
AV is Dead!
Is AV Dead?
ROOTCON
Hacker Conference

"There is no algorithm that can perfectly detect all possible computer viruses."

Fred Cohen, 1987
Pioneer Computer Virus Technology
And Defense

Virus

- Virus is an executable or piece of code that has the capability to replicate and attach itself onto target file

Malware

- Is term used to denote malicious software, including but not limited to worms, Trojans, ransomware and virus
- Often referred to, by some people, as “virus”

Main questions to be answered

WHO

Who are the ones that are saying AV is dead

WHY

Why are they saying that AV is dead

WHAT

What should we learn from all of this

Agenda

- *Historic Malware Facts: A Never Ending War*
- *Proactive Development Of New Weapons*
- *Being Opinionated on Data*
- *Derivation*

AV - Anti-Virus

- *Software originally designed to detect and remove computer virus*
- *Initially based on signature detections and blacklisting technique which uses scan-detect-protect-clean paradigm*
- *Although developed during the 80s, non-IT people are still used to the term AV (antivirus) to refer to the software they use to protect against malware*

A Never Ending War

Virus Worms Trojans

- Encryption, Polymorphism, Metamorphism
- Packing, Armouring, Protectors
- Anti-emulation, anti-debugging

Rootkit, Exploits

- Botnet
- Vulnerability exploitation
- Dormancy
- Stealth

Hijacker Adware Spyware Rogue AV

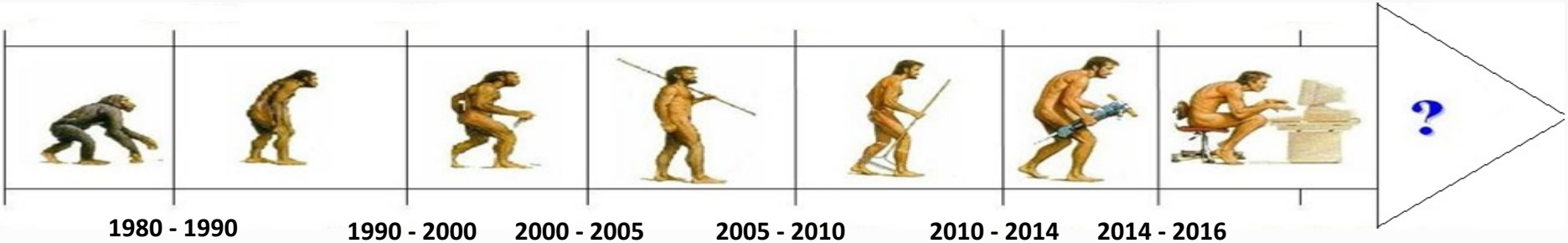
- EULA
- Lawsuits, greyware

Ransomware APT

- Fast flux
- Rapid variance generation
- More laser focused targeted attacks

Malware

- Social engineering
- Stolen digital signatures



1980 - 1990 | 1990 - 2000 | 2000 - 2005 | 2005 - 2010 | 2010 - 2014 | 2014 - 2016

- Signature based detection
- Hashing
- Heuristic
- Emulation
- Intelligent scanning
- Generic unpacking

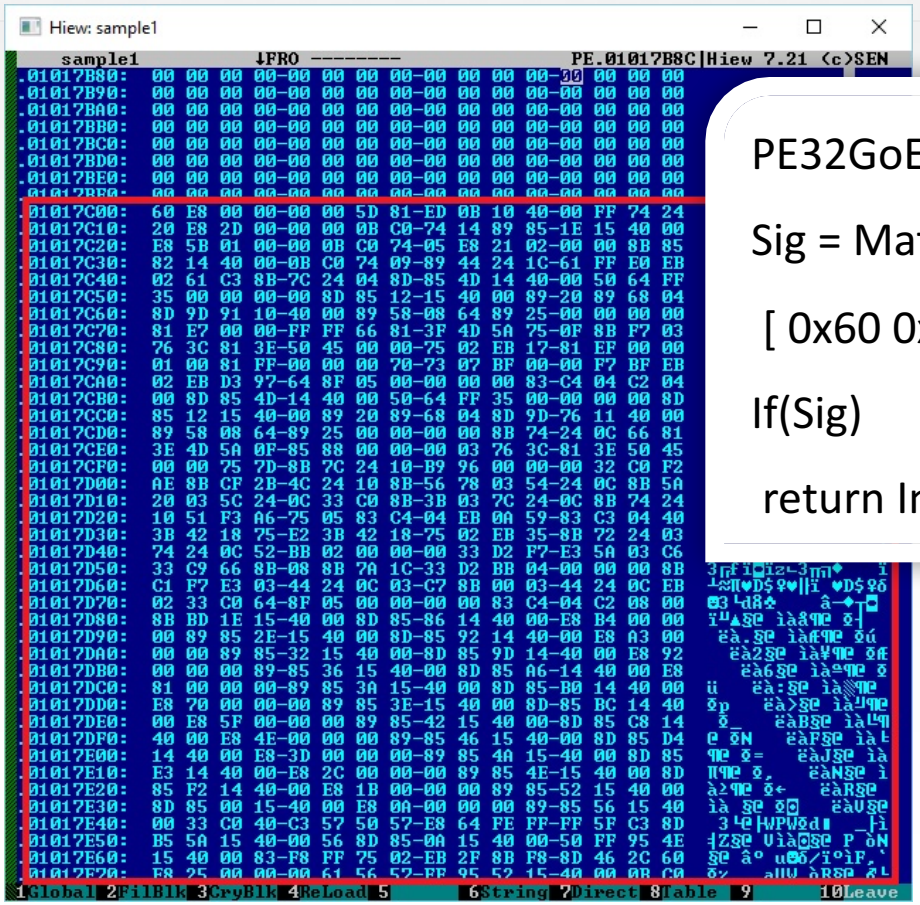
- Behavioural analysis
- Virtualized environments
- Gateway solution
- Cloud
- Antirootkits

Security

- Memory protection (PatchGuard)
- Machine learning
- Data mining
- Anomaly base detections

- NEXT GEN

A Never Ending War



PE32GoEntryPoint()

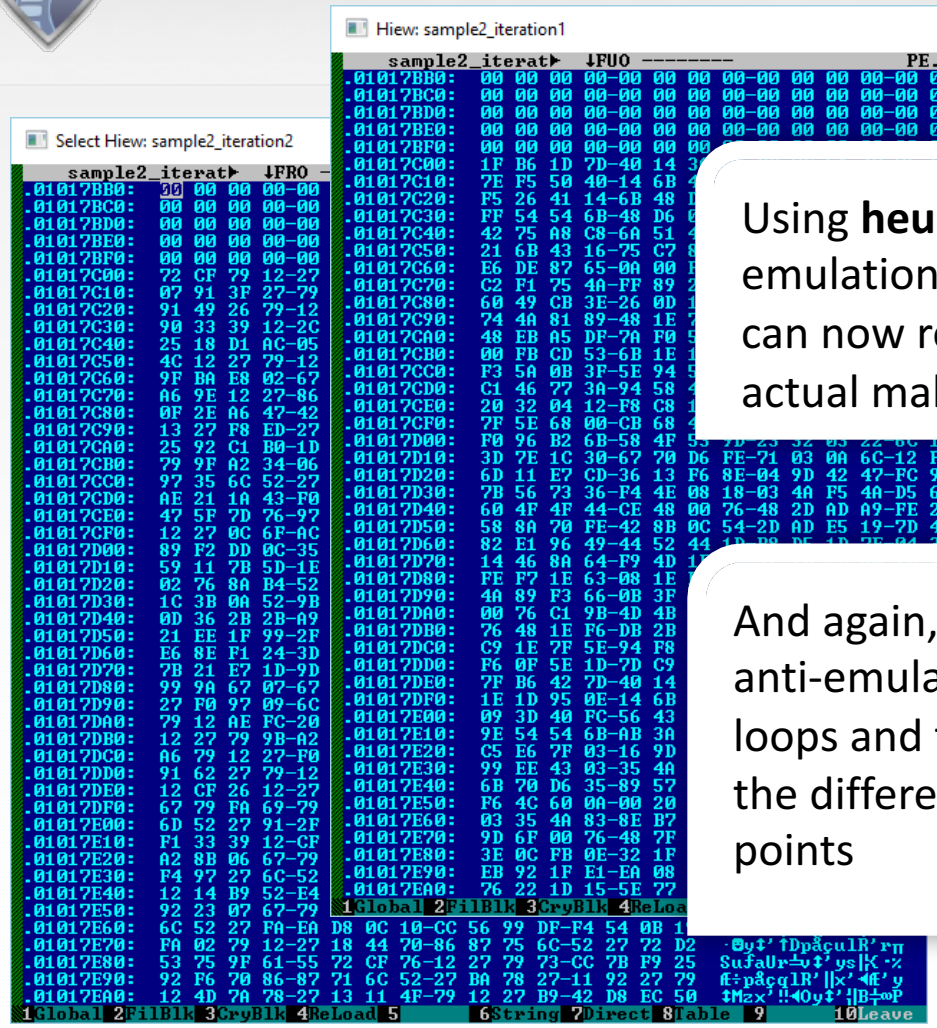
Sig = MatchExactHexa

[0x60 0xe8 0x00 0x00 0x5d 0x81 0xed 0x0b…]

If(Sig)

return Infected

A Never Ending War



Using **heuristic based signature detections**, emulation and intelligent scanning. AV engines can now remove garbage codes and produce the actual malicious code

And again, malware authors responded back with anti-emulation techniques such as near infinite loops and timed based techniques by counting the difference in processor cycles in between 2 points

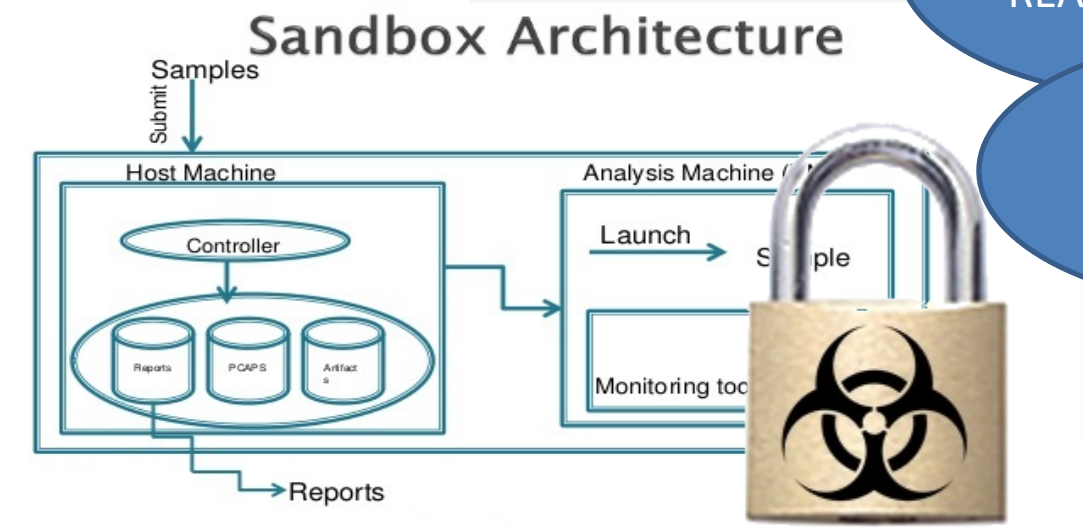
Heuristic based detection are the signature detections that we use nowadays. It's called a 1 to many detection pattern.

The usual heuristic sig can detect from hundreds to thousands sample per sig.

I know of a couple who can catch a million sample with 1 heuristic based signature.

But those are few and rare, as it is very hard to find a common pattern from different variant, families and different generations of malware.

A Never Ending War



Am I running on a REAL machine???

GOTCHA!!!!

Windows 7 64bit

TDL4

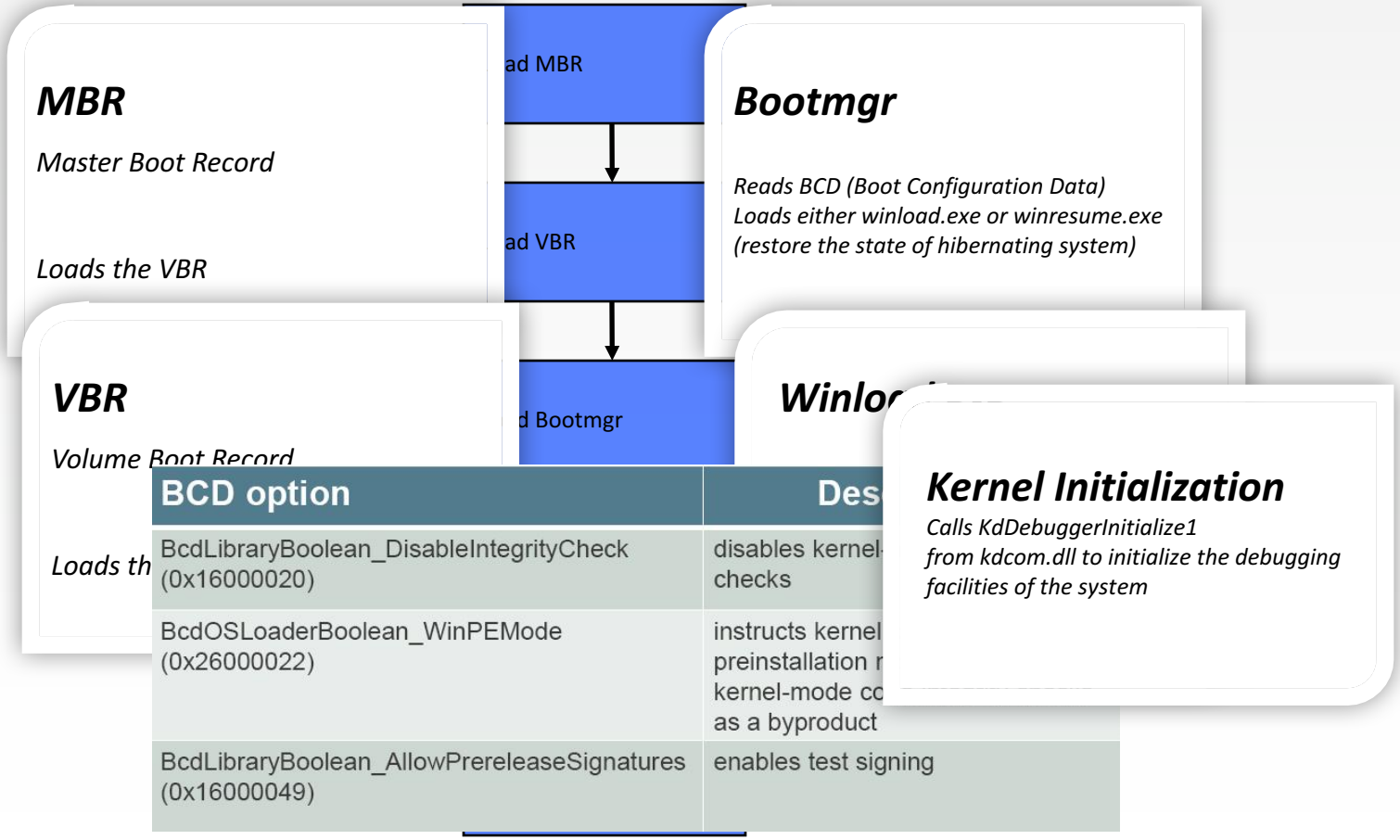
- Code Integrity Policy prevents unsigned kernel-mode drivers on loading
- Windows *PatchGuard* protects modification of
  - SSDT System Service Dispatch Table
  - IDT Interrupt Descriptor Table
  - Global Descriptor Table
  - Patching codes on kernel

"The Master Boot Record (MBR) is the first 512 bytes of a data storage device that contains code for bootstrapping an operating system. It houses the table of primary partitions using the IBM partition table scheme. It's primary purpose is to load the boot sector and pass control to it (volume boot record)"

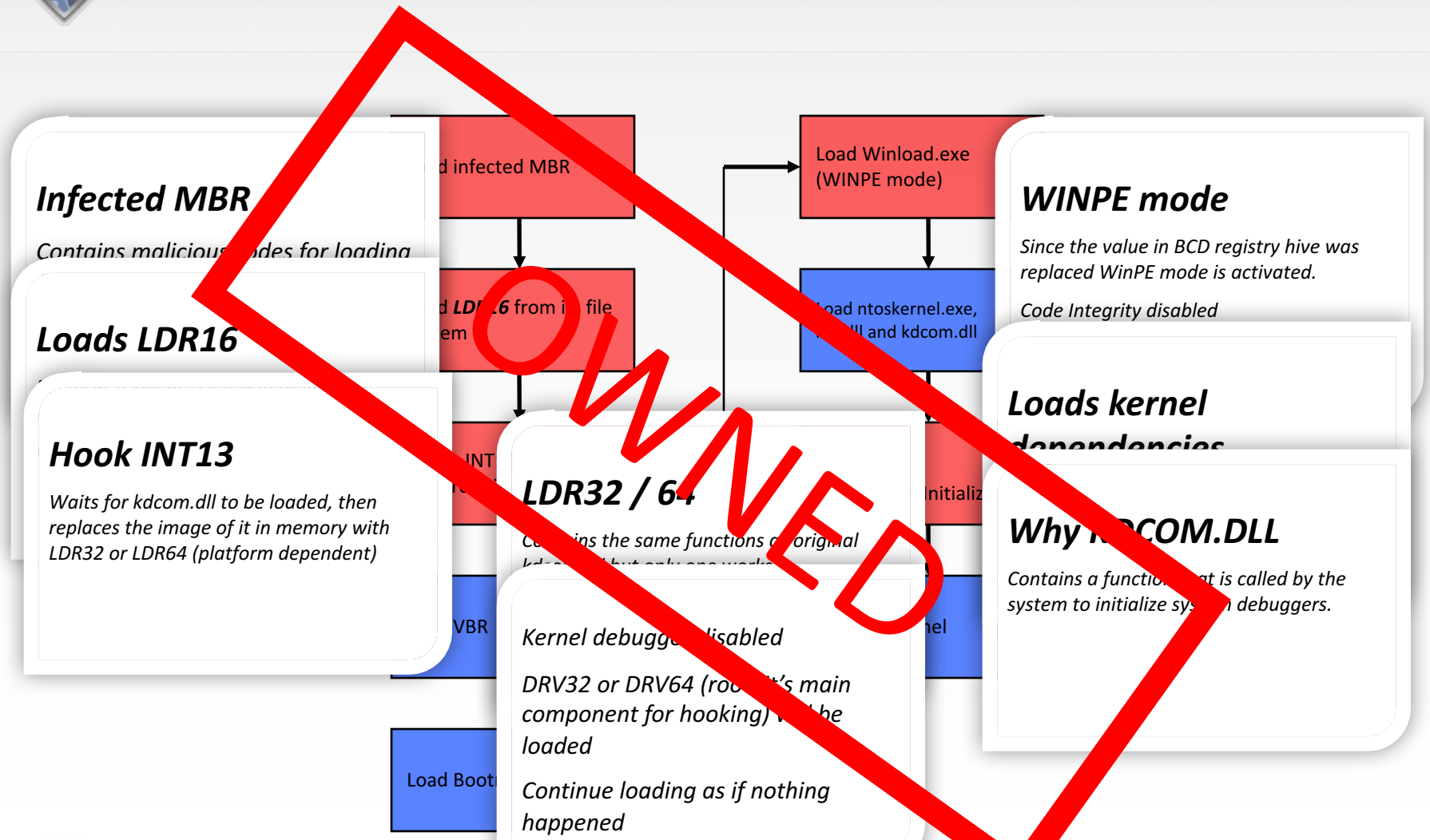
Structure of a master boot record

Address			Description		Size in bytes
Hex	Oct	Dec			
0000	0000	0	code area		**440** (max. 446)
01B8	0670	440	disk signature (optional)		**4**
01BC	0674	444	Usually nulls; 0x0000		**2**
01BE	0676	446	**Table of primary partitions** (Four 16-byte entries, IBM partition table scheme)		**64**
01FE	0776	510	55h	MBR signature; 0xAA55	**2**
01FF	0777	511	AAh		
MBR, total size: 446 + 64 + 2 =					**512**

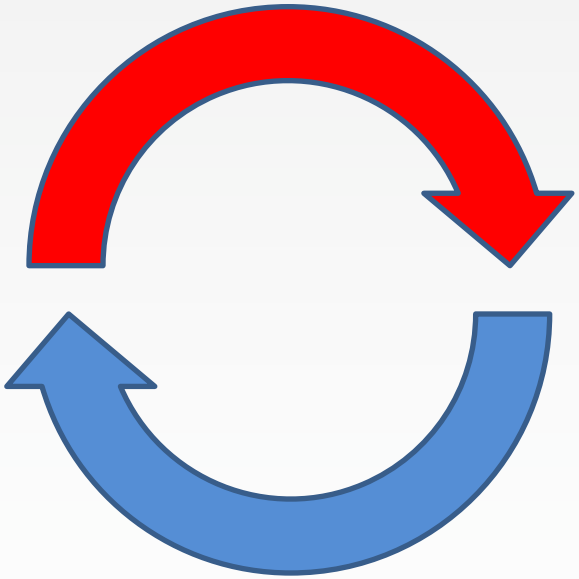
A Never Ending War



A Never Ending War



A Never Ending War



"We are essentially going in circles. We improve only after our adversaries defeat our defenses. Most software is still riddled with vulnerabilities, but the vendors typically make no move to fix one until it becomes publicly disclosed."

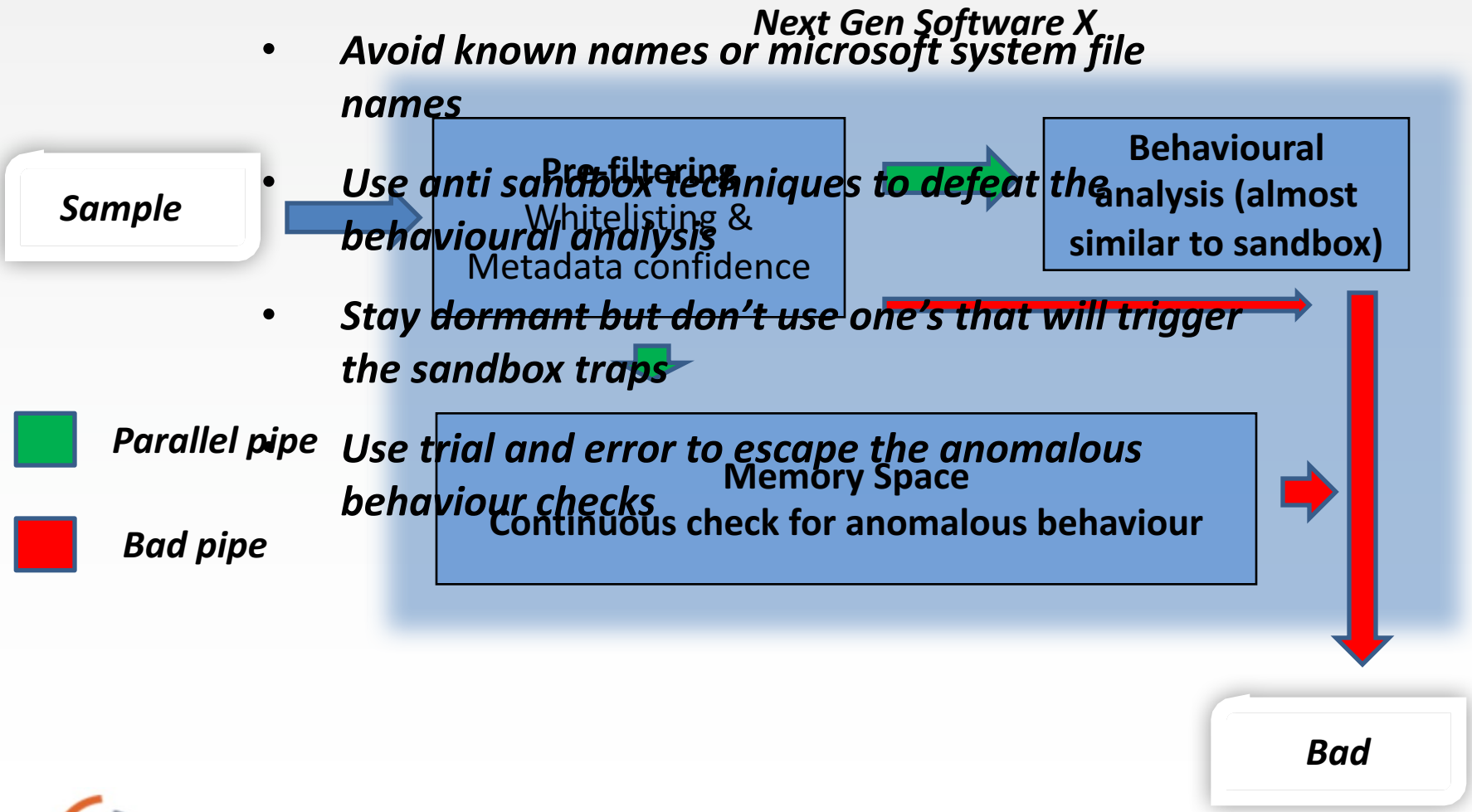
David Hoelzer
Director of Research, Enclave Forensics

WHO?

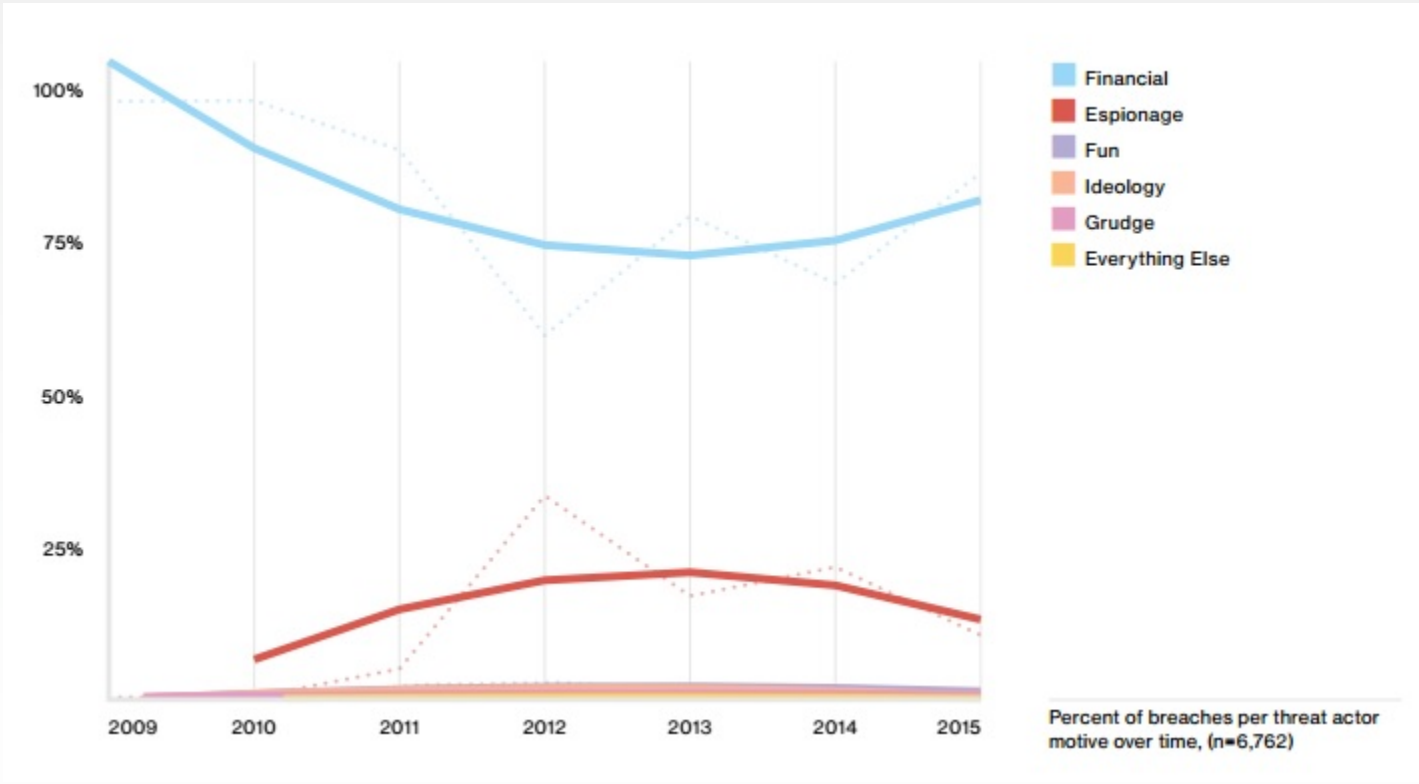
- People who have limited knowledge about the subject
- Irate victims of a malware attacks
- People who have other intent
  - Financial gain
  - Ego
  - Marketing a new technology (Next Gen)
    - 2008, 2014 Big AV companies were quoted saying in, essence, AV is not sufficient anymore

Proactive Development Of New Weapons

- *Avoid known names or microsoft system file names*
- *Use anti sandbox techniques to defeat the behavioural analysis*
- *Stay dormant but don't use one's that will trigger the sandbox traps*
- *Use trial and error to escape the anomalous behaviour checks*



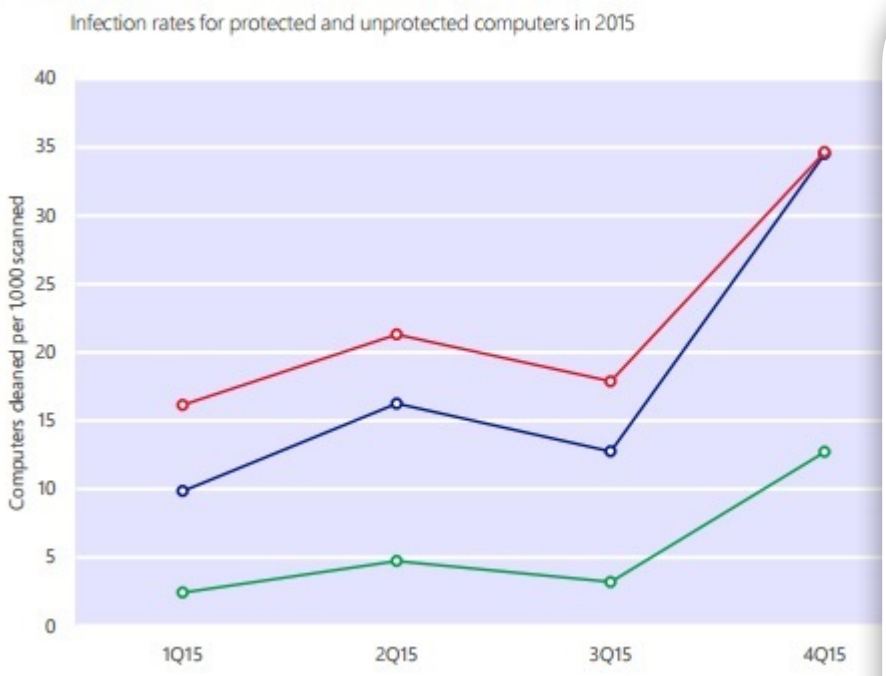
Being Opinionated On Data



2016 Verizon Data Breach Investigations Report

Being Opinionated On Data

Infection Rates For Protected and Unprotected Computers



Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provi
teleme
analyze
pattern
correla

This graph tells us that computers that were unprotected were between *2.7 and 5.6 times* as likely to be infected with malware as computers that were protected.

2015 Microsoft Security Intelligence Report

Being Opinionated On Data

"Antivirus won't protect you from the ever-increasing percentage of malware that's specifically designed to bypass antivirus software, but it will protect you from all the random unsophisticated attacks out there: the "background radiation" of the Internet."

https://www.schneier.com/blog/archives/2014/05/is_**antivirus**_de_1.html

"In an era where anti-malware labs process hundreds of thousands of samples a day, failure to realize the significance of a vanishingly small set of stealthy, low-prevalence samples – however great their subsequent impact – while hardly describable as a success, is hardly a spectacular failure in statistical terms. "[1]

Derivation

- *To react to the evolving threats, "AV" or AM has evolved too*
  - *It does not SOLELY use the simple signature based detection as it did 20 years ago*
  - *Hash(blacklist), whitelisting, Smart patterns or Heuristics are the BASIC functionalities we're using for "AV" these days*
  - *Even 20% protection is better than none (worse case scenario from AUSCERT)*

Derivation

GOOD SECURITY

- ***Does not rely on a single technology for protection***
- ***Multi-layered security is the right approach***
  - ***Good endpoint security (AV/AM)***
  - ***Good network based security***
  - ***Backups***
  - ***Updates and Patches***
  - ***Secure your channels***
  - ***Don't overdo it***

Extra: Getting Opinionated Again

"Consider whether you want to base your security strategy (at home or at work) on a PR exercise based on statistical misrepresentation and misunderstanding. Don't be too optimistic about finding The One True (probably generic) Solution: look for combinations of solution that give you the best coverage at a price you can afford. The principle applies to home users too: the right free antivirus is a lot better than no protection"[1]

[1] www.welive**security**.com/wp-content/uploads/.../avar-2013-paper.pdf

Q?