



Retest: Cutting Malware Losses
infectionvectors.com
July 2007

Overview

The struggle to defend systems against malware infection has been described many ways in the security literature, often in terms of an “arms race.”¹ This race, however, is largely artificial – perpetuated by a reliance on traditional detection tools and rejection of infrastructure redesign. Although there will never be a magic bullet that eliminates malware forever, there are a great many researchers pointing to viable steps that would greatly lessen our defense burdens. This report examines the path we have currently selected as a community and the work of Joanna Rutkowska as an example of research that has long advocated how we could take the lead in the “arms race.”

Examination

There are two means generally employed to assess one’s security posture: scanning for attack entry points and distributing antivirus software to clients. In terms of malware defense, how are we testing the health of our network ecosystems today? There are numerous vulnerability scanners that check common ports/services, patch deficiencies, antivirus signature dates, and configuration deltas. Products like Nessus have been around for years and do a good job of automating compliance testing. At their best, compliance tests quickly assess how well a set of machines are meeting prescribed enterprise policy. They are the eyes and ears of the configuration management team.

Beyond compliance scanning and ensuring our patches are up-to-date, the penetration testing (aka “red teaming”) is popular. At its most efficient, the penetration tester is performing an investigation that is very specific to the target environment. Each attack is tailored to the network under review based on a great deal of research – much like an attacker would perform. The tests may involve using this reconnaissance to craft custom exploits, malcode, and social engineering schemes.

But, how effective is this type of testing for a CIO? “Testing” infrastructure by using custom Trojans and stealth malware is far from the best way to determine how good one’s preventative defenses are working. Every enterprise is vulnerable to this type of attack – there is a proof of concept for any type of malware one could imagine hitting their systems. In addition, finding one hole (or even fifty) to exploit does not provide a measure of how secure the network is (or how many holes are left...).

Of course, there is also the antivirus software, generally signature-based (although there are “heuristic” attempts to determine “badness” of respective executables) which tries to

snatch the malcode before it installs itself. We stay ahead of attackers by closing holes (as they are discovered), writing detectors for specific exploits, and removing programs that have a history of criminal activity. In other words, if we can see it, tag it as evil, then we can craft a tool to stop it. But, as has been popularized by Joanna Rutkowska² (and a challenge issued to her³), we are standing in front of an ever-widening chasm between our traditional detection capabilities and stealth malware.⁴

The Rut of All...

Anyone using email knows that the mass mailer problem has not gone away. Although the Internet is less bothered by the traditional mass mailing worm than it was in 2004, spam bots, phishing-based crimes, and the like are as much a problem as ever. In years past, a call to make fundamental changes to the email infrastructure (requiring authentication to be built into SMTP) was proposed as a requirement to securing email and its legitimate use on the Internet.⁵ That change has yet to occur. The steps we have taken towards email security involve adding layers (and the complementary software/subscriptions) to the network infrastructure in the form of additional filtering signatures, spam detection, and malware detection products on gateway servers.

Over the last few years, Rutkowska has effectively pointed out that fundamental change is required to stay ahead of attackers.⁶ The infrastructure of the Internet (in many cases the hardware/processors themselves) needs extension to deal with the evolution of malware threats. In many of her recent papers/presentations, Rutkowska has expanded on her own taxonomy for malware – one that describes the threats in terms of their subversion of the resident operating system and applications.⁷ The classifications include four “Types” (0-III currently) of malware, which in many ways show an evolution of malware – with increasingly sophisticated mechanisms to hide from the OS and existing detection mechanisms.

From employing legitimate OS functions to introducing its own hypervisor, the “Type” classification may also be viewed as “dimensions” of malware; as examples of each type exploit different strategies, not necessarily evolved from or dependent upon the previous type’s traits (although, if seen as a linear progression, the technology of each has, in fact, matched the respective chronology). While we watch rootkit technology take new dimensions, we persist in fighting it with an antiquated approach. In effect, we are building two dimensional tools to detect three (and sometimes four) dimensional threats.

Starting with OS and processor design, Rutkowska’s proposals can have the same type of impact on system compromise that securing SMTP could have had years ago on email. She has demonstrated that traditional antivirus is inappropriate for stealth malware (things like the much-debated Blue Pill) – our existing tools are the proverbial square pegs in round holes. As she states, we are relying on “hacks” to find specific threats instead of preventing them altogether.

Lapped

Stealth malware, as a class of threats, is still relatively new to security practitioners as a group. Certainly, the press revolving around Rutkowska's Blue Pill has brought badly needed attention to virtualized attacks, but the means with which the "good guys" will use to combat them is not well understood.⁹ That fact, unfortunately, will drive the fear of hypervisor attacks to unreasonable levels, especially given the solutions that are in front of us.

One question, that certainly deserves attention given the arsenal of weapons we use today to fight viruses, is how to even detect stealth malware. From Rutkowska's "Towards Verifiable Operating Systems" presentation, the salient point is made:

<p>"If a stealth malware does its job well... ...then we can not detect it... ...so how can we know that we are infected?"⁸</p>
--

Check for a virus once, if you find it, then you can say you are infected; how many times do you check with the antivirus product and get the "all clear" before you believe it? If you are inclined to believe Ms. Rutkowska's claims regarding Blue Pill, then you never stop checking - or you never start, throwing up your hands at the inevitable losses to malware coders. But it would seem that is not her intent - unlike many of the security writers of the world, she posits solutions to the arms race.

We are in danger of being "lapped" in our race against malware development. As we round the track, however, there is one facet of the work Rutkowska has done that should not be missed: she is showing us the good guys can win. No matter how the "Blue Pill Challenge" is spun by the media (or how it turns out for that matter), the fact remains: she has delivered solutions to the fear-inducing attacks she demonstrates.

References

1. One example of the antivirus/virus fight as an “arms race,” this McAfee blog: McAfee AVERT Labs Blog, 6 November 2006.

<http://www.avertlabs.com/research/blog/index.php/2006/11/06/mcafees-newest-weapon-in-the-fight-against-malware/>.

And:

Roger A. Grimes, “IT under siege: The security arms race.” 26 September 2005. InfoWorld.

http://www.infoworld.com/archives/emailPrint.jsp?R=printThis&A=/article/05/09/26/39FEattack_3.html.

Also, Ms. Rutkowska uses the phrase in an interview:

“Stealth Malware: Interview with Joanna Rutkowska.” IT Observer. 27 March 2006

http://www.it-observer.com/articles/1089/stealth_malware_interview_with_joanna_rutkowska/

2. Rutkowska’s invisiblethings.org and blog are great places to start for anyone unfamiliar with her exceptional work:

<http://invisiblethings.org/>

<http://theinvisiblethings.blogspot.com/>

3. The Challenge, regarding the effectiveness of Ptacek, et al’s detection mechanism against Blue Pill, is explained:

Thomas Ptacek, MatasanoChargen, 27 June 2007.

<http://www.matasano.com/log/895/joanna-we-can-detect-bluepill-let-us-prove-it/>

4. See the interview from IT Observer above for a good description of the race between antivirus programs and viruses. Most notably, later work, such as Blue Pill, shows that any piece of software that rides atop an operating system is likely to be handicapped in a fight with a hypervisor-based rootkit. This point was made by McAfee AVERT Labs’ Joe Telafici, 25 October 2006:

<http://www.avertlabs.com/research/blog/index.php/2006/10/25/the-patchguard-arms-race-has-begun/>.

5. Jason Gordon, “Mass Mailer Demise?” January 2005, infectionvectors.com.

http://www.infectionvectors.com/hotzone/mass_mailer_demise.htm.

6. Joanna Rutkowska, “Fighting Stealth Malware - Toward Verifiable OSES.”

Presentation delivered at the 23th Chaos Communication Congress, 28 December 2006.

http://invisiblethings.org/papers/towards_verifiable_systems.ppt

Joanna Rutkowska, “Subverting Vista Kernel for Fun and Profit.” Presentation delivered at Black Hat Briefings 2006, 3 August 2006.

<http://invisiblethings.org/papers/joanna%20rutkowska%20-%20subverting%20vista%20kernel.ppt>

7. Joanna Rutkowska, "Introducing Stealth Malware Taxonomy." Version 1.01. November 2006. <http://invisiblethings.org/papers/malware-taxonomy.pdf>.

8. Quote taken from slide number 3, entitled "Paradox," of reference [6] above.

9. Some of the press regarding the "Blue Pill" challenge:

Lisa Vaas, "Researchers: 'Blue Pill' Rootkit Detectable." 28 June 2007, eWeek. <http://www.eweek.com/article2/0,1895,2152137,00.asp>.

Dan Goodin, "Showdown persists over '100% undetectable' rootkit." 6 July 2007. The Register. http://www.theregister.co.uk/2007/07/06/blue_pill_showdown/.