



astaro
internet security

Astaro Corporation

Trends in Network Security

David Rogers
Director of Sales & OEM
Astaro Corporation
Office: 781-345-5000
Fax: 781-345-5100
Email: drogers@astaro.com

web

- Surf Protection
- Spyware Protection
- Virus Protection

network

- Virus Protection
- Spam Protection
- Phishing Protection

e-mail

- Firewall
- VPN
- Intrusion Protection

security

www.astaro.com

Agenda

- Astaro Corporate Profile
- Security Market Forecast
- Customer Challenges
- Threat Vector Classifications
- Trends in Network Security
 - Core / Email / Web / Virtualization
- Additional Resources



Astaro Corporate Overview

web

network

e-mail

security



astaro
internet security

Corporate Overview

- Worldwide Presence

- Established in 2000
- Headquartered in Karlsruhe, Germany and Burlington, MA
- NA Support Center in Burlington, MA
- Offices in the UK, United States, and Japan
- 2000+ Solution Providers Worldwide

- #1 Supplier of Open Source Based Security Software

- Protecting 30,000+ networks in over 60 countries
- “Best of Breed” Open Source and Patented Technologies
- 2007: 50% Growth

- Corporate Overview

- 1st to Market with UTM Solution in 2000.
- Available as Appliances or as Software
- Astaro Security Gateway – Integrated and Flexible approach to securing the network perimeter.
 - ✓ Network Security – Firewall, IDS/IPS, and VPN Gateway (SSL VPN now available)
 - ✓ Email Security – Spam Filtering, Anti-Virus, and Phishing Protection
 - ✓ Web Security – Content (URL) Filtering, Anti-Virus, and Spyware Protection
- Astaro Command Center – Management Platform supporting up to 500 installations.
- Clustering and High Availability Configurations for demanding environments.
- Robust for Today, Scalable for Tomorrow!
- Extensive features, Excellent Quality, and Easy to Deploy
- Available as Appliances or as Software



Corporate Sponsorships



Astaro is a General Member of **The Green Grid**, a global consortium dedicated to advancing energy efficiency in data centers and business computing ecosystems.



Netfilter is a set of hooks inside the Linux kernel that allows kernel modules to register callback functions with the network stack. Currently used in the Astaro Security Gateway, Astaro sponsors two full-time developers on the core team and makes monetary contributions to the project.



Clam AntiVirus is a GPL anti-virus toolkit for UNIX, which is integrated with mail servers. The programs are based on a shared library distributed with the Clam AntiVirus package, which you can use with your own software. Furthermore, the virus database is kept up to date. Currently used in the Astaro Security Gateway, Astaro makes monetary contributions to this project.



StrongSwan is an OpenSource IPsec implementation for the Linux operating system. Currently used in the Astaro Security Gateway, Astaro makes ongoing monetary contributions to this project.

Corporate Sponsorships



OpenVPN is a full-featured SSL VPN solution, which can accommodate a wide range of configurations, including remote access, site-to-site VPNs and WiFi security. Currently used in the Astaro Security Gateway, Astaro makes ongoing monetary contributions to this project.



Exim is a message transfer agent for use on Unix systems connected to the Internet. It is freely available and can be installed in place of sendmail, although the configuration of Exim is quite different. Currently used in the Astaro Security Gateway, Astaro makes ongoing monetary and technical contributions to this project.



Firebug integrates with Firefox to put a wealth of development tools at your fingertips while you browse. You can edit, debug and monitor CSS, HTML, and JavaScript live in any web page. Astaro helps develop this project.



Security Now! is a weekly podcast hosted by Leo Laporte of this WEEK in TECH and Steve Gibson of Gibson Research Corporation. Part of the TWiT.tv network and released each Thursday, Security Now! consists of a discussion between Gibson and Laporte on computer security issues and, conversely, insecurity. Astaro currently sponsors this podcast.

Corporate Sponsorships



Wikipedia is a multilingual, web-based, free content encyclopedia project. Wikipedia is written collaboratively by volunteers from all around the world. With rare exceptions, its articles can be edited by anyone with access to the Internet. Astaro currently makes monetary contributions to this project.



The **OpenSSL Project** is a collaborative effort to develop a robust, commercial-grade, full-featured and Open Source toolkit. It implements the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols as well as a full-strength general purpose cryptography library. Currently used in the Astaro Security Gateway, Astaro makes ongoing monetary contributions to this project.

Customers and Recognition

web

network

e-mail

security



astaro
internet security

Customers

Pilgrim Telephone



The Washington Times

Deloitte.



1-800-PetMeds®

America's Largest Pet Pharmacy



ThyssenKrupp
Automotive



BlueCross
BlueShield
Association

SHARP
..... be sharp



SIEMENS

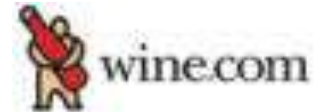


MARITIM



micros®

US DigitalMedia



Recognition and Awards



PRODUCT RATING	
Features	*****
Ease of Use	*****
Performance	*****
Documentation	*****
Support	*****
Value for Money	*****
Overall Rating	*****

Fun: Fully comprehensive UTM with many other features.
 Aggressively hiding web bugs!
 Verdict: A fully loaded gateway security device at a cost so fully loaded price. Recommended.

**SC Magazine 2008 UTM Test Group
"5 Stars All Categories - Recommended"**

**SC Magazine 2007 Europe Awards
"Best Network Security"**

SC Magazine "Best of 2006"

Common Criteria Certified - 2006

Firewall ICSA Labs Certified

**Product of the Year 2005 & 2006
- CRN**

SC Magazine "Best of 2005"

**Best of the Year 2004 / 2005
- PC Magazine**



Network Security Market Forecast and Customer Challenges

web

network

e-mail

security

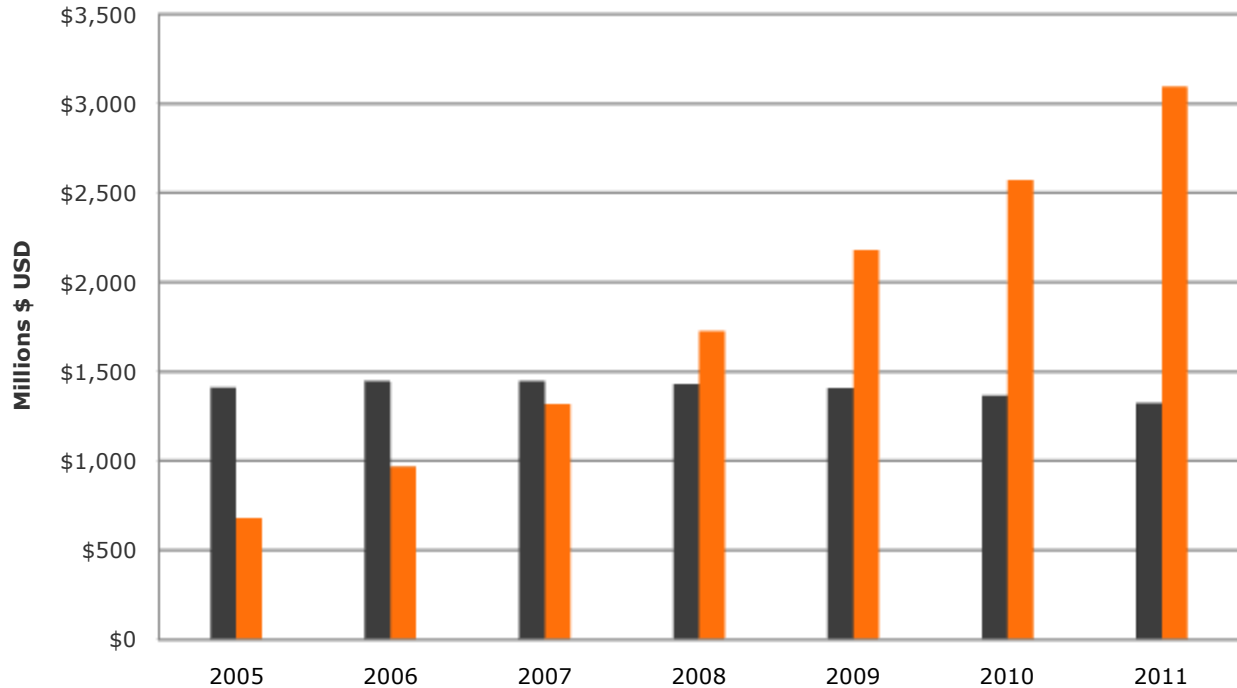


astaro
internet security

Worldwide UTM Appliances vs. FW/VPN Forecast 2005 – 2011

IDC Research

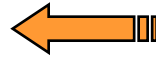
UTM (Unified Threat Management) Shipments are on the rise. Sales of Single function security devices have peaked. Security stance can be improved and budget savings achieved by centralizing network protection mechanisms and deploying multi function solutions such as the Astaro Security Gateway.



	2005	2006	2007	2008	2009	2010	2011
■ FW/VPN	\$1,410	\$1,447	\$1,447	\$1,429	\$1,408	\$1,366	\$1,324
■ UTM	\$681	\$967	\$1,317	\$1,726	\$2,182	\$2,572	\$3,097

Customer Challenges

Difficult to Deploy and Manage

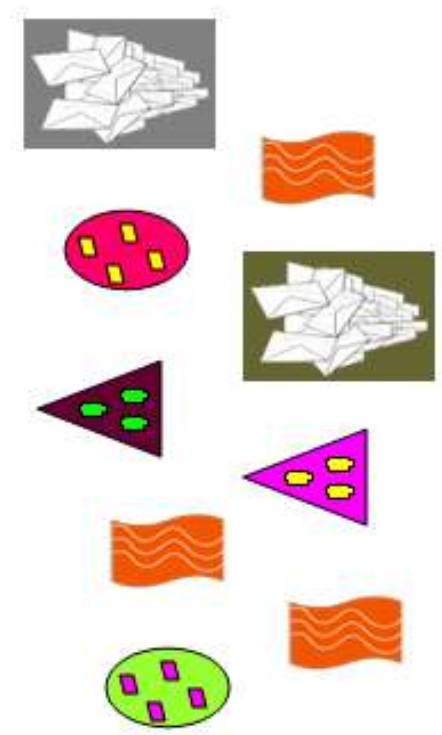
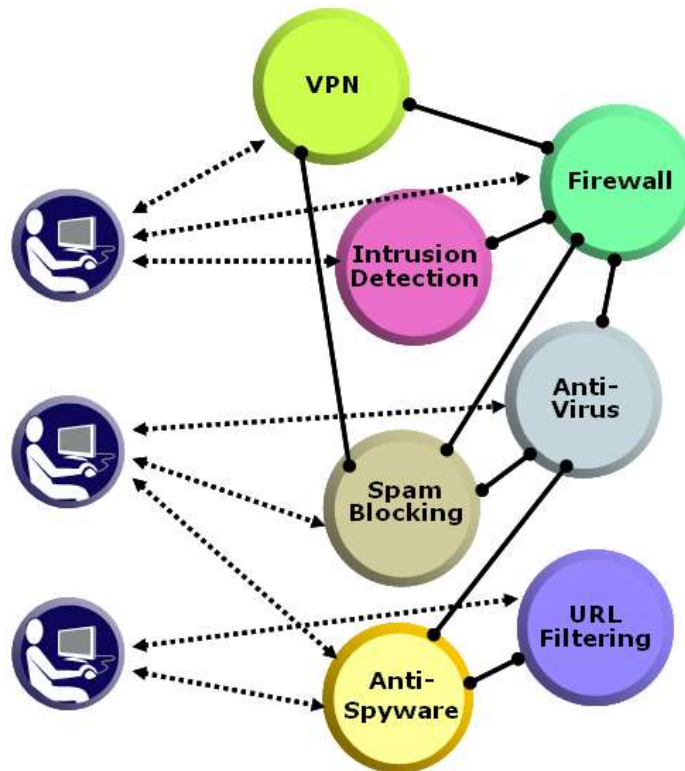


Expense to Maintain (People and System)

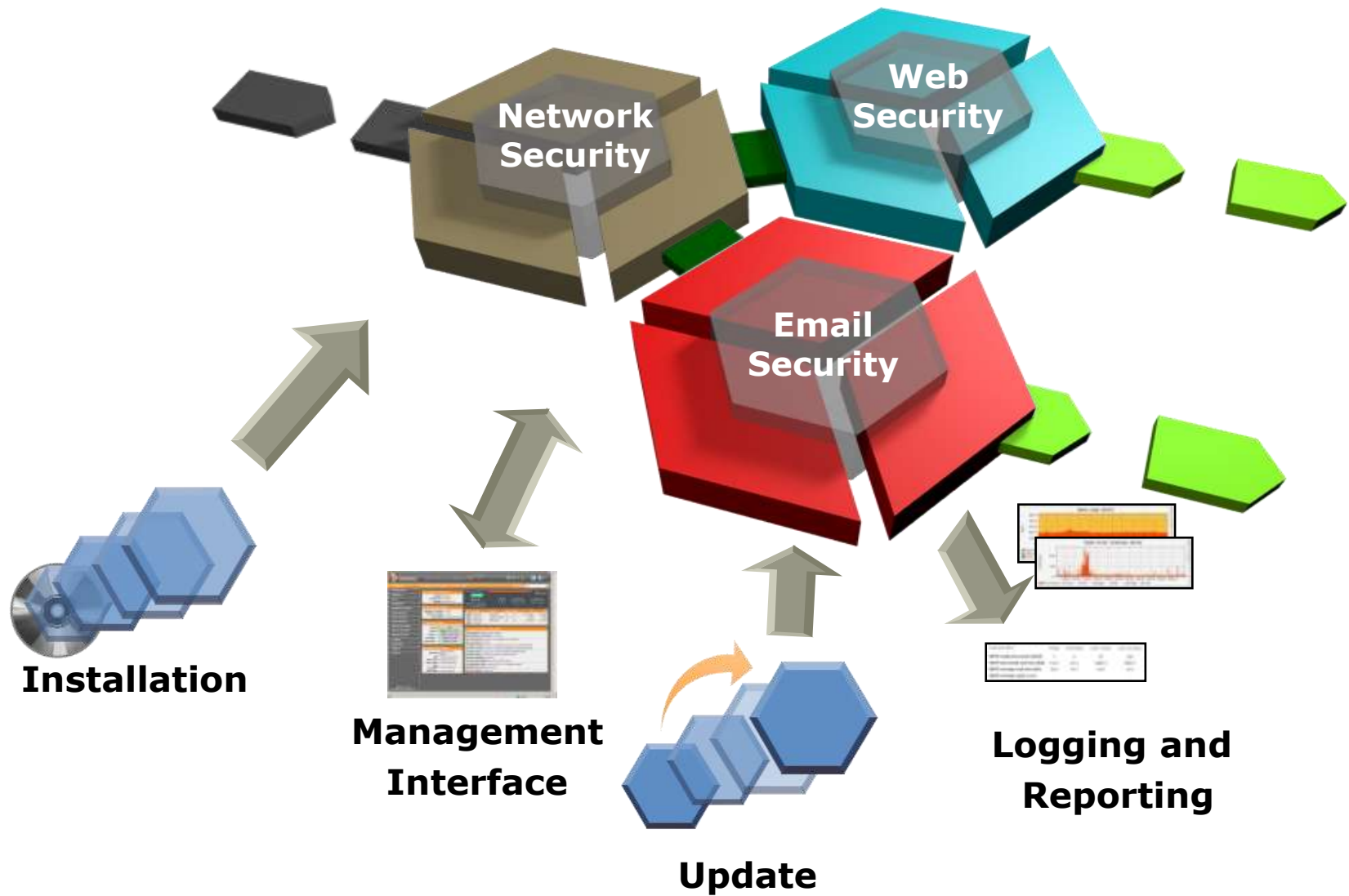


Ongoing and Emerging Threats

- ∞ Evaluate
- ∞ Purchase
- ∞ Train
- ∞ Install
- ∞ Integrate
- ∞ Configure
- ∞ Manage
- ∞ Update



Integrated Threat Protection



Threat Vector Classification

web

network

e-mail

security

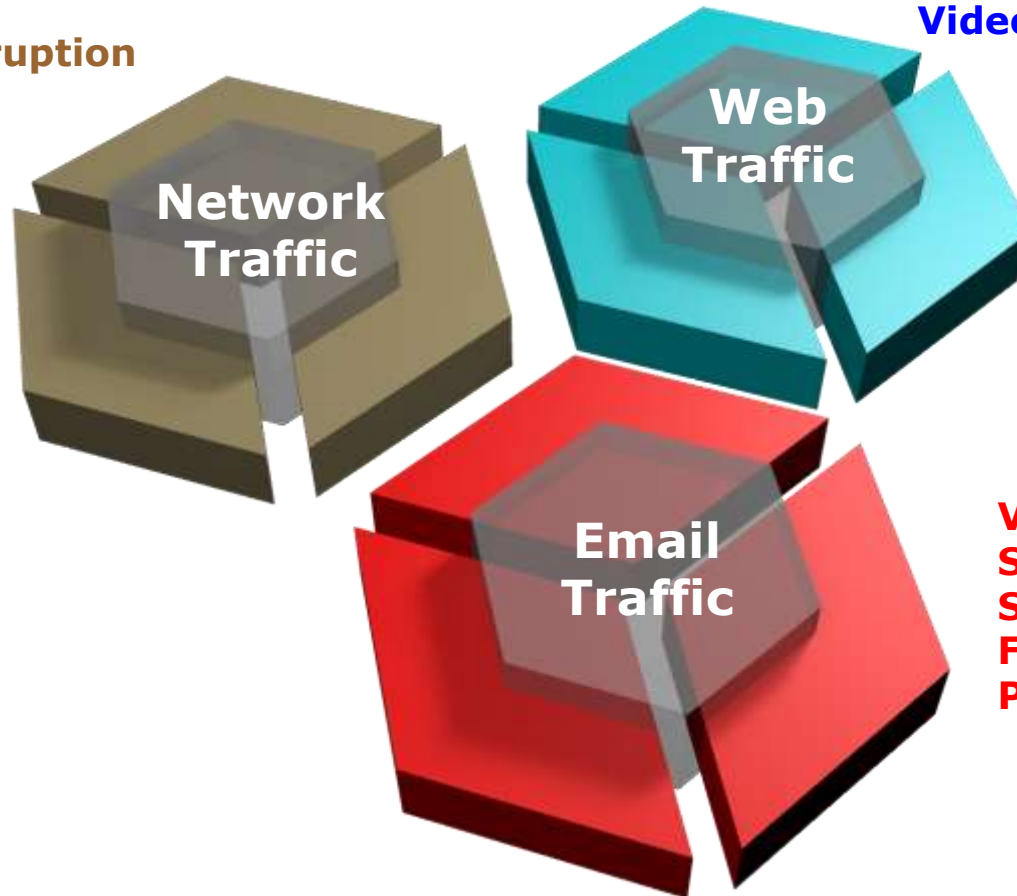


astaro
internet security

Threat Vector Classification

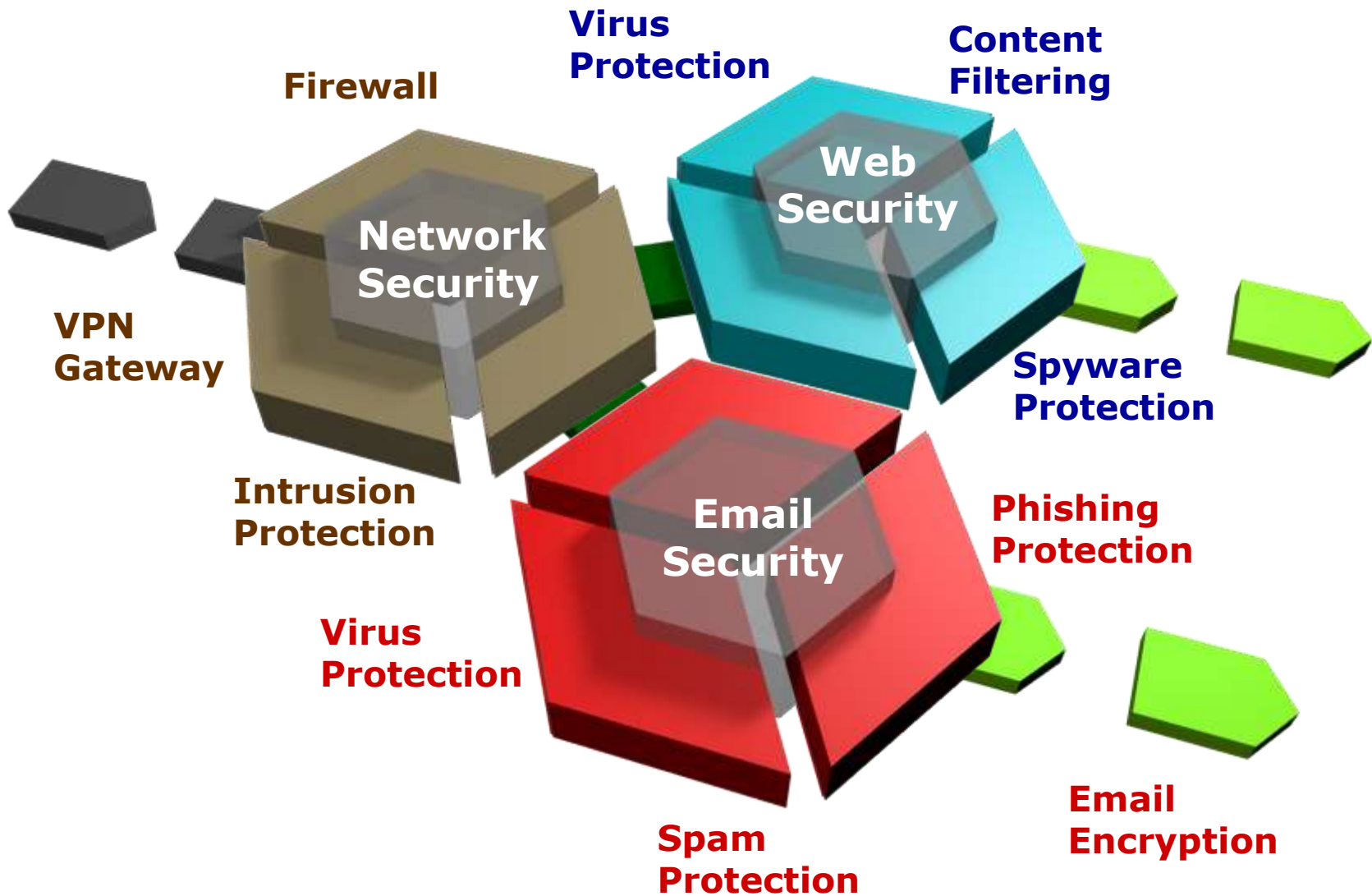
Hack Attacks
Attack traffic
Connection Hijacking
Denial of Service
Probes
VOIP Disruption

Virus infections
Spyware
Adware
Inappropriate Web Surfing
Music downloads
Video downloads



Virus infections
Scams
Spam
File attachments
Personal Info Exploits

Astaro Security Gateway



Trends in Core Network Security

web

network

e-mail

security



astaro
internet security

Growing Demand for Security

Firewall	VPN	Central Report tool
1995	URL Filter	Central Config tool
	IDS	Central Mgmt tool
	Email Anti Virus	Signing/encryption
	Firewall	VoIP Security
		VPN Remote access
		NAC
		Wireless security
		P2P filter
		IM filter
		Anti Spyware
		Multi protocol AV
		IPS
	VPN	VPN
	URL Filter	URL Filter
	IDS	IDS
	Email Anti Virus	Email Anti Virus
	Firewall	Firewall
	2001	2007

2010

**All-In-One
Appliances**

Core Network Security Trends

- Common Sense Approach Prevails
- Insider Threats
 - Effective Acceptable Use and Enforcement
 - Social Engineering
- Remote Access
 - Physical Access and Remote Management
- Internet Radiation
 - Automated Scanners
 - Inside Vulnerabilities – Patch levels
- Alerts and Forensics
 - Acceptable Use Monitoring
- Disaster Recovery
 - Power Failure
 - Hardware Failure



Virtualization Security Trends

web

network

e-mail

security



astaro
internet security

- Virtualization is on the rise
- Virus attacks
 - VMs can be infected just as non-VM machines
- Service attacks
 - Make sure all patches are kept up-to-date.
 - Disable any unused services
- Virtual Network Share Vulnerabilities
 - Minimize all hardware sharing, particularly NICs!
- Spyware
 - Don't surf the internet from the Host Machine.
- Unauthorized Access
 - Turn off all un-used Virtual Machines
 - Restrict physical access



Trends in Email Security

web

network

e-mail

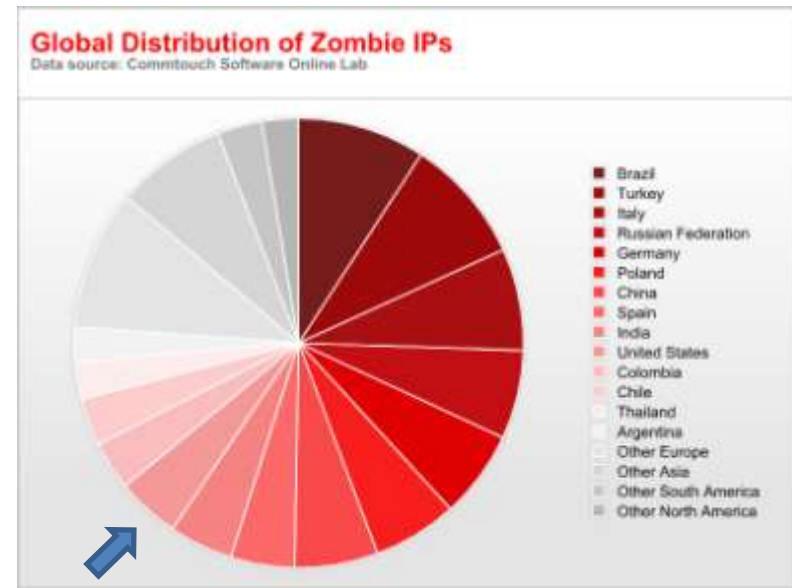
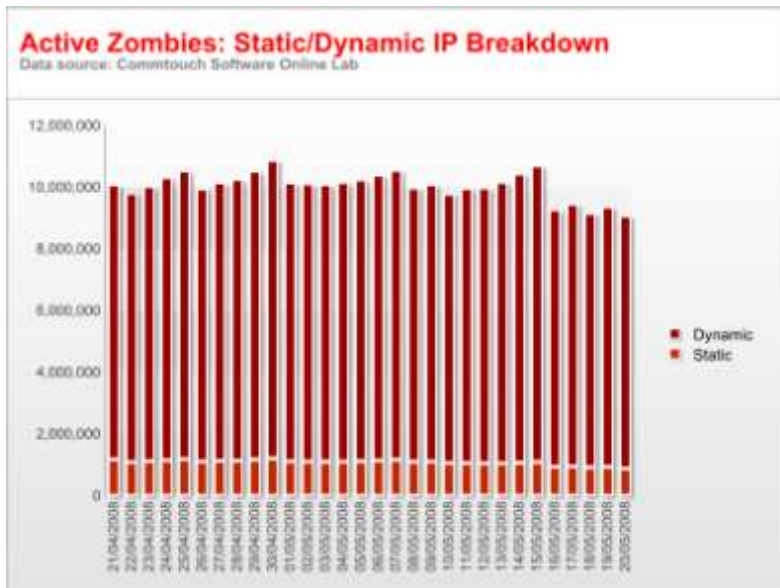
security



astaro
internet security

- Q1 2008

- 60-94% of all Email traffic was SPAM
- 355,000 New Zombies were activated daily to distribute
- Mortgage refinancing SPAM jumped to 10% in January
- Traditional techniques continue
 - PDF Attachment, ecard scams, holiday and event based



- Spammers Leverage Latest News and Events
 - Interest Rate Cut in Jan
 - Mortgage Spam Jumped from 2% to 10%
- Phishing more targeted (Social Engineering)
- Storm (Nuwar) Sample - Ecard
 - Once clicked, automatically downloaded
 - Hijacked Computers
 - Send Spam and Malware
 - DDOS attacks
 - 1.2B Virus messages by Botnet (9/2007)

Sample of "funny postcard" used to distribute Storm malware



Your download will start in 5 seconds.
If your download does not start, [click here](#)

©2000-2008 FunnyPostCard.com - All rights reserved.

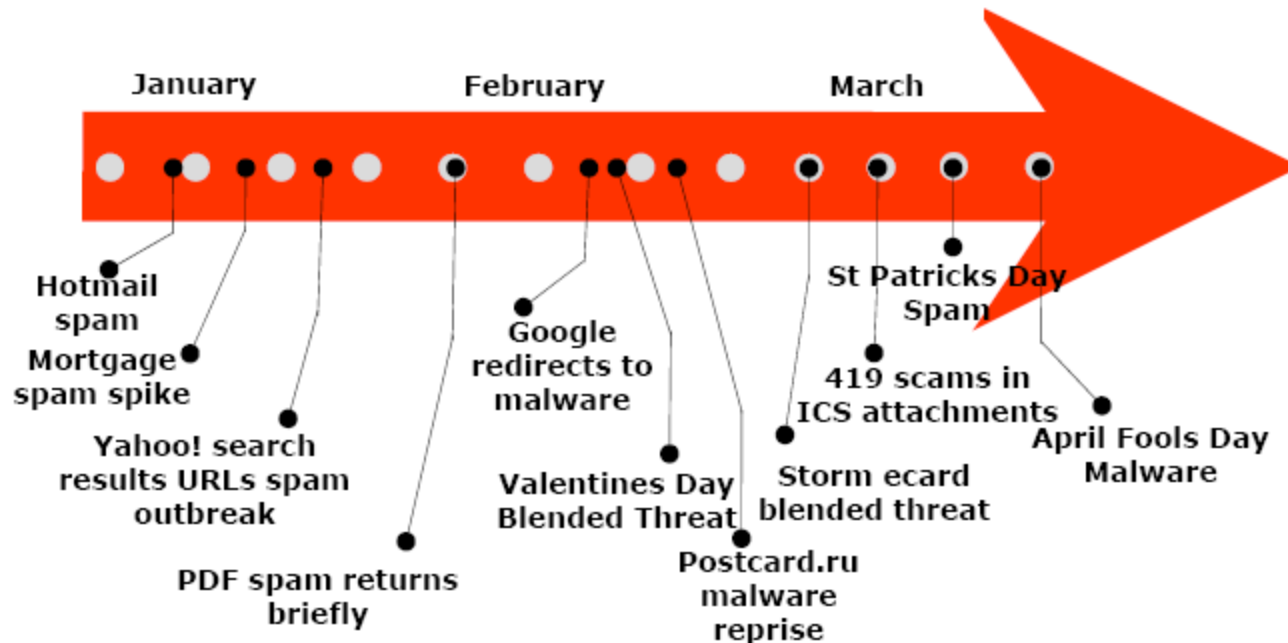
Source: Commtouch Labs

- Additional Techniques

- Host SPAM images on Flickr
- Google Calendar Invites
- Spoofed Email messages
- Spoofed Subject lines
 - Subject: Per our discussion, attached is the meeting agenda...



- Q1 2008 in Review



Trends in Web Security

web

network

e-mail

security



astaro
internet security

- P2P Traffic on the rise
 - Bittorrent, Winny, etc.
- Malware Exploits
 - 3M+ URLs/180,000 Sites automatically download malware
- Virus Infections
- Is your organization a malware host?
- Instant Messaging (AIM, Skype, etc)
 - Population will drive more attention
- Potential for Social Networking Site Targets
 - Facebook
 - Twitter
- Olympics/Sports Sites may become popular targets
- Anywhere there is a large audience...



Key Email & Web Security Capabilities by Astaro

web

network

e-mail

security



astaro
internet security

Email Fingerprinting

web

network

e-mail

security



astaro
internet security

Email Fingerprint Approach

From: QSTR在家創業系統 17:02:25
[Nashw4@taiwanhouse.com.tw]
Sent: Tuesday, June 15, 2006 12:16 AM
To: medeatw
Subject: * 上班族的隱憂 *

2006年，新的一年，新的開始

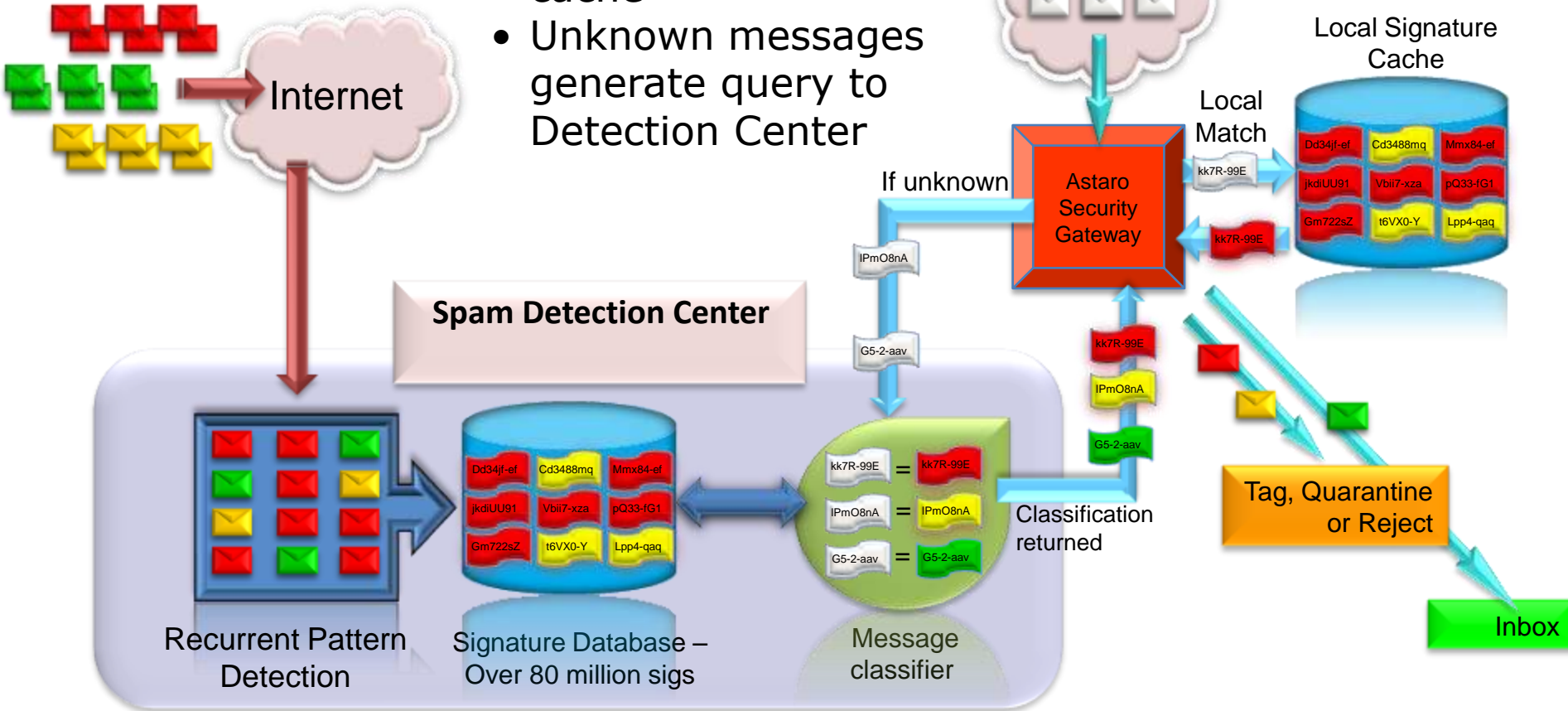
請打下面的電話，或上網索取免費致富小冊子
<http://www.cashcome.net> 索取帳號：
[直接進入索取](#)

現在讓我幫助你重新認識自己，**如果你真的想要改變你的人生，你要的是一份事業，而不只是一份工作的話**，美國QSTR在家創業系統，是結合**網路、郵購、通訊**的三大通路，也是目前全球最熱門的商機，已經幫助許多人成功在家創業賺到錢，這是個已經**證實成功**的系統了，它絕對不只是一般所看到的在家創業系統，它是一個**突破傳統結合趨勢**的全新在家創業系統，你只要按部就班，照著系統的步驟做，就可成功，也就是可以完成你的夢想，你還在猶豫不決什麼? O?

- Language Agnostic
- High Throughput
- CPU / RAM Efficient
- Faster outbreak response

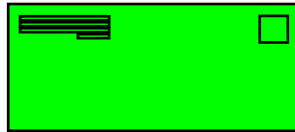
Recurrent Pattern Detection

- Incoming messages checked against local signature cache
- Unknown messages generate query to Detection Center

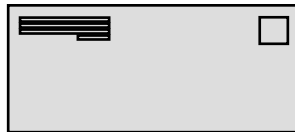


Message Classification

- Messages are classified into five types
- Service center returns message classification to application



Non Spam = definitively known to be legitimate mail. Rarely used.



Uncategorized = Does not raise any suspicion. Majority of mail to Inbox.



Suspected = A legacy category. Treat as Uncategorized.



Bulk Mail = Spam messages from unconfirmed sources.



Confirmed Spam = Positively identified as from known spamming source or matching known spam pattern.

Email Greylisting

web

network

e-mail

security



astaro
internet security

Traditional Scanning

- Perform RBL and other reputation checks
- Accept message for further processing
- Scan message using chosen scanning technology

Cons with traditional scanning:

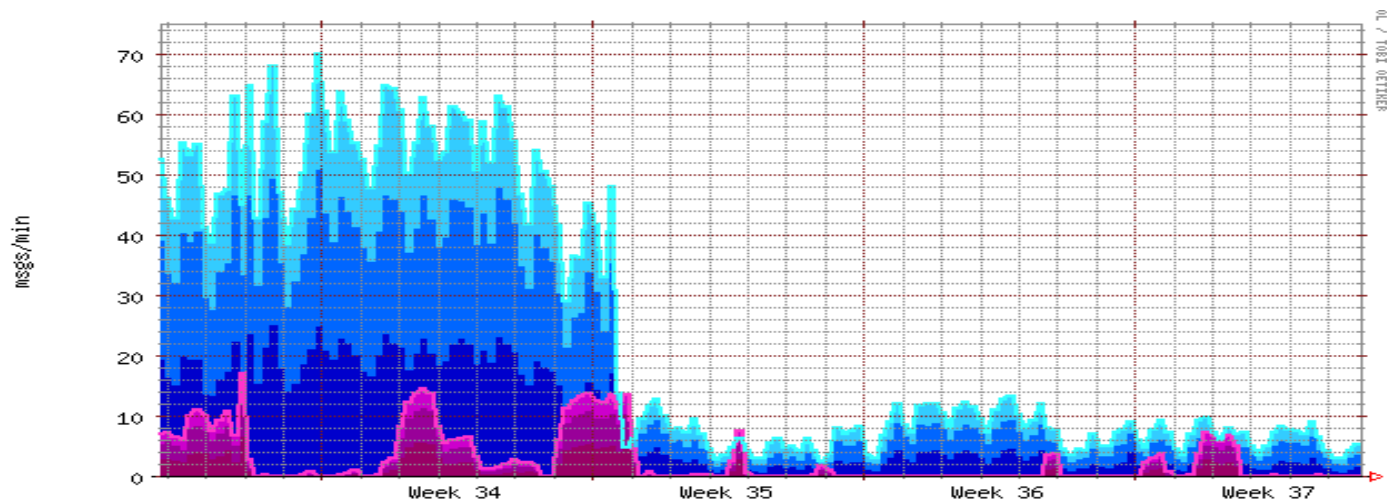
- Repeatable process required for all mail
- Massive resource requirements during spam attacks/outbreaks
- Delays in delivery or device DOS as a result
- Tweaking possible, but no real intelligent database
- Accuracy issues with False Positives and Negatives
- Essential Communication disruption from false positives leads to looser settings with result of more spam passed through.

Greylisting Approach

- Simple in concept, advanced in effect
- Slight defer for initial communication
- Triplet is saved to database
- Exceptions available

Email Security Statistics - Today			
Top email senders			
Total number of messages: 8 752			
Total email traffic: 1.6 GB			
	Email Address	#	Size
1	sgiles@testastaro.com	466	55.0 MB
2	operator@testastaro.com	180	14.4 MB
3	kscrimshire@testastaro.com	164	9.8 MB
4	jcornwell@testastaro.com	160	106.9 MB
5	cshaw@testastaro.com	112	11.6 MB
6	soverstreet@testastaro.com	112	23.3 MB
7	cfooshe@testastaro.com	85	2.4 MB
8	czazzali@testastaro.com	59	24.2 MB
9	prvs=whitney.aaronson=991600f5	56	3.7 MB
10	caruso@rewgroup.net	53	1.2 MB
Top email recipients			
Total number of messages: 8 752			
Total email traffic: 1.6 GB			
	Email Address	#	Size
1	stugiles.hit@hughes.net	466	55.0 MB
2	7038469110@testastaro.com	180	14.4 MB
3	network@testastaro.com	107	316.7 KB
4	cshaw@testastaro.com	88	7.3 MB
5	soverstreet@testastaro.com	88	3.8 MB
6	mbrown@testastaro.com	65	1.4 MB
7	bdenisar@testastaro.com	58	1.5 MB
8	cfooshe@testastaro.com	57	1.4 MB
9	jcornwell@testastaro.com	53	5.7 MB
10	lguyette@testastaro.com	44	2.5 MB
Top spam countries			
Total number of spams: 4 287			
Total spam mail size: 24.0 MB			
		Spams	Traffic
1	United States	2 505	17.7 MB
2	-	390	1.6 MB
3	China	273	470.5 KB
4	Canada	147	1.9 MB
5	Italy	112	214.9 KB
6	United Kingdom	79	295.6 KB
7	Argentina	72	133.8 KB
8	Russian Federation	59	251.6 KB
9	Spain	58	137.1 KB
10	Turkey	53	99.3 KB
Top malware names			
Total number of malware mails: 2			
Total malware mail size: 14.1 KB			
	Malware Name	#	Traffic
1	Email.Phishing.RB-2924	1	7.5 KB
2	HTML.Phishing.Bank-483	1	6.6 KB

The Greylisting Effect



Spam:

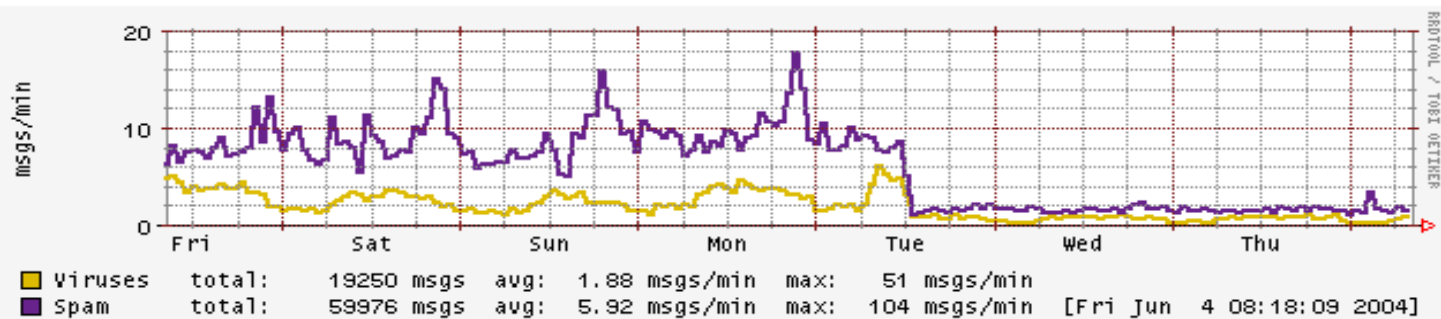
mx1_virus Spam	total:	349068 msgs	max:	143 msgs/min
mx2_virus Spam	total:	369857 msgs	max:	146 msgs/min
mx3_virus Spam	total:	257185 msgs	max:	123 msgs/min

Virus:

mx1_virus Virus	total:	42476 msgs	max:	27 msgs/min
mx2_virus Virus	total:	42391 msgs	max:	23 msgs/min
mx3_virus Virus	total:	23298 msgs	max:	23 msgs/min

total Virus total: 119001 msgs

total Spam total: 1076762 msgs



Phishing Explained

web

network

e-mail

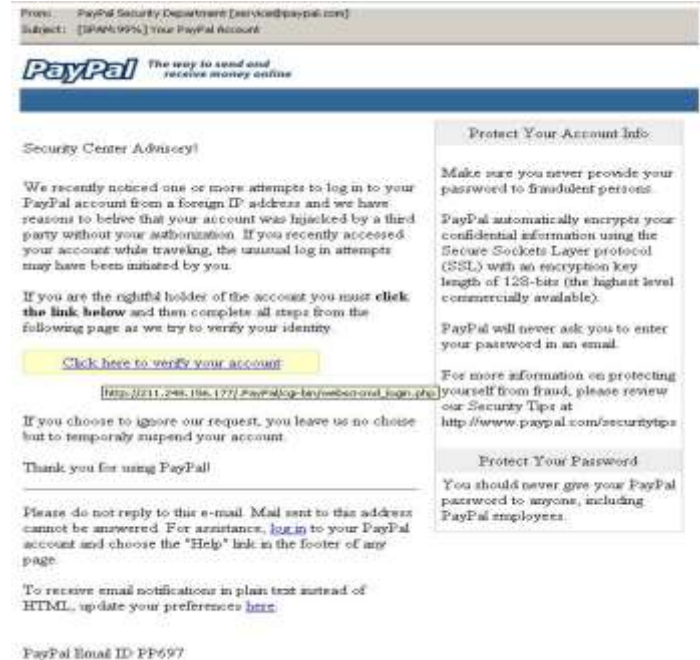
security



astaro
internet security

Phishing Overview

- Goals
- What facilitates?
- The chosen medium
- Exploiting trusted reputations
 - HTML
 - Text
 - Alerts
 - Urgent tones
- Deception via Duplication



Web Filter Whitelisting

web

network

e-mail

security



astaro
internet security

- Analyze/Scan Site
- Site Classification into Category(ies)
- Match Classification to Profile
- White & Blacklist as needed for manual tweaks
- Admins constantly play catch-up and fence-mending
- Reporting is KEY

Top blocked categories			
Total requests: 486			
	Category	Requests	%
1	Spyware	265	54.52
2	Illegal Activities	165	33.95
3	Swimwear / Lingerie	24	4.93
4	Political Extreme / Hate / Discrimination	20	4.11
5	Illegal Drugs	3	0.61
6	Violence / Extreme	3	0.61
7	Erotic / Sex	3	0.61
8	Tobacco	2	0.41
9	Weapons	1	0.20

Surfing Habits

Average User Monthly Activity

- 33 Hours per Month
- 57 minutes per session
- 70 Unique Domains
- 45 seconds per site visit



*Data as of March 2008

*Source: Nielson Netratings (<http://www.nielsen-netratings.com>)

Tedium Interrupted

Scope of project:

- 10-40 Million Sites
- 30-100+ Categories
- Multi-Language
- Local Database vs. Served Database

Top blocked categories

Total requests: 486

	Category	Requests	%
1	Spyware	265	54.52
2	Illegal Activities	165	33.95
3	Swimwear / Lingerie	24	4.93
4	Political Extreme / Hate / Discrimination	20	4.11
5	Illegal Drugs	3	0.61
6	Violence / Extreme	3	0.61
7	Erotic / Sex	3	0.61
8	Tobacco	2	0.41
9	Weapons	1	0.20

Whitelisting Benefits

- Less re-action, more preparation
- Reliable list of allowances
- Immune to new/changing sites
- Reduced need for daily/weekly auditing

Top domains by time spent:			
Total unique domains: 1373			
Total traffic: 1.6 GB			
Domain	Time spent	%	
1 google.com	03:27:25	4.32	
2 yahoo.com	02:37:28	3.28	
3 atdmt.com	02:35:49	3.24	
4 error	02:19:56	2.91	
5 yimg.com	01:57:00	2.43	
6 2mdn.net	01:41:08	2.10	
7 live.com	01:16:29	1.59	
8 2o7.net	01:14:56	1.56	
9 microsoft.com	01:09:31	1.44	
10 msn.com	01:07:52	1.41	

Top users by time spent			
Total unique users: 123			
Total traffic: 1.6 GB			
User	Time spent	%	
1 JohnDoe	00:34:53	6.49	
2 JohnDoe75	00:14:58	2.78	
3 JohnDoe19	00:09:42	1.80	
4 JohnDoe5	00:09:13	1.71	
5 JohnDoe21	00:08:41	1.61	
6 JohnDoe100	00:08:18	1.54	
7 JohnDoe1	00:08:04	1.50	
8 JohnDoe20	00:07:57	1.48	
9 JohnDoe23	00:07:39	1.42	
10 JohnDoe24	00:07:39	1.42	

Top domains by traffic			
Total unique domains: 1373			
Total traffic: 1.6 GB			
Domain	Traffic	%	
1 youtube.com	184.6 MB	11.20	
2 netsmartzkids.org	170.6 MB	10.35	
3 apple.com	127.4 MB	7.73	
4 earthcache.net	120.4 MB	7.30	
5 slackr.com	75.9 MB	4.60	
6 google.com	57.7 MB	3.50	
7 howstuffworks.com	43.5 MB	2.63	
8 yimg.com	35.1 MB	2.12	
9 x2dev.net	32.6 MB	1.98	
10 libsvn.com	28.1 MB	1.70	

Top users by traffic			
Total unique users: 123			
Total traffic: 1.6 GB			
User	Traffic	%	
1 JohnDoe69	176.2 MB	10.69	
2 JohnDoe	172.2 MB	10.45	
3 JohnDoe68	112.9 MB	6.85	
4 JohnDoe70	76.0 MB	4.61	
5 JohnDoe95	69.6 MB	4.22	
6 JohnDoe33	63.5 MB	3.85	
7 JohnDoe81	56.3 MB	3.41	
8 JohnDoe71	46.2 MB	2.80	
9 JohnDoe79	37.2 MB	2.25	
10 JohnDoe17	34.7 MB	2.10	

Resources and Education

- Security Now! Podcast
 - Sponsored by Astaro
- Astaro.com
 - V7 Demo Site: <http://demo.astaro.com/>
 - Free Home Use License and Training
- CU Info Security
 - <http://www.cuinfosecurity.com/>
- Computer Crime and Security Survey
 - <http://www.gocsi.com>
- US-Cert (Computer Emergency Readiness Team)
 - <http://www.us-cert.gov/>
- Privacyrights.org
 - <http://www.privacyrights.org/>
- 2008 CU InfoSecurity Conference
 - June 5-6 – Las Vegas





astaro
internet security

Thank You!

David Rogers
Director of Sales & OEM
Astaro Corporation
Office: 781-345-5000
Fax: 781-345-5100
Email: drogers@astaro.com

web

- Surf Protection
- Spyware Protection
- Virus Protection

network

- Virus Protection
- Spam Protection
- Phishing Protection

e-mail

- Firewall
- VPN
- Intrusion Protection

security

www.astaro.com