

# Attack by custom malware

A.K.A - advanced persistent threat (APT)

New generation  
August Penguin 2013



# About me

Shaya Feedman :: shaya.feedman@gmail.com :: 054-4881601

Age 22

Professional experience:

- self-sufficient Web-Developer for over five years.

- Lecturer and tutor of network, wireless communication and Operational systems at IDF for three years.

- Security assessments and application layer penetration testing as a freelance for about 2 years.

- Information Security solutions integrator and Pentester for about a year.

Specializing in:

- Data networking.

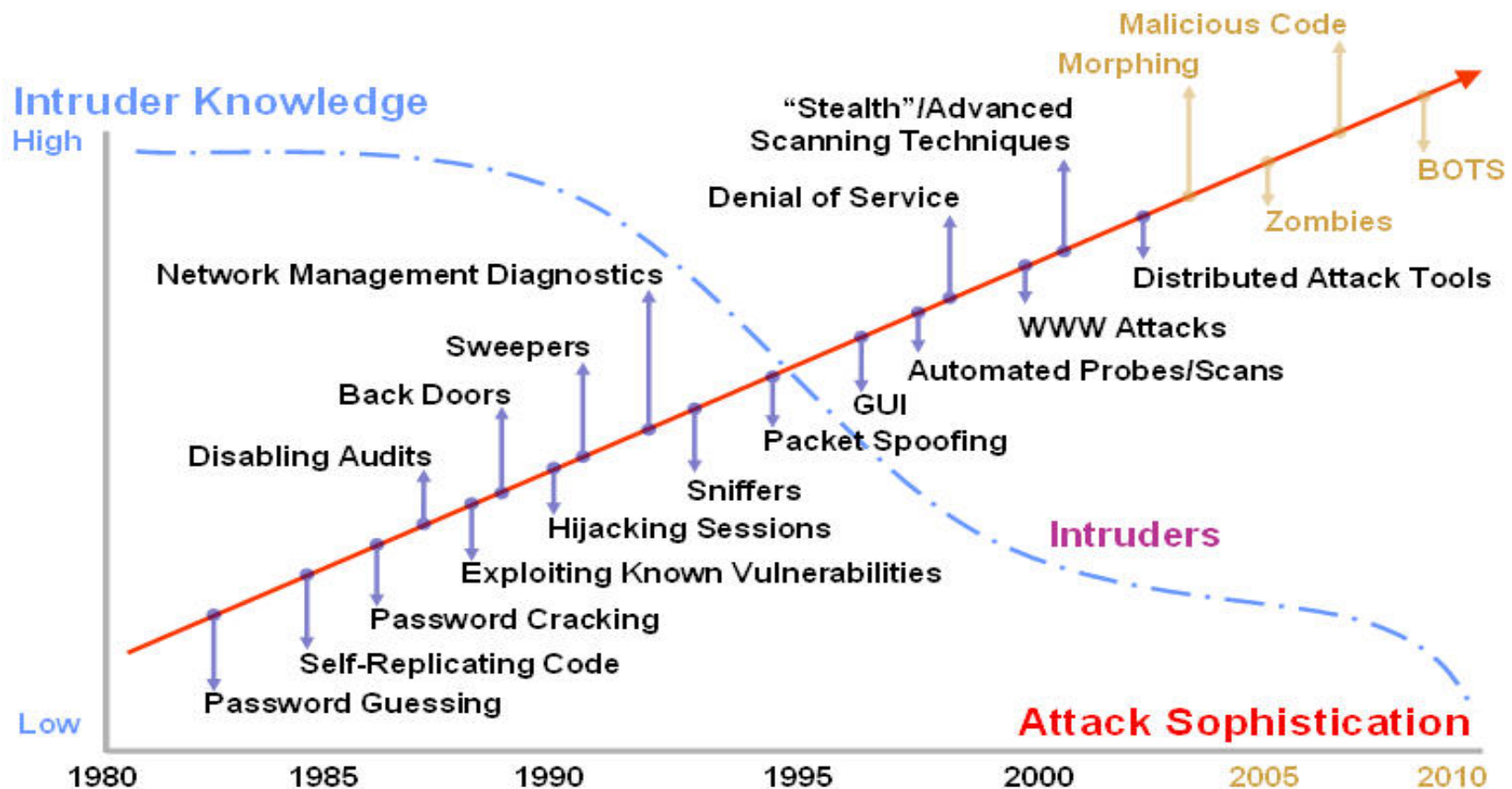
- Information Security.

- Penetration Test.

- Writing and analysing code.

- General Hacking.

# Little bit about attack's history



Sources: Carnegie Mellon University, 2002 and Idaho National Laboratory, 2005

# And... T0Day !!



# What the f\*ck is Custom Malware ?!



**2013**

- Apple
- Central Hudson Gas & Electric Inc.
- Crescent Health
- Walgreens
- Drupal
- Florida Courts
- Facebook
- Living Social (50,000,000)
- Nintendo
- South Africa police
- Twitter
- Ubuntu
- Washington State court system
- TerraCom & YourTel
- Scribd
- Yahoo! Japan (22,000,000)
- Evernote (50,000,000)
- Formspring
- Militarysingles.com
- New York State Electric & Gas
- Oregon Department of Motor Vehicles
- UbiSoft ("unknown")
- Three Iranian banks
- US Army
- University of Wisconsin - Milwaukee
- Stratfor
- US Law Enforcement
- Sutter Medical Foundation
- Writerspace.com
- Blizzard (14,000,000)
- Emory Healthcare
- LinkedIn, eHarmony, Last.fm
- Sega
- Medicaid
- KT Corp.
- Sony Online Entertainment
- Global Payments
- California Department of Child Support Services
- Accendo Insurance

**2012**

- Apple (12,367,232)

**2011**



# Solutions ?

- AntiVirus - X
- Firewall - X
- IPS - really ? - X
- Custom OS and Application - X \ V
- Anomaly Detection - Yeha... but...
- Any ideas ?

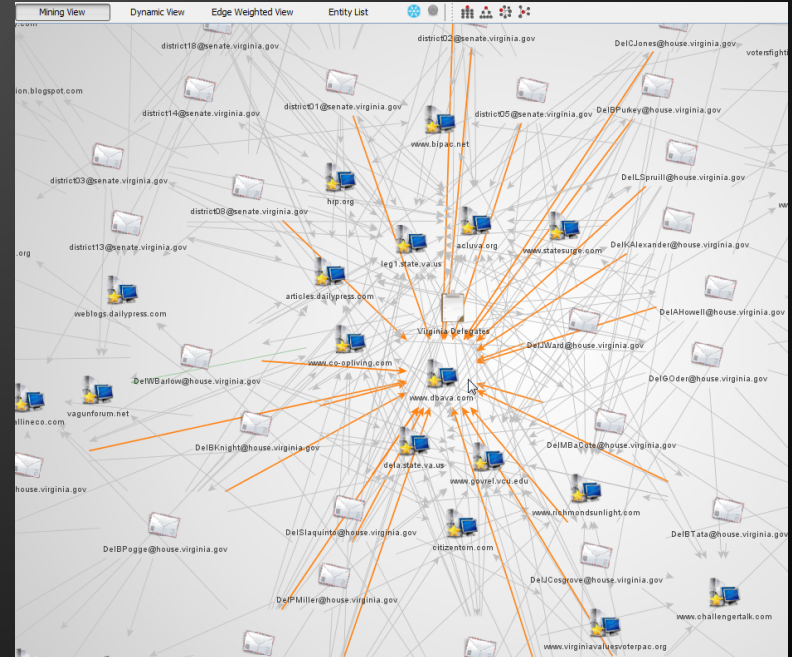
# Learn Your Target





# How To Do it ?

1. Scans.
2. Enumeration.
3. Harvesting.
  - \* Foca.
  - \* Maltego.



# Create scenario attack

- Choose your way
  - Use (un)know tools ?
  - Create script ?
  - Use exploits ?
- Clear !
  - backyard, logfile, port used, registry and any you touch.
- Think different !
  - or leave it...

# So... Really, Thank YOU !

