



SANDBOXING

Virtualizing threat detection.

Tom Ellis
Senior Security Engineer
Cadre Information Security

INTRODUCTION

- Tom Ellis, Senior Security Engineer
- 5 years with Cadre Information Security
- 25+ years of IT experience
- Systems Engineering
- Operations Management
- Project Management
- Security Engineering

Simplifying the business of security.



THE THREAT OF MALWARE

- Over 314 million new pieces of malware were created in 2014 alone.
- Breaches cost the economy \$419 billion in 2014.
- Malware is no longer just vandalism, it is big business.
- Zero Day attacks are a growing problem.
- Traditional security tools are no longer enough to prevent and mitigate malware.
- New tools are needed to combat this.

Simplifying the business of security.



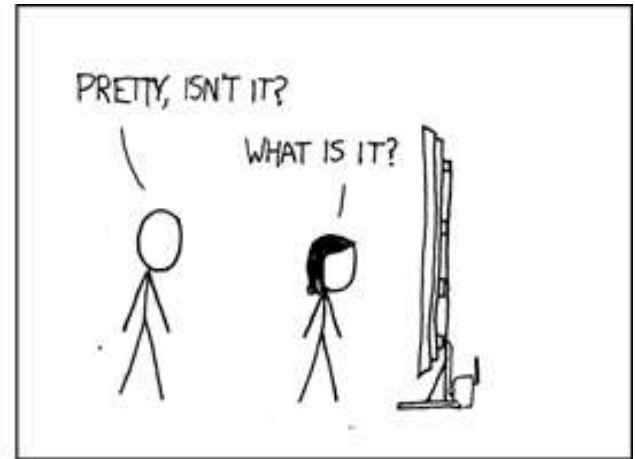
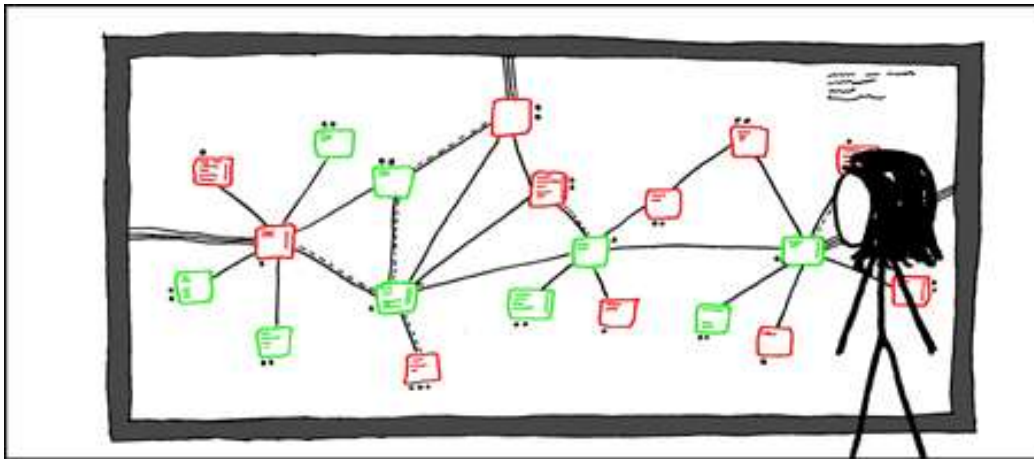
FIGHTING MALWARE THE TRADITIONAL WAY

- Signature based Anti-Virus
- Intrusion Prevention Systems (IPS)
- Firewalls
- User Education
- None of these are enough!


Simplifying the business of security.



CATCH THEM IN THE ACT




I'VE GOT A BUNCH OF VIRTUAL WINDOWS MACHINES NETWORKED TOGETHER, HOOKED UP TO AN INCOMING PIPE FROM THE NET. THEY EXECUTE EMAIL ATTACHMENTS, SHARE FILES, AND HAVE NO SECURITY PATCHES.



BETWEEN THEM THEY HAVE PRACTICALLY EVERY VIRUS.


THERE ARE MAILTROJANS, WARHOL WORMS, AND ALL SORTS OF EXOTIC POLYMORPHICS. A MONITORING SYSTEM ADDS AND WIPES MACHINES AT RANDOM. THE DISPLAY SHOWS THE VIRUSES AS THEY MOVE THROUGH THE NETWORK, GROWING AND STRUGGLING.



YOU KNOW, NORMAL PEOPLE JUST HAVE AQUARIUMS.

GOOD MORNING, BLASTER. ARE YOU AND W32.WELCHIA GETTING ALONG?

WHO'S A GOOD VIRUS? YOU ARE! YES, YOU ARE!



Simplifying the business of security.

SANDBOXING



- Virtualization allows us to inspect files and their behavior in a 'sandbox'.
- The hypervisor owns all the resources.
- Behavior is monitored to determine if the payload is malicious.
- Leverage the data gathered to weigh the potential threat level.

Simplifying the business of security.



IMPLEMENTING SANDBOX THREAT DETECTION

- Cloud based – taking advantage of a vendor's infrastructure to enable detection. This can be very cost effective and leverages data gained from traffic that is sampled world wide.
- On premises – Purpose built appliances that provide the virtual environment needed to detect malware in email attachments, downloaded files, etc. This can be more costly but is a good fit for highly data sensitive enterprises.

Simplifying the business of security.



HOW TO CHOOSE THE RIGHT ONE

- What file types are examined? Do they match up with your business?
- Cloud vs. Appliance?
- Customization. Can it emulate your current environment?

Simplifying the business of security.



THERE IS NO SUCH THING AS A PANACEA

- Some new malware tries to detect if it is running under a hypervisor and modifies its behavior accordingly.
- There is no substitute for end user training. The vast majority of malware is delivered via phishing or spam.
- Security policy and practice needs to be under constant review.
- Multi-Layered defenses are a must. No single security product or approach will keep your data safe.

Simplifying the business of security.



CONCLUSION

- Sandboxing is a logical extension of security best practices.
- A firewall alone is often no longer enough to protect the network and its resources.
- Proper planning and design is required to ensure the proper solution. There is no 'one size fits all' answer.
- A complete, holistic approach to security that includes endpoint protection, strong firewall security, threat emulation, and user training is the answer.

Simplifying the business of security.



QUESTIONS

- Any Questions?
- I can be reached at tom.ellis@cadre.net
- Contact your Cadre sales representative
 - Chris Loughner, Enterprise Security Consultant, chris.loughner@cadre.net
 - David Scott, SMB Security Consultant, david.scott@cadre.net

Simplifying the business of security.

