Cybercrime 1

Adam Petříček, Radek Mocek

Cybercrime

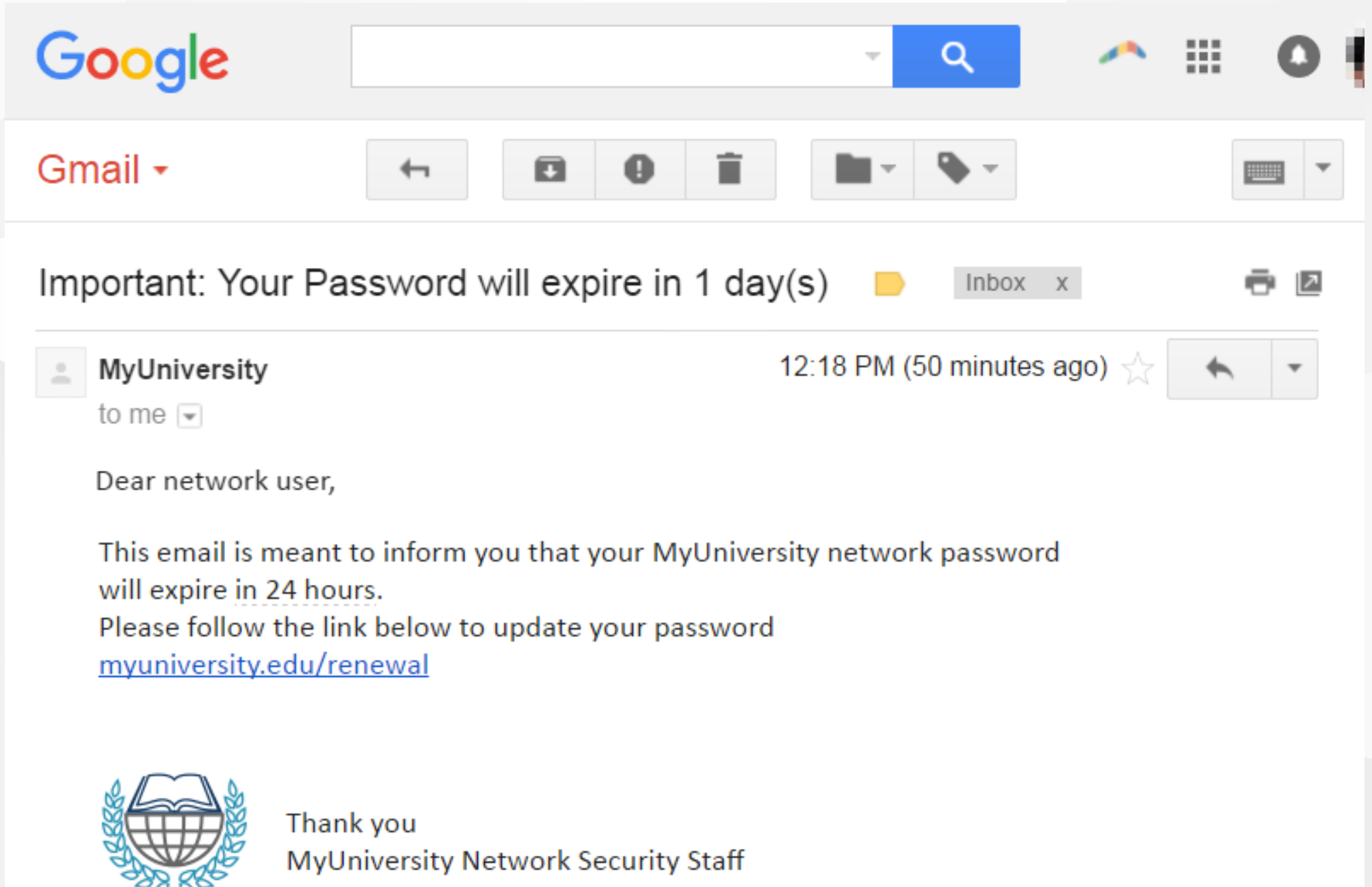
- crime which includes network and a computer
  - is performed with computer or against computer
  - could be performed by individuals or organized groups
- some of the most common threats are **phishing**, **ransomware**, **DoS**, **botnet**, **keylogger**, **SQL injection**
- **malware** is a generic term for describing any software designed to cause trouble

Phishing

- social engineering technique, consists of fraudulent message
- message is trying to get sensitive user information by pretending to look like official message from some service
  - user is redirected to fake website which looks exactly like the real one
  - if user inputs their credentials, the attacker will gain access to them, they could be then used to steal victim's account

HOW TO AVOID:

URL in message could have typo in it (e.g. youutube.com)


Google
Gmail
Important: Your Password will expire in 1 day(s)
Inbox x
MyUniversity
12:18 PM (50 minutes ago)
to me
Dear network user,
This email is meant to inform you that your MyUniversity network password will expire in 24 hours.
Please follow the link below to update your password
myuniversity.edu/renewal
Thank you
MyUniversity Network Security Staff

Ransomware

- attacker blocks and encrypts user's data
- then he blackmails user and demands money for decrypting data
  - attacker can also threaten to publish data (if they're sensitive)
- typically spreads using trojan horse in some malicious software downloaded by user
- payment required by attacker is usually using cryptocurrencies (to avoid being tracked)

HOW TO AVOID:

do not download content from suspicious sources

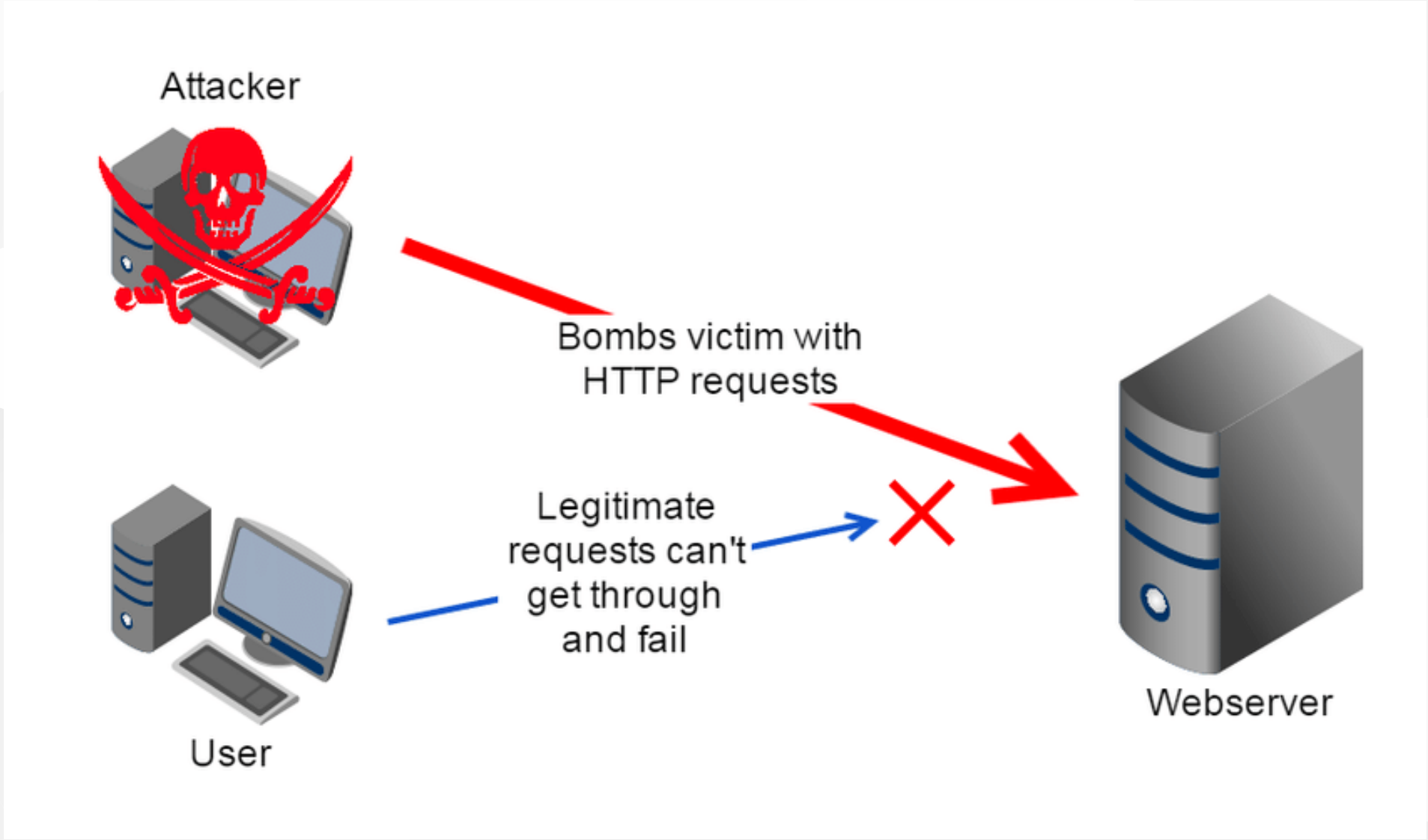

You became victim of the PETYA RANSOMWARE!
The harddisks of your computer have been encrypted with an military grade encryption algorithm. There is no way to restore your data without a special key. You can purchase this key on the darknet page shown in step 2.
To purchase your key and restore your data, please follow these three easy steps:
1. Download the Tor Browser at "https://www.torproject.org/". If you need help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:
http://pety .onion/g
http://pety .onion/g
3. Enter your personal decryption code there:
a6
nF y1
If you already purchased your key, please enter it below.
Key: _

DoS / DDoS

- Denial of Service / Distributed Denial of Service
- attack aimed at servers, trying to make them unavailable for users
  - the goal is not to take control over the service
- performed via sending huge amount of data to the server and overwhelming it
- DDoS is organized DoS using lots of computers all sending data to one target

HOW TO AVOID:

using DDoS protection on your server to check incoming requests

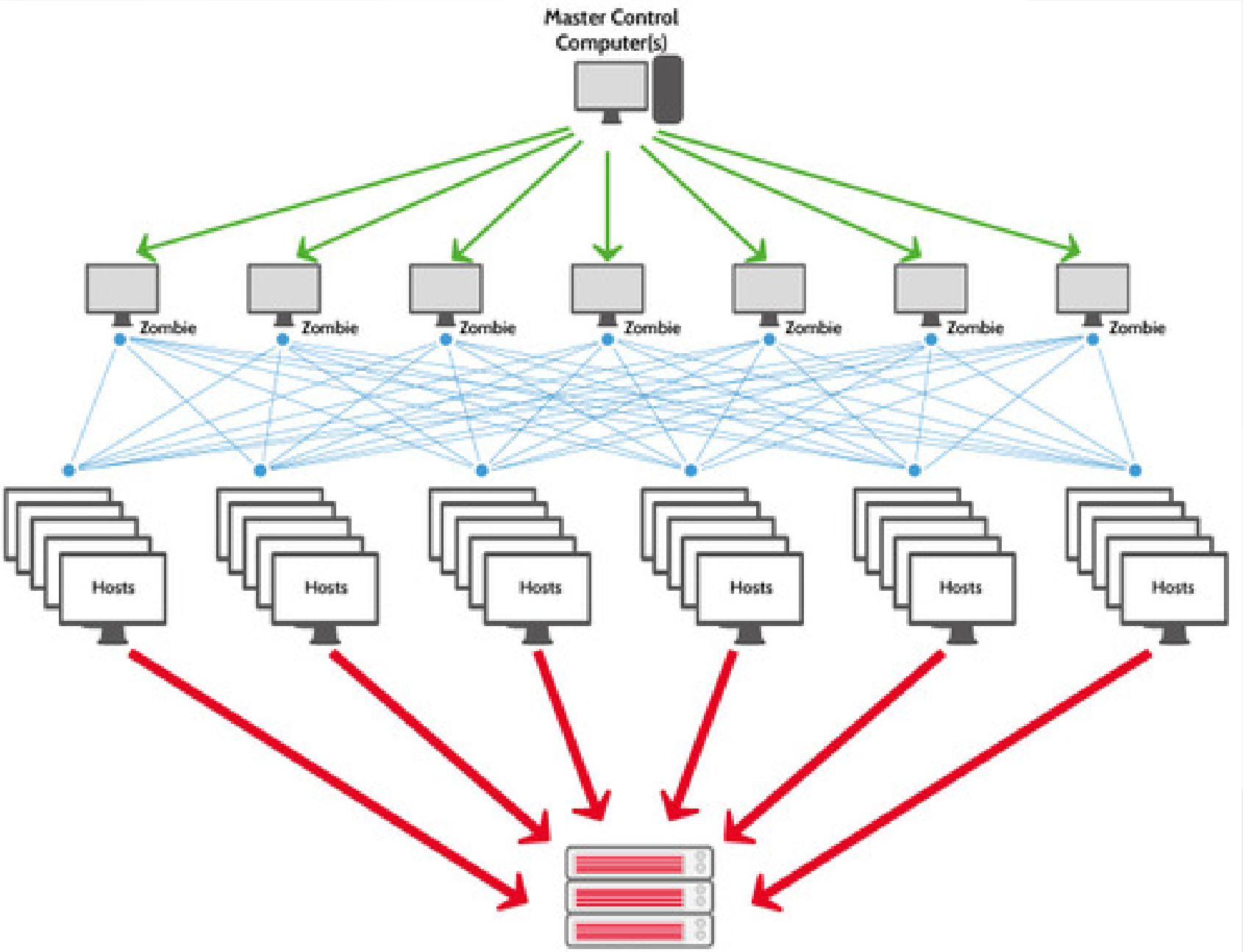

Attacker
Bombs victim with
HTTP requests
Legitimate
requests can't
get through
and fail
User
Webserver

Botnet

- lots of inficated computers (zombies) are controlled from one device to perform different cybercrimes (most often DDoS)
- users typically do not have a clue about their computer being infected
- bot master has to limit number of requests to avoid being caught by ISP

HOW TO AVOID:

you can check your network traffic to find some suspicious requests

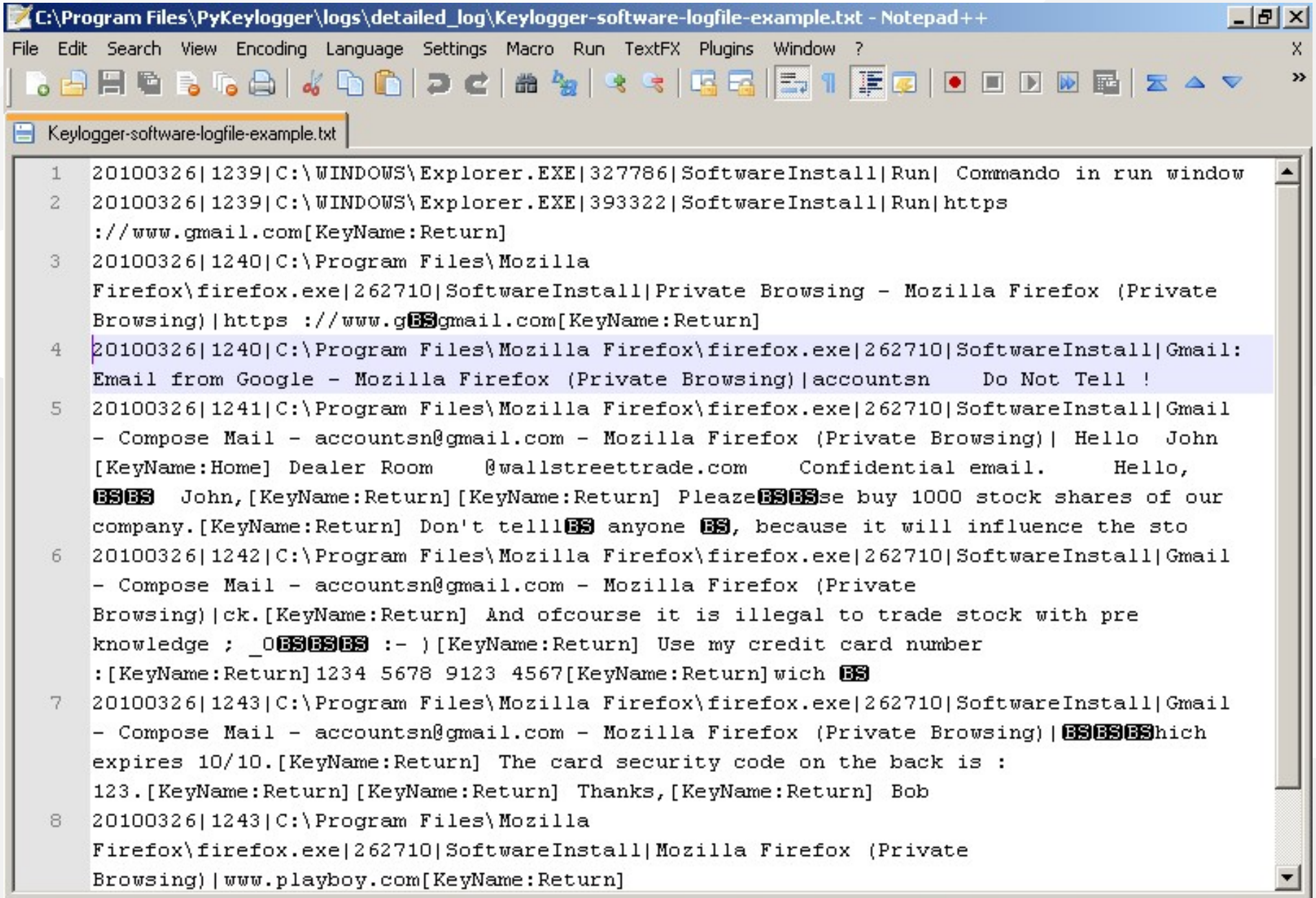

Master Control
Computer(s)
Zombie
Zombie
Zombie
Zombie
Zombie
Zombie
Zombie
Hosts
Hosts
Hosts
Hosts
Hosts
Hosts

Keylogger

- malware which records keys you press and sends them to the attacker
- attacker can gain your credentials using this method
- hardware keyloggers can be harder to detect than software
- your antivirus should usually detect the keylogger before it installs

HOW TO AVOID:

by deleting it if you identify keylogger in your running tasks


C:\Program Files\PyKeylogger\logs\detailed_log\Keylogger-software-logfile-example.txt - Notepad++
File Edit Search View Encoding Language Settings Macro Run TextFX Plugins Window ?
Keylogger-software-logfile-example.txt
1 20100326|1239|C:\WINDOWS\Explorer.EXE|327786|SoftwareInstall|Run| Commando in run window
2 20100326|1239|C:\WINDOWS\Explorer.EXE|393322|SoftwareInstall|Run|https ://www.gmail.com[KeyName:Return]
3 20100326|1240|C:\Program Files\Mozilla Firefox\firefox.exe|262710|SoftwareInstall|Private Browsing - Mozilla Firefox (Private Browsing)|https ://www.gBSgmail.com[KeyName:Return]
4 20100326|1240|C:\Program Files\Mozilla Firefox\firefox.exe|262710|SoftwareInstall|Gmail: Email from Google - Mozilla Firefox (Private Browsing)|accountsn Do Not Tell !
5 20100326|1241|C:\Program Files\Mozilla Firefox\firefox.exe|262710|SoftwareInstall|Gmail - Compose Mail - accountsn@gmail.com - Mozilla Firefox (Private Browsing)| Hello John [KeyName:Home] Dealer Room @wallstreettrade.com Confidential email. Hello, BSBS John,[KeyName:Return][KeyName:Return] PleazeBSBSse buy 1000 stock shares of our company.[KeyName:Return] Don't tellBS anyone BS, because it will influence the sto
6 20100326|1242|C:\Program Files\Mozilla Firefox\firefox.exe|262710|SoftwareInstall|Gmail - Compose Mail - accountsn@gmail.com - Mozilla Firefox (Private Browsing)|ck.[KeyName:Return] And ofcourse it is illegal to trade stock with pre knowledge ; _OBSBSBS :-)[KeyName:Return] Use my credit card number :[KeyName:Return]1234 5678 9123 4567[KeyName:Return]wich BS
7 20100326|1243|C:\Program Files\Mozilla Firefox\firefox.exe|262710|SoftwareInstall|Gmail - Compose Mail - accountsn@gmail.com - Mozilla Firefox (Private Browsing)|BSBSBShich expires 10/10.[KeyName:Return] The card security code on the back is : 123.[KeyName:Return][KeyName:Return] Thanks,[KeyName:Return] Bob
8 20100326|1243|C:\Program Files\Mozilla Firefox\firefox.exe|262710|SoftwareInstall|Mozilla Firefox (Private Browsing)|www.playboy.com[KeyName:Return]

SQL injection

- SQL is language used to manage databases
- this attack targets poorly secured forms on websites
- by typing part of the SQL query directly into the form input, the query would execute and cause trouble in database
- attacker can either try to remove data from database or to gain access to secured data like passwords

HOW TO AVOID:

by securing your SQL query or database

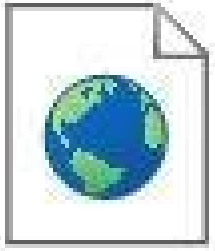
SQL INJECTION

WEB PAGE

USERNAME: WUM

PASSWORD: **********

Select * from wum_Table where user-d='wum' and password 'wumtool';



WEB PAGE

USERNAME: '1' OR '1' = '1'

PASSWORD: **********

Select * from wum_Table where user-d='' 1' OR '1' = '1' and password '1' OR '1' = '1'';

Encryption

- process of securing data by encoding them using various algorithms

Hash

- data are encrypted using complex mathematical functions
- there is no way to get original data back (used to store passwords)

Cypher

- data are encrypted using algorithm with decryption key
- this key is secure and can be used to decrypt data back

Questions

1) Have you ever been a victim of some cybercrime?

2) What protection are you using to prevent downloading malware?

3) How do you make your password secure?

4) How do you identify that message is phishing?

Phrases

- SQL query (Structured Query Language)
- URL (Universal Resource Locator)
- ISP (Internet Service Provider)
- hash
- cryptocurrencies
- log file