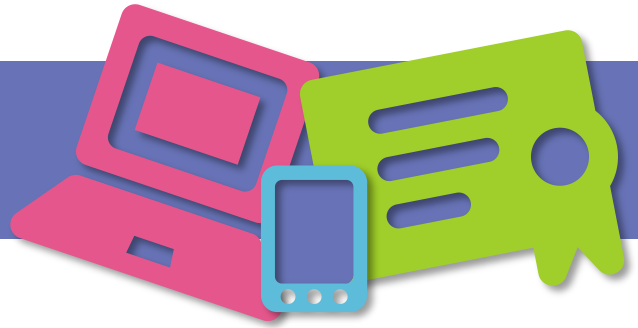
SECURITY 2014

22. ročník konference o bezpečnosti v ICT



Výzkumný projekt automatizovaného zpracování útoků

Michal Drozd

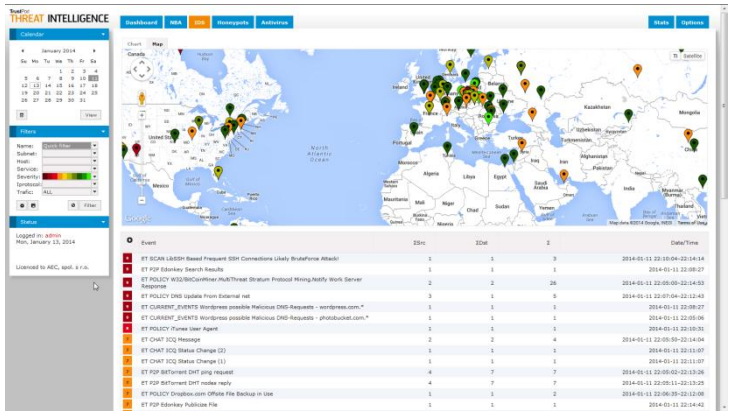
TrustPort a.s.

Agenda

- Výzkumný projekt
- Zaměření a cíle projektu
- Popis detekčních metod
- Co ano a co ne …

Projekt AIPS

- 2009-2013 AEC + VUT
- Zaměření na bezpečnostní technologie
- Cílem:
  - Průzkum stavu detekčních technologií
  - Návrh a vývoj vlastních detekčních metod



Cíle:

- Dozvědět se více o malware
  - Buffer-Overflow Exploits
  - Misconfiguration Exploits
  - C&C, APT, RAT (Remote Access Trojan)
- Otestovat detekční metody
  - Virtualizace (dynamická analýza kódu)
    - Sandbox
    - Shadow Honeypot
  - Analýza síťového chování (NBA, NBAD)
- Návrh vlastního řešení

Pokročilé útoky

Vlastnosti pokročilého malware

- Základní popis
  - Odcházení běžných detekčních mechanizmů
  - Specifické určení
- Využíváné vlastnosti
  - Buffer-Overflow Exploits
  - Misconfiguration Exploits
  - Maskování za jiné aplikace
- Detekční vlastnosti
  - Změna systémových parametrů
  - Zdroj anomálního chování (systém, síť)

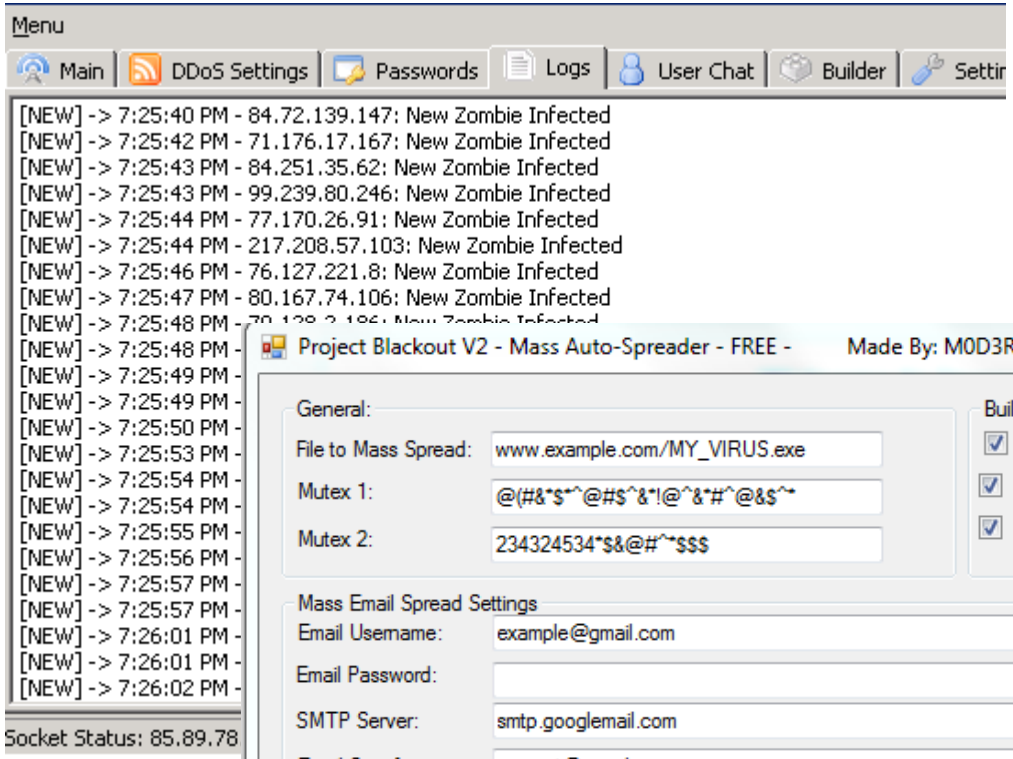
C&C Trojan PC framework #1

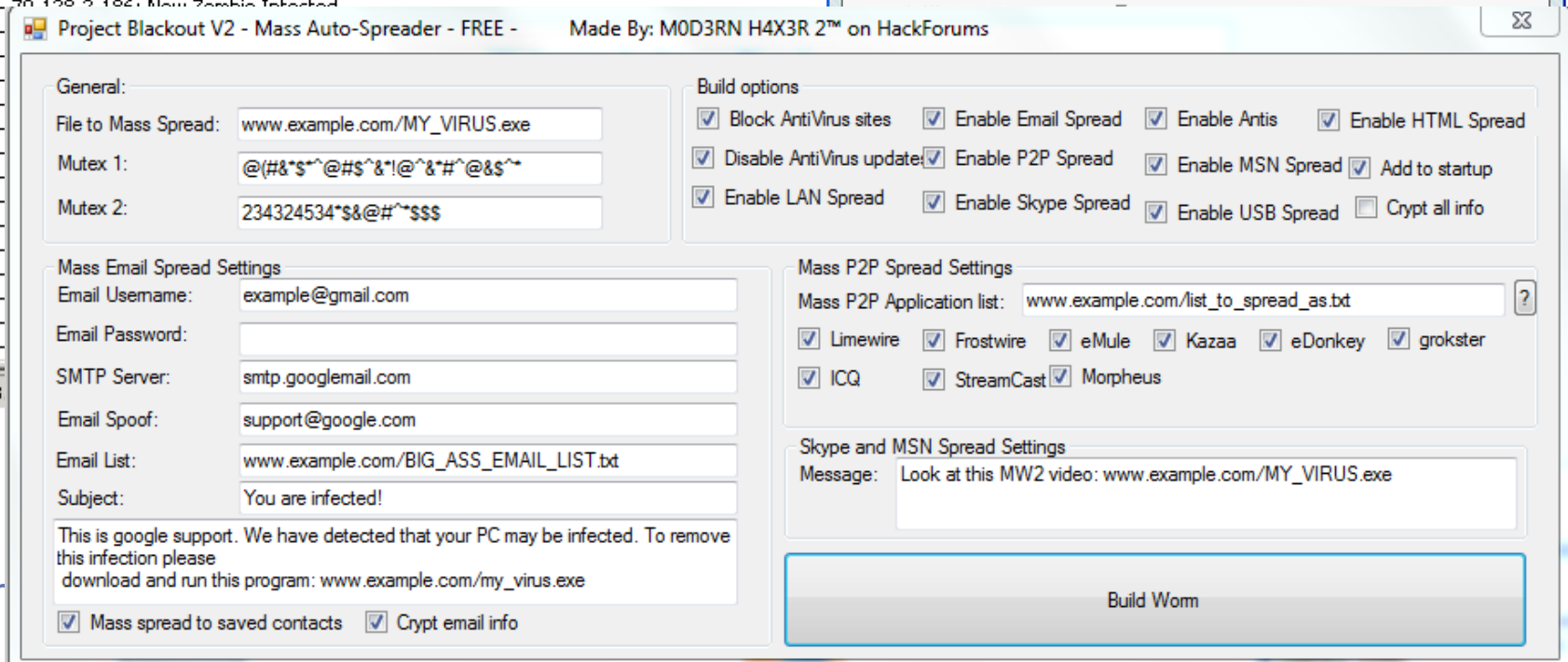
Tabulka s výběrem aktuálně a dostupných C&C frameworků:

Název	Cena kitu	Určení	cVektor	Lokace	Info
Citadel		Krádeže karet WebInject do prohlížeče (tj. podvržení autent. formuláře)	**SSL email** (Yahoo Hotmail, GMAIL)	Japonsko, UAE, Rakousko Turecko	
Beta Bot		Krádež autentizačních údajů na vybrané bankovní aplikace	SSL C2	USA	
Shylock		WebInjecting, Přímá krádež dat	SSL C2, Skype	EU, USA	**Cílen na sandbox** McAfee, FireEye, Symantec
Carberp		WebInject VNC boot sector	**C2 (+ SSL services)**		Mobil platforma(CarMo multifaktorová utentizace) Unikl zdrojový kód (5,7GB)
Hesperbot		Krádeže karet a účtů, webinject do prohlížeče	SSL C2	**Česká Republika,** Řecko, Portugalsko, UK	Nevychází ze Zea!
ZEUS		Základ většiny moderních mwr		GLOBAL	

C&C Trojan PC framework #2

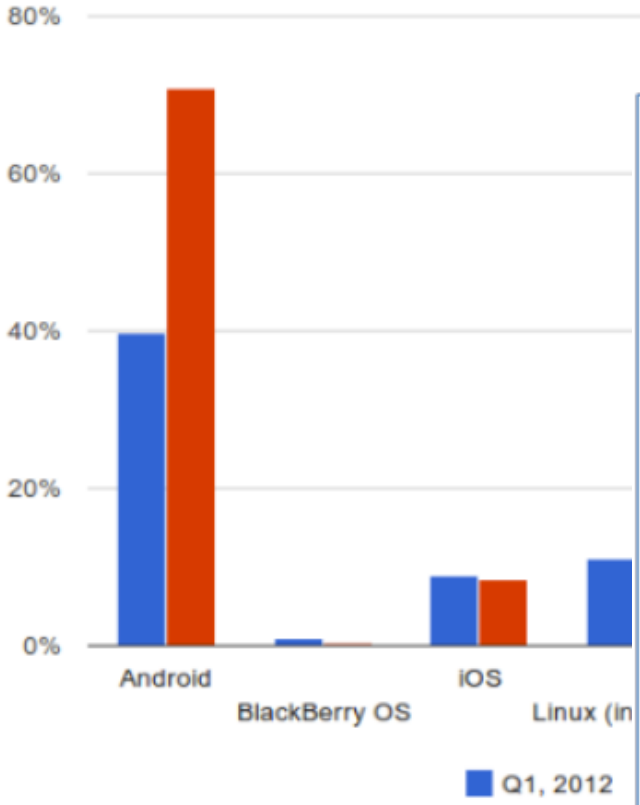
- KR Banker, Ice IX (1800$), TDL, Hiloti, SpyEye, Athena, DoS Pro, V0LK BotNet, BlackOut,...

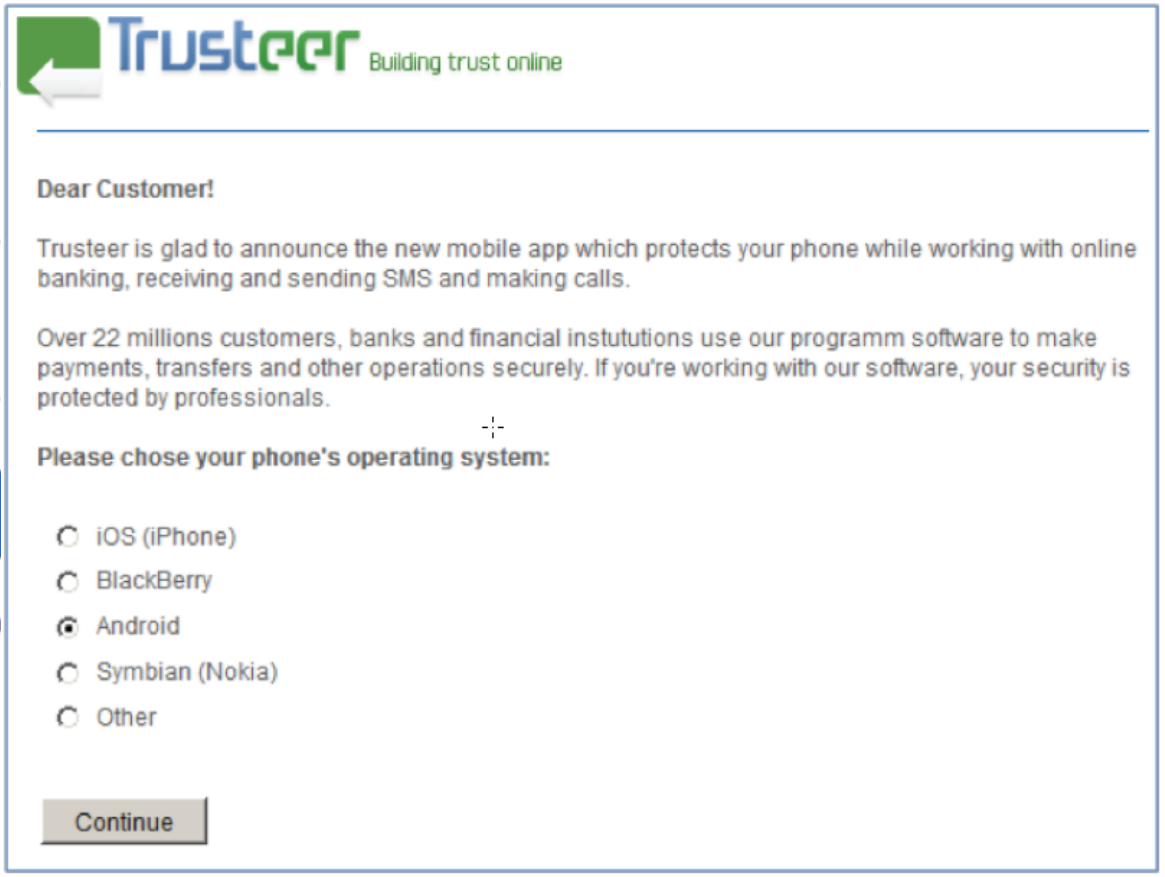




C&C Trojan Mobile framework

- ZitMo, SpitMo, CitMo, CarbMo, Perkele, Pincer,…





Síťové detekční metody

VIRTUALIZACE

ANALÝZA SÍŤOVÉHO CHOVÁNÍ

Virtualizace: SANDBOXING

- Sandboxing
  - Sběr souborů a jejich sledování ve virtuálním prostředí
  - Sledování změn operačního systému a aplikace (registry, knihovny, …)
  - Monitoring chování souboru (PDF, DOC, SWF,…)
  - Nutnost verzování prostředí
  - OpenSource: Cuckoo sandbox
  - http, smtp,
- Výhody
  - Detekce neznámých a cílených malware
  - Jasný přehled o tom co se dělo
  - Zero false positive detekce ☺

Virtualizace: SANDBOXING

- Nevýhody
  - Nedostatky detekce
    - Časové bomby
    - Logické bomby
    - Interakce s uživatelem
  - Nutnost verzování (Acrobat Reader v1, v2, v3, …)
- Na co si dát pozor?
  - Podporované aplikace (Acrobat Reader, MS Office, …), lze přidávat vlastní?
  - Podporované operační systémy (Microsoft, Android, iOS)
  - Podpora komunikačních protokolů

Virtualizace: SHADOW HONEYPOT

- Taint analýza
  - Detekce napadení typu buffer overflow u vnějších služeb (smb, netbios, ntp, rdp, pop3, smtp, http…)
  - Typ buffer overflow only
  - Virtualizace HW registrů (procesoru a paměti)
  - QEMU, ARGOS
- Výhody
  - Detekce neznámých buffer overflow zranitelností v externích službách
  - Využití v projektu (zdroj expertních znalostí)

Behaviorální analýza (NBA, NBAD)

- Analýza síťového chování
  - Filosofie: „Přítomnost malware se projeví na síti“.
  - Nestandardní, anomální komunikace.
  - Různé přístupy a výstupy
- Detekované události
  - portscan, lámání hesel, únik dat, porušení pravidla
  - predikovatelná komunikace
  - …
- OpenSource:
  - BRO IDS
  - nfdump + nfsen + moduly pro specifickou analýzu

Behaviorální analýza (NBA, NBAD)

- Výhody
  - Detekce neznámých a bolestivých útoků
  - Přehled nad chováním sítě a uživatelů
  - Network troubleshooting
  - Široké možnosti využití

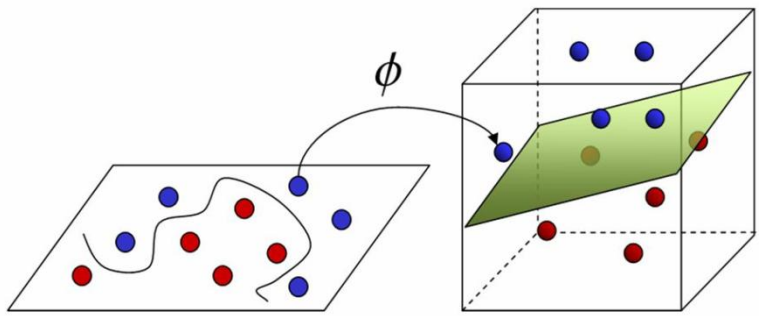
- Nevýhody
  - False positive detekce
  - Omezené možnosti detekce
  - Časově náročná analýza
  - Neefektivní uživatelské rozhraní

Behaviorální analýza

- Zdroj dat (detekční množiny)
  - NetFlow (+DPI) 9 - 20 parametrů
  - Network stream
  - Jiné detekční množiny
    - Moores‘ discriminants (2005) – 280 parametrů (offline)
    - ASNM (2012) - 800/60 parametrů (online)
      - Session based
      - Frekvenční charakteristika spojení
      - Prodlevy a peaky uvnitř flow
      - L4-L7 header informace
      - Kontext toků a událostí

Behaviorální analýza

- Analýza dat
  - Co detekovat (anomálie , podobnost, pravidla, ..)
  - Jak detekovat
  - Pravidla
  - Umělá inteligence: MINDS (2004) -kNN, SVM, …
  - Pokročilé metody
    - Model sítě, zařízení a služeb
    - Predikovatelné chování
    - Podobnost chování
    - Fůze více metod



Behaviorální analýza

- Prezentace výsledků
  - Předdefinované filtry
  - Přímé filtrování
  - Manažerské výstupy
- Korelace dat
  - vstupy dalších aplikací
  - SNMP, IDS, Antivirus, proces monitor, …
- Další využití
  - Fraud detection
  - Application/Network Perforamance monitoring

End Point detekce

- Virtualizace
  - Bromium
  - Izolace potenciálně škodlivého kódu
- Behaviorální analýza
  - Analýza chování systémových volání

SECURITY 2014

22. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

Michal Drozd

TrustPort a.s.

michal.drozd@trustport.com