Operating System Commands

What are the standard Windows processes?

* **System**
* **Idle**
* **Smss**
* **Crss.exe**
* **Wininit.exe**
* **Services.exe**
* **Svchost.exe**
* **Taskhost.exe**
* **Winlogon.exe**
* **Explorer.exe**
* **Registry**
* **Memory compression**
* **Dwm.exe**
* **Dllhost.exe**

Which one will have more than one process if multiple users are logged on?

-Taskhost

Networking

What does a network switch use to determine which port a packet should be forwarded to?

* **The switch uses the MAC address.**

What type of attack takes advantage of this tool by filling it to capacity so any new traffic is forwarded to all ports?

* **Denial of Service Attack**

Security Principles

What are the 6 tenants of the STRIDE threat model? Describe each.

Security Principles

What are the 6 tenants of the STRIDE threat model? Describe each.

**SPOOFING-Spoofing refers to the act of posing as someone else (i.e. spoofing a user) or claiming a false identity**

**TAMPERING-Tampering refers to malicious modification of data or processes. Tampering may occur on data in transit, on data at rest, or on processes**

**REPUDIATION-Repudiation refers to the ability of denying that an action or an event has occurred.**

**INFORMATION DISCLOSURE-Information Disclosure refers to data leaks or data breaches. This could occur on data in transit, data at rest, or even to a process.**

**DENIAL OF SERVICE-Denial of Service refers to causing a service or a network resource to be unavailable to its intended users.**

**ELEVATION OF PRIVILEGES- Elevation of Privileges refers to gaining access that one should not have.**

Cyber Threat Intelligence

Using information from this recent CTI report, provide examples for each of the four points of the Diamond Model.

Adversary

* **BeagleBoyz**
* **North Korea**

Infrastructure

IP Adressess:

112[.]175[.]92[.]57

113[.]114[.]117[.]122

117[.]239[.]241.2

SHA256 HASH:

#### 05/feed9762bc46b47a7dc5c469add9f163c16df4ddaafe81983a628da5714461

#### 7c/f5d86cc75cd8f0e22e35213a9c051b740bd4667d9879a446f06277782bffd1

Victims:

* **targeted financial institutions in the following nations from 2015 through 2020: Argentina, Brazil, Bangladesh, Bosnia and Herzegovina, Bulgaria, Chile, Costa Rica, Ecuador, Ghana, India, Indonesia, Japan, Jordan, Kenya, Kuwait, Malaysia, Malta, Mexico, Mozambique, Nepal, Nicaragua, Nigeria, Pakistan, Panama, Peru, Philippines, Singapore, South Africa, South Korea, Spain, Taiwan, Tanzania, Togo, Turkey, Uganda, Uruguay, Vietnam, Zambia**
* **Bank Executives/Bankemployees**

Capabilities:

* **Utilize spearphishing and watering holes,**
* **the BeagleBoyz demonstrated the use of social engineering tactics by carrying out job-application themed phishing attacks**
* **The BeagleBoyz use a variety of techniques to run their code on local and remote victim systems**