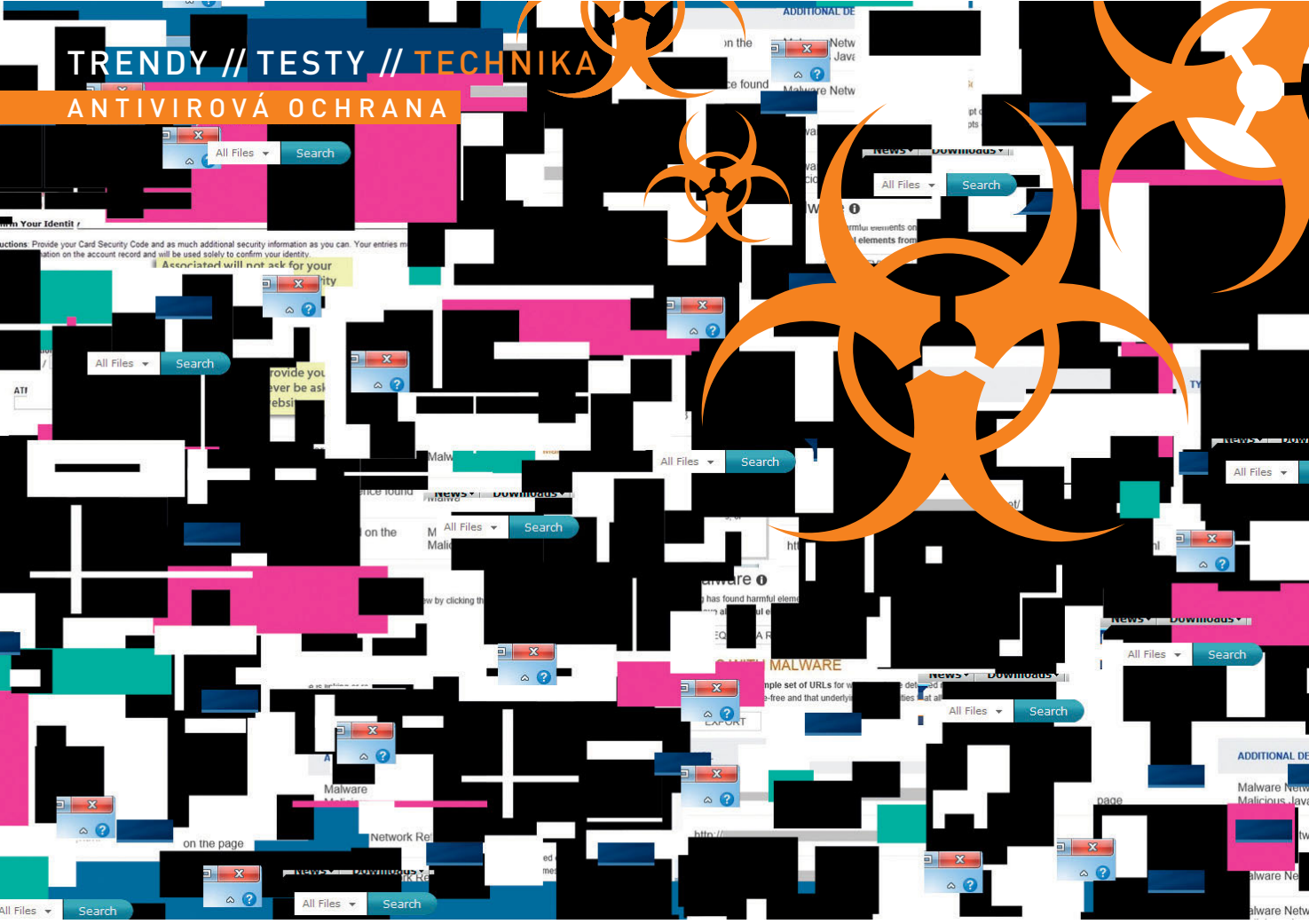


PODEZŘENÍ NA VIRY
Jak se můžete chránit

Malware ohrožuje jak vaše data, tak vaše peníze. Ukážeme vám, jak můžete útoky virů detekovat a ochránit tak svá zařízení.

PETR KRATOCHVÍL

Redaktor Chipu zkoumá nejnovější triky hackerů a tvůrců virů. I díky tomu vám může poskytnout užitečné rady a návrhy, jak se lze před virovými útoky chránit.

Od dob zábavných a neškodných virů už uplynula pěkná řádka let. Nejnovější malware má na mušce nejen data na vašich přístrojích, ale také peníze v bance nebo přístupové údaje k webovým službám. Smutné bohužel je, že obvykle jsou uživatelé vždy o krok za podvodníky. My vám ukážeme několik nejpoužívanějších metod: od staršího, ale stále oblíbeného útoku „Man in the Browser“ až po nejnovější triky podvodníků. Poradíme vám, jak poznat, že jste se stali oběťmi malwaru, a jak se před podobnými hrozbami bránit. Nebudou chybět ani nástroje, které vám tuto obranu usnadní.

Ochrana na webu i pro smartphony

Pomocí informací z tohoto článku se můžete chránit nejen před nejnovějšími strategiemi internetové bankovní mafie, ale i před starými viry, které váš počítač zašifrují a pokoušejí se z vás vymámit výkupné. Nabídneme vám užitečné tipy i pro chytré telefony, protože tvůrci virů nedávno tuto platformu objevili jako dobrý zdroj příjmů a pomocí drahých prémiových SMS dokážou většině nepřipravených uživatelů znepříjemnit život.

INTERNETOVÉ BANKOVNICTVÍ

Únos účtu

Hackeři dokážou získat přístup k vašemu účtu – stačí jen jedno vaše neopatrné kliknutí na nesprávné místo.

Není žádnou novinkou, že se počítačoví zločinci snaží získat přístup k bankovnímu účtu a vybrat z něj peníze. Obvykle k tomuto účelu používají phishing, při kterém podvodníci posílají zprávu, která vypadá, jako by byla odeslána bankou. Pokud uživatel dopis otevře, dozví se, že banka zákazníkovi oznamuje, že vzhledem k tomu či onomu důvodu by měl být účet uzamčen. Abyste tomu zabránili, musíte se přihlásit ke svému účtu na webové stránce banky pomocí svých přístupových údajů. Důležité ale je, že byste se měli přihlásit kliknutím na odkaz v e-mailu, který vede na podvodný web hackerů. Nepříjemné je, že jak dopisy z banky, tak i podvržené bankovní weby jsou téměř bez chybičky. Dávno pryč jsou doby, kdy i naprostému začátečníkovi napověděl „špatný češtin ve banka zprávy". Na počátku tohoto roku bylo podobnými útoky postiženo přibližně 600 bank a naprostá většina zpráv i bankovních webů byla výborné kvality.

Oblíbenou variantou jsou také zmanipulované výpisy z účtů nebo zavádějící hypertextové odkazy, které vás navedou na stránku, kde je do vašeho počítače propašován nejnovější malware, který přístupové údaje do banky vyčmuchá.

Obrana: Zdravý rozum a obezřetnost

Abyste se nezařadili mezi oběti útoků tohoto typu, stačí jen používat zdravý rozum a při práci s počítačem přemýšlet. Je pravděpodobné, že by vám banka blokovala účet a chtěla po vás zadávání citlivých údajů do e-mailu?

Pokud z hlediska svých účtů nemáte úplně čisté svědomí a chcete si raději vše zkontrolovat, zadávejte adresu banky ručně do prohlížeče – pozor, nedoporučujeme používat ani záložky, protože je nejnovější varianty malwaru umí zmanipulovat. Jakmile jste na stránkách banky, před zadáním přístupových údajů ještě zkontrolujte identifikační údaje: vlevo od adresního řádku by měl být vidět certifikát, který se po kliknutí rozbalí a nabídne podrobnější údaje. Klíčové je jméno provozovatele, které by mělo být podobné jménu banky.

Za téměř dokonalé bylo až donedávna považováno dvoufaktorové zabezpečení, kde každá bankovní operace byla potvrzována zadáním kódu například SMS z mobilního telefonu. Nicméně v současnosti existuje i malware, který manipuluje celým oknem prohlížeče a dokáže zmanipulovat i zmiňované zadávání kódů. Tyto útoky jsou označovány jako „Man in the browser" a lze je odhalit jen pomocí kvalitního antivirového nástroje. To, že je váš počítač napaden, lze ale odhalit i v rámci potvrzovací SMS zprávy, ve které jsou uvedeny podrobnosti transakce (jaká částka a na který účet).

SHRNUTÍ BEZPEČNOSTNÍCH ZÁSAD: JAK NENALETĚT PODVODNÍKŮM

- Nikdy neotvírejte e-maily s podezřelým obsahem, jejichž odesilatel je neznámý.
- Přístupové údaje k finančním účtům zadávejte jen na webech těchto institucí.
- Vždy zkontrolujte, zda je aktivní bezpečné spojení (SSL) a zda má web správný certifikát.
- Své účty pravidelně kontrolujte, abyste snadněji odhalili jeho případné zneužití.
- Používejte co nejlepší bezpečnostní nástroje, nejlépe s heuristickou detekcí.

JAK HACKEŘI MOHOU ZÍSKAT PŘÍSTUP K VAŠEMU ÚČTU

Nejjednodušší způsob stále funguje nejlépe: podvodníci stále využívají phishing. Pomocí falešných e-mailů a webových stránek se útočníci snaží získat přístup k citlivým informacím.

ČESKÁ SPOŘITELNA

Vážený kliente/klientko,

Jelikož využíváte služeb naší banky, tzn. osobní účet v České spořitelně, ke kterému máte aktivovanou debetní kreditní kartu VISA a v poslední době jsme zaznamenali na Vašem účtu podezřelé platební transakce, je potřeba aktualizovat data Vaší kreditní karty , v opačném případě bude Vaše kreditní karta zablokovaná a Váš účet pozastaven na dobu neurčitou. Chceme pouze ověřit, že transakce na Vašem účtě opravdu provádíteVy, jako disponent účtu a ne někdo jiný.

Pošlete nám prosím níže vyplněné parametry:

Jméno a příjmení: _____

Rodné číslo: _____/_____

Bydliště: _____

Tel.číslo:_____

Číslo kreditní karty: _____

Platnost karty od a do: _____

CVC kód (poslední 3 čísla na zadní straně): _____

Vizitka zaměstnance:

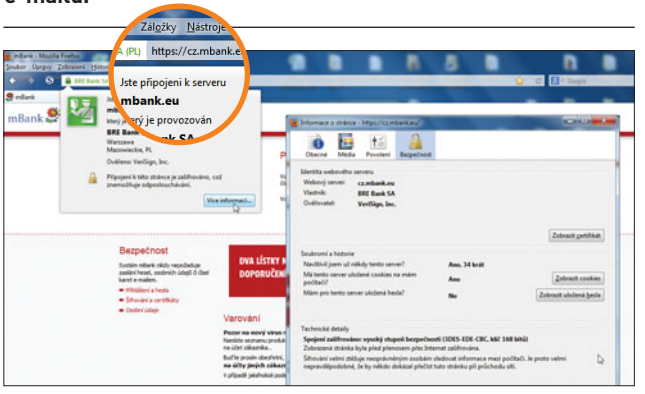
Bankéř klientského centra
Pro rozvoj
platebních karet

Bezpečnost při platbách kartou
Kontrola klientu a jejich platebních karet
Česká spořitelna,a.s.
csas@csas.cz - cic-csas@tym.cz

S pozdravem
Bankéř klientského centra

Česká spořitelna,a.s., Praha 4 Olbrachtova 1929/62 PSČ 140 00, IČ 45 24 47 82
zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl B, vložka 1171

Často lze rozpoznat falešné e-maily pomocí falešné adresy odesílatele, někdy také díky neohrabanému jazyku. Obecně ale platí, že banka po vás nikdy nebude chtít zadávat citlivá data do e-mailu.



U bankovních stránek byste se měli vždy ujistit, že je komunikace s webem zabezpečená – adresa by vždy měla začínat řetězcem „https". Při každé návštěvě také zkontrolujte, zda má web platný certifikát.

WINDOWS
Viry v systému

Některý malware se může do systému integrovat tak důkladně, že ho nedokážou odstranit ani antivirové programy. Pak je čas na speciální nástroje.

Podle průzkumu společnosti Kaspersky Lab se malware do vašeho počítače nejčastěji dostane prostřednictví USB flash disků nebo přímo z internetu. Většina malwaru jen krade citlivá data a sleduje záznamy klávesnice, stále častěji se ale objevuje vyděračský software. Tento ransomware zašifruje váš počítač a přístup k němu vám obnoví až po zaplacení výkupného – obvykle ve výši několika set až tisíc korun. Platba probíhá prostřednictvím nedetekovatelného řešení pro převod peněz (jako je paysafecard, Ukash nebo MoneyPak), a po jejím provedení dostane uživatel odblokovací kód. Zajímavé je, že u notebooků vyděrači s oblibou do zprávy přidávají fotku z kamery, aby uživatel věděl, že hackeři mají počítač zcela pod kontrolou.

O tom, že jde o nebezpečný fenomén, svědčí i fakt, že podle bezpečnostních expertů si takto i malé zločinecké skupiny mohou vydělat kolem 400 tisíc amerických dolarů za měsíc. Dobrou zprávou pro uživatele ale je, že pro celou řadu takovýchto vyděračských virů existuje dešifrovací klíč (nebo přímo kód) – najdete ho obvykle na webových stránkách výrobců antivirů. Pokud pro váš počítač nefunguje, pomohou vám speciální nástroje. Doporučujeme například program Norton Power Eraser, který si můžete bezplatně stáhnout na **www.slunecnice.cz/sw/norton-power-eraser**.

Život uživatelům neusnadňují ani rootkity, které jsou součástí komplikovanějších malwarů. Tento malware se dostane tak hluboko do systému, že ho obvykle nedokáže rozeznat ani běžný antivirový systém. Díky tomu má malware prakticky volné pole působnosti a může v počítači hledat citlivá data a přístupové údaje k bankovním či internetovým účtům. I proti těmto hrozbám lze použít zmiňovaný Power Eraser, mnohem lepším řešením je ale bootovací antivir, který najdete na Chip DVD. Podrobný test bootovacích antivirů navíc najdete v příštím čísle Chipu.

Lepší ochrana: Placená, nebo zdarma?

Základní bezpečnostní pravidlo zní: Pokud chcete mít svá data a finance ve svém počítači v bezpečí, měl by být nainstalován antivirový program s nejnovějšími aktualizacemi. Obecně platí, že především díky rozsáhlejším schopnostem (například heuristice) a vlastnostem (častějším aktualizacím virové databáze) je lepší používat placené antiviry. Ty lze doporučit především náročnějším uživatelům, kteří více využívají rozsáhlé internetové zdroje a na webu tráví hodně času.

Zkušenější uživatelé ale mohou dosáhnout dobrých výsledků i pomocí bezplatných nástrojů. Vhodná je například kombinace firewallu a bezplatného antivirového řešení. Čtenáři Chipu mohou zdarma využít profesionální bezpečnostní balík AVG Internet Security.

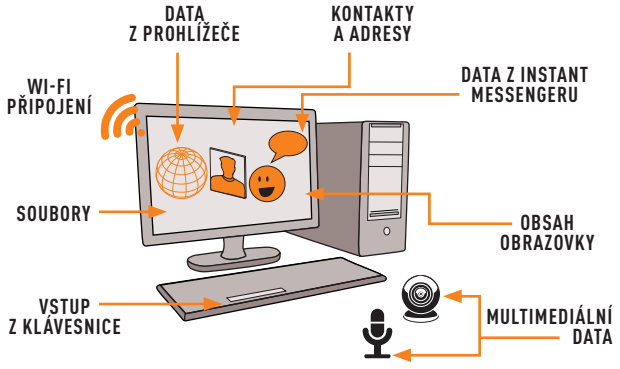
SHRNUTÍ BEZPEČNOSTNÍCH ZÁSAD: JAK NENALETĚT PODVODNÍKŮM

- **Před použitím vždy datové nosiče proskenujte (stačí použít i on-line skener).**
- **Jednou za čas počítač zkontrolujte pomocí speciálního nástroje na detekci rootkitů – v ideálním případě bootovacím antivirem.**
- **Pravidelně skenujte svůj systém a používejte kompletní sken.**
- **Nedůvěřujte slepě virtuálním počítačům – některý malware už ho umí překonat.**
- **Mějte vždy v antiviru aktuální signatury a pravidelně záplatujte svůj systém a aplikace.**

Ransomware zašifruje data na počítači a pro jejich odemčení je požadováno zadání kódu 1. Ten byste měli obdržet, pokud vyděrači pošlete peníze 2. V článku ale najdete tip, jak můžete počítač odemknout bez placení.

TAKTO VIRY SHROMAŽĎUJÍ INFORMACE

Pokud malware pronikne do systému počítače, může číst nebo měnit data téměř ze všech oblastí.



VIRY V ČÍSLECH

Počítačoví zločinci mají jen jeden cíl, ale mnoho způsobů, jak ho dosáhnout.

77 procent veškerého malwaru je vyvinuto pouze pro jediný účel: maximální zisk.

74 tisíc nových domén bylo v roce 2012 vytvořeno pouze k šíření malwaru.

3,4 milionu počítačů po celém světě je součástí sítě botů. Pochopitelně bez vědomí uživatele.

32 procent všeho malwaru na počítači špehuje a data posílá hackerovi.

PLACENÁ INZERCE

MOBILNÍ ZAŘÍZENÍ
SMS viry & spol.

Většina obětí virů pro mobilní telefony si útok vůbec neuvědomí.

V současné době existuje pro mobilní zařízení přes 50 tisíc virů, přičemž asi 95 procent z nich je napsáno pro Android. Důvod je zřejmý: Android je otevřenější než jakýkoliv jiný systém a uživatel má obvykle maximální práva. I když pro Apple iOS existuje méně virů, i tento mobilní operační systém má celou řadu slabých míst. Ta mohou být hackery zneužita k průniku do systému především tehdy, pokud mají přímý přístup k zařízení (uživatel provedl jailbreak). Většina autorů malwaru se ale soustřeďuje především na Android, protože zde mají obvykle cestu volnou. Ve snaze nalákat oběti na infikované webové stránky skrývají počítačoví zločinci URL těchto stránek stále častěji v QR kódech. Ty často obsahují návnadu s pornografickým obsahem, který uživatel opravdu získá – ale s viry.

Mimořádně nepříjemnou vlastností mobilního malwaru je to, že uživatel obvykle nemá šanci běžným způsobem nákazu odhalit – telefon se nechová zvláštně ani nedochází k jeho zatuhnutí. Jediným náznakem tak může být například menší výdrž na baterii, protože většina malwaru funguje nepřetržitě na pozadí. Pravda ale je, že před většinou aktuálních hrozeb váš chytrý telefon ochrání mobilní antivirové řešení.

Používejte jen oficiální obchody s aplikacemi

Mezi nejoblíbenější metody hackerů, jak dostat malware do telefonu, patří tzv. přebalení. Podvodníci si vyberou oblíbenou aplikaci či hru (často placenou) a do neoficiálního obchodu s aplikacemi přidají její upravenou bezplatnou verzi. Ta sice na první pohled často funguje podobně jako originál, je k ní ale přibalen vir. A pokud se při instalaci aplikace zeptá, zda ji přidělíte obvyklá práva, získá tyto práva také malware. I proto se někteří hackeři zaměřují na aplikace, které mají přístup k citlivým datům uživatele (kontakty, SMS zprávy, poloha...).

Je ale jasné, že v Google Play na podobné podvody nenarazíte – podvodníci se zaměřují především na menší neoficiální obchody, které nejsou pod kontrolou Googlu. Pokud tedy chcete pro svůj přístroj podobná rizika minimalizovat, doporučujeme nestahovat aplikace z neznámých zdrojů.

Mezi hrozby však nepatří jen aplikace kradoucí citlivé údaje – stále častěji se začínají objevovat aplikace sloužící k odesílání prémiových SMS. Ty dokážou během několika málo minut udělat útratu v řádech tisíců korun. Pokud prémiové SMS nevyužíváte, doporučujeme je přímo zakázat, nebo si alespoň u operátora nastavit limit, po jehož překročení budete informováni. I před těmito hrozbami vás mobilní antiviry ochrání.

Je také důležité zdůraznit, že pro iOS od Applu nemají antivirová řešení téměř žádný smysl – tento systém s celou řadou omezení ani neumožňuje antivirům prohledat celý smartphone na přítomnost virů. U tohoto operačního systému je pro bezpečnost klíčovým slovem aktualizace. Přístroj je nejlépe chráněn pouze s nejnovější verzí systému a pravidelné záplaty by měly zajistit ochranu před zranitelnostmi.

SHRNUTÍ BEZPEČNOSTNÍCH ZÁSAD: JAK NENALETĚT PODVODNÍKŮM

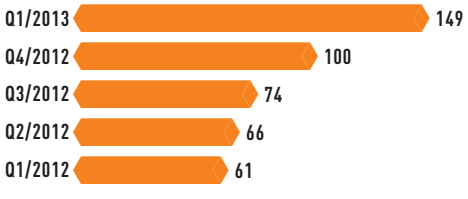
- **Instalujte pouze aplikace z oficiálních obchodů Google Play a Apple App Store.**
- **Na smartphone s Androidem si nainstalujte antivirový program (doporučení viz níže).**
- **Pokud se akumulátor vybije rychleji, než je obvyklé, může to být příznak virové nákazy – nainstalujte si antivirový program.**
- **SMS zprávy od neznámých odesílatelů obsahující URL adresu mažte.**
- **Pravidelně kontrolujte, zda se na vašem účtu za mobilní telefon nevyskytují položky, které by mohly pocházet z prémiových SMS.**

VĚNUJTE POZORNOST VÝBĚRU ZDROJŮ APLIKACÍ

Pokud chcete mít jistotu, že si do mobilního zařízení nestahujete malware, používejte pouze oficiální appstory Googlu a Applu. V nich jsou totiž aplikace testovány a hrozba nákazy je zde nižší. Nevěřte žádným neoficiálním zdrojům, zejména v případě výhodných nabídek, nebo dokonce placených her či aplikací zdarma. Majitelé telefonů s Androidem navíc mohou zakázat stahování aplikací z neoficiálních zdrojů.

NOVÉ RODINY MALWARU PRO SMARTPHONY

Na základě statistik společnosti F-Secure bylo v prvním čtvrtletí letošního roku detekováno 149 nových rodin nebo variant malwaru. Navíc jde o rostoucí trend.



NEJLEPŠÍ ANTIVIR PRO ANDROID

V jednom z minulých Chipů jsme otestovali více než dvacet antivirových nástrojů pro platformu Android. Vítězem testu byla aplikace TrustGo Mobile Security, dobře si vedly i nástroje od firmy Symantec a Trend Micro. Jejich volbou rozhodně nic nezkazíte.