evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
UNIVERSITAS MASARYKIANA BRUNENSIS
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

MALWARE

INFORMAČNÍ BEZPEČNOST

6. 3. 2013 KISK FF MU

PROČ TO?

- Jeden z nejběžnějších a nejdříve pociťovaných problémů bezpečnosti IT
- V 2012 s 0,8 % na 11. místě mezi nejčastějšími zdrojovými zeměmi nákazy z webových stránek, současně ale 5. místo mezi nejméně infikovanými, tj. 23,5 % počítačů (Kaspersky Security Bulletin 2012)
- Výzkum v USA a VB: 13 % nepoužívá antivir, dalších 9 % si není jisto, firewall nepoužívá také 13 %, jistých si není 21 % dotázaných; 52 % účastníků nezná své nastavení pro ochranu soukromí (The state of computer privacy)

MALWARE

- = Malicious Software, škodlivý software, škodlivé kódy
- Často chybně označováno „viry“
- Tento problém spojen výhradně s IT
- Vysoké, ale často nepřesné povědomí veřejnosti

ZPŮSOB INFIKOVÁNÍ

- Jako součást jiné aplikace SI nepotřebné – program dělá i to, co má
- Samostatný software větší problém odhalení – není tak obvyklý
- Časté SI – pro úspěšné infikování většinou potřebná spolupráce uživatele, ale ne vždy nezbytná
- Běžná cesta přes špatné nastavení či známými bezpečnostními dírami (chybí aktualizace), např. ActiveX jako dialer X zlepšení některých funkcí webových stránek

ZDROJE INFIKOVÁNÍ - WEB

- Nevhodný a nelegální obsah, hl. pornografie a nelegálně šířená díla - „třetina nelegálních programů umístěných na internetu je infikovaná“ (Přibyl, Základní pravidla bezpečného pohybu na internetu)
- Korektní stránky - Podle bezpečnostní společnosti Sophos se denně objevuje 16173 nakažlivých webových stránek, z nichž 90 % přestavují stránky s jinak nezávadným obsahem (Přibyl, Sophos varuje)

ZDROJE INFIKOVÁNÍ – E-MAIL

- Nákazu způsobí:
  - Text v HTML, možná infikace již zobrazením náhledu
  - Příloha, často nezbytné otevřít, starší metoda
- Častý spoofing, SI => důvěra

DALŠÍ ZDROJE INFEKCE

- Jakýkoli komunikační kanál (k dopravení malwaru k oběti)
  - Klasické např. IM, P2P sítě
  - Elektronické sociální sítě, mobilní komunikační služby…
- Připojitelné k různým typům souborů – od spustitelných přes dokumenty po MP3

ČINNOST MALWARU PO INFIKOVÁNÍ

- Může dělat vše, na co naprogramován
- Obvykle se snaží:
  - Skrýt: např. vytvořením mnoha i upravených kopií, vypnutím ochranných prvků…
  - Dále se šířit: u moderních kódů už obvykle bez pomoci uživatele
- V současnosti minimum destrukce, více špionáž – dáno změnou pohnutek tvůrců

UKÁZKY NEJČASTĚJŠÍCH ČINNOSTÍ

- Manipulace s OS, programy a soubory na disku, ale třeba i CD/DVD mechanikou, vč. změny lokálního záznamu DNS
- Získávání konkrétních či všech informací o uživateli a jejich odesílání, vč. pohybu myši a signálu z mikrofonu či kamery
- Vydírání uživatele (ransomware)
- Stahování a instalace dalšího malwaru (dropper)
- Zneužití k nelegálním činnostem (uložení dat, rozesílání spamu…), až plné ovládnutí počítače, často používáno k dDoS či jako proxy serveru

MOŽNOST ODHALENÍ – NEOBVYKLÉ CHOVÁNÍ

- Změna velikosti, názvů nebo obsahu souborů
- Zmenšování volného místa na disku
- Zpomalení výkonu počítače nebo připojení k internetu
- Nečekaně vysoká aktivita na disku nebo na internetu
- Samospouštění neznámých programů
- Poruchy programů a OS

TYPY KÓDŮ

- Na hraně škodlivosti shareware a adware – uživatel souhlasí s činnostmi, které ho mohou poškodit (viz SI)
- Podobně cookie – stejně jako ActiveX mohou zneužít funkce, kterou mají pomáhat
- Označení kategorií klasických typů malwaru z pohledu uživatele nepodstatné
- Význam přesné terminologie při odborném pohledu – označení typických charakteristik, problém v nepřesné hranici

VIRY

- První typ malwaru, dnes se téměř nevyskytují
- „Historicky je počítačový virus program, který napadne spustitelný nebo přeložený (object) soubor.“ (Klander, s. 385) - HOSTITEL
- Termín poprvé použil Fred Cohen v roce 1983 a předvedl ukázku
- Další možné členění: bootovací, souborové, stealth, polymorfní, generické…, makroviry (s OS Win95)
- První virus v oběhu = bootovací virus Brain v r. 1987, o rok později pro něj vydán antivir

ČERVI

- Dnes mnohem častější než viry – šíří se rychleji, mohou mít více funkcí (spojení kategorií)
- Mohou se šířit samostatně, vždy ale v síťovém prostředí
- Kontakty z adresářů, uložené, stanovené IP adresy, kombinace doménových jmen…
- Další dělení: e-mailové, síťové
- Často SI, spooofing
- 1. Worm (R. T. Morris) 2.11.1988 – v napadeném počítači se množil a rozesílal, až počítač „zamrzl“

TROJSKÉ KONĚ

- Nereplikují se, ale umožňují ovládnutí systému
- „…se na první pohled chová jako zcela legální program, ve skutečnosti však tajně provádí škodlivé operace“ (Král, 21)
- Nejčastěji spojeny se zadními vrátky (backdoor) a droppery
- Zdarma nástroj pro vzdálenou správu – klient + server
- Opět SI a spoofing; hůř hned odhalitelný – dělá, co sliboval

SPYWARE

- „Špehovací“ software – informace ukládá a většinou odesílá
- Často těžké odhalit – vznik z korektních důvodů (děti, zaměstnanci…)
- Problém rozlišení využití a zneužití (marketing, pomoc uživateli, licence za informace…) – podstatné seznámení uživatele se špehováním
- Reálně (nelegálně) lze i dnes umístit na veřejně dostupné počítače – problém důvěryhodnosti správců
- „Legální“ placené aplikace

SLEDOVANÉ INFORMACE

- Informace o zařízení i uživateli
- Již bylo shromažďováno: přehled nainstalovaných programů (vč. registračních údajů), historie navštívených stránek, využité odkazy, založené weby, časové období používání počítače/internetu, hesla a uživatelská jména, text e-mailů atd.
- Ohrozitelná jakákoli digitální stopa
- I korektně získané bylo zneužito (Toysmart)

MÉNĚ ZNÁMÉ KATEGORIE

- Keylogger: monitorují stisknuté klávesy
- Cookie a webbug: spyware na webu, i legální
- Backdoor/bot: otvírá skrytou cestu pro ovládnutí zařízení, vytváří zombie
- Browser Hijacker: mění nastavení webového prohlížeče
- Dropper: po infikaci nainstalují množství neseného malwaru
- Downloader: další malware stahují z definovaných webů
- Logická bomba: má určen spouštěcí pokyn pro škodlivou rutinu
- Password Stealer: určený speciálně k odcizování hesel
- Rootkit: pracuje na nízké úrovni OS, takže umí skrýt sebe i další aplikace a mění způsob práce systému, proto jej bezpečnostní programy špatně detekují a odstraňují
- Ransomware: blokuje přístup k datům a vydírá

PŘÍKLADY

- 1989 „AIDS Information Diskette Incident“ – 20 tis. dopisů s infikovanou disketou, která měla obsahovat informace o AIDS, ale zašifroval soubory na disku, klíč měl být doručen po finanční úhradě
- 2000 ILoveYou - „bližší informace o vysoké finanční transakci na Vašem účtu najdete v příloze“ (infikoval 10 % počítačů připojených k internetu)
- 2000 United Bank of Switzerland – zaměstnancům e-mail „žádost o zaměstnání“ – šel po heslech
- 2001 Anna Kournikova – jeden z prvních z generátoru
- 2001 Code Red – jeden z prvních hacktivismů (tvářil se z Číny)
- 2005 Sony BMG prodávala CD obsahující rootkit, který měl sloužit jako ochrana před nelegálními kopiemi
- 2009 Ikee – cílem odblokované iPhone (instalace neautorizovaného)
- 2010 – Stuxnet

OCHRANA - DŮVODY

- Ochrana vlastních dat i identity
- Ochrana vlastní bezúhonnosti – zneužití počítače na dálku k nelegálním činnostem
- Úspora času a nervů

OCHRANA – CHOVÁNÍ UŽIVATELŮ

- Pozor na problematický obsah
- Vše stažené prověřit
- Opatrná práce s e-maily a jejich přílohami (dle odesilatele, pak obsahu, problematické hned smazat)
- Stahování a instalace jen toho, co uživatel opravdu potřebuje
- Číst varování, hlášení, certifikáty…

OCHRANA – BEZPEČNOSTNÍ APLIKACE

- Antiviry = první bezpečnostní aplikace
- Od té doby se změnily ony i hrozby, proti kterým stojí
- Velmi různorodé (specializované X všeobecné, různé techniky, nástroje, nastavení…)
- Obecně chrání nejen proti virům
- Specializované – antirootkit, antispyware
- Firewall – ochrana proti nechtěnému transferu dat (kontrola paktů, uzavření portů, odhalení skenování portů…)

FUNKCE „ANTIMALWARU“

- Porovnávání signatur (nejstarší)
- Heuristická analýza (najde i nový malware)
- Analýza chování
- Kontrola integrity
- Sledování veškeré komunikace (hl. e-mailů a příloh)
- Rezidentní a nerezidentní ochrana
- Automatické aktualizace

ODBORNÉ SPECIALIZOVANÉ ZDROJE

- webové stránky CERT,
- Virový radar,
- Virus Bulletin,
- Securelist,
- Viry.cz

LEGISLATIVNÍ PROTIOPATŘENÍ

- Jedno z prvních opatření proti počítačové kriminalitě v ČR v 90. letech § 257a Poškození a zneužití záznamu na nosiči informací TrZ v již neplatném znění
- V aktuálním znění TrZ nahrazen § 230 Neoprávněný přístup k počítačovému systému a nosiči informací, § 231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat a § 232 Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti – mnohem přesnější a jasnější

LEGISLATIVNÍ PROTIOPATŘENÍ - APLIKACE

- Použitelné nejen na malware, ale na každý neoprávněný zásah do počítačového systému (tj. nejen PC)
- Chrání nosič i obsah
- Nutný úmysl poškodit, ne nedbalost

POUŽITÁ LITERATURA

- BITTO, Ondřej. Po čem touží útočníci. Computer. 2007, č. 18, s. 14-15. ISSN 1210-8790.
- BITTO, Ondřej. Temná zákoutí ještě temnější. Computer. 2006, č. 9, s. 92. ISSN 1210-8790.
- BITTO, Ondřej. Útočníci dospívají a jsou zákeřní. Computer. 2008, č. 8, s. 12. ISSN 1210-8790.
- BOTT, Ed, SIECHERT, Carl. Mistrovství v zabezpečení Microsoft Windows 2000 a XP. 1. vyd. Brno: Computer Press, 2004. 696 s. ISBN 80-722-6878-3.
- DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. Brno: Computer Press, 2004. 190 s. ISBN 80-251-0106-1.
- Kaspersky Security Bulletin 2012. KASPERSKY. Securelist [online]. © 1997-2013 [cit. 2013-03-03]. Dostupné z: http://www.securelist.com/en/analysis/204792255/Kaspersky_Security_Bulletin_2012_The_overall_statistics_for_2012
- KLANDER, Lars. Hacker Proof: váš počítač, vaše síť a vaše připojení k Internetu Je to opravdu bezpečné?. Kamila Chybová. 1. vyd. Brno: UNIS Publishing, s.r.o., c1998. 648 s. ISBN 80-86097-15-3.
- KRÁL, Mojmír. Bezpečnost domácího počítače: Prakticky a názorně. 1. vyd. Praha: Grada, 2006. 334 s. ISBN 80-247-1408-6.

POUŽITÁ LITERATURA (2)

- MALINA, Patrik. Jak se kradou bankovní hesla. PC World [online]. Praha: IDG Czech, 2007, č. 1 [cit. 2007-04-09]. Dostupný z: http://pcworld.cz/ostatni/jak-se-kradou-bankovni-hesla-5469. ISSN 1210-1079.
- MITNICK, Kevin. Umění klamu. Překlad Luděk Vašta. HELION S.A., 2003. 348 s. ISBN 83-7361-210-6.
- NÁDENÍČEK, Petr. Počítačové viry známé a neznámé: Spyware: moderní čmuchal inormačního věku. PC World [online]. Praha: IDG Czech, 2006, č. 5 [cit. 2007-04-09]. Dostupný z: http://www.pcworld.cz/pcw.nsf/ab74a33c54d5239fc1257148004c82e8/3c030da0bbc0e822c1257197005686 04?OpenDocument. ISSN 1210-1079.
- PŘIBYL, Tomáš. Sophos varuje : weby představují nebezpečí [online]. 2008 [cit. 2009-03-28]. Dostupný z: http://www.saferinternet.cz/uvodni-strana/440-3
- PŘIBYL, Tomáš. Základní pravidla bezpečného pohybu na internetu [online]. 2008 [cit. 2009-03-29]. Dostupný z: http://www.saferinternet.cz/novinky/406-3
- The state of computer privacy : Steganos 2008 survey into PC security [online]. 2008 [cit. 2009-03-29]. Dostupný z: www.steganos.com/uploads/media/Steganos_Press_Release_2008-10-24_SurveyPCusersGraphicsWhitePaper.pdf
- Trestní zákoník, v platném znění

Děkuji za pozornost.

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ