MALWARE

MALWARE

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

ZDROJE INFIKOVÁNÍ - WEB

- Nevhodný a nelegální obsah, hl. pornografie a nelegálně šířená díla - „třetina nelegálních programů umístěných na internetu je infikovaná“
- 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, byť stále hojně používaná

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 (krádeže dat a osobních informací) – dáno změnou pohnutek tvůrců

UKÁZKY NEJČASTĚJŠÍCH ČINNOSTÍ

- Manipulace s OS, programy a soubory na disku, ale třeba i CD/DVD mechanikou
- Získávání konkrétních či všech informací o uživateli a jejich odesílání, vč. pohybu myši a signálu z mikrofonu či kamery
- Vydírání uživatele (ransomware) – zaplať a dostaneš zpět svoje data
- 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
- Spouštění neznámých www stránek prohlížečem
- Poruchy programů a OS

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

DĚLENÍ VIRŮ

- **boot viry** (Boot Viruses) – napadají boot sektor, MBR a tím si zajistí své spuštění hned při startu počítače
- **souborové viry** (File Viruses) – jejich hostitelem jsou soubory, podle způsobu infekce se dělí souborové viry na přepisující, parazitické a doprovodné
- **multipartitní viry** (Multipartite Viruses) – napadají více částí (boot sektor i soubory)
- **makroviry** (Macroviruses) – šíří se v prostředí aplikací podporujících makra (MS Word, MS Excel)

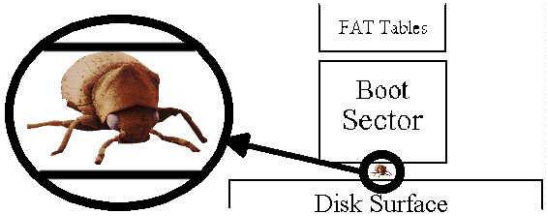
VLASTNOSTI VIRŮ

- současné počítačové viry nemohou poškodit technické vybavení počítače, mohou však smazat obsah paměti

- existují „mýty“ o poškozování FDD, HDD, monitorů apod., většinou však jde o chybně navržená zařízení
- formátováním pevného disku se virus nemusí vždy odstranit, neboť kód viru může být zapsán ještě v Master Boot Recordu (MBR)

PROJEVY POČÍTAČOVÝCH VIRŮ

- destrukce dat
- zobrazování různých zpráv na obrazovce
- vyluzování různých zvuků a melodií (Yankee Doodle)
- vtipkování s uživatelem (vkládání vtipných komentářů do textových souborů, různé animace, ...)
- simulace selhání technického vybavení
- zpomalování činnosti počítače



PROJEVY POČÍTAČOVÝCH VIRŮ

- Ale hlavně v dnešní době….

- Krádeže osobních dat! – hesla, čísla účtu, naše data (soubory), osobní údaje

RANSOMWARE

- Vyděračský software neboli *ransomware* je druh škodlivého softwaru, který zabraňuje přístupu k počítači, který je infikován. Tento program zpravidla vyžaduje zaplacení výkupného (anglicky *ransom*) za zpřístupnění počítače. Některé formy ransomware šifrují soubory na pevném disku (kryptovirální vydírání), jiné jen zamknou systém a výhrůžnou zprávou se snaží donutit uživatele k zaplacení.

RANSOMWARE


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt

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“
- Nejčastěji spojeny se zadními vrátky (backdoor) – tedy tajným přístupem do PC pro hackera

oPASSWORD STEALING - TROJANI (PWS)

oSKUPINA TROJSKÝCH KONÍ, KTERÁ OBVYKLE SLEDUJE JEDNOTLIVÉ STISKY KLÁVES (KEYLOGGERS) A TYTO UKLÁDÁ A NÁSLEDNĚ I ODESÍLÁ NA DANÉ E-MAILOVÉ ADRESY. MAJITELÉ TĚCHTO EMAILOVÝCH ADRES (NEJČASTĚJI SAMOTNÍ AUTOŘI TROJSKÉHO KONĚ) TAK MOHOU ZÍSKAT I VELICE DŮLEŽITÁ HESLA. TENTO TYP INFILTRACE LZE KLASIFIKOVAT I JAKO SPYWARE.

oDESTRUKTIVNÍ TROJAN

oKLASICKÁ FORMA, POD KTEROU JE POJEM TROJSKÝCH KONÍ OBECNĚ CHÁPÁN. POKUD JE TAKOVÝ TROJSKÝ KŮŇ SPUŠTĚN, PAK LIKVIDUJE SOUBORY NA DISKU, NEBO HO ROVNOU KOMPLETNĚ ZFORMÁTUJE. DO TÉTO KATEGORIE MŮŽEME ZAŘADIT I VĚTŠINU BAT TROJANŮ, TJ. ŠKODLIVÝCH DÁVKOVÝCH SOUBORŮ S PŘÍPONOU BAT. V TOMTO PŘÍPADĚ MŮŽE PŘEKVAPIT SNAD JEN OBČASNÉ JEDNODUCHÉ KÓDOVÁNÍ OBSAHU, DÍKY ČEMUŽ NENÍ NA PRVNÍ POHLED ZŘEJMÉ, CO TAKOVÝ KÓD PROVÁDÍ.

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

ADWARE

-Jde o produkt, který znepříjemňuje práci s PC reklamou

- Typickým příznakem jsou „vyskakující“ pop-up reklamní okna během surfování, společně s vnucováním stránek (např. výchozí stránka internet exploreru), o které nemá uživatel zájem. část adware je doprovázena tzv. „eula“ - end user license agreement – licenčním ujednáním. uživatel tak v řadě případů musí souhlasit s instalací.

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