How to Know If You’ve Been Hacked

Introduction

Computer Hack

Email Hack

Cyber Space
Internet Networks

Know Normal
To detect “Abnormal”

Indicators

Investigation
Connections

Indicators

Investigation
Last Sign Ins Email Settings
Hello!

I am Said Varlioglu

2017 – 2020 – Information Security Analyst, Cincinnati OH
2020 – 2021 – Cyber Security Analyst, Dallas TX
2021 – Present – Incident Response Engineer, Dallas TX

2019 - Master of Science, School of IT, University of Cincinnati
2023 - Ph.D. Student, School of IT, University of Cincinnati
What is “being hacked”? 

Unauthorized access to your device

Violation of CIA triad:

**Confidentiality**
- refers to protecting information (data and system) from being accessed by unauthorized parties.

**Integrity**
- Maintaining the accuracy, consistency, and trustworthiness of data over its entire life cycle.

**Availability**
- Data and systems being available for use.
- Non-repudiation: The ability to assure that the sender accepts the authenticity of their signature message.
In order to detect “abnormal”, we need to know “normal”

How is our cyber space?

What is my IP Address?

What is my WiFi?

How much RAM (Memory)?

How much disk size?

How long computer battery last?

Does my email account have a recovery email or phone?

Does my email account have a forwarding rule?
How is “your cyber space”?

Network Environment

- a Laptop
- a Smart Phone
- an IoT device
- a Modem
- an Email
- an Online Bank Account
- a Smart TV
- others…
Let’s look at our “Normal”

What is my IP?
https://whatismyipaddress.com/

What is IP?
- Internet Protocol to communicate devices each other

Laptop on Wi-Fi
IPv4: 24.166.238.99

Phone on Wi-Fi
IPv4: 24.166.238.99

Phone on the Carrier Internet
IPv4: 172.30.203.43
Let’s look at our “Normal” Device Network Information

What is an internal IP?

- Internet Protocol to communicate devices each other in an internal network, like in a home network
Let’s look at our “Normal”

How many devices in my home network?

Check your router

192.168.1.1

or

192.168.1.0

(usually)
How much data your device send and receive?

Check Data Usage
How is CPU usage of my device?

Check Task Manager
How much data your device send and receive?

Check Task Manager
How much data your device send and receive?

Resource Monitor
Where my computer connects to

Resource Monitor – Network – TCP Connections
What Wi-Fi profiles were used by my device?

Command Prompt

`netsh wlan show profiles`
What are the passwords of Wi-Fi profile?

Command Prompt

```cmd
netsh wlan show profile name="<Wi-Fi Name>" key=clear
```
What commands were run on Command Prompt?

Command Prompt

doskey /history
How to Know If Your Computer Has been Hacked?

Indicators: “Abnormal” activities

- Ransomware note
- Frequent crashes or unusually slow computer performance
- Restarting Itself
- Unknown Turned On Camera
- Abnormal File Names
- High Network Activity
- Unknown Remote Desktop Application
- Frequent pop-up windows, especially the ones that encourage you to visit unusual sites, or download antivirus
- Antimalware, Task Manager or Registry Editor is disabled
- High CPU Usage
- Unknown programs that startup when you start your computer
- Your friends receive social media invitations from you that you didn’t send
How to Know If Your Computer Has been Hacked?

Investigate: Network Connections whether there is a malicious connection

Command Prompt

C:\>netstat -p TCP -abno > connections.txt
C:\>notepad connections.txt
How to Know If Your Computer Has been Hacked?

Investigate: Network Connections whether there is a malicious connection

Connections.txt

Copy all data to an excel and export only Foreign Addresses
How to Know If Your Computer Has been Hacked?

Investigate: Network Connections whether there is a malicious connection

Copy Foreign IP Addresses and submit

https://www.infobyip.com/ipbulklookup.php
How to Know If Your Computer Has been Hacked?

Investigate: Network Connections

[Table showing IP addresses and locations]

https://www.infobyip.com/ipbulklookup.php

Check the results

Look for “abnormal”

Last IP Address seems to be unusual
How to Know If Your Computer Has been Hacked?

Investigate: Network Connections

https://www.virustotal.com/

Check the first suspicious IP address on Virus Total

Virus Total is an open-source threat intelligence service by Google
How to Know If Your Computer Has been Hacked?

Investigate: Network Connections

https://www.virustotal.com/

Check the related domains under this IP address
How to Know If Your Computer Has been Hacked?

Investigate: Network Connections

https://global.sitesafety.trendmicro.com/

Check the domain on Site Safety Center
How to Know If Your Email Has been Hacked?

**Indicators: “Abnormal” activities**

- Unknown Sign In Locations
- Frequent Two Factor Authentication Calls
- Deleted Sent Messages without Knowledge
- Mass emails being sent from your email account
- Your friends receive unexpected email from your account
- Unknown forwarding rules
- Unknown inbox rules
- Opened Emails without knowledge
- Phishing Emails to your contacts
How to Know If Your Email Has been Hacked?

### Email Categories:

<table>
<thead>
<tr>
<th>Types of Emails</th>
<th>Example Email Address</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Personal Email</strong></td>
<td><a href="mailto:john.doe@gmail.com">john.doe@gmail.com</a></td>
</tr>
<tr>
<td></td>
<td><a href="mailto:john.doe@yahoo.com">john.doe@yahoo.com</a></td>
</tr>
<tr>
<td><strong>Business Email</strong></td>
<td><a href="mailto:john.doe@ncu.edu">john.doe@ncu.edu</a></td>
</tr>
<tr>
<td></td>
<td><a href="mailto:john.doe@oh.gov">john.doe@oh.gov</a></td>
</tr>
<tr>
<td></td>
<td><a href="mailto:john.doe@trendmicro.com">john.doe@trendmicro.com</a></td>
</tr>
<tr>
<td><strong>Business Group Email</strong></td>
<td><a href="mailto:admissions@ncu.edu">admissions@ncu.edu</a></td>
</tr>
<tr>
<td></td>
<td><a href="mailto:askhr@uc.edu">askhr@uc.edu</a></td>
</tr>
<tr>
<td></td>
<td><a href="mailto:helpdesk@trendmicro.com">helpdesk@trendmicro.com</a></td>
</tr>
<tr>
<td><strong>Disposable Email</strong></td>
<td><a href="mailto:928938@tempemail.co">928938@tempemail.co</a></td>
</tr>
</tbody>
</table>
How to Know If Your Email Has been Hacked? **GMAIL**

**Investigate:**

Gmail Last Sign Ins

In Gmail, you can see the last sign-in activities using “Details” button that is in the bottom of the page.
Investigate:

Gmail Last Sign Ins

Visit Security Checkup for more details

<table>
<thead>
<tr>
<th>Access Type [2] (Browser, mobile, POP3, etc.)</th>
<th>Location [IP address] [2]</th>
<th>DateTime (Displayed in your time zone)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browser (Chrome)</td>
<td>United States (KY)</td>
<td>1:35 am (6 minutes ago)</td>
</tr>
<tr>
<td>Browser (Chrome)</td>
<td>United States (KY)</td>
<td>1:34 am (6 minutes ago)</td>
</tr>
<tr>
<td>Unknown</td>
<td>United States (KY)</td>
<td>1:33 am (1 minute ago)</td>
</tr>
<tr>
<td>Browser (Chrome)</td>
<td>United States (OH)</td>
<td>1:31 am (3 minutes ago)</td>
</tr>
<tr>
<td>Browser (Chrome)</td>
<td>United States (OH)</td>
<td>1:28 am (6 minutes ago)</td>
</tr>
<tr>
<td>Browser (Chrome)</td>
<td>United States (KY)</td>
<td>1:21 am (13 minutes ago)</td>
</tr>
</tbody>
</table>

* indicates activity from the current session

This computer is using IP address 2603.6011.4840:47.44ae975.bc3:cd43a. (United States (KY))
Investigate:

Also, you can see other details under Security Checkup

- The signed-in devices
- Recent events with location and OS (Operating System) information
- Other details
Investigate:

Email Account

Email forwarding is feature to forward emails to another account.

However, attackers exploit frequently this rule. Why?

- Attackers forward emails to read messages easily
- Attackers forward emails by deleting originals in the victim’s mailbox to hide emails from the victim
- Attackers forward emails during phishing campaign to avoid the victim be aware of it
Investigate:

Email Account

Under Activity Controls, we can see the

- Web & App Activity
- Location History
- YouTube History
How to Know If Your Email Has been Hacked? OUTLOOK

**Investigate:**

In Outlook, to see your recent activity, follow the steps below:

1. My Account
2. My Sign-ins – Review Recent Activity
How to Know If Your Email Has been Hacked?

OUTLOOK

Investigate:

Outlook

- Recent activity
  - You should recognize each of these recent activities. If one looks unfamiliar, you should review your security info.

  - Location: Kentucky, US
    - Operating System: Windows 10
    - Browser: Google Chrome
    - IP: 24.166.238.99

  - Location: Texas, US
    - Operating System: Windows 10
    - Browser: Google Chrome
    - IP: 54.108.32.41

Look unfamiliar?
How to Know If Your Email Has been Hacked? OUTLOOK

Investigate:

Outlook

1). Investigate:

2).
How to Know If Your Email Has been Hacked? OUTLOOK

Outlook Email Inbox Rule

The attackers exploit this feature frequently in phishing campaigns.

In this example rule,

- It deletes all the coming messages.
- It also marks all the coming messages as read.
- The attacker uses only ‘.’ (a dot) for the rule name to hide the rule.
- Some attackers forward the emails to themselves before delete function.

The victim never receive emails.