RSAC Studio

The Day My Kids Brought Home Malware

Kellman Meghu
@kellman

#RSAC

No certificate trust was harmed in the making of this presentation.


TELETOON


Barbie

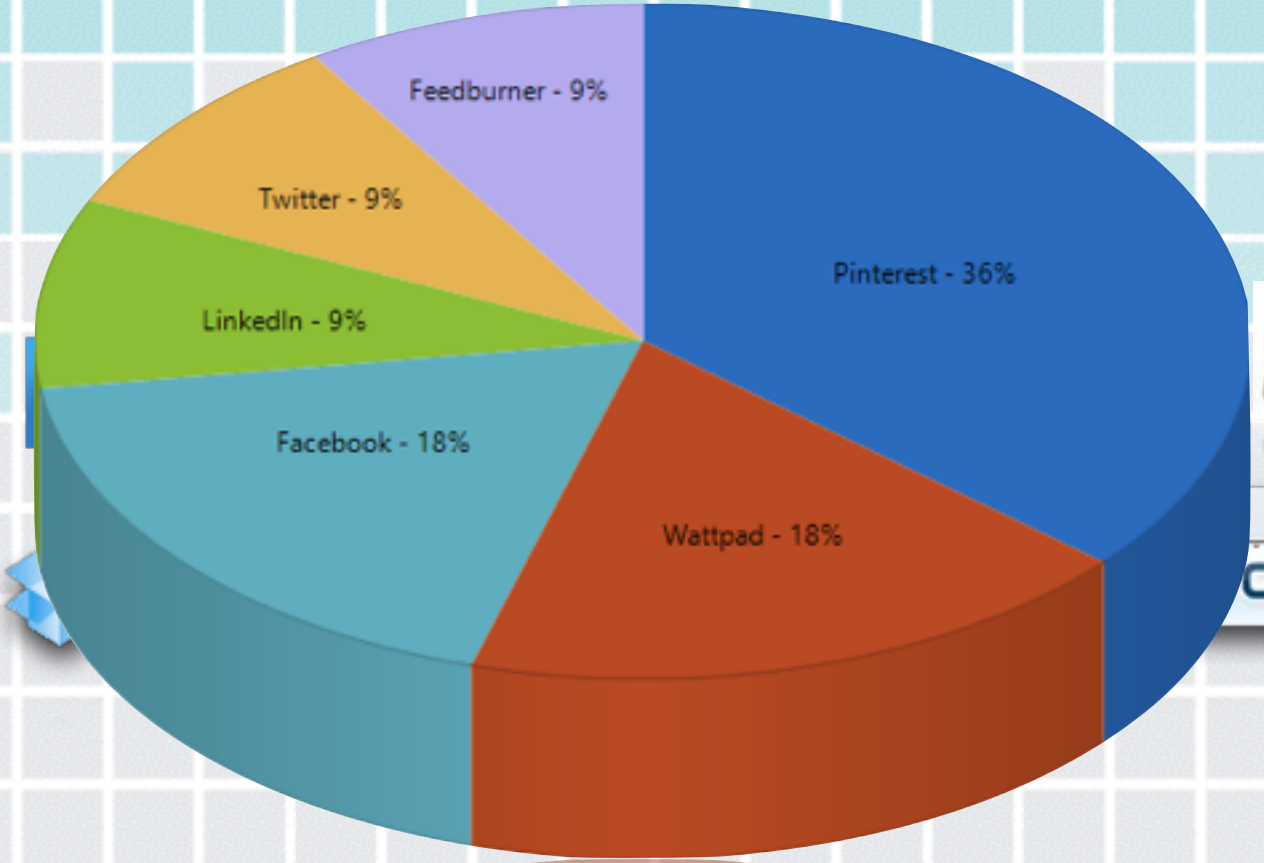

TELETOON


funnyjunk


Barbie

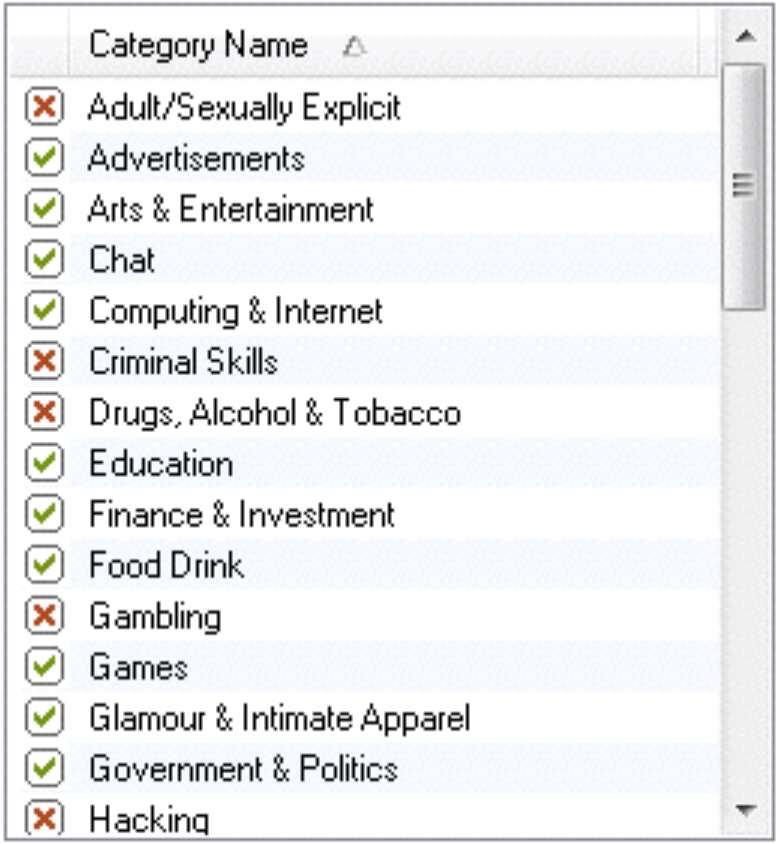
http://funnyjunk.com
accessed


ICQ
AIM
HTTP·Tunnel
skype
facebook
plaxo
Linked in
myspace
Gmail
YouTube
Dropbox
buddy


Feedburner - 9%
Twitter - 9%
LinkedIn - 9%
Facebook - 18%
Pinterest - 36%
Wattpad - 18%


ARIZONA
SOLD
FOR SALE
THE GRAND CANYON STATE
WELCOMES YOU

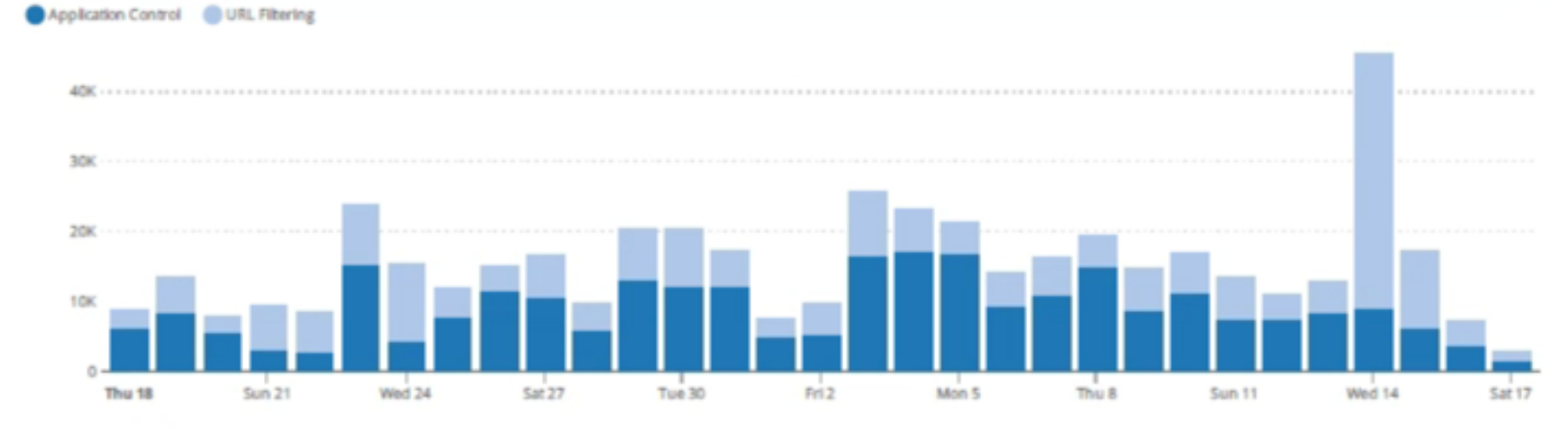
Categories:



Legend:

- Allow category
- Block category

Activity Timeline

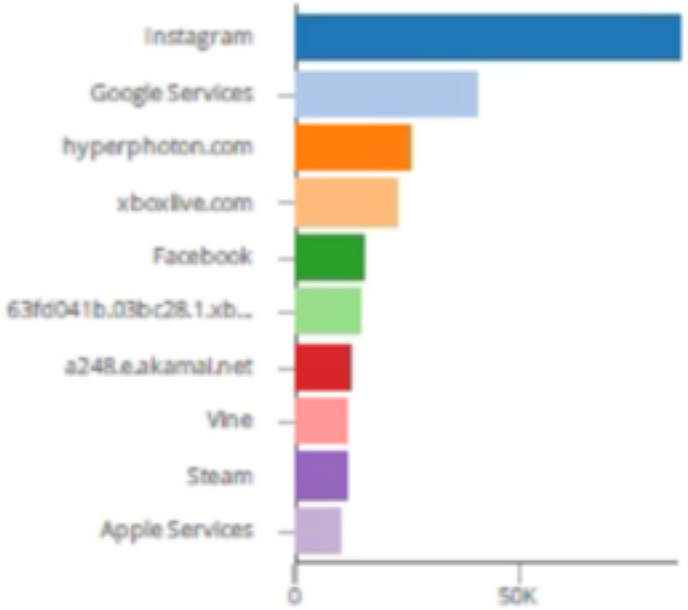


APPLICATION & URL FILTERING Report

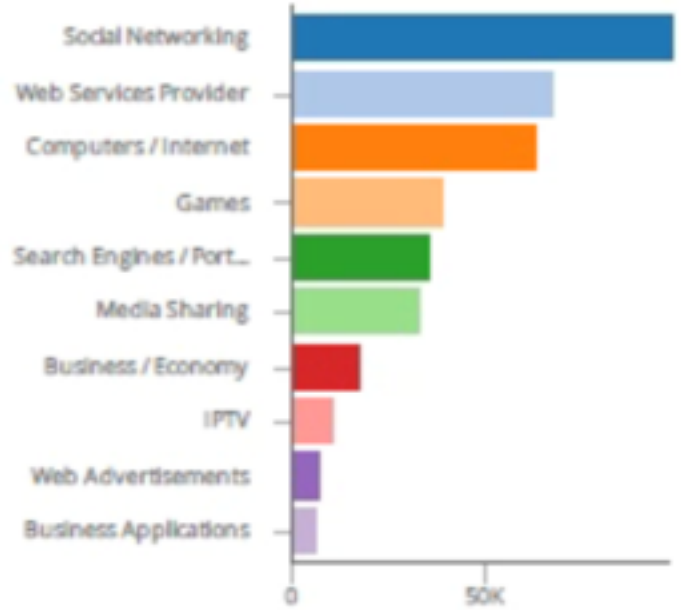
Dec 18, 2014 12:00 AM - **Jan 17, 2015** 1:01 PM

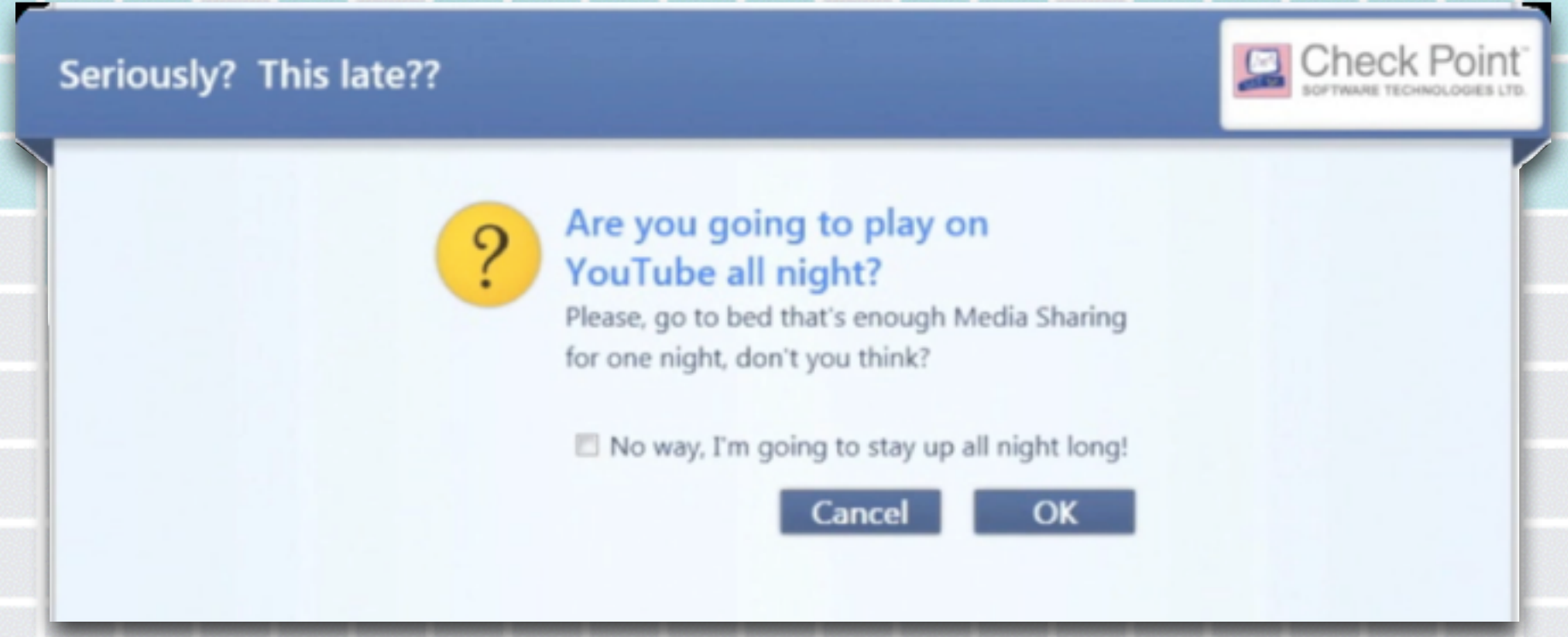
General Activity

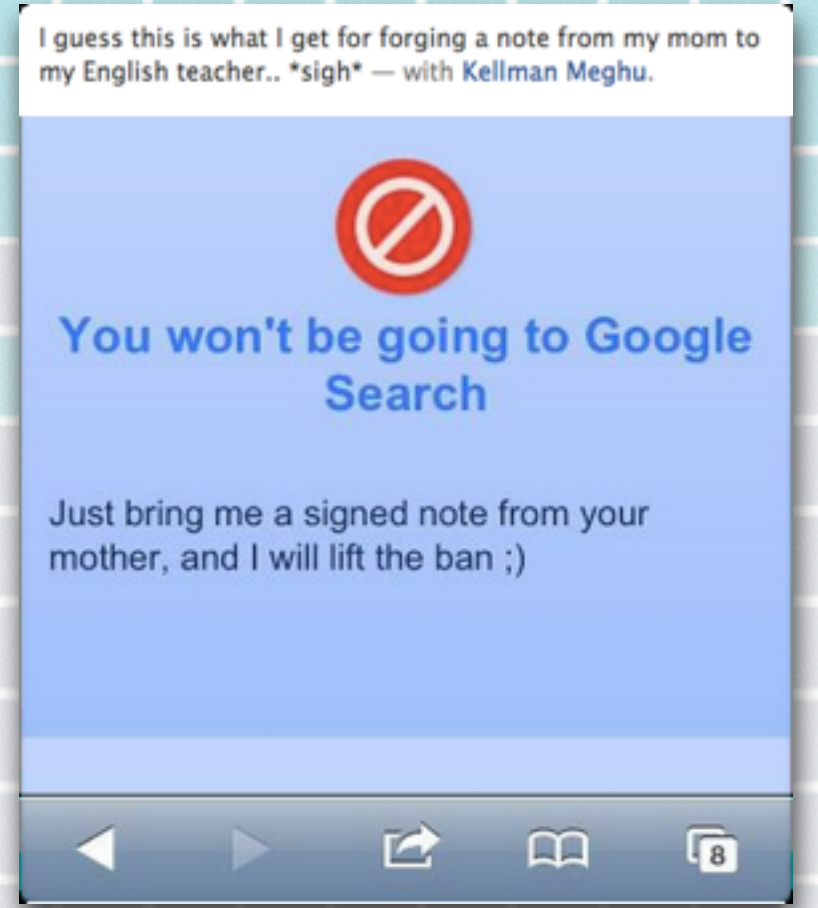
Top Applications

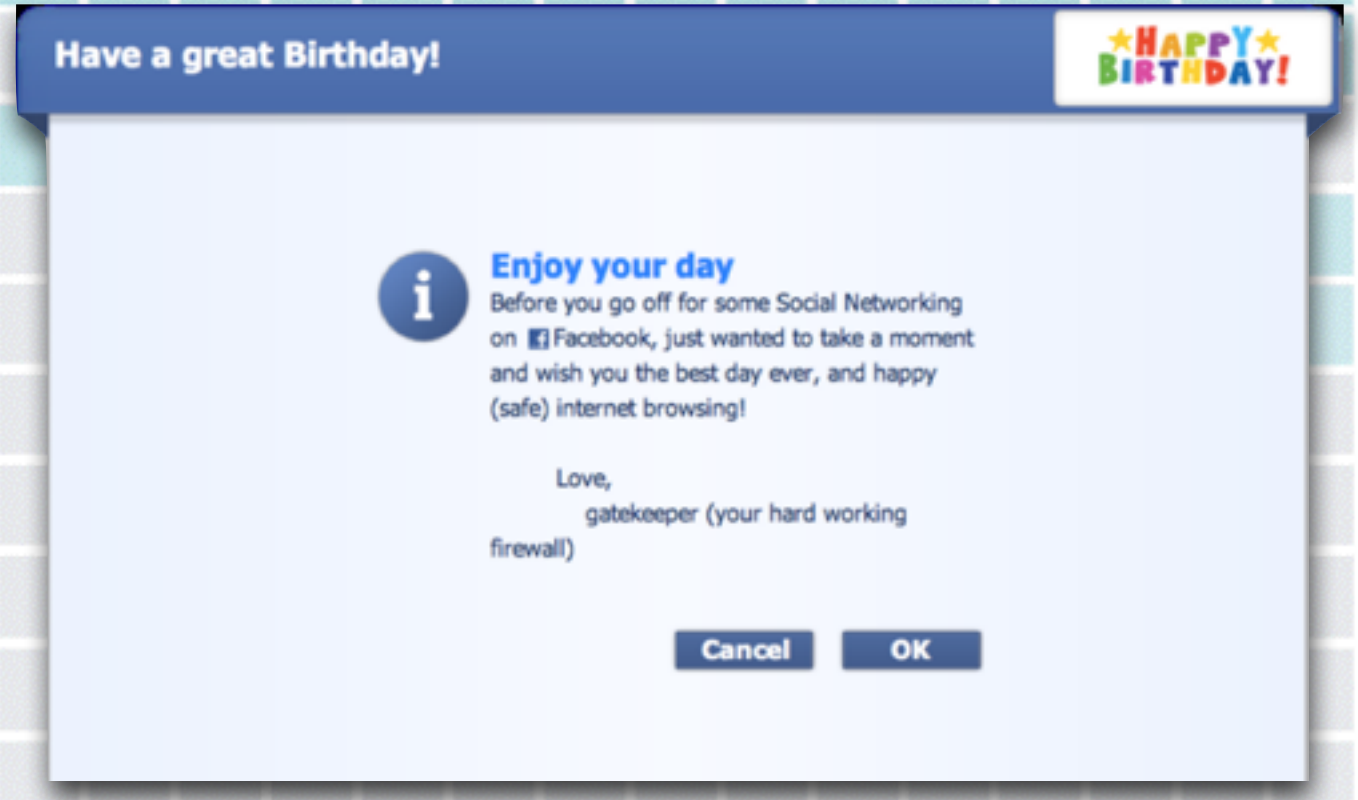


Top Categories

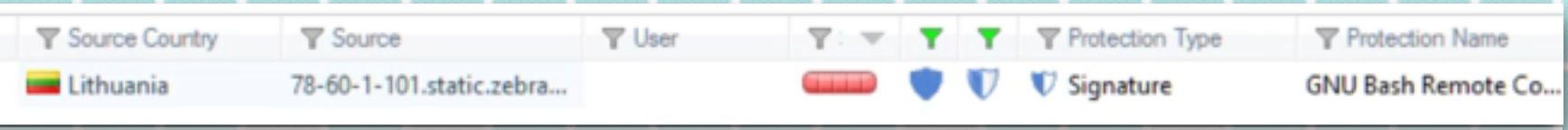



Seriously? This late??
Check Point
SOFTWARE TECHNOLOGIES LTD.
Are you going to play on YouTube all night?
Please, go to bed that's enough Media Sharing for one night, don't you think?
No way, I'm going to stay up all night long!
Cancel
OK


I guess this is what I get for forging a note from my mom to my English teacher.. *sigh* — with Kellman Meghu.
You won't be going to Google Search
Just bring me a signed note from your mother, and I will lift the ban ;)
8

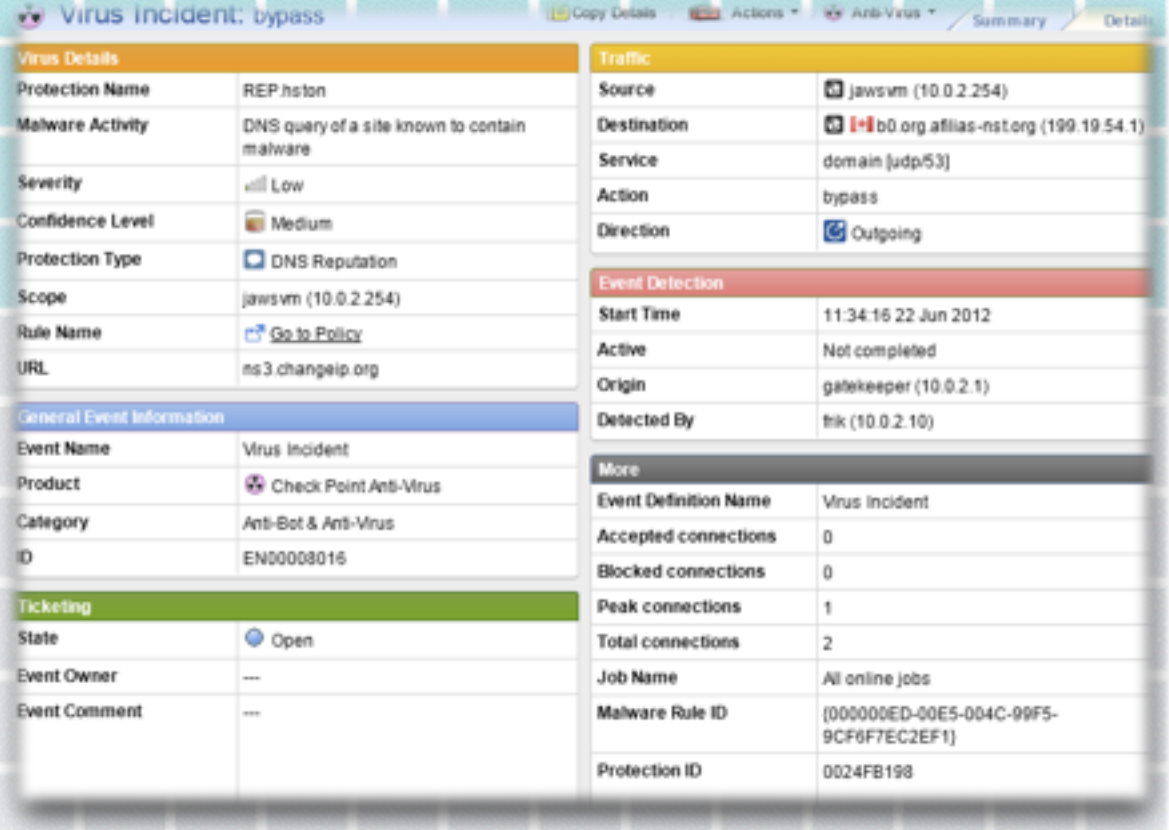

Have a great Birthday!
HAPPY BIRTHDAY!
Enjoy your day
Before you go off for some Social Networking on Facebook, just wanted to take a moment and wish you the best day ever, and happy (safe) internet browsing!
Love,
gatekeeper (your hard working firewall)
Cancel
OK


HomeNet
PIR8
sick beard
FreeNAS
tv
tv



More	
URL	http://99.253.4.27/
Event Name	IPS
WEB Client Type	Other: () { : } echo BANG: $(cat /etc/passwd)
Firewall Rule UID	73A87676-1346-4D64-BF13-E3E359B65DA1
Protection ID	asm_dynamic_prop_ZDBASHRCE

Anti-Bot & Anti-Virus / More / By Protection Name (By Number of Events)


Virus Incident: bypass
Copy Details
Actions
Anti-Virus
Summary
Details
Virus Details
Protection Name
REP.hston
Malware Activity
DNS query of a site known to contain malware
Severity
Low
Confidence Level
Medium
Protection Type
DNS Reputation
Scope
jawsvm (10.0.2.254)
Rule Name
Go to Policy
URL
ns3.changeip.org
General Event Information
Event Name
Virus Incident
Product
Check Point Anti-Virus
Category
Anti-Bot & Anti-Virus
ID
EN00008016
Ticketing
State
Open
Event Owner

Event Comment

Traffic
Source
jawsvm (10.0.2.254)
Destination
b0.org.afilias-nst.org (199.19.54.1)
Service
domain [udp/53]
Action
bypass
Direction
Outgoing
Event Detection
Start Time
11:34:16 22 Jun 2012
Active
Not completed
Origin
gatekeeper (10.0.2.1)
Detected By
frik (10.0.2.10)
More
Event Definition Name
Virus Incident
Accepted connections
0
Blocked connections
0
Peak connections
1
Total connections
2
Job Name
All online jobs
Malware Rule ID
{000000ED-00E5-004C-99F5-9CF6F7EC2EF1}
Protection ID
0024FB198

Virus Incident: bypass

jawsvm (10.0.2.254)

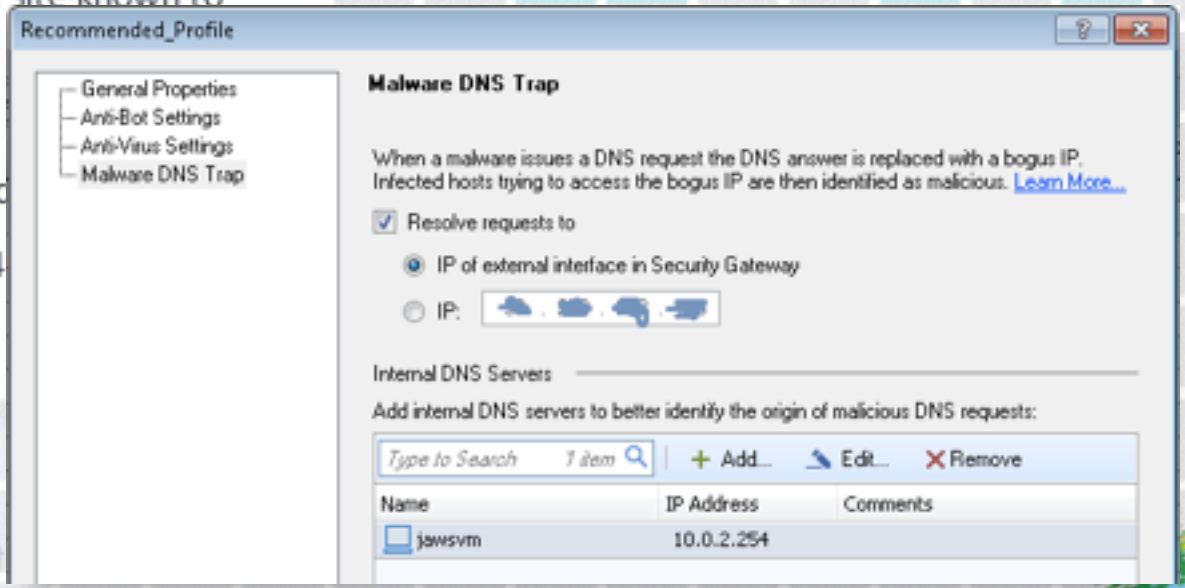
REP.hston (DNS Reputation) bypassed

DNS query of a site known to contain malware

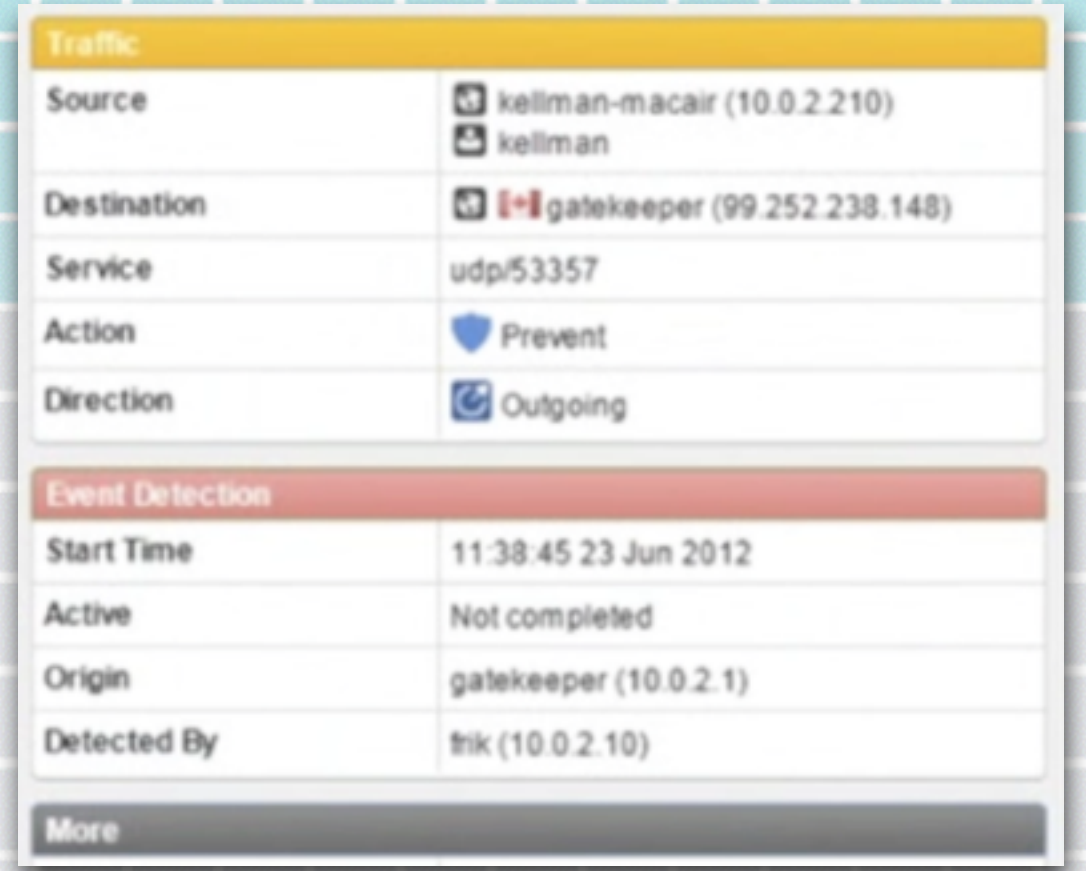
Low Severity

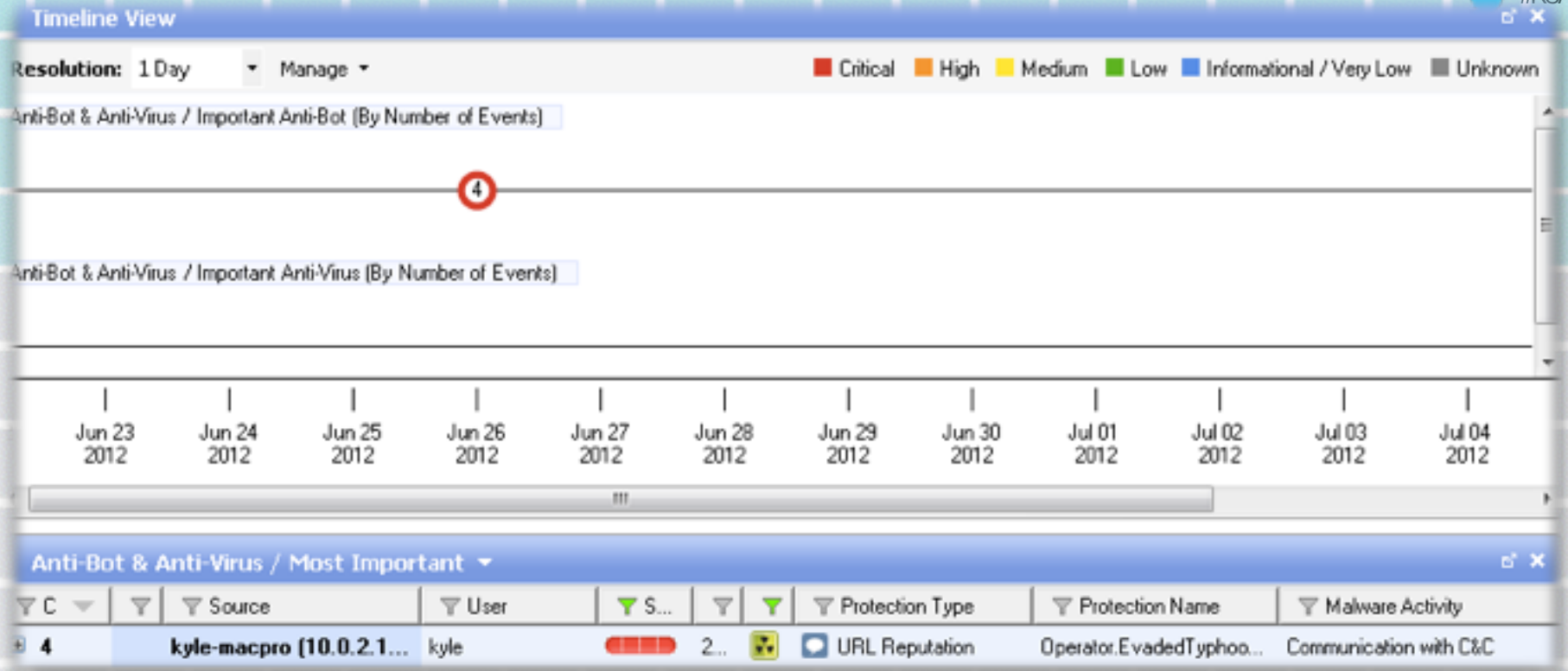
Medium Confid

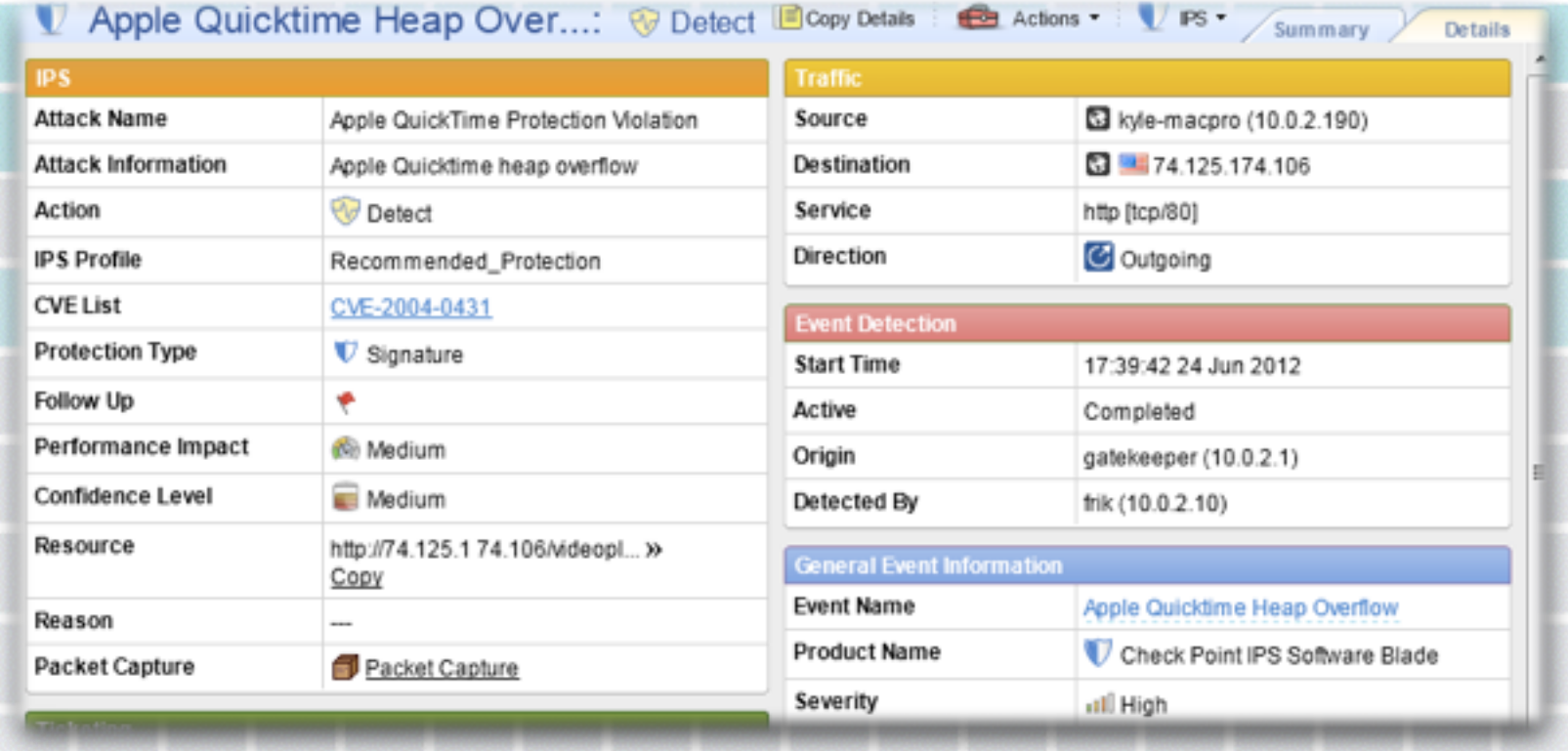
Today at 11:34



Anti-Bot & Anti-Virus / More / By Protection Name (By Number of Events)


Traffic
Source
kellman-macair (10.0.2.210)
kellman
Destination
gatekeeper (99.252.238.148)
Service
udp/53357
Action
Prevent
Direction
Outgoing
Event Detection
Start Time
11:38:45 23 Jun 2012
Active
Not completed
Origin
gatekeeper (10.0.2.1)
Detected By
frik (10.0.2.10)
More


Timeline View
Resolution: 1 Day
Manage
Critical
High
Medium
Low
Informational / Very Low
Unknown
Anti-Bot & Anti-Virus / Important Anti-Bot (By Number of Events)
4
Anti-Bot & Anti-Virus / Important Anti-Virus (By Number of Events)
Jun 23 2012
Jun 24 2012
Jun 25 2012
Jun 26 2012
Jun 27 2012
Jun 28 2012
Jun 29 2012
Jun 30 2012
Jul 01 2012
Jul 02 2012
Jul 03 2012
Jul 04 2012
Anti-Bot & Anti-Virus / Most Important
C
Source
User
S...
Protection Type
Protection Name
Malware Activity
4
kyle-macpro (10.0.2.1...
kyle
2...
URL Reputation
Operator.EvadedTyphoo...
Communication with C&C


Apple Quicktime Heap Over...:
Detect
Copy Details
Actions
IPS
Summary
Details
IPS
Attack Name
Apple QuickTime Protection Violation
Attack Information
Apple Quicktime heap overflow
Action
Detect
IPS Profile
Recommended_Protection
CVE List
CVE-2004-0431
Protection Type
Signature
Follow Up
Performance Impact
Medium
Confidence Level
Medium
Resource
http://74.125.1 74.106/videopl... »
Copy
Reason

Packet Capture
Packet Capture
Traffic
Source
kyle-macpro (10.0.2.190)
Destination
74.125.174.106
Service
http [tcp/80]
Direction
Outgoing
Event Detection
Start Time
17:39:42 24 Jun 2012
Active
Completed
Origin
gatekeeper (10.0.2.1)
Detected By
frik (10.0.2.10)
General Event Information
Event Name
Apple Quicktime Heap Overflow
Product Name
Check Point IPS Software Blade
Severity
High

Threat Description:

There is an integer overflow in the media file parsing mechanism within Apple QuickTime, a tool that allows users to play, create, and deliver multimedia.

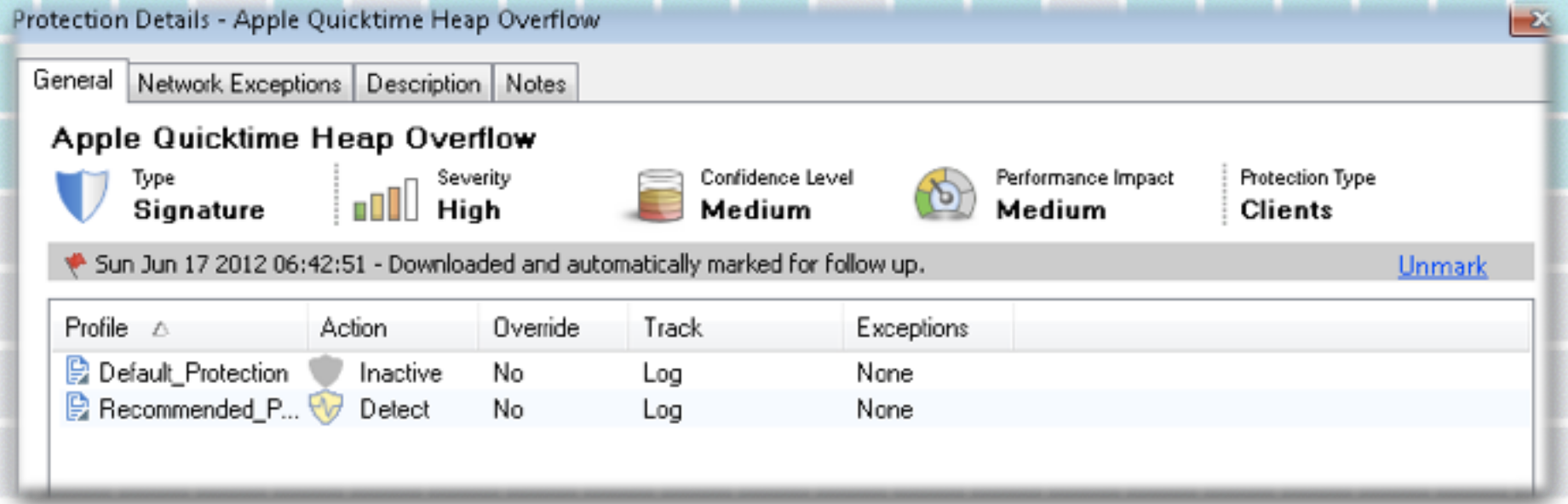
There is a vulnerability in the media file parser within Apple QuickTime. It is possible for a remote attacker to execute arbitrary code on the victim's computer in the context of the victim user when they open a malicious QuickTime file.

It is expected that a vulnerable QuickTime program will terminate upon the launch of a malicious QuickTime file. The QuickTime application must be restarted for renewed QuickTime accessibility.

However, it is possible that a specially crafted QuickTime file will facilitate the execution of arbitrary code on the remote server in the context of the user opening or viewing the malicious file.

IPS Protection:

This protection will detect and block attempts to exploit this vulnerability


Protection Details - Apple Quicktime Heap Overflow
General
Network Exceptions
Description
Notes
Apple Quicktime Heap Overflow
Type
Signature
Severity
High
Confidence Level
Medium
Performance Impact
Medium
Protection Type
Clients
Sun Jun 17 2012 06:42:51 - Downloaded and automatically marked for follow up.
Unmark
Profile
Action
Override
Track
Exceptions
Default_Protection
Inactive
No
Log
None
Recommended_P...
Detect
No
Log
None

SensorNET

Bot addresses

Malware Sites

Signatures

Check Point ThreatCloud™

Check Point
SOFTWARE TECHNOLOGIES LTD.

Cindy

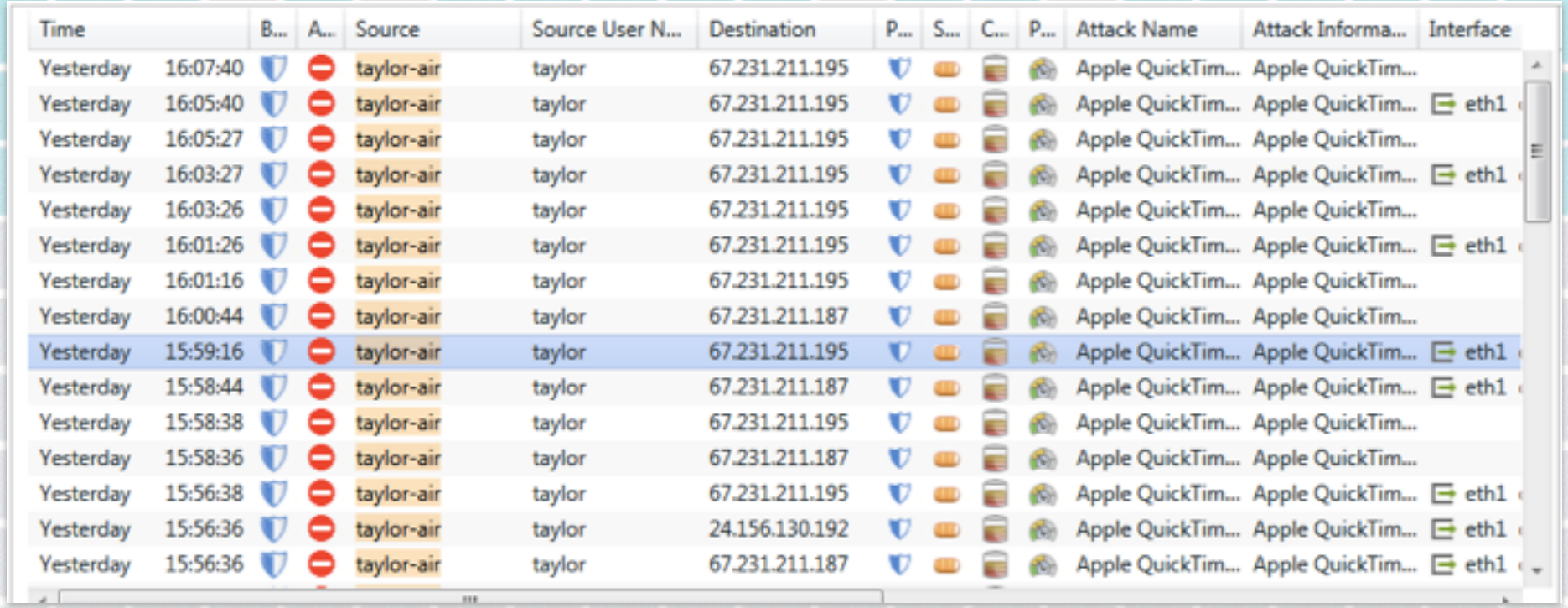
To: Kellman Meghu

Fwd: [redacted] VIP Server Information

Check out this new little scam. Now, if I didn't know BETTER I may click that link several times over, but I DO KNOW BETTER.

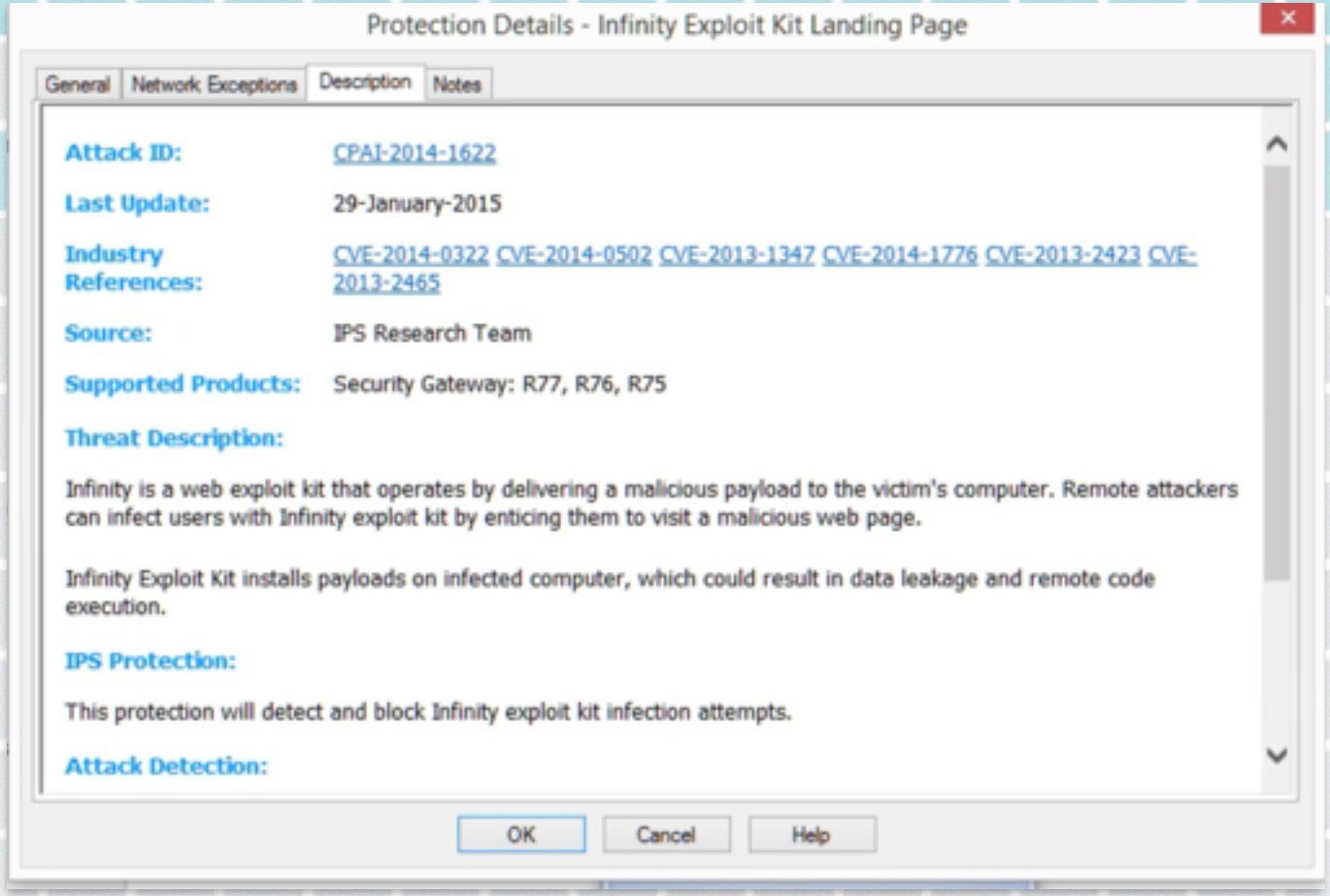
---------- Forwarded message ----------

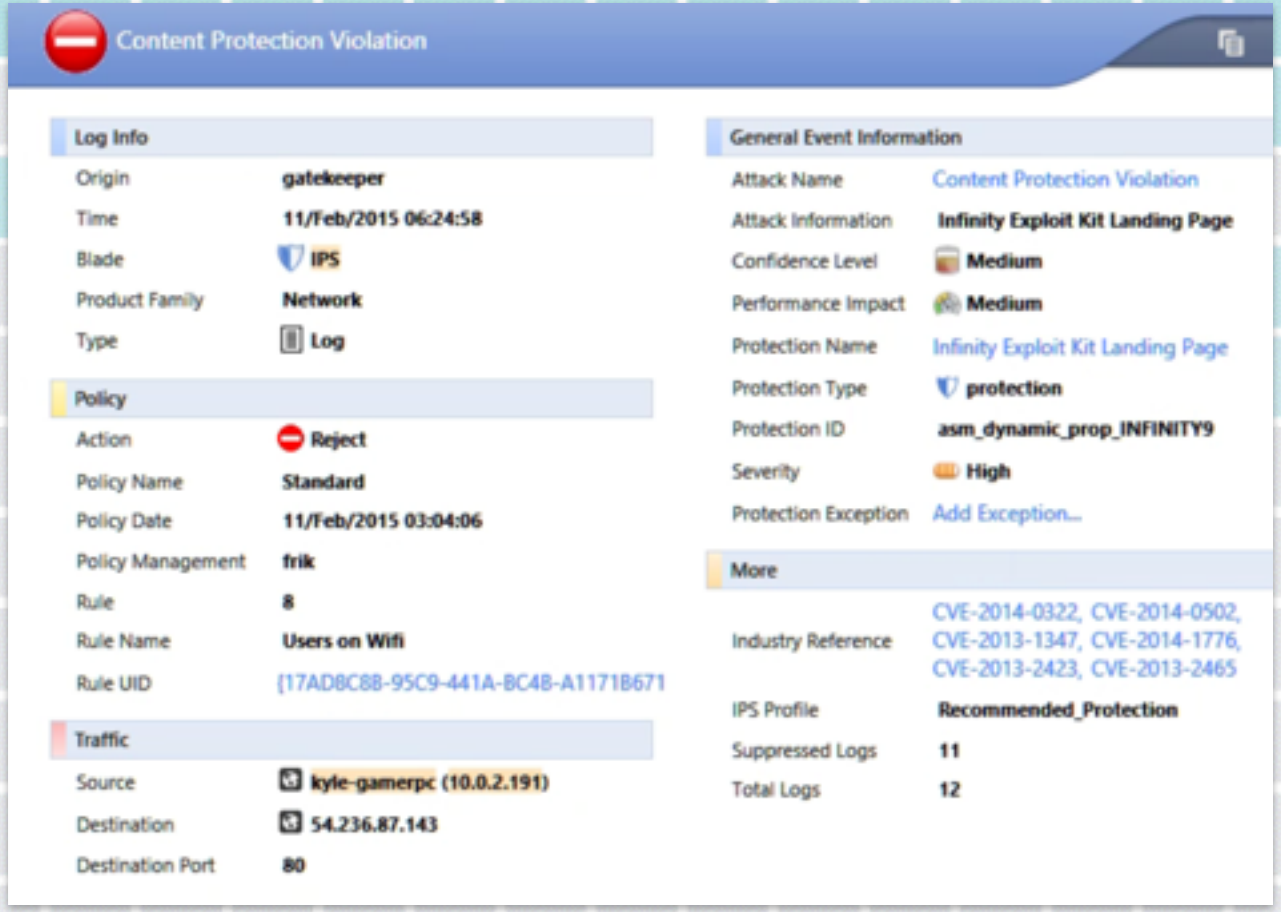

Log Details
Apple QuickTime Protection Violation
Log Info
Origin gatekeeper
Time Yesterday 16:01:26
Blade IPS
Product Family Network
Type Log
Policy
Action Reject
Policy Name Standard
Policy Date 15/Dec/2013 21:36:01
Policy Management tnk
Rule 7
Rule Name Users on Wifi
Rule UID {17AD8C88-95C9-441A-BC48-A117186729
Traffic
Source taylor-air (10.0.2.182)
Destination 67.231.211.195
Service http (TCP/80)
Interface Direction outbound
Interface Name eth1
Protocol TCP (6)
Destination Port 80
Source Port 58048
Service Name http
Source User Name taylor
User taylor
General Event Information
Attack Name Apple QuickTime Protection Violation
Attack Information Apple QuickTime Targa file buffer overflow
Confidence Level Medium
Performance Impact Medium
Protection Name Apple QuickTime Targa File Buffer Overflow
Protection Type protection
Protection ID asm_dynamic_prop_AMSN20121108_11
Severity High
Protection Exception Add Exception...
Details
Resource http://userimages-akm.imvu.com/productdata/14027964/2/eyebrows001_alpha.tga
More
Industry Reference CVE-2012-3755
Proxy Source IP 10.0.2.182
Reject ID 52acc726-10002-182000a-c0000001
IPS Profile Recommended_Protection
Session ID 71c916d5
Update Version 634158224

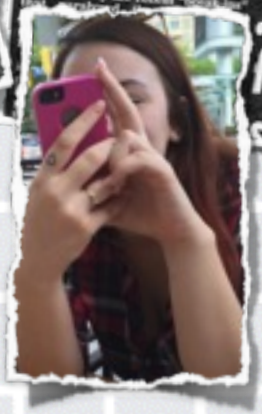


Time	B...	A...	Source	Source User N...	Destination	P...	S...	C...	P...	Attack Name	Attack Informa...	Interface
Yesterday 16:07:40			taylor-air	taylor	67.231.211.195					Apple QuickTim...	Apple QuickTim...	
Yesterday 16:05:40			taylor-air	taylor	67.231.211.195					Apple QuickTim...	Apple QuickTim...	eth1
Yesterday 16:05:27			taylor-air	taylor	67.231.211.195					Apple QuickTim...	Apple QuickTim...	
Yesterday 16:03:27			taylor-air	taylor	67.231.211.195					Apple QuickTim...	Apple QuickTim...	eth1
Yesterday 16:03:26			taylor-air	taylor	67.231.211.195					Apple QuickTim...	Apple QuickTim...	
Yesterday 16:01:26			taylor-air	taylor	67.231.211.195					Apple QuickTim...	Apple QuickTim...	eth1
Yesterday 16:01:16			taylor-air	taylor	67.231.211.195					Apple QuickTim...	Apple QuickTim...	
Yesterday 16:00:44			taylor-air	taylor	67.231.211.187					Apple QuickTim...	Apple QuickTim...	
Yesterday 15:59:16			taylor-air	taylor	67.231.211.195					Apple QuickTim...	Apple QuickTim...	eth1
Yesterday 15:58:44			taylor-air	taylor	67.231.211.187					Apple QuickTim...	Apple QuickTim...	eth1
Yesterday 15:58:38			taylor-air	taylor	67.231.211.195					Apple QuickTim...	Apple QuickTim...	
Yesterday 15:58:36			taylor-air	taylor	67.231.211.187					Apple QuickTim...	Apple QuickTim...	
Yesterday 15:56:38			taylor-air	taylor	67.231.211.195					Apple QuickTim...	Apple QuickTim...	eth1
Yesterday 15:56:36			taylor-air	taylor	24.156.130.192					Apple QuickTim...	Apple QuickTim...	eth1
Yesterday 15:56:36			taylor-air	taylor	67.231.211.187					Apple QuickTim...	Apple QuickTim...	eth1


Express yourself in the world's largest 3D Chat and Dress-Up community!
Member Login
85,707 people online now
in 91 different countries!
Sign in with:
Choose Your FREE Avatar
Over 3 Million people
like IMVU on Facebook!
FREE


Protection Details - Infinity Exploit Kit Landing Page
General
Network Exceptions
Description
Notes
Attack ID:
CPAI-2014-1622
Last Update:
29-January-2015
Industry References:
CVE-2014-0322 CVE-2014-0502 CVE-2013-1347 CVE-2014-1776 CVE-2013-2423 CVE-2013-2465
Source:
IPS Research Team
Supported Products:
Security Gateway: R77, R76, R75
Threat Description:
Infinity is a web exploit kit that operates by delivering a malicious payload to the victim's computer. Remote attackers can infect users with Infinity exploit kit by enticing them to visit a malicious web page.
Infinity Exploit Kit installs payloads on infected computer, which could result in data leakage and remote code execution.
IPS Protection:
This protection will detect and block Infinity exploit kit infection attempts.
Attack Detection:
OK
Cancel
Help


Content Protection Violation
Log Info
Origin gatekeeper
Time 11/Feb/2015 06:24:58
Blade IPS
Product Family Network
Type Log
Policy
Action Reject
Policy Name Standard
Policy Date 11/Feb/2015 03:04:06
Policy Management frik
Rule 8
Rule Name Users on Wifi
Rule UID {17AD8C88-95C9-441A-BC4B-A1171B671
Traffic
Source kyle-gamerpc (10.0.2.191)
Destination 54.236.87.143
Destination Port 80
General Event Information
Attack Name Content Protection Violation
Attack Information Infinity Exploit Kit Landing Page
Confidence Level Medium
Performance Impact Medium
Protection Name Infinity Exploit Kit Landing Page
Protection Type protection
Protection ID asm_dynamic_prop_INFINITY9
Severity High
Protection Exception Add Exception...
More
Industry Reference CVE-2014-0322, CVE-2014-0502, CVE-2013-1347, CVE-2014-1776, CVE-2013-2423, CVE-2013-2465
IPS Profile Recommended_Protection
Suppressed Logs 11
Total Logs 12



The Day My Kids Brought Home Malware

Kellman Meghu

@kellman

Check Point
SOFTWARE TECHNOLOGIES LTD.