REPORT ON WEBINAR

Topic: Cyber Security

Organised by: PMP Planet

Date, Time: July 3, 2020, 11:00 am

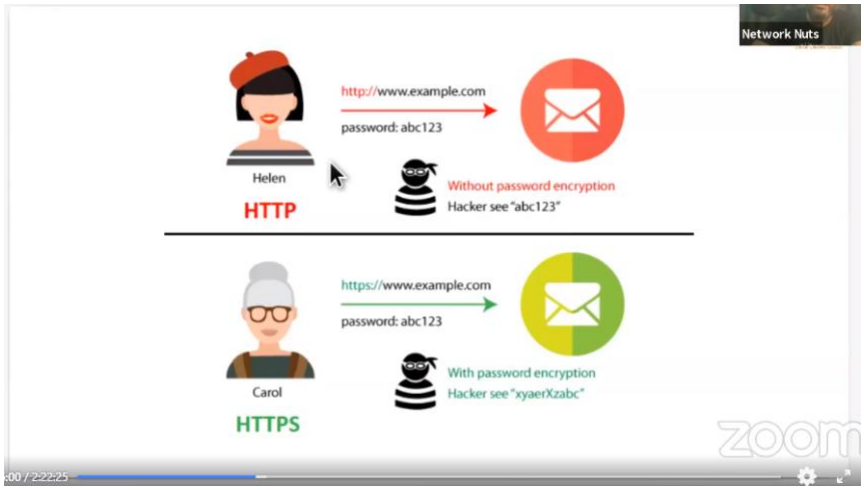
Speaker : Mr. Alok Srivatava

Attendees: Ritu Arora, Shilpa Aggarwal, Nidhi Arora, Jyoti Khurana, Alka Sanan, Sonia Gumber, Shreha Bisla, Priyanka Kochagaway

The webinar on the topic "Cyber Security" was conducted by PMP Publishers. The main points covered in the webinar were:

- The difference between Information Security and Cyber Security.
- Terminologies related to Cyber security were explained
- The use of domain tools like Whois were explained.
- Addressed the concern of fake accounts creation by various students
- Explained various terms like cat fishing, data mining, cookies etc
- Elaborated how a general online user can fall into various traps
- Described the different types of hackers and their roles
- Various hacking methodologies were discussed.
- Explained how passwords are cracked within minutes and personal information or confidential data can be hacked
- Alerted people about Phishing attacks
- Various types of security attacks like DOS attacks – Denial of Services attacks, MITM attacks, XSS attacks
- Various types of malware like virus, worms, trojans, adware, spyware, ransomware
- Demonstrated how govt agencies map cyber attacks
- Use of a reputed anti-virus is important
- Two Factor Authentication or two step verification, as we call it, should be enabled on our devices.
- Steps on how to ensure security of our wifi systems were discussed.
- Password management is important. Passwords should be lengthy and should not contain any personal names.

- Last but not the least, anyone can be a target of a cyber attack, so all should follow the security measures and be safe online.



HTTP & HTTPS

- Hyper Text Transfer Protocol
- Determines how browser and web servers communicate
- Connection will be dropped once the request is catered - stateless
- HTTPS - Secure. Is a secure version of HTTP and communication is encrypted.

Hacking Methodology

#1 FOOTPRINTING

- Passive method of gaining info about a target.
- "whois" queries. google search. job based posting to find what tech. target use.

#2 SCANNING

- More active way of gathering information.
- Using "port scanning", ping sweeps & physical visit to target facility.

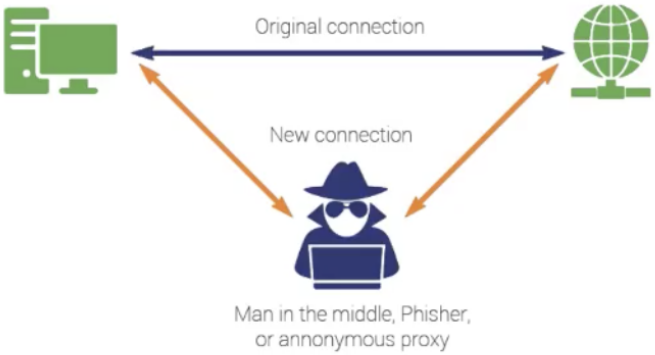
#3 ENUMERATION

- Gathering more information about victim.
- Getting username / passwords.

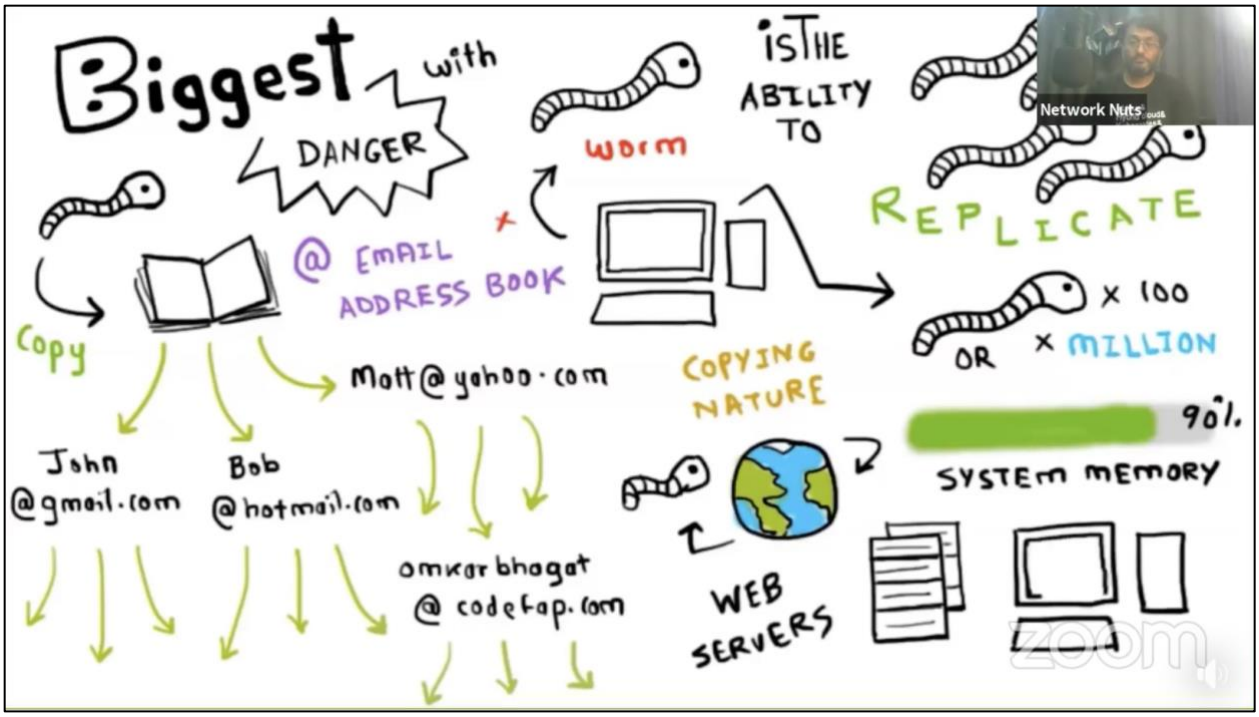
#4 SYSTEM HACKING

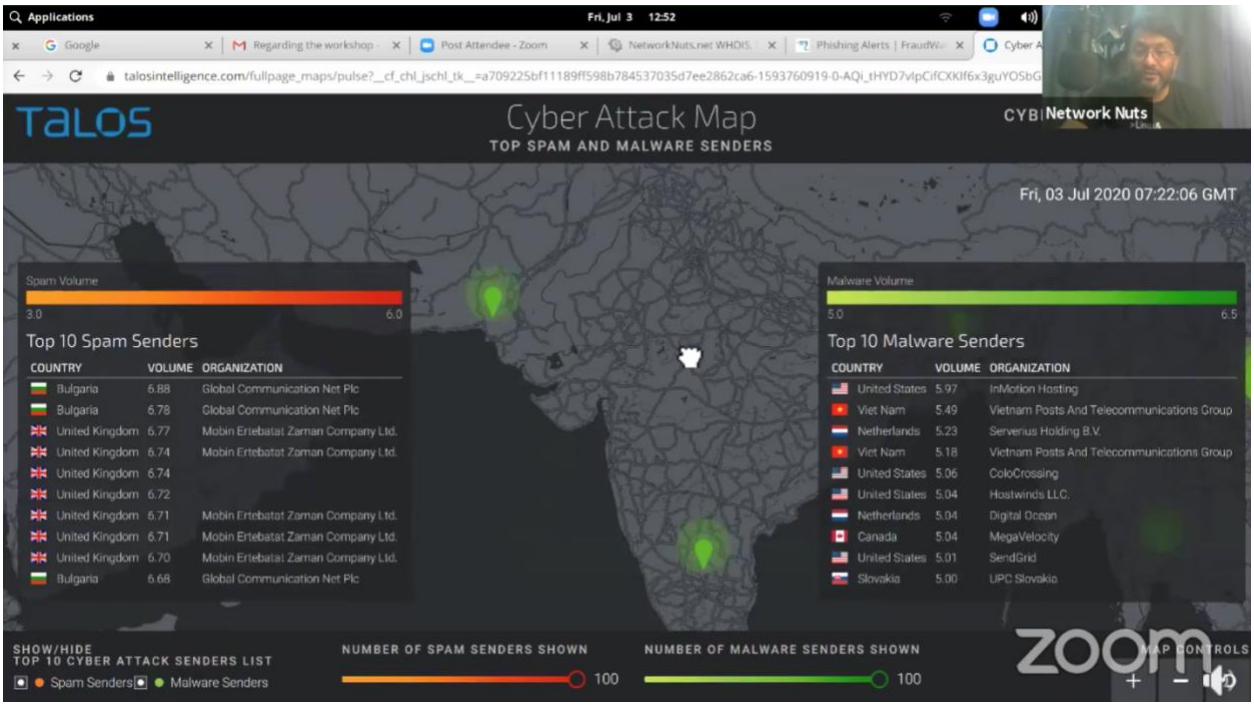
- Attack the victim by using all the information gathered in above 3 steps.

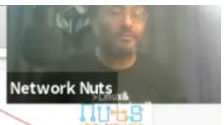
MAN IN THE MIDDLE ATTACK



MITM

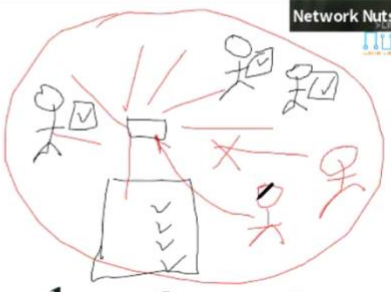

Biggest
with
DANGER
worm
+
@ EMAIL ADDRESS BOOK
Copy
Matt@yahoo.com
John @gmail.com
Bob @hotmail.com
omkar bhagat @ codekap.com
IS THE ABILITY TO
REPLICATE
x 100
OR x MILLION
COPYING NATURE
90%
SYSTEM MEMORY
WEB SERVERS
Network Nuts
zoom


Applications
Fri, Jul 3 12:52
talosintelligence.com/fullpage_maps/pulse?__cf_chl_jschl_tk__=a709225bf11189ff598b784537035d7ee2862ca6-1593760919-0-AQi_tHYD7vlpCifCXKlf6x3guYOSbG
TALOS
Cyber Attack Map
TOP SPAM AND MALWARE SENDERS
Network Nuts
Fri, 03 Jul 2020 07:22:06 GMT
Spam Volume
3.0
6.0
Top 10 Spam Senders
COUNTRY VOLUME ORGANIZATION
Bulgaria 6.88 Global Communication Net Plc
Bulgaria 6.78 Global Communication Net Plc
United Kingdom 6.77 Mobin Ertebatat Zaman Company Ltd.
United Kingdom 6.74 Mobin Ertebatat Zaman Company Ltd.
United Kingdom 6.74
United Kingdom 6.72
United Kingdom 6.71 Mobin Ertebatat Zaman Company Ltd.
United Kingdom 6.71 Mobin Ertebatat Zaman Company Ltd.
United Kingdom 6.70 Mobin Ertebatat Zaman Company Ltd.
Bulgaria 6.68 Global Communication Net Plc
Malware Volume
5.0
6.5
Top 10 Malware Senders
COUNTRY VOLUME ORGANIZATION
United States 5.97 InMotion Hosting
Viet Nam 5.49 Vietnam Posts And Telecommunications Group
Netherlands 5.23 Serverius Holding B.V.
Viet Nam 5.18 Vietnam Posts And Telecommunications Group
United States 5.06 ColoCrossing
United States 5.04 Hostwinds LLC.
Netherlands 5.04 Digital Ocean
Canada 5.04 MegaVelocity
United States 5.01 SendGrid
Slovakia 5.00 UPC Slovakia
SHOW/HIDE TOP 10 CYBER ATTACK SENDERS LIST
Spam Senders
Malware Senders
NUMBER OF SPAM SENDERS SHOWN
100
NUMBER OF MALWARE SENDERS SHOWN
100
zoom



WIRELESS SECURITY

- Change default SSID. Don't give provocating names like "hackifyoucan". They can backfire
- Never use default username & password.
- Use WPA2 (wifi protection access 2)
- Change default IP address. Which is generally http://192.168.1.1 or http://192.168.0.1
- Turn off DHCP
- Disable remote access
- MAC binding, if possible



Wireless Security