

Computer Forensics



What is Computer Forensics?

- Scientific process of preserving, identifying, extracting, documenting, and interpreting data on a computer
- Used to obtain potential legal evidence



Computer Forensics Procedures

The Forensic Paradigm

```
graph TD; A[The Forensic Paradigm] --> B[Identification]; A --> C[Collection]; A --> D[Analysis and Evaluation]; A --> E[Reporting];
```

Identification

- Identify specific objects that store important data for the case analysis

Collection

- Establish a chain of custody and document all steps to prove that the collected data remains intact and unaltered

Analysis and Evaluation

- Determine the type of information stored on digital evidence and conduct a thorough analysis of the media

Reporting

- Prepare and deliver an official report

Identification



4/23/24 Any action that modifies the crime scene could invalidate evidence in court 4

Forensic, Phishing, Malware

Identification: Common Mistakes ...

- You are the investigator, which objects do you think will be useful for investigations?
 1. Computer (case and power supply)
 2. Just the hard drive (without computer)
 3. Monitor
 4. Keyboard and mouse
 5. Media (CD, DVD, USB drives, etc.)
 6. Printer
 7. ...

**Digital forensics does not replace
traditional forensic analysis**

Collection

- To collect computer evidence, care must be taken not to change the evidence
 - Imaging media using a write-blocking tool to ensure the suspect device is not be modified
 - Establishing and maintaining the **chain of custody**
 - Documenting everything that has been done
 - Using only tools and methods that have been tested and evaluated to validate their accuracy and reliability

Digital Forensic Constraints

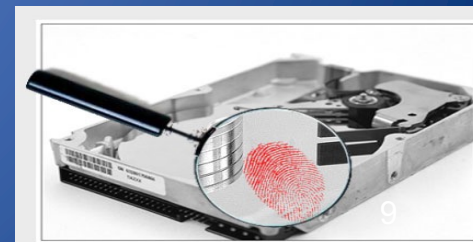
- Chain of custody
 - Maintain possession of all objects
 - Must be able to trace evidence back to source
 - “Prove” source integrity
- Priority by volatility
 - Some data is more volatile
 - RAM > swap > disk > CDs/DVDs
 - Idea: capture more volatile evidence first

Image Evidence: Laptop

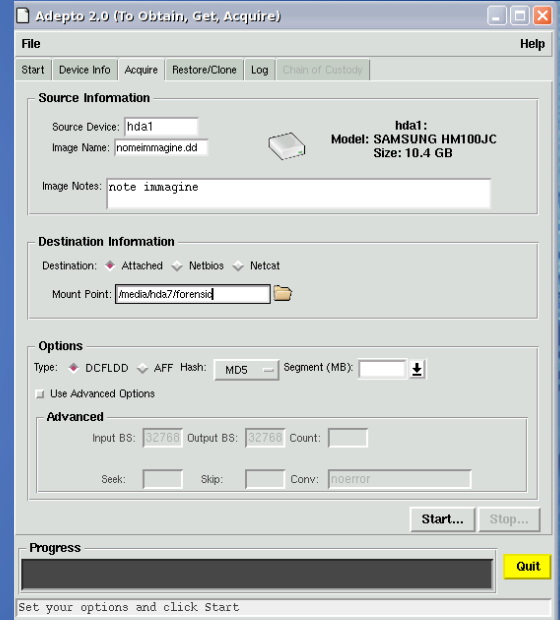
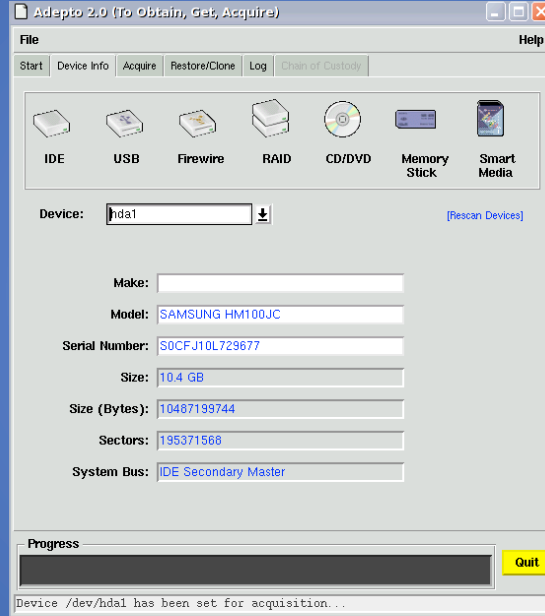


Why Use Disk Images

- Information on digital media is easily changed.
- Once changed it is usually impossible to detect that a change has taken place (or to revert the data back to its original state) unless other measures have been taken
- A common practice is calculate a cryptographic hash to establish a check point
- Examining a live file system changes state of the evidence
- The computer/media is the “crime scene”
- Protecting the crime scene is paramount as once evidence is contaminated, it cannot be decontaminated
- **Really only one chance to do it right!**



Adepto



The chain of custody
Forensic, Phishing, Malware



ADEPTO DIGITAL EVIDENCE CHAIN OF CUSTODY FORM

Case No: 20071220-1

Page: of:

ELECTRONIC MEDIA/COMPUTER DETAILS

Serial:	Description:		
1	Nuova immagine di test, cartella correttamente cancellati.		
Manufacturer:	Model No:	Serial No:	
SAMSUNG	USB to ATA/ATAPI	C2226000000	

IMAGE DETAILS

Date/Time:	Created By:	Method Used:	Image Name:	Segment:
12/20/07 08:58:57	mirko	dcfldd	disk20071220-1.dd	1
Storage Drive:	MD5:			
1	Total (md5): f0d6ae7120f560c1f87f7409f9e9cbdl			

CHAIN OF CUSTODY

Tracking No:	Date/Time:	FROM:	TO:	Reason:
NA	12/20/07 08:58:57	dcfldd See Hash	mirko	Initiate Custody
	Date:	Name/Org:	Name/Org:	
	Time:	Signature:	Signature:	
	Date:	Name/Org:	Name/Org:	
	Time:	Signature:	Signature:	
	Date:	Name/Org:	Name/Org:	
	Time:	Signature:	Signature:	
	Date:	Name/Org:	Name/Org:	
	Time:	Signature:	Signature:	
	Date:	Name/Org:	Name/Org:	
	Time:	Signature:	Signature:	
	Date:	Name/Org:	Name/Org:	
	Time:	Signature:	Signature:	

Chain of Custody

Collection: Common Mistakes ...

- What is the first step to collect evidence, when you find:
 - A computer turned on
 - A computer turned off

A computer on a crime scene should be considered fully adversarial

Analysis and Evaluation

- Know where evidence can be found
- Understand techniques used to hide or “destroy” digital data
- Toolbox of techniques to discover hidden data and recover “destroyed” data
- Cope with HUGE quantities of digital data...
- Ignore the **irrelevant**, target the **relevant**
- Thoroughly understand circumstances which may make “evidence” unreliable
 - If you have a hard drive with a broken sector that gives different result, what happens when you hash the entire drive?

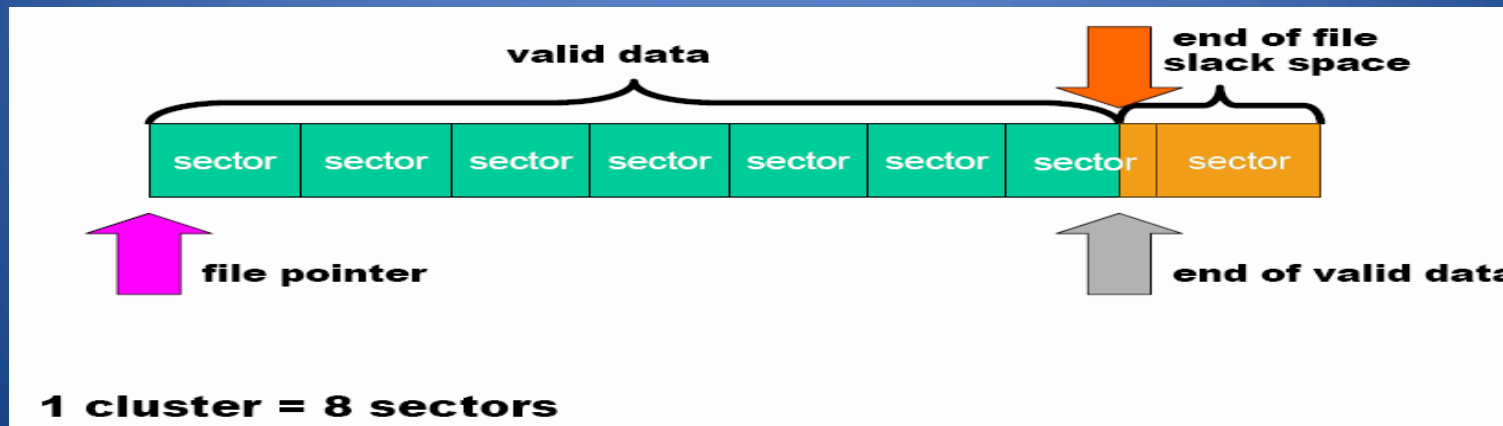
Where is the Evidence?

- Undeleted files, expect some names to be incorrect
- Deleted files
- Windows registry
- Print spool files
- Hibernation files
- Temp files (all those .TMP files in Windows!)
- Slack space
- Swap files
- Internet browsing histories
- Alternate or “hidden” partitions
- On a variety of removable media (USB drives, backup tapes, ...)

Hidden Data in the Hard Drive

Slack Space

- Slack space is the space between
 - The logical end of the file (i.e., the end of the data actually in the file) and
 - The physical end of the file (i.e., the end of the last sector devoted to the file).



Digital Forensics Tools

- Forensics tools are typically command line tools that are guaranteed not to alter the disk:
 - **HELIX** or **KALI** a live cd with a plenty of forensic tools ready to be used
 - **ENCASE** a series of proprietary forensic software products produced by Guidance Software
 - ...

Open Source vs. Closed Source



Commercial products such as EnCase are recognized by law.
What is the best approach?

Bitstream vs. Backups

- Forensic copies (Bitstream)
 - **Bit for bit copying** captures all the data on the copied media
 - Including hidden and residual data (e.g., slack space, swap, residue, unused space, deleted files etc.)
- Often the “smoking gun” is found in the residual data.
- Logical vs. physical image

Reporting

- Accurately describe the details of an incident
- Be understandable to decision makers
- Be able to withstand legal scrutiny
- Be unambiguous and not open to misinterpretation
- Be easily referenced
- Contain all information required to explain the conclusions
- Offer valid conclusions, opinions, or recommendations when needed
- Create report in a timely manner

**Corporation X
Security Investigations**

This form is to be used for one to ten pieces of evidence

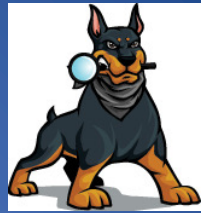
Case No.:		Investigating Organization:	
Investigator:			
Nature of Case:			
Location where evidence was obtained:			

	Description of evidence:	Vendor Name	Model No./Serial No.
Item #1			
Item #2			
Item #3			
Item #4			
Item #5			
Item #6			
Item #7			
Item #8			
Item #9			
Item #10			

Evidence Recovered by:		Date & Time:	
Evidence Placed in Locker:		Date & Time:	

Item #	Evidence Processed by	Disposition of Evidence	Date/Time

Autopsy



- Sleuthkit.org Autopsy allows to perform analysis on the disk image
- It is used to investigate disk images:
 - Timeline analysis, keyword search, web artifacts, hash filtering, data carving, multimedia and indicators of compromise
- e.g. <https://tryhackme.com/room/autopsy2ze0>



Anti-Forensic and Data Security

- Anti-forensic techniques try to frustrate forensic investigators and their techniques
- Securely deleting data, so that it cannot be restored with forensic methods
- Prevent the creation of certain data in the first place
- Data which was never there, obviously cannot be restored with forensic methods.

How to Hide Data?

- Cryptography
- Steganography
 - The process of hiding data inside other data (e.g. image files).
- Change file names and extensions
 - E.g. rename a .doc file to a .tmp file
- Hidden tracks
 - most hard disks have # of tracks hidden (i.e. track 0)
 - They can be used to hide/read data by using a hex editor
- Deleted Files
 - not truly deleted, merely marked for deletion.

**During Forensic is important to do not
use any tools that write to the disk**

Steganography

- hiding a secret message by embedding it into another message in order to prevent detection by modifying the less important bits

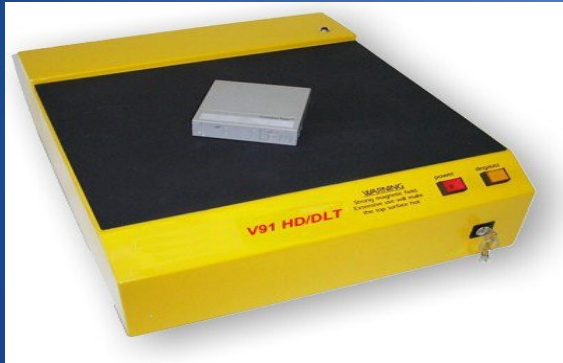
Original Media



Modified Media



Privacy Through Media Destruction



Degausser
Magnetic Field

or

or

Thermite

shredder

Thermite



Thermite is a pyrotechnic composition of a metal powder and a metal oxide
rust + aluminium-iron oxide + hard drive = hard drive death.

Disk Wiping

- **Simple erase**
 - The data is still on the drive but the segment has been marked as available
 - Next time data is written to the drive it MAY overwrite the segment
- **Destructive erase**
 - First overwrites all data in the file with random data
 - Next marks the segment as available
 - It may be possible to find ghost images of what was previously on the disk surface



PHISHING

Phishing

- Attempt to fraudulently acquire sensitive information
 - Passwords, credit card numbers, etc.
- Usually copies the HTML of a website and tries to pass off as a sub-site of that page.
- Phishers create a page or e-mail (**spam**) that appears to be from another source
- Usually relies on the user not exploring the page in depth
- Famous phishing attempts are PayPal and E-Bay scams
- Examples on www.phishtank.com

From: PayPal Security Department [service@paypal.com]
Subject: [SPAM:99%] Your PayPal Account



Security Center Advisory!

We recently noticed one or more attempts to log in to your PayPal account from a foreign IP address and we have reasons to believe that your account was hijacked by a third party without your authorization. If you recently accessed your account while traveling, the unusual log in attempts may have been initiated by you.

If you are the rightful holder of the account you must **click the link below** and then complete all steps from the following page as we try to verify your identity.

[Click here to verify your account](#)

http://211.248.156.177/.PayPal/cgi-bin/websrcmd_login.php

If you choose to ignore our request, you leave us no choice but to temporarily suspend your account.

Thank you for using PayPal!

Please do not reply to this e-mail. Mail sent to this address cannot be answered. For assistance, [log in](#) to your PayPal account and choose the "Help" link in the footer of any page.

To receive email notifications in plain text instead of HTML, update your preferences [here](#).

PayPal Email ID PP697

Protect Your Account Info

Make sure you never provide your password to fraudulent persons.

PayPal automatically encrypts your confidential information using the Secure Sockets Layer protocol (SSL) with an encryption key length of 128-bits (the highest level commercially available).

PayPal will never ask you to enter your password in an email.

For more information on protecting yourself from fraud, please review our Security Tips at <http://www.paypal.com/securitytips>

Protect Your Password

You should never give your PayPal password to anyone, including PayPal employees.

My Apple ID

Extended Validation Certificate

Sign in to manage your

Sign in.

My Apple ID

Verify your email address.

Please verify the email address, associated with your Apple ID

Sign in to Verify your email address.

[Forgot your Apple ID?](#)

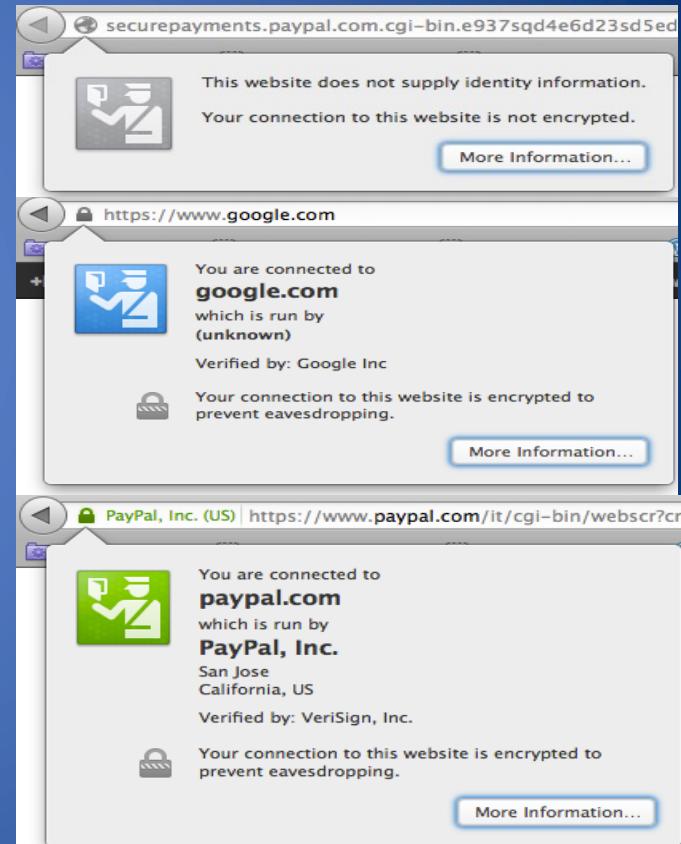
Extended Validation Certificate: Firefox

- Instant Website ID
 - A color-coded system makes it easy to check on suspicious sites and avoid Web forgeries.
- Anti-Phishing & Anti-Malware
 - Firefox protects you from trojan horses and spyware, and warns you away from fraudulent sites.



4/23/24

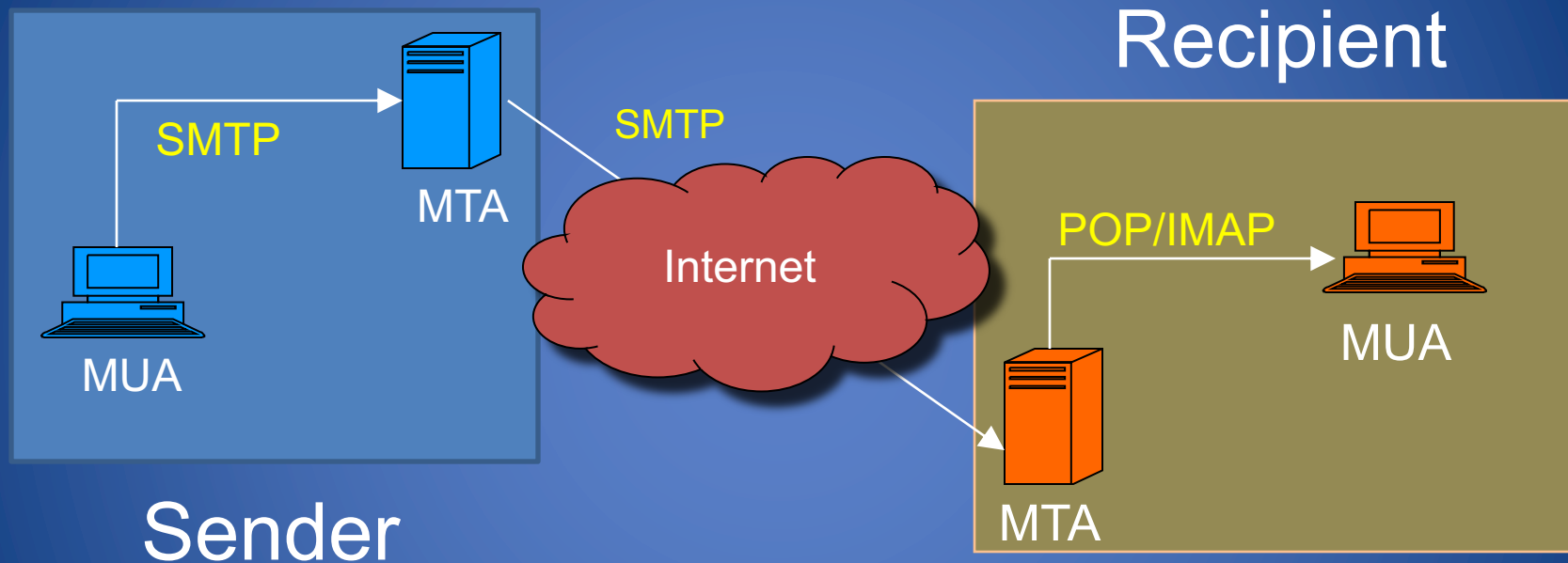
Forensic, Phishing, Malware



“why would anyone give their personal data to a phisher?”

- **Spear Phishing**
 - Phishing attempts directed at specific individuals or companies
 - Attackers may gather personal information about their target to increase their probability of success
- **Whaling**
 - Attacks directed specifically at senior executives and other high profile targets within businesses,
- These attacks are very difficult to understand and usually use email system

E-mail Transport



- **MUA:** mail user agent, *aka* mail client
- **MTA:** mail transport agent, *aka* mail server

SMTP

- Simple Mail Transfer Protocol
 - Client connects to server on TCP port 25
 - RFC 821 (1982) – 2821 (2001)
 - Client sends commands to server
 - Server acks or notifies of error
- Security issues
 - Sender not authenticated
 - Message and headers transmitted in plain text
 - Message and header integrity not protected
 - Spoofing and Spamming trivial to accomplish

- Example SMTP session

HELO mail.cs.brown.edu

MAIL FROM:<potus@whitehouse.gov>

RCPT TO:<bernardo@cs.brown.edu>

DATA

Subject: Executive order

From: 'Joe'<potus@whitehouse.gov>

To: 'bernardo'<bernardo@cs.brown.edu>

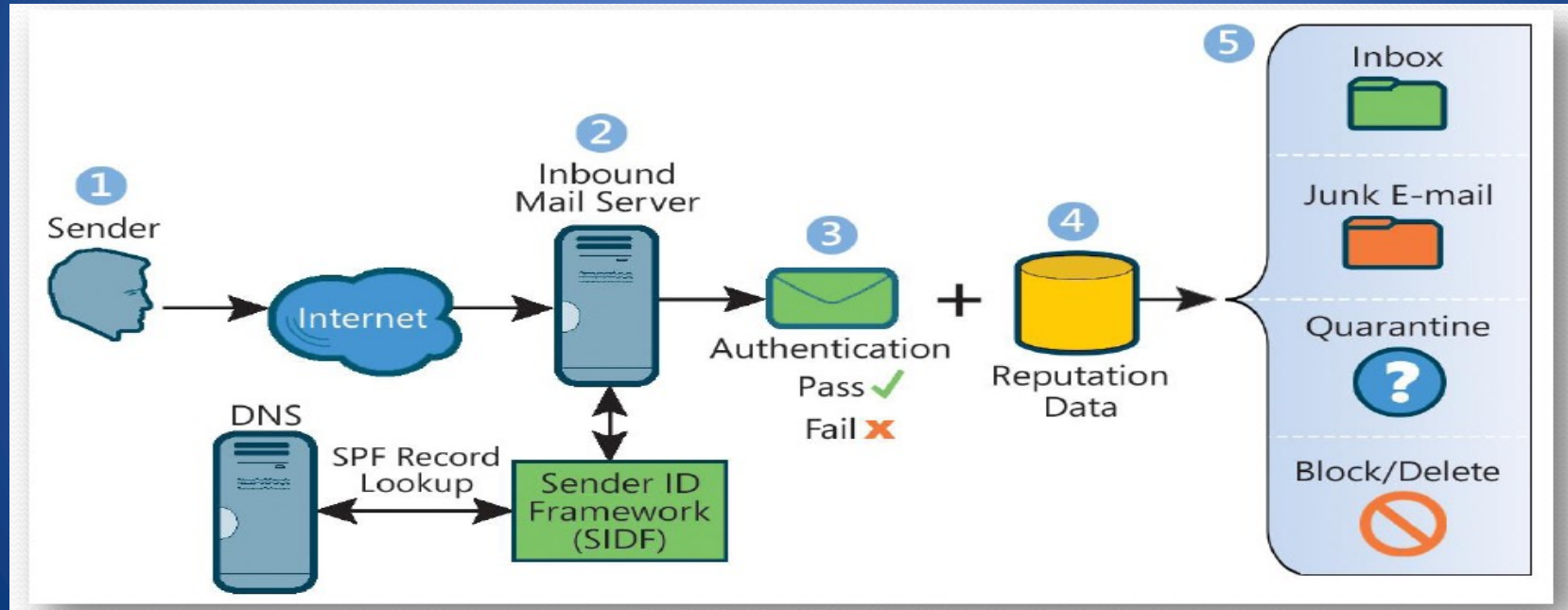
Date: April 10, 2024

You are hereby ordered to grade all the students of CSCI 1660 class with A.

The President of the United States

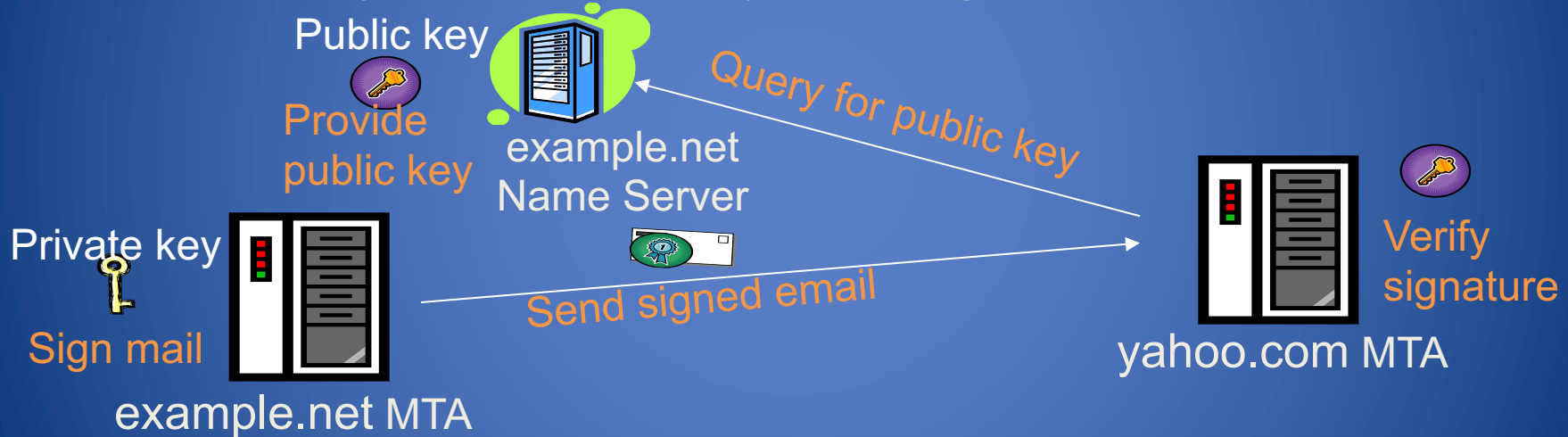
Sender ID and Sender Policy Framework (SPF)

- Store DNS records about servers authorized to send mail for a given domain
- Look up domain in From header to find IP address of authorized mail server



DomainKeys Identified Mail (DKIM)

- Sender's mail server signs email to authenticate domain
- Public key of server available in DNS record
- To be used in conjunction with other spam filtering methods



DomainKey-Signature: a=rsa-sha1; s=mail;
d=example.net; c=simple; q=dns;
b=Fg...5J

Authentication-Results: example.net
from=bob@example.net;
domainkeys=pass;

DMARC

- Domain-based Message Authentication, Reporting & Conformance
- Allows you to get reports back on the effectiveness of your SPF and DKIM investments
- Validates that the “From” header is the same as the domains validated by SPF and DKIM
- Provides clear instructions to the receiving server on what to do with emails that fail SPF or DKIM



Author Composes & Sends Email

Sending Mail Server Inserts DKIM Header

Email Sent to Receiver

SENDER
RECEIVER

IP Blocklists, Reputation, Rate Limits, etc.

Standard Validation Tests

Validate and Apply Sender DMARC Policy

Retrieve Verified DKIM Domains

Retrieve "Envelope From" via SPF

Apply Appropriate DMARC Policy

Anti-Spam Filters, etc.
Standard Processing

Passed

Quarantine



Failure Report sent to Sender

Update the periodic Aggregate Report to be sent to Sender

DMARC.org

Viruses, Worms, Trojans, Rootkits

- **Malware :**
 - A software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system
 - It can be classified into several categories, depending on propagation and concealment
- **Propagation**
 - **Virus:** human-assisted propagation (e.g., open email attachment)
 - **Worm:** automatic propagation without human assistance
- **Concealment**
 - **Rootkit:** modifies operating system to hide its existence
 - **Trojan:** provides desirable functionality but hides malicious operation
- Various types of payloads, ranging from annoyance to crime, breaks of Confidentiality, Integrity, and Availability

A Brief History of Malware

Early History

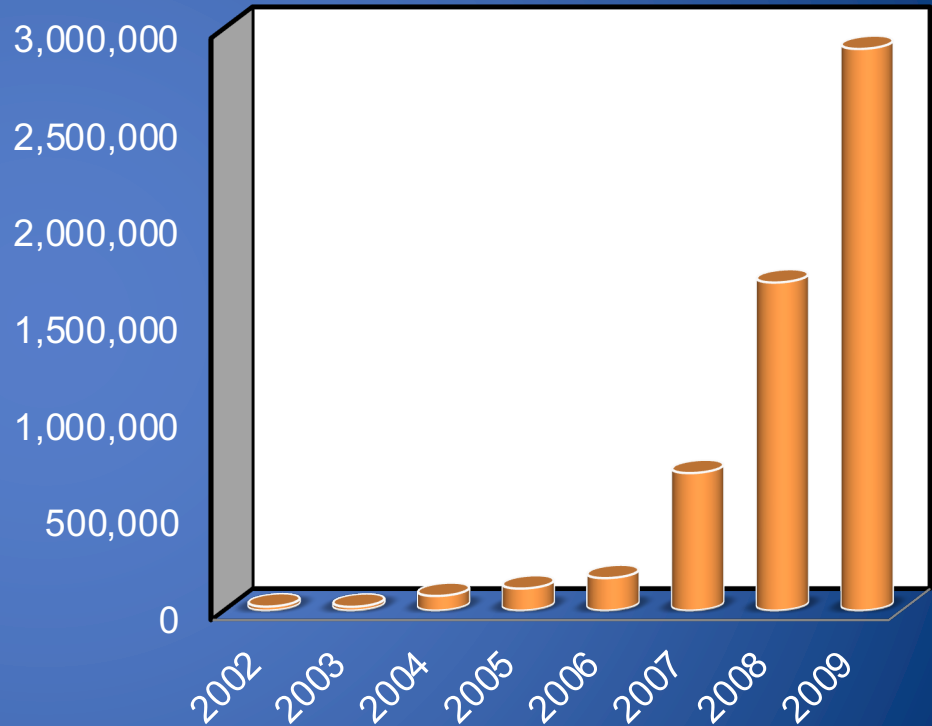
- 1972: sci-fi novel “When HARLIE Was One” features self-reproducing computer program called VIRUS
- 1982: high-school student Rich Skrenta wrote first virus released in the wild, Elk Cloner, a boot sector virus
- 1984: first academic use of “virus” by PhD student **Fred Cohen**, who credits advisor Len Adleman
- 1986: (c)Brain, by Basit and Amjood Farooq Alvi, credited with being first virus to infect PCs
- 1987: CHRISTMA EXEC targeting IBM VM/CMS systems was first email worm
- 1988: first internet worm, **Morris Worm** by Cornell student Robert Tappan Morris



Source: Wired, <https://www.wired.com/2011/07/0726first-computer-fraud-indictment/>

Previous Decade 2000-2009

- New malware threats have grown from 20K to 3M in the period 2002-2009
- Most of the growth has been from 2006 to 2009
- Growth in professional cybercrime and online fraud led to demand for professionally developed malware
- New malware often a custom-designed variation of known one
- Most notable: MELISSA, ILOVEYOU, CODE RED, NIMDA, etc.
- Let see the modern malwares...



Source: Symantec Internet Security Threat Report

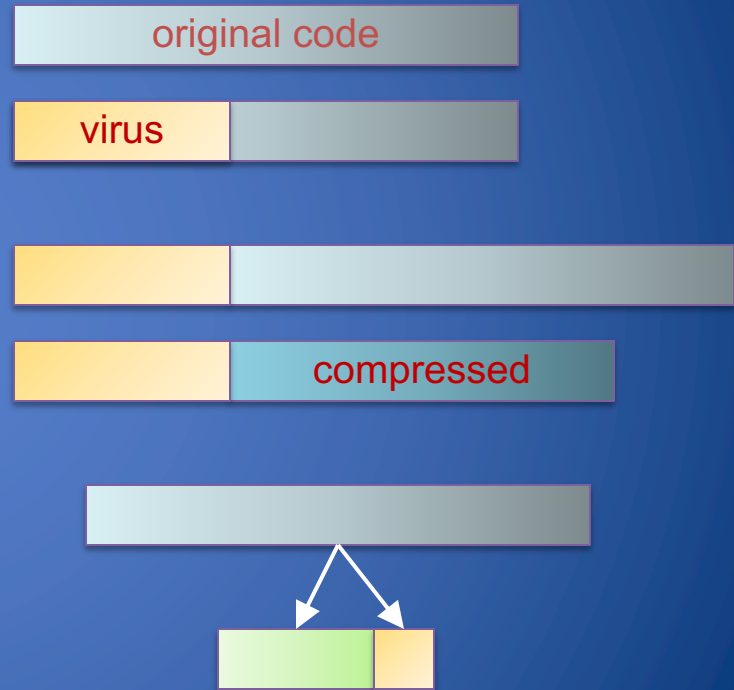
Malware Vectors, Propagation and Concealment

Some Malware Vectors

- Compromised Legitimate Websites
 - Theft of credentials
 - Malicious downloads Mobile Apps
 - Exfiltration of personal information
 - Invasive ads
- IoT Devices
 - Rarely patched
 - Provide access to private networks of homes and offices
- Email through phishing or spamming
 - Includes malicious links or attachments
 - Tricks users to send money or reveal passwords with social engineering
 - Mass distribution or targeted to specific users
 - About 50% of email volume is malware-related

Infection Types

- Overwriting
 - Destroys original code
- Pre-pending
 - Keeps original code, possibly compressed
- Infection of libraries
 - Allows virus to be memory resident
 - E.g., kernel32.dll
- Macro viruses
 - Infects MS Office documents
 - Often installs in main document template



Worm Development

- Identify vulnerability still unpatched
- Write code for
 - Exploit of vulnerability
 - Generation of target list
 - Random hosts on the internet
 - Hosts on LAN
 - Divide-and-conquer
 - Installation and execution of payload
 - Querying/reporting if a host is infected
- Initial deployment on botnet
- Worm template
 - Generate target list
 - For each host on target list
 - Check if infected
 - Check if vulnerable
 - Infect
 - Recur
- Distributed graph search algorithm
 - Forward edges: infection
 - Back edges: already infected or not vulnerable

Concealment

- **Encrypted virus**
 - Decryption engine + encrypted body
 - Randomly generate encryption key
 - Detection looks for decryption engine
- **Polymorphic virus**
 - Encrypted virus with random variations of the decryption engine (e.g., padding code)
 - Detection using CPU emulator
- **Metamorphic virus**
 - Different virus bodies
 - Approaches include code permutation and instruction replacement
 - Challenging to detect

Rootkits

- A rootkit modifies the operating system to hide its existence
 - E.g., modifies file system exploration utilities (e.g., ls, cd, ...)
 - Hard to detect using software that relies on the OS itself
- RootkitRevealer for Windows
 - By Bryce Cogswell and Mark Russinovich (Sysinternals)
 - Two scans of file system
 - **High-level scan** using the Windows API
 - **Raw scan** using disk access methods
 - Discrepancy reveals presence of rootkit
 - Could be defeated by rootkit that intercepts and modifies results of raw scan operations

Malware Detection

Detection Works Where Prevention Fails

- Detection is the act of noticing or discovering something

Detection by its appearance

- Detects specific malicious **signatures**
- Often uses fast pattern matching techniques
- Problems?
 - False negative
Signature Evasion

Detection by its behavior

- Detects **anomalies** on a normal system/network activity
- Often uses machine learning
- Problems?
 - False positive
Legitimate behavior could be not standard

High Cost of Errors

- False Positives FP require expensive analysis time
- False Negatives can be catastrophic
- Examples?
 - Airport Security:** FP is when ordinary items such as keys or coins get mistaken for weapons (machine goes "beep")
 - Quality Control:** FP is when a good quality item gets rejected, and a FN is when a poor quality item gets accepted
 - Presumption of innocence:** "It is better that ten guilty persons FN escape than that one innocent suffer FP"
 - Antivirus software:** a FP is when a normal file is thought to be a virus

Heuristic Analysis

- Useful to identify new and “zero day” malware
- Code analysis
 - Based on the instructions, the antivirus can determine whether or not the program is malicious, i.e., program contains instruction to delete system files,
- Execution emulation (sandbox)
 - Run code in isolated emulation environment
 - Monitor actions that target file takes
 - If the actions are harmful, mark as virus
- Heuristic methods can trigger false alarms

Quarantine/Virus Chest

- A suspicious file can be isolated in a folder or database called **quarantine**:
 - E.g., if the result of the heuristic analysis is positive and you are waiting for updates of the signatures
- The suspicious file is not deleted but made harmless: the user can decide when to remove it or eventually restore it in case of a false positive
 - Interacting with a file in quarantine is possible only through the antivirus program
- A file in quarantine is often stored encrypted to prevent its execution
- The quarantine system architecture is typically proprietary

How to Check if AV Software is Running?

- Eicar signature:
 - X5O!P%@AP[4\PZX54(P^)7CC)7}\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H*
- www.caro.org
- www.eicar.org

AntiVirus evaluation

- **Shield**

- Background process (service/daemon)
- Scans each time a file is touched (open, copy, execute, etc.)

- **On-demand**

- Scan on explicit user request or according to regular schedule
- On a suspicious file, directory, drive, etc.

Performance test of scan techniques

- **Comparative/Performance:** check the number of already known viruses that are found and the time to perform the scan
- **False alarm test:** number of false viruses detected
- **Heuristic / Behaviour Tests:** measure the proactive protection capabilities

Anti-viruses are ranked using both parameters: <http://www.av-comparatives.org/>

Resources

- Symantec's Internet Security Threat Report
–Published annually
- Countdown to zero day by Kim Zetter, 2014
- Art of Computer Virus Research and Defense
by Peter Szor
- <http://virus.wikidot.com/>

Ransomware

Overview

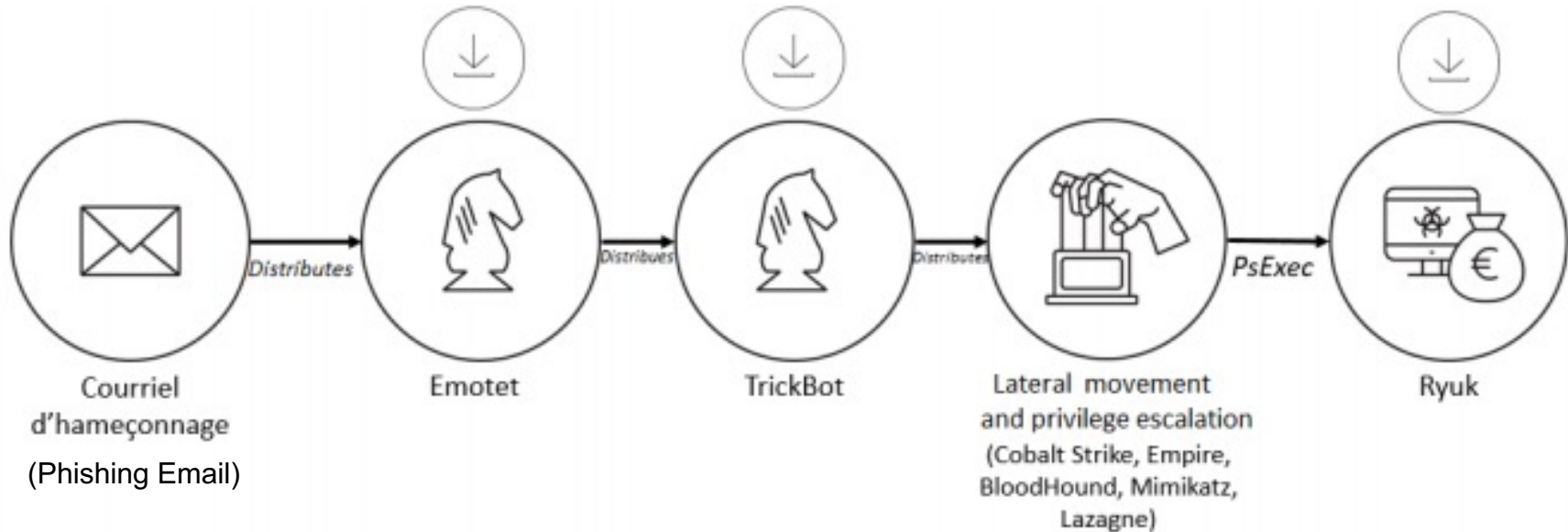
- Ransomware takes control of the victim machine as in a botnet
- Basic Idea:
 - Malware gains access to filesystem and encrypts all the files it can with a key known only to the attacker
 - Victim must pay ransom in Bitcoin (or other Crypto currency) in order to regain access to files
- No guarantee that you actually get the key

Ryuk Ransomware



- Ransomware used to target enterprise systems (Windows)
- Attributed to cybercriminal group called “Wizard Spider”
 - Same group responsible for “TrickBot” wire fraud attacks
- “Big Game Hunting”

Supply Chain (of Infection)



Ryuk Ransomware: Technical Details

- Delivery:
 - *Emotet* malware-as-a-service
 - “Mealybug” operators sell usage of their botnet of infected computers to other hacking groups
 - In Ryuk, *Emotet* used to deliver *Trickbot* loader via email attachments/links
 - Example: Excel file with malicious macro, Google Drive file named “.pdf” but is actually an executable...

Ryuk Ransomware: Technical Details

- Installation:
 - *TrickBot* checks if system is 32-bit or 64-bit, then downloads a Ryuk *dropper* for the bit version
 - Deleted shortly after; rarely recovered by victims
 - Ryuk *dropper* crafts executable with random name which deletes the dropper
 - Executable performs the ransomware encryption

Ryuk Ransomware: Technical Details

- Encryption:
 - Each *dropper* gets an RSA public key
 - Attackers know the private key
 - Generate symmetric key for each file
 - Encrypt the file with AES-CBC
 - Encrypt the key with the RSA public key
 - Append the key ciphertext to the file ciphertext
 - Releasing private key is sufficient to decrypt files

Ryuk Ransomware: Technical Details

- Lateral Movement:
 - *Eternal Blue* is used to infect other hosts on the network by attacking the SMB protocol
 - Other “legitimate” pentesting software is used to find filesystem mounts and escalate privileges:
 - *Cobalt Strike*
 - *Metasploit*
 - Reuse Kerberos protocol authentication tickets from current user’s machine to gain access to other machines

Ryuk Ransomware: Lateral Movement

- Before attempting to infect, Ryuk reads through victim ARP table and sends “Wake-On-LAN” packet to each host
- Accesses filesystem mounts
- Copies Ryuk binary to target host
- Remotely creates Windows scheduled task to execute Ryuk binary
- Ryuk looks for network shares on the victim IT infrastructure
 - Private IP ranges are scanned:
10.0.0.0/8 - 172.16.0.0/16 -192.168.0.0/16.

Ryuk Ransomware: Technical Details

- Ransom Notes:

Your network has been penetrated.

All files on each host in the network have been encrypted with a strong algorithm.

Backups were either encrypted or deleted or backup disks were formatted.
Shadow copies also removed, so F8 or any other methods may damage encrypted data but not recover.

We exclusively have decryption software for your situation
No decryption software is available in the public.

DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME OR MOVE the encrypted and readme files.
DO NOT DELETE readme files.
This may lead to the impossibility of recovery of the certain files.

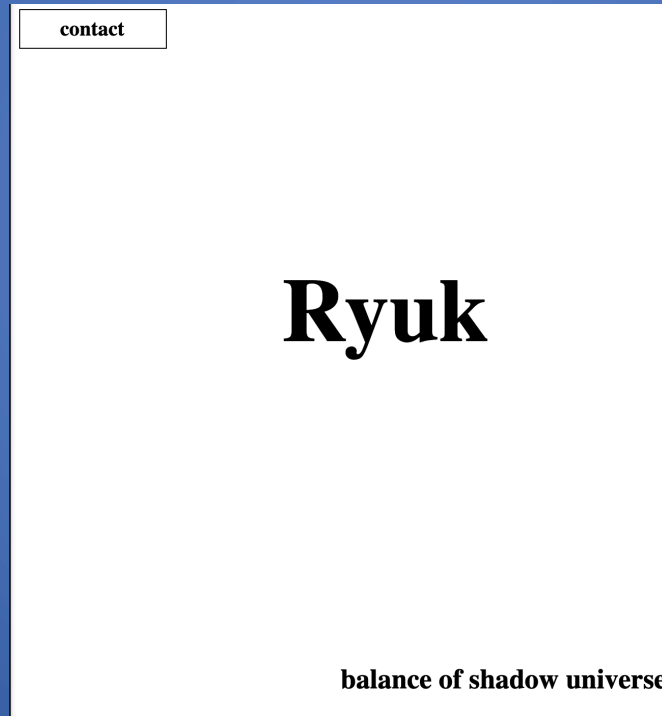
To get info (decrypt your files) contact us at
KurtSchweickardt@protonmail.com
or
KurtSchweickardt@tutanota.com

BTC wallet:
14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk

Ryuk
No system is safe

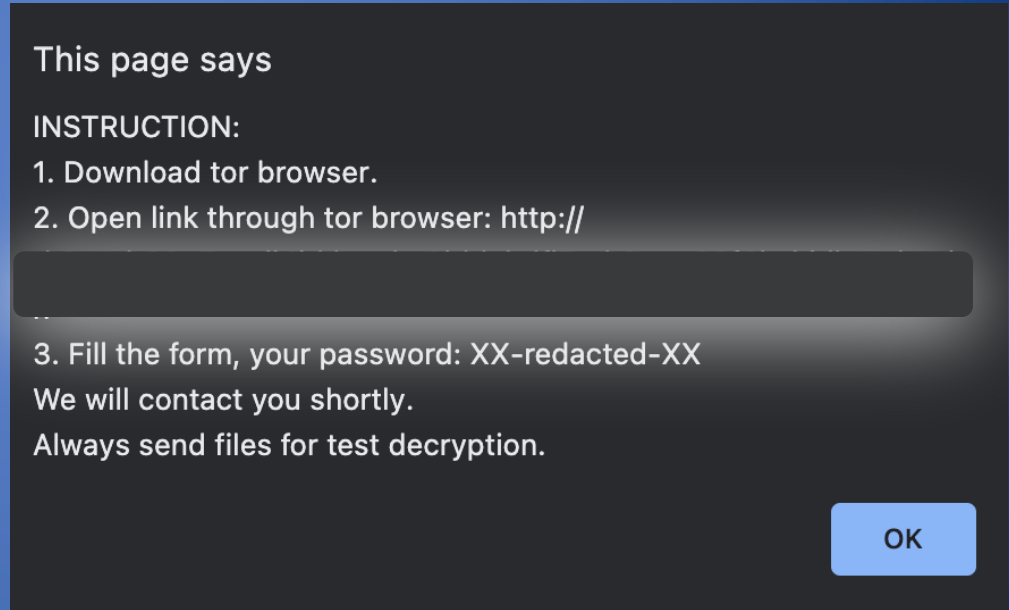
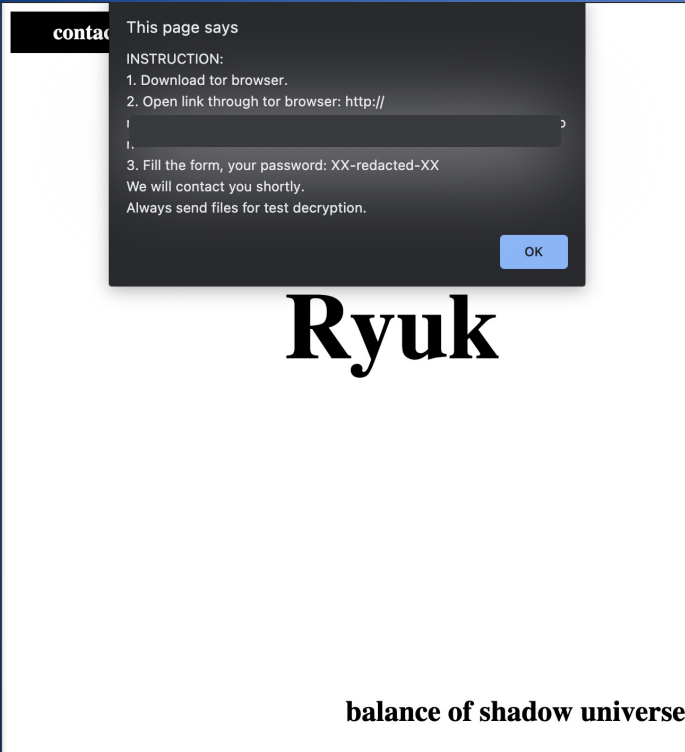
Ryuk Ransomware: Technical Details

- Ransom Notes:



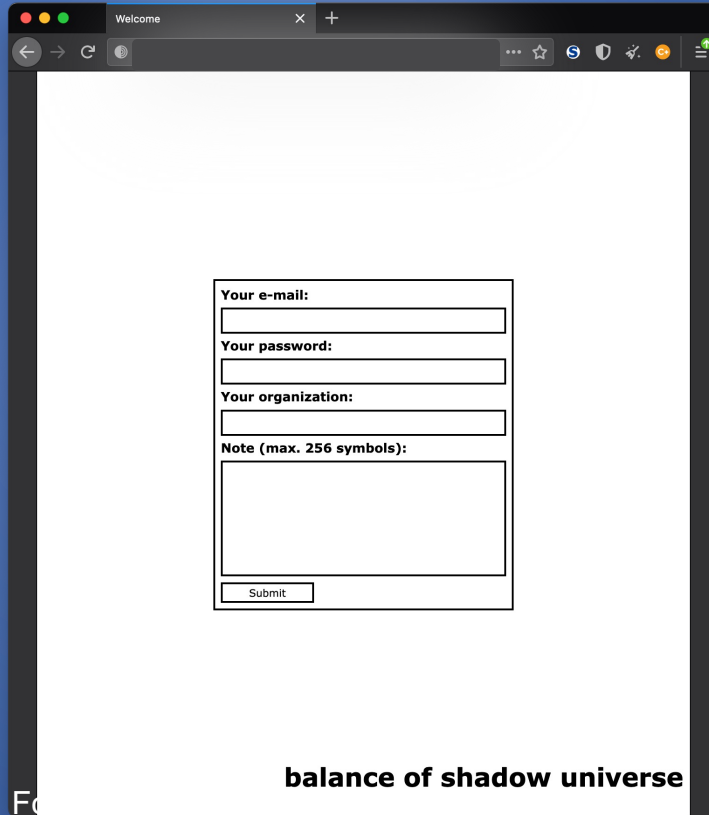
Ryuk Ransomware: Technical Details

- Ransom Notes:



Ryuk Ransomware: Technical Details

- Ransom Notes:



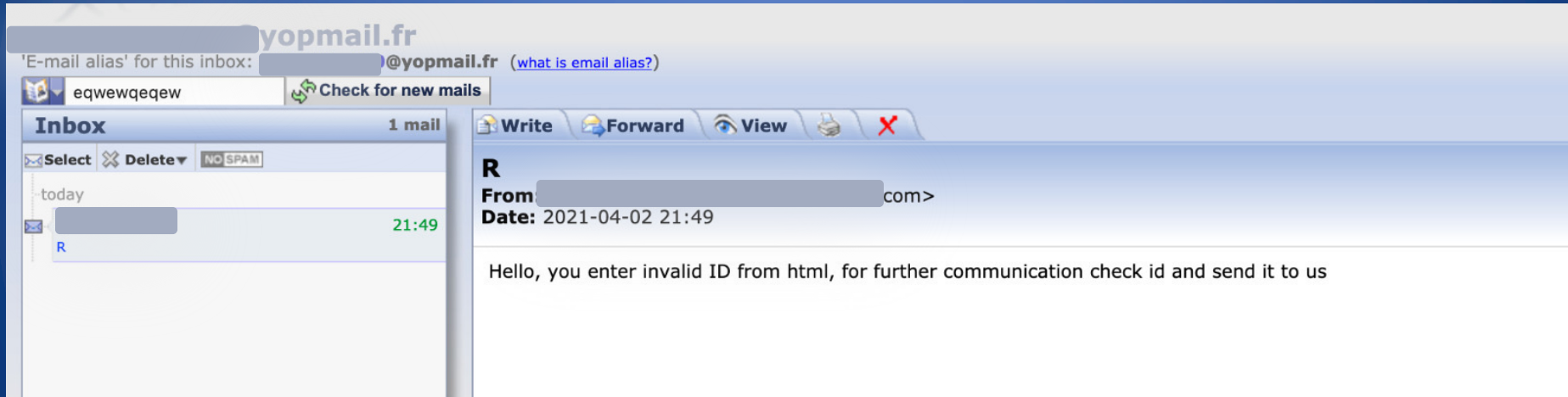
A screenshot of a web browser window displaying a ransom note form. The browser's address bar shows "Welcome" and various navigation icons. The form is centered on a white background and contains the following fields:

- Your e-mail:** A single-line text input field.
- Your password:** A single-line text input field.
- Your organization:** A single-line text input field.
- Note (max. 256 symbols):** A larger multi-line text input area.
- Submit**: A button at the bottom of the form.

At the bottom right of the browser window, the text "balance of shadow universe" is visible.

Ryuk Ransomware: Technical Details

- Collecting Ransoms:



Ryuk Ransomware: Interesting Notes

- System stability:
 - Encrypting all files might damage system
 - Ryuk maintains “skip list” (.exe, .dll, .hrmlog)
 - Still can cause system instability (pro or con?)
 - Skip list also includes large but “un-ransomable” files
 - Chrome, Firefox, Recycle.bin
 - Derived from *Hermes* ransomware
 - Hermes was sold for \$300 per use
 - Buyer specified two email addresses and an RSA public key and received compiled copy using info

“Double” Ransomwares

- Sometimes, Ryuk can exfiltrate files in addition to encrypting them
- One ransom to retrieve files, one to prevent their release
 - Currently ongoing double ransom negotiations between cybercriminals and Florida school district
 - Opening ask of \$40 million in Bitcoin!

Ryuk Ransomware: Interesting Notes

- Corporate criminality:
 - Between attackers: Emotet and Trickbot are “SaaS for criminals”
 - Hacking groups work as “Trickbot affiliates” and sell Trickbot usage to other groups
 - Trickbot payloads include an “affiliate identifier” for payment
 - Between attacker and victim: Negotiations and tech support

HELLO CWT_company !

IF YOU ARE READING THIS, IT'S MEAN YOUR DATA WAS ENCRYPTED AND YOU SENSITIVE PRIVATE INFORMATION WAS STOLEN!
READ CAREFULLY THE WHOLE INSTRUCTION NOTES TO AVOID DIFFICULTIES WITH YOUR DATA

by RAGNAR_LOCKER !

YOU HAVE TO CONTACT US via LIVE CHAT IMMEDIATELY TO RESOLVE THIS CASE AND MAKE A DEAL
(contact information you will find at the bottom of this notes)

!!!!!! WARNING !!!!!

DO NOT Modify, rename, copy or move any files or you can DAMAGE them and decryption will be impossible.
DO NOT use any third-party or public Decryption software, it also may DAMAGE files.
DO NOT Shutdown or Reset your system, it can DAMAGE files

There is ONLY ONE possible way to get back your files - contact us and pay for the special DECRYPTION KEY !
For your GUARANTEE we will decrypt 2 of your files FOR FREE, as a proof that it works.

Don't waste your TIME, the link for contact us will be deleted if there is no contact made in closest time and you will NEVER restore your DATA.
!!! HOWEVER if you will contact us within 2 day since get penetrated - you can get a very SPECIAL PRICE.

! WARNING !
whole your network was fully COMPROMISED!

We has DOWNLOADED more than 2 TB of your PRIVATE SENSITIVE Data, including your Billing info, Insurance cases, Financial reports,
Business audit, Banking Accounts! Also we have corporate correspondence, information about your clients such as AXA Equitable, Abbot Laboratories, AIG, Amazon,
Boston Scientific, Facebook, J & J, SONOCO, Estee Lauder and many others.
We got even more info about your partners and even about your staff, there are some screenshots just as a proofs of what we got on you.

Screenshots:

<http://prntscr.com/to31n0> (from here was downloaded almost every file)
<https://prnt.sc/to2kqk>
<https://prnt.sc/to2lbp>
<https://prnt.sc/tnz00z> your trial balances in USD
<https://prnt.sc/tnzqxk>
<https://prnt.sc/to2qlx>
<http://prnt.sc/to2rab>

Whole data that gathered from your private files and directories could be published in MASS MEDIA for BREAKING NEWS! Yours partners, clients and investors would be notified about LEAK.

However if we make a deal everything would be kept in secret and all your data will be restored.

You can take a look for some more examples of what we have, right now it's a private hidden page, but it could become accessible for Public View if you decide NOT pay.
Use Tor Browser to open the link: <http://p6o7m73ujalhgkiv.onion/?BatxqaHm8RkxIP16Z1xB>
to view the page's content use password: GME5SYUN0A