Threat Intelligence Sources

- Organizations are now pooling resources and knowledge about the latest attacks with the broader security community
- One type of shared information is the evidence of an attack
- *Key risk indicators* (*KRI*s) are metrics of the upper and lower bounds of specific indicators of normal network activity
  - These indicators may include the total network logs per second, number of failed remote logins, network bandwidth, and outbound email traffic
- A KRI exceeding its normal bounds could be an **indicator of compromise** (**IOC**)
  - An IOC shows that a malicious activity is occurring but is still in the early stages of an attack
  - IOC information aids others in their predictive analysis or discovering an attack before it occurs

Categories of Sources (1 of 3)

- Two categories of threat intelligence sources are open source and closed source
- Open Source Information
  - “open source” refers to anything that could be freely used without restrictions
  - Open source threat intelligence information is often called open source intelligence (OSINT)
  - Cyber Information Sharing and Collaboration Program (CISCP) enables actionable, relevant, and timely unclassified information exchange through partnerships
  - CISP services include:
    - *Analyst-to-analyst technical exchanges*
    - *CISCP analytical products*
    - *Cross industry orchestration*
    - *Digital malware analysis*

CENGAGE

Categories of Sources (2 of 3)

- Two concerns around public information sharing centers are:
  - Privacy – an organization that is the victim of an attack must be careful not to share proprietary or sensitive information when providing IOCs and attack details
  - Speed – **Automated Indicator Sharing** (**AIS**) enables the exchange of cyberthreat indicators between parties through computer-to-computer communication
    - Two tools facilitate AIS:
      - ▸ **Structured Threat Information Expression** (**STIX**) is a language and format used to exchange cyberthreat intelligence
      - ▸ **Trusted Automated Exchange of Intelligence Information** (**TAXII**) is an application protocol for exchanging cyberthreat intelligence over HTTPS

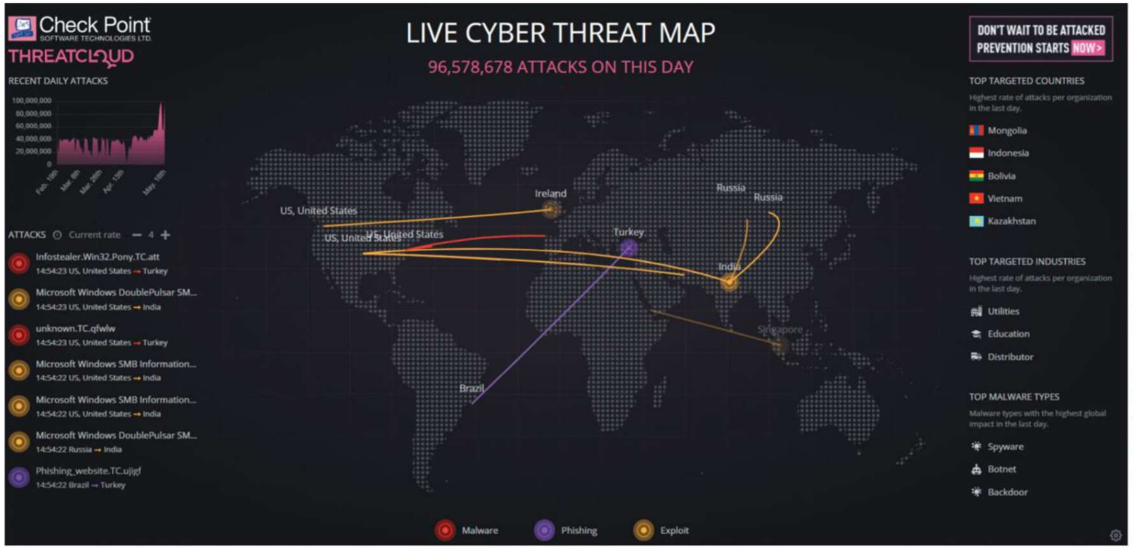
Categories of Sources (3 of 3)

- Closed Source Information
  - **Closed source** is proprietary
  - Organizations that are participants in closed source information are part of private information sharing centers that restrict both access to data and participation
  - All candidates must go through a vetting process and meet certain criteria

Sources of Threat Intelligence (1 of 3)

- Sources of threat intelligence that are useful:
  - *Vulnerability database* is a repository of known vulnerabilities and information as to how they have been exploited
  - *Threat maps* illustrate cyberthreats overlaid on a diagrammatic representation of a geographical area
  - *File and code repositories* are where victims of an attack can upload malicious files and software code that can be examined by others to learn more about the attacks and craft their defenses
  - *Dark web* – security professionals and organizations use the dark web on a limited basis to look for signs that information critical to that enterprise is being sought out or sold on the dark web

Sources of Threat Intelligence (2 of 3)



LIVE CYBER THREAT MAP

96,578,678 ATTACKS ON THIS DAY

RECENT DAILY ATTACKS

ATTACKS Current rate − 4 +

Infostealer.Win32.Pony.TC.att
14:54:23 US, United States → Turkey

Microsoft Windows DoublePulsar SM...
14:54:23 US, United States → India

unknown.TC.qfwlw
14:54:23 US, United States → Turkey

Microsoft Windows SMB Information...
14:54:22 US, United States → India

Microsoft Windows SMB Information...
14:54:22 US, United States → India

Microsoft Windows DoublePulsar SM...
14:54:22 Russia → India

Phishing_website.TC.ujigf
14:54:22 Brazil → Turkey

DON'T WAIT TO BE ATTACKED
PREVENTION STARTS NOW>

TOP TARGETED COUNTRIES
Highest rate of attacks per organization in the last day.

- Mongolia
- Indonesia
- Bolivia
- Vietnam
- Kazakhstan

TOP TARGETED INDUSTRIES
Highest rate of attacks per organization in the last day.

- Utilities
- Education
- Distributor

TOP MALWARE TYPES
Malware types with the highest global impact in the last day.

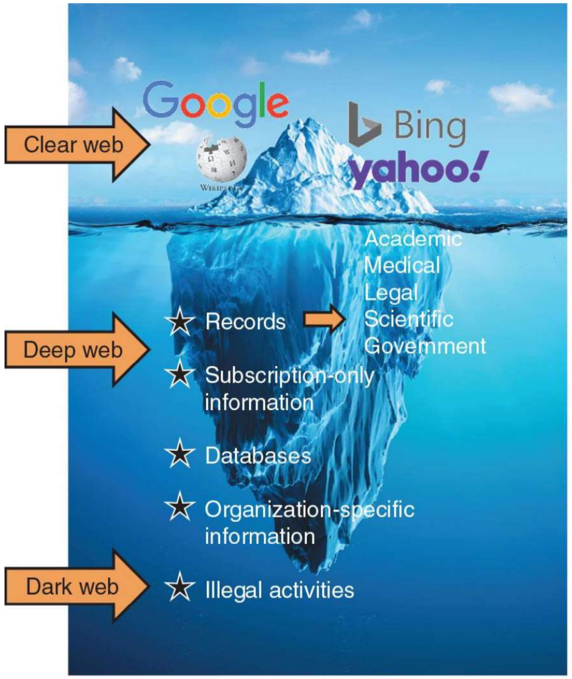
- Spyware
- Botnet
- Backdoor

Source: Check Point Software Technologies Ltd.

Figure 4-1 Threat map

Figure 4-1 Threat map

Sources of Threat Intelligence (3 of 3)



Source: Romolo Tavani/Shutterstock.com

Figure 4-2 Dark web

Figure 4-2 Dark web

Knowledge Check Activity 1

What is the significance of a KRI exceeding its normal bounds?

a. It must be referred to the DHS.

b. It could be an IOC.

c. It probably contains a TTP.

d. An AIS should be generated.

Knowledge Check Activity 1: Answer

What is the significance of a KRI exceeding its normal bounds?

Answer: b. It could be an IOC*.*

A key risk indicator (KRI) exceeding its normal bounds could be an indicator of compromise (IOC).

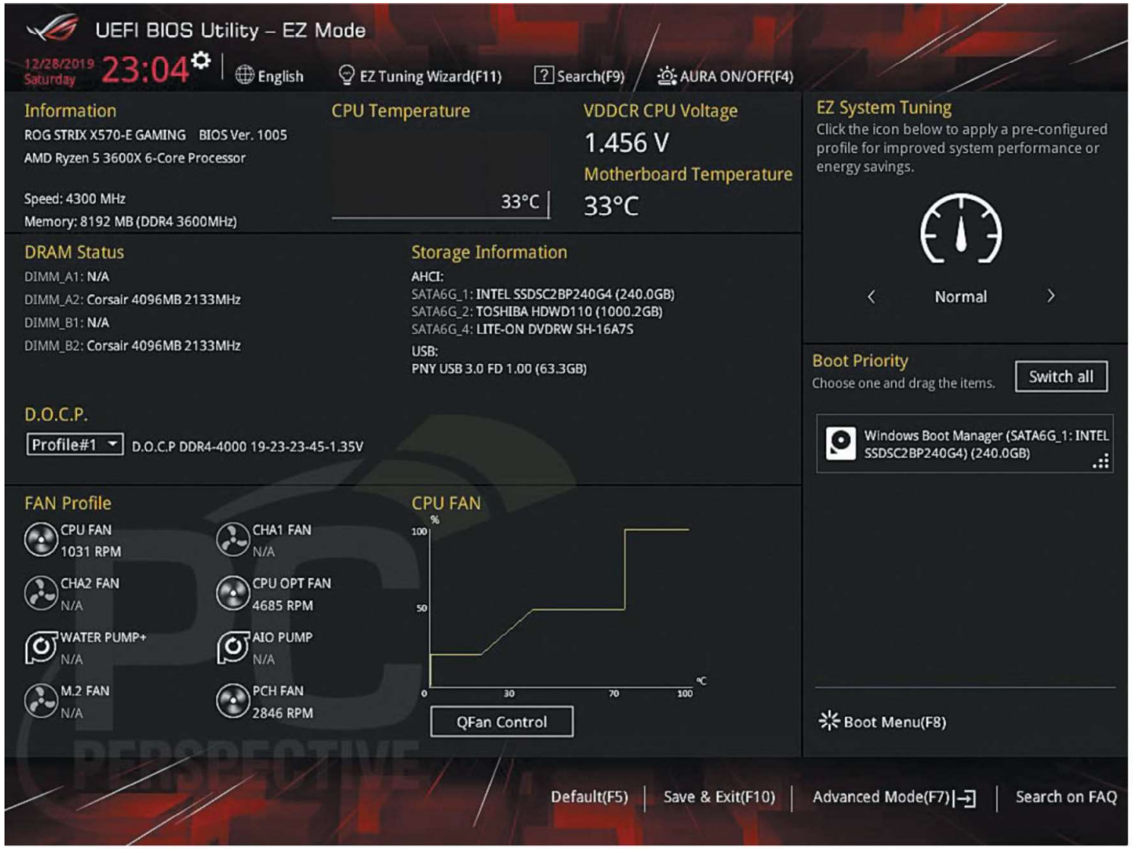
Securing Endpoint Computers

- Securing endpoint computers primarily involves three major tasks:
  - *Confirming* that the computer has started securely
  - *Protecting* the computer from attacks
  - *Hardening* it for even greater protection

Confirm Boot Integrity (1 of 3)

- Ensuring secure startup involves the Unified Extensible Firmware Interface (UEFI) and its boot security features
- Unified Extensible Firmware Interface (UEFI)
  - Early booting processes used firmware called the *BIOS* (*Basic Input/Output System*)
  - To add functionality, an improved firmware interface was developed to replace BIOS
  - **UEFI** includes:
    - The ability to access hard drives that are larger than 2TB
    - Support for an unlimited number of primary hard drive partitions
    - Faster booting
    - Support for networking functionality in the UEFI firmware itself to aid in troubleshooting

Confirm Boot Integrity (2 of 3)



UEFI BIOS Utility – EZ Mode

12/28/2019 Saturday 23:04

Information
ROG STRIX X570-E GAMING BIOS Ver. 1005
AMD Ryzen 5 3600X 6-Core Processor
Speed: 4300 MHz
Memory: 8192 MB (DDR4 3600MHz)

CPU Temperature
33°C

VDDCR CPU Voltage
1.456 V

Motherboard Temperature
33°C

EZ System Tuning
Click the icon below to apply a pre-configured profile for improved system performance or energy savings.
Normal

DRAM Status
DIMM_A1: N/A
DIMM_A2: Corsair 4096MB 2133MHz
DIMM_B1: N/A
DIMM_B2: Corsair 4096MB 2133MHz

Storage Information
AHCI:
SATA6G_1: INTEL SSDSC2BP240G4 (240.0GB)
SATA6G_2: TOSHIBA HDWD110 (1000.2GB)
SATA6G_4: LITE-ON DVDRW SH-16A7S
USB:
PNY USB 3.0 FD 1.00 (63.3GB)

Boot Priority
Choose one and drag the items.
Windows Boot Manager (SATA6G_1: INTEL SSDSC2BP240G4) (240.0GB)

D.O.C.P.
Profile#1 D.O.C.P DDR4-4000 19-23-23-45-1.35V

FAN Profile
CPU FAN 1031 RPM
CHA1 FAN N/A
CHA2 FAN N/A
CPU OPT FAN 4685 RPM
WATER PUMP+ N/A
AIO PUMP N/A
M.2 FAN N/A
PCH FAN 2846 RPM

Source: ASUS

Figure 4-3 UEFI user interface

Figure 4-3 UEFI user interface

Confirm Boot Integrity (3 of 3)

- Boot Security
  - The ability to update the BIOS in firmware opened the door for a threat actor to create malware to infect the BIOS (called a *BIOS attack*)
  - Boot security involves validating that each element used in each step of the boot process has not been modified
  - This process begins with validation of the boot software, then it can validate the software drivers, and so on until control has been handed over to the OS
    - Called *chain of trust* because each element relies on the confirmation of the previous element to know that the entire process is secure
    - The strongest starting point is hardware, which cannot be modified like software (known as **hardware root of trust**)

Protect Endpoints (1 of 4)

- Protection on computer endpoints can be accomplished through software installed on the endpoint, such as:
  - Antivirus software, antimalware, web browser protections, and monitoring and response systems
- Antivirus
  - **Antivirus** (**AV**) software can examine a computer for file-based virus infections and monitor computer activity (such as scanning new documents that might contain a virus)
  - Log files created by AV products can provide beneficial info regarding attacks
  - Many AV products use signature-based monitoring, called *static analysis*
  - A newer approach to AV is heuristic monitoring, called *dynamic analysis*

Protect Endpoints (2 of 4)

- Antimalware
  - **Antimalware** is a suite of software intended to provide protections against multiple types of malware
  - Antimalware spam protection is often performed using a technique called *Bayesian filtering*
    - Filters by analyzing every word in each email and determines how frequently a word occurs in a spam pile versus a nonspam pile
  - Another component of an antimalware suite is *antispyware*, which helps prevent computers from becoming infected by spyware
    - Uses pop-up blockers, which allow the user to select the level of blocking, ranging from blocking all pop-ups to allowing specific pop-ups

Protect Endpoints (3 of 4)

- Web Browsers
  - Web browsers offer the following security on endpoint computers:
    - Secure cookies are sent to a web server with an encrypted request over the secure HTTPS protocol
      - This prevents an unauthorized person from intercepting a cookie that is being transmitted between the browser and the web server
    - HTTP Response Header are headers that tell the browser how to behave while communicating with the website

Protect Endpoints (4 of 4)

- Monitoring and Response Systems
  - There are three types of monitoring and response systems for endpoint computers:
    - **Host Intrusion Detection Systems** (**HIDS**) is a software-based application that runs on an endpoint computer and can detect an attack has occurred
    - **Host Intrusion Prevention Systems** (**HIPS**) monitor endpoint activity to immediately block a malicious attack by following specific rules
    - **Endpoint Detection and Response** (**EDR**) tools are considered more robust than HIDS and HIPS
      - An EDR can aggregate data from multiple endpoint computers to a centralized database
      - EDR tools can perform more sophisticated analytics that identify patterns and detect anomalies