DÉTECTER ET RÉAGIR FACE AUX CYBER-ATTAQUES – RETOUR D'EXPÉRIENCE D'UNE EXPÉRIMENTATION TECHNICO-OPÉRATIONNELLE MULTINATIONALE

sopra Cyber Test Systems

SOMMAIRE

PRÉSENTATION DE L'EXERCICE COMBINED ENDEAVOR 2014

sopra

PRÉSENTATION DE L'EXERCICE « COMBINED ENDEAVOR »

Ce sont près de 2500 personnels issus de 40 pays différents qui participent à cet exercice. Combined Endeavor se déroule sur la base de l'US Army à Grafenwoehr, du 25 août au 12 septembre.

Le but de cet exercice qui a lieu chaque année depuis 1995 (sponsorisé par EUCOM sous la direction du quartier général des Forces armées américaines en Europe) est de coordonner entre eux les systèmes de communication et d'information des États qui participent aux opérations de maintien de la paix. Lors de cet exercice sont réalisés la planification, le test et la documentation d'interopérabilité entre les participants dans le domaine du CIS (Communication-and-Information-System).

sopra Cyber Test Systems

PRINCIPAUX OBJECTIFS CYBER DE L'EXERCICE « COMBINED ENDEAVOR » 2014

- Tester la capacité des nations à détecter, réagir, reporter et remédier aux attaques,
- Pousser les nations à collaborer et se coordonner lors de cyber-attaques de grande ampleur,
- Planifier des audits spécifiques afin de déterminer si les systèmes d'information sont protégés, contrôlés.
- Signaler les conclusions de l'audit et faire des recommandations aux parties prenantes lors de la communication des résultats afin d'apporter des changements si nécessaire.

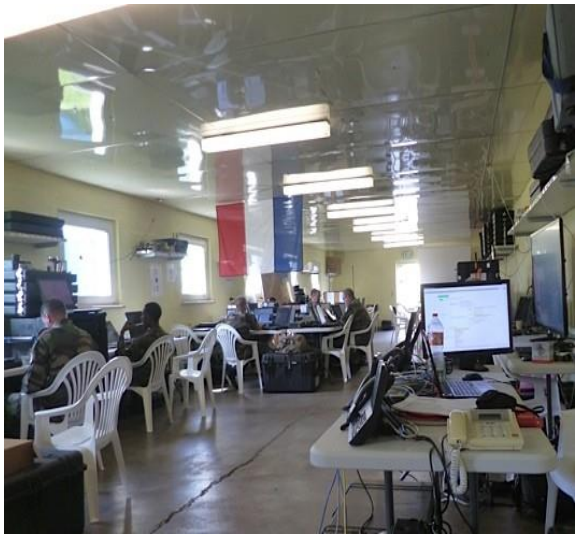
sopra Cyber Test Systems

POSITIONNEMENT DE LA FRANCE DANS L'EXERCICE

sopra

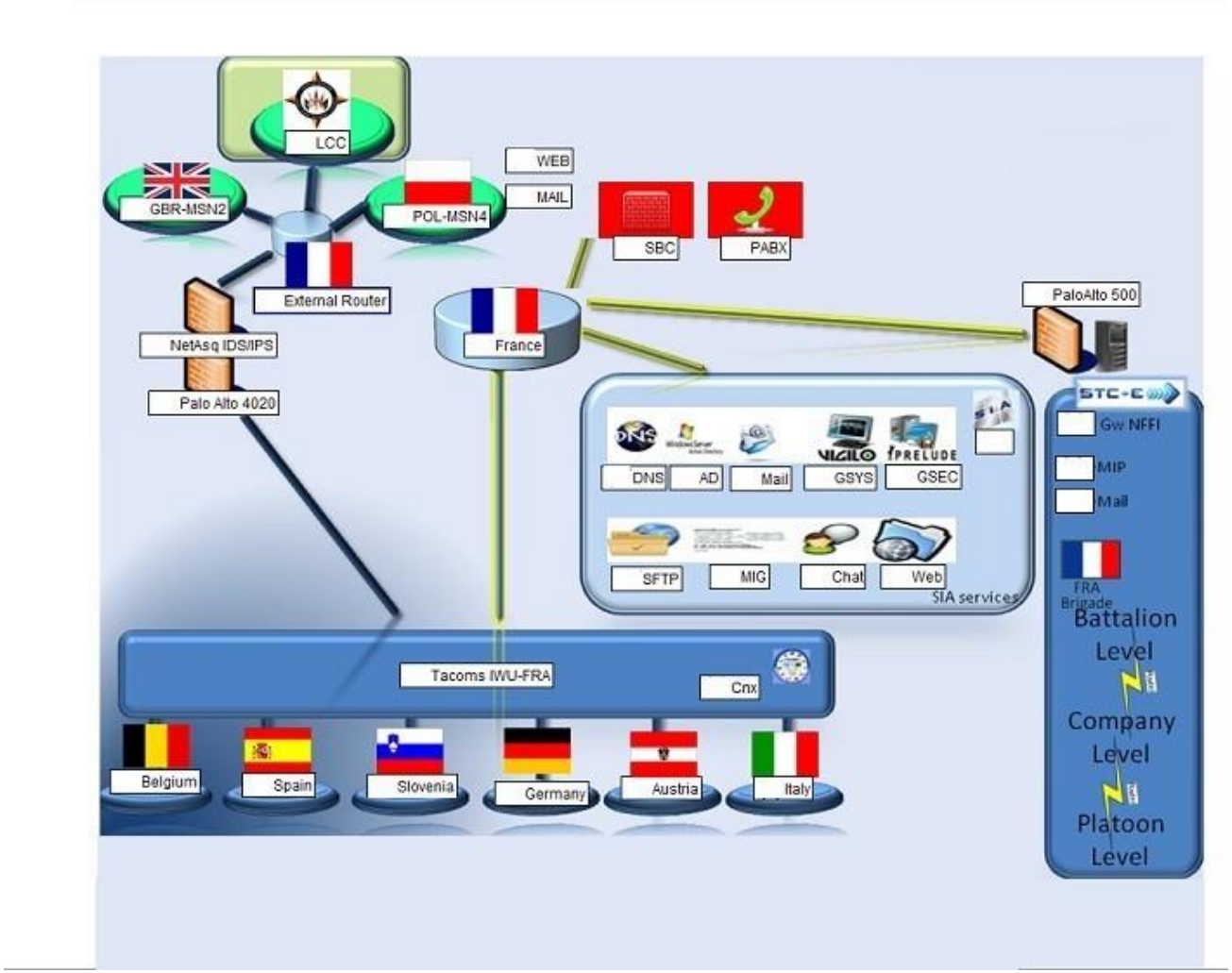
POSITIONNEMENT DE LA FRANCE DANS L'EXERCICE

L'exercice est divisé en « Mission Network » interconnectés entre eux. Au sein de chaque « Mission Network », les pays sont organisés sous la forme d'un ordre de bataille dans lequel une brigade a pour subordonnée plusieurs bataillons.



Dans ce cadre, la France tient le rôle de brigade et donc aussi celui de « Lead Nation ». Outre l'interconnexion avec les autres MSN et le CJTF, elle a offert aux nations de son niveau un ensemble de services (pont de visioconférence, DNS, NTP, HUB NFFI, PKI …)

CARTOGRAPHIE RESEAU VUE DU POSITIONNEMENT FRANCE



TESTS REALISES PAR LA RED TEAM

sopra

TESTS REALISES

- Networks Scanning
- Vulnerability Scans
- Spear Phishing Emails
- Malicious Attachments & Websites
- Password Auditing
- Anti Virus Check
- Brute Force Attacks

SOLUTIONS UTILISEES POUR LES TESTS

- Nessus/OpenVAS Vulnerability Scanners
- NMAP (Network Mapping)
- Nikto/OpenWASP (Web Servers)
- Hydra (Password Auditing)
- Metasploit (Password Auditing Feature/Passive Scanning)
- McAfee Vulnerability Manager

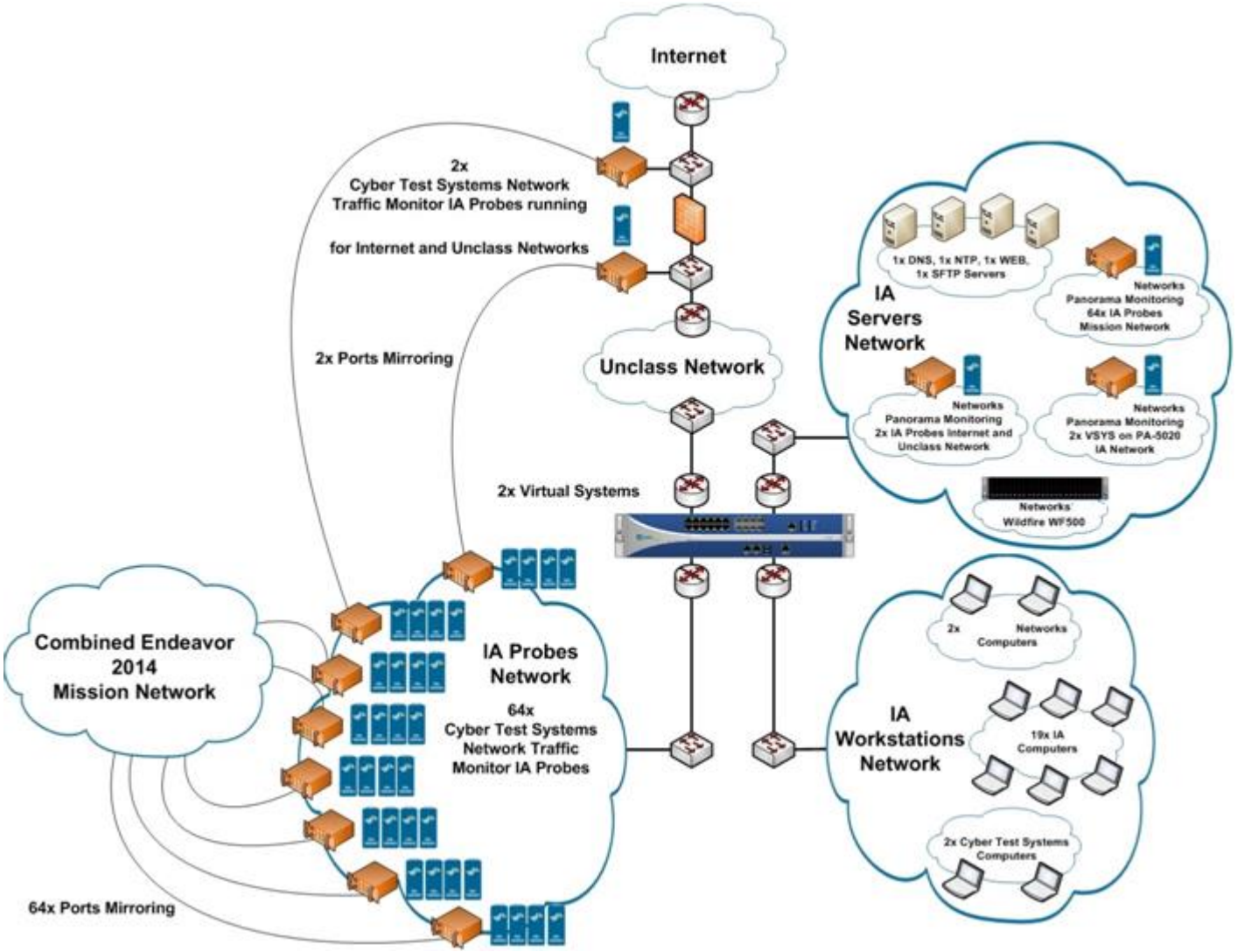
VULNÉRABILITÉS TROUVÉES

- Beaucoup de services non autorisés ont été identifiés (TELNET, etc.)
- Beaucoup de “backdoors” installé sur les systèmes cependant les nations ont été immédiatement notifiés.
- Compte par défaut et mot de passe vide ont été découvert sur de nombreux équipements (Tandberg’s, IP Phones, etc.)
- Équipement configuré pour permettre une connexion sans authentification (IP Phones)
- Logiciel non à jour ont été détecté au niveau des serveurs web (sujet à des attaques de type DDoS)
- Nombreuses vulnérabilités associé à des possibilités de certificat auto signés et donc à des attaques de type ‘Man in the Middle”.

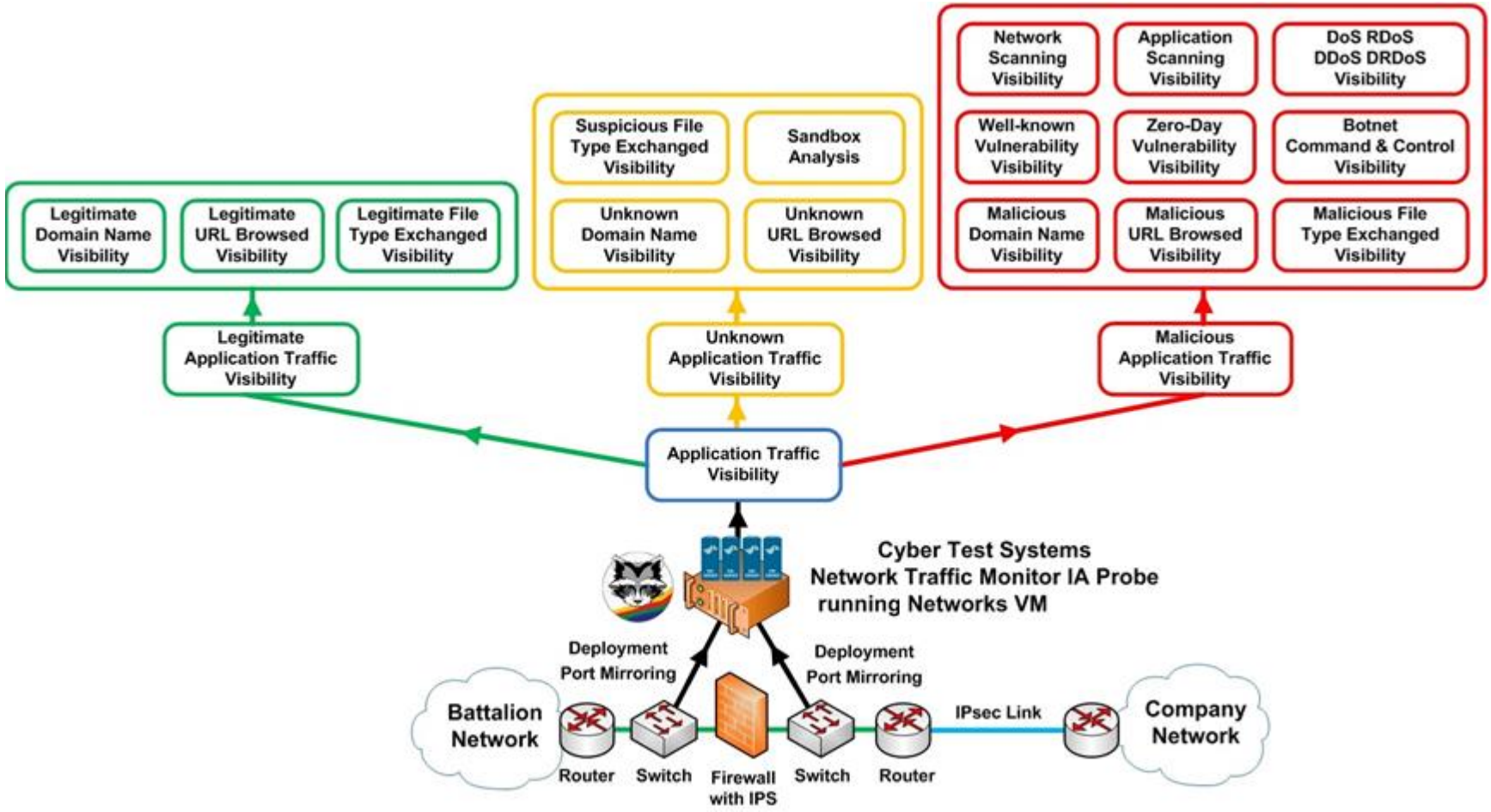
PRÉSENTATION DES ATTAQUES OBSERVÉES PAR LES SONDES CYBER TEST SYSTEMS MISES EN PLACE DANS L'EXERCICE

sopra

NETWORK INFRASTRUCTURE MONITORING COMBINED ENDEAVOR NETWORKS



DEPLOYMENT OF CYBER TEST SYSTEMS NETWORK TRAFFIC MONITOR IA PROBE



NETWORK TRAFFIC STATISTICS NETWORK COMMAND SIDE

HIGH LEVEL VIEW OF THE NETWORK TRAFFIC USED IN CHAIN OF COMMAND

- **Statistics from all IA Probes deployed on Mission Network**

Type of Information	CE2014 Statistics
Number of unique application protocols	146
Number of unique file types exchanged	26
Number of unique threats alerts	316

- **Statistics from all IA Probes deployed at Division Level**

Type of Information	CE2014 Statistics
Number of unique application protocols	146
Number of unique file types exchanged	26
Number of unique threats alerts	316

- **Statistics from all IA Probes deployed at Brigade Level**

Type of Information	CE2014 Statistics
Number of unique application protocols	67
Number of unique file types exchanged	15
Number of unique threats alerts	20

- **Statistics from all IA Probes deployed at Battalion Level**

Type of Information	CE2014 Statistics
Number of unique application protocols	44
Number of unique file types exchanged	9
Number of unique threats alerts	68

- **Statistics from all IA Probes deployed on Company Level**

Type of Information	CE2014 Statistics
Number of unique application protocols	99
Number of unique file types exchanged	12
Number of unique threats alerts	170

- **Statistics from all IA Probes deployed on Platoon Level**

Type of Information	CE2014 Statistics
Number of unique application protocols	21
Number of unique file types exchanged	1
Number of unique threats alerts	9

TOP 25 FILE TYPES EXCHANGED IN THE ENTIRE MISSION NETWORK

	Threat/Content Name	ID	Threat/Content Type	Repeat Count
1	JAR File	52116	file	753.9 K
2	Windows BAT	52128	file	21.1 K
3	ZIP	52004	file	21.0 K
4	Microsoft MSOFFICE	52033	file	2.1 K
5	Microsoft Office 2007 Word Document	52140	file	834
6	Microsoft Word	52012	file	514
7	Adobe Shockwave Flash File	52145	file	382
8	Microsoft Office 2007 Word Document	52022	file	378
9	PNG File Upload	52100	file	312
10	Java Class File	52117	file	162
11	MP3 File	52054	file	116
12	Microsoft Office 2007 XLS Document	52141	file	112
13	Microsoft Office 2007 PPT Document	52142	file	112
14	RTF File	52044	file	100
15	Microsoft Word	52001	file	90
16	JPEG File Upload	52097	file	74
17	CMD Windows Script File	52133	file	64
18	CMD Windows Script File	52092	file	64
19	Microsoft Office 2007 XLS Document	52024	file	56
20	Microsoft Office 2007 PPT Document	52023	file	50
21	Microsoft Excel	52013	file	18
22	BMP File Upload	52098	file	12
23	WMV File	52046	file	8
24	Adobe Portable Document Format (PDF)	52021	file	8
25	Microsoft PowerPoint	52000	file	4

sopra Cyber Test Systems

TOP 25 APPLICATION PROTOCOLS USED IN THE ENTIRE MISSION NETWORK

	Risk	Application Name	Sessions	Bytes	Threats
1	2	rtp	8.1 K	57.2 G	0
2	1	unknown-udp	5.9 K	18.7 G	1
3	0	Webcop	2.4 M	17.4 G	5.4 K
4	1	rtcp	6.3 K	14.3 G	0
5	2	ms-wmi	1.8 K	12.4 G	0
6	4	web-browsing	975.3 K	10.8 G	186.4 K
7	2	snmpv2	3.9 M	4.7 G	0
8	2	netflow	6.6 K	3.6 G	0
9	4	ssl	183.6 K	2.8 G	54
10	2	ping	10.9 M	2.8 G	0
11	4	dns	11.8 M	2.4 G	155.4 K
12	0	C2-MIP	18.6 K	2.4 G	0
13	2	ldap	100.7 K	2.2 G	36
14	2	syslog	80.2 K	2.1 G	0
15	4	flash	201	1.9 G	0
16	4	ms-rdp	2.9 K	1.7 G	14
17	2	snmpv1	399.3 K	1.6 G	0
18	3	snmp-trap	198.3 K	1.3 G	0
19	5	jabber	37.3 K	1.1 G	2
20	5	smtp	55.5 K	1.1 G	168
21	0	NetInspector	13.3 K	1.0 G	0
22	1	unknown-tcp	42.6 K	922.0 M	9.4 K
23	3	sharepoint-base	7.7 K	812.4 M	13.7 K
24	0	NFFI-over-tcp	28.2 K	807.9 M	0
25	2	netbios-ns	520.6 K	480.1 M	1.2 K

THREATS BY SEVERITY SEEN IN THE ENTIRE MISSION NETWORK

- **Number of threats by severity**

Type of Information	Statistics	Distribution
Number of threats with critical severity	3.3 K	1 %
Number of threats with high severity	64.6 K	19.1 %
Number of threats with medium severity	18.9 K	5.6 %
Number of threats with low severity	41.0 K	12.1 %
Number of threats with informational severity	210.6 K	62.2 %
Total number of threats seen during Combined Endeavor 2014	338.4 K	100 %

- **Number of unique threats by severity**

Severity	Statistics	Distribution
Number of unique threats with critical severity	15	4.7 %
Number of unique threats with high severity	177	56.0 %
Number of unique threats with medium severity	56	17.8 %
Number of unique threats with low severity	31	9.8 %
Number of unique threats with informational severity	37	11.7 %
Total number of unique threats seen during Combined Endeavor 2014	316	100 %

TOP 25 THREATS SEEN IN THE ENTIRE MISSION NETWORK

	Severity	Threat/Content Name	ID	Threat/Content Type	Count
1	INFORMATIONAL	Microsoft Communicator INVITE Flood Denial of Service Vulnerability	31993	vulnerability	35.5 K
2	HIGH	SIP INVITE Method Request Flood Attempt	40016	vulnerability	31.1 K
3	INFORMATIONAL	FTP Login Failed	40000	vulnerability	24.4 K
4	HIGH	FTP: login Brute-force attempt	40001	vulnerability	24.3 K
5	INFORMATIONAL	Microsoft Windows SMB Negotiate Request	35364	vulnerability	19.2 K
6	INFORMATIONAL	SSH2 Login Attempt	31914	vulnerability	11.1 K
7	LOW	SIP Register Request Attempt	33592	vulnerability	7.5 K
8	HIGH	HTTP Unauthorized Brute-force Attack	40031	vulnerability	6.0 K
9	MEDIUM	PHP Remote File Include Vulnerability	33327	vulnerability	4.8 K
10	LOW	HTTP Cross Site Scripting Attempt	32658	vulnerability	4.8 K
11	LOW	HTTP Directory Traversal Vulnerability	30844	vulnerability	4.8 K
12	HIGH	HTTP: User Authentication Brute-force Attempt	40006	vulnerability	4.3 K
13	INFORMATIONAL	HTTP Unauthorized Error	34556	vulnerability	3.9 K
14	INFORMATIONAL	HTTP OPTIONS Method	30520	vulnerability	3.4 K
15	INFORMATIONAL	HTTP WWW-Authentication Failed	31708	vulnerability	2.5 K
16	MEDIUM	Microsoft Windows SMB NTLM Authentication Lack of Entropy Vulnerability	40034	vulnerability	2.5 K
17	HIGH	Generic HTTP Cross Site Scripting Attempt	31477	vulnerability	2.3 K
18	HIGH	Cisco IOS HTTP Configuration Arbitrary Administrative Access Vulnerability	30921	vulnerability	1.8 K
19	INFORMATIONAL	SIP Bye Request Attempt	34520	vulnerability	1.6 K
20	HIGH	HTTP /etc/passwd access attempt	35107	vulnerability	1.2 K
21	CRITICAL	Microsoft IIS Escaped Characters Decoding Command Execution Vulnerability	30444	vulnerability	1.0 K
22	HIGH	HTTP /etc/passwd Access Attempt	30852	vulnerability	986
23	HIGH	SSH User Authentication Brute-force Attempt	40015	vulnerability	963
24	HIGH	Generic HTTP Cross Site Scripting Attempt	31475	vulnerability	777
25	INFORMATIONAL	NetBIOS nbtstat query	31707	vulnerability	749

TOP OF THREATS WITH CRITICAL/HIGH/MEDIUM SEVERITY

	Severity	Threat/Content Name	ID	Repeat Count
1	CRITICAL	Microsoft IIS Escaped Characters Decoding Command Execution Vulnerability	30444	2.7 K
2		phpBB viewtopic.php Highlighting Feature Arbitrary PHP Code Execution	30092	244
3		Joomla Visites Component Remote File Include Vulnerability	34439	138
4		HTTP Cross Site Scripting Vulnerability	35864	90
5		PCCS Mysql Database Admin Tool Username and Password Disclosure Vulnerability	36102	20
6		IBM Rational Quality Manager and Test Lab Manager Remote Code Execution Vulnerability	34181	17
7		phf CGI program remote command execution vulnerability	32790	14
8		Microsoft IIS ASP.NET NULL Byte Injection Information Disclosure Vulnerability	32735	13

	Severity	Threat/Content Name	ID	Repeat Count
1	HIGH	SIP INVITE Method Request Flood Attempt	40016	21.6 K
2		FTP: login Brute-force attempt	40001	12.1 K
3		HTTP /etc/passwd Access Attempt	30852	5.6 K
4		Generic HTTP Cross Site Scripting Attempt	31477	4.5 K
5		HTTP Unauthorized Brute-force Attack	40031	3.9 K
6		HTTP /etc/passwd access attempt	35107	3.5 K
7		HTTP: User Authentication Brute-force Attempt	40006	2.6 K
8		SSH User Authentication Brute-force Attempt	40015	2.3 K

	Severity	Threat/Content Name	ID	Repeat Count
1	MEDIUM	PHP Remote File Include Vulnerability	33327	8.9 K
2		Microsoft Windows SMB NTLM Authentication Lack of Entropy Vulnerability	40034	6.8 K
3		HTTP SQL Injection Attempt	30514	1.4 K
4		Oracle 9i Application Server Dynamic Monitoring Services Anonymous Access	33756	380
5		HTTP SQL Injection Attempt	33338	183

NETWORK TRAFFIC STATISTICS
INTERNET SIDE BEFORE FIREWALL
AND
UNCLASS NETWORK SIDE BEFORE FIREWALL

HIGH LEVEL VIEW OF THE NETWORK TRAFFIC SEEN ON INTERNET AND UNCLASS NETWORK

- **Statistics from both IA Probes deployed on Internet Side and Unclass Network Side**

Type of Information	Statistics
Number of unique application protocols	440
Number of unique file types exchanged	63
Number of unique threats alerts	366

- **Statistics from the IA Probe deployed on Internet Side before Firewall**

Type of Information	Statistics
Number of unique application protocols	351
Number of unique file types exchanged	63
Number of unique threats alerts	86

- **Statistics from the IA Probe deployed on Unclass Network after Firewall**

Type of Information	Statistics
Number of unique application protocols	440
Number of unique file types exchanged	63
Number of unique threats alerts	366

TOP 25 APPLICATION PROTOCOLS SEEN BY THE IA PROBE FROM INTERNET TO UNCLASS NETWORK BEFORE FIREWALL

	Risk	Application Name	Sessions	Bytes	Threats
1	4	ssl	2.2 M	670.3 G	0
2	4	web-browsing	3.6 M	319.5 G	4.9 K
3	4	facebook-base	541.4 K	121.8 G	1
4	3	open-vpn	98	112.1 G	0
5	3	itunes-mediastore	92	98.3 G	0
6	4	ms-update	26.9 K	79.8 G	0
7	1	paloalto-updates	22.2 K	72.2 G	0
8	4	youtube-base	11.7 K	38.4 G	0
9	5	skype	90.7 K	37.2 G	0
10	4	apple-appstore	22.1 K	37.0 G	0
11	3	ciscovpn	126	31.4 G	0
12	4	dropbox	61.4 K	28.8 G	0
13	5	http-video	6.2 K	27.8 G	168
14	4	flash	42.2 K	25.1 G	14
15	2	gre	46	24.0 G	0
16	4	ssh	93	19.8 G	37
17	2	telnet	1.9 K	18.0 G	2
18	4	ultrasurf	781	17.2 G	0
19	4	gmail-base	40.9 K	15.7 G	0
20	2	ipsec-esp	15	15.4 G	0
21	4	rtmp	1.3 K	14.1 G	0
22	3	symantec-av-update	17.0 K	12.6 G	0
23	3	google-play	1.4 K	10.7 G	0
24	1	apt-get	4.8 K	6.7 G	0
25	2	google-analytics	104.0 K	6.4 G	13

sopra Cyber Test Systems

TOP 25 FILE TYPES EXCHANGED SEEN BY THE IA PROBE FROM INTERNET TO UNCLASS NETWORK BERFORE FIREWALL

	Name	ID	Type	Repeat Count
1	ZIP	52004	file	539.9 K
2	Adobe Shockwave Flash File	52145	file	154.6 K
3	Microsoft Cabinet (CAB)	52003	file	75.3 K
4	JAR File	52116	file	34.1 K
5	Java Class File	52117	file	32.4 K
6	Microsoft PE File	52060	file	11.8 K
7	GZIP	52014	file	9.5 K
8	Android Package File Detected	52108	file	7.7 K
9	MP4 Detected	52104	file	5.9 K
10	MP3 File	52054	file	4.5 K
11	Windows Executable (EXE)	52020	file	4.1 K
12	Windows Dynamic Link Library (DLL)	52019	file	3.1 K
13	Adobe Portable Document Format (PDF)	52021	file	2.1 K
14	FLV File	52047	file	2.0 K
15	RAR	52015	file	1.5 K
16	Microsoft MSOFFICE	52033	file	823
17	Quicktime MOV File	52049	file	464
18	Activex CAB File	52042	file	300
19	Windows Batch (BAT)	52009	file	282
20	Activex File	52041	file	250
21	PNG File Upload	52100	file	244
22	MSI File	52089	file	209
23	TAR	52005	file	152
24	JPEG File Upload	52097	file	140
25	CMD Windows Script File	52133	file	122

sopra Cyber Test Systems

TOP 25 THREATS SEEN BY THE IA PROBE FROM UNCLASS NETWORK TO INTERNET BEFORE FIREWALL

	Severity	Threat/Content Name	ID	Threat/Content Type	Count
1	LOW	SIP Register Request Attempt	33592	vulnerability	509.0 K
2	HIGH	SIP Register Message Brute-force Attack	40023	vulnerability	193.5 K
3	INFORMATIONAL	Generic GET Method Buffer Overflow Vulnerability	34267	vulnerability	8.0 K
4	INFORMATIONAL	DGA NXDOMAIN response	36518	vulnerability	7.0 K
5	MEDIUM	SCAN: Host Sweep	8002	scan	4.0 K
6	INFORMATIONAL	HTTP Unauthorized Error	34556	vulnerability	4.0 K
7	INFORMATIONAL	HTTP WWW-Authentication Failed	31708	vulnerability	3.4 K
8	INFORMATIONAL	HTTP OPTIONS Method	30520	vulnerability	2.5 K
9	LOW	JavaScript Obfuscation Detected	31825	vulnerability	1.8 K
10	INFORMATIONAL	DNS ANY Request	34842	vulnerability	1.3 K
11	MEDIUM	Suspicious DNS Query (generic:svc-stats.linkury.com)	4047973	spyware	1.0 K
12	INFORMATIONAL	HTTP Request ACE Encoded Domain Name Access	31298	vulnerability	775
13	MEDIUM	Suspicious DNS Query (generic:oss.aliyuncs.com)	4070566	spyware	753
14	MEDIUM	Suspicious DNS Query (generic:pi.smarterpowerunite.com)	4042853	spyware	746
15	LOW	HTTP GET Requests Long URI Anomaly	30800	vulnerability	398
16	INFORMATIONAL	SSH2 Login Attempt	31914	vulnerability	346
17	CRITICAL	Bot: Mariposa Command and Control	12652	spyware	324
18	INFORMATIONAL	Microsoft Communicator INVITE Flood Denial of Service Vulnerability	31993	vulnerability	255
19	MEDIUM	Suspicious DNS Query (generic:storage.stgbssint.com)	4054467	spyware	204
20	INFORMATIONAL	Microsoft ASP.NET Remote Unauthenticated Denial of Service Vulnerability	32513	vulnerability	192
21	MEDIUM	Suspicious DNS Query (generic:1iqk3uqtclwos1hz32sv.org)	4032853	spyware	176
22	LOW	HTTP Cross Site Scripting Vulnerability	34851	vulnerability	147
23	LOW	JavaScript Obfuscation Detected	31826	vulnerability	131
24	INFORMATIONAL	DGA NXDOMAIN response Found	40040	vulnerability	129
25	LOW	SSL Double Client Hello Cipher Suite Length Mismatch	32467	vulnerability	114

sopra Cyber Test Systems

THREATS BY SEVERITY SEEN FROM INTERNET BEFORE FIREWALL AND UNCLASS NETWORK BEFORE FIREWALL

- **Number of threats by severity**

Type of Information	Statistics	Distribution
Number of threats with critical severity	239	0.3 %
Number of threats with high severity	90	0.1 %
Number of threats with medium severity	3.5 K	4.5 %
Number of threats with low severity	39.1 K	50.5 %
Number of threats with informational severity	34.6 K	44.6 %
Total number of threats seen during Combined Endeavor 2014	77.5 K	100 %

- **Number of unique threats by severity**

Type of Information	Statistics	Distribution
Number of unique threats with critical severity	2	2.4 %
Number of unique threats with high severity	7	7.8 %
Number of unique threats with medium severity	52	57.7 %
Number of unique threats with low severity	12	13.3 %
Number of unique threats with informational severity	17	18.8 %
Total number of unique threats seen during Combined Endeavor 2014	90	100 %

TOP 25 THREATS SEEN BY THE IA PROBE ON INTERNET SIDE BEFORE FIREWALL GIVING ACCESS TO UNCLASS NETWORK

	Severity	Threat/Content Name	ID	Threat/Content Type	Count
1	LOW	Sipvicious.Gen User-Agent Traffic	13272	spyware	13.5 K
2	INFORMATIONAL	DGA NXDOMAIN response	36518	vulnerability	7.1 K
3	INFORMATIONAL	HTTP Unauthorized Error	34556	vulnerability	4.0 K
4	INFORMATIONAL	HTTP WWW-Authentication Failed	31708	vulnerability	3.5 K
5	INFORMATIONAL	DNS ANY Request	34842	vulnerability	2.4 K
6	INFORMATIONAL	HTTP OPTIONS Method	30520	vulnerability	1.8 K
7	LOW	JavaScript Obfuscation Detected	31825	vulnerability	653
8	MEDIUM	Suspicious DNS Query (generic:bgwboo.com)	407...	spyware	555
9	MEDIUM	Suspicious DNS Query (generic:etnkragvqojrxryq.info)	404...	spyware	468
10	INFORMATIONAL	HTTP Request ACE Encoded Domain Name Access	31298	vulnerability	447
11	MEDIUM	Suspicious DNS Query (generic:oaxyka.com)	404...	spyware	294
12	INFORMATIONAL	Microsoft remote desktop connect initial attempt	33020	vulnerability	263
13	LOW	SIP Register Request Attempt	33592	vulnerability	180
14	LOW	HTTP Cross Site Scripting Vulnerability	34851	vulnerability	156
15	INFORMATIONAL	DGA NXDOMAIN response Found	40040	vulnerability	140
16	LOW	Morto RDP Request Traffic	13274	spyware	128
17	INFORMATIONAL	Generic GET Method Buffer Overflow Vulnerability	34267	vulnerability	106
18	INFORMATIONAL	Microsoft ASP.NET Remote Unauthenticated Denial of Service Vulnerability	32513	vulnerability	102
19	LOW	JavaScript Obfuscation Detected	31826	vulnerability	84
20	MEDIUM	Suspicious DNS Query (generic:gpoxqi.com)	405...	spyware	77
21	INFORMATIONAL	Microsoft Communicator INVITE Flood Denial of Service Vulnerability	31993	vulnerability	70
22	LOW	HTTP GET Requests Long URI Anomaly	30800	vulnerability	69
23	LOW	UNIX Portmapper Remote Infomation Retrieving Attempt	32796	vulnerability	66
24	INFORMATIONAL	SSH2 Login Attempt	31914	vulnerability	37
25	INFORMATIONAL	Failed Authentication Through Mail Protocol	31709	vulnerability	34

sopra Cyber Test Systems

TOP 25 OF CRITICAL/HIGH/MEDIUM THREATS

	Severity	Threat/Content Name	ID	Repeat Count
1	CRITICAL	Bot: Mariposa Command and Control	12652	226
2		Win32.Conficker.C p2p	12544	13

	Severity	Threat/Content Name	ID	Repeat Count
1	HIGH	PHP CGI Query String Parameter Handling Code Injection Vulnerability	34858	24
2		PHP CGI Query String Parameter Handling Code Injection Vulnerability	34790	24
3		SIP INVITE Method Request Flood Attempt	40016	14
4		GIF File With Embeded JavaScript Obfuscation Exploit	34194	9
5		TippingPoint IPS Audit Log Telnet Failure Cross-Site Scripting	33096	9
6		Symantec AntiVirus RAR Archive Decompression Buffer Overflow	31386	9
7		Multiple Vendor Telnet Client env_opt_add Buffer Overflow	30486	1

	Severity	Threat/Content Name	ID	Repeat Count
1	MEDIUM	Suspicious DNS Query (generic:lyekbv.com)	4070566	1.2 K
2		Suspicious DNS Query (generic:etnkragvqojnxryq.info)	4042853	984
3		Suspicious DNS Query (generic:ggirkj.com)	4047973	639
4		Suspicious DNS Query (generic:xqduqrj.info)	4054467	163
5		Suspicious user-agent strings	10004	46
6		Suspicious DNS Query (generic:dupuwj.com)	4047992	36
7		Suspicious DNS Query (generic:yzurdo.com)	4071154	35
8		Suspicious DNS Query (generic:v1v2x1l5c6oqxdh1k842.com)	4032853	28
9		Suspicious DNS Query (conficker:duryqma.cc)	4053993	28
10		Suspicious DNS Query (generic:nsoz5ffw2r14.www5.gmz.cc)	4046884	24
11		PHP CGI Query String Parameter Handling Information Disclosure and DoS Vulnerability	34804	24

CONTACTS

SOPRA **www.sopra.com**

Yann PITAULT @ yann.pitault@sopra.com

CYBER TEST SYSTEMS **www.cybertestsystems.com**

ANNEXES

TOP 25 OF THREATS WITH CRITICAL SEVERITY

	Severity	Threat/Content Name	ID	Repeat Count
1	CRITICAL	Bot: Mariposa Command and Control	12652	226
2		Win32.Conficker.C p2p	12544	13

TOP 25 OF THREATS WITH HIGH SEVERITY

	Severity ▲	Threat/Content Name	ID	Repeat Count
1	HIGH	PHP CGI Query String Parameter Handling Code Injection Vulnerability	34858	24
2		PHP CGI Query String Parameter Handling Code Injection Vulnerability	34790	24
3		SIP INVITE Method Request Flood Attempt	40016	14
4		GIF File With Embeded JavaScript Obfuscation Exploit	34194	9
5		TippingPoint IPS Audit Log Telnet Failure Cross-Site Scripting	33096	9
6		Symantec AntiVirus RAR Archive Decompression Buffer Overflow	31386	9
7		Multiple Vendor Telnet Client env_opt_add Buffer Overflow	30486	1

TOP 25 OF THREATS WITH MEDIUM SEVERITY

	Severity	Threat/Content Name	ID	Repeat Count
1	MEDIUM	Suspicious DNS Query (generic:lyekbv.com)	4070566	1.2 K
2		Suspicious DNS Query (generic:etnkragvqojrxryq.info)	4042853	984
3		Suspicious DNS Query (generic:ggirkj.com)	4047973	639
4		Suspicious DNS Query (generic:xqduqrj.info)	4054467	163
5		Suspicious user-agent strings	10004	46
6		Suspicious DNS Query (generic:dupuwj.com)	4047992	36
7		Suspicious DNS Query (generic:yzurdo.com)	4071154	35
8		Suspicious DNS Query (generic:v1v2x1l5c6oqxdh1k842.com)	4032853	28
9		Suspicious DNS Query (conficker:duryqma.cc)	4053993	28
10		Suspicious DNS Query (generic:nsoz5ffw2r14.www5.gmz.cc)	4046884	24
11		PHP CGI Query String Parameter Handling Information Disclosure and DoS Vulnerability	34804	24
12		Suspicious DNS Query (generic:smrmpcugjwur.info)	4087839	20
13		Suspicious DNS Query (generic:hdozyk.com)	4019179	20
14		Suspicious DNS Query (generic:jqlomoiyjrqf.org)	4039883	20
15		Suspicious DNS Query (generic:aoguue.com)	4042665	16
16		Suspicious DNS Query (generic:adpiik.com)	4071025	15
17		Suspicious DNS Query (generic:nbeyeo.com)	4047998	13
18		Suspicious DNS Query (generic:olbnqc.com)	4030143	12
19		Suspicious DNS Query (generic:vu914a1s3z2oe1qyxd5d.net)	4055304	11
20		HTTP SQL Injection Attempt	30514	10
21		Suspicious DNS Query (generic:63je6ct10tj60zlosq68.com)	4061361	8
22		Buffer overflow in the On-Access Scanner in McAfee VirusScan	31438	8
23		Suspicious DNS Query (generic:vsrrhi.com)	4032335	8
24		Suspicious DNS Query (generic:17mjyg71onmb7df4dulq.net)	4061355	8
25		Suspicious DNS Query (generic:ulukrv.com)	4045248	8

TOP 25 OF THREATS WITH LOW SEVERITY

	Severity	Threat/Content Name	ID	Repeat Count
1	LOW	SIP Register Request Attempt	33592	23.7 K
2		Sipvicious.Gen User-Agent Traffic	13272	13.2 K
3		JavaScript Obfuscation Detected	31825	1.2 K
4		HTTP Cross Site Scripting Vulnerability	34851	298
5		HTTP GET Requests Long URI Anomaly	30800	217
6		JavaScript Obfuscation Detected	31826	161
7		Morto RDP Request Traffic	13274	125
8		UNIX Portmapper Remote Infomation Retrieving Attempt	32796	66
9		HTTP Directory Traversal Vulnerability	30844	64
10		Microsoft ASP.Net Information Leak Vulnerability	33436	20
11		Snort URIContent Rules Detection Evasion Vulnerability	33334	1
12		Invalid HTTP Version Found	34386	1

TOP 25 OF THREATS WITH INFORMATIONAL SEVERITY

	Severity	Threat/Content Name	ID	Repeat Count
1	INFORMATIONAL	DGA NXDOMAIN response	36518	14.0 K
2		HTTP Unauthorized Error	34556	6.6 K
3		HTTP WWW-Authentication Failed	31708	5.6 K
4		HTTP OPTIONS Method	30520	3.4 K
5		DNS ANY Request	34842	3.0 K
6		HTTP Request ACE Encoded Domain Name Access	31298	905
7		DGA NXDOMAIN response Found	40040	269
8		Microsoft remote desktop connect initial attempt	33020	255
9		Microsoft ASP.NET Remote Unauthenticated Denial of Service Vulnerability	32513	210
10		Microsoft Communicator INVITE Flood Denial of Service Vulnerability	31993	144
11		SSH2 Login Attempt	31914	77
12		Failed Authentication Through Mail Protocol	31709	68
13		Generic GET Method Buffer Overflow Vulnerability	34267	52
14		Adobe PDF File With Embedded Javascript	31971	13
15		Suspicious or malformed HTTP Referer field	35554	10
16		SIP Bye Request Attempt	34520	8
17		HTTP Non RFC-Compliant Response Found	32880	7