UNIVERSITY OF SAN FRANCISCO
CHANGE THE WORLD FROM HERE

# **Information Security at USF:** threats (attacks), vulnerabilities, countermeasures, risk

Nick Recchia, Ed.D
ITS – Security Services
October 22, 2013

# Overview

Presenters:

**Nick Recchia**
ITS Security Administrator

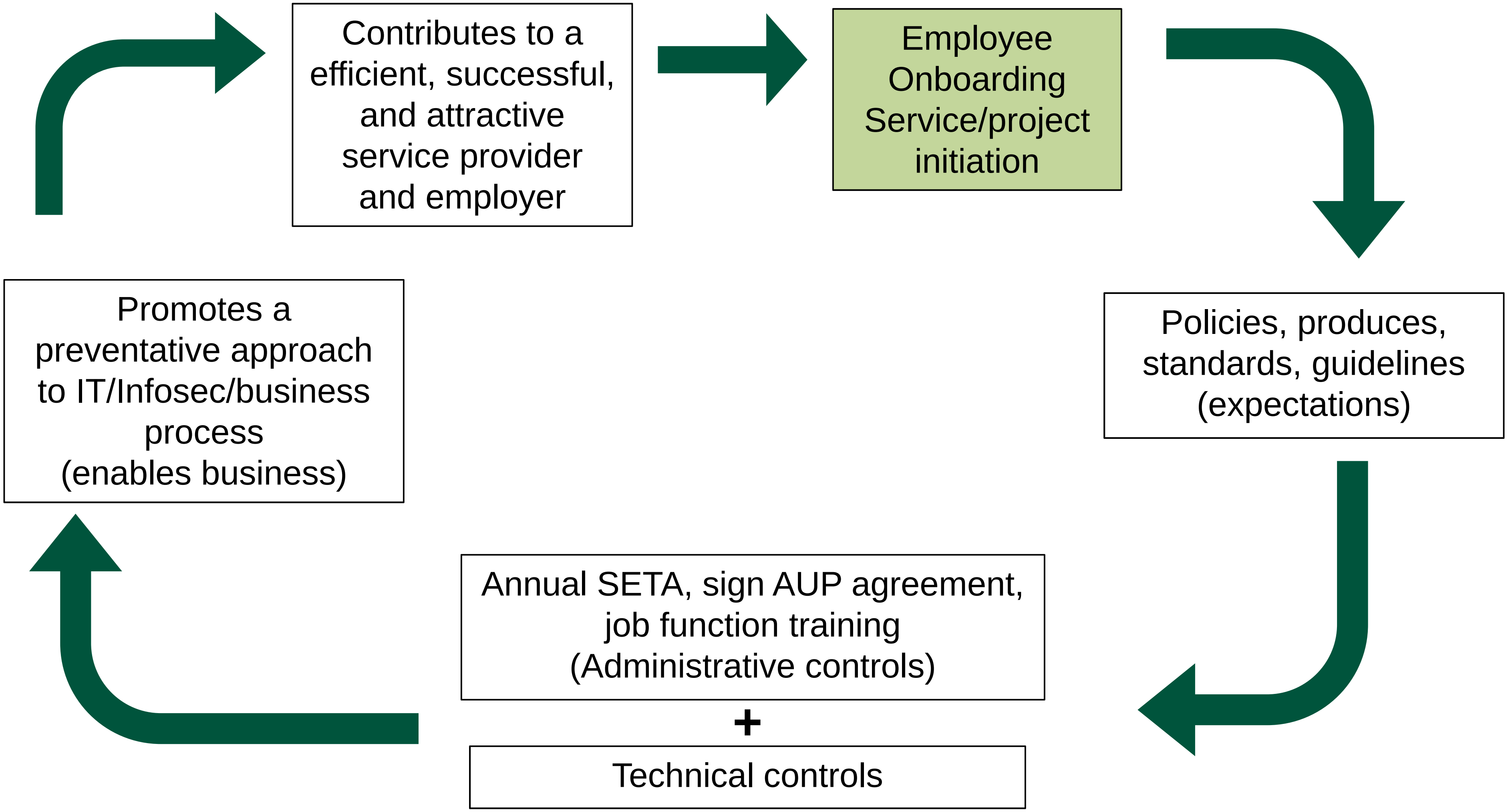
**Walter Petruska**
Information Security Officer &
Director, Security Services

## Overview

Agenda:

1. Introduction
2. Holistic approach to Information Security
3. Org structure and Information Security
4. Vulnerabilities & threats (attacks)
5. USF network: exploring countermeasures and preventing common threats (attacks)
6. Question/discussion

# Introduction



Employee Onboarding Service/project initiation

Policies, produces, standards, guidelines (expectations)

Annual SETA, sign AUP agreement, job function training (Administrative controls)

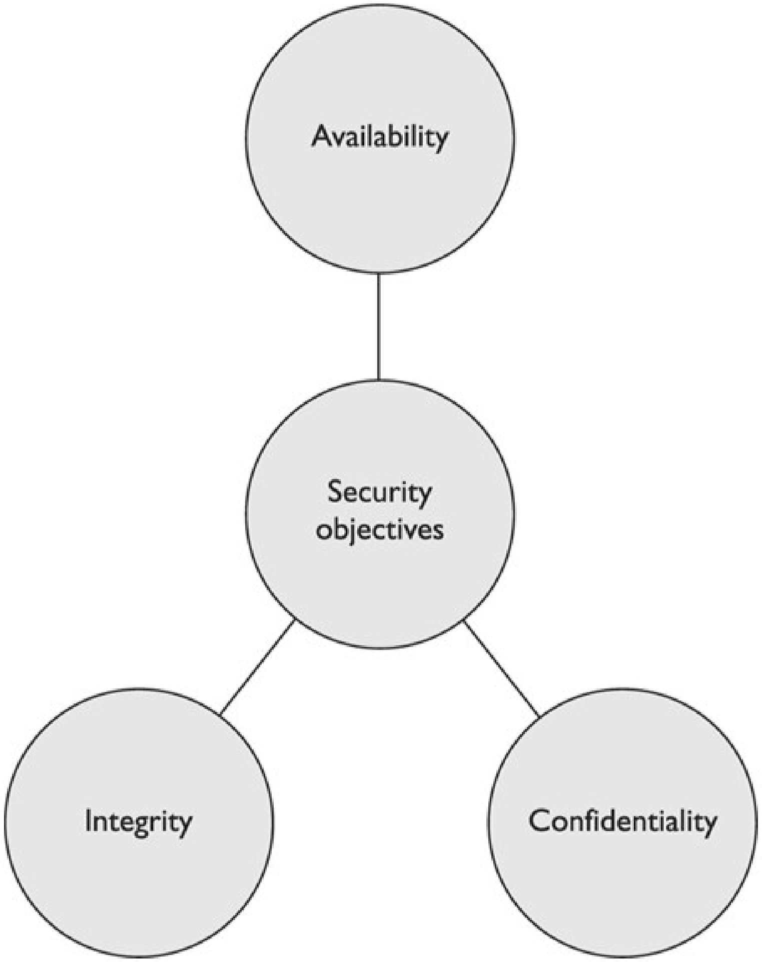
+

Technical controls

Promotes a preventative approach to IT/Infosec/business process (enables business)

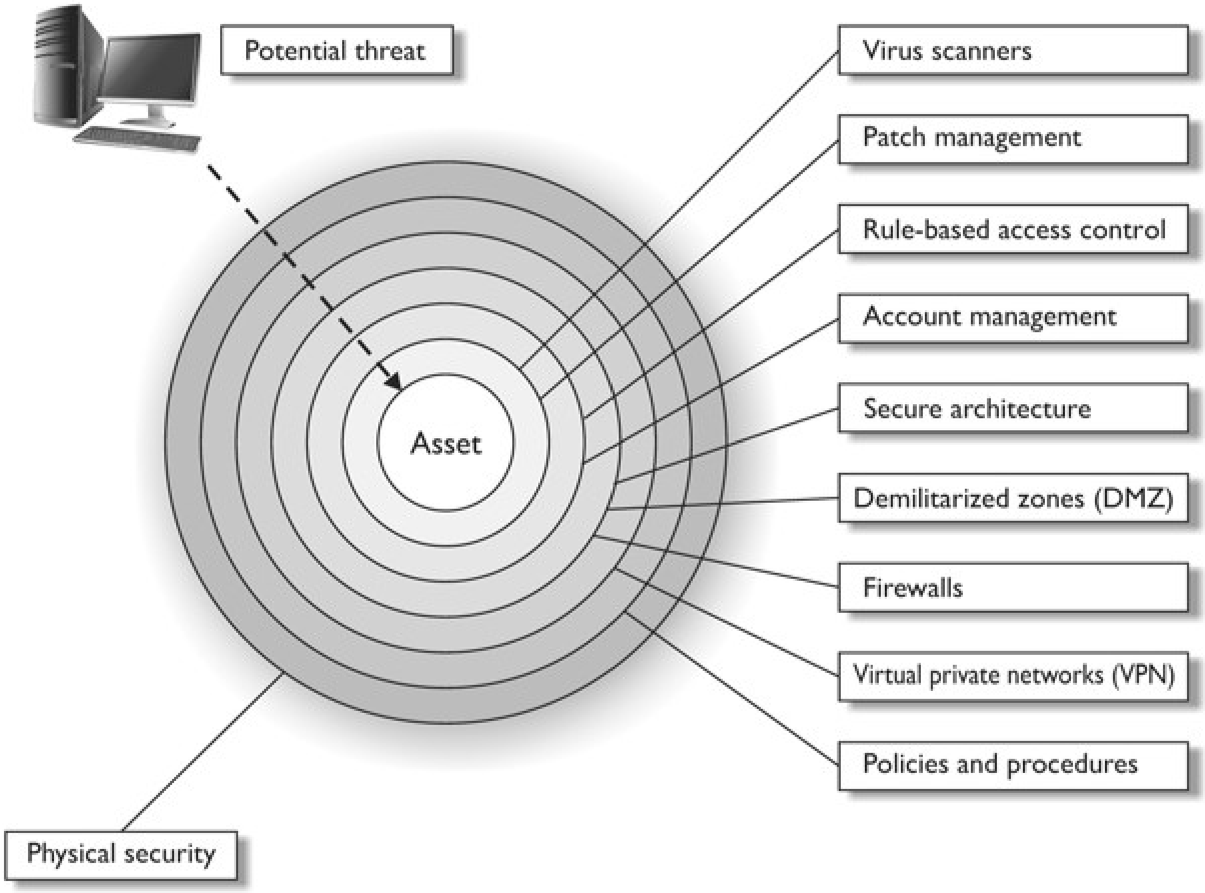
Contributes to a efficient, successful, and attractive service provider and employer

# Introduction



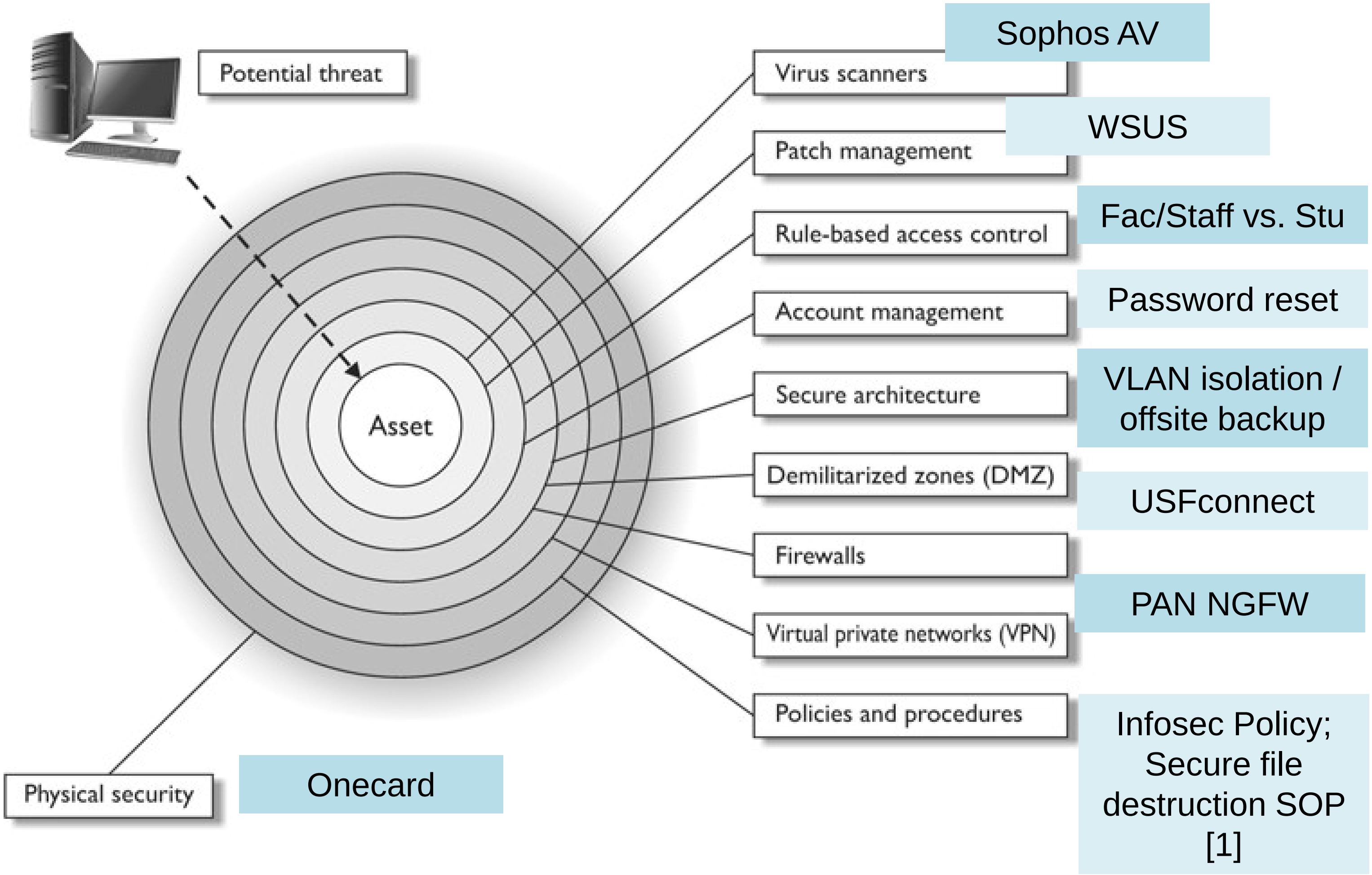
Reference: **CISSP All-in-One Exam Guide, 6th Edition, page 22**

# Holistic approach to Information Security



Reference: **CISSP All-in-One Exam Guide, 6th Edition, page 29**

# Holistic approach to Information Security



Sophos AV

WSUS

Fac/Staff vs. Stu

Password reset

VLAN isolation / offsite backup

USFconnect

PAN NGFW

Infosec Policy; Secure file destruction SOP [1]

Onecard

Reference: **CISSP All-in-One Exam Guide, 6th Edition, page 29**
[1] http://www.usfca.edu/its/about/policies/infosec/

# Holistic approach to Information Security

1. **Vulnerability:** weakness or lack of countermeasure

2. **Threat agent:** entity that can exploit a vulnerability

3. **Threat:** is the danger of a threat agent exploiting a vulnerability

1. **Risk:** the probability of a threat agent exploiting a vulnerability, and the associated impact

2. **Exposure:** presence of a vulnerability, which exposes the organization to a threat

3. **Safeguard:** control that is put into place to reduce a risk; also called a countermeasure

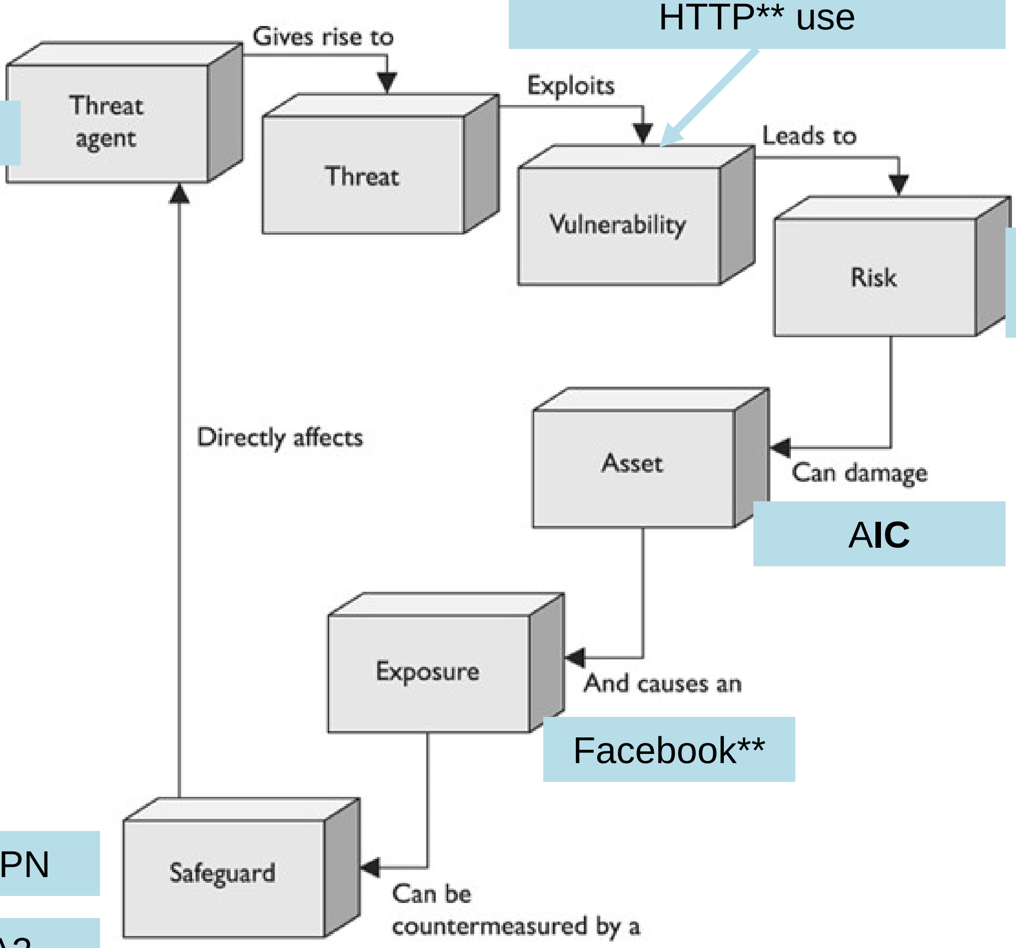
Reference: **CISSP All-in-One Exam Guide, 6th Edition, page 28**

# Holistic approach to Information Security

FireSheep

Unsecured wireless* and HTTP** use

Attacker



probability & what will result?

AIC

Facebook**

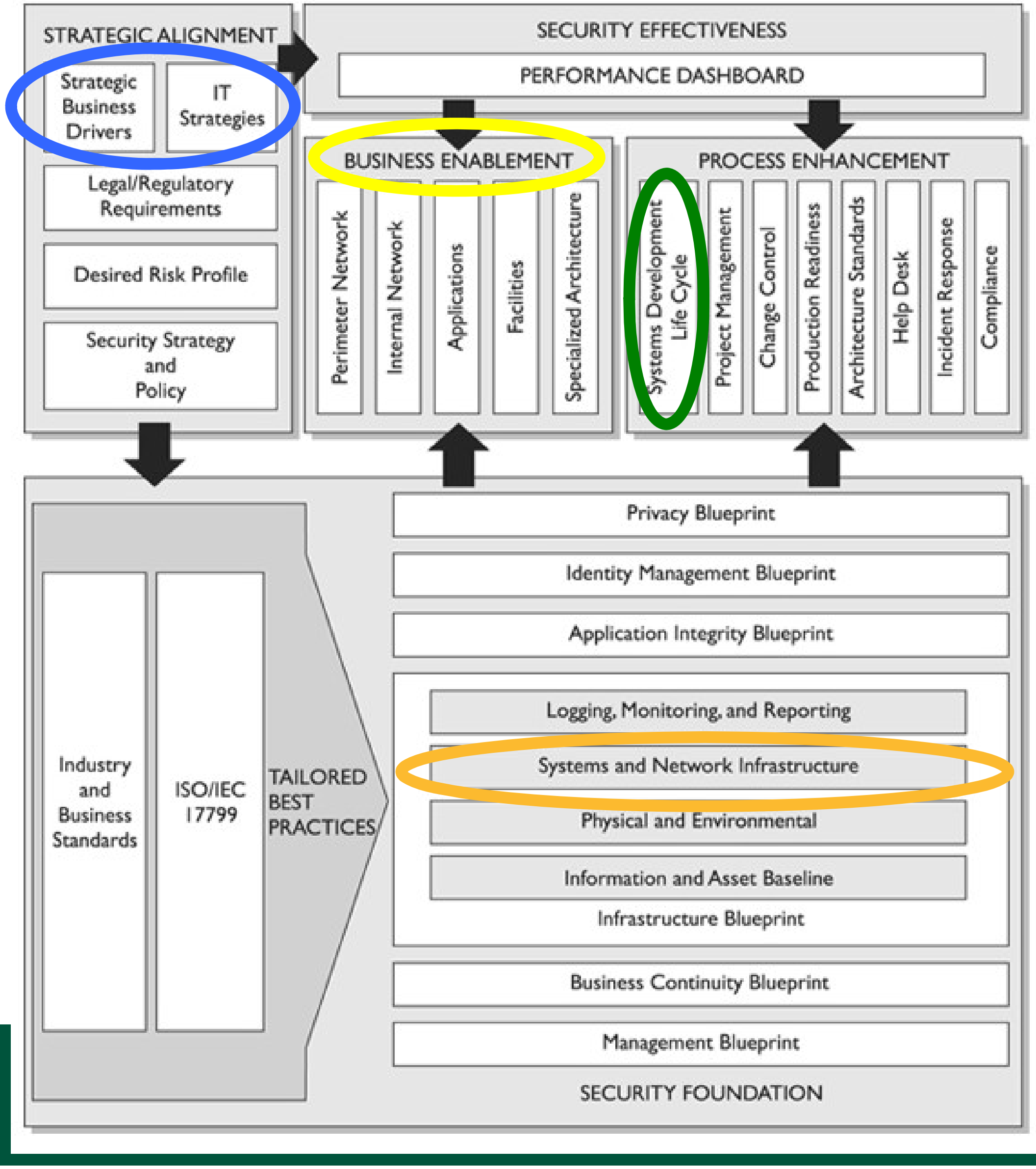
Use VPN

*WPA2

Reference: **CISSP All-in-One Exam Guide, 6th Edition, page 29**

# Holistic approach to Information Security

Reference: **CISSP All-in-One Exam Guide, 6th Edition, page 67**



# Org structure and risk

Top-down Approach

- security program should be implemented in a **top down approach**
- initiation, support, and direction come from top management: → middle management → staff members
- make sure the people actually responsible for protecting the company's assets (senior management) are driving the program.

Reference: **CISSP All-in-One Exam Guide, 6th Edition, page 63**

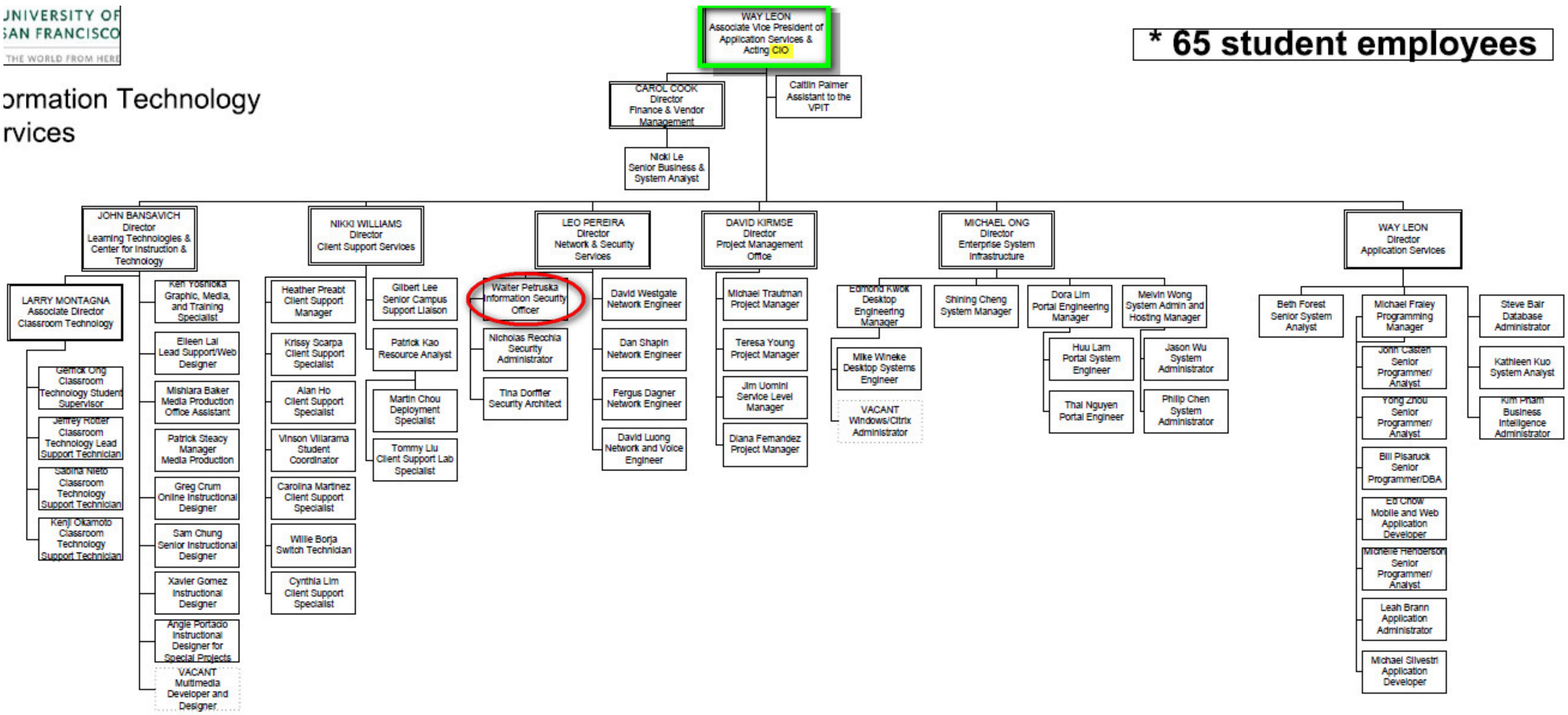
# Org structure and risk

Bottom-up Approach

- **bottom-up approach** refers to staff members (usually IT) try to develop a security program without getting proper management support and direction.
- bottom-up approach is commonly less effective, not broad enough to address all security risks, and doomed to fail.

Reference: **CISSP All-in-One Exam Guide, 6th Edition, page 63**

# USF ITS (Information Technology Services)



UNIVERSITY OF SAN FRANCISCO
THE WORLD FROM HERE

ormation Technology
rvices

* 65 student employees

WAY LEON
Associate Vice President of Application Services & Acting CIO

CAROL COOK
Director
Finance & Vendor Management

Caitlin Palmer
Assistant to the VPIT

Nicki Le
Senior Business & System Analyst

JOHN BANSAVICH
Director
Learning Technologies & Center for Instruction & Technology

LARRY MONTAGNA
Associate Director
Classroom Technology

Gerrick Ong
Classroom Technology Student Supervisor

Jeffrey Rotter
Classroom Technology Lead Support Technician

Sabina Nieto
Classroom Technology Support Technician

Kenji Okamoto
Classroom Technology Support Technician

Ken Yoshioka
Graphic, Media, and Training Specialist

Eileen Lai
Lead Support/Web Designer

Mishiara Baker
Media Production Office Assistant

Patrick Steacy
Manager
Media Production

Greg Crum
Online Instructional Designer

Sam Chung
Senior Instructional Designer

Xavier Gomez
Instructional Designer

Angie Portacio
Instructional Designer for Special Projects

VACANT
Multimedia Developer and Designer

NIKKI WILLIAMS
Director
Client Support Services

Heather Preabt
Client Support Manager

Krissy Scarpa
Client Support Specialist

Alan Ho
Client Support Specialist

Vinson Villarama
Student Coordinator

Carolina Martinez
Client Support Specialist

Willie Borja
Switch Technician

Cynthia Lim
Client Support Specialist

Gilbert Lee
Senior Campus Support Liaison

Patrick Kao
Resource Analyst

Martin Chou
Deployment Specialist

Tommy Liu
Client Support Lab Specialist

LEO PEREIRA
Director
Network & Security Services

Walter Petruska
Information Security Officer

Nicholas Recchia
Security Administrator

Tina Dorffler
Security Architect

David Westgate
Network Engineer

Dan Shapin
Network Engineer

Fergus Dagner
Network Engineer

David Luong
Network and Voice Engineer

DAVID KIRMSE
Director
Project Management Office

Michael Trautman
Project Manager

Teresa Young
Project Manager

Jim Uomini
Service Level Manager

Diana Fernandez
Project Manager

MICHAEL ONG
Director
Enterprise System Infrastructure

Edmond Kwok
Desktop Engineering Manager

Mike Wineke
Desktop Systems Engineer

VACANT
Windows/Citrix Administrator

Shining Cheng
System Manager

Dora Lim
Portal Engineering Manager

Huu Lam
Portal System Engineer

Thai Nguyen
Portal Engineer

Melvin Wong
System Admin and Hosting Manager

Jason Wu
System Administrator

Philip Chen
System Administrator

WAY LEON
Director
Application Services

Beth Forest
Senior System Analyst

Michael Fraley
Programming Manager

John Casten
Senior Programmer/ Analyst

Yong Zhou
Senior Programmer/ Analyst

Bill Pisaruck
Senior Programmer/DBA

Ed Chow
Mobile and Web Application Developer

Michelle Henderson
Senior Programmer/ Analyst

Leah Brann
Application Administrator

Michael Silvestri
Application Developer

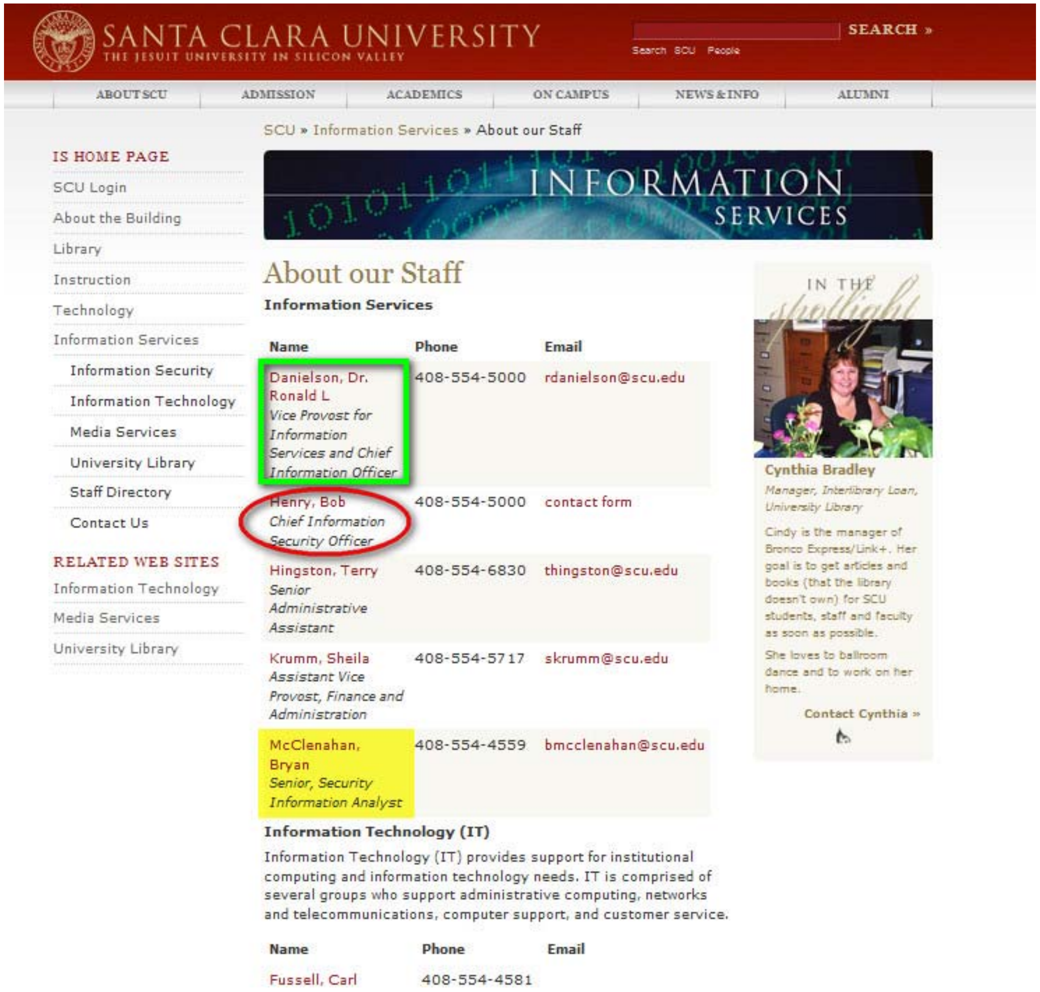
Steve Bair
Database Administrator

Kathleen Kuo
System Analyst

Kim Pham
Business Intelligence Administrator

Reference: http://www.usfca.edu/its/about/staff/

# SCU IS (Information Services)



## About our Staff

**Information Services**

| Name | Phone | Email |
|---|---|---|
| Danielson, Dr. Ronald L<br>*Vice Provost for Information Services and Chief Information Officer* | 408-554-5000 | rdanielson@scu.edu |
| Henry, Bob<br>*Chief Information Security Officer* | 408-554-5000 | contact form |
| Hingston, Terry<br>*Senior Administrative Assistant* | 408-554-6830 | thingston@scu.edu |
| Krumm, Sheila<br>*Assistant Vice Provost, Finance and Administration* | 408-554-5717 | skrumm@scu.edu |
| McClenahan, Bryan<br>*Senior, Security Information Analyst* | 408-554-4559 | bmcclenahan@scu.edu |

**Information Technology (IT)**

Information Technology (IT) provides support for institutional computing and information technology needs. IT is comprised of several groups who support administrative computing, networks and telecommunications, computer support, and customer service.

| Name | Phone | Email |
|---|---|---|
| Fussell, Carl | 408-554-4581 | |

**Cynthia Bradley**

*Manager, Interlibrary Loan, University Library*

Cindy is the manager of Bronco Express/Link+. Her goal is to get articles and books (that the library doesn't own) for SCU students, staff and faculty as soon as possible.

She loves to ballroom dance and to work on her home.

Contact Cynthia »

Reference: http://www.scu.edu/is/about/

# SCU IS (Information Services)

**Santa Clara University: Hacker changed grades of 60 students**

By Sean Webby and Lisa Fernandez Mercury NewsPosted: 11/14/2011

Santa Clara University's academic records database was recently hacked to improve the grades of more than 60 former and current undergraduate students, the university announced Monday.
The university called in the FBI, which is assisting in the ongoing investigation, according to university officials. No arrests have been reported.

"We are taking it quite seriously," said Dennis Jacobs, Santa Clara's provost and vice president for academic affairs. **"We are reviewing and enhancing all security measures to reduce the likelihood of any intrusion in the future.“**

The FBI, in a written statement issued Monday, confirmed it is involved in the investigation.
SCU officials said they were unaware of any other hacking incidents at the university. This one was particularly sophisticated, they said, and was only discovered when a former student came forward in August because she noticed a grade on her transcript was better than the one on a previously printed transcript.

Reference:
http://nakedsecurity.sophos.com/2011/11/16/fbi-investigates-santa-clara-university-hack-draft/
http://www.mercurynews.com/breaking-news/ci_19334460

# **SANS Institute** (System Administration, Networking, and Security Institute)

**Organizational Information Security from Scratch -** *A Guarantee for Doing It Right*

The foundation for establishing the necessary protections and demonstrating the required diligence towards protecting your organization's proprietary information can be found in a security infrastructure that has been around in one form or another since the early 1990's. It provides a means to combine the technical protections (network firewalls, intrusion detection systems, traffic analyzers, etc.) with business processes (risk & vulnerability testing, information security policies and procedures, etc.) into an overall...

Reference: http://www.sans.org/reading-room/whitepapers/standards/organizational-information-security-scratch-guarantee-541?show=organizational-information-security-scratch-guarantee-541&cat=standards

# Executive Management

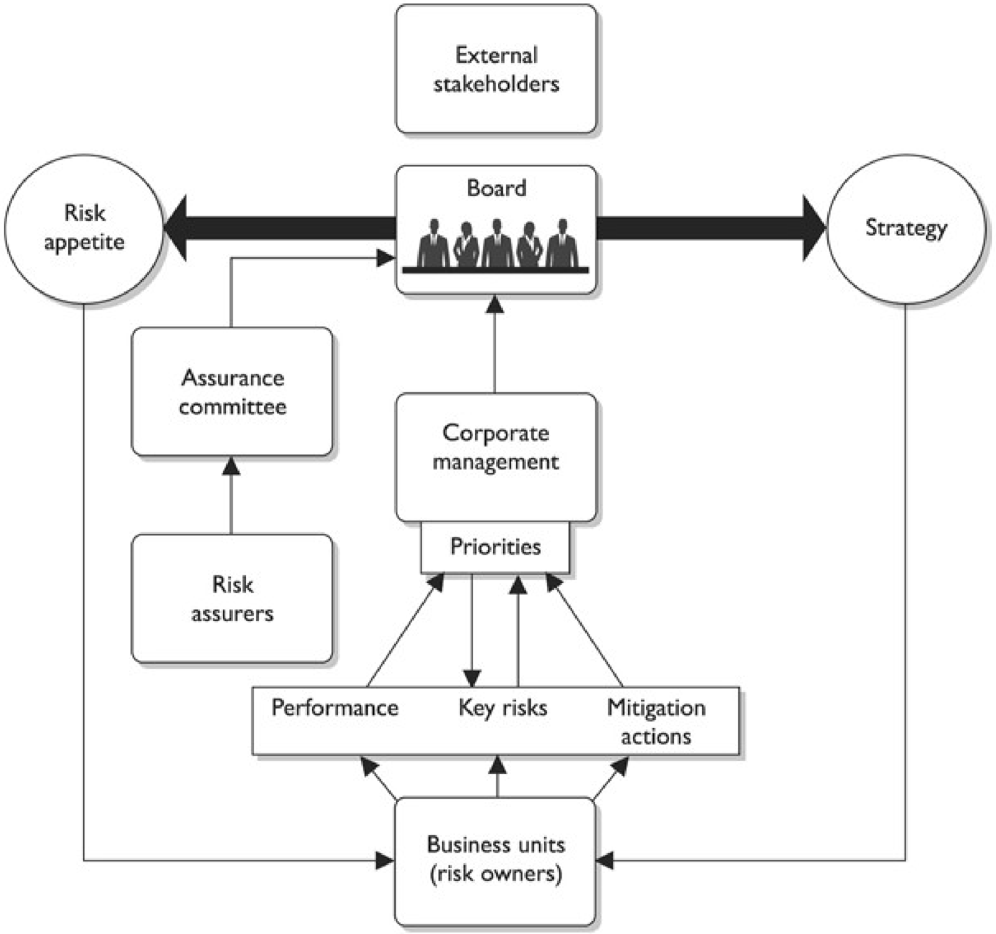


**Figure 2-14** Risk must be understood at different departments and levels.

Reference: **CISSP All-in-One Exam Guide, 6th Edition, page 117**

# CCSF Breach 2012; Accreditation loss 2014?

Line of computers in the computer room at City College of San Francisco in Batmale Hall in San Francisco, Calif., on Thursday, January 12, 2012. A computer virus which has been on the San Francisco City College servers for the past 10 years may have had the personal information of 40k to 100k students and faculty compromised. Photo: Liz Hafalia, The Chronicle

Reference:
http://www.sfgate.com/education/article/Viruses-stole-City-College-of-S-F-data-for-years-2502338.php

http://www.sfexaminer.com/sanfrancisco/city-college-of-san-francisco-loses-accreditation-faces-closure/Content?oid=2496026

# The 8 Most Common Causes of Data Breaches

## (May 2013)

1) Weak and Stolen Credentials, a.k.a. Passwords
2) Back Doors, Application Vulnerabilities
3) Malware
4) Social Engineering
5) Too Many Permissions
6) Insider Threats
7) Physical Attacks
8) Improper Configuration, User Error

Reference:
www.darkreading.com/attacks-breaches
http://www.verizonenterprise.com/DBIR/2013/

# The 2013 Data Breach Investigations Report

"…some organizations will be a target *regardless* of what they do, but most become a target *because* of what they do (or don't do)." DBIR p.48

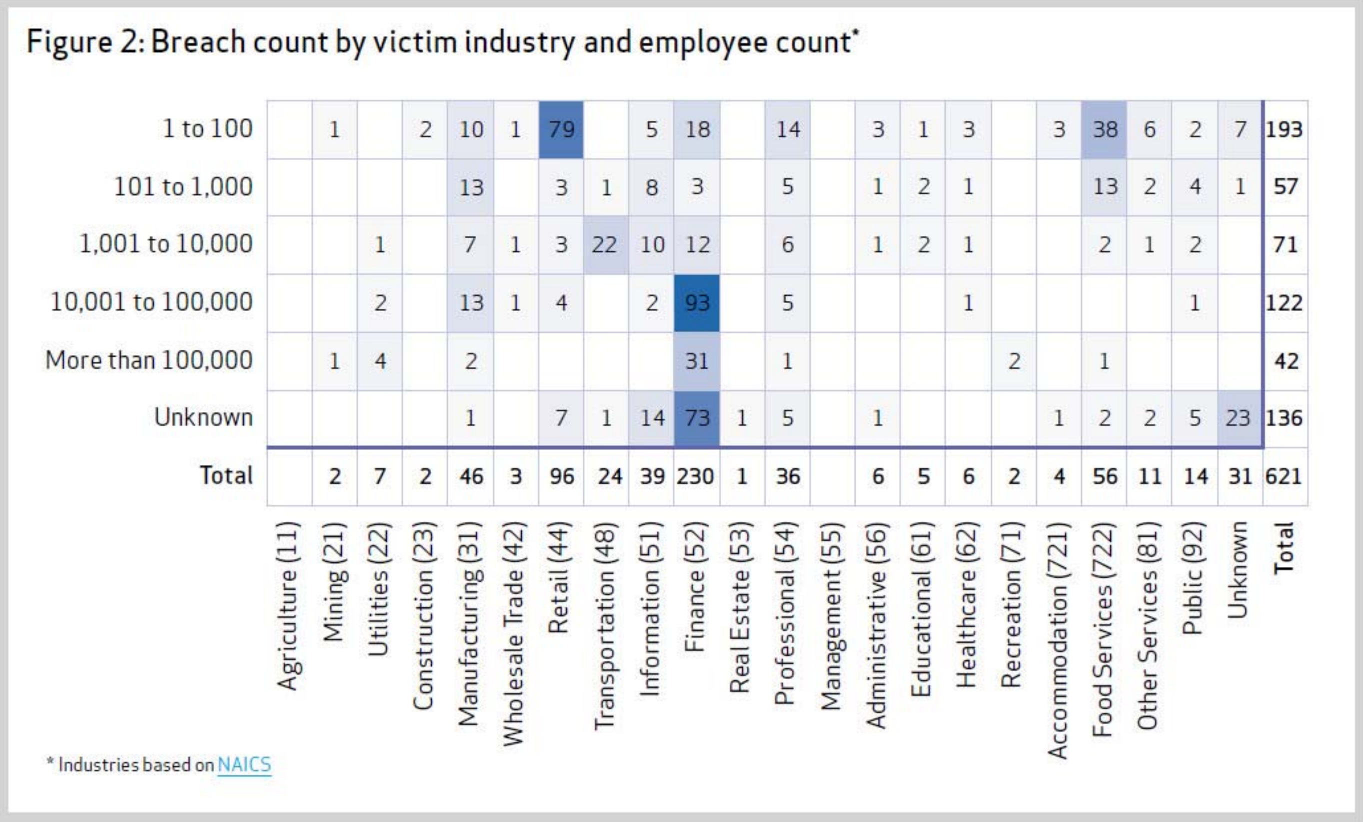


Figure 2: Breach count by victim industry and employee count*

| | Agriculture (11) | Mining (21) | Utilities (22) | Construction (23) | Manufacturing (31) | Wholesale Trade (42) | Retail (44) | Transportation (48) | Information (51) | Finance (52) | Real Estate (53) | Professional (54) | Management (55) | Administrative (56) | Educational (61) | Healthcare (62) | Recreation (71) | Accommodation (721) | Food Services (722) | Other Services (81) | Public (92) | Unknown | Total |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 to 100 | | 1 | | 2 | 10 | 1 | 79 | | 5 | 18 | | 14 | | 3 | 1 | 3 | | 3 | 38 | 6 | 2 | 7 | 193 |
| 101 to 1,000 | | | | | 13 | | 3 | 1 | 8 | 3 | | 5 | | 1 | 2 | 1 | | | 13 | 2 | 4 | 1 | 57 |
| 1,001 to 10,000 | | | 1 | | 7 | 1 | 3 | 22 | 10 | 12 | | 6 | | 1 | 2 | 1 | | | 2 | 1 | 2 | | 71 |
| 10,001 to 100,000 | | | 2 | | 13 | 1 | 4 | | 2 | 93 | | 5 | | | | 1 | | | | | 1 | | 122 |
| More than 100,000 | | 1 | 4 | | 2 | | | | | 31 | | 1 | | | | | 2 | | 1 | | | | 42 |
| Unknown | | | | | 1 | | 7 | 1 | 14 | 73 | 1 | 5 | | 1 | | | | 1 | 2 | 2 | 5 | 23 | 136 |
| Total | | 2 | 7 | 2 | 46 | 3 | 96 | 24 | 39 | 230 | 1 | 36 | | 6 | 5 | 6 | 2 | 4 | 56 | 11 | 14 | 31 | 621 |

* Industries based on NAICS

Reference:
http://www.verizonenterprise.com/DBIR/2013/ ;p.13 & 48

# The 2013 Data Breach Investigations Report

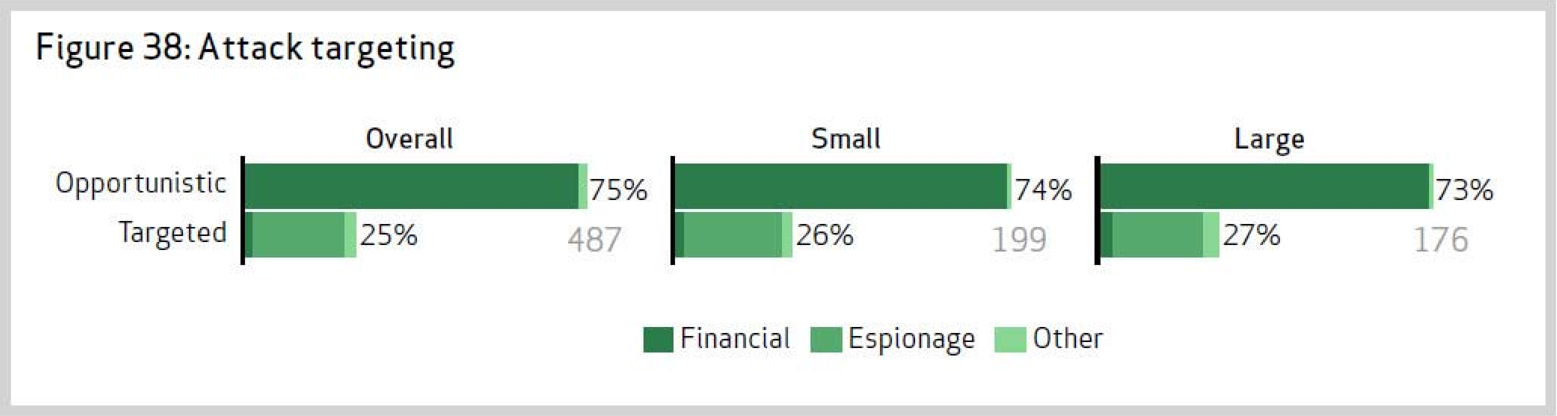


Figure 38: Attack targeting

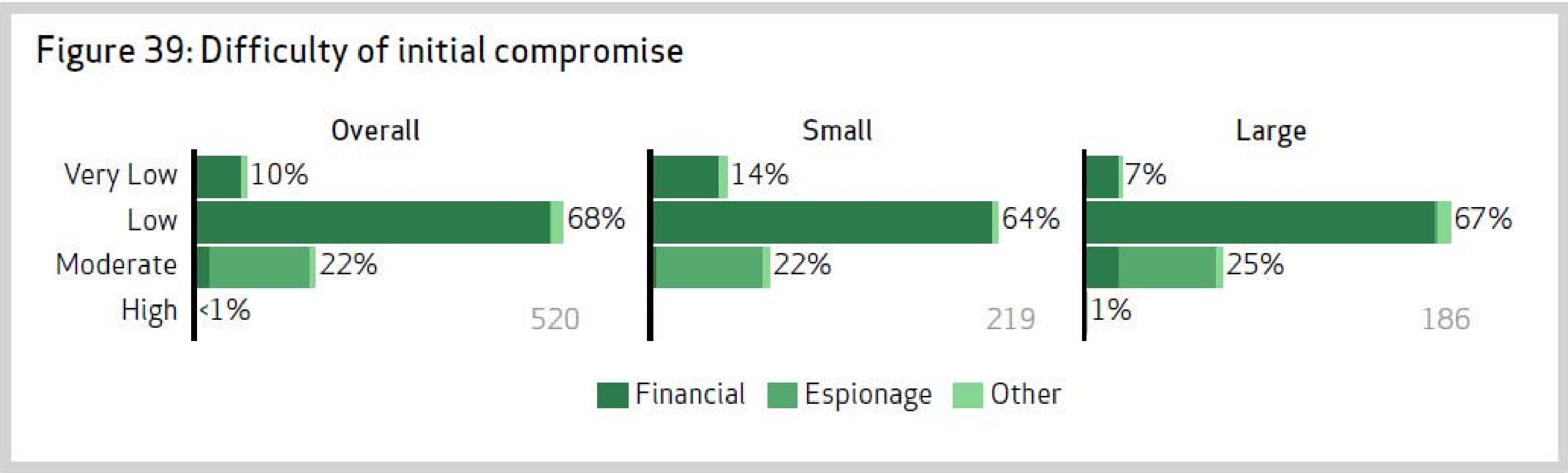
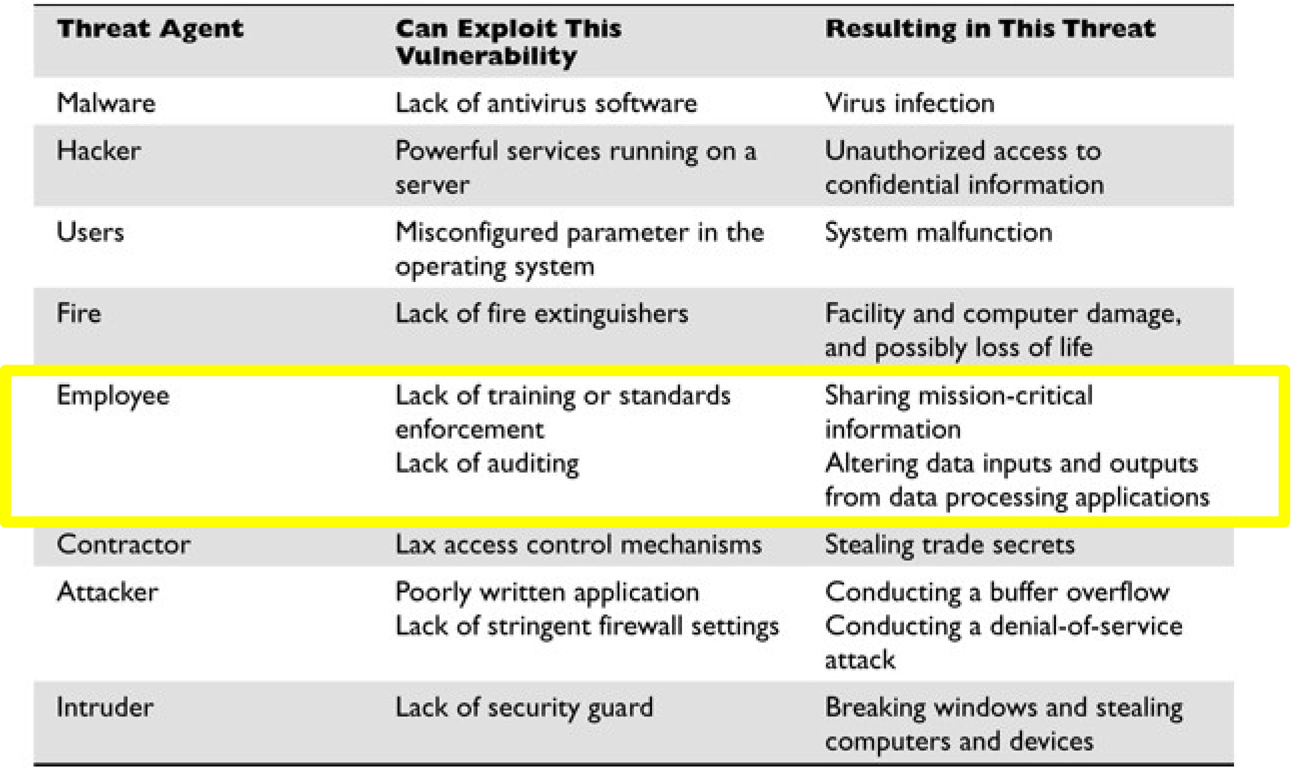


Figure 39: Difficulty of initial compromise

Reference:
http://www.verizonenterprise.com/DBIR/2013/ ;p.48 & 49

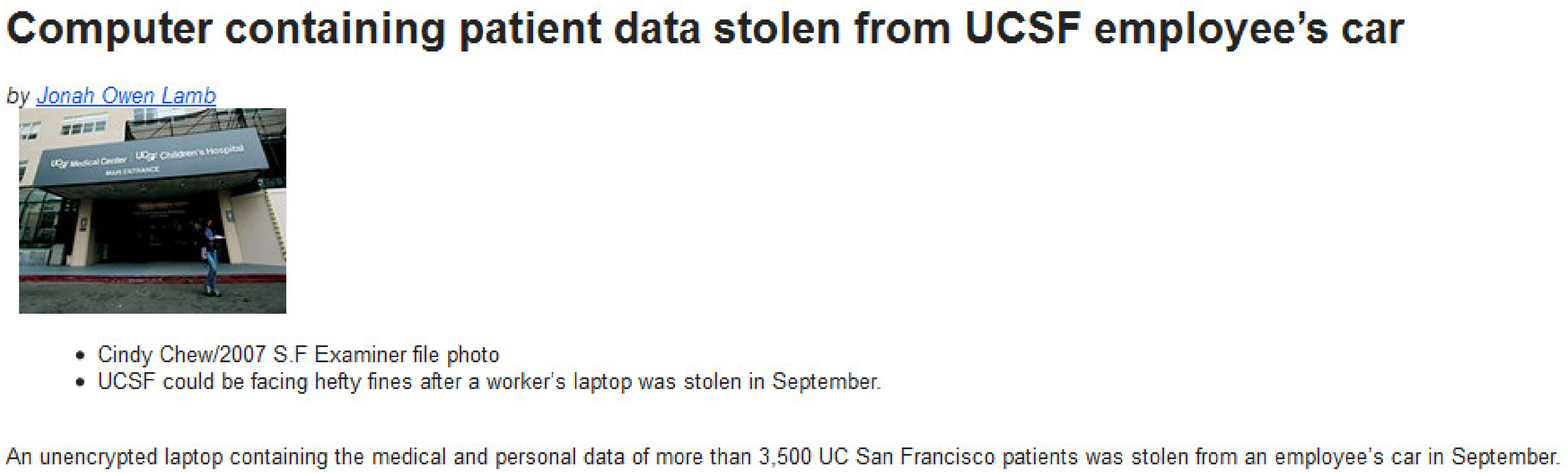
# Threat Agents



| Threat Agent | Can Exploit This Vulnerability | Resulting in This Threat |
|---|---|---|
| Malware | Lack of antivirus software | Virus infection |
| Hacker | Powerful services running on a server | Unauthorized access to confidential information |
| Users | Misconfigured parameter in the operating system | System malfunction |
| Fire | Lack of fire extinguishers | Facility and computer damage, and possibly loss of life |
| Employee | Lack of training or standards enforcement<br>Lack of auditing | Sharing mission-critical information<br>Altering data inputs and outputs from data processing applications |
| Contractor | Lax access control mechanisms | Stealing trade secrets |
| Attacker | Poorly written application<br>Lack of stringent firewall settings | Conducting a buffer overflow<br>Conducting a denial-of-service attack |
| Intruder | Lack of security guard | Breaking windows and stealing computers and devices |

Reference: **CISSP All-in-One Exam Guide, 6th Edition, page 78**

# **Threat Agent -** employee



## Computer containing patient data stolen from UCSF employee's car

*by* *Jonah Owen Lamb*

- Cindy Chew/2007 S.F Examiner file photo
- UCSF could be facing hefty fines after a worker's laptop was stolen in September.

An unencrypted laptop containing the medical and personal data of more than 3,500 UC San Francisco patients was stolen from an employee's car in September.

Date of occurrence: 09/2013

Reference: **http://www.sfexaminer.com/sanfrancisco/computer-containing-patient-data-stolen-from-ucsf-employees-car/Content?oid=2599830**

UNIVERSITY OF SAN FRANCISCO

# USF ITS Related

## **Vulnerabilities** > Threats

1. **BYOD (ResHalls)** > malware can spread
2. **File Sharing** > malware can spread
3. **Admin Account Access** > computer compromise
4. **Immature Patch Management practices** > Unpatched machine > Vulnerable to attacks
5. **Lack of required SETA** > user error / social engineering

# USF ITS Related Countermeasures

1. Palo Alto Networks NGFW
2. Network Access Control
3. Sophos Antivirus Security and Control
4. QualysGuard Vulnerability Management
5. Center for Information Security (Sec. benchmarks)
6. Security Education Training Awareness (SETA)

# 1) Palo Alto Networks NGFW

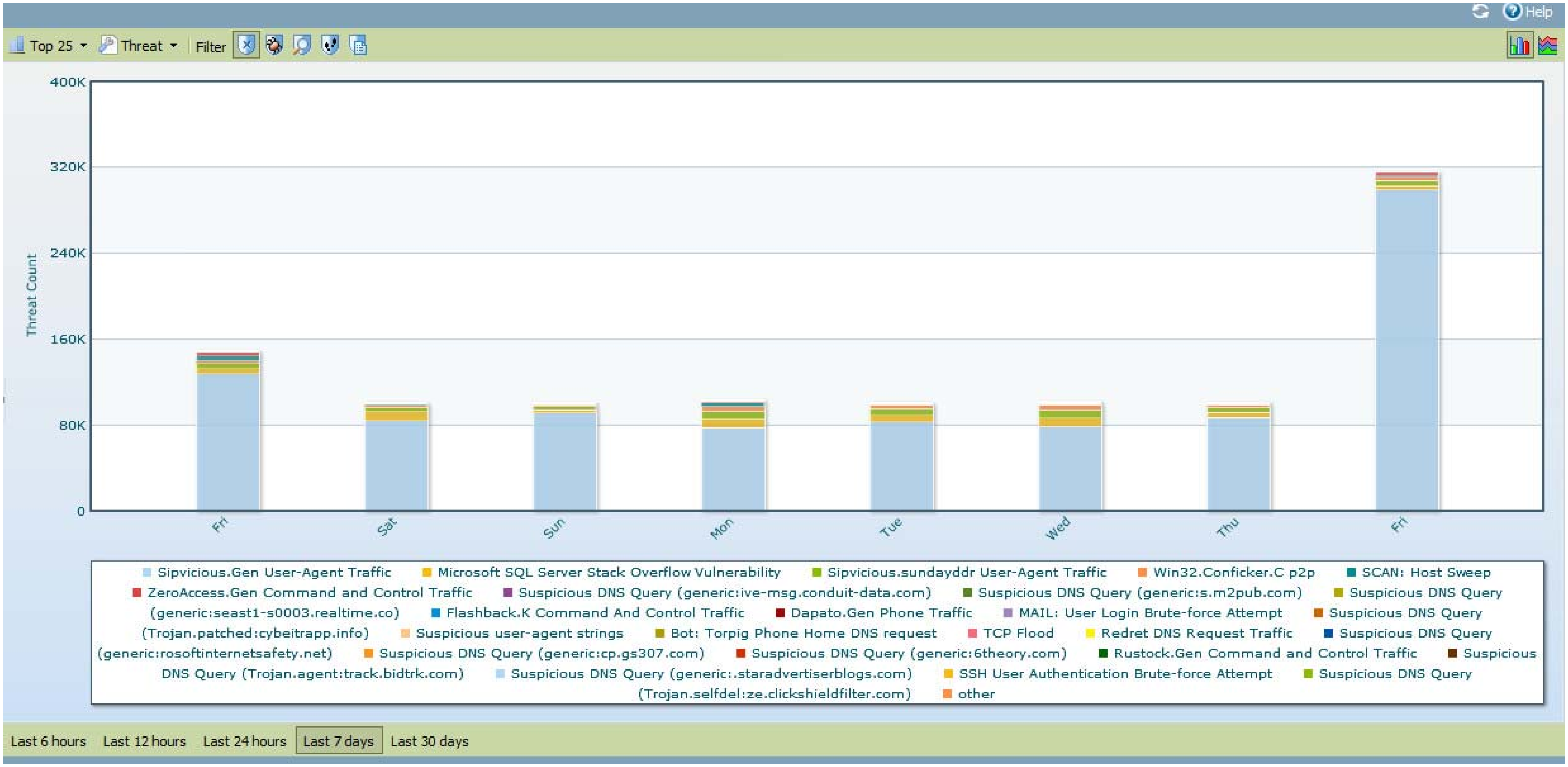
## Firewall Overview:

The Palo Alto Networks firewall allows you to specify security policies based on accurate identification of each application seeking access to your network.

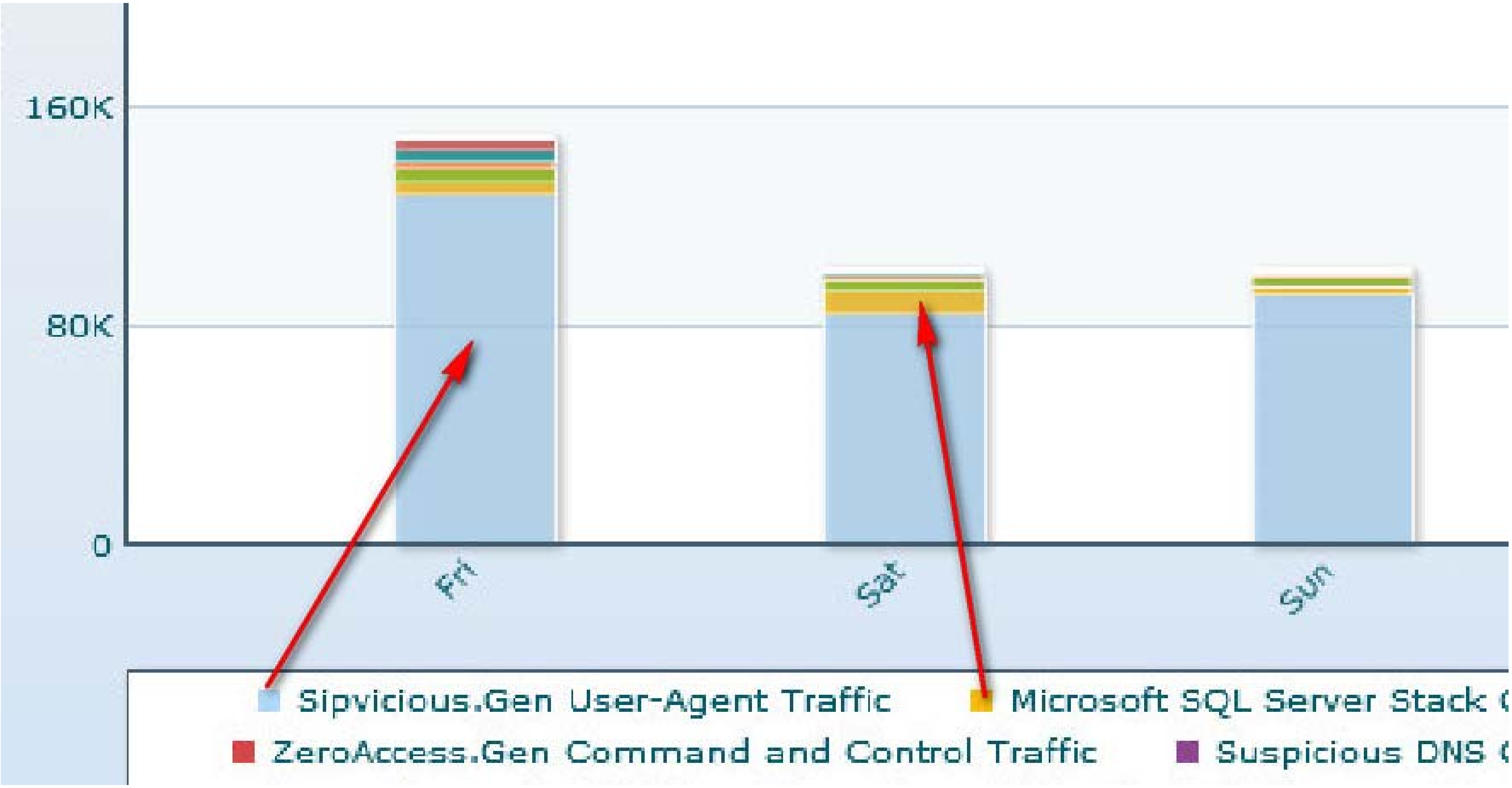
***Unlike traditional*** *firewalls that identify applications only by protocol and port number,* ***this firewall uses packet inspection and a library of application signatures to distinguish between applications that have the same protocol and port, and to identify potentially malicious applications that use non-standard ports.***

For example, you can define security policies for specific applications, rather than rely on a single policy for all port 80 connections. For each identified application, you can specify a security policy to block or allow traffic based on the source and destination zones and addresses (IPv4 and IPv6). Each security policy can also specify security profiles to protect against viruses, spyware, and other threats.

# **PA NGFW top 25 Threats:** 9/27/13 to 10/04/13

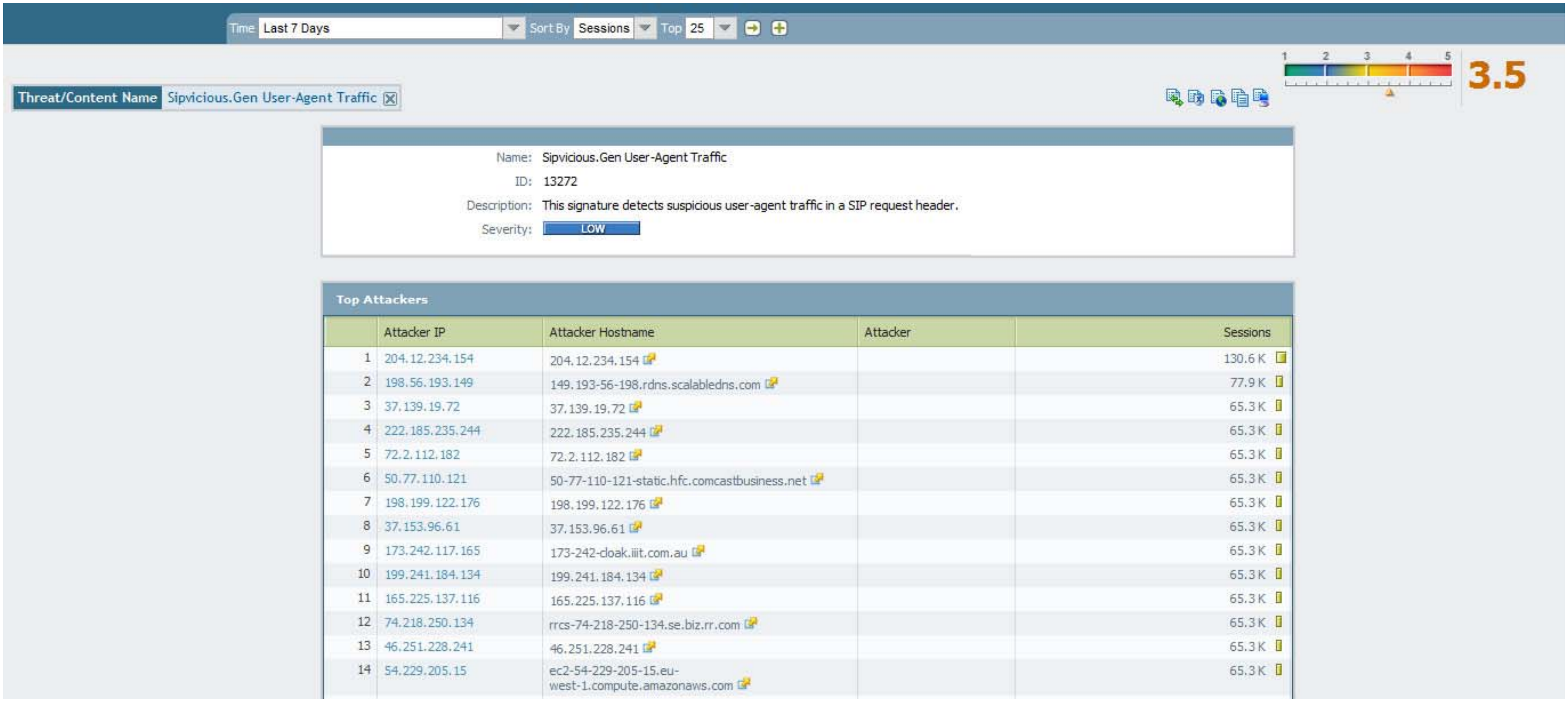

Help
Top 25
Threat
Filter
Threat Count
400K
320K
240K
160K
80K
0
Fri
Sat
Sun
Mon
Tue
Wed
Thu
Fri
Sipvicious.Gen User-Agent Traffic
Microsoft SQL Server Stack Overflow Vulnerability
Sipvicious.sundayddr User-Agent Traffic
Win32.Conficker.C p2p
SCAN: Host Sweep
ZeroAccess.Gen Command and Control Traffic
Suspicious DNS Query (generic:ive-msg.conduit-data.com)
Suspicious DNS Query (generic:s.m2pub.com)
Suspicious DNS Query (generic:seast1-s0003.realtime.co)
Flashback.K Command And Control Traffic
Dapato.Gen Phone Traffic
MAIL: User Login Brute-force Attempt
Suspicious DNS Query (Trojan.patched:cybeitrapp.info)
Suspicious user-agent strings
Bot: Torpig Phone Home DNS request
TCP Flood
Redret DNS Request Traffic
Suspicious DNS Query (generic:rosoftinternetsafety.net)
Suspicious DNS Query (generic:cp.gs307.com)
Suspicious DNS Query (generic:6theory.com)
Rustock.Gen Command and Control Traffic
Suspicious DNS Query (Trojan.agent:track.bidtrk.com)
Suspicious DNS Query (generic:.staradvertiserblogs.com)
SSH User Authentication Brute-force Attempt
Suspicious DNS Query (Trojan.selfdel:ze.clickshieldfilter.com)
other
Last 6 hours
Last 12 hours
Last 24 hours
Last 7 days
Last 30 days

# **PA NGFW top 25 Threats (zoom):** 9/27/13 to 10/04/13



UNIVERSITY OF SAN FRANCISCO

# **PA NGFW Top Threats #1:** Sipvicious.Gen User-Agent Traffic



Threat/Content Name Sipvicious.Gen User-Agent Traffic ☒

Name: Sipvicious.Gen User-Agent Traffic

ID: 13272

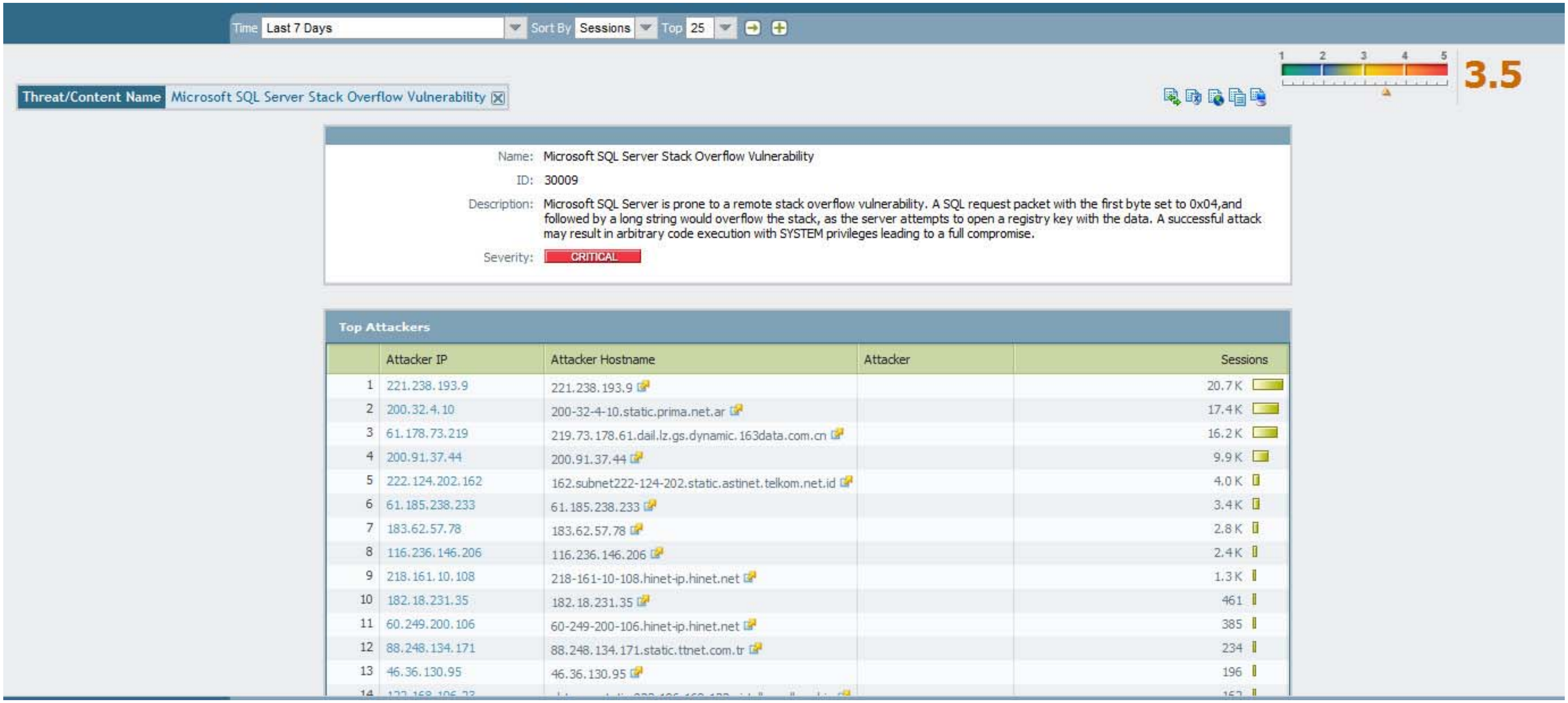
Description: This signature detects suspicious user-agent traffic in a SIP request header.

Severity: LOW

**Top Attackers**

| | Attacker IP | Attacker Hostname | Attacker | Sessions |
|---|---|---|---|---|
| 1 | 204.12.234.154 | 204.12.234.154 | | 130.6 K |
| 2 | 198.56.193.149 | 149.193-56-198.rdns.scalabledns.com | | 77.9 K |
| 3 | 37.139.19.72 | 37.139.19.72 | | 65.3 K |
| 4 | 222.185.235.244 | 222.185.235.244 | | 65.3 K |
| 5 | 72.2.112.182 | 72.2.112.182 | | 65.3 K |
| 6 | 50.77.110.121 | 50-77-110-121-static.hfc.comcastbusiness.net | | 65.3 K |
| 7 | 198.199.122.176 | 198.199.122.176 | | 65.3 K |
| 8 | 37.153.96.61 | 37.153.96.61 | | 65.3 K |
| 9 | 173.242.117.165 | 173-242-cloak.iiit.com.au | | 65.3 K |
| 10 | 199.241.184.134 | 199.241.184.134 | | 65.3 K |
| 11 | 165.225.137.116 | 165.225.137.116 | | 65.3 K |
| 12 | 74.218.250.134 | rrcs-74-218-250-134.se.biz.rr.com | | 65.3 K |
| 13 | 46.251.228.241 | 46.251.228.241 | | 65.3 K |
| 14 | 54.229.205.15 | ec2-54-229-205-15.eu-west-1.compute.amazonaws.com | | 65.3 K |

# **PA NGFW Top Threats #2:** Microsoft SQL Server Stack Overflow Vulnerability



Threat/Content Name: Microsoft SQL Server Stack Overflow Vulnerability

Name: Microsoft SQL Server Stack Overflow Vulnerability

ID: 30009

Description: Microsoft SQL Server is prone to a remote stack overflow vulnerability. A SQL request packet with the first byte set to 0x04,and followed by a long string would overflow the stack, as the server attempts to open a registry key with the data. A successful attack may result in arbitrary code execution with SYSTEM privileges leading to a full compromise.

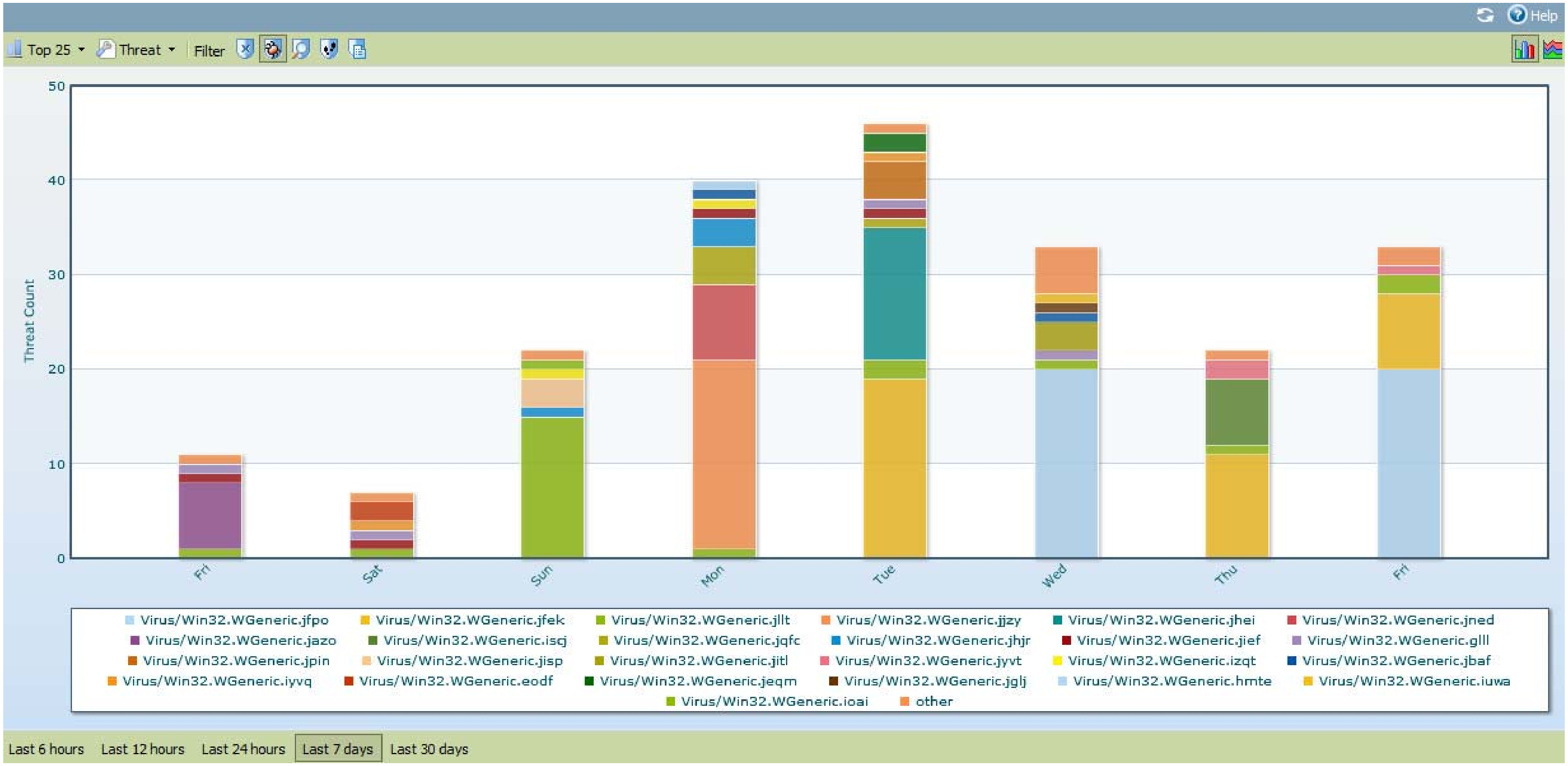
Severity: CRITICAL

**Top Attackers**

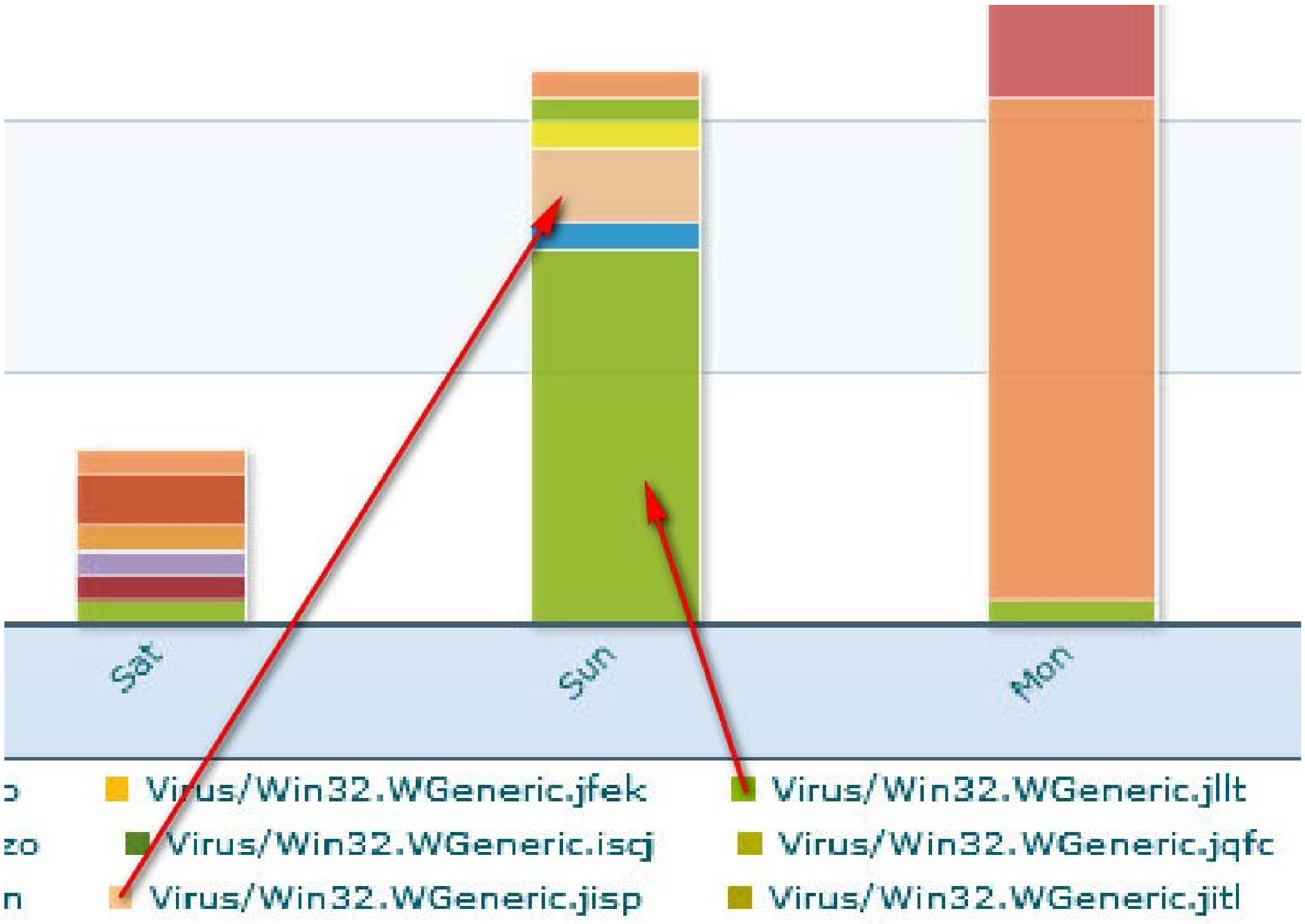
| | Attacker IP | Attacker Hostname | Attacker | Sessions |
|---|---|---|---|---|
| 1 | 221.238.193.9 | 221.238.193.9 | | 20.7 K |
| 2 | 200.32.4.10 | 200-32-4-10.static.prima.net.ar | | 17.4 K |
| 3 | 61.178.73.219 | 219.73.178.61.dail.lz.gs.dynamic.163data.com.cn | | 16.2 K |
| 4 | 200.91.37.44 | 200.91.37.44 | | 9.9 K |
| 5 | 222.124.202.162 | 162.subnet222-124-202.static.astinet.telkom.net.id | | 4.0 K |
| 6 | 61.185.238.233 | 61.185.238.233 | | 3.4 K |
| 7 | 183.62.57.78 | 183.62.57.78 | | 2.8 K |
| 8 | 116.236.146.206 | 116.236.146.206 | | 2.4 K |
| 9 | 218.161.10.108 | 218-161-10-108.hinet-ip.hinet.net | | 1.3 K |
| 10 | 182.18.231.35 | 182.18.231.35 | | 461 |
| 11 | 60.249.200.106 | 60-249-200-106.hinet-ip.hinet.net | | 385 |
| 12 | 88.248.134.171 | 88.248.134.171.static.ttnet.com.tr | | 234 |
| 13 | 46.36.130.95 | 46.36.130.95 | | 196 |
| 14 | 122.168.106.23 | [illegible] | | [illegible] |

UNIVERSITY OF SAN FRANCISCO

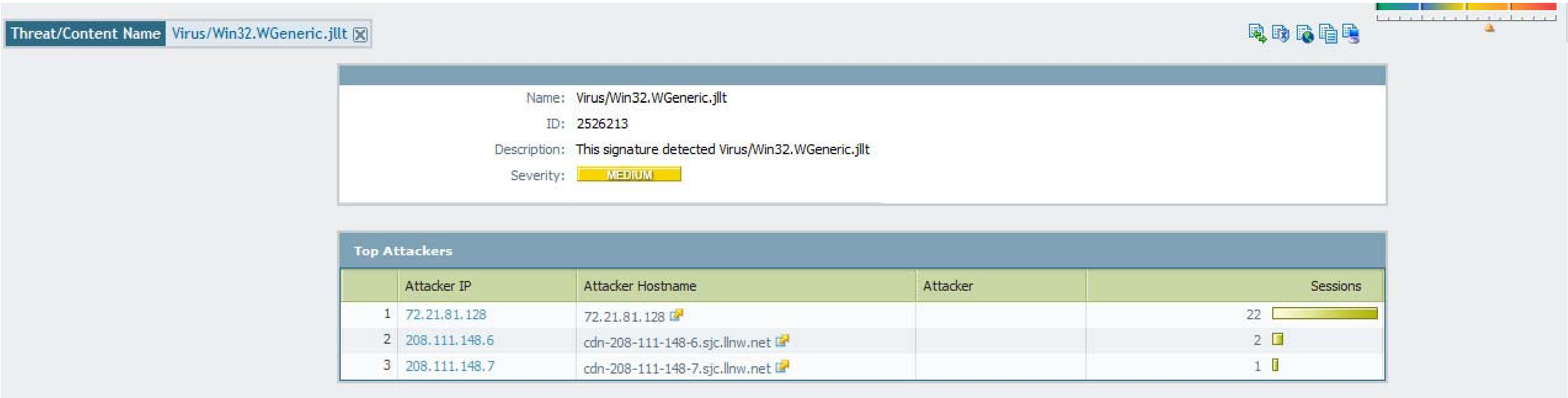
# PA NGFW top 25 Viruses: 9/27/13 to 10/04/13


Help
Top 25
Threat
Filter
Threat Count
50
40
30
20
10
0
Fri
Sat
Sun
Mon
Tue
Wed
Thu
Fri
Virus/Win32.WGeneric.jfpo
Virus/Win32.WGeneric.jfek
Virus/Win32.WGeneric.jllt
Virus/Win32.WGeneric.jjzy
Virus/Win32.WGeneric.jhei
Virus/Win32.WGeneric.jned
Virus/Win32.WGeneric.jazo
Virus/Win32.WGeneric.iscj
Virus/Win32.WGeneric.jqfc
Virus/Win32.WGeneric.jhjr
Virus/Win32.WGeneric.jief
Virus/Win32.WGeneric.glll
Virus/Win32.WGeneric.jpin
Virus/Win32.WGeneric.jisp
Virus/Win32.WGeneric.jitl
Virus/Win32.WGeneric.jyvt
Virus/Win32.WGeneric.izqt
Virus/Win32.WGeneric.jbaf
Virus/Win32.WGeneric.iyvq
Virus/Win32.WGeneric.eodf
Virus/Win32.WGeneric.jeqm
Virus/Win32.WGeneric.jglj
Virus/Win32.WGeneric.hmte
Virus/Win32.WGeneric.iuwa
Virus/Win32.WGeneric.ioai
other
Last 6 hours
Last 12 hours
Last 24 hours
Last 7 days
Last 30 days

# **PA NGFW top 25 Viruses (zoom):** 9/27/13 to 10/04/13



# **PA NGFW top Viruses #1:** Virus/Win32.WGeneric.jllt



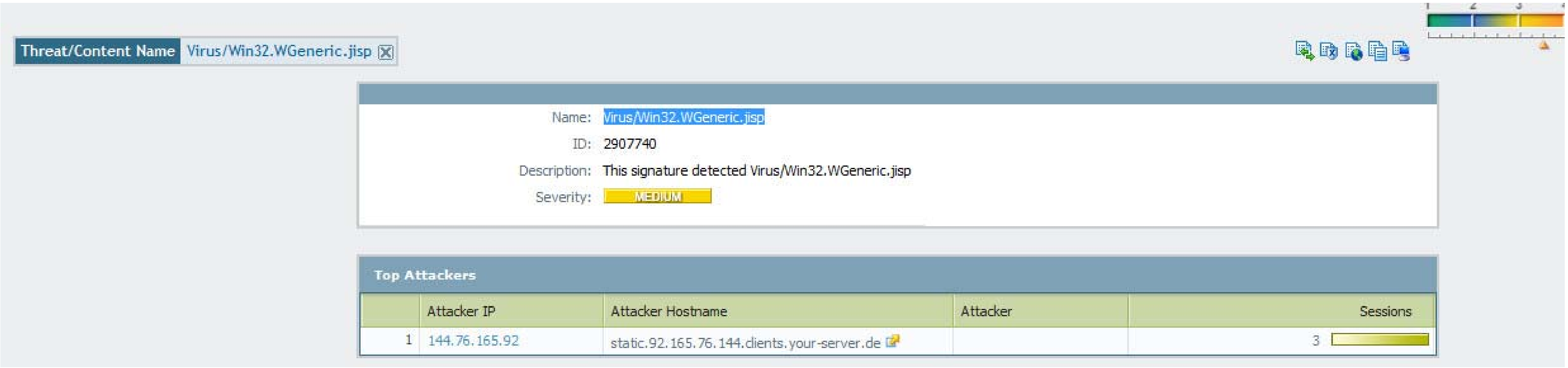
Threat/Content Name Virus/Win32.WGeneric.jllt

Name: Virus/Win32.WGeneric.jllt
ID: 2526213
Description: This signature detected Virus/Win32.WGeneric.jllt
Severity: MEDIUM

**Top Attackers**

| | Attacker IP | Attacker Hostname | Attacker | Sessions |
|---|---|---|---|---|
| 1 | 72.21.81.128 | 72.21.81.128 | | 22 |
| 2 | 208.111.148.6 | cdn-208-111-148-6.sjc.llnw.net | | 2 |
| 3 | 208.111.148.7 | cdn-208-111-148-7.sjc.llnw.net | | 1 |

# **PA NGFW top Viruses #2:** Virus/Win32.WGeneric.jisp



Threat/Content Name Virus/Win32.WGeneric.jisp ☒

Name: Virus/Win32.WGeneric.jisp

ID: 2907740

Description: This signature detected Virus/Win32.WGeneric.jisp

Severity: MEDIUM

**Top Attackers**

| | Attacker IP | Attacker Hostname | Attacker | Sessions |
|---|---|---|---|---|
| 1 | 144.76.165.92 | static.92.165.76.144.clients.your-server.de | | 3 |

# **PA NGFW:** Wildfire

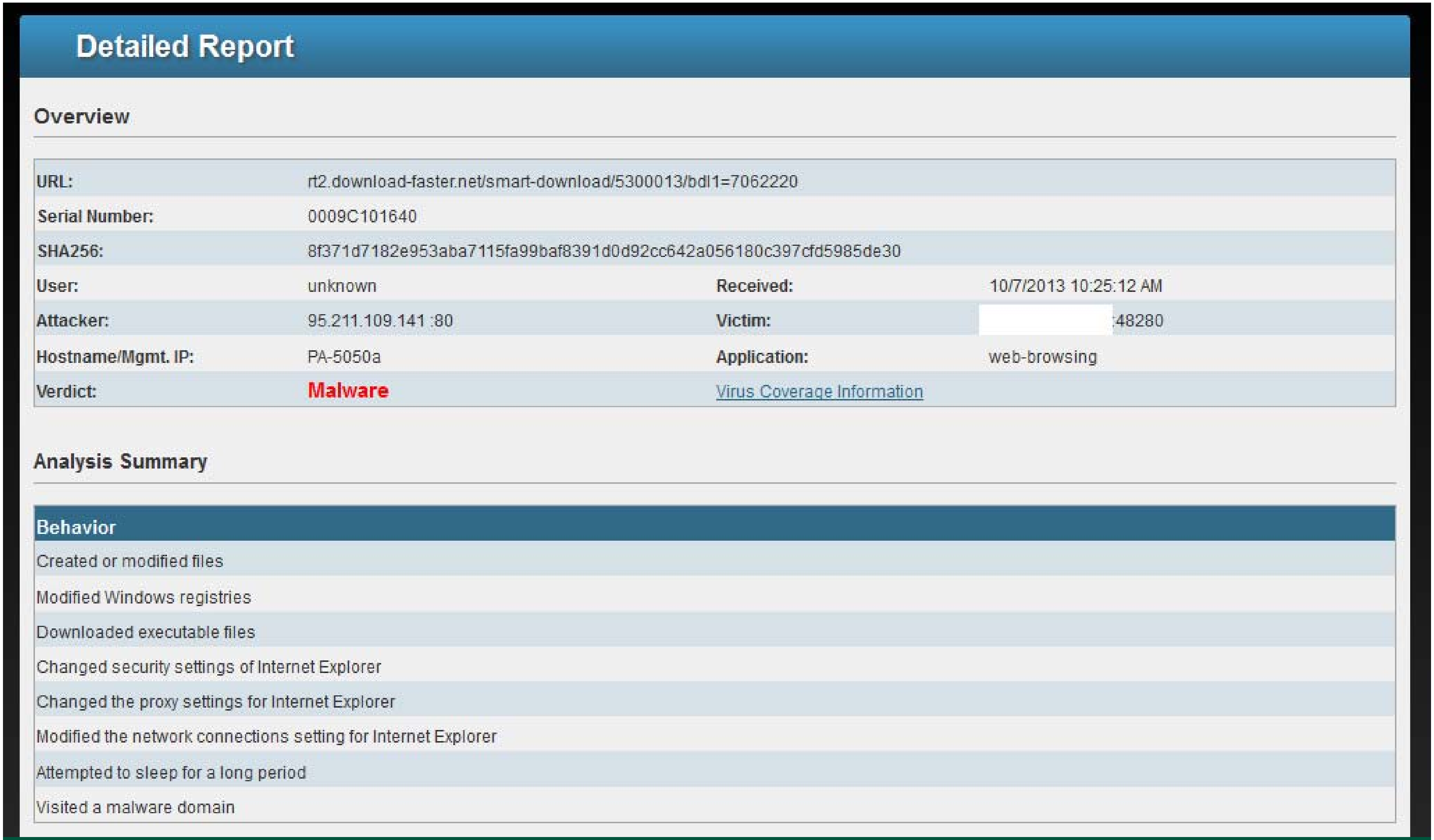
The file "GTA - The Crowd (Original Mix) [GodsPlaylist].exe" is uploaded from firewall PA-5050a at 2013-10-07 17:25:12.
URL: rt2.download-faster.net/smart-download/5300013/bdl1=7062220
User: unknown
Application: web-browsing
Source IP/Port:95.211.109.141/80
Destination IP/Port: **********/48280
Device S/N: 0009C101640

## This sample is malware

Here is the summary of the sample's behaviors:

-Created or modified files
-Modified Windows registries
-Downloaded executable files
-Changed security settings of Internet Explorer
-Visited a malware domain
-Changed the proxy settings for Internet Explorer
-Modified the network connections setting for Internet Explorer
-Attempted to sleep for a long period

# **PA NGFW:** Wildfire full report



## Detailed Report

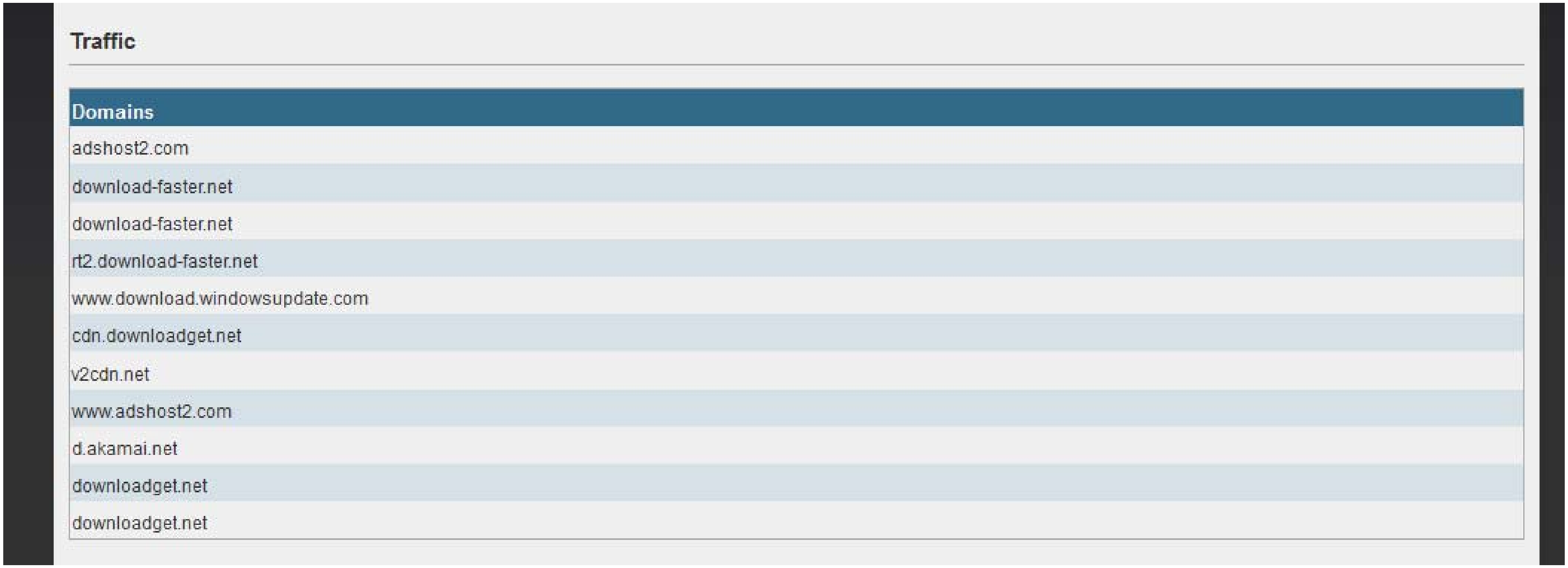
### Overview

| | | | |
|---|---|---|---|
| **URL:** | rt2.download-faster.net/smart-download/5300013/bdl1=7062220 | | |
| **Serial Number:** | 0009C101640 | | |
| **SHA256:** | 8f371d7182e953aba7115fa99baf8391d0d92cc642a056180c397cfd5985de30 | | |
| **User:** | unknown | **Received:** | 10/7/2013 10:25:12 AM |
| **Attacker:** | 95.211.109.141 :80 | **Victim:** | [redacted]:48280 |
| **Hostname/Mgmt. IP:** | PA-5050a | **Application:** | web-browsing |
| **Verdict:** | **Malware** | Virus Coverage Information | |

### Analysis Summary

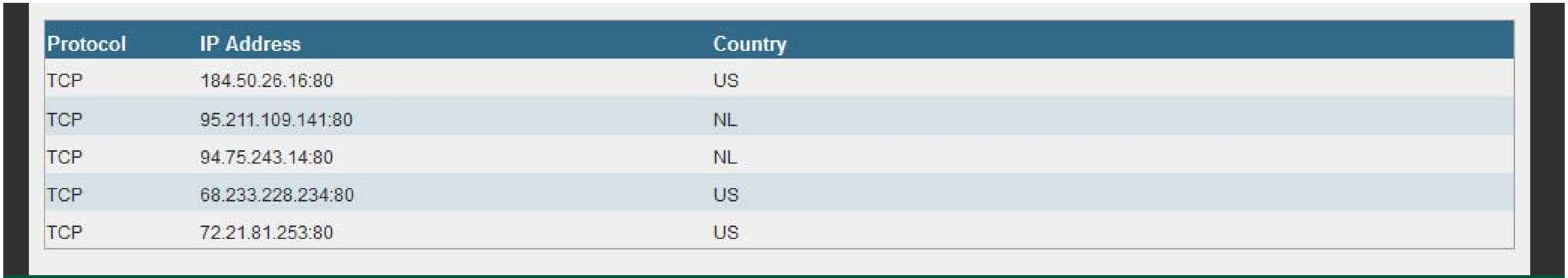
| **Behavior** |
|---|
| Created or modified files |
| Modified Windows registries |
| Downloaded executable files |
| Changed security settings of Internet Explorer |
| Changed the proxy settings for Internet Explorer |
| Modified the network connections setting for Internet Explorer |
| Attempted to sleep for a long period |
| Visited a malware domain |

# **PA NGFW:** Wildfire full report



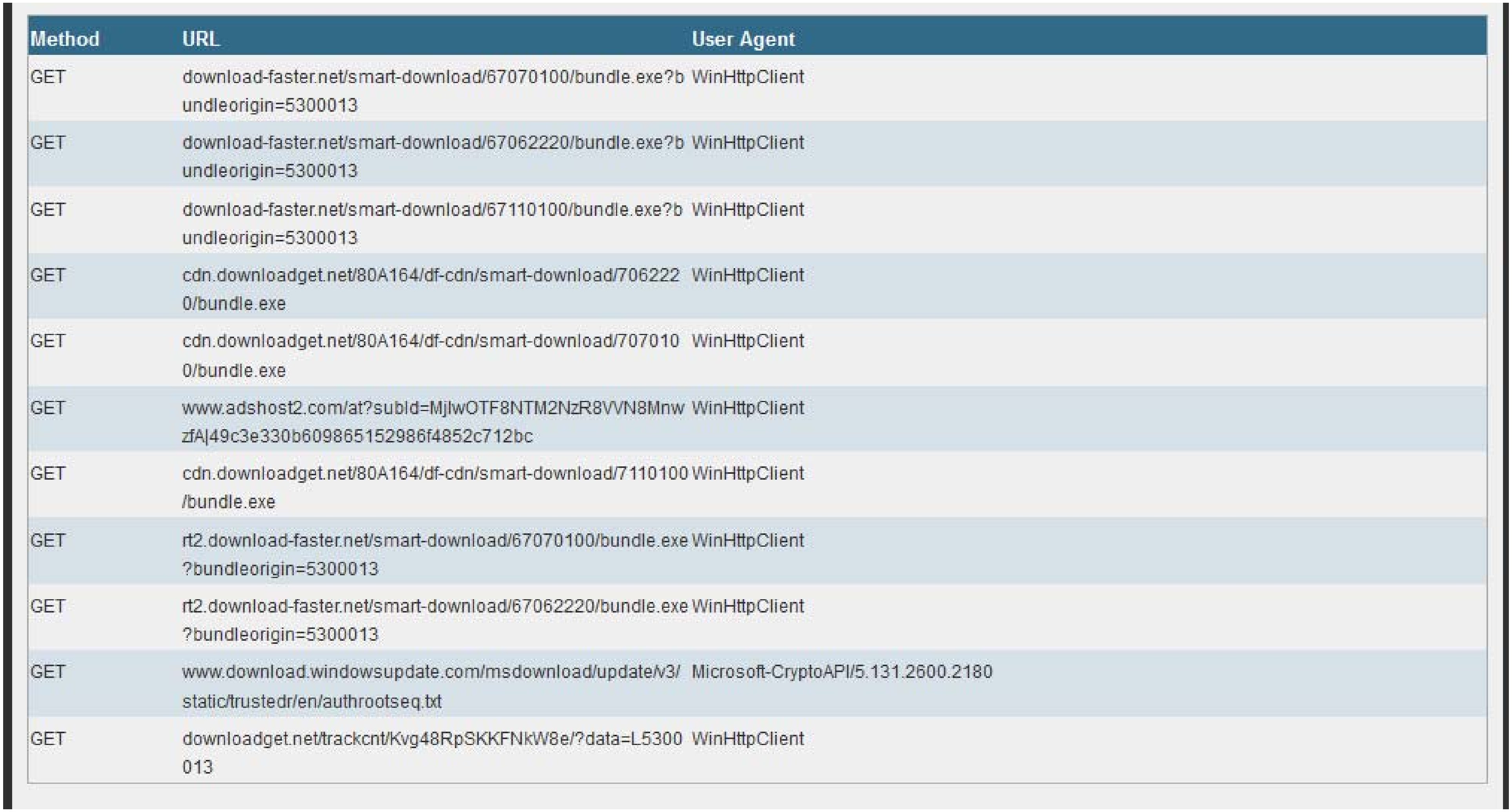
### Traffic

| Domains |
|---|
| adshost2.com |
| download-faster.net |
| download-faster.net |
| rt2.download-faster.net |
| www.download.windowsupdate.com |
| cdn.downloadget.net |
| v2cdn.net |
| www.adshost2.com |
| d.akamai.net |
| downloadget.net |
| downloadget.net |

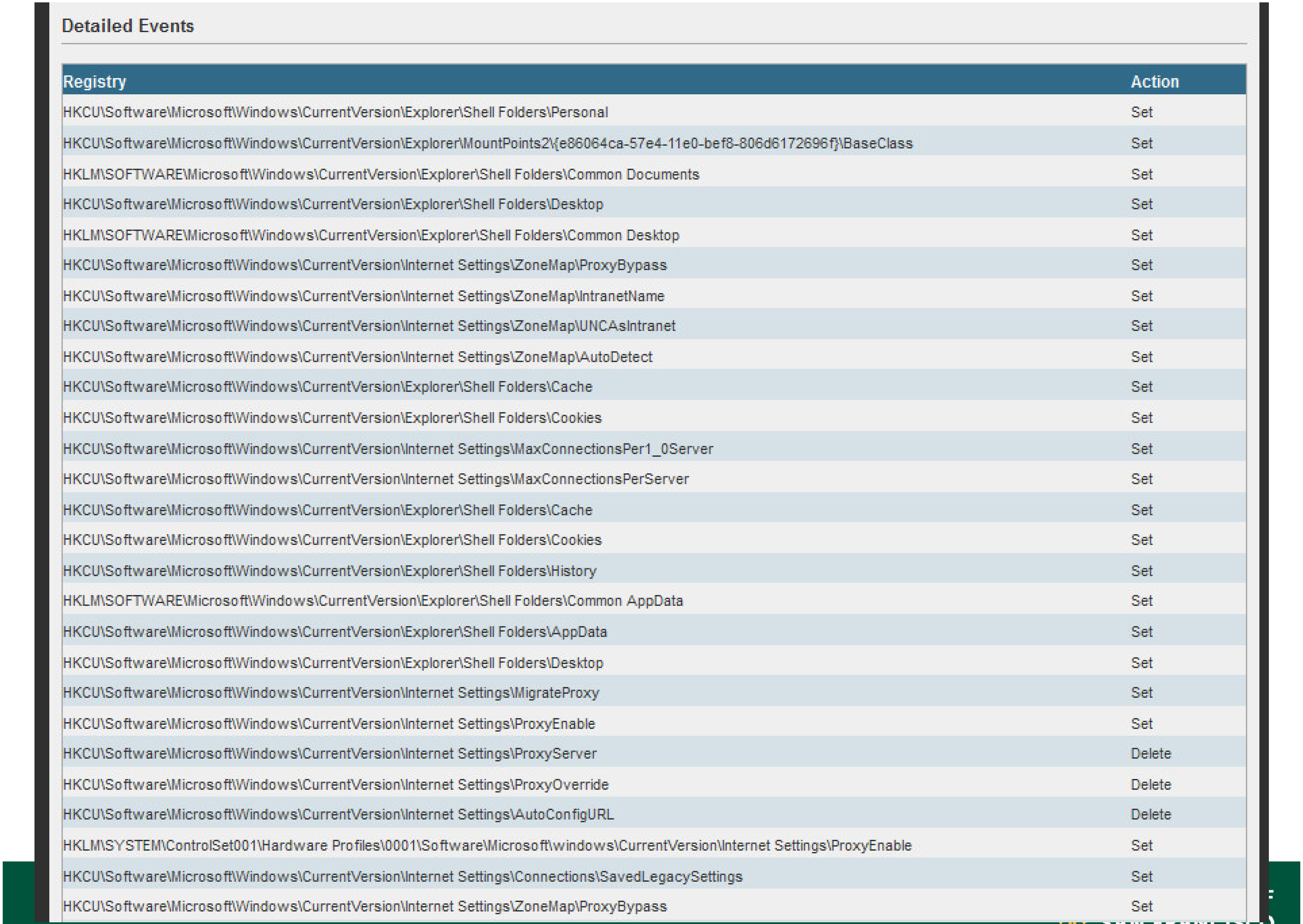


| Protocol | IP Address | Country |
|---|---|---|
| TCP | 184.50.26.16:80 | US |
| TCP | 95.211.109.141:80 | NL |
| TCP | 94.75.243.14:80 | NL |
| TCP | 68.233.228.234:80 | US |
| TCP | 72.21.81.253:80 | US |

# **PA NGFW:** Wildfire full report



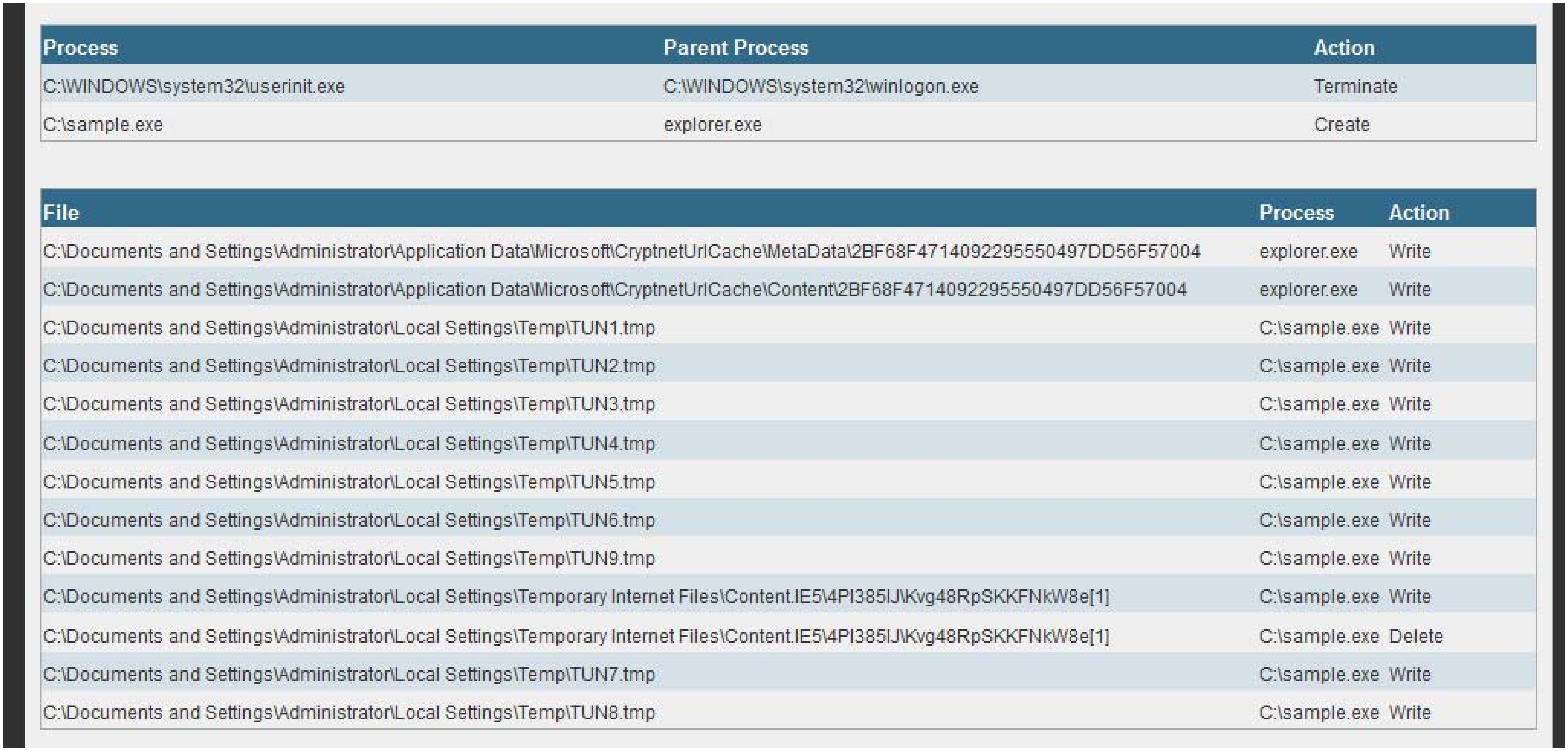
| Method | URL | User Agent |
|---|---|---|
| GET | download-faster.net/smart-download/67070100/bundle.exe?bundleorigin=5300013 | WinHttpClient |
| GET | download-faster.net/smart-download/67062220/bundle.exe?bundleorigin=5300013 | WinHttpClient |
| GET | download-faster.net/smart-download/67110100/bundle.exe?bundleorigin=5300013 | WinHttpClient |
| GET | cdn.downloadget.net/80A164/df-cdn/smart-download/7062220/bundle.exe | WinHttpClient |
| GET | cdn.downloadget.net/80A164/df-cdn/smart-download/7070100/bundle.exe | WinHttpClient |
| GET | www.adshost2.com/at?subId=MjIwOTF8NTM2NzR8VVN8MnwzfA\|49c3e330b609865152986f4852c712bc | WinHttpClient |
| GET | cdn.downloadget.net/80A164/df-cdn/smart-download/7110100/bundle.exe | WinHttpClient |
| GET | rt2.download-faster.net/smart-download/67070100/bundle.exe?bundleorigin=5300013 | WinHttpClient |
| GET | rt2.download-faster.net/smart-download/67062220/bundle.exe?bundleorigin=5300013 | WinHttpClient |
| GET | www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootseq.txt | Microsoft-CryptoAPI/5.131.2600.2180 |
| GET | downloadget.net/trackcnt/Kvg48RpSKKFNkW8e/?data=L5300013 | WinHttpClient |



## Detailed Events

| Registry | Action |
|---|---|
| HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Personal | Set |
| HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{e86064ca-57e4-11e0-bef8-806d6172696f}\BaseClass | Set |
| HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Common Documents | Set |
| HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Desktop | Set |
| HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Common Desktop | Set |
| HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass | Set |
| HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName | Set |
| HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet | Set |
| HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect | Set |
| HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cache | Set |
| HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cookies | Set |
| HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\MaxConnectionsPer1_0Server | Set |
| HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\MaxConnectionsPerServer | Set |
| HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cache | Set |
| HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cookies | Set |
| HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\History | Set |
| HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Common AppData | Set |
| HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\AppData | Set |
| HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Desktop | Set |
| HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\MigrateProxy | Set |
| HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable | Set |
| HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer | Delete |
| HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride | Delete |
| HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL | Delete |
| HKLM\SYSTEM\ControlSet001\Hardware Profiles\0001\Software\Microsoft\windows\CurrentVersion\Internet Settings\ProxyEnable | Set |
| HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings | Set |
| HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass | Set |

# **PA NGFW:** Wildfire full report

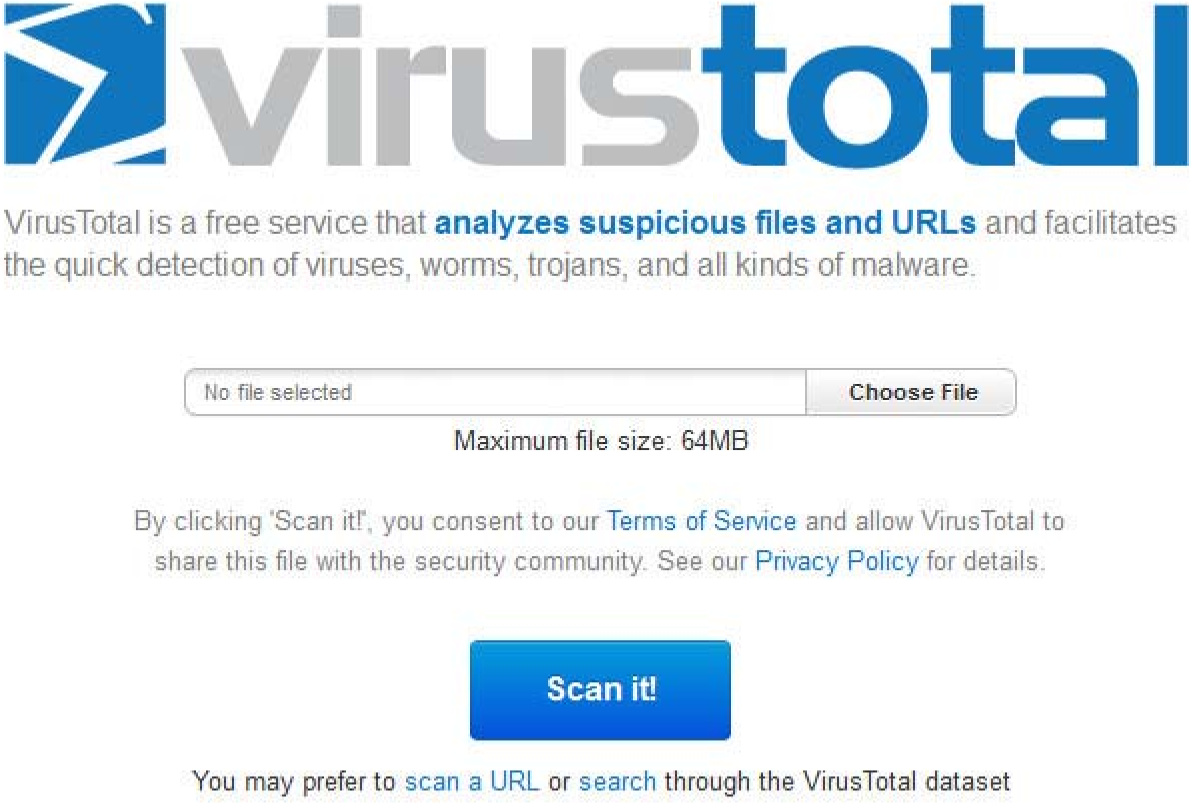


| Process | Parent Process | Action |
|---|---|---|
| C:\WINDOWS\system32\userinit.exe | C:\WINDOWS\system32\winlogon.exe | Terminate |
| C:\sample.exe | explorer.exe | Create |

| File | Process | Action |
|---|---|---|
| C:\Documents and Settings\Administrator\Application Data\Microsoft\CryptnetUrlCache\MetaData\2BF68F4714092295550497DD56F57004 | explorer.exe | Write |
| C:\Documents and Settings\Administrator\Application Data\Microsoft\CryptnetUrlCache\Content\2BF68F4714092295550497DD56F57004 | explorer.exe | Write |
| C:\Documents and Settings\Administrator\Local Settings\Temp\TUN1.tmp | C:\sample.exe | Write |
| C:\Documents and Settings\Administrator\Local Settings\Temp\TUN2.tmp | C:\sample.exe | Write |
| C:\Documents and Settings\Administrator\Local Settings\Temp\TUN3.tmp | C:\sample.exe | Write |
| C:\Documents and Settings\Administrator\Local Settings\Temp\TUN4.tmp | C:\sample.exe | Write |
| C:\Documents and Settings\Administrator\Local Settings\Temp\TUN5.tmp | C:\sample.exe | Write |
| C:\Documents and Settings\Administrator\Local Settings\Temp\TUN6.tmp | C:\sample.exe | Write |
| C:\Documents and Settings\Administrator\Local Settings\Temp\TUN9.tmp | C:\sample.exe | Write |
| C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\4PI385IJ\Kvg48RpSKKFNkW8e[1] | C:\sample.exe | Write |
| C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\4PI385IJ\Kvg48RpSKKFNkW8e[1] | C:\sample.exe | Delete |
| C:\Documents and Settings\Administrator\Local Settings\Temp\TUN7.tmp | C:\sample.exe | Write |
| C:\Documents and Settings\Administrator\Local Settings\Temp\TUN8.tmp | C:\sample.exe | Write |

# **PA NGFW:** Wildfire leverages **VirusTotal**

https://www.virustotal.com/



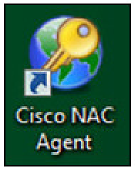
VirusTotal is a free service that **analyzes suspicious files and URLs** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.

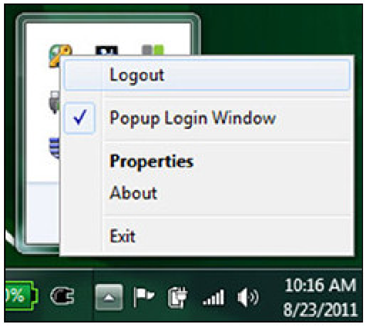
Maximum file size: 64MB

By clicking 'Scan it!', you consent to our Terms of Service and allow VirusTotal to share this file with the security community. See our Privacy Policy for details.

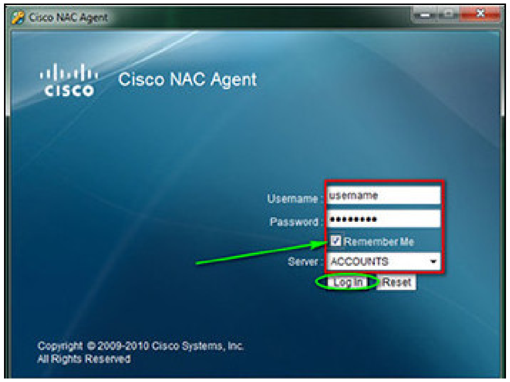
You may prefer to scan a URL or search through the VirusTotal dataset

# 2) Network Access Control – posture assessment / compliance



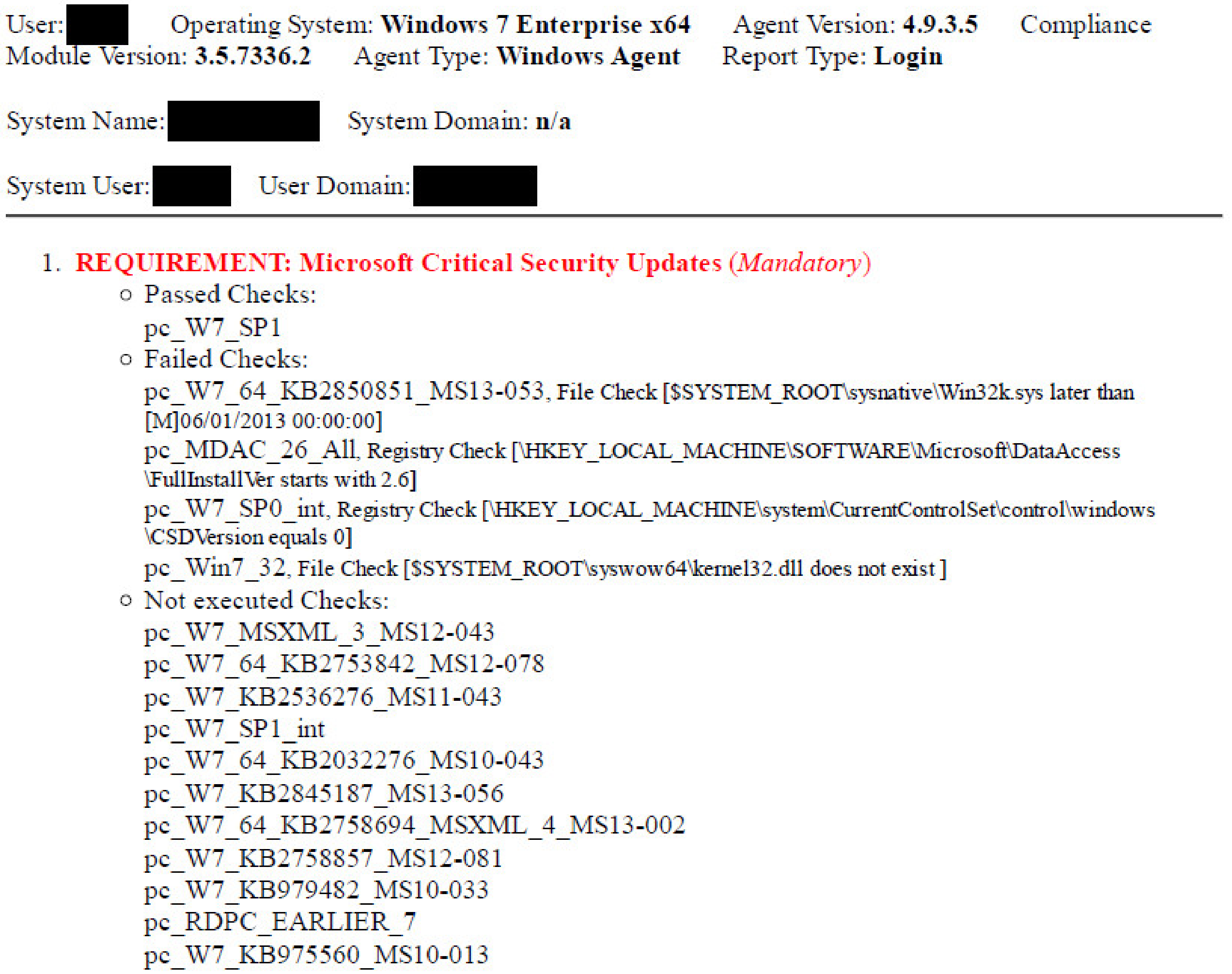


4. The Cisco NAC Agent is now installed. You will be automatically prompted to log into the agent (see visuals below):



Reference:
http://www.usfca.edu/its/help/studentcomputing/rooms/
http://www.usfca.edu/its/help/studentcomputing/nac/

# **Network Access Control –** posture assessment / compliance



User: [redacted] Operating System: **Windows 7 Enterprise x64** Agent Version: **4.9.3.5** Compliance Module Version: **3.5.7336.2** Agent Type: **Windows Agent** Report Type: **Login**

System Name: [redacted] System Domain: **n/a**

System User: [redacted] User Domain: [redacted]

1. **REQUIREMENT: Microsoft Critical Security Updates** (*Mandatory*)
   - Passed Checks:
     pc_W7_SP1
   - Failed Checks:
     pc_W7_64_KB2850851_MS13-053, File Check [$SYSTEM_ROOT\sysnative\Win32k.sys later than [M]06/01/2013 00:00:00]
     pc_MDAC_26_All, Registry Check [\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DataAccess \FullInstallVer starts with 2.6]
     pc_W7_SP0_int, Registry Check [\HKEY_LOCAL_MACHINE\system\CurrentControlSet\control\windows \CSDVersion equals 0]
     pc_Win7_32, File Check [$SYSTEM_ROOT\syswow64\kernel32.dll does not exist ]
   - Not executed Checks:
     pc_W7_MSXML_3_MS12-043
     pc_W7_64_KB2753842_MS12-078
     pc_W7_KB2536276_MS11-043
     pc_W7_SP1_int
     pc_W7_64_KB2032276_MS10-043
     pc_W7_KB2845187_MS13-056
     pc_W7_64_KB2758694_MSXML_4_MS13-002
     pc_W7_KB2758857_MS12-081
     pc_W7_KB979482_MS10-033
     pc_RDPC_EARLIER_7
     pc_W7_KB975560_MS10-013

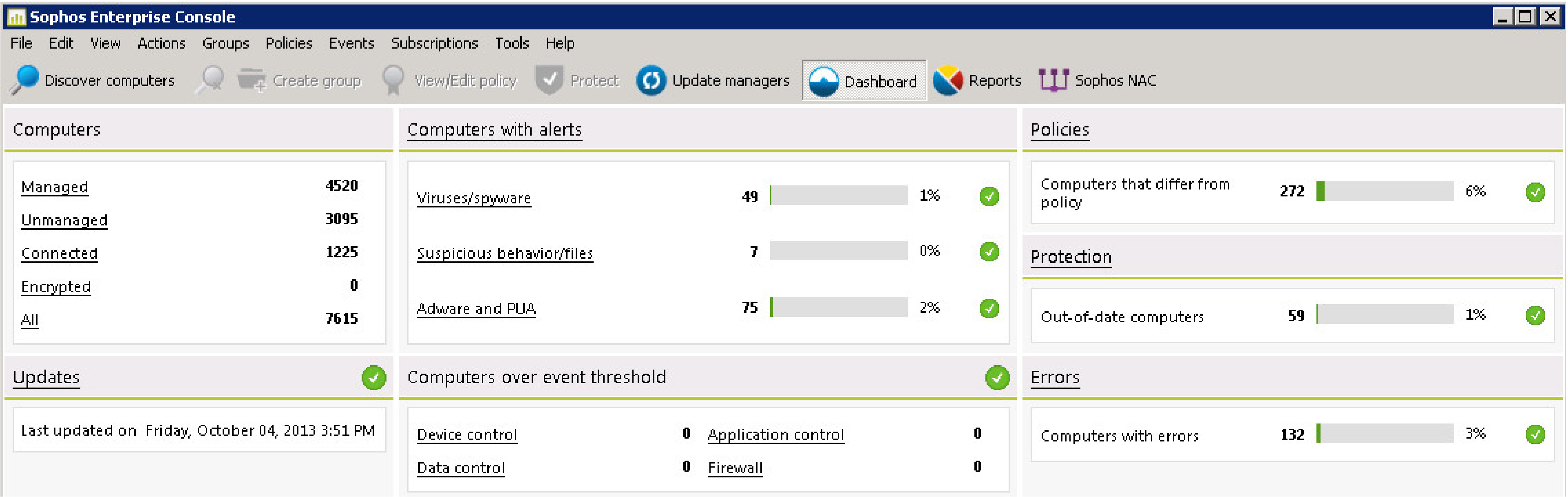
# 3) Sophos Antivirus Security and Control

SOPHOS

Enduser Protection Suites

The All-in-One Security Suite

# **Sophos AV:** Admin dashboard10/04/13



Computers

| | |
|---|---|
| Managed | 4520 |
| Unmanaged | 3095 |
| Connected | 1225 |
| Encrypted | 0 |
| All | 7615 |

Computers with alerts

| | | | |
|---|---|---|---|
| Viruses/spyware | 49 | 1% | ✓ |
| Suspicious behavior/files | 7 | 0% | ✓ |
| Adware and PUA | 75 | 2% | ✓ |

Policies

| | | | |
|---|---|---|---|
| Computers that differ from policy | 272 | 6% | ✓ |

Protection

| | | | |
|---|---|---|---|
| Out-of-date computers | 59 | 1% | ✓ |

Updates ✓

Last updated on Friday, October 04, 2013 3:51 PM

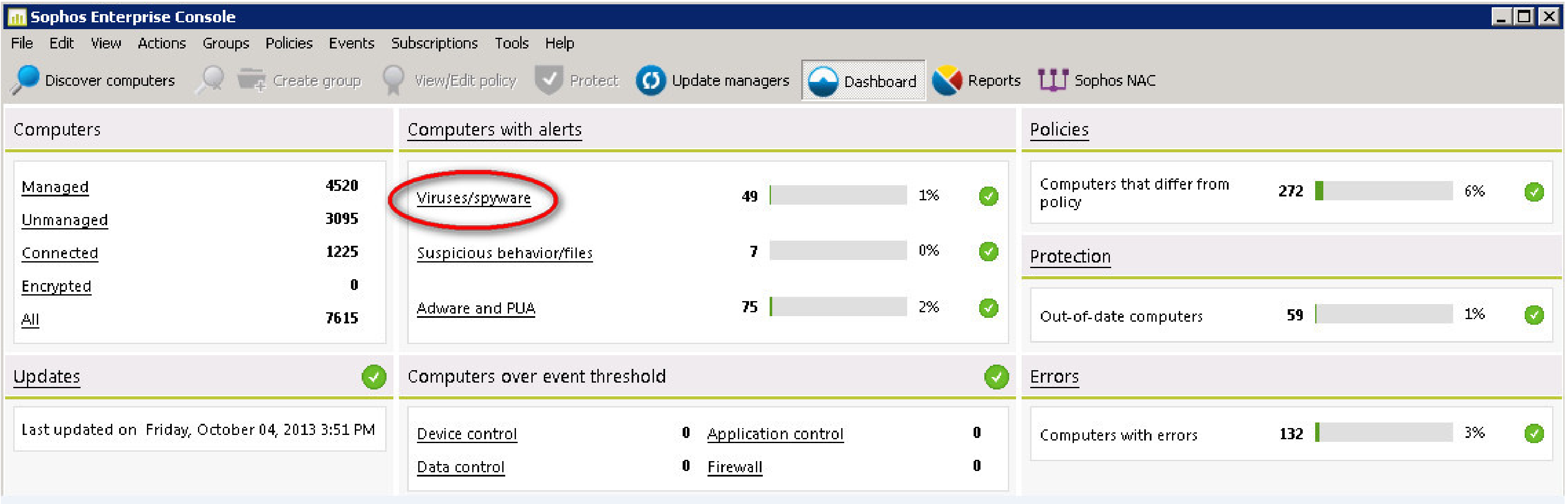
Computers over event threshold ✓

| | | | |
|---|---|---|---|
| Device control | 0 | Application control | 0 |
| Data control | 0 | Firewall | 0 |

Errors

| | | | |
|---|---|---|---|
| Computers with errors | 132 | 3% | ✓ |

# **Sophos AV:** Admin dashboard 10/04/13



Computers

| | |
|---|---|
| Managed | 4520 |
| Unmanaged | 3095 |
| Connected | 1225 |
| Encrypted | 0 |
| All | 7615 |

Computers with alerts

| | | | |
|---|---|---|---|
| Viruses/spyware | 49 | 1% | ✓ |
| Suspicious behavior/files | 7 | 0% | ✓ |
| Adware and PUA | 75 | 2% | ✓ |

Policies

| | | | |
|---|---|---|---|
| Computers that differ from policy | 272 | 6% | ✓ |

Protection

| | | | |
|---|---|---|---|
| Out-of-date computers | 59 | 1% | ✓ |

Updates ✓

Last updated on Friday, October 04, 2013 3:51 PM

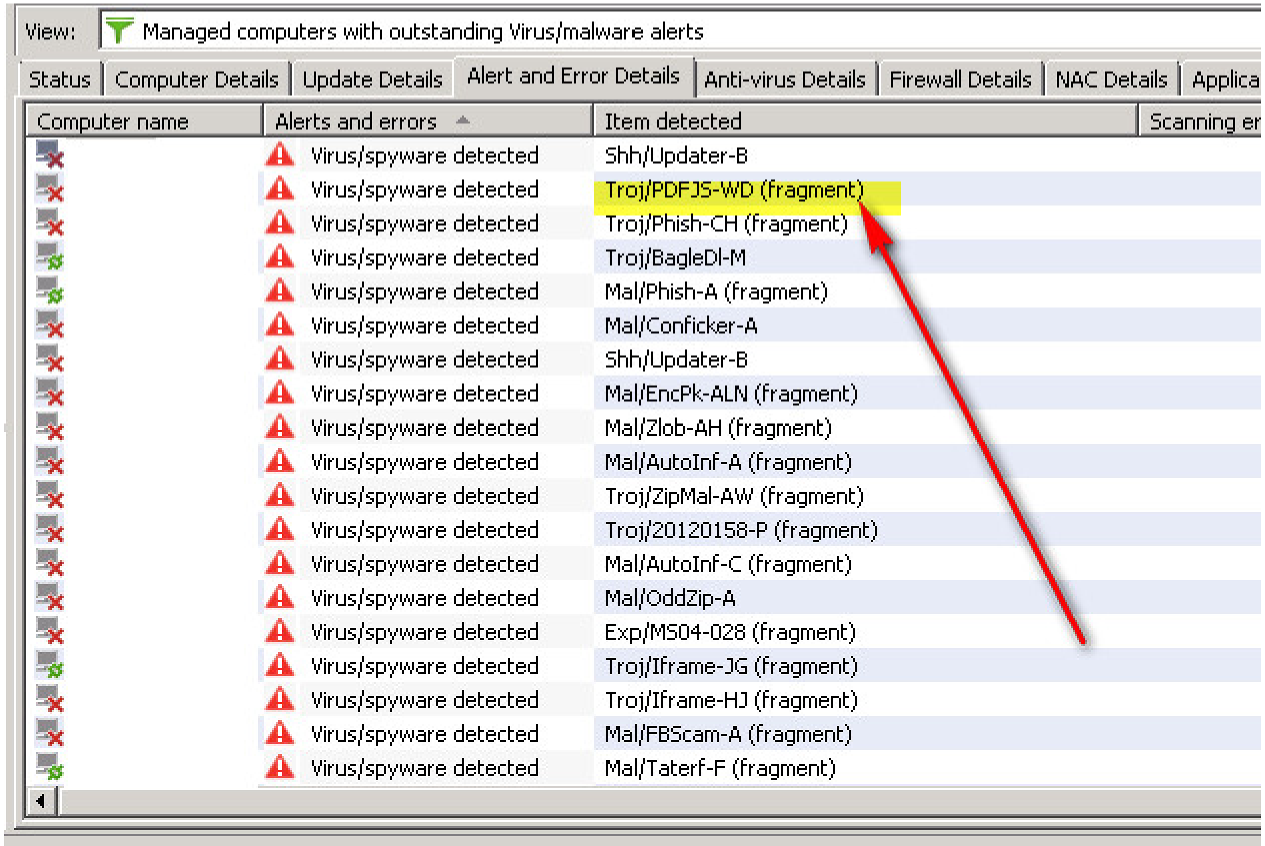
Computers over event threshold ✓

| | | | |
|---|---|---|---|
| Device control | 0 | Application control | 0 |
| Data control | 0 | Firewall | 0 |

Errors

| | | | |
|---|---|---|---|
| Computers with errors | 132 | 3% | ✓ |

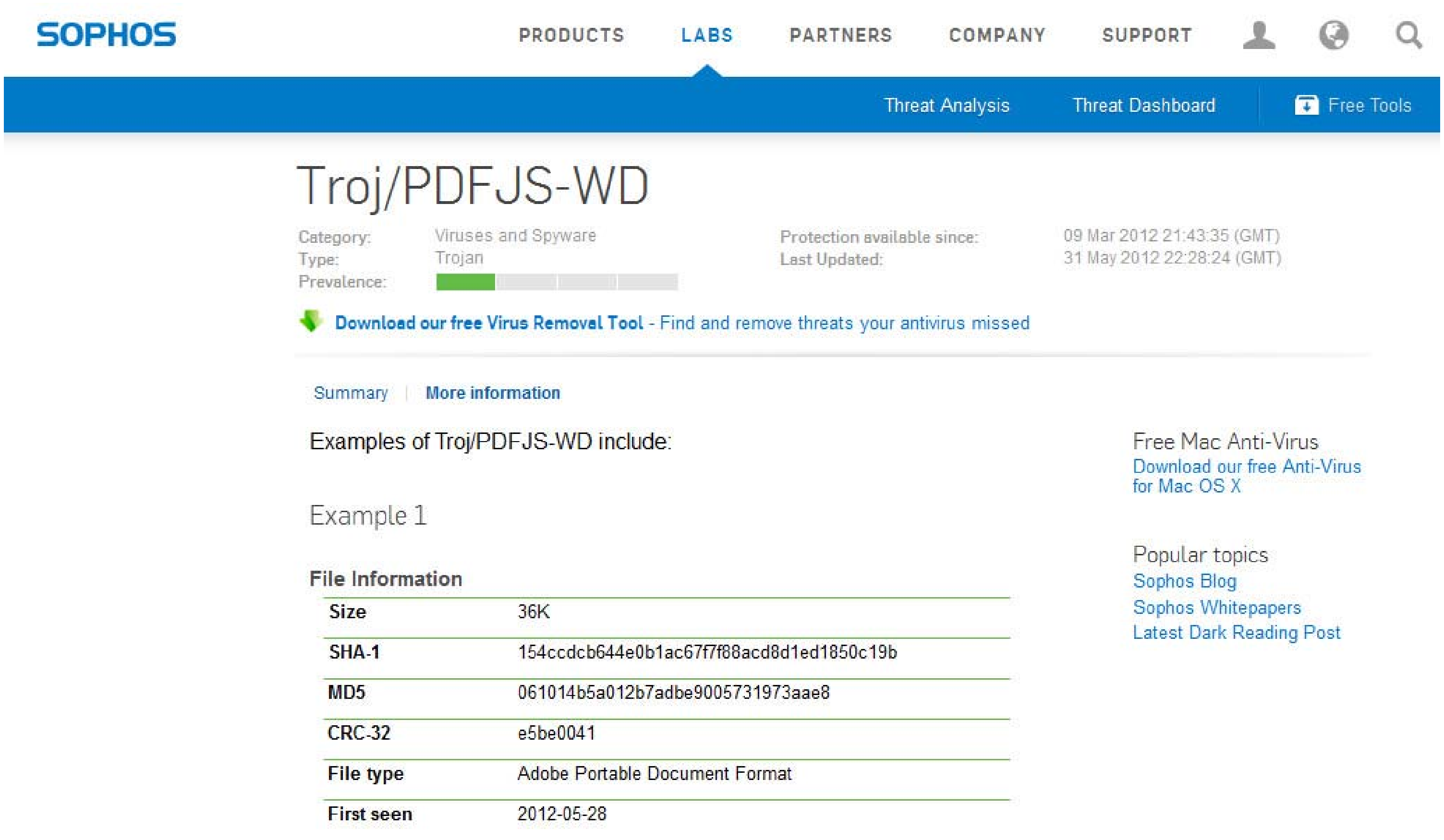
# **Sophos AV:** Admin dashboard 10/04/13



View: Managed computers with outstanding Virus/malware alerts

| Computer name | Alerts and errors | Item detected | Scanning er |
|---|---|---|---|
| | ⚠ Virus/spyware detected | Shh/Updater-B | |
| | ⚠ Virus/spyware detected | Troj/PDFJS-WD (fragment) | |
| | ⚠ Virus/spyware detected | Troj/Phish-CH (fragment) | |
| | ⚠ Virus/spyware detected | Troj/BagleDl-M | |
| | ⚠ Virus/spyware detected | Mal/Phish-A (fragment) | |
| | ⚠ Virus/spyware detected | Mal/Conficker-A | |
| | ⚠ Virus/spyware detected | Shh/Updater-B | |
| | ⚠ Virus/spyware detected | Mal/EncPk-ALN (fragment) | |
| | ⚠ Virus/spyware detected | Mal/Zlob-AH (fragment) | |
| | ⚠ Virus/spyware detected | Mal/AutoInf-A (fragment) | |
| | ⚠ Virus/spyware detected | Troj/ZipMal-AW (fragment) | |
| | ⚠ Virus/spyware detected | Troj/20120158-P (fragment) | |
| | ⚠ Virus/spyware detected | Mal/AutoInf-C (fragment) | |
| | ⚠ Virus/spyware detected | Mal/OddZip-A | |
| | ⚠ Virus/spyware detected | Exp/MS04-028 (fragment) | |
| | ⚠ Virus/spyware detected | Troj/Iframe-JG (fragment) | |
| | ⚠ Virus/spyware detected | Troj/Iframe-HJ (fragment) | |
| | ⚠ Virus/spyware detected | Mal/FBScam-A (fragment) | |
| | ⚠ Virus/spyware detected | Mal/Taterf-F (fragment) | |

# **Sophos AV:** Admin dashboard 10/04/13



## Troj/PDFJS-WD

| | | | |
|---|---|---|---|
| Category: | Viruses and Spyware | Protection available since: | 09 Mar 2012 21:43:35 (GMT) |
| Type: | Trojan | Last Updated: | 31 May 2012 22:28:24 (GMT) |
| Prevalence: | 🟩 | | |

Download our free Virus Removal Tool - Find and remove threats your antivirus missed

Summary | More information

Examples of Troj/PDFJS-WD include:

Example 1

**File Information**

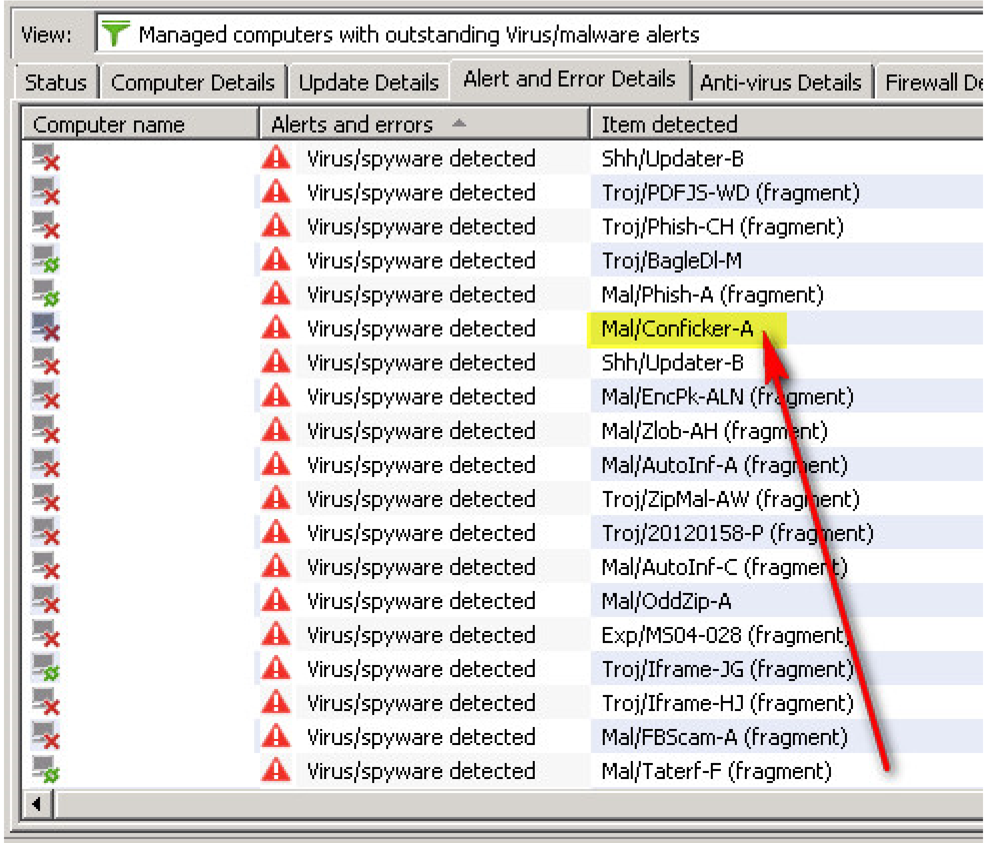
| | |
|---|---|
| **Size** | 36K |
| **SHA-1** | 154ccdcb644e0b1ac67f7f88acd8d1ed1850c19b |
| **MD5** | 061014b5a012b7adbe9005731973aae8 |
| **CRC-32** | e5be0041 |
| **File type** | Adobe Portable Document Format |
| **First seen** | 2012-05-28 |

Free Mac Anti-Virus
Download our free Anti-Virus for Mac OS X

Popular topics
Sophos Blog
Sophos Whitepapers
Latest Dark Reading Post

Reference: https://secure2.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/Troj~PDFJS-WD/detailed-analysis.aspx

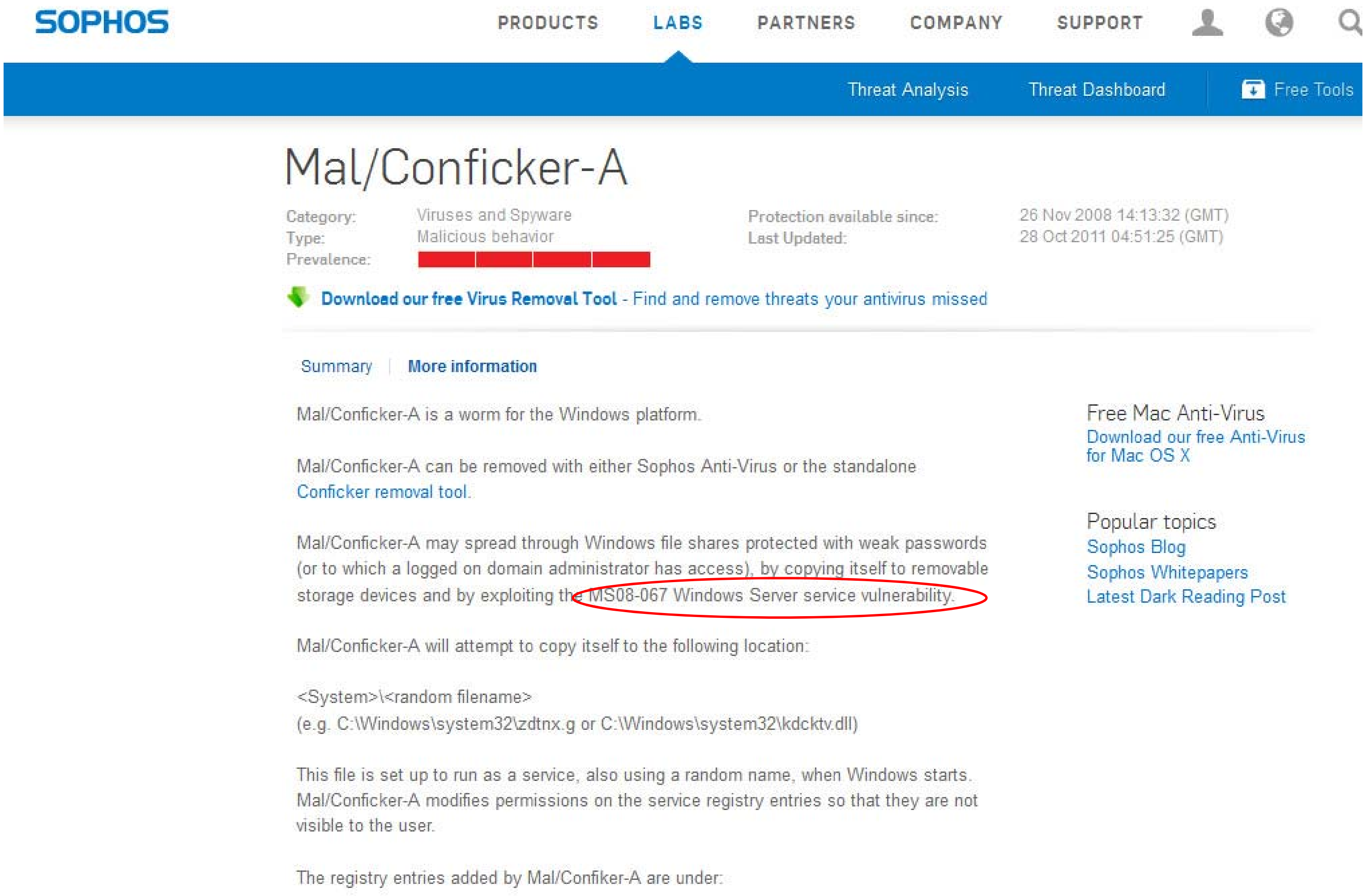
# **Sophos AV:** Admin dashboard 10/04/13



View: Managed computers with outstanding Virus/malware alerts

| Computer name | Alerts and errors | Item detected |
|---|---|---|
| | Virus/spyware detected | Shh/Updater-B |
| | Virus/spyware detected | Troj/PDFJS-WD (fragment) |
| | Virus/spyware detected | Troj/Phish-CH (fragment) |
| | Virus/spyware detected | Troj/BagleDl-M |
| | Virus/spyware detected | Mal/Phish-A (fragment) |
| | Virus/spyware detected | Mal/Conficker-A |
| | Virus/spyware detected | Shh/Updater-B |
| | Virus/spyware detected | Mal/EncPk-ALN (fragment) |
| | Virus/spyware detected | Mal/Zlob-AH (fragment) |
| | Virus/spyware detected | Mal/AutoInf-A (fragment) |
| | Virus/spyware detected | Troj/ZipMal-AW (fragment) |
| | Virus/spyware detected | Troj/20120158-P (fragment) |
| | Virus/spyware detected | Mal/AutoInf-C (fragment) |
| | Virus/spyware detected | Mal/OddZip-A |
| | Virus/spyware detected | Exp/MS04-028 (fragment) |
| | Virus/spyware detected | Troj/Iframe-JG (fragment) |
| | Virus/spyware detected | Troj/Iframe-HJ (fragment) |
| | Virus/spyware detected | Mal/FBScam-A (fragment) |
| | Virus/spyware detected | Mal/Taterf-F (fragment) |

# **Sophos AV:** Admin dashboard 10/04/13



## Mal/Conficker-A

Category: Viruses and Spyware
Type: Malicious behavior
Prevalence: 🟥🟥🟥🟥

Protection available since: 26 Nov 2008 14:13:32 (GMT)
Last Updated: 28 Oct 2011 04:51:25 (GMT)

**Download our free Virus Removal Tool** - Find and remove threats your antivirus missed

Summary | **More information**

Mal/Conficker-A is a worm for the Windows platform.

Mal/Conficker-A can be removed with either Sophos Anti-Virus or the standalone Conficker removal tool.

Mal/Conficker-A may spread through Windows file shares protected with weak passwords (or to which a logged on domain administrator has access), by copying itself to removable storage devices and by exploiting the MS08-067 Windows Server service vulnerability.

Mal/Conficker-A will attempt to copy itself to the following location:

<System>\<random filename>
(e.g. C:\Windows\system32\zdtnx.g or C:\Windows\system32\kdcktv.dll)

This file is set up to run as a service, also using a random name, when Windows starts. Mal/Conficker-A modifies permissions on the service registry entries so that they are not visible to the user.

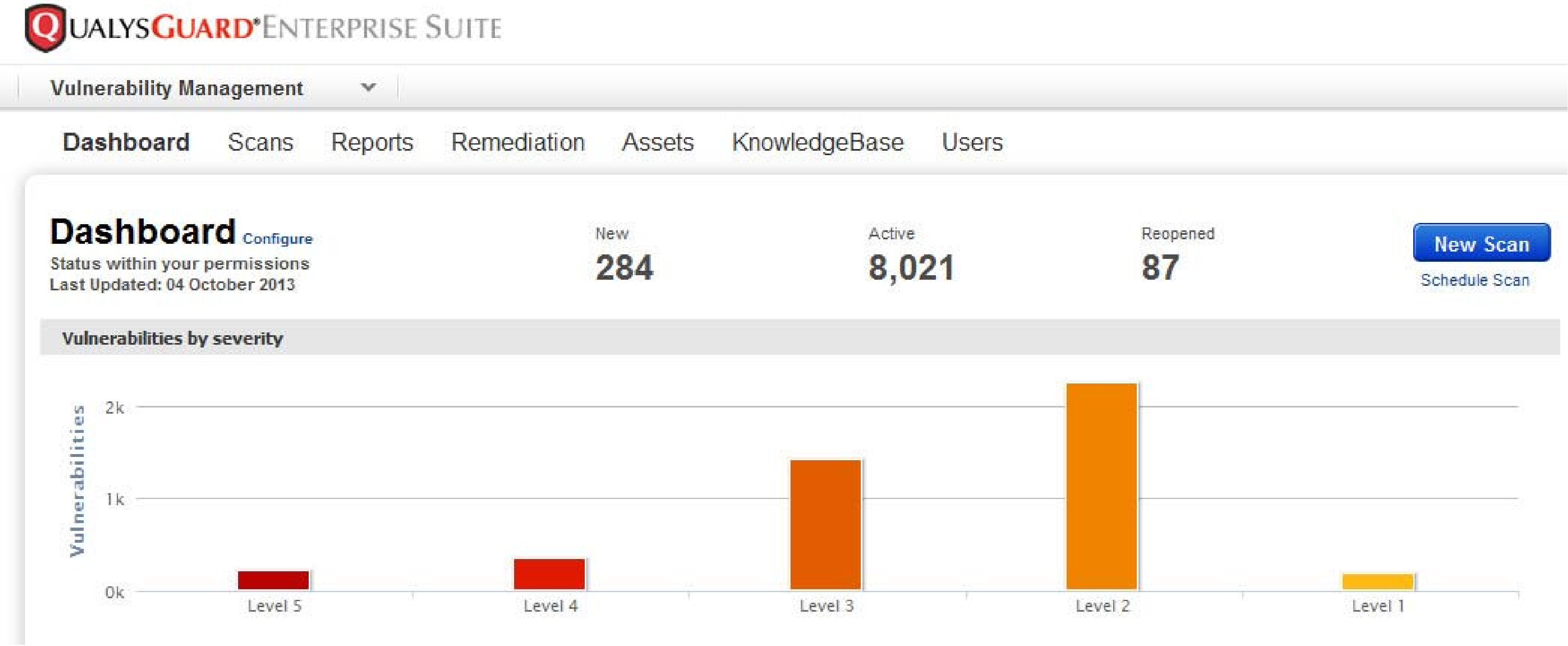
The registry entries added by Mal/Confiker-A are under:

Free Mac Anti-Virus
Download our free Anti-Virus for Mac OS X

Popular topics
Sophos Blog
Sophos Whitepapers
Latest Dark Reading Post

Reference: https://secure2.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/Mal~Conficker-A/detailed-analysis.aspx

# 4) QualysGuard Vulnerability Management:
Admin dashboard 10/4/13



**Dashboard**

Status within your permissions

Last Updated: 04 October 2013

| New | Active | Reopened |
|---|---|---|
| 284 | 8,021 | 87 |

# **QualysGuard Vulnerability Management:** now/then

```
Summary of discovered Vulnerabilities (Trend)

Severity 5 "Urgent"   : 8    (-1)
Severity 4 "Critical" : 65   (-3)
Severity 3 "Serious"  : 440  (-1)
Severity 2 "Medium"   : 1361 (-3)
Severity 1 "Minimal"  : 150  (=)

Total                 : 2024
```

```
Summary of discovered Vulnerabilities (Trend)

  Severity 5 "Urgent"   : 100 (0,1,99,0)
  Severity 4 "Critical" : 195 (0,0,195,0)
  Severity 3 "Serious"  : 1283 (7,13,1263,-6)
  Severity 2 "Medium"   : 1585 (13,14,1558,-9)
  Severity 1 "Minimal"  : 124 (4,0,120,-24)

  Total                 : 3287
```

Vulnerability Trend Status:
(NEW,REOPENED,ACTIVE,-CLOSED) processed for this scan
(note that TOTAL = NEW + REOPENED + ACTIVE for this scan, with CLOSED already fixed)

# **QualysGuard Vulnerability Management:** now/then

**Date: 09/2010**

Summary of discovered Vulnerabilities (Trend)

Severity 5 "Urgent" : 8 (-1)
Severity 4 "Critical" : 65 (-3)
Severity 3 "Serious" : 440 (-1)
Severity 2 "Medium" : 1361 (-3)
Severity 1 "Minimal" : 150 (=)

Total : 2024

**Date: 09/2013**

Summary of discovered Vulnerabilities (Trend)

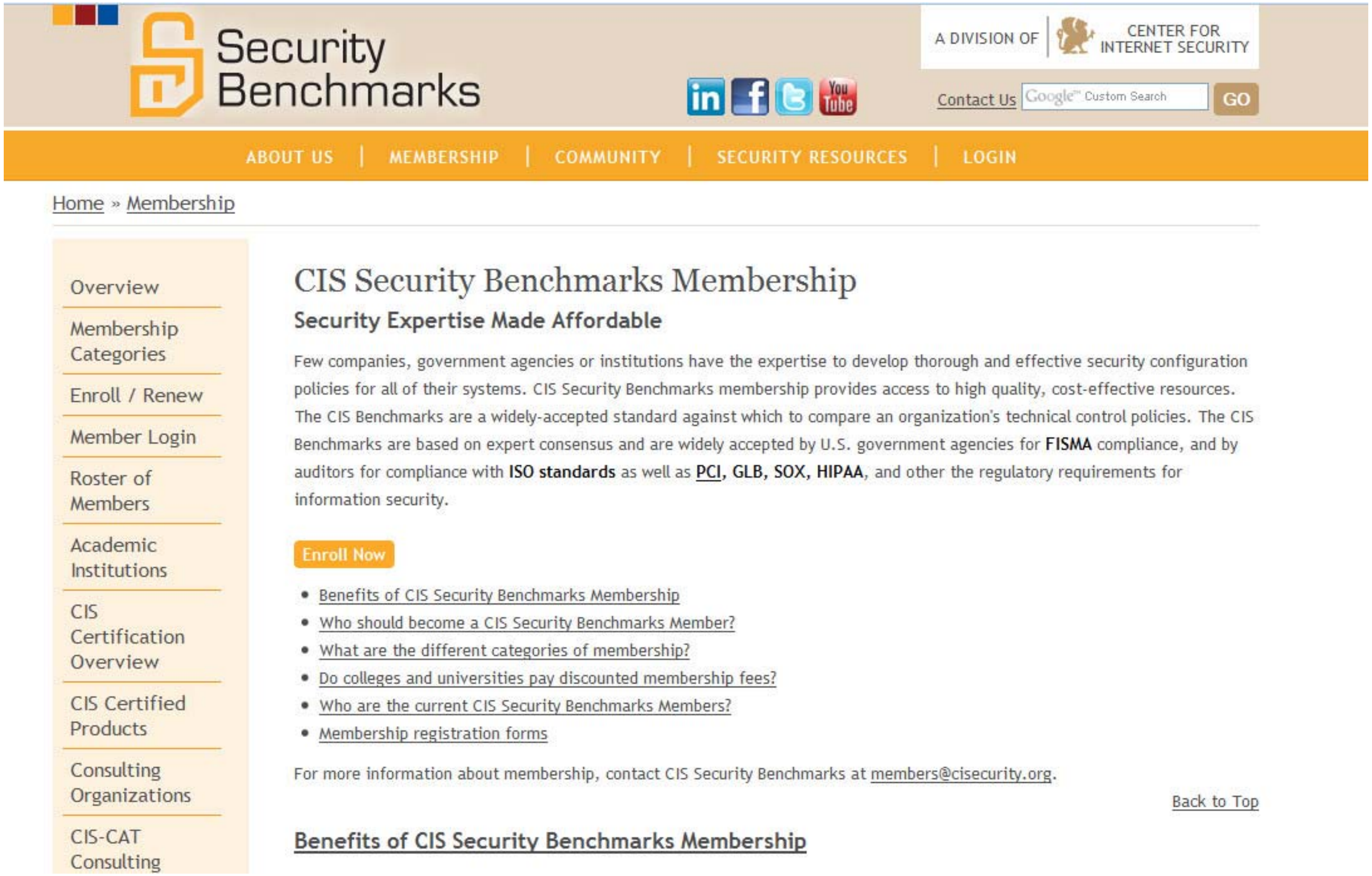
Severity 5 "Urgent" : 100 (0,1,99,0)
Severity 4 "Critical" : 195 (0,0,195,0)
Severity 3 "Serious" : 1283 (7,13,1263,-6)
Severity 2 "Medium" : 1585 (13,14,1558,-9)
Severity 1 "Minimal" : 124 (4,0,120,-24)

Total : 3287

Vulnerability Trend Status:
(NEW,REOPENED,ACTIVE,-CLOSED) processed for this scan
(note that TOTAL = NEW + REOPENED + ACTIVE for this scan, with CLOSED already fixed)

# 5) Center for Information Security

http://benchmarks.cisecurity.org/membership/



## CIS Security Benchmarks Membership

### Security Expertise Made Affordable

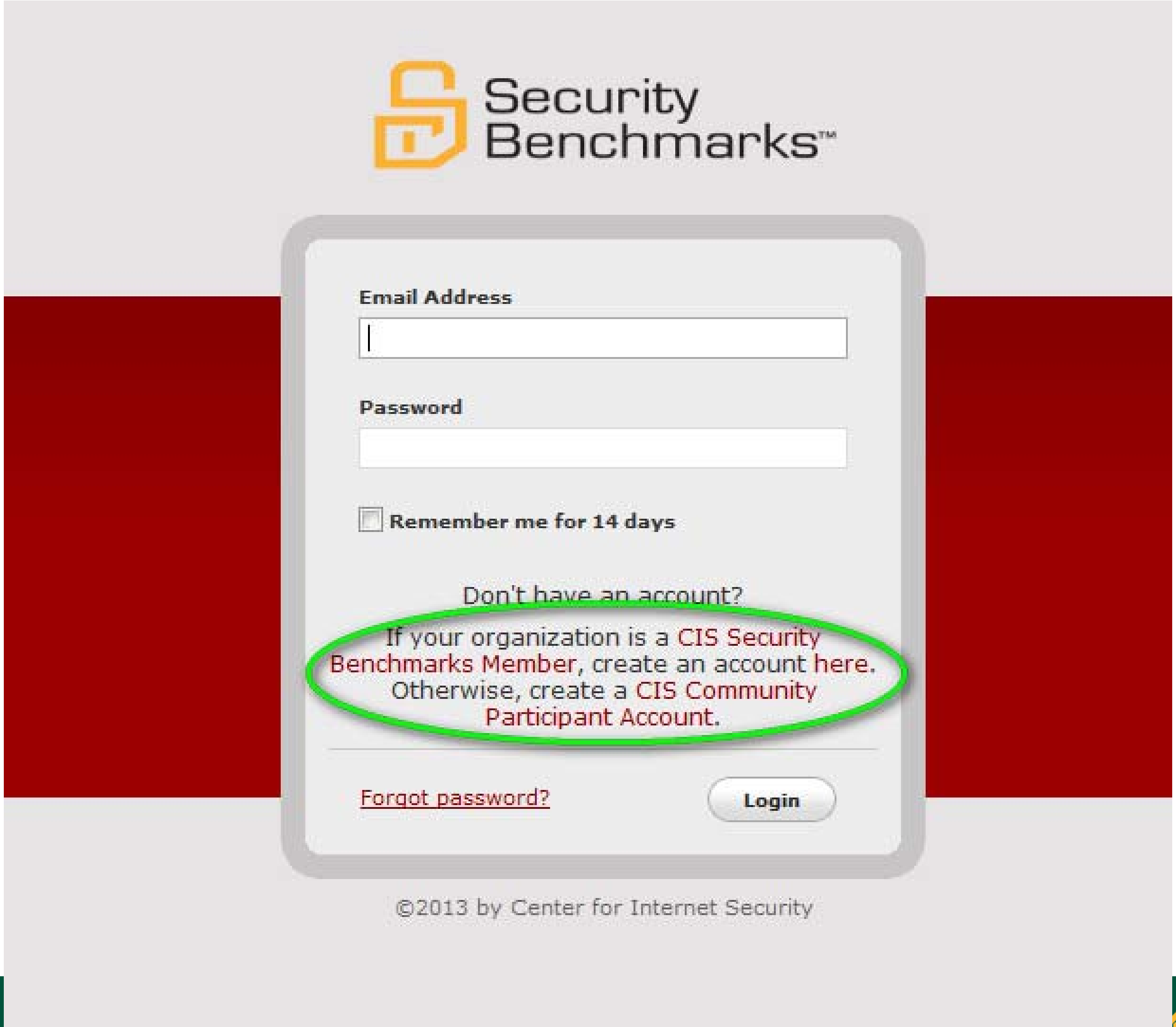
Few companies, government agencies or institutions have the expertise to develop thorough and effective security configuration policies for all of their systems. CIS Security Benchmarks membership provides access to high quality, cost-effective resources. The CIS Benchmarks are a widely-accepted standard against which to compare an organization's technical control policies. The CIS Benchmarks are based on expert consensus and are widely accepted by U.S. government agencies for **FISMA** compliance, and by auditors for compliance with **ISO standards** as well as **PCI**, **GLB**, **SOX**, **HIPAA**, and other the regulatory requirements for information security.

- Benefits of CIS Security Benchmarks Membership
- Who should become a CIS Security Benchmarks Member?
- What are the different categories of membership?
- Do colleges and universities pay discounted membership fees?
- Who are the current CIS Security Benchmarks Members?
- Membership registration forms

For more information about membership, contact CIS Security Benchmarks at members@cisecurity.org.

### Benefits of CIS Security Benchmarks Membership

# **Center for Information Security –** create account



Email Address

Password

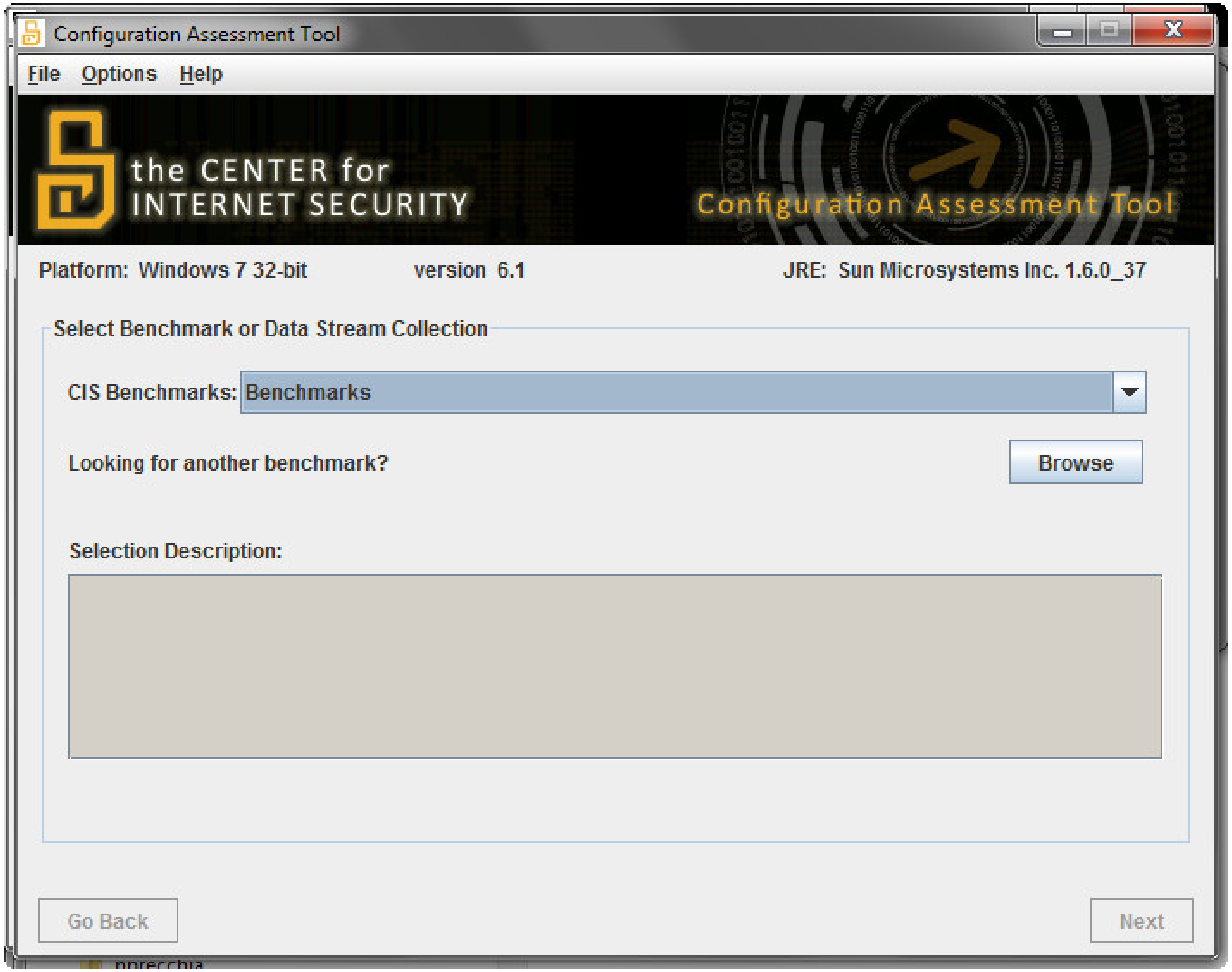
□ Remember me for 14 days

Don't have an account?

If your organization is a CIS Security Benchmarks Member, create an account here. Otherwise, create a CIS Community Participant Account.

©2013 by Center for Internet Security

# Center for Information Security – CIS-CAT


Configuration Assessment Tool
File
Options
Help
the CENTER for INTERNET SECURITY
Configuration Assessment Tool
Browse
Go Back
Next

Platform: Windows 7 32-bit    version 6.1    JRE: Sun Microsystems Inc. 1.6.0_37

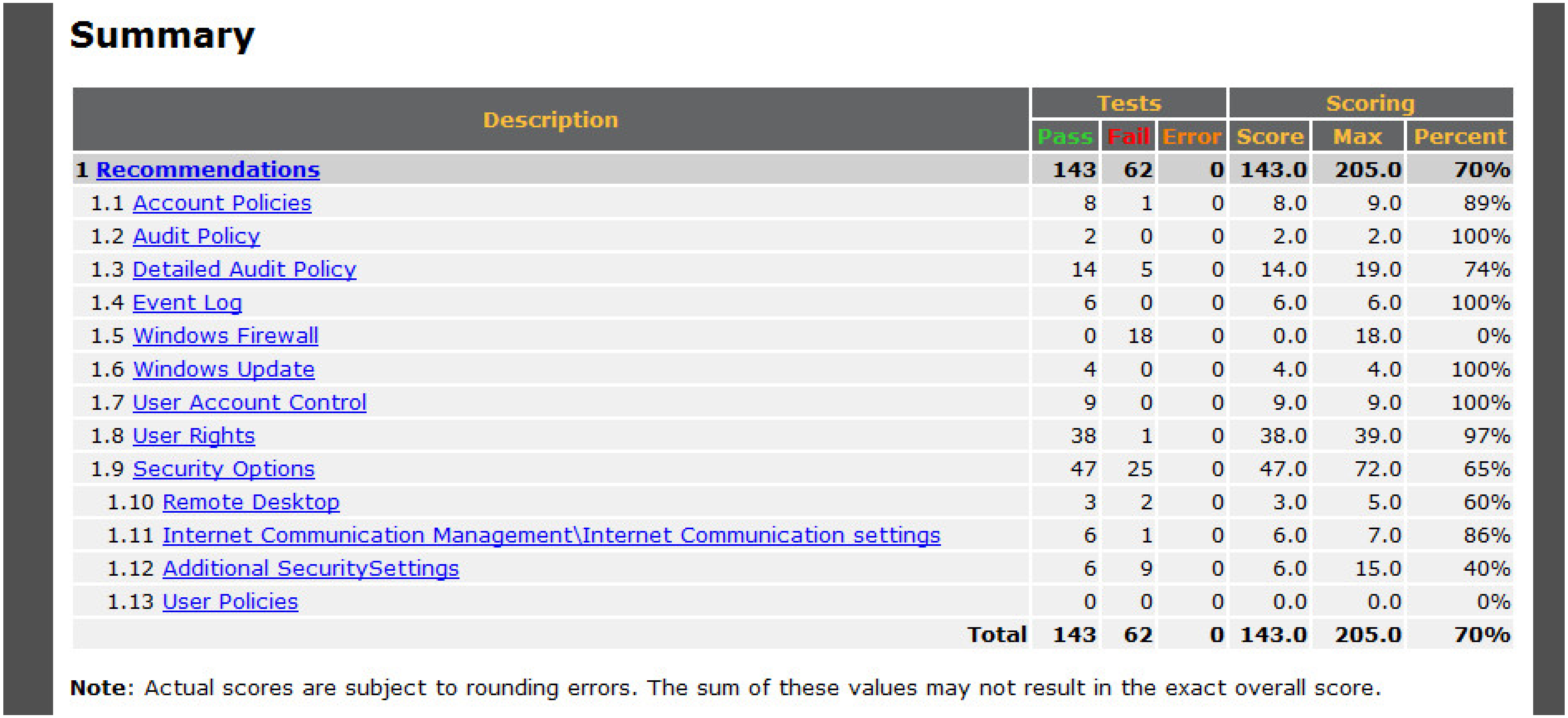
Select Benchmark or Data Stream Collection

CIS Benchmarks: Benchmarks

Looking for another benchmark?

Selection Description:

# Center for Information Security – CIS-CAT

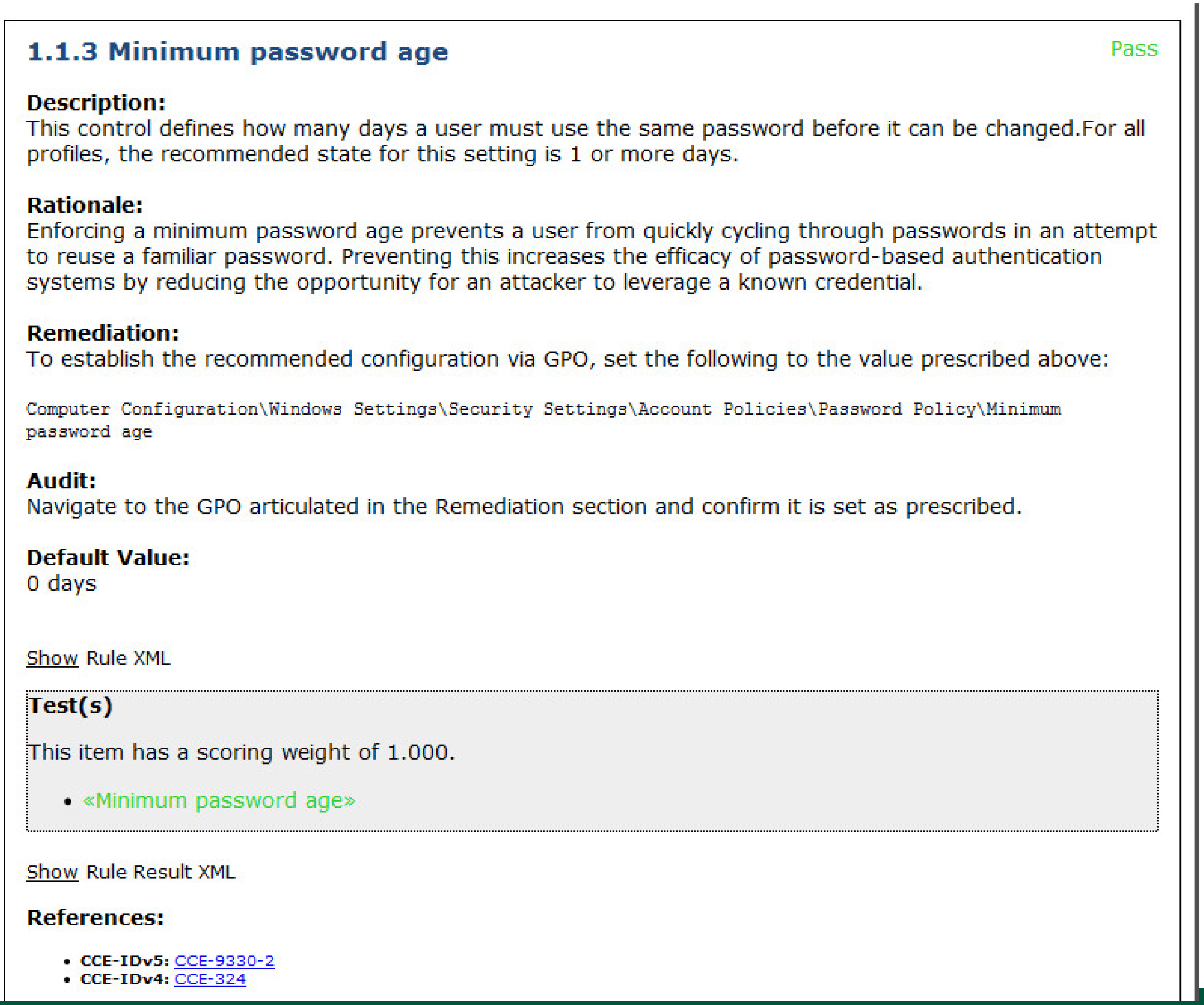


## Summary

| Description | Tests | | | Scoring | | |
|---|---|---|---|---|---|---|
| | Pass | Fail | Error | Score | Max | Percent |
| **1 Recommendations** | **143** | **62** | **0** | **143.0** | **205.0** | **70%** |
| 1.1 Account Policies | 8 | 1 | 0 | 8.0 | 9.0 | 89% |
| 1.2 Audit Policy | 2 | 0 | 0 | 2.0 | 2.0 | 100% |
| 1.3 Detailed Audit Policy | 14 | 5 | 0 | 14.0 | 19.0 | 74% |
| 1.4 Event Log | 6 | 0 | 0 | 6.0 | 6.0 | 100% |
| 1.5 Windows Firewall | 0 | 18 | 0 | 0.0 | 18.0 | 0% |
| 1.6 Windows Update | 4 | 0 | 0 | 4.0 | 4.0 | 100% |
| 1.7 User Account Control | 9 | 0 | 0 | 9.0 | 9.0 | 100% |
| 1.8 User Rights | 38 | 1 | 0 | 38.0 | 39.0 | 97% |
| 1.9 Security Options | 47 | 25 | 0 | 47.0 | 72.0 | 65% |
| 1.10 Remote Desktop | 3 | 2 | 0 | 3.0 | 5.0 | 60% |
| 1.11 Internet Communication Management\Internet Communication settings | 6 | 1 | 0 | 6.0 | 7.0 | 86% |
| 1.12 Additional SecuritySettings | 6 | 9 | 0 | 6.0 | 15.0 | 40% |
| 1.13 User Policies | 0 | 0 | 0 | 0.0 | 0.0 | 0% |
| **Total** | **143** | **62** | **0** | **143.0** | **205.0** | **70%** |

**Note:** Actual scores are subject to rounding errors. The sum of these values may not result in the exact overall score.

# Center for Information Security – CIS-CAT



### 1.1.3 Minimum password age

Pass

**Description:**
This control defines how many days a user must use the same password before it can be changed.For all profiles, the recommended state for this setting is 1 or more days.

**Rationale:**
Enforcing a minimum password age prevents a user from quickly cycling through passwords in an attempt to reuse a familiar password. Preventing this increases the efficacy of password-based authentication systems by reducing the opportunity for an attacker to leverage a known credential.

**Remediation:**
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy\Minimum
password age
```

**Audit:**
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

**Default Value:**
0 days

Show Rule XML

**Test(s)**

This item has a scoring weight of 1.000.

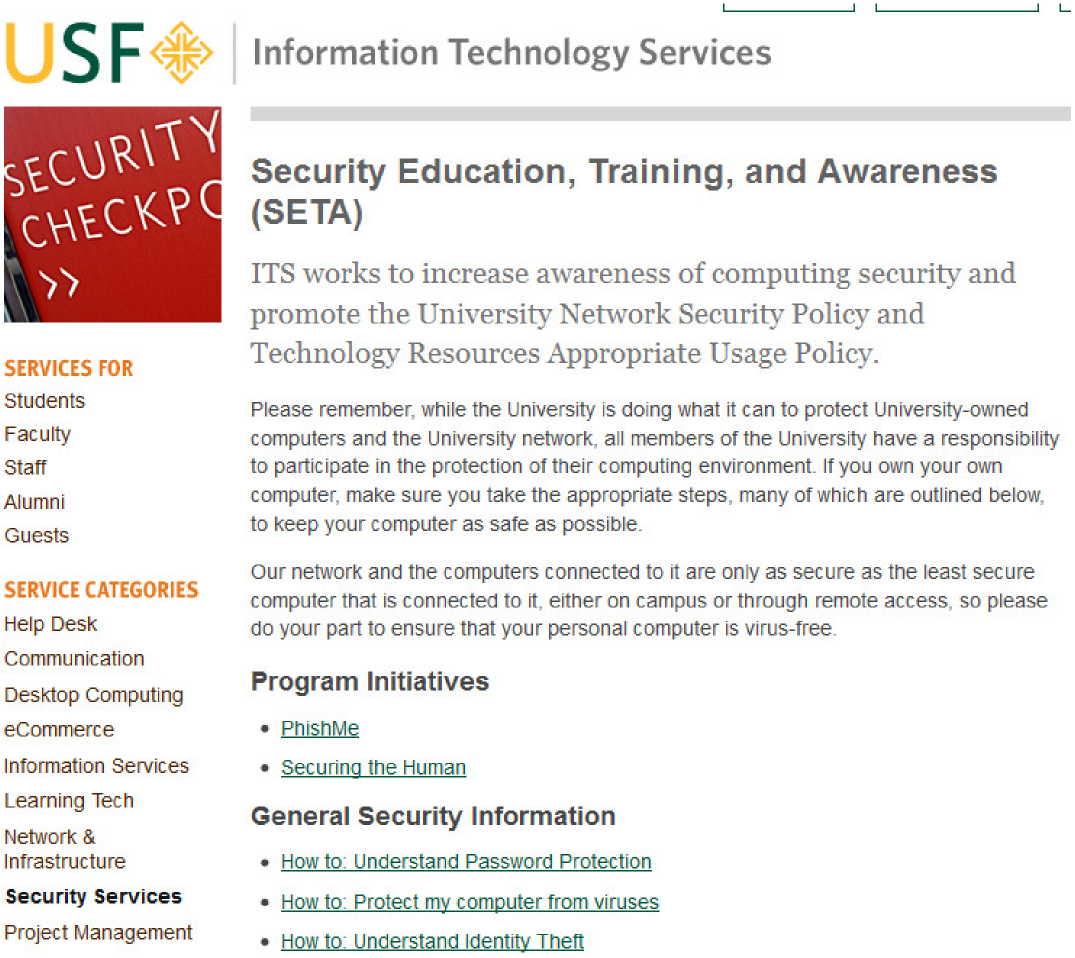
- «Minimum password age»

Show Rule Result XML

**References:**

- **CCE-IDv5:** CCE-9330-2
- **CCE-IDv4:** CCE-324

# 6) Security Education Training Awareness (SETA)



USF | Information Technology Services

SERVICES FOR

- Students
- Faculty
- Staff
- Alumni
- Guests

SERVICE CATEGORIES

- Help Desk
- Communication
- Desktop Computing
- eCommerce
- Information Services
- Learning Tech
- Network & Infrastructure
- **Security Services**
- Project Management

## Security Education, Training, and Awareness (SETA)

ITS works to increase awareness of computing security and promote the University Network Security Policy and Technology Resources Appropriate Usage Policy.

Please remember, while the University is doing what it can to protect University-owned computers and the University network, all members of the University have a responsibility to participate in the protection of their computing environment. If you own your own computer, make sure you take the appropriate steps, many of which are outlined below, to keep your computer as safe as possible.

Our network and the computers connected to it are only as secure as the least secure computer that is connected to it, either on campus or through remote access, so please do your part to ensure that your personal computer is virus-free.

### Program Initiatives

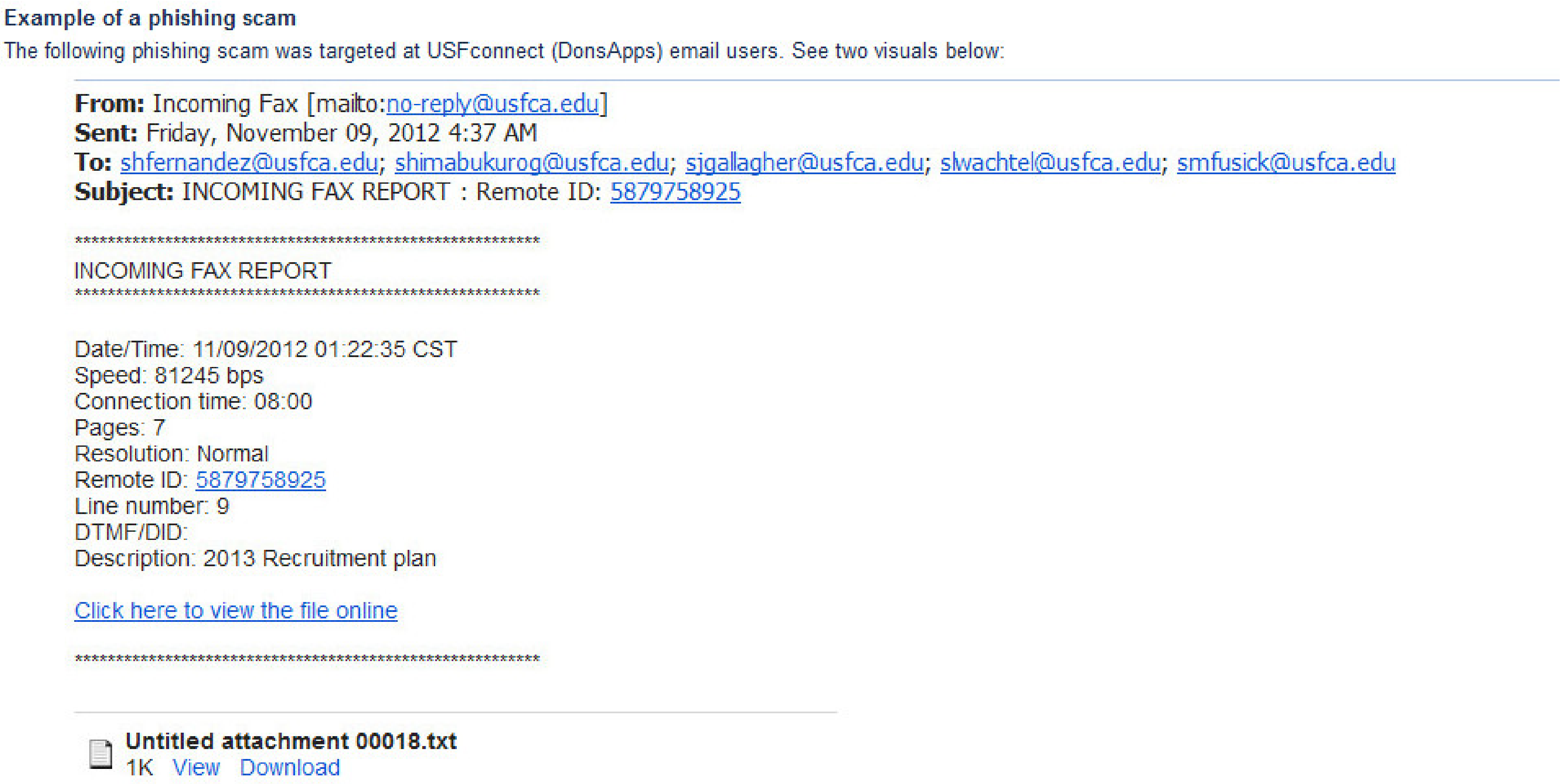
- PhishMe
- Securing the Human

### General Security Information

- How to: Understand Password Protection
- How to: Protect my computer from viruses
- How to: Understand Identity Theft

Reference: http://www.usfca.edu/its/security/seta/

# 6a) SETA - PhishMe



**Example of a phishing scam**

The following phishing scam was targeted at USFconnect (DonsApps) email users. See two visuals below:

**From:** Incoming Fax [mailto:no-reply@usfca.edu]
**Sent:** Friday, November 09, 2012 4:37 AM
**To:** shfernandez@usfca.edu; shimabukurog@usfca.edu; sjgallagher@usfca.edu; slwachtel@usfca.edu; smfusick@usfca.edu
**Subject:** INCOMING FAX REPORT : Remote ID: 5879758925

```
************************************************************
INCOMING FAX REPORT
************************************************************
```

Date/Time: 11/09/2012 01:22:35 CST
Speed: 81245 bps
Connection time: 08:00
Pages: 7
Resolution: Normal
Remote ID: 5879758925
Line number: 9
DTMF/DID:
Description: 2013 Recruitment plan

Click here to view the file online

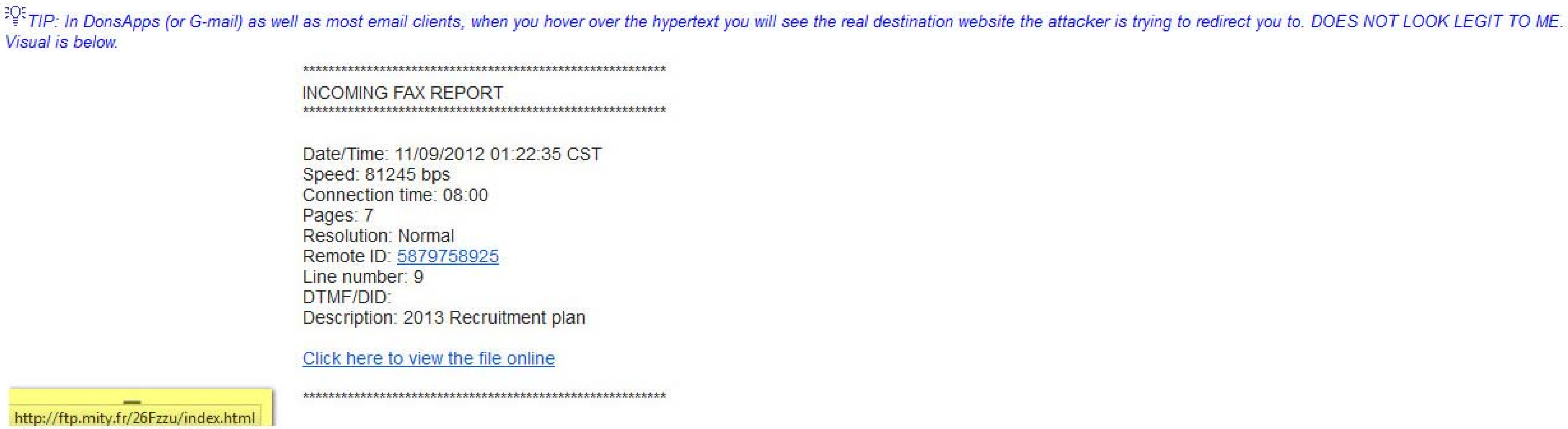
```
************************************************************
```

**Untitled attachment 00018.txt**
1K View Download

Reference: http://www.usfca.edu/its/security/seta/phishme//

UNIVERSITY OF SAN FRANCISCO

# SETA - PhishMe



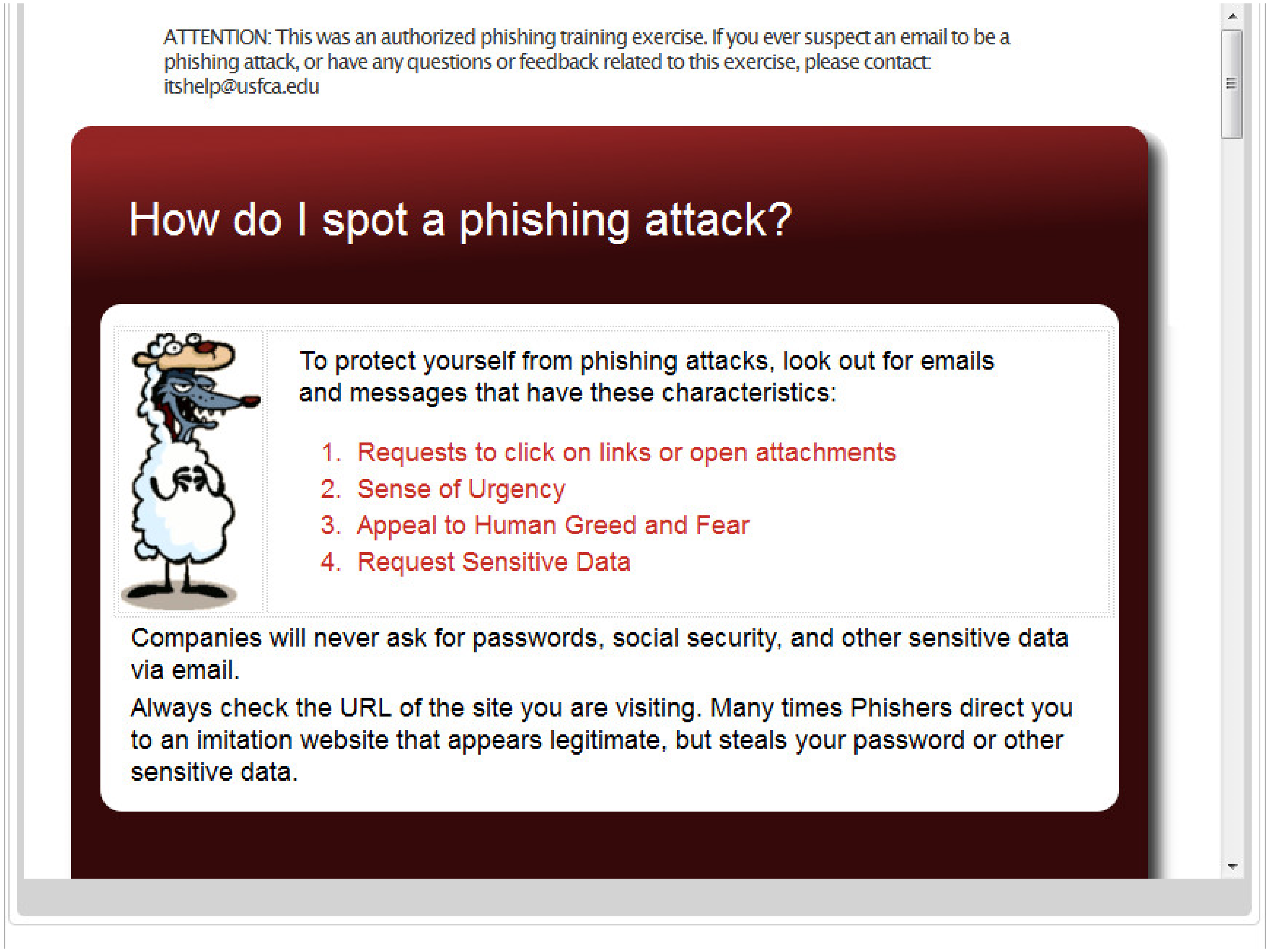
*TIP: In DonsApps (or G-mail) as well as most email clients, when you hover over the hypertext you will see the real destination website the attacker is trying to redirect you to. DOES NOT LOOK LEGIT TO ME. Visual is below.*

```
************************************************************
INCOMING FAX REPORT
************************************************************

Date/Time: 11/09/2012 01:22:35 CST
Speed: 81245 bps
Connection time: 08:00
Pages: 7
Resolution: Normal
Remote ID: 5879758925
Line number: 9
DTMF/DID:
Description: 2013 Recruitment plan

Click here to view the file online

************************************************************
```

http://ftp.mity.fr/26Fzzu/index.html

Reference: http://www.usfca.edu/its/security/seta/phishme//

# SETA - PhishMe



ATTENTION: This was an authorized phishing training exercise. If you ever suspect an email to be a phishing attack, or have any questions or feedback related to this exercise, please contact: itshelp@usfca.edu

## How do I spot a phishing attack?

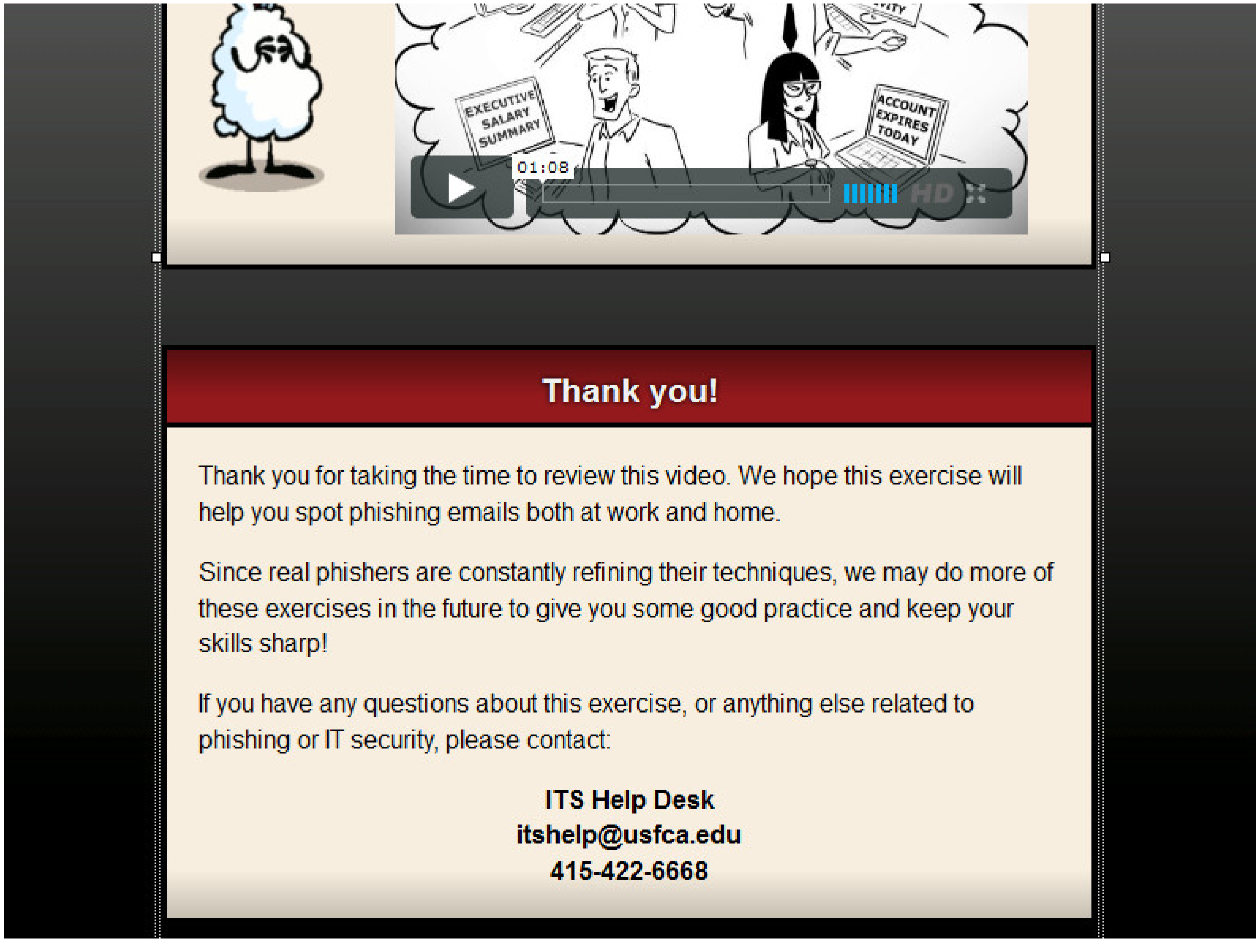
To protect yourself from phishing attacks, look out for emails and messages that have these characteristics:

1. Requests to click on links or open attachments
2. Sense of Urgency
3. Appeal to Human Greed and Fear
4. Request Sensitive Data

Companies will never ask for passwords, social security, and other sensitive data via email.

Always check the URL of the site you are visiting. Many times Phishers direct you to an imitation website that appears legitimate, but steals your password or other sensitive data.

# SETA - PhishMe



**Thank you!**

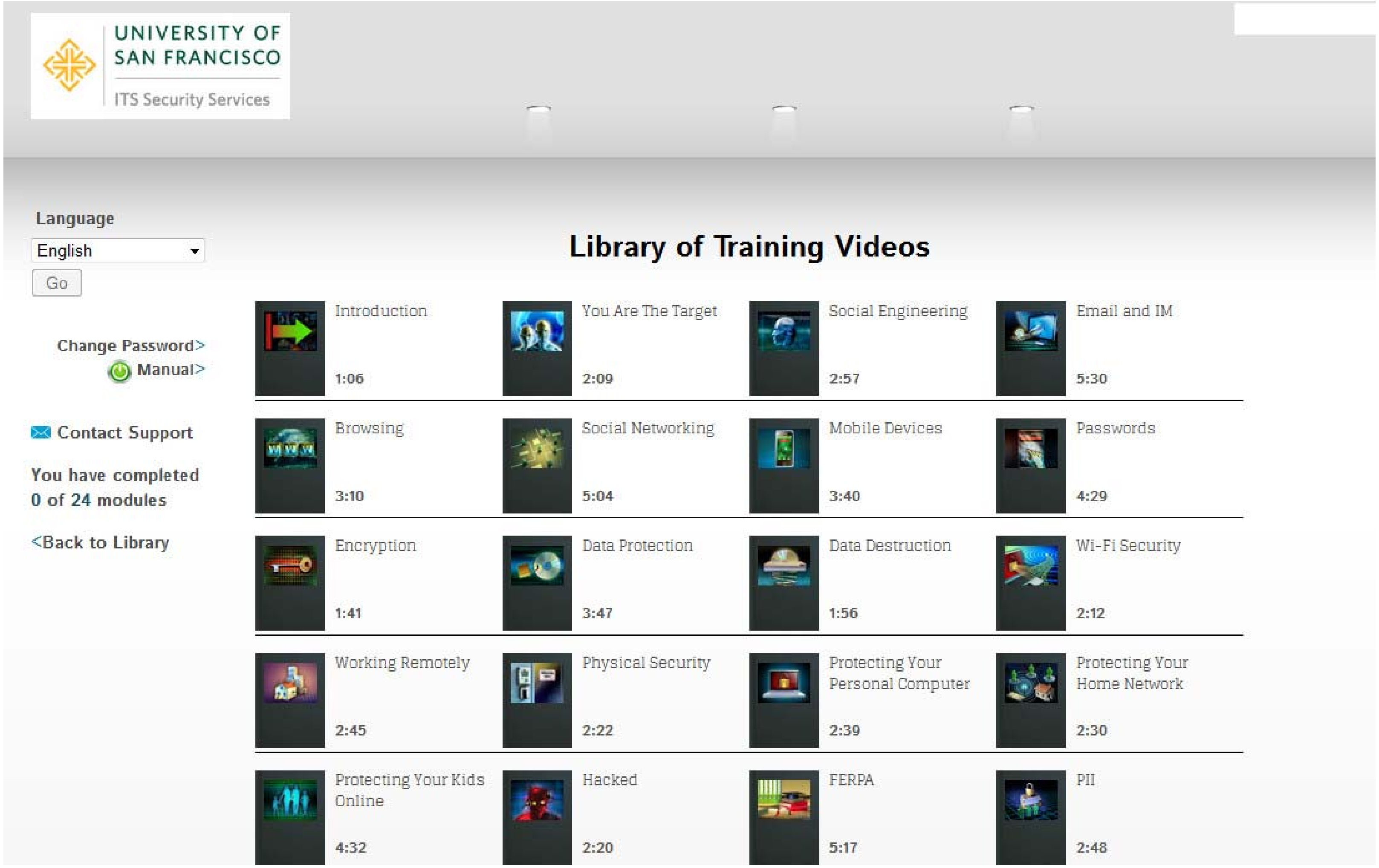
Thank you for taking the time to review this video. We hope this exercise will help you spot phishing emails both at work and home.

Since real phishers are constantly refining their techniques, we may do more of these exercises in the future to give you some good practice and keep your skills sharp!

If you have any questions about this exercise, or anything else related to phishing or IT security, please contact:

**ITS Help Desk**
**itshelp@usfca.edu**
**415-422-6668**

# 6b) SETA – STH (Securing The Human)



UNIVERSITY OF SAN FRANCISCO

ITS Security Services

Language

English

Go

Change Password>

Manual>

Contact Support

You have completed 0 of 24 modules

<Back to Library

## Library of Training Videos

| | | | |
|---|---|---|---|
| Introduction<br>1:06 | You Are The Target<br>2:09 | Social Engineering<br>2:57 | Email and IM<br>5:30 |
| Browsing<br>3:10 | Social Networking<br>5:04 | Mobile Devices<br>3:40 | Passwords<br>4:29 |
| Encryption<br>1:41 | Data Protection<br>3:47 | Data Destruction<br>1:56 | Wi-Fi Security<br>2:12 |
| Working Remotely<br>2:45 | Physical Security<br>2:22 | Protecting Your Personal Computer<br>2:39 | Protecting Your Home Network<br>2:30 |
| Protecting Your Kids Online<br>4:32 | Hacked<br>2:20 | FERPA<br>5:17 | PII<br>2:48 |

# SETA – STH (Securing The Human)

# Summary:
## USF ITS Related Countermeasures

1. **Palo Alto Networks NGFW:** *IPS/malware protection NETWORK*
2. **Network Access Control:** *endpoint protection (posture compliance)*
3. **Sophos Antivirus Security and Control:** *system & endpoint protection*
4. **QualysGuard Vulnerability Management:** *system & endpoint assessment*
5. **Center for Information Security (Sec. benchmarks):***system & endpoint assessment*
6. **Security Education Training Awareness (SETA):** *ongoing enduser training*

# Questions / Discussion