Horizon Scanning of Workplace Trends and Technologies Fostering Innovation and Creative Thinking

John Ezekiel Miclat, RL

UP Marine Science Institute

What I do in life

- Systems Administration
- Network Administration
- Web Development
- PC Gaming
- PC Building
- Photography

Horizon Scanning of Workplace **Trends** and Technologies Fostering Innovation and Creative Thinking


SECURITY

New Malware targeting Routers

VPNFilter

(Largent, 2018)

Router

Linksys E1200

(Belkin International, Inc., 2018)

ASUS RT-N66U

(ASUSTek Computer, Inc., 2018)

VPNFilter

- A malicious software that could be installed remotely to a specific set of routers that has **default administrative credentials** to steal sensitive information.
  - **Username: admin**
  - **Password: admin**
- Researched extensively by CISCO's TALOS Intelligence Group and the Federal Bureau of Investigation (FBI)

(Largent, 2018)

Known Targeted Devices

ASUS DEVICES:
RT-AC66U (new)
RT-N10 (new)
RT-N10E (new)
RT-N10U (new)
RT-N56U (new)
RT-N66U (new)

D-LINK DEVICES:
DES-1210-08P (new)
DIR-300 (new)
DIR-300A (new)
DSR-250N (new)
DSR-500N (new)
DSR-1000 (new)
DSR-1000N (new)

HUAWEI DEVICES:
HG8245 (new)

LINKSYS DEVICES:
E1200
E2500
E3000 (new)
E3200 (new)

LINKSYS DEVICES (CONT.):
E4200 (new)
RV082 (new)
WRVS4400N

MIKROTIK DEVICES:
CCR1009 (new)
CCR1016
CCR1036
CCR1072
CRS109 (new)
CRS112 (new)
CRS125 (new)
RB411 (new)
RB450 (new)
RB750 (new)
RB911 (new)
RB921 (new)
RB941 (new)
RB951 (new)
RB952 (new)
RB960 (new)
RB962 (new)
RB1100 (new)
RB1200 (new)

MIKROTIK DEVICES (CONT.):
RB2011 (new)
RB3011 (new)
RB Groove (new)
RB Omnitik (new)
STX5 (new)

NETGEAR DEVICES:
DG834 (new)
DGN1000 (new)
DGN2200
DGN3500 (new)
FVS318N (new)
MBRN3000 (new)
R6400
R7000
R8000
WNR1000
WNR2000
WNR2200 (new)
WNR4000 (new)
WNDR3700 (new)
WNDR4000 (new)
WNDR4300 (new)
WNDR4300-TN (new)

NETGEAR DEVICES (CONT.):
UTM50 (new)

QNAP DEVICES:
TS251
TS439 Pro
Other QNAP NAS devices running QTS software

TP-LINK DEVICES:
R600VPN
TL-WR741ND (new)
TL-WR841N (new)

UBIQUITI DEVICES:
NSM2 (new)
PBE M5 (new)

UPVEL DEVICES:
Unknown Models* (new)

ZTE DEVICES:
ZXHN H108N (new)

(Largent, 2018)

Mode of Infection

- Attempt to login to the router's administration panel using default credentials
- If successful, install itself inside the router's flash memory
- Determine the router's model and hardware capabilities
- If the router's model and hardware capabilities satisfies the malware's requirements, commence operation. Otherwise, execute the self-destruct module to prevent detection.

(Largent, 2018)

VPNFilter - Modules

- '**ssler**' (Endpoint exploitation module — JavaScript injection)
  - Intercepts, inspects, and manipulates all outgoing web (HTTP and HTTPS) requests before being sent to the true HTTP/HTTPS Server
  - If the module encounters any POST request that contain a username and password, the information is stored and transmitted to the malware creators' servers

- '**dstr**' (device destruction module)
  - acts as the malware's self-destruct mechanism which allows it to delete itself from the router to prevent detection

(Largent, 2018)

VPNFilter - Modules

- ‘ps’ (stage 3 packet sniffer)
  - Grants the malware the ability to view network traffic
  - Scans the network for BasicAuth requests which is commonly used to login to routers
  - Data from these requests are logged and could be used to infect other routers

(Largent, 2018)

Prevention/Removal

- Disconnect the router from the internet
- Reset the router to factory defaults
- Change the router's default administration credentials
- Reconnect the router to the internet

(Largent, 2018)

Takeaway

- When buying networking equipment, always change its default administrator credentials!

https://blog.talosintelligence.com/2018/06/vpnfilter-update.html

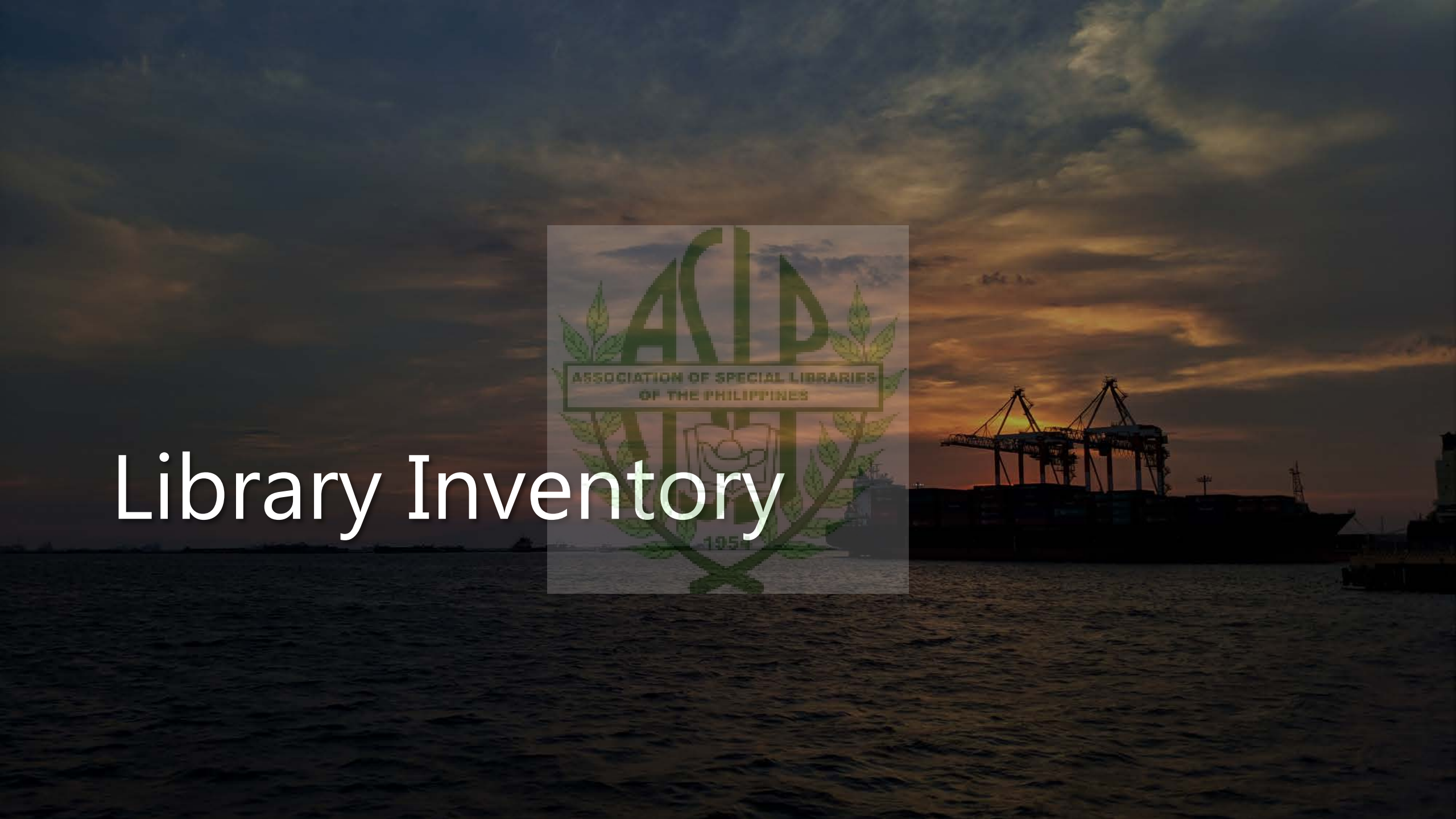
Horizon Scanning of Workplace Trends and **Technologies Fostering Innovation and Creative Thinking**


PROBLEM

INNOVATION AND CREATIVE THINKING


RESOURCEFUL


COLLABORATE



Library Inventory

Partner Institutions

UP School of Economics Library

- 101,960 Volumes
- takes about a month to finish inventory
- Labour-intensive

Resources

Web Development Skills
- HTML, PHP, SQL (MariaDB 10.3), JavaScript (jQuery, AngularJS)

Web Development Frameworks
- Bootstrap, Mobile Angular UI

Hardware
- Android Smartphones
- Laptops and Netbooks (to be used with existing barcode scanners)
- Desktop Workstation (to be used as a Server)
- Wireless Router


MISA DEMO

https://gitlab.com/techkiel/misa

Library Market Research

Partner Institutions

- UP School of Economics Library
  - Mr Brian Lloyd Dayrit, RL
- UP Virata School of Business Library
  - Ms Cossette Martinez, RL

Resources

Web Development Skills
- HTML, PHP, SQL (MariaDB 10.3), JavaScript (jQuery)

Web Development Frameworks
- Bootstrap, Bootswatch, Charts.js

Hardware
- Android Tablets
- Apple iPads
- Laptops and Notebooks
- Desktop Workstation (to be used as a Server)


ENcounter DEMO

CPD and Attendance Tracking

Partner Institutions

- Philippine Digestive Health Week (2017 –)
  - Philippine Society of Gastroenterology
  - Philippine Society of Digestive Endoscopy
  - Hepatology Society of the Philippines

- Association of Special Libraries of the Philippines (2018 –)

Resources

Web Development Skills
- HTML, PHP, SQL (MariaDB 10.3), JavaScript (jQuery, AngularJS)

Web Development Frameworks
- Bootstrap, Mobile Angular UI, TCPDF

Hardware
- Mobile Workstation (to be used as a Server)
- Cloud-based Virtual Machine (for certificate validation system)
- Laptops/Notebooks
- Zebra MK590 Micro Kiosk/Barcode Scanner
- Enterprise/Prosumer-grade Wireless Router


CATS DEMO

Important Points to Consider

- Proper Documentation
- Users' Training
- Turnover to System Administrator
- Maintenance Contract (if outsourced)


If the tool or technology isn’t here yet, let’s develop it.

Q & A Session

Breakout Group Activity (30 mins)

- As a group, think of a Library name
- Taking to account the issues that you experience in your own library:
  - Vote among yourselves which issue do you want to address using the concepts discussed in the lecture
  - Determine what skills and resources do you need to get it done
  - Think of a catchy name for the system which will be developed
- Select a member to briefly present your output

Don’t forget to write your names!


Brief Presentation

Resources Used

- Largent, W. (2018). VPNFilter Update - VPNFilter exploits endpoints, targets new devices. Retrieved from https://blog.talosintelligence.com/2018/06/vpnfilter-update.html [Accessed 6 Jun. 2018].
- Belkin International, Inc. (2018). *Linksys E1200 N300 Wi-Fi Router*. [image] Available at: https://www.linksys.com/images/productmt_aem/697904/renditions/cq5dam.web.1000.1000.jpeg [Accessed 8 Jun. 2018].
- ASUSTeK Computer Inc. (2018). *ASUS RT-N66U Dual-Band Wireless-N900 Gigabit Router*. [image] Available at: https://www.asus.com/media/global/products/PZkFHlMrGWzVROxT/P_setting_fff_1_90_end_500.png [Accessed 8 Jun. 2018].

Photo: Manila Bay Sunset captured from the deck of BRP Gregorio Velasquez (AGR 702) [formerly R/V Melville] at Pier 13, Manila South Harbor. Miclat (2018)