

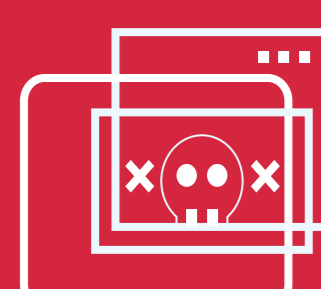
KYBERNETICKÉ ÚTOKY: SLOVNÍČEK POJMŮ

SoftwareONE vám pomůže překonat úskalí spojená s kybernetickou bezpečností. Vytvořili jsme pro vás průvodce běžným žargonem nejmodernějších pojmů a taktik kyberpodvodníků:



Adware

Software, který ve vašem počítači zobrazuje reklamní obsah a může obsahovat škodlivé odkazy nebo vést na škodlivý web.



Bot nebo Web bot a webový prohlížeč (web crawler)

Automatizovaný program, jako je web crawler, který provádí nebo simuluje lidské aktivity na internetu. Web boty lze použít k převzetí kontroly nad počítači, zahájení útoků a kompromitování dat. Mohou působit jako součást smíšené hrozby.



Armády botnetů nebo zombí

Skupina počítačů, které byly napadeny a dostaly se pod kontrolu útočnicka prostřednictvím malwaru. Jsou používány, aby zahájily útoky typu odmítnutí služby (denial-of-service, DoS), posílaly spam nebo prováděly další škodlivou činnost.



Sklizení pověření (Credential Harvesting)

Vytvořením podobných webů (jako je například azure.microsoft.com) se stránkou, která přesně napodobuje portál Azure, lze třeba uživatele přimět k zadání hesel, která jsou útočnickem zachycena a použita.



Odepření služby (Denial-of-Service, DoS)

Útok na počítač nebo síť, při kterém je zaplněna šířka pásma připojení nebo jsou přetíženy další zdroje až do bodu, kdy budou služby počítače nebo sítě pro klienty nedostupné.



Vybírání odpadků (Dumpster Diving)

Zloději se prohřabávají koši na odpadky a hledají účty nebo jiné dokumenty, které obsahují vaše osobní údaje.



Odcizení identity

Někdo ukradne vaše osobní finanční informace nebo provede podvodné platby či výběry z vašich účtů. Podvodníci někdy tyto informace použijí k čerpání úvěru nebo založení bankovního účtu a nechají oběť odpovídat za všechny poplatky.



Keylogger

Software, který sleduje a zaznamenává vše, co uživatel zadá na klávesnici počítače. Používá se pro účely technické podpory a dohledu.



Malware

Malware, známý také jako „škodlivý software“ (malicious software), je navržen tak, aby poškodil, napadl nebo převzal neoprávněnou kontrolu nad počítačovým systémem. Malware zahrnuje viry, červy, trojské koně, některé keyloggery, spyware, adware a boty.



Farmaření (Pharming)

Platná webová adresa a webová stránka nelegálně přesměrovávají na web, který není legitimní. Tyto „falešné“ weby požadují osobní údaje, jako jsou čísla kreditních karet, informace o bankovních účtech, rodná čísla a další citlivé informace.



Phishing

Podvod, který zahrnuje použití replik existujících webových stránek k pokusu o vylákání osobních nebo finančních údajů a hesel.



Vyskakovací okna

Forma webových reklam, která se na obrazovce počítače objevuje jako „vyskakovací okno“. Vyskakovací okna mají zvyšovat provoz na webu nebo zachytávat e-mailové adresy. Někdy jsou však vyskakovací reklamy navrženy se zákeřným úmyslem, například když se objeví jako požadavek finanční instituce na osobní údaje.



Ransomware

Typ škodlivého softwaru navrženého k blokování přístupu k počítačovému systému, dokud není zaplacená požadovaná částka peněz. Přestože se ransomware obvykle zaměřuje na jednotlivce, je jen otázkou času, než se zaměří i na firmy.



RetroVirus

Tento virus se zaměřuje konkrétně na obranu vašeho počítače. Bude hledat chyby zabezpečení operačního systému vašeho počítače nebo v jakémkoli bezpečnostním softwaru třetí strany, a to obvykle v kombinaci s jinou formou útoku.



Sociální inženýrství

Metoda klamání uživatelů, aby vyzradili soukromé informace. Často je spojeno s phishingem, pharmingem, spammem a dalšími internetovými podvody.



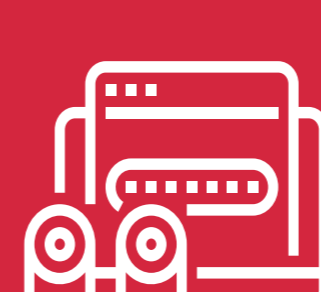
Spam

Nevyžádaný e-mail, obvykle hromadně odesílaný na velký počet náhodných účtů. Často obsahuje reklamy na produkty nebo služby. Lze jej minimalizovat pomocí softwaru na filtrování e-mailů.



Spim nebo Instant Spam

Nevyžádané zprávy přes komunikátory, obvykle hromadně zasílané velkému počtu uživatelských účtů; často obsahují marketingové materiály a odkazy na webové stránky produktů.



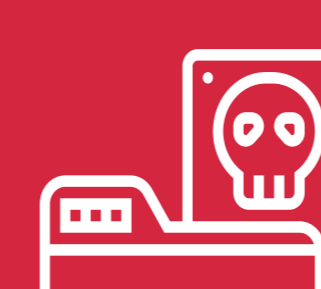
Spoofing

Útočník se maskuje za někoho jiného poskytováním falešných dat. Běžné příklady: spoofing webových stránek nebo URL.



Spraying Attack

Místo cílení na jednoho uživatele a jeho heslo použije útočník proti všem uživatelským účtům ve společnosti jedno snadno uhodnutelné heslo (například název společnosti a rok). Jediným úderem pak získá přístup k účtu.



Spyware

Program, který sleduje, co uživatelé dělají, a předává informace někomu jinému. Nejčastěji se instaluje při stahování bezplatného softwaru z internetu.



Trojské koně

Trojský kůň je škodlivý kód, který je maskovaný nebo skrytý v jiném programu, jenž se jeví jako bezpečný (jako v mýtu o trojském koni). Po spuštění programu umožňuje trojský kůň útočnickům získat neoprávněný přístup k počítači za účelem krádeže informací a způsobení škod. Trojské koně se běžně šíří prostřednictvím e-mailových příloh a stahování z internetu.



Virus

Škodlivý program, který se připojuje k dalším softwarovým aplikacím a souborům, aby je bez vědomí uživatele infikoval, čímž narušuje činnost počítače. Viry mohou přenášet takzvaný „payload“, spustitelné skripty určené k poškození, odstranění nebo odcizení informací z počítače. Virus je samoreplikační program, což znamená, že se sám kopíruje. Virus obvykle počítač infikuje a začne se replikovat, jen když uživatel spustí napadený program nebo otevře „infikovaný“ soubor.



Vishing

Typ phishingového útoku, kdy útočník ve falešném e-mailu použije místní telefonní číslo jako prostředek k získání vašich citlivých informací. Nic netušící volající je poté oklamán automatizovaným telefonním systémem, aby předal své citlivé informace.



Červ (Worm)

Podobný jako virus, ale s přidaným nebezpečným prvkem. Stejně jako virus se i červ může sám kopírovat, červ se však nemusí připojovat k jiným programům a nevyžaduje, aby jej uživatel odeslal do jiných počítačů.