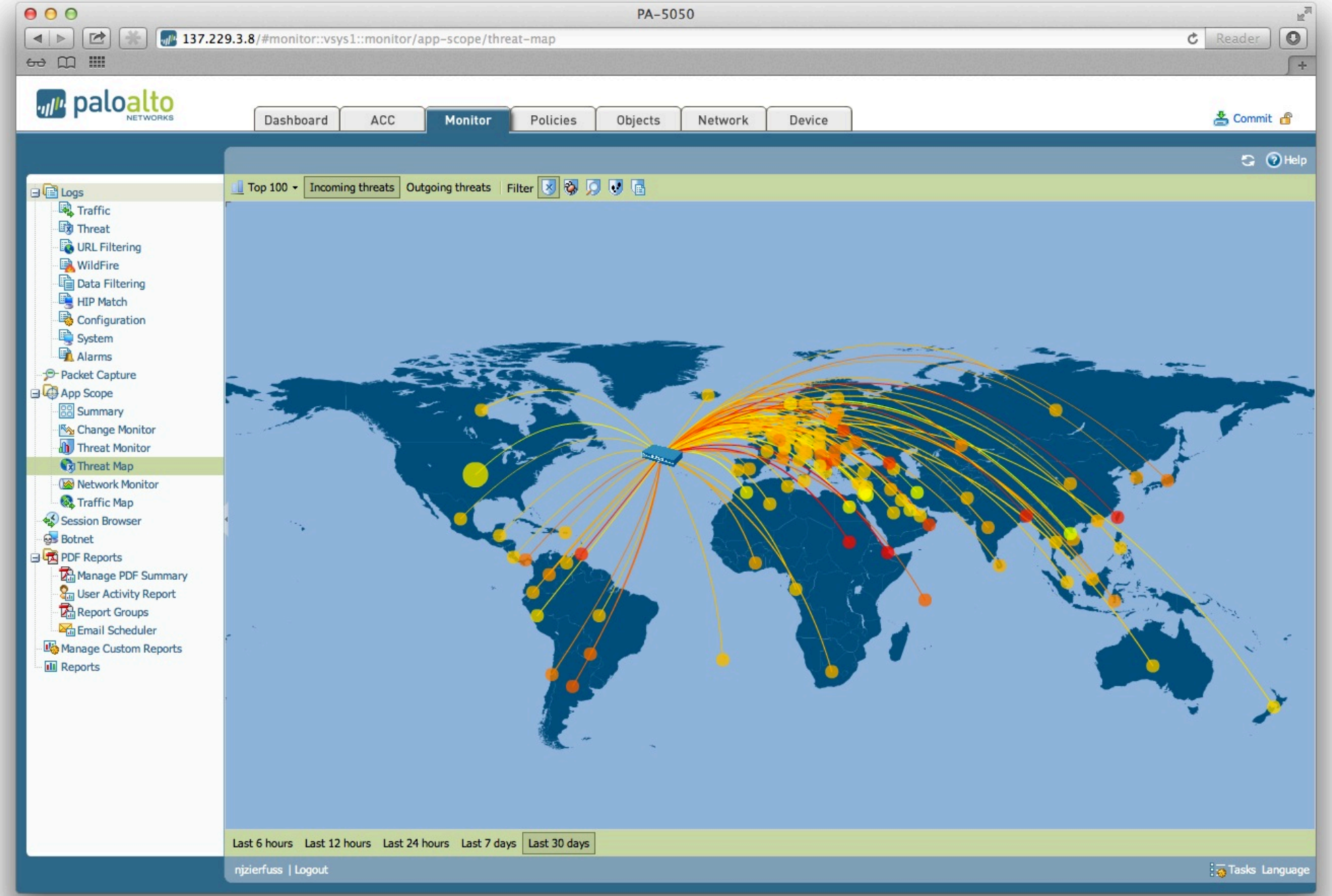
UNIVERSITY OF ALASKA

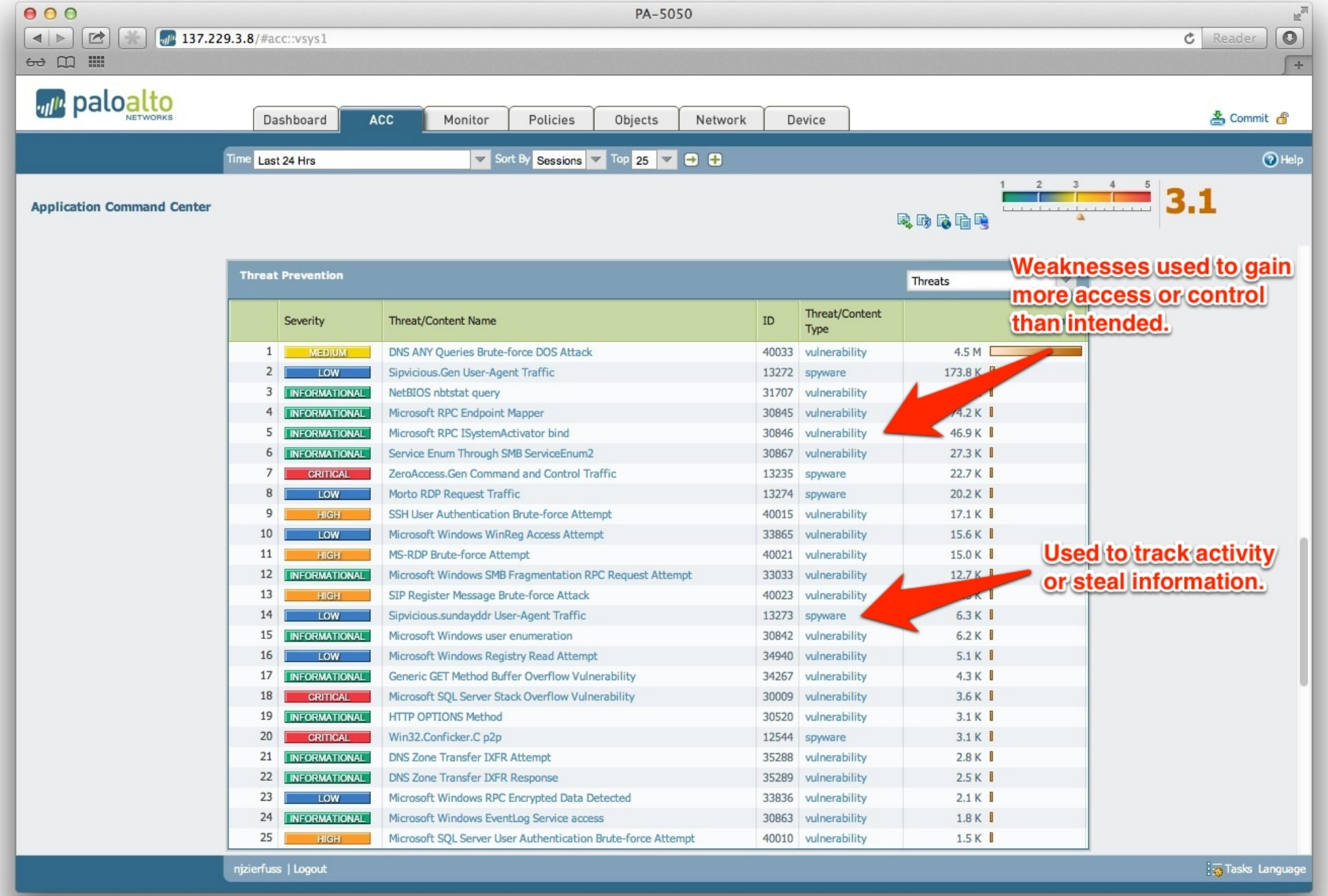
IT Update - Security

Malware Detection and Prevention

Office of Information Technology

April 11, 2013


PA-5050
137.229.3.8/#monitor::vsys1::monitor/app-scope/threat-map
Reader
paloalto NETWORKS
Dashboard
ACC
Monitor
Policies
Objects
Network
Device
Commit
Help
Logs
Traffic
Threat
URL Filtering
WildFire
Data Filtering
HIP Match
Configuration
System
Alarms
Packet Capture
App Scope
Summary
Change Monitor
Threat Monitor
Threat Map
Network Monitor
Traffic Map
Session Browser
Botnet
PDF Reports
Manage PDF Summary
User Activity Report
Report Groups
Email Scheduler
Manage Custom Reports
Reports
Top 100
Incoming threats
Outgoing threats
Filter
Last 6 hours
Last 12 hours
Last 24 hours
Last 7 days
Last 30 days
njzierfuss | Logout
Tasks
Language


PA-5050
137.229.3.8/#acc::vsys1
Reader
paloalto NETWORKS
Dashboard
ACC
Monitor
Policies
Objects
Network
Device
Commit
Time Last 24 Hrs
Sort By Sessions
Top 25
Help
Application Command Center
1 2 3 4 5
3.1
Threat Prevention
Threats
Weaknesses used to gain more access or control than intended.
Used to track activity or steal information.
Severity
Threat/Content Name
ID
Threat/Content Type
1 MEDIUM DNS ANY Queries Brute-force DOS Attack 40033 vulnerability 4.5 M
2 LOW Sipvicious.Gen User-Agent Traffic 13272 spyware 173.8 K
3 INFORMATIONAL NetBIOS nbtstat query 31707 vulnerability
4 INFORMATIONAL Microsoft RPC Endpoint Mapper 30845 vulnerability
5 INFORMATIONAL Microsoft RPC ISystemActivator bind 30846 vulnerability 46.9 K
6 INFORMATIONAL Service Enum Through SMB ServiceEnum2 30867 vulnerability 27.3 K
7 CRITICAL ZeroAccess.Gen Command and Control Traffic 13235 spyware 22.7 K
8 LOW Morto RDP Request Traffic 13274 spyware 20.2 K
9 HIGH SSH User Authentication Brute-force Attempt 40015 vulnerability 17.1 K
10 LOW Microsoft Windows WinReg Access Attempt 33865 vulnerability 15.6 K
11 HIGH MS-RDP Brute-force Attempt 40021 vulnerability 15.0 K
12 INFORMATIONAL Microsoft Windows SMB Fragmentation RPC Request Attempt 33033 vulnerability
13 HIGH SIP Register Message Brute-force Attack 40023 vulnerability
14 LOW Sipvicious.sundayddr User-Agent Traffic 13273 spyware 6.3 K
15 INFORMATIONAL Microsoft Windows user enumeration 30842 vulnerability 6.2 K
16 LOW Microsoft Windows Registry Read Attempt 34940 vulnerability 5.1 K
17 INFORMATIONAL Generic GET Method Buffer Overflow Vulnerability 34267 vulnerability 4.3 K
18 CRITICAL Microsoft SQL Server Stack Overflow Vulnerability 30009 vulnerability 3.6 K
19 INFORMATIONAL HTTP OPTIONS Method 30520 vulnerability 3.1 K
20 CRITICAL Win32.Conficker.C p2p 12544 spyware 3.1 K
21 INFORMATIONAL DNS Zone Transfer IXFR Attempt 35288 vulnerability 2.8 K
22 INFORMATIONAL DNS Zone Transfer IXFR Response 35289 vulnerability 2.5 K
23 LOW Microsoft Windows RPC Encrypted Data Detected 33836 vulnerability 2.1 K
24 INFORMATIONAL Microsoft Windows EventLog Service access 30863 vulnerability 1.8 K
25 HIGH Microsoft SQL Server User Authentication Brute-force Attempt 40010 vulnerability 1.5 K
njzierfuss | Logout
Tasks Language

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 soft**ware**, 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.