Jak chránit e-shop před únikem hesel a malware. Radí bezpečnostní expert Michal Špaček

18.5.2026 - Kateřina Linhartová | Blog.shoptet

Praktický návod pro e-shopaře: Jak se bránit malwaru a krádeži hesel. Přinášíme rozhovor s bezpečnostním expertem Shoptetu Michalem Špačkem. Jak v praxi útočníci zneužívají hesla, cookies i falešné faktury?

Michal Špaček, Head of Security Shoptet, nám v rozhovoru přiblíží základy, které má znát každý majitel e-shopu. Jak si chránit svá hesla, jak nastavit spolupráci se Shoptet Partnery, když jim chcete dát přístupy do administrace e-shopu. Vysvětlí, jak funguje malware a ukáže i příklady ukradených dat z praxe.

Co je malware a jak mi může zkomplikovat život?

Malware je zkratka z malicious software, v překladu škodlivý software. Často se tomu také říká počítačové viry. Má více podob, známý je např. ransomware, který zašifruje disk, znepřístupní data a poté požaduje výkupné, za které (možná) dostanete heslo k dešifrování.

Relativní novinkou je kategorie infostealer, škodlivý software, který krade informace z napadeného počítače a obvykle se jinak neprojevuje. Infostealer se zaměřuje na všechno, co by se mohlo někomu hodit. Hesla, cookies, soubory na ploše i v dokumentech, skeny občanského průkazu, uložená čísla platebních karet apod. To všechno stáhne a odešle majiteli, kteří nejčastěji bývají ze států od nás na východ.

Odeslaná data se pak často přeprodávají, vyměňují a nabízí ke stažení i zadarmo, dostanou se tak k celkem velkému množství zájemců o nějakou neplechu.

Jak malware ohrožuje e-shop

Co se může stát, když malware ukradne heslo do administrace e-shopu?

Pokud vám malware ukradne heslo do administrace e-shopu, vidíme nejčastěji tyto věci, které mizerové provedou:

- Změní číslo účtu a potom platby nechodí na účet vám, ale jim.
- Začnou rozesílat spoustu nevyžádaných e-mailů (spam) ze schránky napadeného e-shopu.
- Vloží do stránek falešnou platební bránu, nebo přesměrování na nějaké online kasino.

Tohle jsou pro útočníky nejkratší cesty, jak si přijít k penězům, ale možností mají mnohem více. Mohou stáhnout seznam zákazníků a buď ho prodávat dále, nebo zákazníkům vaším jménem posílat spam, případně zkoušejí podvody typu „zaplaťte doplatek". Je dobré dodat, že ne všichni útočníci jsou tak sofistikovaní, jak nám často vykreslují různé filmy. Někteří ani nevědí, co s takovým získaným přístupem dělat, a tak ho jen jako ověřený často přeprodají dále.

Ale na to nelze rozhodně spoléhat…

Ne, každý takový pokus je jiný. Zkráceně řečeno, útočníci se snaží vydělat peníze způsobem, který o ně připraví vás, nebo vaše zákazníky. A mohou z toho být zbytečné trable pro vás – včetně hlášení na ÚOOÚ kvůli porušení zabezpečení osobních údajů.

Důležité je uvědomit si, že jako provozovatel e-shopů máte i hesla do systémů dopravců a různých marketingových nástrojů, kde lze také napáchat nemalé škody.

Zajímavá je i ta lidská stránka, říkáte si – proč nechodí do práce stejně jako ostatní? Četl jsem přiznání jednoho takového překupníka, který v celém řetezci ani nebyl na začátku, a ten psal, že druhá možnost byla jít do války. Místo toho zasedl k počítači a zjistil, že i bez odborných znalostí se peníze dají vydělat, tak do války nešel. Pravda, v porovnání s tím je přeprodávání ukradených dat a hesel asi ta lepší varianta.

Co je 2FA a proč mít dvoufaktorové přihlášení v e-shopu

E-shopaře bude ale zajímat, jak svá hesla mohou ochránit na Shoptetu a co se děje ve chvíli, kdy heslo unikne.

My v Shoptetu se snažíme naše klienty upozorňovat, pokud někde na Internetu najdeme jejich údaje. Ale vždy je to reakce, která z principu věci přichází až poté, co problém nastane. Malware krade data bez meškání, jeho páníčci pak také nečekají, až si toho všimnete.

Přinášíme také nástroje, které na tyto i jiné hrozby reagují. Již dříve jsme přidali dvoufaktorové ověřování přihlášení (2FA), posíláme informace o přihlášení z neznámého prohlížeče, což může znamenat ukradené heslo.

Viděli jsme mnoho pokusů o změnu bankovních účtů, proto jsme to znesnadnili tak, aby to útočníci nemohli dělat. Existuje také možnost využívat typ účtu s oprávněním Partner, který bez zapnutého 2FA nedovolí Shoptet Partnerovi, například kodérovi administraci používat.

Snažíme se také e-shopům pomáhat, pokud se ozvou, že mají nějaké podezření. Takto jsme například pomohli odhalit hacknutou poštovní schránku u několika koncových zákazníků, kterým e-shop poslal fakturu, ale útočník ji obratem stáhl, pozměnil bankovní údaje a znovu ji zákazníkovi odeslal z podobné adresy, ze které faktura přišla z e-shopu. Na té nové byl dokonce původní QR kód pro platbu – překrytý novým s útočníkovým číslem, který byl nepatrně posunut a ten původní šel označit a zkopírovat.

Zmiňoval jsi 2FA. Když si ho v e-shopu aktivujeme, znamená to, že máme zcela po starostech?

Samotné 2FA stačit nemusí. Malware krade i cookies z prohlížečů, pomocí kterých se 2FA často obchází. Aby aplikace nepožadovala zadávání 2FA kódů při každém přihlášení, tak se do cookie zapíše „následujících 30 dní 2FA nevyžaduj“, nebo „tohle je známý prohlížeč“. A když infostealer ukradne cookie s takovou informací, tak ji útočník může využít ve svém prohlížeči a tím 2FA přeskočit.

Takže pro vyšší bezpečnost doporučuješ spíše nezaklikávat možnost „Nevyžaduj následujících 30 2FA“, ale zadávat při každém přihlášení?

Pokud si do počítače stahujete viry a neoficiální vylepšení her, nebo používáte nelegální software,

tak by to stálo za zvážení. Já bych ale spíš doporučil na to jít od lesa: nepoužívat nelegální software a nestahovat neoficiální doplňky a cheaty do her. Ta možnost „Nevyžaduj následujících X dní“ je pohodlná, a tak lidem bude méně vadit udělat ten krok navíc jednou za měsíc.

Já jsem pro si 2FA zapnout všude, kde je to možné, a to i přestože nedokáže vyřešit všechny možné situace. Pásy v autě si také zapínám, i když vím, že mě neochrání před sousedem, který neumí moc couvat do svého parkovacího místa.

Příklady ukradených dat

Jak se může malware dostat do počítače nebo telefonu?

Tady se nevyhneme cizím slovům, ale netechničtí e-shopaři by se neměli nechat odradit od dalšího čtení, vše si vzápětí srozumitelně vysvětlíme. Dostat se tam může například přes cracky, keygeny, falešné přílohy, podvodné odkazy, herní módy, neoficiální stahování programů apod.

Společně s ukradenými daty malware odesílá i informace o napadeném zařízení, takže je vidět operační systém (macOS není výjimkou), kolik má počítač paměti i jak rychlý je procesor a jaká je IP adresa. Malware také informuje o tom, kde se spustil, z čehož se dá odvodit, co si kdo stáhl.

Můžeme si uvést reálné příklady, které se v ukradených datech objevují:

- Kiddions Mod Menu.exe doplněk a rozšíření hry GTA,
- Licence_Version_Loader.exe Pokus o obejití licenční ochrany programů jako např. Adobe Photoshop,
- Různé doplňky operačního systému a nástroje jako např. FnHotkeyUtility.exe, ZenSync.exe a další.

Všechny tyto programy mají ale pár věcí společných: snaží se na první pohled vypadat jako pomocníci, ať už tu pomoc potřebujete s čímkoliv. Ale jen se otočíte, tak vám vrazí kudlu do zad. Jsou také obvykle staženy z různých neoficiálních zdrojů, z diskuzních fór apod. V případě programů jako např. Licence_Version_Loader.exe to vlastně ani jinak nejde.

Dostávají se infostealery a viry do počítačů a jiných zařízení ještě jinak?

Infostealery a viry se do počítačů i jiných zařízení také dostávají jako programy maskující se za různé dokumenty, nezaplacené faktury a žádosti od „právníků” k odstranění nelegálního obsahu.

Několikrát jsme také viděli dokument, který se jmenoval: Popis_pracovní_pozice.docx[50 mezer].exe, kde těch 50 mezer opravdu bylo jako mezery, takže to na první a vlastně i na druhý pohled vypadalo jako wordovský dokument.

Slovníček pojmů

- **Crack** – program na prolomení licenční ochrany jiného programu tím, že jej přímo upraví. Cracky mohou a často obsahují i přibalené viry.
- **Keygen** – generátor licenčních klíčů. Vytvoří falešný, ale přesto funkční klíč. Ten se poté zadává do obvykle neupraveného programu, za který uživatel nechce platit, také obvykle obsahuje viry.
- **Infostealer** – typ viru, který „jenom“ krade data z napadeného počítače.

Jak malware rozpoznat?

Proč je pirátský software tak rizikový, i když si člověk samotný program ani nenainstaluje? Mohu ho jako běžný uživatel rozpoznat?

Samotné viry, nebo obecně malware může být a bývá už v instalačním programu, stačí tedy spustit obvykle nějaký setup.exe a vir už se může aktivovat, aniž bych si program nainstalovali. Viry také mohou být v keygenu nebo cracku, pokud je třeba nějak obejít licenční ochranu.

Na první pohled se to těžko poznává, ale programy nebo doplňky stahované mimo oficiální zdroje jsou velice podezřelé. Pirátský Photoshop těžko budete stahovat z oficiálního zdroje, ale je skoro jisté, že v doplňcích do her nebo právě ve Photoshopu staženém z náhodného diskuzního fóra nějaký malware bude. A když už to chcete vyzkoušet, tak prosím ne na počítači, kde máte pracovní věci. V případě e-shopu se to týká nejen majitele, ale všech uživatelů, kteří k jeho správě mají přístup.

Jak se chránit před malware

Jaká je prevence? Na co si dát pozor?

Na počítači, kde máte pracovní věci a přístup k administracím e-shopů, přístup do všech DPD a Zásilkoven, nedělat nic nepracovního. Nepoužívat doplňky do her, nestahovat a neinstalovat pirátský Photoshop.

Když něco vypadá trochu divně (různá hlášení podobná tomu, že na webu máte nelegální obsah), nebo to naopak vypadá moc dobře (nabídka nové práce nebo odměny za něco), tak to nechte plavat, nebo se s někým poraďte. Tyto věci často zneužívají lidskou zvídavost i strach, a proto je těžké s nimi bojovat technickými prostředky.

Útoky typu „ClickFix“ (česky by se dalo přeložit jako „klikni sem a tím to vyřeš“) se vás snaží přesvědčit, abyste k prokázání, že jste člověk, ještě na počítači něco spustili. Na klasické captche najdete všechny motorky nebo semafory a pak vás stránka ještě vyzve k tomu, abyste zmáčkli Win+R a pak Ctrl+V a pak Enter. Tím jak jsme kliknuli na motorky a semafory v captche, tak se vám do schránky vám vložil příkaz, který poté pomocí Ctrl+V a Enteru spustíte. Příkaz stáhne vir, spustí ho u vás na počítači, ale vy máte radost, že nejste robot.

Co má člověk udělat hned, pokud podobný soubor spustil nebo má podezření, že jeho zařízení mohlo být napadené?

Lidé na to obvykle přijdou pozdě. Až když jim začnou chodit upozornění na podezřelé nebo nové přihlášení z Google, Facebooku apod. Infostealer malware se schválně snaží nijak neprojevovat, jeho úkolem je jen krást údaje a data.

Shoptet posílá e-mailové upozornění po přihlášení z neznámého prohlížeče. Pokud vám takové oznámení přijde, věnujte mu prosím pozornost. Může jít o situaci, kdy přihlášení použil útočník na svém počítači.

Co dělat při úniku hesla do administrace e-shopu

Pokud máte podezření, nebo vir je potvrzen, tak je důležité změnit hesla, ideálně všechna a úplně všude – k e-shopu, do e-mailu apod. Je třeba to udělat z „čistého“ zařízení. Teprve poté se pokuste napadené zařízení odvirovat. Jde o čas, útočníci mají zkoušení přihlašovacích údajů automatizované

a rychlé.

Služby jako Google i zmíněný Facebook a stejně tak Shoptet nabízí seznam posledních přihlášení, to je dobré prozkoumat (Nastavení -> Administrace -> Správci obchodu a tab Seznam přihlašování). V některých případech lze neznámé zařízení odebrat, jindy stačí změnit heslo.

Pojďme si projít konkrétní postup, co dělat, pokud mám podezření na únik hesla do administrace.

Pokud máte podezření nebo rovnou potvrzení, že uniklo heslo do administrace e-shopu, tak změňte hesla z nezavirovaného zařízení.

Začněte e-shopem, změňte heslo do administrace a rovnou si nastavte 2FA, pokud ještě nemáte. Pokud máte u Shoptetu i e-mailovou schránku, tak nezapomeňte heslo změnit i tam. Podívejte se také, jestli si někdo nějakou e-mailovou schránku nepřidal – občas to mizerové dělají kvůli rozesílání spamu. Zkontrolujte HTML kódy v editoru vzhledu, správnost bankovního účtu, aby se neposílaly faktury s číslem cizího účtu.

Podívejte se, jestli neproběhl nějaký „neobjednaný“ export objednávek a zákazníků, v obou případech to najdete na záložce Přístupový log. Také je dobré zkontrolovat nahrané soubory do e-shopu – útočníci občas nahrají nějaký vlastní obrázek jako jakýsi podpis ve stylu „byl jsem tu, Fantomas“. Pokud nebudete vědět nebo si nebudete jistí, napište nebo zavolejte na podporu Shoptetu. Je to lepší než si říkat, že se přece nic nestalo.

Shrnutí: Co zkontrolovat, pokud došlo k úniku hesel

Proveďte tyto kontroly:

- jestli unikly nějaké údaje,
- jestli někdo nevyexportoval seznam objednávek,
- jestli někdo nepřidal nebo nepřesměroval e-mailovou schránku,
- jestli někdo nezměnil stránky e-shopu a nepřidal na ně jiné číslo účtu.

Poučte se z toho, omezte práva, smažte staré uživatele, nastavte si všude možné 2FA, která může příští útok zastavit!

Jak správně nastavit účty a přístupy do e-shopu

- **Zapnout dvoufaktorové ověřování** všude, kde je to možné.
- U Shoptet Partnerů, agentur nebo kodérů **využívat typ účtu Partner, který vyžaduje 2FA**.
- Omezovat **práva uživatelů** podle toho, co skutečně potřebují.
- **Mazat** staré nebo nepoužívané uživatele.
- Pravidelně kontrolovat, **kdo má přístup do administrace** e-shopu.
- Myslet i na **přístupy do rozhraní dopravců, marketingových nástrojů** a dalších navázaných služeb.
- **Poučit všechny uživatele** s přístupem do administrace, že **riziko se týká i jejich zařízení.**

FAQ: Malware, infostealery a bezpečnost e-shopu

Jaký je postup při úniku hesla do administrace e-shopu?

Změňte hesla z nezavirovaného zařízení. Začněte e-shopem, změňte heslo do administrace a rovnou si nastavte 2FA, pokud ještě nemáte. Pokud máte u Shoptetu i e-mailovou schránku, tak nezapomeňte heslo změnit i tam. Podívejte se také, jestli si někdo nějakou e-mailovou schránku nepřidal (občas to dělají kvůli rozesílání spamu). Zkontrolujte HTML kódy v editoru vzhledu, správnost bankovního účtu, aby se neposílaly faktury s číslem cizího účtu. Podívejte se, jestli neproběhl nějaký „neobjednaný“ export objednávek a zákazníků.

Co je malware?

Malware je zkratka z anglického **malicious software**, tedy škodlivý software. Často se mu obecně říká počítačový virus. Malware může mít různé podoby. V rozhovoru je zmíněný například **ransomware**, který zašifruje disk, znepřístupní data a následně požaduje výkupné za jejich možné dešifrování.

Dá se malware poznat na první pohled?

Podezřelé jsou hlavně programy a doplňky stahované mimo oficiální zdroje. Může jít o doplňky do her nebo pirátský Photoshop stažený z náhodného diskuzního fóra.

Jaká data může útočník pomocí infostealeru získat?

Hesla, cookies, přístupy do služeb, dokumenty, možnost obejití 2FA.

https://blog.shoptet.cz/malware-eshop-hesla