Malware

What is it?

What are some types?

Some Classifications

Adware

Spyware

Potentially Unwanted (Program | Application) [PUP or PUA]

Trojan

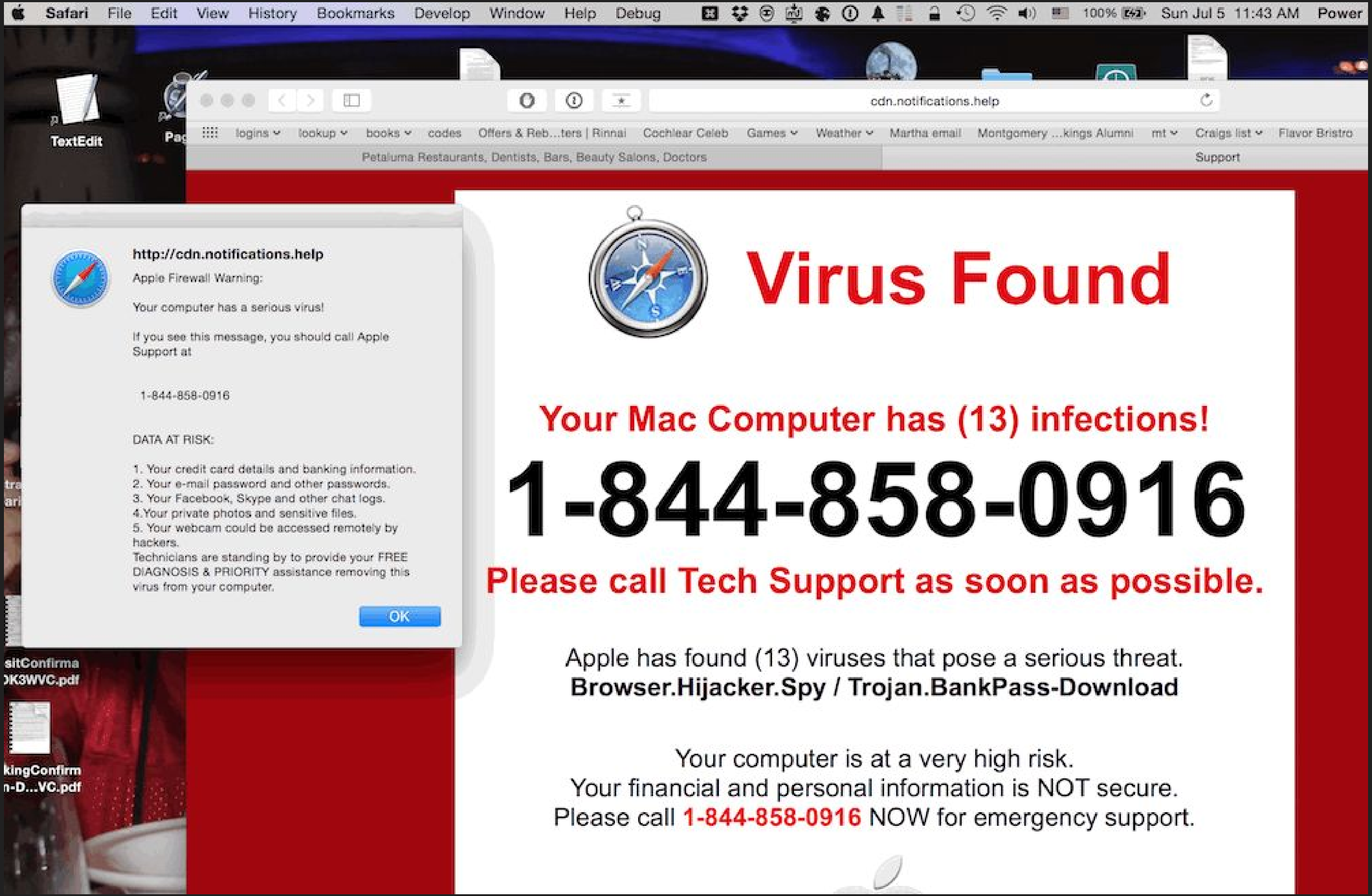
Rootkit

Ransomware

Virus

Worm

Bot


Safari File Edit View History Bookmarks Develop Window Help Debug
100% Sun Jul 5 11:43 AM Power
TextEdit
Pag
cdn.notifications.help
logins lookup books codes Offers & Reb…ters | Rinnai Cochlear Celeb Games Weather Martha email Montgomery …kings Alumni mt Craigs list Flavor Bristro
Petaluma Restaurants, Dentists, Bars, Beauty Salons, Doctors
Support
sitConfirma
)K3WVC.pdf
kingConfirm
n-D…VC.pdf
OK

http://cdn.notifications.help

Apple Firewall Warning:

Your computer has a serious virus!

If you see this message, you should call Apple Support at

1-844-858-0916

DATA AT RISK:

1. Your credit card details and banking information.
2. Your e-mail password and other passwords.
3. Your Facebook, Skype and other chat logs.
4.Your private photos and sensitive files.
5. Your webcam could be accessed remotely by hackers.

Technicians are standing by to provide your FREE DIAGNOSIS & PRIORITY assistance removing this virus from your computer.

Virus Found

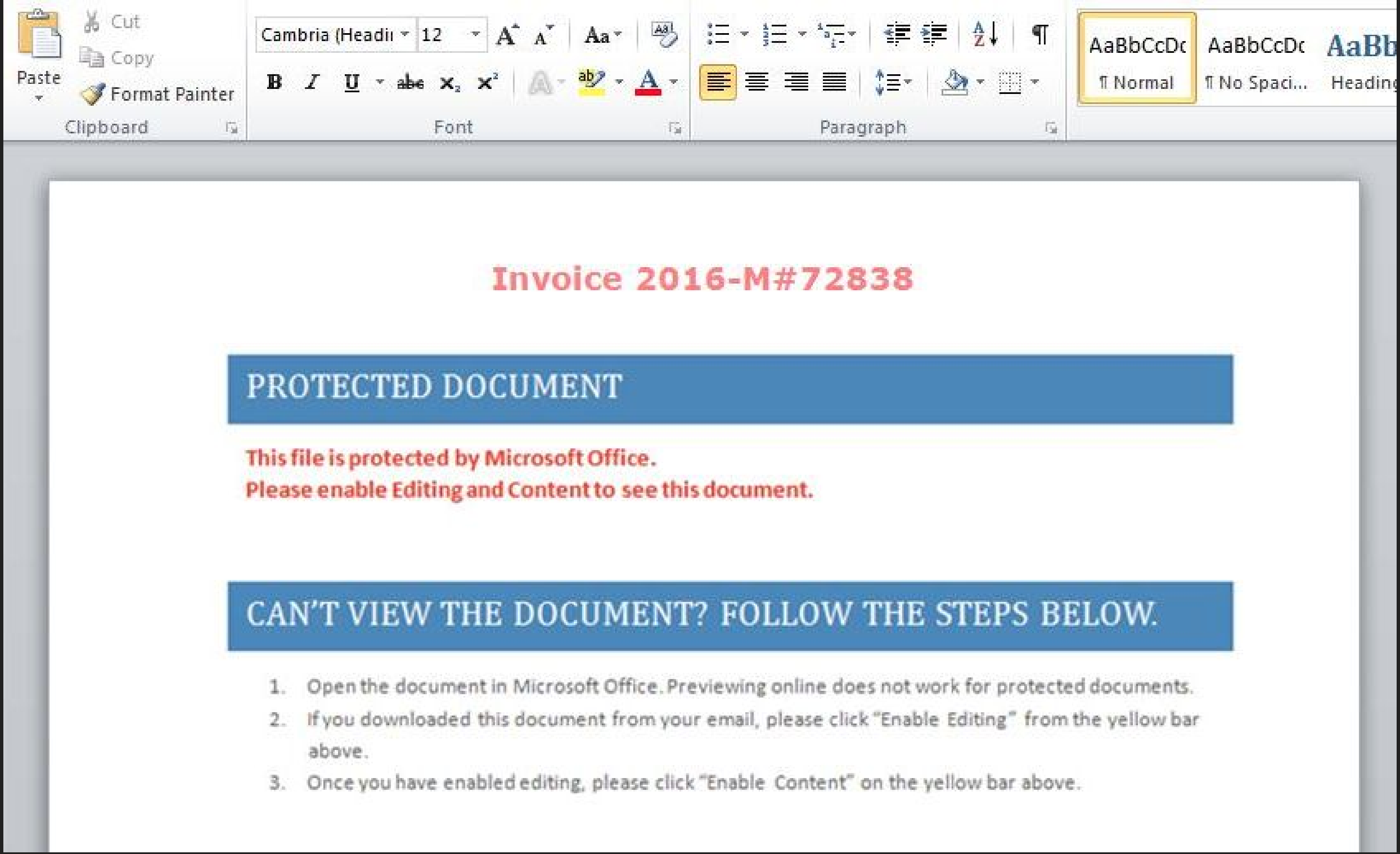
Your Mac Computer has (13) infections!

1-844-858-0916

Please call Tech Support as soon as possible.

Apple has found (13) viruses that pose a serious threat.
Browser.Hijacker.Spy / Trojan.BankPass-Download

Your computer is at a very high risk.
Your financial and personal information is NOT secure.
Please call 1-844-858-0916 NOW for emergency support.



Invoice 2016-M#72838

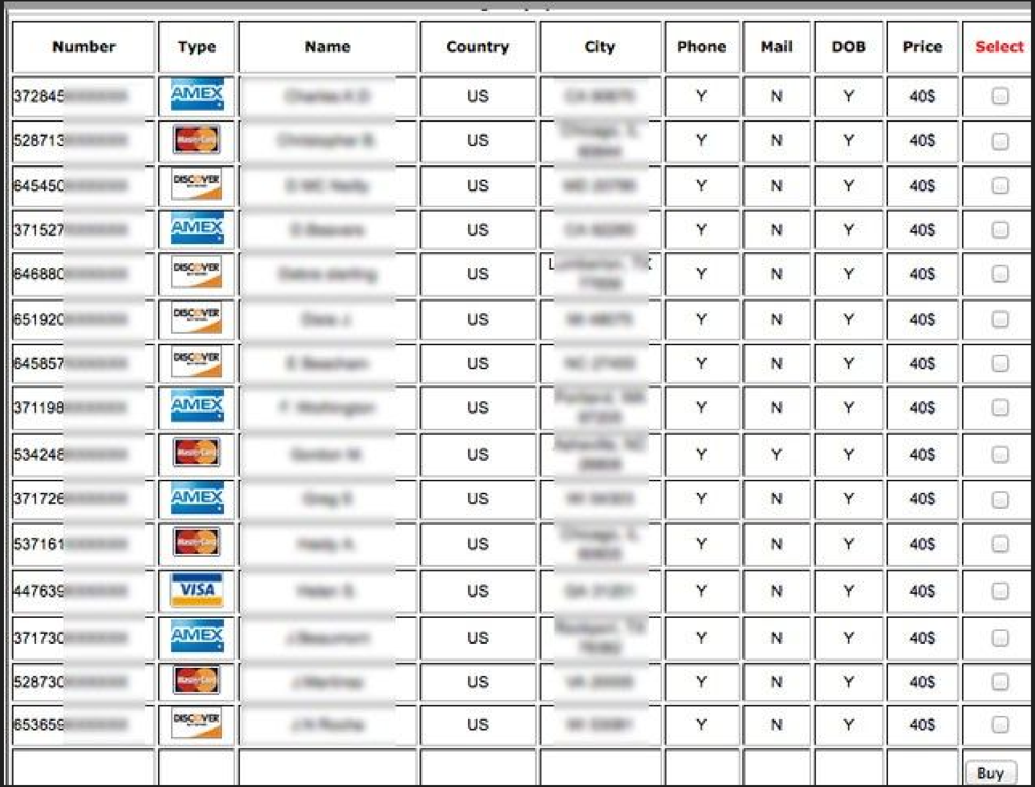
PROTECTED DOCUMENT

This file is protected by Microsoft Office.
Please enable Editing and Content to see this document.

CAN'T VIEW THE DOCUMENT? FOLLOW THE STEPS BELOW.

1. Open the document in Microsoft Office. Previewing online does not work for protected documents.
2. If you downloaded this document from your email, please click "Enable Editing" from the yellow bar above.
3. Once you have enabled editing, please click "Enable Content" on the yellow bar above.

Why do people make it?



Number	Type	Name	Country	City	Phone	Mail	DOB	Price	Select
372845[redacted]	AMEX	[redacted]	US	[redacted]	Y	N	Y	40$	□
528713[redacted]	MasterCard	[redacted]	US	[redacted]	Y	N	Y	40$	□
645450[redacted]	DISCOVER	[redacted]	US	[redacted]	Y	N	Y	40$	□
371527[redacted]	AMEX	[redacted]	US	[redacted]	Y	N	Y	40$	□
646880[redacted]	DISCOVER	[redacted]	US	[redacted]	Y	N	Y	40$	□
651920[redacted]	DISCOVER	[redacted]	US	[redacted]	Y	N	Y	40$	□
645857[redacted]	DISCOVER	[redacted]	US	[redacted]	Y	N	Y	40$	□
371198[redacted]	AMEX	[redacted]	US	[redacted]	Y	N	Y	40$	□
534246[redacted]	MasterCard	[redacted]	US	[redacted]	Y	Y	Y	40$	□
371726[redacted]	AMEX	[redacted]	US	[redacted]	Y	N	Y	40$	□
537161[redacted]	MasterCard	[redacted]	US	[redacted]	Y	N	Y	40$	□
447639[redacted]	VISA	[redacted]	US	[redacted]	Y	N	Y	40$	□
371730[redacted]	AMEX	[redacted]	US	[redacted]	Y	N	Y	40$	□
528730[redacted]	MasterCard	[redacted]	US	[redacted]	Y	N	Y	40$	□
653659[redacted]	DISCOVER	[redacted]	US	[redacted]	Y	N	Y	40$	□
									Buy

Some Motivations

Making $$$

Stealing Information - Nation states / military adversaries

Releasing Information - hacktivism

Taking down services - military / hacktivism

Pranks

Because you can

What are some common infection vectors?

Common Infection Vectors

Phishing emails

Infected websites and advertisements

Exploit kits

- Browser / Application exploits

Social Engineering

Infected removable media

Self-propagating

Common Exfiltration Mechanisms

- Collecting data / host enumeration
  - Common services like PowerShell and WMI
  - Keyloggers, microphone, video camera
- Command and Control Infrastructure
  - Backdoors
  - Common ports and services
    - Looks like legitimate traffic
  - Custom protocols

Common Persistence Mechanisms

Modifying registry keys

Scheduled tasks

Startup Programs

Browser Plugins

DLL search order hijacking

Shortcut Hijacking

Bootkits

How can you detect malware?

Common Detection Mechanisms

AntiVirus

Intrusion Detection / Prevention Systems

Noticeable differences in common operations

- Popups / browser changes
- Slow, full disk drive, system crashes
- Unusual processes

Some Anti-Detection Mechanisms

Anti-Debugging

Code and data obfuscation

- Packers

Anti-VM / Selective execution

Hides in legitimate processes

API hooks

Sleep when not in use

How can you protect against or mitigate malware infections?

Prevention

AntiVirus / Intrusion Prevention Systems

Awareness training

Spam filters / Ad blockers

Safe browsing habits

Updates and patches

Use a virtual machine

Remediation

Backups! Online and offline - validate cleanliness

Reimage

AntiVirus / Cleaners

Manual removal (forensics) / reverse engineering

Write signatures, conduct training to prevent reoccurrence

Resources

VirusTotal

ThreatCrowd

urlQuery

Hybrid Analysis

Malware Traffic Analysis

Malware don't need Coffee

Common Vulnerabilities and Exposures

VirtualBox

Examples

Stuxnet - Nation-state threat actors

Popcorn Time Ransomware - backstabbing

OSX Pirrit Adware - actually gets root

SLocker Android Ransomware

Conficker Worm and Botnet

Mirai Botnet

Demo?

https://www.virustotal.com/en/file/8a0ba8a5d155cfa1c32c5faa43948408fbeed595ee84bf4839bd0d04762c41d6/analysis/

https://www.hybrid-analysis.com/sample/8a0ba8a5d155cfa1c32c5faa43948408fbeed595ee84bf4839bd0d04762c41d6?environmentId=100

Group Homework Assignment

~3-5 people per group, individual submission

Pick a malware sample (not CryptoWall) & write it on the board (no duplicates)

Write a formal report (will probably be >3 pages and look sort of like this) containing:

1. An executive-level overview of the malware, what threat does it present for a company?
2. The threat actor's motivation for making or deploying the malware
3. Common infection, exploitation, and persistence vectors
4. How a company might detect the malware - note if it employs any anti-detection mechanisms
5. Suggestions for mitigating an infection and preventing further infections
6. Include references and resources as an appendix - don't copy / paste from existing reports, that's plagiarism
7. Relevant screenshots are welcome / encouraged