Is Anti-Virus Worth It?

Timothy D. Morgan

OWASP Chapter Meeting

November 17, 2015

A Shift in Perception?

Several well-known security researchers have recently proposed that anti-virus software may be a *net negative* for security.

What is Anti-Virus?

- Does a variety of things, but primarily:
  - Tries to detect attacks on software (exploits)
  - Tries to detect malware (payloads)
- Main threats it helps with:
  - Known, but unpatched vulnerabilities
  - Unsafe user behavior

Anti-Virus Limitations

- Always playing catch-up
  - Won't stop 0-days
  - Won't catch payloads/encoders never seen before
  - Can't keep up with many published techniques
- Vendors *try* to generalize, but attackers can always test first
- Detecting a breach *after* the fact is useful, but...

Additional Risk of Using Anti-Virus

- Anti-virus runs with full privileges
  - Parses hundreds of file formats
  - Reviews network traffic
- Written in low-level languages (C/C++)
- A **huge** attack surface: recipe for disaster?

Mix Vulnerabilities with...

Tavis Ormandy's work:

- Numerous critical vulnerabilities in Sophos AV (2011-2012)
- Remote root exploit in ESET AV (June 2015)
- Several remote SYSTEM exploits in Kaspersky AV (September 2015)
- RCE in Avast AV, with more to come (September 2015)

More Vulnerabilities, and...

Joxean Koret attacked ~17 AV products in 2014:

- RCE in most of these: Avast, AVG, Avira, BitDefender, Comodo, DrWeb, ESET, F-Prot, F-Secure, Panda, eScan
- Many AVs share engines... more products vulnerable than listed

A Dash of Negligence

Ormandy and Koret both point out that many AV companies aren't using modern safety measures:

- Failing to compile with mitigations like /GS
- Failing to use sandboxes for parsing & unpacking

"Why is it harder to exploit browsers or document readers than security products?"

— Joxean Koret

This is Not the First Time.

SANS' Top Internet Security Risks of **2007**, Risk #10:

> *"Multiple remote code execution vulnerabilities have been discovered in the anti-virus software provided by vendors including Symantec, F-Secure, Trend Micro, McAfee, Computer Associates, ClamAV, and Sophos. AV software has also been found to be vulnerable to "evasion" attacks, whereby malware bypasses anti-virus scanning."*

From the Horse's Mouth

Bryan Dye, Symantec (May 2014) said:

- Anti-virus "is dead"
- Catches less than half of attacks
- Not a money maker

If AV firms have slim margins, can we expect them to be proactive about preventing future vulnerabilities?

Anti-Virus on Balance

- Software vulnerabilities
  - AV prevents exploit of some
  - Introduces new ones
  - Currently AV may be easier to exploit
- User behavior exploits
  - AV blocks some payloads
  - Impossible to know how many it doesn't stop
- AV costs money
  - Could we spend it on better patch management?
  - Could we spend it on better user awareness?