CyCon
2014

Malware
is Called Malicious for a Reason: The Risks of Weaponizing Code

6th Annual Conference on Cyber Conflict Proceedings

NATO Cooperative Cyber Defence Centre of Excellence

Tallinn, Estonia

(clearer text, without slide builds)

A. Lee
S. Cobb

eset

Authors

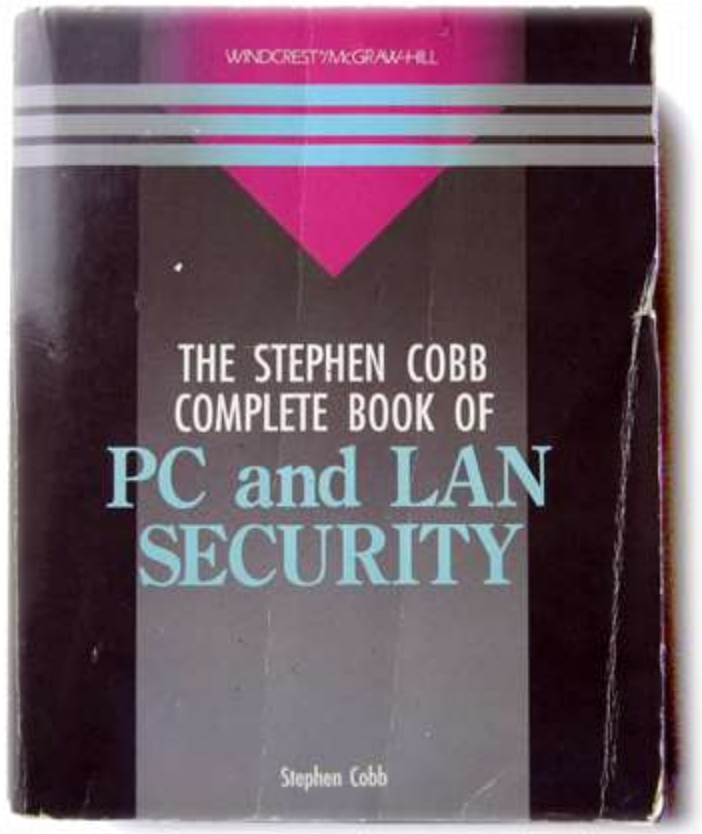
- Andrew Lee
- CEO, ESET North America
- Former Chief Research Officer
- MSc Computer Security (2010)

- Stephen Cobb
- Senior Security Researcher, ESET
- CISSP (1996)
- MSc Security & Criminology (2016, hopefully)

ESET: Founded in Bratislava, Slovakia, 1992
Makes IT security products, like NOD32 AV

Some history…

- Stephen Cobb ~~Complete~~ Book of PC & LAN Security (1991)
- Employee #5 at antivirus software testing company ICSA Labs (1995)
- Adjunct Prof. Masters in IA, Norwich University (2002-2008)
- First anti-spam router, acquired by Symantec (2004)



Perspective and key points

- A view from the front lines
- The appeal of “good viruses” and “righteous malware”
- Historical objections
- Key risks of using malware for offense or active defense
- Ideas for further research?

Malware is Called Malicious for a Reason: The Risks of Weaponizing Code

Stephen Cobb
Research Department
ESET North America
San Diego, USA
stephen.cobb@eset.com

Andrew Lee
Office of the CEO
ESET North America
San Diego, USA
andrew.lee@eset.com

Abstract: The allure of malware, with its tremendous potential to infiltrate and disrupt digital systems, is understandable. Criminally motivated malware is now directed at all levels and corners of the cyber domain, from servers to endpoints, laptops, smartphones, tablets, and industrial control systems. A thriving underground industry today produces ever-increasing quantities of malware for a wide variety of platforms, which bad actors seem able to deploy with relative impunity. The urge to fight back with “good” malware is understandable. In this paper we review and assess the arguments for and against the use of malicious code for either active defense or direct offense. Our practical experiences analyzing and defending against malicious code suggest that the effect of deployment is hard to predict with accuracy. There is tremendous scope for unintended consequences and loss of control over the code itself. Criminals do not feel restrained by these factors and appear undeterred by moral dilemmas like collateral damage, but we argue that persons or entities considering the use of malware for “justifiable offense” or active defense need to fully understand the issues around scope, targeting, control, blowback, and arming the adversary. Using existing open source literature and commentary on this topic we review the arguments for and against the use of “malicious” code for “righteous” purposes, introducing the term “righteous malware”. We will cite select instances of prior malicious code deployment to reveal lessons learned for future missions. In the process, we will refer to a range of techniques employed by criminally-motivated malware authors to evade detection, amplify infection, leverage investment, and execute objectives that range from denial of service to information stealing, fraudulent, revenue generation, blackmail and surveillance. Examples of failure to retain control of criminally motivated malicious code development will also be examined for what they may tell us about code persistence and life cycles. In closing, we will present our considered opinions on the risks of weaponizing code.

Keywords: malware, weaponize, malicious code, active defense, cyber conflict,

Plague infected bodies and Tallin city wall

A. Lee
S. Cobb

The short version

- Hurling infected bodies over city walls in 1710?
  - Bad idea
- Deploying malicious code in 2014
  - Bad idea
- “Malware = biological weapons of cyber conflict”
- White worms are mythical creatures

Defining malware

- Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an IS [Information System]
  - *National Information Assurance (IA) Glossary*
  - The definition of record for CIA/NSA/DoD/etc.

Malware and the Tallinn Rules

43: Indiscriminate Means and Methods

48: Weapons Review

49: Indiscriminate Attacks

50: Clearly Separated Distinct Military Objectives

51: Proportionality

A. Lee
S. Cobb

Deploying malware

- Virus, worm, Trojan
- Email attachment
- Website drive-by
- Removable media
- Chipping hardware
- Updating firmware
- Planting code

A. Lee
S. Cobb

Malicious Code in the Software Life Cycle

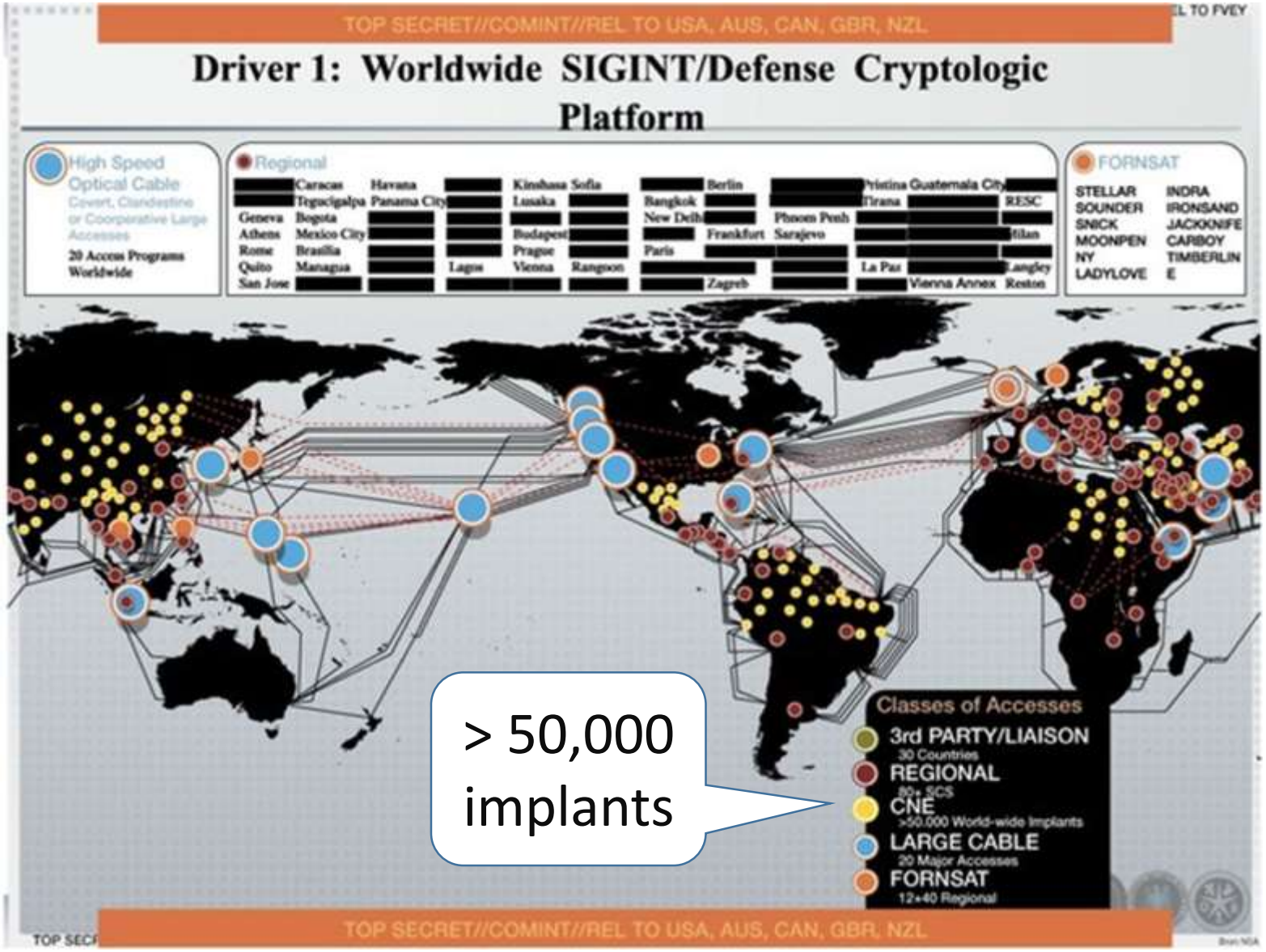
1. Acquisition
2. Requirements
3. Design
4. Construction
5. Testing
6. Installation (delivery, distribution, installation)
7. Maintenance (operation, maintenance, and disposal)

Guidance for Addressing Malicious Code Risk, NSA, 2007

A. Lee
S. Cobb

What is “righteous malware”

- It’s in the eye of the beholder
  - Software or firmware deployed with intent to advance a just cause by performing an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an IS [Information System]
- Examples?
  - Stuxnet, Shamoon, DarkComet RAT, Blackshades


TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL
Driver 1: Worldwide SIGINT/Defense Cryptologic Platform
High Speed Optical Cable
Covert, Clandestine or Cooperative Large Accesses
20 Access Programs Worldwide
Regional
Caracas
Havana
Tegucigalpa
Panama City
Geneva
Bogota
Athens
Mexico City
Rome
Brasilia
Quito
Managua
San Jose
Kinshasa
Sofia
Lusaka
Budapest
Prague
Lagos
Vienna
Rangoon
Berlin
Bangkok
New Delhi
Frankfurt
Paris
Zagreb
Pristina
Guatemala City
Tirana
Phnom Penh
Sarajevo
Milan
La Paz
Langley
Vienna Annex
Reston
RESC
FORNSAT
STELLAR
SOUNDER
SNICK
MOONPEN
NY
LADYLOVE
INDRA
IRONSAND
JACKKNIFE
CARBOY
TIMBERLIN
E
> 50,000 implants
Classes of Accesses
3rd PARTY/LIAISON
30 Countries
REGIONAL
80+ SCS
CNE
>50,000 World-wide Implants
LARGE CABLE
20 Major Accesses
FORNSAT
12+40 Regional
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

A. Lee
S. Cobb

The “good” virus

- A fascination as old as computing
- Self-replicating code that performs beneficial functions (e.g. patching or backup)
- Some virus writers persisted despite outbreaks of ‘benign’ code
- *Are ‘Good’ Computer Viruses Still a Bad Idea?*
  - Vesselin Bontchev, Virus-L and comp.virus, EICAR ’94

12 reasons why “good viruses” are a bad idea

TECHNICAL REASONS	
Lack of Control	Spread cannot be controlled, unpredictable results
Recognition Difficulty	Hard to allow good viruses while denying bad
Resource Wasting	Unintended consequences (typified by the Morris Worm)
Bug Containment	Difficulty of fixing bugs in code once released
Compatibility Problems	May not run when needed, or cause damage when run
Effectiveness	Risks of self-replicating code over conventional alternatives
ETHICAL AND LEGAL REASONS	
Unauthorized Data Modification	Unauthorized system access or data changes illegal or immoral
Copyright and Ownership Problems	Could impair support or violate copyright of regular programs
Possible Misuse	Code could be used by persons will malicious intent
Responsibility	Sets a bad example for persons with inferior skills, morals
PSYCHOLOGICAL REASONS	
Trust Problems	Potential to undermine user trust in systems
Negative Common Meaning	Anything called a virus is doomed to be deemed bad

V. Bontchev, “Are ‘Good’ Computer Viruses Still a Bad Idea?” EICAR’94

12 risks inherent in malware deployment

TECHNICAL REASONS	
Lack of Control	Spread cannot be controlled, unpredictable results
Recognition Difficulty	Hard to allow good viruses while denying bad
Resource Wasting	Unintended consequences (typified by the Morris Worm)
Bug Containment	Difficulty of fixing bugs in code once released
Compatibility Problems	May not run when needed, or cause damage when run
Effectiveness	Risks of self-replicating code over conventional alternatives
ETHICAL AND LEGAL REASONS	
Unauthorized Data Modification	Unauthorized system access or data changes illegal or immoral
Copyright and Ownership Problems	Could impair support or violate copyright of regular programs
Possible Misuse	Code could be used by persons will malicious intent
Responsibility	Sets a bad example for persons with inferior skills, morals
PSYCHOLOGICAL REASONS	
Trust Problems	Potential to undermine user trust in systems
Negative Common Meaning	Anything called a virus is doomed to be deemed bad

V. Bontchev, “Are ‘Good’ Computer Viruses Still a Bad Idea?” EICAR’94

A. Lee
S. Cobb

All risks must be addressed, but focus on 4

TECHNICAL REASONS	
Lack of Control	Spread cannot be controlled, unpredictable results
Recognition Difficulty	Hard to allow good viruses while denying bad
Resource Wasting	Unintended consequences (typified by the Morris Worm)
Bug Containment	Difficulty of fixing bugs in code once released
Compatibility Problems	May not run when needed, or cause damage when run
Effectiveness	Risks of self-replicating code over conventional alternatives
ETHICAL AND LEGAL REASONS	
Unauthorized Data Modification	Unauthorized system access or data changes illegal or immoral
Copyright and Ownership Problems	Could impair support or violate copyright of regular programs
Possible Misuse	Code could be used by persons will malicious intent
Responsibility	Sets a bad example for persons with inferior skills, morals
PSYCHOLOGICAL REASONS	
Trust Problems	Potential to undermine user trust in systems
Negative Common Meaning	Anything called a virus is doomed to be deemed bad

A. Lee
S. Cobb

All risks must be addressed, but focus on 4

1. Recognition Difficulty
2. Compatibility Problems & Effectiveness
3. Possible Misuse
4. Trust Problems

A. Lee
S. Cobb

1. Recognition Difficulty

- Hard to allow good viruses while denying bad
- No self-respecting antivirus company is going to give your righteous malware a free pass

A. Lee
S. Cobb

Bear in mind the AV community is global

- Major AV vendors encompass many countries
  - ESET *Slovakia* AVG *Czech Republic*
  - McAfee *USA* Kaspersky *Russia*
  - Symantec *USA* Trend Micro *Japan,*
  - Avira *Germany* Avast! *Czech Republic*
- Active in many more (e.g. ESET operates in 180)
- "Your cyber defense is only as good as your relationship with industry." – Dr. Jamie Shea

2. Compatibility and Effectiveness

- May not run when needed, or may cause damage when run
- Huge potential for unintended consequences
- Reduce risk with detailed intel on the target?
- Raises issue of Effectiveness:
  - Does the effort to get enough intel to execute safely exceed the effort of a less risky path to same end?

3. Possible Misuse

- Could be re-used by persons with malicious intent
- Yes, your own code could be used against you
- The key ingredient for making malware is brains
- Brains are very mobile, no country has a lock
- "The most valuable cyber weapon you can possess? The talented individual.“ – Jarno Limnéll

4. Trust Problems

- Potential to undermine user trust in systems
- 60% now less trusting of technology companies
  - e.g. Internet service providers, software companies
- Very real risk of economic damage

A. Lee
S. Cobb

Harris Poll on behalf of ESET, February 4-6, 2014, 2,034 U.S. adults ages 18 and older

Companies and consumers impacted

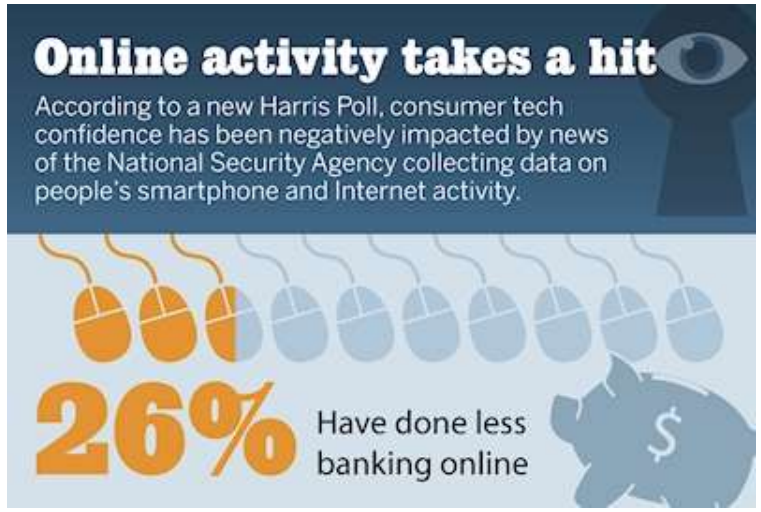
- Cloud providers
- Banks
- Companies like Cisco
- Online retailers
- Healthcare providers
- Governments

NASDAQ

CSCO

A. Lee
S. Cobb

85% of Americans are aware of NSA revelations, 47% of them have changed their online behavior



Harris Poll on behalf of ESET, February 4-6, 2014, 2,034 U.S. adults ages 18 and older

A. Lee
S. Cobb

Righteous malware deployment checklist:

Control	Can you control the actions of the code in all environments it may infect?
Detection	Can the code complete its mission before detection?
Attribution	Can you guarantee the code is deniable or claimable, as needed?
Legality	Will the code be illegal in any jurisdictions in which it is deployed?
Morality	Will deployment of the code violate any treaties, codes, and other international norms?
Misuse	Can the code, or its techniques, strategies or design principles be copied by adversaries, competing interests, or criminals?
Erosion of Trust	Have you considered harmful effects that deployment of the code, including knowledge of the deployment, could have on trust placed in your government and institutions including trade and commerce?

A. Lee
S. Cobb

Further research?

- Mathematical model of malware risks
  - Enumerate variables
  - Calculate compound probabilities
- Comprehensive survey of malware researchers
  - Update the “Good virus bad idea” paper

A. Lee
S. Cobb

Summary: deploying malware

- Comes with many risks that are known and well-documented
- Carries serious potential to undermine the very societies it is intended to defend

A. Lee
S. Cobb

Thank you!

- Stephen.Cobb@ESET.com
- Twitter @zcobb
- www.SlideShare.net/zcobb
- www.LinkedIn/in/StephenCobb
- www.WeLiveSecurity.com