

Cyber Operations: **Malware**

Maj Brian M. Hawkins, USMC
Office: 326 Michelson, x3-6572
bhawkins@usna.edu

Please turn in completed **Blue** / **Gold** Cyber Recon Worksheets...

Name/alpha/section: / /		My Network (circle): BLUE / GOLD	
My Host IP: 3 / 0	My WEB server IP: 4 / 0	My DNS server IP: 3 / 0	
Full Host Name:	Full Host Name:	Full Host Name:	

Target Hosts on your Opponent's Network:

www.blue.net OR www.gold.net	IP address:	Full Host Name:	OS:	15 / 0	
Port	Service	Service Software Name & Version	Port	Service	Service Software Name & Version

Other	IP address:	Full Host Name:	OS:	10 / 0	
Port	Service	Service Software Name & Version	Port	Service	Service Software Name & Version

DNS server	IP address:	Full Host Name:	OS:	5 / 0	
Port	Service	Service Software Name & Version	Port	Service	Service Software Name & Version

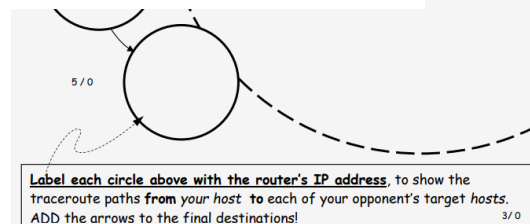
Network is (circle): BLUE / GOLD
as shown in the lab for each of
on the opponent network: 30 / 0

Network (no firewall)



10 / 0
Opponent website clues:
Provide a list of underlined
usernames and also any clues
to potential user passwords
for each username:

Describe any other clues you
discovered on the opponent's
website: (web page
vulnerabilities, hidden or
encrypted content...)



Learning Targets

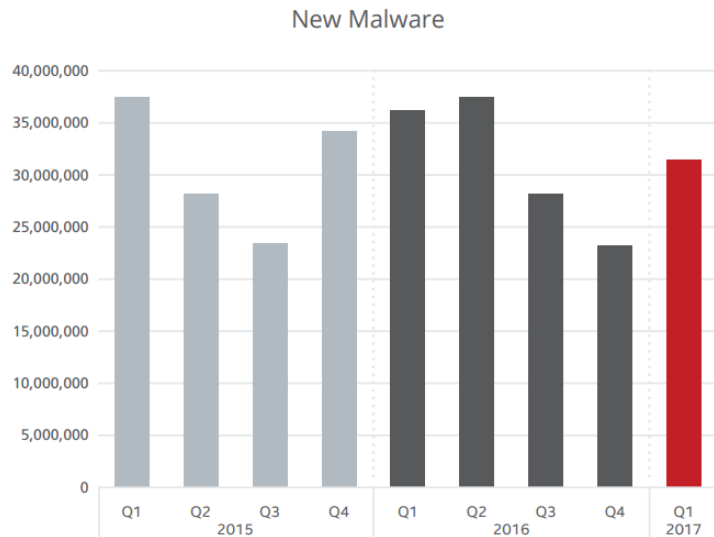
- Explain what malware is.
- Describe different types of malware:
 - virus, worm, trojan
- Give an example of malware used in an operational context.

Outline

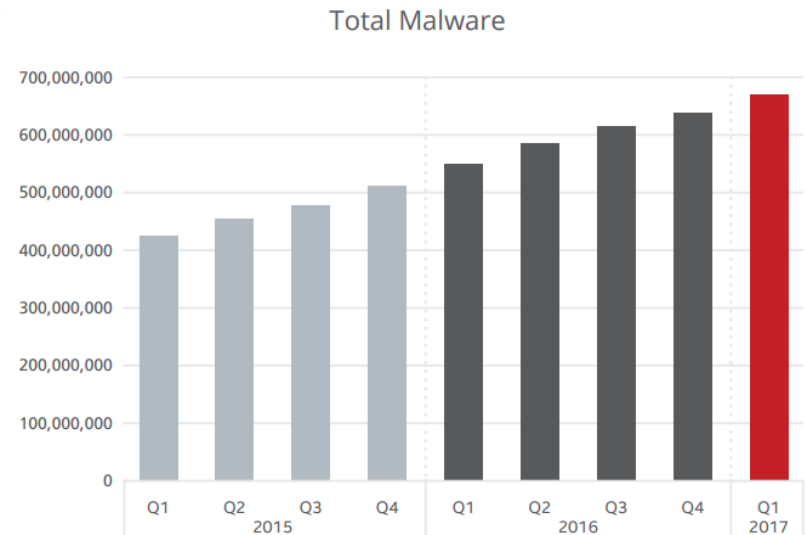
- Why is Malware important
- What is Malware
- Malware types
- MSG Board DEMO
- Case studies
- Surprise :)

Why is Malware Important?

- It's everywhere!
- It causes lots of problems



Source: McAfee Labs, 2017.



Source: McAfee Labs, 2017.

What is malware?

- **Malicious Software**
 - Violates 1 or more of the five cybersecurity pillars [CIANA]
- Common Functions
 - Exfiltrate (steal) files
 - Delete files
 - Hold files for ransom
 - Turn system into a zombie
 - Install keylogger
 - Activate microphone or camera
 - Foothold for future attacks

Malware Types

- **Virus**
 - Infects systems or files
 - Can replicate, but requires human interaction
 - Mostly unknown to the user
- **Worm**
 - Like a virus, but can self propagate
- **Trojan Horse**
 - Useful software that holds a malicious payload
 - Ex. Game that also has a keylogger

Trojan: Scareware

- User visits a website
 - Window pops up indicating there are 100 viruses on the computer
 - User downloads and installs advertised anti-virus program
 - Program indicates viruses are removed
 - Instead the program has installed malware without victim knowledge
 - Often botnets are created this way

Viruses and Trojans provide a different kind of attack vector...

- tricking users into letting us in, rather than defeating firewalls, authentication, etc.

Self Replicating Code

A BASIC EXAMPLE

The good 'ol Message Board

- Go to:
 - <http://rona.academy.usna.edu/~bhawkins/msg3/mb.html>
- Create a new account
- Post a simple message

```
<em id="foo">
I love SY110!
<script type="text/javascript">
if(Math.random()<0.05)
{
  document.location="mb.cgi?msg="
  +
  encodeURIComponent('<em id="foo">' +
document.getElementById("foo").innerHTML + '</em>');
}
</script>
</em>
```

CASE STUDIES

Samy Worm

- Attack against MySpace
- Posted “Samy is my hero” to user’s page
 - When another user viewed the page it would be posted to their own page
- Infected one million users in 20 hours



Samy Kamkar

CNET • Security • Samy opens new front in worm war

Samy opens new front in worm war

Security experts fear would-be attackers will copy the worm, which exploits an unaddressed scripting flaw.

Security

by Munir Kotadia
October 20, 2009 9:40 AM PDT



The newly discovered Samy worm is one of the first to exploit a cross-site scripting vulnerability, a technique security experts fear could be used to open a new front in attacks. Samy is a self-propagating worm that appears to have been written by a member of MySpace.com, a community site dedicated to helping friends stay in touch and share pictures. By exploiting vulnerabilities in the MySpace.com site, the worm added a million users to the author's "friends" list.

Although the worm is no threat to other Web sites, security experts say the new self-propagating cross-site scripting (XSS) worm will likely be copied by other writers of malicious software.

Adam Biviano, senior systems engineer at Trend Micro Australia and New Zealand, explained that the MySpace.com user—called Samy—had created a "malicious" profile by taking advantage of a flaw in the Web site's design. The profile, when viewed, automatically activated code to add the visitor to Samy's "Friends" list.

<https://www.cnet.com/news/samy-opens-new-front-in-worm-war/>

Duqu

- Infiltration
 - Phishing attack with a Word document attached
- The Exploit
 - Exploited a vulnerability in how Word handles fonts
- The consequence
 - Installed keylogger and screen capture utility

<http://www.verizonenterprise.com/DBIR/2015/>

23%

OF RECIPIENTS NOW
OPEN PHISHING
MESSAGES AND
11% CLICK ON
ATTACHMENTS.



From: Jason B <bjason1[REDACTED].com>

Sent: Bc 17.04.2011 14:26

To: [REDACTED]

Cc:

Subject: [REDACTED] Request for services

 Message  [REDACTED]request.doc (262 KB)

Dear Sir

I found the details of your company on your web site, and would like to establish business cooperation with your company. In the attached file, please see a list of requests.

Thank you,
Best Regards
Mr. B. Jason
Marketing Manager

Please send me the following information:

1. Your company's profile
2. Recommendations from previous costumers
3. Price list for inland shipping
4. Price list for storage of goods
5. Do you supply marine shipping?



Mirai

- October 21, 2016: BOTNET DDoS against DNS infrastructure



Krebs on Security
In-depth security news and investigation

30 **New Mirai Worm Knocks 900K Germans Offline**
NOV 16

More than 900,000 customers of German ISP **Deutsche Telekom** (DT) were knocked offline this week after their Internet routers got infected by a new variant of a computer worm known as **Mirai**. The malware wriggled inside the routers via a newly discovered vulnerability in a feature that allows ISPs to remotely upgrade the firmware on the devices. But the new Mirai malware turns that feature off once it infects a device, complicating DT's cleanup and restoration efforts.

Security experts say the multi-day outage is a sign of things to come as cyber criminals continue to aggressively scour the Internet of Things (IoT) for vulnerable and poorly-secured routers, Internet-connected cameras and digital video recorders (DVRs). Once enslaved, the IoT devices can be used and rented out for a variety of purposes — from conducting **massive denial-of-service attacks** capable of knocking large Web sites offline to **helping cybercriminals stay anonymous online**.



My New Book!



A New York Times

Buy at A

Donate

“More than 900,000 customers of German ISP **Deutsche Telekom** (DT) were knocked offline this week after their Internet routers got infected by a new variant of a computer worm known as **Mirai**.”

<https://krebsonsecurity.com/2016/11/new-mirai-worm-knocks-900k-germans-offline/>

Ransomware

Malware that steals, deletes, or encrypts a victims files and then requests payment to restore the data.

Ransomware Took San Francisco's Public Transit for a Ride

Hackers forced the light rail network to leave service to avoid a massive disruption to service.

by Jamie Condliffe November 28, 2016



While the city dealt with a ransomware attack, passengers got

Hospital pays ransom, ransomware demands more money

BY LEE MATHEWS
05.24.2016 :: 11:17AM EST



Ransomware infections can be a good idea to pay up, and a hospital in

Home > Cybercrime & Cybersecurity > Report: Ransomware on Internet-Enabled Medical Devices a Growing Threat

Report: Ransomware on Internet-Enabled Medical Devices a Growing Threat

Cybercrime & Cybersecurity

51

This post was originally published here: [post](#)

Cyber attackers are increasingly breaching Internet-enabled medical devices using ransomware and this is likely to continue for the next two to four years, according to Intel Security's recent McAfee Labs 2017 Threats Predictions Report.

According to the threat predictions report, in which Intel Security interviewed 31 security thought leaders, while it is not currently known why attackers are breaching medical devices that collect patient data, the attacks are happening and medical data is being exfiltrated.

"More ominously, medical devices that monitor and control human systems—including pacemakers, insulin pumps, and nerve stimulators—are all becoming Internet enabled. Unethical attackers will see these medical devices as the next step in their journey beyond hospital ransomware attacks. Hospitals are successful ransomware targets partly because they need immediate access to information. A pacemaker is an ultimate example of the need for immediate access, so attackers will attempt to find vulnerabilities in these devices as they become Internet enabled and will be able to extort a great deal of money if they are successful," the report authors wrote.

Facebook

Facebook

ransomidrop.com



WannaCry

ransomware cryptoworm

- May 2017 -- targeted computers running the **Microsoft Windows** operating system by **encrypting data** and demanding **ransom** payments in the **Bitcoin cryptocurrency**.
- Affected **16 hospitals** in England and Scotland, and up to **70,000 devices** – including computers, MRI scanners, and blood-storage refrigerators
- 200,000 computers were infected across 150 countries
 - Most affected countries:
 - Russia, Ukraine, India and Taiwan.



Ooops, your files have been encrypted!

English

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

CMT from Monday to Friday

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

[About bitcoin](#)

[How to buy bitcoins?](#)

[Contact Us](#)



Send \$300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Copy

Check Payment

Decrypt

Petya

- Ransomware discovered in 2016
- Infects master boot record (MBR) to encrypts a hard drive's file system table and prevents Windows from booting.
- Demands user make payment in Bitcoin in order to regain access to the system.

```

uu$::$:::$:::$:::$uu
uu$$$$$$$$$$$$$$$$$$$$uu
u$$$$$$$$$$$$$$$$$$$$$u
u$$$$$$$$$$$$$$$$$$$$$u
u$$$$$$$$$$$$$$$$$$$$$u
u$$$$$$$$$$$$$$$$$$$$$u
u$$$$$$$$$$$$$$$$$$$$$u
u$$$$$$$*   *$$$$*   *$$$$$u
*$$$$$*       u$u       $$$*$
$$$u         u$u         u$$$
$$$u         u$$$u       u$$$
*$$$$$uu$$$   $$$uu$$$$$*
*$$$$$$$$$*   *$$$$$$$$$*
u$$$$$$$$$u$$$$$$$$$u
u$*$*$*$*$*$*$*$*$*$u
uuu          $$$u$ $ $ $ $u$$          uuu
u$$$$$      $$$$$u$u$u$$$      u$$$$$
$$$$$uu     *$$$$$$$$$$$*      uu$$$$$$$
u$$$$$$$$$$$$$$$$$uu      *****      uuuu$$$$$$$$$$$$$
$$$$$*$$*$$$$$$$$$$$$uuu      uu$$$$$$$$$$$$$*$$*$$$*
***          **$$$$$$$$$$$$$$$$uu **$***
uuuu *$$$$$$$$$$$$$$$$uuu
u$$$$uuu$$$$$$$$$$$$uu **$$$$$$$$$$$$$$$$uuu$$$
$$$$$$$$$$$$$*$$$*          **$$$$$$$$$$$$$$$$$*
*$$$$$$$*                    **$$$$$$$*
$$$*          PRESS ANY KEY!          $$$*$

```


FLATRON

Oops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send \$300 worth of Bitcoin to following address:

1Mz7153HMuxXTuR2R1t78wGSdzaAtMbBWx

2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key:

cyDnsh-fSebwG-yPU1Av-ybXzTa-B1CqTi-4GWHtW-11SnPk-NpAF58-KEhgW1-wLhPRb

If you already purchased your key, please enter it below.

Key: _

Proof of Concept - Pacemaker



<https://vimeo.com/187962970>

MALWARE DEFENSE

Malware Defense

- Principle of least privilege
- Be careful when opening E-mail attachments or links
- Install anti-virus software, and keep it up to date!
- Disable autorun
- Be careful with USB thumb drives
- Install operating system updates
- Only visit trusted websites
- Report suspicious/abnormal activity
- Backup files
- Turn off system when not in use

Surprise!...

- Go to the webpages that you made for class...

<https://rona.academy.usna.edu/~m21xxxx/>

Learning Targets

- Explain what malware is.
- Describe different types of malware: virus, worm, trojan.
- Give an example of malware used in an operational context.

Questions?

- Malware BB HW due 07:45 Wednesday