

# Top Ten Cyber Threats



**Margaret M. McMahon, Ph.D.**

**ICCRTS 2014**

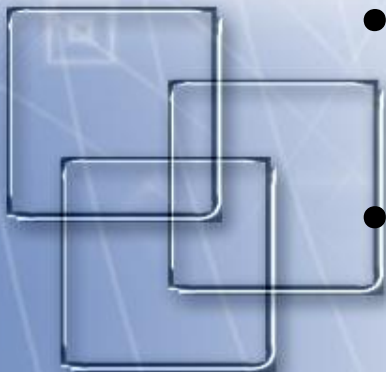


# Introduction



# Outline

- Motivation
- How malware affects a system
- Top Ten (Simple to complex)
  - Brief description
  - Explain impacts
  - Main takeaways
  - Relevance to Command and Control
- Increase awareness of cybersecurity threats and vulnerabilities
- Conclusion



# Motivation

- Connected computers are vulnerable
  - Direct attacks
  - Automated attacks
- Several key concepts emerge
- Bridge language and topics of malware from academia to operational community



# How Malware Affects a System

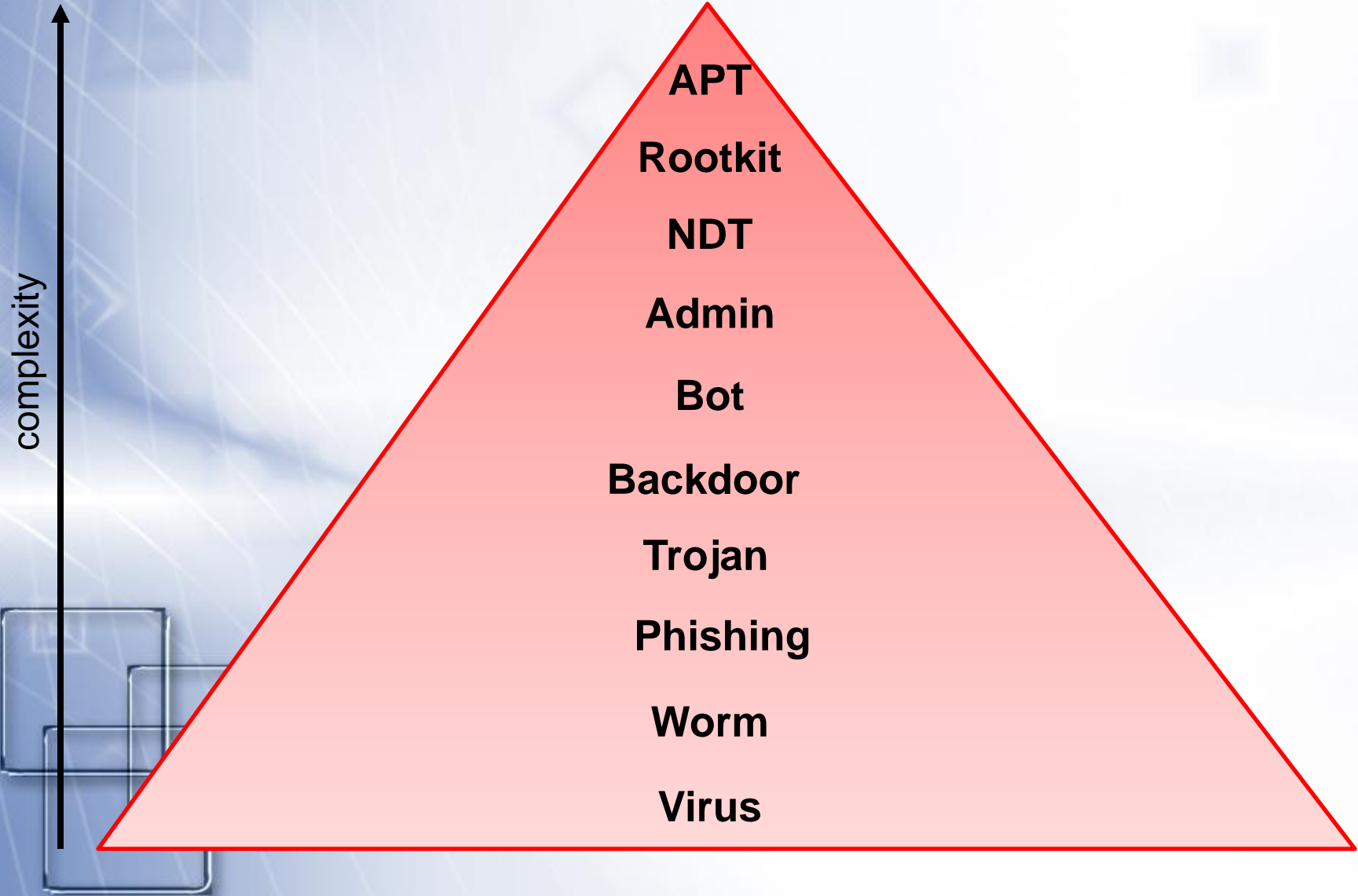
- Look at FROP
  - Files
  - Registry
  - Open Ports
  - Processes
- Add, delete, modify

How to analyze:

- Snapshot
- Compare after infection, restart



# Top Ten



# Virus

- Define:
  - Part of Program
  - Manual Propagation (also macros)
- Impact:
  - Disruption or destruction
- Takeaway:
  - AV Scan incoming e-mail and documents
  - Do not click on links



# Virus: Relevance to C2

- Malware that disrupts C2 can be downloaded as a virus attachment in an e-mail





# Worm

- Define:
  - Propagates automatically
  - Consumes resources
- Impact:
  - Any networked computer is vulnerable
- Takeaway:
  - Control propagation
  - Harden shared drives with password protection



# Worm: Relevance to C2

- Lose bandwidth in a communications channel
- Lose processor cycles on a key computer in a network  
(e.g. an air operations center)



# Phishing

- Define:
  - Phishing, spear phishing, whaling
- Impact:
  - Easier than breaking into a system
  - Can target based on social media participation
- Takeaway:
  - Don't click on links in e-mails
  - Don't open e-mails from people you don't know



# Phishing: Relevance to C2

- Social engineering can be used
- E-mails to key personnel



# Trojan

- Define:
  - Package something undesirable together with something desirable
- Impact:
  - Legitimate software delivers something extra
- Takeaway:
  - Can be easily constructed (iExpress)
  - Check published Md5 hashes
  - Install: backdoor, bot, admin tools



# Trojan: Relevance to C2

- Delivery mechanism for malicious code that can disrupt and delay C2 channels



# Backdoors

- Define: Enter computer system not in a normal manner
- Impact:
  - Trojan can open a port and install reverse shell
  - New user added with trusted connection
  - Easter egg: programmer adds code to allow special privileges
- Takeaway:
  - Start with your own source code and compile



# Backdoors: Relevance to C2

- Intruder can access, modify, or delete critical configuration information in a C2 node





# Bots

- Define:
  - Individual machines called zombies
  - Part of a C2 structure
  - Distributed processing
    - Distributed Denial of Service (DDoS)
    - Password cracking
  - Financial gain
- Impact:
  - Bots call home for C2
  - Can download file(s) to execute
  - Coordinate with other bots
  - 61.5% of traffic on the Internet in 2013



# Bots (continued)

- Takeaway:
  - Different actions at different times because of bot leasing
  - Bots are noisy on a network



# Bots: Relevance to C2

- A radio with limited bandwidth used in an amphibious assault
  - Beaconing
  - Covert exfiltration of critical information



# Admin Tools

- Define:
  - Legitimate opening of a port for access
  - Installing server
- Impact:
  - Whole frameworks are available
- Takeaway:
  - Remote trouble shooting leaves an open door
  - Remote user can add, delete, modify:
    - Files, processes, registry, network
  - Need to check indicators against a baseline of normal activity



# Admin Tools: Relevance to C2

- Full control to add, delete and modify anything on a computer
- Allow remote access to video feeds
- An intruder is present in the room or on the computer to observe actions or intentions
- Could be installed via Trojan horse vector



# Network Diagnostic Tools

- Define:
  - Used by system administrator inside network
  - Checklist for vulnerabilities
  - NMAP
- Impact:
  - Used in conjunction with other malware
  - Once inside network
    - Can get a full map of internal network
- Takeaway:
  - Many tools used for good or evil
  - Use IDS to see if unauthorized scanning activity



# Network Diagnostic Tools: Relevance to C2

- Network tools scan for vulnerabilities
- Provide a blueprint for a successful attack on the computers in a network



# Rootkits

- Define:
  - Hide files, processes, registry keys and open ports
- Impact:
  - Interfere with operating system reporting of processes, file system contents
  - You don't know what you don't know
- Takeaway:
  - Cannot trust normal tools
  - Do not use unsigned drivers
  - Kernel mode: May need to reload system





# Rootkits: Relevance to C2

- A rootkit on a node allows any or all of the above types of malware to operate covertly
- Cannot see the process or file
- Need special tools to diagnose



# Advanced Persistent Threat

- Define:
  - Combination of all of the above
  - Being used by trained, persistent people
  - Funded by governments, criminals
- Impact:
  - Target a specific organization, for a specific goal
  - You may be the target
- Takeaway:
  - Be frightened: it's real



# Advanced Persistent Threat: Relevance to C2

- Major offensive effort
- May have to accept that dedicated attackers will get into C2 nodes
  - Accept that they will enter a system
  - Reduce how long they are in a system
  - Noisier to get out than in
  - Deny them outgoing communications




# Increasing Cyberthreat Awareness


- Learn about current threats
- Learn about a specific virus / malware
- Use trusted databases:
  - Malware's characteristics
  - Method of infection
  - Removal
  - Variants
  - Area of the world where the malware is currently proliferating



# National Vulnerability Database



Sponsored by  
DHS National Cyber Security Division/US-CERT



National Institute of  
Standards and Technology

## National Vulnerability Database

automating vulnerability management, security measurement, and compliance checking

<a href="#">Vulnerabilities</a>	<a href="#">Checklists</a>	<a href="#">800-53/800-53A</a>	<a href="#">Product Dictionary</a>	<a href="#">Impact Metrics</a>	<a href="#">Data Feeds</a>	<a href="#">Statistics</a>
<a href="#">Home</a>	<a href="#">SCAP</a>	<a href="#">SCAP Validated Tools</a>	<a href="#">SCAP Events</a>	<a href="#">About</a>	<a href="#">Contact</a>	<a href="#">Vendor Comments</a>

**Mission and Overview**

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

**Resource Status**

**NVD contains:**

- 60348 [CVE Vulnerabilities](#)
- 227 [Checklists](#)
- 248 [US-CERT Alerts](#)
- 2818 [US-CERT Vuln Notes](#)
- 10286 [OVAL Queries](#)
- 83734 [CPE Names](#)

Last updated: 2/4/2014

CVE Publication rate: 19.2

**Email List**

### National Vulnerability Database Version 2.2

NVD is the U.S. government repository of standards based vulnerability management data represented using the [Security Content Automation Protocol \(SCAP\)](#). This data enables automation of vulnerability management, security measurement, and compliance. NVD includes databases of security checklists, security related software flaws, misconfigurations, product names, and impact metrics.

**Federal Desktop Core Configuration settings (FDCC)**

NVD contains content (and pointers to tools) for performing configuration checking of systems implementing the [FDCC](#) using the Security Content Automation Protocol ([SCAP](#)). [FDCC Checklists](#) are available here (to be used with SCAP FDCC capable tools). [SCAP FDCC Capable Tools](#) are available here.

**NVD Primary Resources**

- [Vulnerability Search Engine](#) (CVE software flaws and CCE misconfigurations)
- [National Checklist Program](#) (automatable security configuration guidance in XCCDF and OVAL)
- [SCAP](#) (program and protocol that NVD supports)
- [SCAP Compatible Tools](#)
- [SCAP Data Feeds](#) (CVE, CCE, CPE, CVSS, XCCDF, OVAL)
- [Product Dictionary](#) (CPE)
- [Impact Metrics](#) (CVSS)
- [Common Weakness Enumeration](#) (CWE)

---

**NVD/SCAP Recent Activity:**

- October 3rd - 5th, 2012: [8th Annual IT Security Automation Conference](#)
- October 31st - November 2nd, 2011: [7th Annual IT Security Automation Conference](#)
- August 29th - 30th, 2011: [EMAP Developer Workshop](#)
- September 27th - 29th, 2010: [6th Annual IT Security Automation Conference](#)



# Security Focus Homepage



## Symantec Connect

A technical community for Symantec customers, end-users, developers, and partners.

[Join the conversation >](#)

## Vulnerabilities

### [Oracle MySQL Server CVE-2014-0431 Remote Security Vulnerability](#)

2014-02-05

<http://www.securityfocus.com/bid/64897>

### [Mozilla Firefox/Thunderbird/SeaMonkey CVE-2014-1478 Multiple Memory Corruption Vulnerabilities](#)

2014-02-05

<http://www.securityfocus.com/bid/65324>

### [Mozilla Firefox/Thunderbird/SeaMonkey CVE-2014-1477 Multiple Memory Corruption Vulnerabilities](#)

2014-02-05

<http://www.securityfocus.com/bid/65317>

### [ImpressCMS Arbitrary File Access And Multiple Cross Site Scripting Vulnerabilities](#)

2014-02-05

<http://www.securityfocus.com/bid/65279>

### [Oracle MySQL Server CVE-2013-5894 Remote Security Vulnerability](#)

2014-02-05

<http://www.securityfocus.com/bid/64873>

### [Oracle MySQL Server CVE-2014-0427 Remote Security Vulnerability](#)

2014-02-05

<http://www.securityfocus.com/bid/64868>

### [Oracle MySQL Server CVE-2013-5881 Remote Security Vulnerability](#)

2014-02-05

<http://www.securityfocus.com/bid/64885>

### [Oracle MySQL Server CVE-2014-0386 Remote Security Vulnerability](#)

2014-02-05

<http://www.securityfocus.com/bid/64904>

### [Oracle MySQL Server CVE-2014-0433 Remote Security Vulnerability](#)

2014-02-05

<http://www.securityfocus.com/bid/64895>

### [Oracle MySQL Server CVE-2014-0402 Remote Security Vulnerability](#)

2014-02-05

<http://www.securityfocus.com/bid/64908>

# McAfee Threat Center



An Intel Company

Business Home | About Us | Purchase



TESTED 04-FEB

Threat Center

Products & Solutions

Services

Support

Partners

Community

Business Home



## Breaking Advisory

January 14, 2014: As announced, Microsoft has released their January Security Bulletins. A total of 4 bulletins have been released. Affected software includes Microsoft Windows, Office, and Server Software. 1 of the bulletins is rated as 'Important' and carries a potential impact of remote code execution. [Learn](#)

[More](#) ➔

## Threat Center



### McAfee Labs 2014 Predictions Report

[Download Report](#) ➔

### Feedback

- [Submit a Virus or Malware Sample](#)
- [Dispute a URL or Classification](#)
- [Dispute a Detection](#)

### Search the Threat Library

- |  |   |   |
|--|---|---|
| <input type="radio"/> Application Name | <input type="radio"/> IP Address              | <input type="radio"/> Website URL / Address |
| <input type="radio"/> DNS Server       | <input checked="" type="radio"/> Malware Name | <input type="radio"/> Vulnerability Name    |
| <input type="radio"/> Intrusion Attack | <input type="radio"/> Domain Name             |   |



NSS Labs Endpoint Protection: Test Report

The

# 2014 US State of Cybercrime Survey

- Co-sponsored by PwC, CSO magazine, the CERT® Division of the Software Engineering Institute at Carnegie Mellon University, and the United States Secret Service
- The most frequent types of incidents:
  - Malware
  - Phishing
  - Network interruption
  - Spyware
  - Denial of service attacks
- Cyberadversaries use sophisticated targeting techniques
  - Criminals,
  - Nation-states





# Education

- About Threats
- Behavior of infected computers
  - Investigate qualities of different types of malicious software
  - Changes to infected computer's files and registry, and the network and process activity
- Malicious Network Traffic Analysis
  - Explore the network delivery methods
  - Determine if there has been abnormal network behavior
  - Isolate any malware transmitted over the network



# Conclusions

- Every threat is still out there
  - Slightly changed to create a new signature
  - Combined threats for more complex attacks
  - Malware is available in kits
- Firewalls, and defense-in-depth
- Keep AV up-to-date
  - Only identifies known signatures
  - Cannot detect zero-day threats
- Keep users up-to-date
  - Understanding “normal” processes and traffic
- Education is the key to meet the threat



# Thank You!

- Questions?
- To learn more:  
[www.anrc-services.com](http://www.anrc-services.com)  
[mac@anrc-services.com](mailto:mac@anrc-services.com)

