehrávané zprávy, někdy vytvořené za pomocí generátorů, které převádí text na řeč. Telefonní čísla útočníků vypadají jako čísla reálné instituce, za kterou se vydávají (tzv. spoofing).

Smishing

V případě smishingu nebo také SMS phishingu zasílají útočníci **podvodnou zprávu na mobilní telefon**. Zpráva většinou vyzývá ke kliknutí na podvodný odkaz nebo obsahuje telefonní číslo či e-mail, přes které má oběť kontaktovat instituci, za kterou se útočníci vydávají.

Page hijacking

Jedná se o typ phishingu, kdy jsou **uživatelé nevědomě směřováni na podvodný web**. Útočníci vytvoří duplikát již existující webové stránky a internetové vyhledávače začnou tento web upřednostňovat před původním legitimním webem. Případně útočníci kompromitují legitimní webové stránky, aby uživatele přesměrovali na ty škodlivé.

Catfishing

Podvodná činnost, při které si útočník vytvoří na internetu (zpravidla na sociálních sítích) falešnou identitu za účelem kompromitování oběti, navázání vztahů, kyberšikaně nebo kvůli vidině finančního zisku.

Jak phishing poznat?

E-mailová zpráva může obsahovat oficiální logo i další prvky legitimní komunikace, a přesto může jít o phishing. Níže naleznete několik rad, které vám pomohou phishing rozpoznat.

7 rad na rozpoznání phishingu:

1. **Neočekávaný e-mail** – Nevyžádané e-maily od neznámých osob není nutné otevírat. A když už, pak rozhodně se zvýšenou pozorností.
2. **Požadavek na osobní údaje** – Žádná seriózní banka nebo finanční instituce po vás nebude chtít vyplnění hesla do internetového bankovnictví v e-mailu.
3. **Špatná gramatika** – Pokud vám zrovna nenapsal váš známý dysgrafik, pak jsou překlepy a špatná čeština varovným signálem, který by mohl znamenat podvodnou zprávu.
4. **Přílišná naléhavost** – Útočníci chtějí uživatele donutit provést požadovanou akci co nejrychleji, aby o tom neměl čas přemýšlet. Pokud tedy na vás e-mail příliš tlačí a nutí kliknout na tlačítko či odkaz, a provést zadání vašich přihlašovacích údajů, změnu hesla nebo provést okamžitou platbu buďte ve střehu.
5. **Velmi výhodná nabídka** – Zboží zadarmo, služba za nesmyslně výhodnou cenu, nově nalezený příbuzný milionář z Afriky, to vše je typické pro phishing.
6. **Podezřelá e-mailová doména** - E-mail je odeslán z veřejné e-mailové domény (např. gmail.com, yahoo.com, seznam.cz) nebo je název domény špatně napsaný (airbank.cz à airbnak.cz).
7. **Podezřelá URL adresa** – Adresa odkazu, na který máte kliknout, neodpovídá odesílateli a povaze zprávy. Při přejetí odkazu myší neodpovídá náhled URL adresy názvu odkazu ve zprávě.

Co je malware?

Termín malware je kombinací dvou slov – malicious, což znamená škodlivý, a software. Do kategorie malware řadíme veškerý škodlivý kód, přičemž nezáleží na způsobu, jakým napadá počítače, ani na chování nebo na výsledku jeho činnosti.

Malware obsahuje celou řadu různých kategorií škodlivého kódu – od **trójských koní, ransomwaru, virů, červů** až po **bankovní malware**. Obecně se dá říci, že jde o veškerý software, který byl vytvořen se škodlivým záměrem.

Jak poznat malware?

Pro nezkušené „oko“ je velmi těžké škodlivé soubory rozpoznat. Upozornit vás může podivné chování ve vašem internetovém prohlížeči (např. změna vaší domovské stránky nebo zobrazování nezvyklých upozornění a vyskakovacích oken), výrazné zpomalení funkcí vašeho zařízení, vyšší spotřeba paměti nebo mobilních dat, nižší výdrž baterie nebo nové aplikace, které jste sami do zařízení nenainstalovali.

Pokud používáte bezpečnostní program, můžete být v klidu. Antivirové programy obsahují celou řadu technologií, které dokážou zachytit a odstranit malware.

Jaké druhy malwaru existují?

- **trojský kůň** - maskuje se za věrohodný soubor nebo program, aby uživatele přiměl k jeho stažení a instalaci
- **ransomware** - odepírá uživateli přístup k jeho zařízením nebo datům a šifruje je do doby, než je zaplaceno výkupné
- **spyware** - tajně sbírá informace o uživateli a jeho zařízení a následně je odesílá kyberzločinci
- **počítačový virus** - dokáže se kopírovat a šířit do dalších počítačů, upravuje legitimní hostitelské soubory nebo programy a spouští svůj kód, když uživatel spustí infikovaný program
- **červ** - na rozdíl od počítačového viru se dokáže sám kopírovat a šířit bez vědomí uživatele a není závislý na hostitelském souboru

Jak malware funguje?

Autoři škodlivého kódu jsou při hledání cestiček, jak infikovat zařízení, velmi kreativní. Většinou se snaží útočit z více směrů např. přes neznámé **zranitelnosti**, s použitím **phishingu**, **skrýváním** v paměti nebo **imitací** legálních procesů v počítači.

Dlouhodobě největší úspěchy však útočníci slaví s cílením na nejslabší článek řetězce, kterým je samotný uživatel. Velmi úspěšné a levné tak jsou **podvodné e-mailové kampaně**, které útočí s pomocí technik sociálního inženýrství. K nakažení zařízení pak stačí jedno nešťastné kliknutí.

Jak se zbavit malwaru?

Škodlivý kód můžete obecně odstranit dvěma způsoby – automaticky a manuálně. Manuální odstranění je podstatně složitější, protože škodlivý program se často sám chová tak, aby vám zabránil ve svém odinstalování. V takovém případě zkuste spustit telefon v nouzovém režimu a odebrat aplikaci, která podle vás způsobuje nestandardní chování telefonu.

Automaticky vám malware pomůže odstranit bezpečnostní program. Nainstalujte antivirový program určený pro váš operační systém a spusťte detekci. Pokud si navíc aktivujete automatické skenování a aktualizace, budete chráněni před nejnovějšími hrozbami i v budoucnu. Aktualizace obsahují důležité opravy nově objevených bezpečnostních chyb.

Pokud zatím žádné bezpečnostní řešení nepoužíváte, můžete využít pro rychlou jednorázovou kontrolu **ESET Online Scanner**, který vás upozorní na potenciální hrozby a nechtěné aplikace.

Jak se bránit malwaru?

Základem jsou **pravidelné aktualizace** operačního systému a používaného softwaru. Ideálně naistalovat **kvalitní antivirus pro Windows**, který dokáže automaticky detekovat a odstranit přicházející hrozby.

Zapomínat bychom neměli ani na **pravidelnou zálohu dat**, nejlépe bychom měli udržovat tři kopie dat, která chceme chránit. Tyto kopie pak uložte alespoň na dva různé typy úložných médií. A posledním kouskem skládačky, ne však ve smyslu důležitosti, je používání zdravého rozumu aneb dvakrát měř, jednou řež. Například při nalezení stránky nebo e-mailu s podezřele výhodnou nabídkou nákupu produktu nebo služby není žádoucí ihned klikat na odkazy a funkční tlačítka. Stačí se porozhlédnout na internetu, zda se s podobnou nabídkou už někdo setkal, a zda je legitimní.

Nejčastější počítačové viry a hrozby zaměřené na **domácí uživatele:**