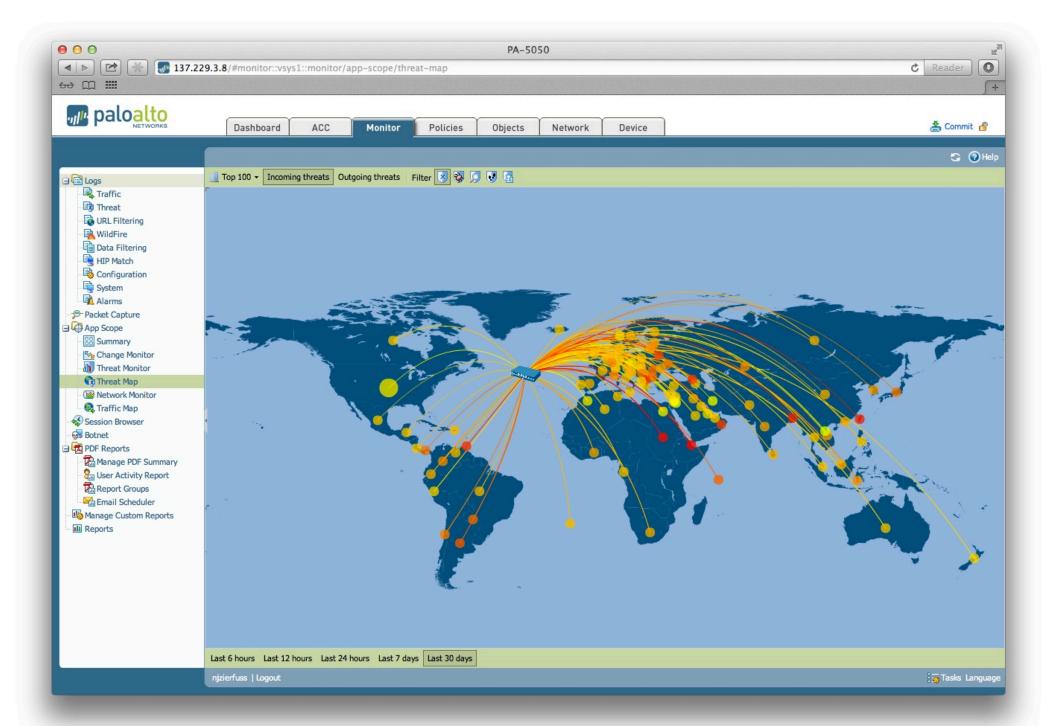
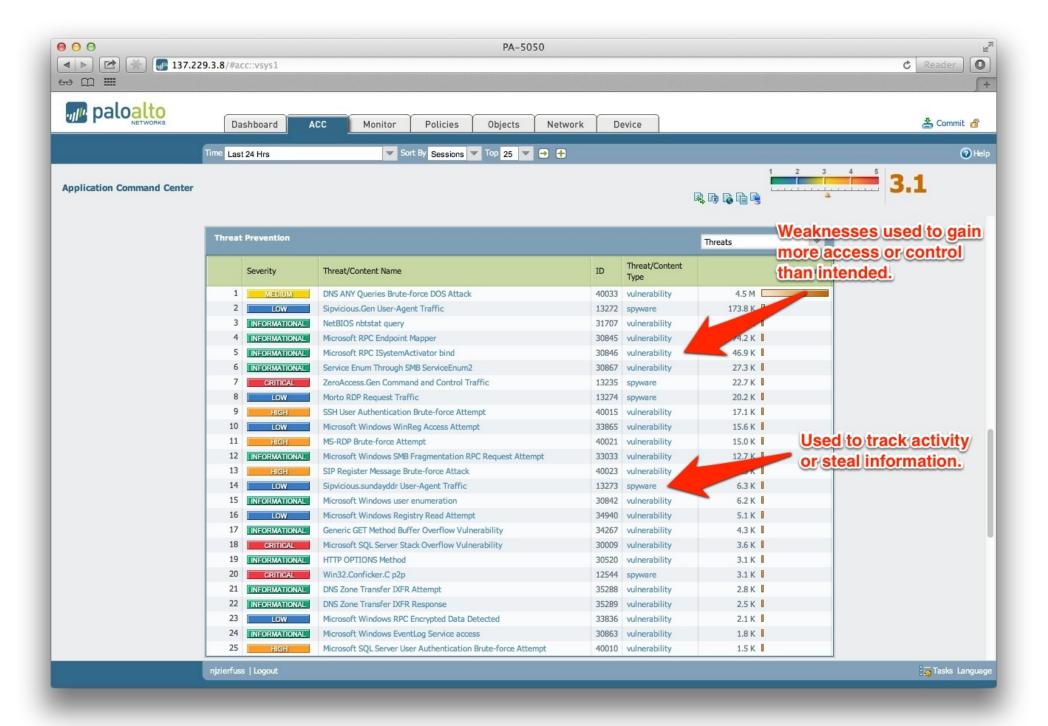
**UNIVERSITY OF ALASKA** 

## IT Update - Security

## Malware Detection and Prevention

Office of Information Technology
April 11, 2013





## **Common Computer Security Terms & Definitions**

**Advanced persistent threat** (**APT**) refers to a group, such as a foreign government, with both the capability and the intent to persistently and effectively target a specific entity.

**Botnet** is a jargon term for a collection of software robots, or bots, that run autonomously and automatically. The term is often associated with malicious software but it can also refer to the network of computers using distributed computing software.

A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users.

**E-mail spoofing** is a term used to describe fraudulent e-mail activity in which the sender address and other parts of the e-mail header are altered to appear as though the e-mail originated from a different source

**File sharing** is the practice of sharing digital information, such as music and video files, often in violation of copyright laws. It includes both the manual sharing of files using removable media and the use of peer-to-peer computer networks to allow direct access download.

**Malware**, a portmanteau from the words **mal**icious and software, is software designed to infiltrate or damage a computer system without the owner's informed consent.

A **peer-to-peer** (or **P2P**) computer network uses diverse connectivity between participants in a network and the cumulative bandwidth of network participants rather than conventional centralized resources where a relatively low number of servers provide the core value to a service or application. P2P networks are typically used for connecting nodes via largely *ad hoc* connections. Such networks are useful for many purposes.

Sharing content files (see file sharing) containing audio, video, data or anything in digital format is very common, and real time data, such as telephony traffic, is also passed using P2P technology.

**Phishing** is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.

**Spam** is the abuse of electronic messaging systems (including most broadcast mediums, digital delivery systems) to send unsolicited bulk messages indiscriminately.

In the context of network security, a **spoofing attack** is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.

**Spyware** is computer software that is installed surreptitiously on a personal computer to collect information about a user, their computer or browsing habits without the user's informed consent.

A **Trojan horse** is a program which seems to be doing one thing, but is actually doing another. A trojan horse can be used to set up a back door in a computer system such that the intruder can gain access later.

A computer **virus** is a computer program that can copy itself and infect a computer without the permission or knowledge of the owner.

A vulnerability scanner is a tool used to quickly check computers on a network for known weaknesses.

**Weaponization** is to take a technique for exploiting a vulnerability and packaging it for simplified, targeted, persistent and semi-autonomous usage.