



ENJOY SAFER TECHNOLOGY™

Is Anti-Virus Dead?

Aryeh Goretsky, Distinguished Researcher



October 21, 2015

#ESETCast



ENJOY SAFER TECHNOLOGY™

Aryeh Goretsky

Distinguished Researcher

Aryeh is ESET's Distinguished Researcher and has been with the company for over nine years.

A twenty-six year veteran of fighting viruses, today he is responsible for threatscape monitoring, investigations and working with researchers in and outside of ESET globally.

He was the first employee at McAfee and is a veteran of several software and networking startups. He has received industry awards from Microsoft, Lenovo and *Securing our eCity* for his efforts to help make computing safer.



#ESETCast



ENJOY SAFER TECHNOLOGY™

Agenda

- Overview of the death of AV (1980s-today)
- History of threats
- History of defenses
- What is malware, anyways?
- What is anti-malware?
- Virus Bulletin 2015 highlights (if I have time)
- Q&A



#ESETCast



ENJOY SAFER TECHNOLOGY™

Not on the Agenda

This is an overview-level presentation, not a deep dive session. Not going to drill down into:

- history of viruses
- history of anti-virus software
- examples of next-gen technology
- not going to be very ESET-specific

While mentioned in passing, each of these is a multi-hour discussion by itself.



#ESETCast



Who says 'AV is dead,' anyways?



Why say 'AV is dead?,' anyways

The question of anti-malware software being dead comes up perennially. Why is that?

- those who do not understand the problem
- those who do not understand the solution
- those who are financially motivated
- those who have hidden agendas



Choice words

“For me for the last three years I’ve been feeling that the anti-virus industry sucks. If you have 5.5 million new viruses out there how can you claim this industry is doing the right job?”

— **[Eva Chen \(2008\)](#)**

CEO, Trend Micro



Choice words

“Antivirus ‘is dead.’ We don’t think of antivirus as a moneymaker in any way.”

— **[Brian Dye \(2014\)](#)**

SVP Information Security, Symantec*

****Mr. Dye is no longer with Symantec***



Choice words recontextualized

Sometimes, it comes from within the anti-malware industry. Why?

- **it's easy to get quoted out of context**
 - questions get reframed, cherry-picked, etc.
- **people have agendas**
 - responding to criticism
 - boosting shareholder value
 - getting a lot of page views



A Quick History of Viruses



Virus (*n.*) – A computer program that modifies other computer programs to include a copy of itself, *i.e.*, they exhibit parasitism. Computer viruses can be said to be recursively self-replicating.

(a generally-accepted industry definition)



Fred Cohen's Ph.D thesis *Computer Viruses – Theory and Experiments* is published in 1984.

First definition of a “computer virus” as:

*a computer program that can affect other computer programs by modifying them in such a way as to include a (possibly evolved) copy of itself **



*Actual definition (via Dr. Cohen's thesis):

1.1 WHAT IS A COMPUTER VIRUS?

I would like to start with a formal definition

$$\forall M \forall V (M, V) \in VS \Leftrightarrow [V \in TS] \text{ and } [M \in TM] \text{ and}$$

$$[\forall v \in V [\forall H_M [\forall t \forall j$$

$$\begin{aligned} & [1) P_M(t) = j \text{ and} \\ & 2) \square_M(t) = \square_M(0) \text{ and} \\ & 3) (\square_M(t, j), \dots, \square_M(t, j + |v| - 1)) = v] \\ \Rightarrow & [\exists v' \in V [\exists t' > t [\exists j' \\ & [1) [(j' + |v'|) \leq j] \text{ or } [(j + |v|) \leq j']] \text{ and} \\ & 2) (\square_M(t', j'), \dots, \square_M(t', j' + |v'| - 1)) = v' \text{ and} \\ & 3) [\exists t'' \text{ s.t. } [t < t'' < t'] \text{ and} \\ & [P_M(t'') \in j', \dots, j' + |v'| - 1] \\ &]]]]]]]] \end{aligned}$$

FIGURE 1.1 Formal definition.



A Quick History of Anti-virus



An old signature-based AV program

```
VIRUSCAN  Version 0.3V19

From: McAfee Associates  408 988

3832

VIRUSCAN scans diskettes or entire systems and identifies any
pre-existing PC virus infection.  VIRUSCAN will indicate the
specific files or system areas that are infected and will identify
the virus strain which has caused the infection.  Removal can then
be done manually or, if the infection is widespread, automatic
removal utilities are available which can disinfect each virus
strain.

VIRUSCAN version 0.3V19 can identify 19 major virus strains
and numerous sub-varieties for each strain.  The 19 viruses include
the ten most common viruses which account for over 90% of all
reported PC infections.  These common viruses include:

- Pakistani Brain
- Jerusalem
- Alameda
- Cascade (1701/1704)
```



Defining Anti-Virus

In 1984, Dr. Cohen also described the three atomic (or fundamental) techniques used to detect computer viruses:

- behavior blocking
- change detection
- signature matching
(fingerprint, pattern, hash, etc.)



Defining Anti-Virus

In 1984, Dr. Cohen also described the three atomic (or fundamental) techniques used to detect computer viruses:

- behavior blocking
- change detection
- signature matching
(fingerprint, pattern, hash, etc.)

I don't have formal mathematical proofs for these. Sorry.



Defining Anti-Malware

That was over 30 years ago. Today's threats:

- **are more sophisticated**
- **are more dangerous**
 - **financially motivated (selling spam, bot, DDoS...)**
 - **espionage (economic, intelligence, military...)**
- **require new concepts & ideas for defending systems**



Defining Anti-Malware

Today, all modern security programs use a broad range of techniques to detect these sophisticated threats using the following fundamentals:



Defining Anti-Malware

Today, all modern programs use a broad range of techniques to detect these sophisticated threats using the following fundamentals:

- Behavior blocking
- Change detection
- Signature matching
(fingerprint, pattern, hash, etc.)



Defining Anti-Malware

Today, all modern programs use a broad range of techniques to detect these sophisticated threats using the following atomic methods:

- Behavior blocking
- Change detection
- Signature matching
(fingerprint, pattern, hash, etc.)

Often when saying “they’re not AV.” 😊



Do you think Anti-virus is dead?

- Yes
- No
- Don't know



Malicious Software

- **An umbrella term encompassing all malicious software (malware)**
- **Overwhelming majority of malware these days is non-viral in nature:**
 - not self-replicating
 - not parasitic
- **Many different types, no universal agreement about classification**



Some malware types

- Adware
- Agents
- APTs
- Backdoor
- Bootkits
- Bots
- Botnets
- C&C servers
- DDoS
- Dialers
- Downloaders
- Droppers
- Exploit Kits
- Hoaxes
- Keyloggers
- Packers/crypters
- Memory-only processes
- Phishes
- PUAs
- Ransomware
- Remote Access Tools
- Rootkits
- Spyware
- Trojans
- Viruses
- Web Injects
- Worms
- Zero-days
- Zombies



To put things in perspective:

These days, when people are talking about computer viruses, they usually mean some other kind of malware.



Why call it Anti-Virus?

Public has awareness of computer viruses:

**IMAGE
DELETED**

So they know they need to buy “AV” software to protect themselves.



AV Perception

- **Lack of understanding how anti-malware (née -virus) works, even from other parts of security industry.**
- **Think that if programs don't provide 100% protection they provide 0% protection.**
- **Assume programs are simply matching hex strings, checksums, hashes, other predetermined values.**



What people think signatures are

- **Old technologies like fingerprint, pattern-matching, CRC-driven signatures were getting phased out in the mid-1990s**
- **Some were relatively sophisticated (regex, fuzzy logic, similarity matching, heuristics, etc.)**
- **May still be used for legacy detection (DOS, Classic Mac) in some cases**



What signatures really are

At anti-malware firms, *signatures* are scripts or macros written in their proprietary languages used for describing:

- **Packers, cryptors, obfuscators**
(automatically detect + decrypt)
- **Multiple families of malware**
(covers several families + variants, accounts for polymorphism, etc.)
- **Heuristics**
(behaviors repeatedly observed in malware...)
- **Cloud API Calls**
(reputational/server-side analysis...)

Think of them as *maps* of malicious behavior.



Are Viruses Still Even a Problem?

- **Viruses account for <10% threats seen daily**
- **Viruses are never going to be extinct.**
- **Attackers will blend techniques from them and other malicious programs**
- **Criminals want your money and will look for ways to continue stealing it**



Building Better Anti-Malware

30-year-old+ ideas can today be applied, used and even combined in new & interesting ways.

When you get it right you can:

- **Improve security**
- **Increase performance**
- **Reduce false positives**



‘Modern’ Anti-Malware Techniques

CODE-SIGNING

- **change detection**

CLOUD-BASED

- **client/server computing model**
- **move CPU intensive activities from local PC to anti-malware company’s servers**

CONTEXT SENSITIVITY

- **use riskier signatures, heuristic thresholds**
- **more likely to generate false positives on downloads, but that’s OK**



‘Modern’ Anti-Malware Techniques

DETONATION CHAMBER

- **behavioral analysis inside emulator or sandbox**
- **Determination based on codified set of rules (aka signatures)**

GENERIC DETECTION

- **teaching neural networks to...**
 - **create signatures for families (easy)**
 - **but not cause false positives (hard)**

INDICATORS OF COMPROMISE (IOCs)

- **signatures for evidence of infection**



‘Modern’ Anti-Malware Techniques

HEURISTICS

- **metasignatures derived from observed behavior, other signatures, etc.**
- **signatures calculated for behaviors**

HIPS

- **behavior blocking... for applications**

NIDS

- **signatures... for malicious network traffic**

WHITELISTING

- **change detection**



How many new malware samples do you think the ESET virus lab sees per day?

- 250
- 2,500
- 25,000
- 250,000
- 2,500,000



The smörgåsbord of techniques

Can you use new and old tech to protect PCs?

- ESET receives about 250,000 new samples of malware a day
- ESET does not add 250,000 signatures a day

Would anyone care to make a guess how many signatures ESET adds a day?



The smörgåsbord of techniques

The screenshot shows the ESET Virus Radar website interface. At the top is a navigation bar with links for Home, Threat Encyclopaedia, Glossary, Statistics, Update Info, Tools, and Reports. Below the navigation bar is a banner featuring the ESET logo and the text "VIRUS RADAR" next to a stylized robot head. A breadcrumb trail reads "HOME > Update Info > Detail". There are four tabs: "Update Info" (selected), "Android", "Windows Mobile", and "Symbian". The main content area displays "Update 12400" for the date "2015-10-13". A summary line states: "Total: 115 (6 Android, 2 BAT, 1 JS, 1 Linux, 12 MSIL, 1 NSIS, 1 PowerShell, 6 SWF, 2 VBA, 1 VBS, 82 Win32)". Below this is a list of specific malware techniques:

- Android/Exploit.Lotoor.GG
- Android/Top.AB
- Android/TrojanDownloader.Agent.DV
- Android/TrojanDropper.Agent.DI
- Android/TrojanDropper.Shedun.Q
- Android/TrojanSMS.Agent.BLT
- BAT/KillFiles.NJJ
- BAT/KillFiles.NJK
- JS/ExtenBro.Agent.AW
- Linux/Gafgyt.CO
- MSIL/Bladabindi.BC



The smörgåsbord of techniques

The screenshot shows the ESET Virus Radar website. The navigation bar includes links for Home, Threat Encyclopaedia, Glossary, Statistics, Update Info, Tools, and Reports. The main header features the ESET logo and 'VIRUS RADAR' text, with a background image of a robot head. Below the header, a breadcrumb trail reads 'HOME > Update Info > Detail'. There are four tabs: 'Update Info', 'Android', 'Windows Mobile', and 'Symbian'. The 'Update Info' tab is active, displaying 'Update 12400'. A red box highlights the date '2015-10-13' and a red arrow points to it. Another red box highlights the total count: 'Total: 115 (6 Android, 2 BAT, 1 JS, 1 Linux, 12 MSIL)'. A third red box highlights the detailed breakdown: 'Total: 115 (6 Android, 2 BAT, 1 JS, 1 Linux, 12 MSIL, 1 NSIS, 1 PowerShell, 6 SWF, 2 VBA, 1 VBS, 82 Win32)'. Below this, a list of malware techniques is shown:

- Android/Exploit.Lotoor.GG
- Android/Top.AB
- Android/TrojanDownloader.Agent.DV
- Android/TrojanDropper.Agent.DI
- Android/TrojanDropper.Shedun.Q
- Android/TrojanSMS.Agent.BLT
- BAT/KillFiles.NJJ
- BAT/KillFiles.NJK
- JS/ExtenBro.Agent.AW
- Linux/Gafgyt.CO
- MSIL/Bladabindi.BC



The smörgåsbord of techniques

Anti-malware software can

- block 100s-1,000s of malware samples a day using specific signatures
- block 100,000s of malware samples a day using other techniques (*generic + heuristic signatures, etc.*)

**Keep in mind, a single signature might detect a family of malware that has billions of permutations*



Recap

Next generation security programs are based on three fundamental, atomic mechanisms:

- **Behavior blocking**
- **Change detection**
- **Signature matching**

So are “old” anti-virus/anti-malware programs.



Recap

What does this all mean, though?

- **Even the oldest technologies can be applied in novel ways**
- **It is important to keep track of research**
- **Innovations can occur both inside and outside the anti-malware space**
- **Keep on researchin'**



2015

PRAGUE 

30 Sept - 2 Oct 2015



Virus Bulletin 2015 highlights

Economic sanctions on malware

Prof. Igor Muttik *Intel Security*

- **increase costs to malware ecosystem**
 - technologies to de-incentivize malware authors





Virus Bulletin 2015 highlights

[The Kobayashi Maru Dilemma](#)*

Morton Swimmer, *Trend Micro*; Nick FitzGerald, *independent researcher*; Andrew Lee, *ESET*

- **Offensive hacking**
 - Is attacking the attackers legal? Ethical?



**bonus points for Star trek reference*



Virus Bulletin 2015 highlights

discussions about

- APTs
- Certificate technologies
- Linux malware
- Packers





I would like to request one of the following

- Contact from ESET Sales
- Technical Demo
- Business trial
- Information on becoming a Reseller Partner or MSP
- None of the Above

Q+A Discussion





Bibliography

- Dr. Fred Cohen's web site: <http://all.net/>
- [*Paper: Hype heuristics, signatures and the death of AV \(again\)*](#) – Virus Bulletin
- [*Presentation: Economic sanctions on malware*](#) - Virus Bulletin
- [*Presentation: The Kobayashi Maru Dilemma*](#) - Virus Bulletin
- [*Signatures, product testing, and the lingering death of AV*](#) – We Live Security
- [*Symantec Develops New Attack on Cyberhacking*](#) – Wall Street Journal
- [*Trend Micro's CEO says 'AV industry sucks'*](#) – The Register



Join Us Next Time...



ENJOY SAFER TECHNOLOGY®

EMV MANDATE

WHAT BUSINESSES NEED TO KNOW

October 28, 2015 10am PDT

LIVEWebcast

#ESETcast



Stephen Cobb
Sr. Security Researcher, ESET



ENJOY SAFER TECHNOLOGY™

Thank You

No presentation gets done in a void, and I'd like to thank my co-workers for their assistance:

Bruce P. Burrell, Jakub Debski, David Harley, Juraj Malcho, Roman Kováč & Thomas Uhlemann

And thank you for attending!

#ESETCast



ENJOY SAFER TECHNOLOGY™

Aryeh Goretsky



WWW.ESET.COM
WWW.WELIVESECURITY.COM



aryeh.goretsky@eset.com



[@goretsky \(personal\)](https://twitter.com/goretsky) / [@esetna](https://twitter.com/esetna) / [@welivesecurity](https://twitter.com/welivesecurity)



[/u/goretsky](https://www.reddit.com/u/goretsky)



[fb.com/goretsky](https://www.facebook.com/goretsky)

#ESETCast