Imperial College
London

Network and Web Security

Malware

Dr Sergio Maffeis
Department of Computing
Course web page: https://331.cybersec.fun

MALicious softWARE

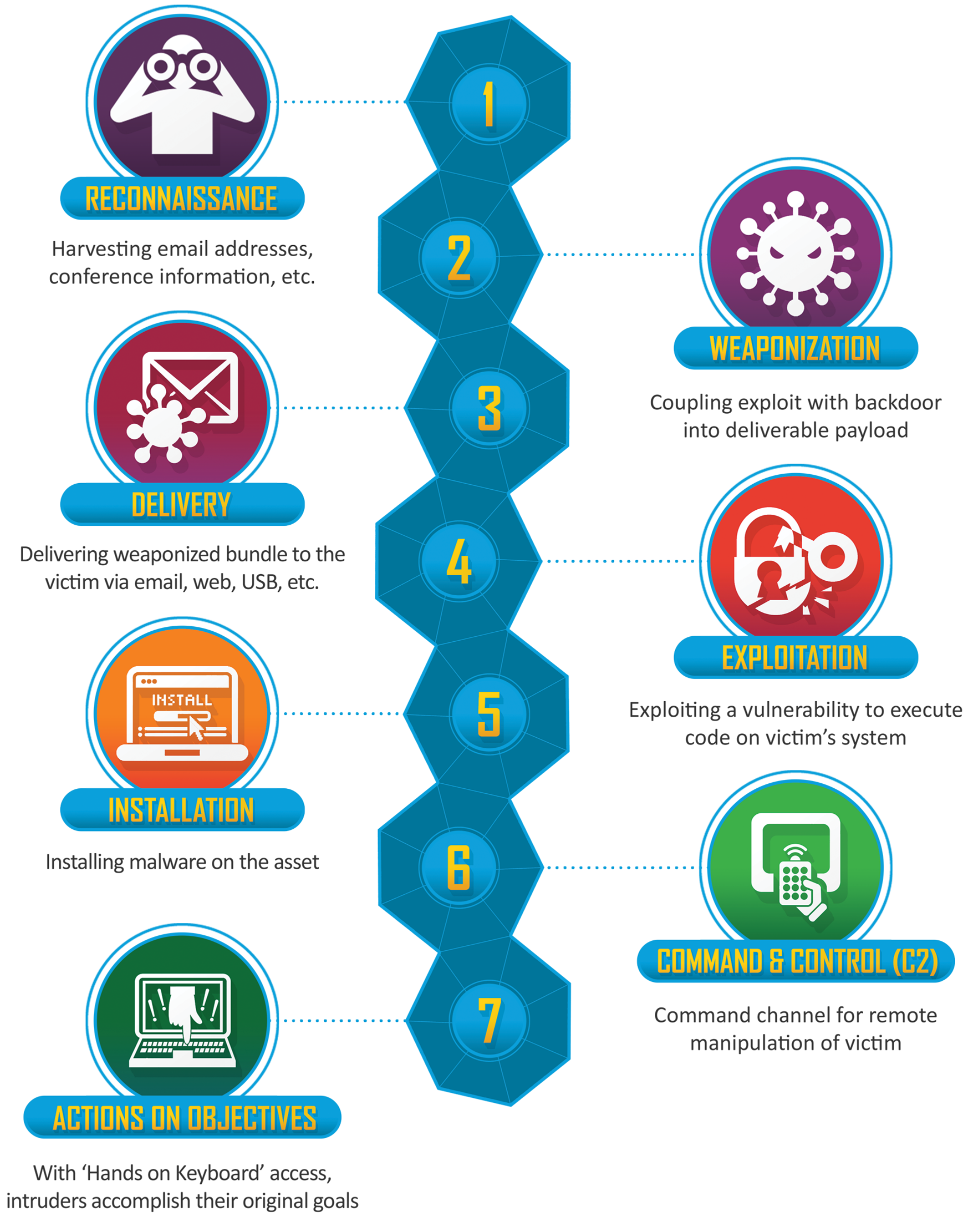
- By infection vector
  - **Virus**: malicious code that copies itself into existing programs
  - **Worm**: self-replicating program that infects other machines over the network or removable devices
  - **Trojan**: malicious program that provides some useful service in order to pose as legitimate
  - **Spoofed software**: fake antivirus or fake software updates
  - **Drive-by download**: code executed by visiting a malicious website
- By purpose
  - **Rootkit**: modifies the OS to hide malicious activity of itself or other malware
  - **Backdoor**: opens a network connection for repeated access by the attacker
  - **RAT**: remotely control the machine in a targeted attack
  - **Botnet**: recruit the machine into a botnet
  - **Keylogger**: log keystrokes to steal user credentials
  - **Spyware**: steal sensitive documents
  - **Ransomware**: block access to machine or data until ransom is paid
  - **Cryptominer**: mines cryptocurrency using victim resources
  - **Adware**: displays intrusive advertisement

Malware attributes

- Format
  - Injected code added to a legitimate program (virus)
  - DLL that is called by a legitimate program (fake software updates)
  - Script run by an application (macro virus)
  - Standalone executable that is run by the user or automatically by the system (trojan)
  - Malicious code loaded in volatile memory only (fileless malware)
- Propagation
  - Installed by the attacker
    - Self-replication (worm)
    - Exploiting vulnerabilities (drive-by download)
  - Installed by the user
    - Social engineering (fake antivirus)
    - Compromised certificate (fake software updates)
- Privileges
  - Root: it *owns* the machine (rootkit)
  - User: can do limited damage (spyware), but can also attempt elevation of privilege to become root

APTs

- APTs: Advanced Persistent Threats
- Targeted attacks
  - Aim to infect high-value victims
    - Company executive, politician, activist, nuclear power plant workstation
  - Specific to the victim, often human-driven
  - Compromise intermediate systems in order to reach victim host
- Avoid detection
  - Use of rootkits to hide presence
  - Exfiltrate large dataset a bit at a time using covert channels
- Exploit target over time
  - Wait for interesting information to enter the system
  - Retain access in order to exploit system at a later date



1 RECONNAISSANCE

Harvesting email addresses, conference information, etc.

2 WEAPONIZATION

Coupling exploit with backdoor into deliverable payload

3 DELIVERY

Delivering weaponized bundle to the victim via email, web, USB, etc.

4 EXPLOITATION

Exploiting a vulnerability to execute code on victim's system

5 INSTALLATION

Installing malware on the asset

6 COMMAND & CONTROL (C2)

Command channel for remote manipulation of victim

7 ACTIONS ON OBJECTIVES

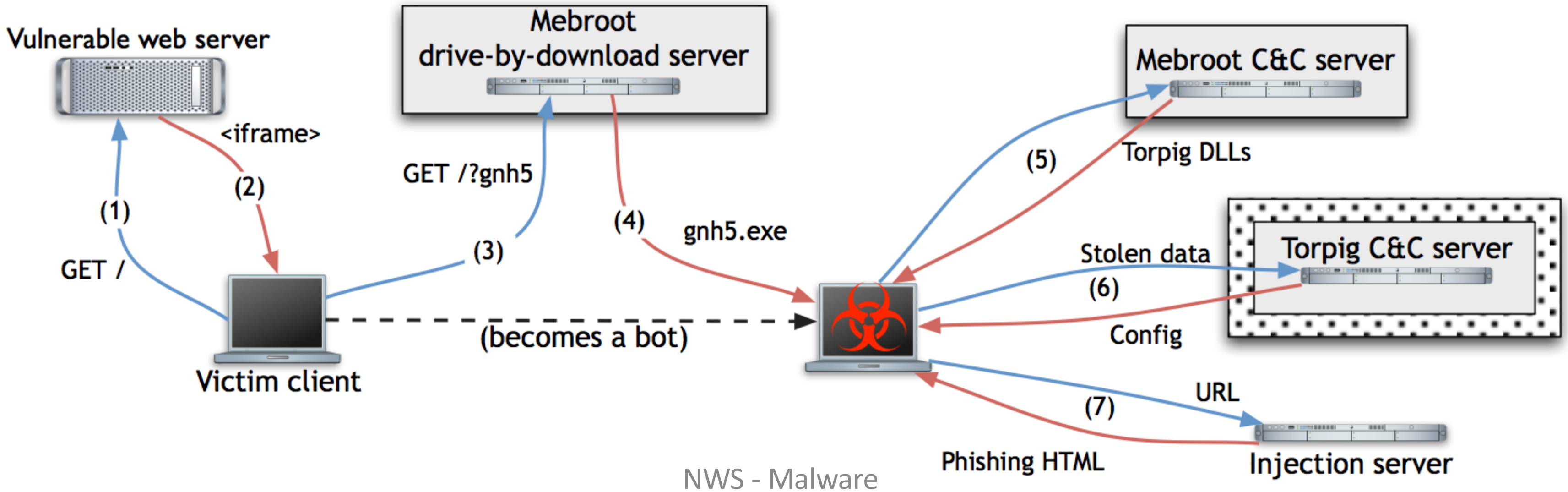
With 'Hands on Keyboard' access, intruders accomplish their original goals

Lockheed Martin's Cyber Kill Chain® framework

Botnets

- Generic attacks infect as many machines as possible
  - Deliver low-cost attacks with low chance of success
  - Value in numbers: build a ***botnet***
- One attacker (the *botmaster*) can control hundred of thousands of infected machines (*bots*)
- Bots connect to a *command-and-control (C&C)* server to receive instructions on what to do: code to execute, attack parameters
- Sophisticated *C&C* architectures
  - Peer-to-peer, hierarchical, star topology
  - Encrypted and stealthy communication of commands and results
  - Botmaster server may keep changing IP to avoid detection (fast flux/domain flux)
- Recommended reading: researchers from UCSB infiltrated a botnet to study its behaviour

(Stone-Gross et al., CCS 2009)

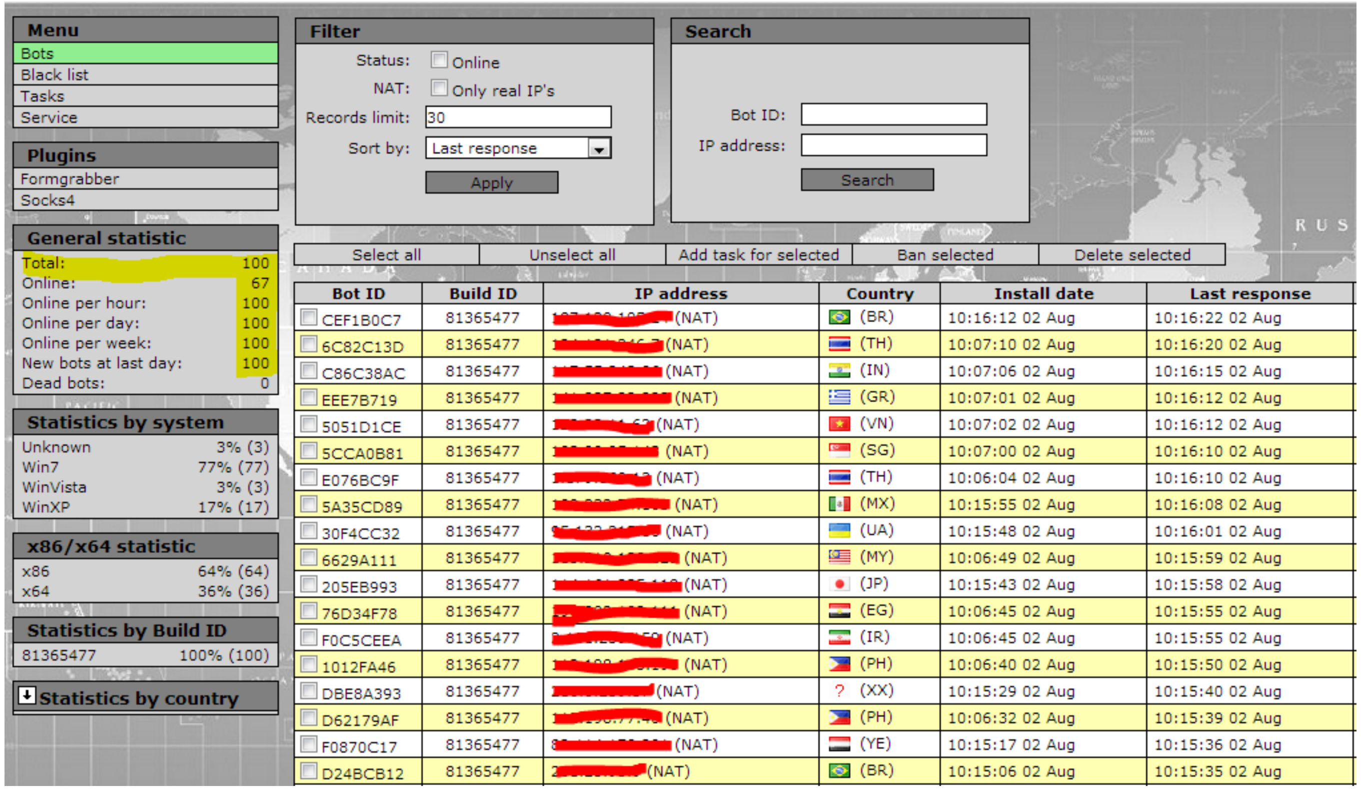


Botnet goals

- **Data theft**: steal sensitive data from users
  - Credit card numbers
  - Passwords (email, social networks, gaming)
- **Spam**: deliver unrequested email
  - Advertising illegal, counterfeit goods
  - Spread malicious attachments
  - Fraud, deception: romance scams, phishing
- **Distributed denial of service** (DDOS): flood web servers with requests
  - Take down servers or slow them down significantly
  - Blackmail companies under attack
  - Disrupt communications on the target network
- **Credential stuffing**: attempt to login with leaked credentials to see which works
- **Card cracking**: bruteforce missing information for card payments
- **Network scanning**: attempt to probe other hosts
- **Click fraud**: generate advertising revenue from bogus user clicks
  - Startup from Imperial students, bought by Google: http://www.spider.io
- **Cryptojacking**: use bot resources to mine cyptocurrencies

The botnet economy

- Botnets have their own sophisticated economy
  - Botmaster can rent spare capacity to other criminals on the market
    - $1 = 10 machines in the US, 100 machines in Asia
  - Very organized: 24/7 technical support, training, complaints department..



Status: □ Online
NAT: □ Only real IP's
Records limit: 30
Sort by: Last response

Bot ID:
IP address:

General statistic

Total:	100
Online:	67
Online per hour:	100
Online per day:	100
Online per week:	100
New bots at last day:	100
Dead bots:	0

Statistics by system

Unknown	3% (3)
Win7	77% (77)
WinVista	3% (3)
WinXP	17% (17)

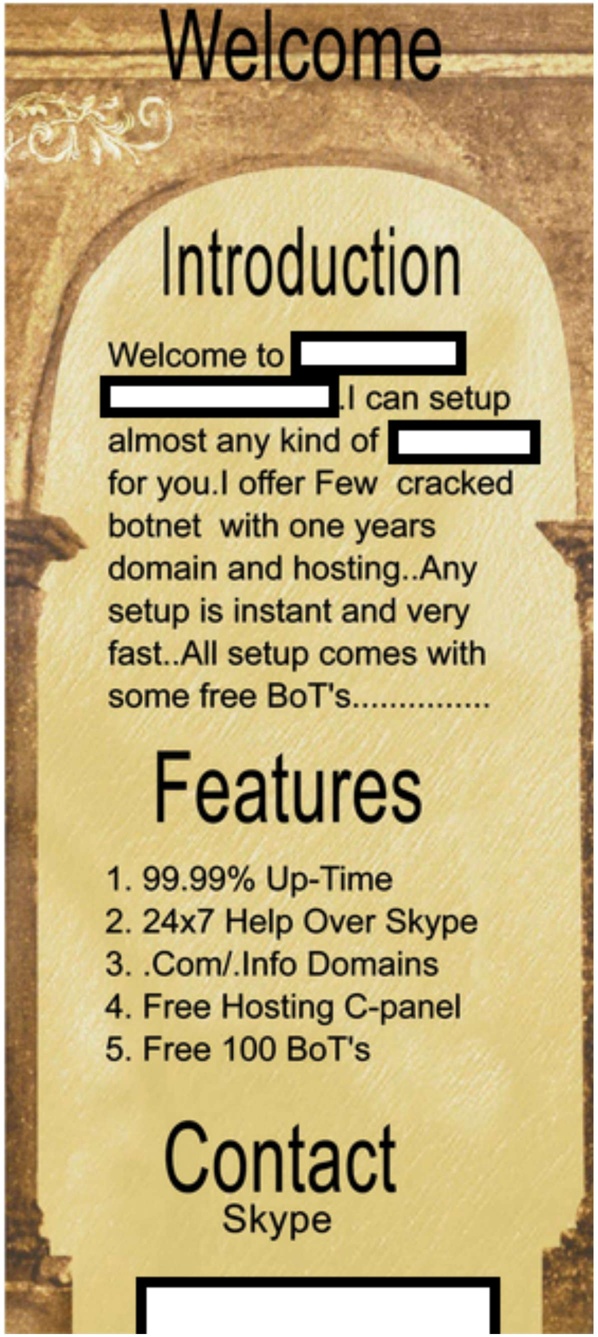
x86/x64 statistic

x86	64% (64)
x64	36% (36)

Statistics by Build ID

81365477	100% (100)

Bot ID	Build ID	IP address	Country	Install date	Last response
□ CEF1B0C7	81365477	[redacted](NAT)	(BR)	10:16:12 02 Aug	10:16:22 02 Aug
□ 6C82C13D	81365477	[redacted](NAT)	(TH)	10:07:10 02 Aug	10:16:20 02 Aug
□ C86C38AC	81365477	[redacted] (NAT)	(IN)	10:07:06 02 Aug	10:16:15 02 Aug
□ EEE7B719	81365477	[redacted] (NAT)	(GR)	10:07:01 02 Aug	10:16:12 02 Aug
□ 5051D1CE	81365477	[redacted](NAT)	(VN)	10:07:02 02 Aug	10:16:12 02 Aug
□ 5CCA0B81	81365477	[redacted] (NAT)	(SG)	10:07:00 02 Aug	10:16:10 02 Aug
□ E076BC9F	81365477	[redacted] (NAT)	(TH)	10:06:04 02 Aug	10:16:10 02 Aug
□ 5A35CD89	81365477	[redacted] (NAT)	(MX)	10:15:55 02 Aug	10:16:08 02 Aug
□ 30F4CC32	81365477	[redacted] (NAT)	(UA)	10:15:48 02 Aug	10:16:01 02 Aug
□ 6629A111	81365477	[redacted] (NAT)	(MY)	10:06:49 02 Aug	10:15:59 02 Aug
□ 205EB993	81365477	[redacted](NAT)	(JP)	10:15:43 02 Aug	10:15:58 02 Aug
□ 76D34F78	81365477	[redacted] (NAT)	(EG)	10:06:45 02 Aug	10:15:55 02 Aug
□ F0C5CEEA	81365477	[redacted] (NAT)	(IR)	10:06:45 02 Aug	10:15:55 02 Aug
□ 1012FA46	81365477	[redacted] (NAT)	(PH)	10:06:40 02 Aug	10:15:50 02 Aug
□ DBE8A393	81365477	[redacted](NAT)	? (XX)	10:15:29 02 Aug	10:15:40 02 Aug
□ D62179AF	81365477	[redacted] (NAT)	(PH)	10:06:32 02 Aug	10:15:39 02 Aug
□ F0870C17	81365477	[redacted] (NAT)	(YE)	10:15:17 02 Aug	10:15:36 02 Aug
□ D24BCB12	81365477	[redacted](NAT)	(BR)	10:15:06 02 Aug	10:15:35 02 Aug



Welcome

Introduction

Welcome to [redacted] [redacted].I can setup almost any kind of [redacted] for you.I offer Few cracked botnet with one years domain and hosting..Any setup is instant and very fast..All setup comes with some free BoT's...............

Features

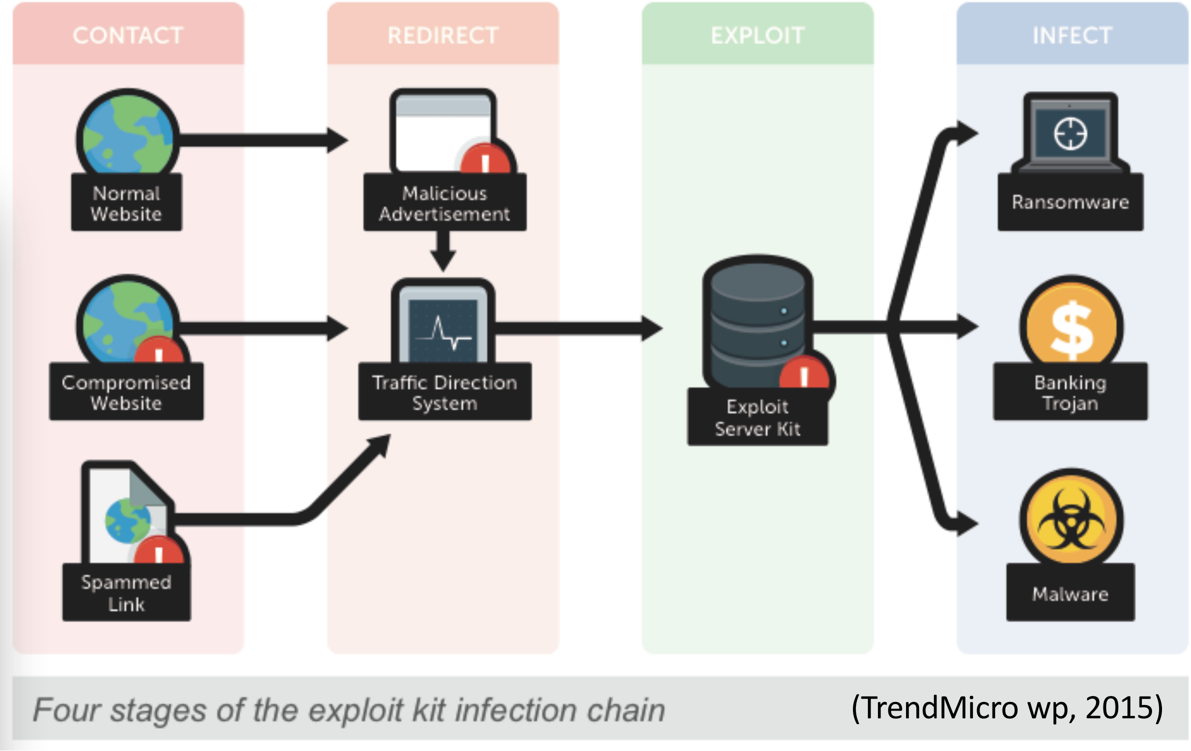
1. 99.99% Up-Time
2. 24x7 Help Over Skype
3. .Com/.Info Domains
4. Free Hosting C-panel
5. Free 100 BoT's

Contact

Skype

[redacted]

Commoditised malware



Four stages of the exploit kit infection chain (TrendMicro wp, 2015)

- Exploit kits: “commercial” malware toolkits sold or rented out to criminals
  - Capabilities: automated vulnerability analysis, exploitation and post-exploitation
  - Include Anti-Virus evasion techniques
    - Exploiting CVE-2013-7331 to find files in the system: kl1.sys => Kaspersky AV installed
  - Operator needs to subscribe to traffic from spam and malicious ads
  - Comes with administration console fine tune parameters, select victims
    - Users with a certain demographic, from a certain geographical area

Malware analysis

- Samples are captured
  - Cleaning up after an infection
  - Running *honeypots*: intentionally vulnerable machines that attract attacks
- Look for effects on storage, system settings, network traffic
- Often analysis is done in a VM sandbox
- Challenges
  - Sometimes hard to trigger malicious behaviour
  - Malware can try and kill logging processes and IDSs in the guest OS
  - Approx 16% of malware detects virtualization and behaves differently

Malware detection

- Extract *signatures* from analysed malware samples
- Static signatures
  - Sequences of bytes typical of the malware code
  - Motivated by speed and portability
  - Collecting millions of signatures is also good for Antivirus marketing
    - Moral hazard
  - Evasion
    - *Metamorphic* malware: samples are made artificially different from each other using different obfuscation parameters
    - *Crypting* services scan existing malware and against malware detection services, and transform it (encryption, obfuscation) until it is no longer detected: *FUD* (**f**ully **u**n**d**etctable malware)
- Dynamic signatures (behavioural analysis)
  - Monitor host for patterns of system calls typically made by malware
    - Read file, open network connection, send data, …
  - Evasion
    - Malware mixes malicious behaviour with spurious legitimate behaviour

Malware prevention

- Defenses
  - Antivirus: scan existing and downloaded files for static signatures
  - End-Point Protection (EPP): monitor host for dynamic signatures
  - Browser-deployed blacklists: prevent access to web pages known to host phishing and malware
    - Google Safe Browsing
  - Network based filtering based on Cyber Threat Intelligence feeds
    - https://abuse.ch, CIRCL, Facebook Threat Exchange, …
- Signatures and blacklists are based on previous infections or proactive threat hunting
  - Either way, the attacker gets a window of opportunity before detection
- Prevention
  - Educate humans to avoid direct installs
  - Update and patch software in response to vulnerability disclosures
    - Most malware uses known vulnerabilities from CVE database
    - Although “serious” malware can contain zero-days (Stuxnet had 5!)
  - Research on **Certified secure systems**
    - Vision*: hardware and software should come with proof of correctness and/or security*
    - Harvard, Upenn, MIT, INRIA, NICTA, Microsoft Research, etc.
    - Imperial’s contribution: JSCert, RIAPAV/RIVESST