Malicious Softwares:

Conosciamoli meglio...

PLAYHACK.

Chi sono?

Graziano `emdel` Mariano

Ho conseguito ad Ottobre la laurea triennale in **Ingegneria delle Telecomunicazioni** presso il Politecnico di Torino ed attualmente, presso lo stesso ateneo, seguo il corso di laurea specialistica in Ingegneria Telematica. Mi occupo di sicurezza informatica, nello specifico di *offensive coding* e *mobile security*, portando avanti ricerche all'interno del collettivo Playhack.net Security.

Introduzione

MALWARE (MW)

Definizione: - Codice con intenzioni malevole
[**MAL**icious soft**WARE** (SW)]
- Termine generico → molta confusione

Tipologie: - Virus
- Worms
- Trojan horses
- Backdoors
- Spyware etc…

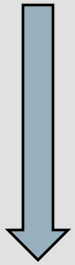
Vediamo di capirci qualcosa…

Virus

Definizione: Programmi che si autoreplicano

Motivo: Cyber-vandalism

Cyber-Vandalism: - Blocco del sistema
- Cancellazione risorse
- Visualizzazione messaggi



Sono la forma più antica di MW → utente

Come: Si inietta in un eseguibile e lentamente si duplica in altri → infezione altre macchine

Worm

Definizione: Simile ai Virus → si autoreplica

Differenze:

Tipo	Replica	Utente
Virus	File-File, Exe-Exe	Si
Worm	Internet	No

Worm non infetta altri file

Vantaggi: Diffusione esponenziale in poco tempo

Come: Ricerca ⟺ Infezione

Contagio: Diverse tecniche (vulnerabilità, email, IM)

Modalità contagio

- **Vulnerabilità** (Conficker (RPC))

- **E-Mail:** Manda copie di sé a tutti i contatti
- **P2P** (Emule, Limewire, DC): Si copia nella cartella condivisa

- **IM** (Skype, MSN): Cerca di inviarsi a tutti i contatti
- **IRC** (mIRC, XChat): Si invia sul network IRC
- **Dispositivi Mobili:** Aggira difese aziendali (si copia in tutte le risorse di rete accessibili)

Trojan Horse

Timeo Danaos et dona ferentur – Laocoonte

Definizione: Il cavallo di Troia diventa un programma

Cosa: MW appare innocuo eseguendo parallelamente all'attività di "remote control" delle funzioni normali (mostrare una Immagine, riprodurre un file audio etc..)

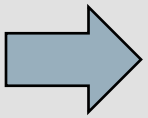
Come: - Inserire codice maligno in SW benigno

- Creare l'eseguibile con estensione innocua (.mp3, .jpg, .avi etc..)

Backdoor

Definizione: MW che crea un **Canale di Accesso** per l'attaccante sul PC vittima.

Motivo: Garantirsi un accesso sui computer infetti

Come: - Spesso inserite nel sorgente di SW (poca attenzione dei vendor)  (Mancanza Code Review)

- Meno praticabile nell'Open Source per la disponibilità libera dei sorgenti

Spyware/Adware

Definizione: SW per spiare/pubblicità/panico.

Adware: (*advertising-supported software).* Fanno apparire sul nostro pc popup pubblicitari o banner. Prendono informazioni sulle nostre abitudini da navigatori e le usano per mandarci pubblicita' mirata. (Licenza d'uso → Software gratuito)

Spyware: Come adware ma senza consenso dell'utente

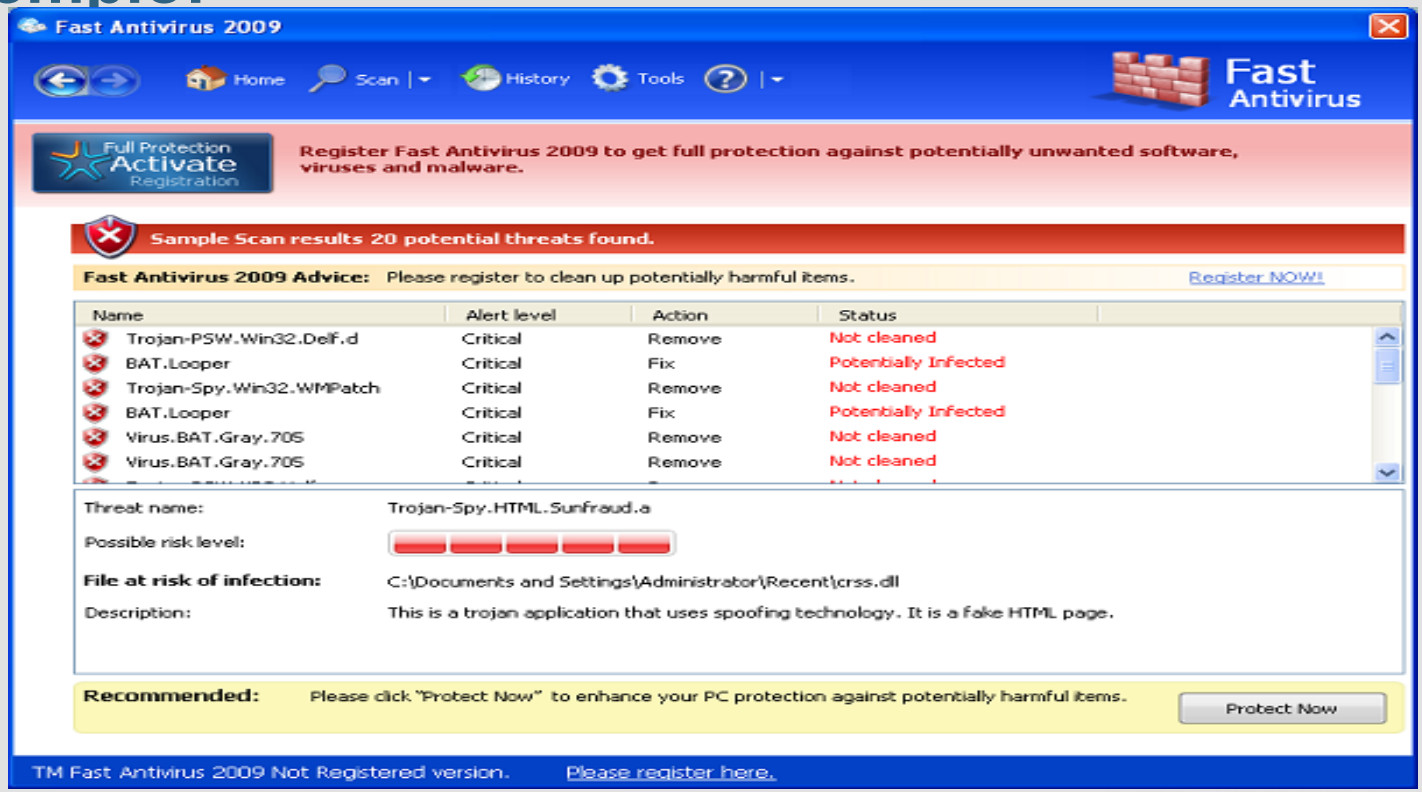
(Redirecting su siti di phishing, Organizzazioni criminali (PIN etc))

Problemi: Male implementati → Riducono prestazioni

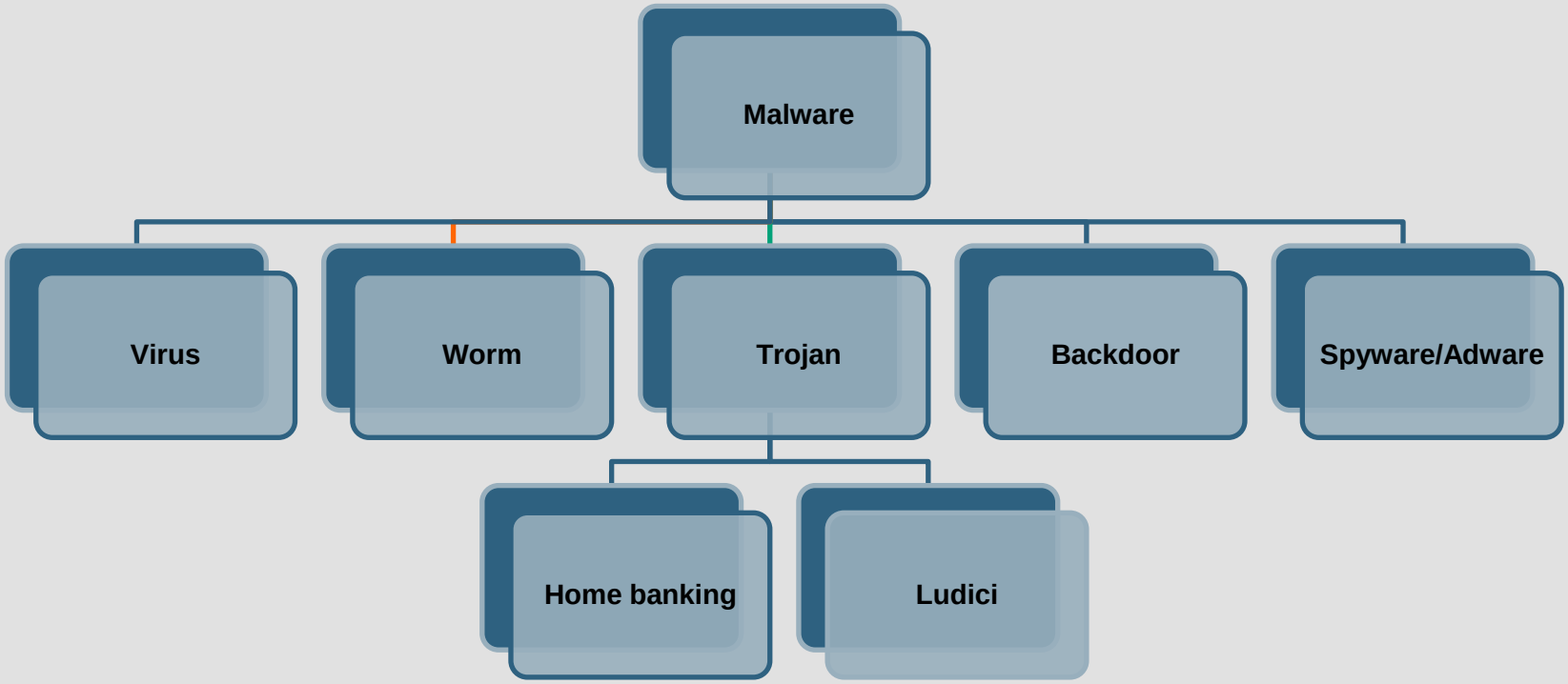
Scareware

Definzione: Sfrutta trucchi psicologici per la compromissione della macchine

Esempio:



Riassunto



Evoluzione

Prima: Virus come quelli biologici
- malattia
- infezione

Oggi: Senza sintomi
- nascosti
- informazioni

polimorfismo

Falsi miti: 15enne che crea virus → Fine vandalismo

Fine fun

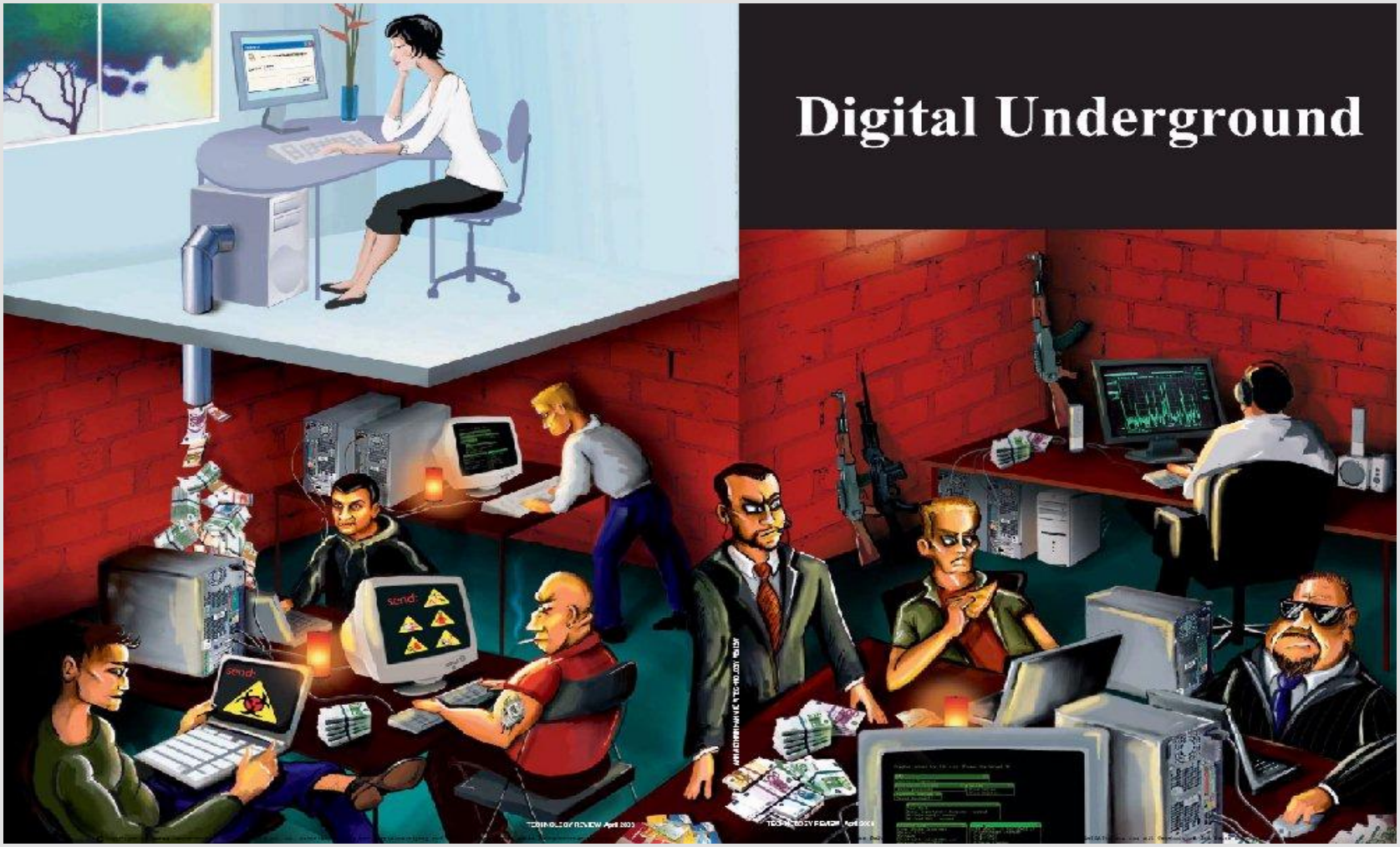
Realtà: Organizzazioni criminali → Inizio profit

Mercato informazioni

↓

industria criminale

Cybercrime



L’industria

Il fatto: Mercato nero underground

Oggetto: Raccolta informazioni e credenziali

Fine: Lucro

Offerta: Affitto Botnet, Servizio Hosting dedicati a distribuzione MW, campagne phishing, spam pedo/pornografia.

Nota: Sottile linea tra cybercrime e cyberterrorismo (in alcuni stati)

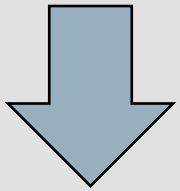
Modus Operandi

VELOCITA'

- 6 giorni dopo una falla di sicurezza c'e' il relativo exploit
- Poche ore per infettare i sistemi con quel bug

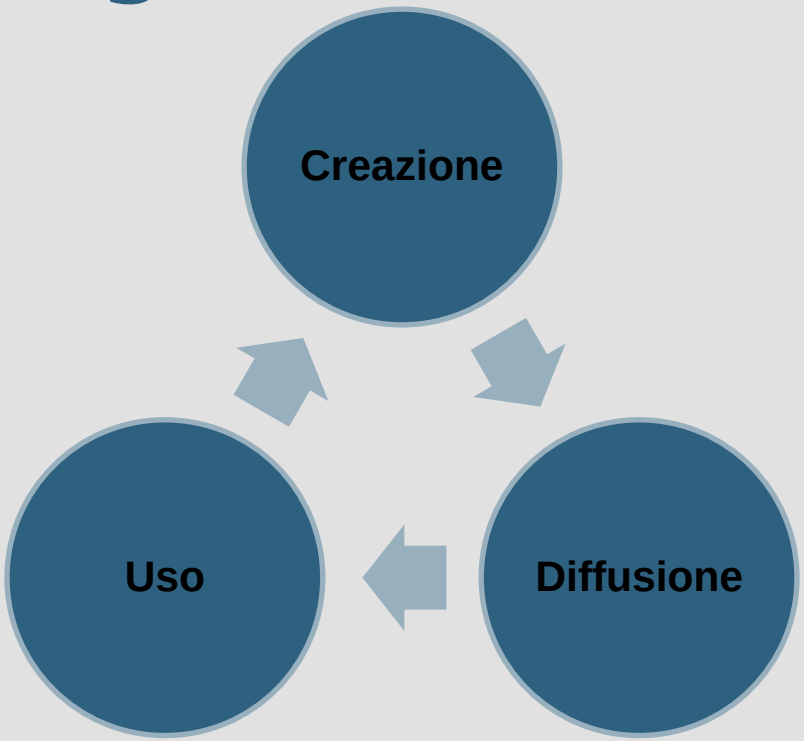
RICERCA

- Tecniche di hiding sofisticate (Rootkit)
- Bug Hunting



Professionisti

Organizzazione



Ogni fase e’ fatta da cellule diverse (Gerarchia)

Virus 2008 creati per la vendita (Mercato)

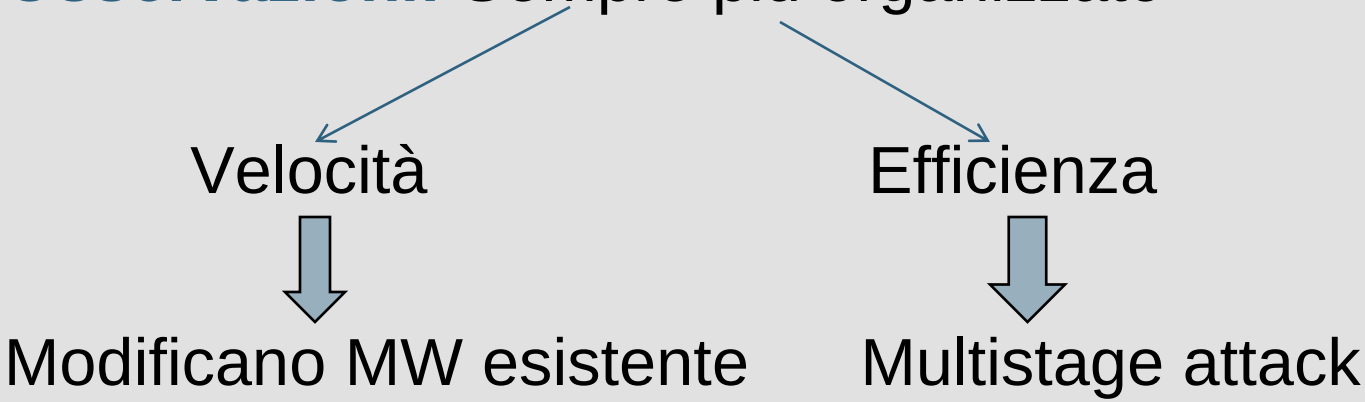
Mercato

Come: Monitorando la proliferazione di MW

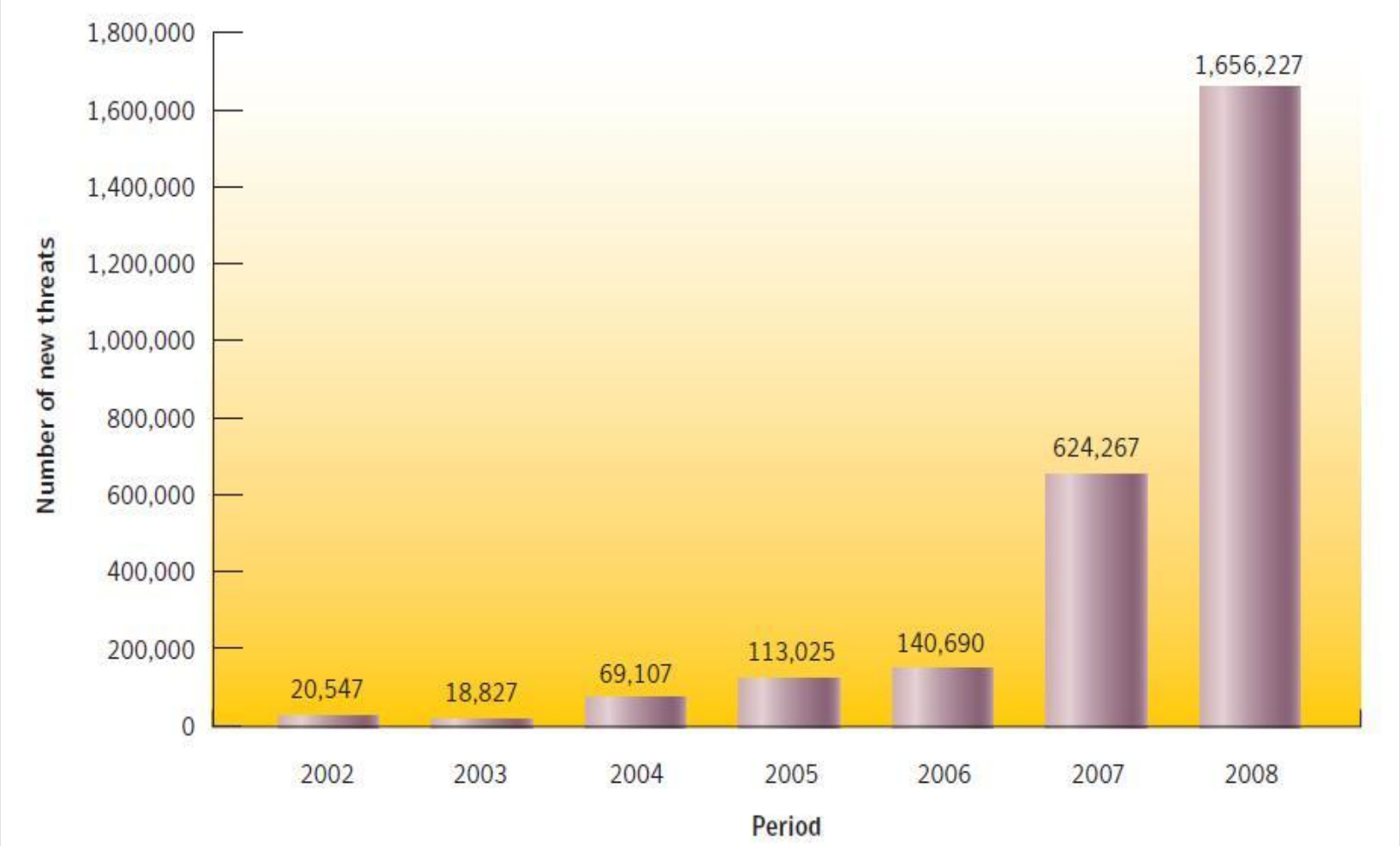
Numeri: 1,6M nuovi MW nel 2008 (Symantec)

Aumento del 265% (rispetto 2007)

Osservazioni: Sempre più organizzato



Crescita

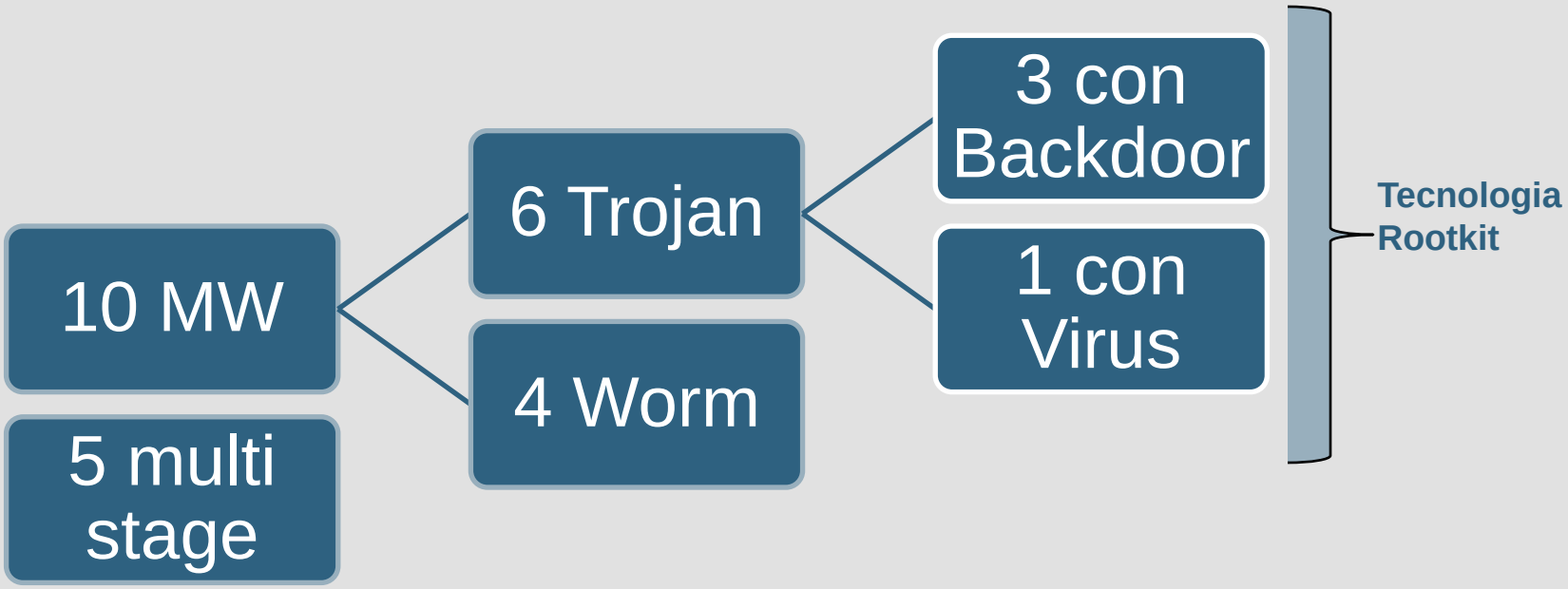


Complessità

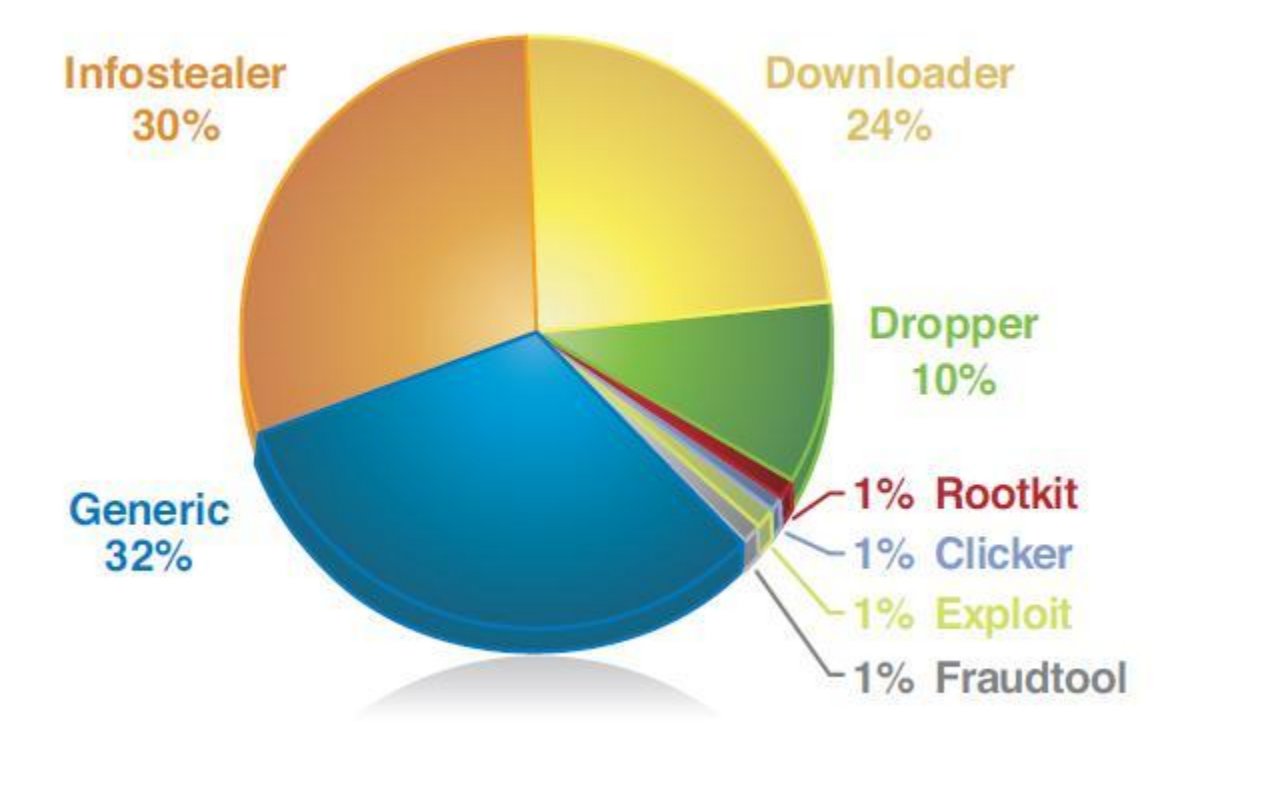
Il fatto: Nuovi MW sempre più complessi

Tendenza: Mix delle varie tipologie

Esempio: (Top Ten Symantec)



Quanti Trojan…



Termine generico → confusione

Multistage Attack

Definizione: Tipo di attacco diviso in vari stadi

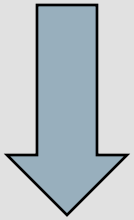
Stadi:

Profilazione vittime

Compromissione iniziale: Si fa un profilo del PC

Primo invio: Dal profilo si riceve il relativo trojan

Ricezione di altro MW (spesso adware)



Tendenza: Automatizzare, Kit, ExploitPack

Esempio:

Vittima non interessante → No InfoStealer

→ Sì Trojan che manda spam

Danni & costi

Tipologie: - Diretti
- Indiretti

Diretti: Disinfestazione → Team specializzato
Downtime → Forza lavoro ferma
Costi prevenzione

Indiretti: No vandalismo → Guadagno
Nascosti → Keylogger etc

Indiretti > Diretti

Rimedi

Sicurezza rete aziendale:

- Non sufficiente sicurezza perimetrale (con tutte le appliance)

MA

- Distribuzione MW è via Web → Utente NON rete

E' NECESSARIA

- Sicurezza granulare → Singole postazioni
- Educare dipendenti → Consapevolezza in navigazione
- Auditing della propria infrastruttura

Links Utili

Generici:

- ✓ www.playhack.net
- ✓ www.evilfingers.com

Trends ed articoli interessanti:

- ✓ http://www.kaspersky.com/it/reading_room
- ✓ http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf
- ✓ http://www.eset.com/threat-center/blog/
- ✓ http://www.bizeul.org/files/RBN_study.pdf

Ringraziamenti

In ordine random:

- Claudio “Nex” Guarnieri
- Davide “Ocean” Quarta
- Swirl
- Evilcry
- Insomniac

Q&A

PLAYHACK.

Contatti

E-mail: emdel@playhack.net

Siti: http://www.playhack.net
http://mariano-graziano.llab.it

Slide reperibili su:

http://files.playhack.net/slides/