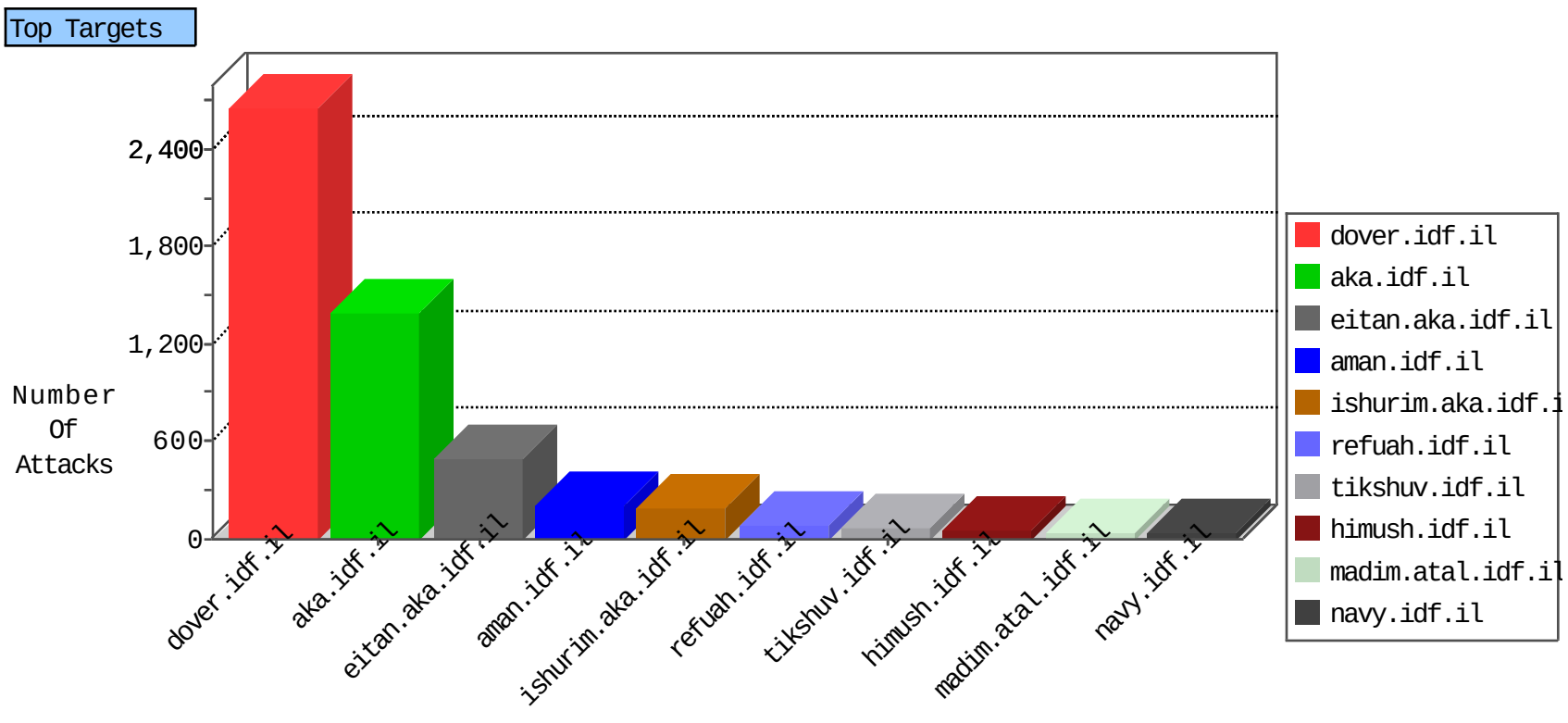
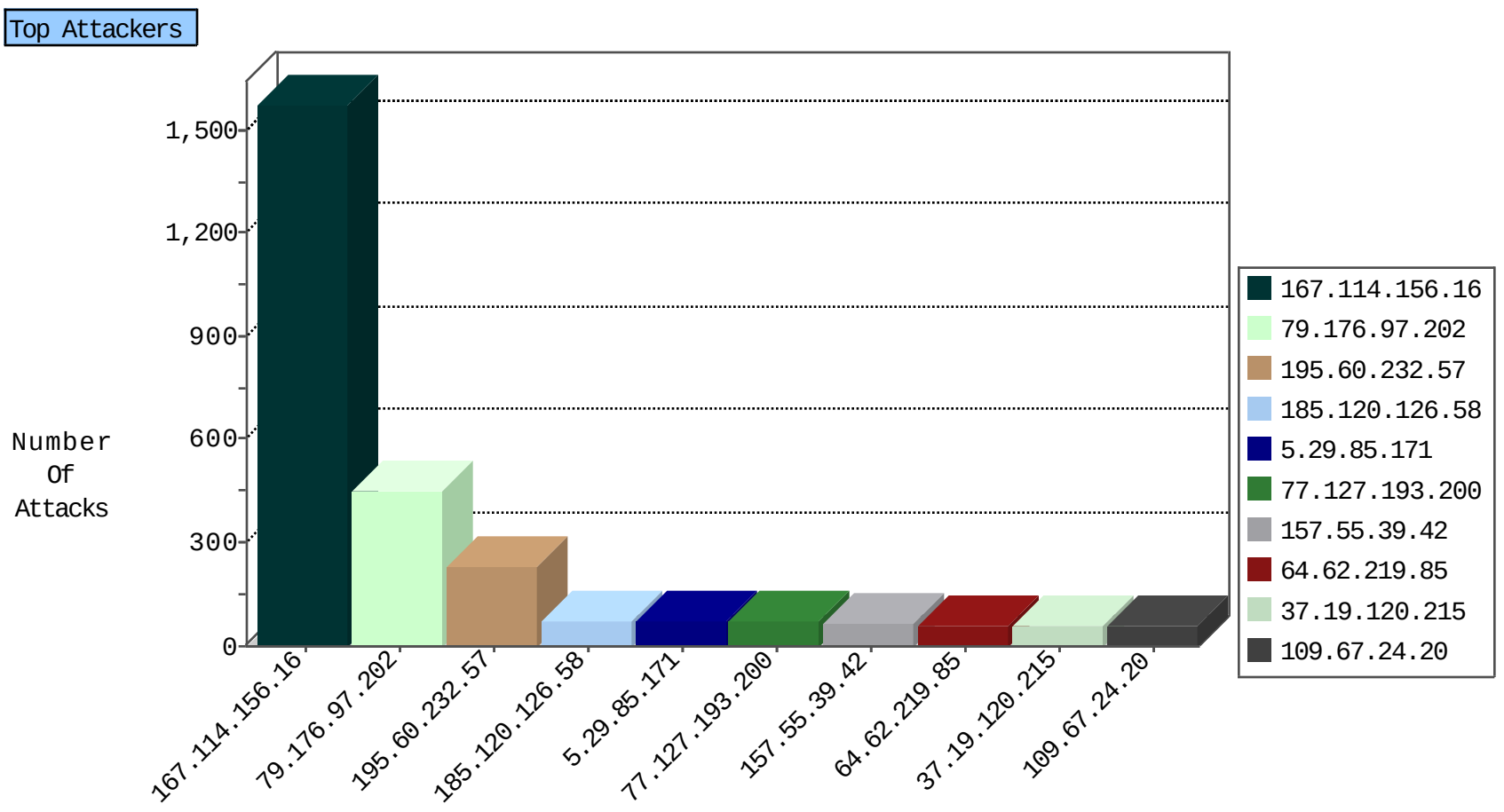
12-13-2015-21:04:00 to 12-13-2015-22:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



12-13-2015-21:04:00 to 12-13-2015-22:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3157
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	4
5.136.138.229	Russian Federation	147.237.76.148	gqcenter.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
46.166.139.20	Netherlands	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1

12-13-2015-21:04:00 to 12-13-2015-22:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-13-2015-21:04:00 to 12-13-2015-22:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
59.45.79.117	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
203.197.205.118	147.237.76.199	India	e.nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
59.45.79.117	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
196.47.173.21	147.237.76.38	Cote D'Ivoire	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
189.198.111.223	147.237.72.14	Mexico	dover.idf.il(old)	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.45.79.117	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
87.68.62.159	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.77.179	China	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
223.199.80.11	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.45.79.117	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
203.197.205.118	147.237.76.199	India	e.nakchal.idf.il	ET SCAN NMAP -f -sS	1
59.45.79.117	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
91.218.246.103	147.237.0.35	Russian Federation	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
40.115.58.160	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.176	China	matpash.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1

12-13-2015-21:04:00 to 12-13-2015-22:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.176.97.202	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	414
195.60.232.57	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	120
195.60.232.57	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	98
77.127.193.200	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	66
185.120.126.58		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	50
157.55.39.42	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	38
5.29.85.171	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	35
5.29.85.171	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	35
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
37.26.146.174	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
176.13.4.155	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	33
109.67.24.20	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	28
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	28
109.67.24.20	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	28
79.179.160.140	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
185.120.126.58		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	25
157.55.39.42	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
79.180.132.156	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
37.19.120.215	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	24
37.19.120.215	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	23
176.13.4.214	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	23
176.31.117.76	France	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	23
85.250.60.105	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	22
85.250.60.105	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	22
37.142.68.31	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
64.62.219.85	United States	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
37.142.68.31	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	19
84.229.161.201	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	16
84.229.161.201	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
31.210.187.183	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
176.12.143.81	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
82.81.13.84	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
157.55.39.31	United States	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.86.95	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
85.64.228.138	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
64.62.219.85	United States	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
149.88.140.146	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
85.64.228.138	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
176.13.19.49	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
79.181.120.53	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
84.109.115.213	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
176.13.7.45	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
176.13.2.72	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
85.130.243.113	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
176.12.142.86	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
46.19.85.20	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
79.181.120.53	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
46.19.86.64	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
157.55.39.173	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
212.179.90.106	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12

12-13-2015-21:04:00 to 12-13-2015-22:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.176.97.202	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 79.176.97.202	Block	33
84.94.38.200	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	21
2.52.45.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
23.236.52.170	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 23.236.52.170	Block	6
46.19.85.96	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.64	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.16.108	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.127.157.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.178.210.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.20.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
93.173.137.95	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
213.57.14.239	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/promotioncube/	Block	2
46.19.85.212	Israel	147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
207.46.13.171	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.85.212	Israel	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	2
109.66.178.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	2
176.13.0.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
46.19.85.212	Israel	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	2
109.66.178.20	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	2
107.178.195.163	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
79.179.99.94	Israel	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	1
185.120.125.50		147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
132.66.222.158	Israel	147.237.72.156	aman.idf.il	Unknown HTTP Request Method Â®Â¾ZFt in URL v[ÃŠ[[#20]]×€Â¹ÂŠf[Ë†[[#25]]Â¼[Ö¶[[#3]]&×Ÿ`Ö²[[#20]]Ã¼×¥×ƒ×'×€ÂŒv×žu&rfÂžÖ¼Â¸×ªÂžpiÂšÂ¼Ö·Ã¼mÂ©6[[#21]]Ãœ}f[[#31]]bÃšsÖ·k[[#8]]lâ€ 2cr>>u!×´6×´×™ÃœcÂ¨Ãžâ€"g%u[[#30]]~[[#3]]Â§â€™@×°×´kÂš,Â¿×,h{[[#27]]Ã¿ÂŠ_Ã–Â´[[#19]]cgu	Block	1
2.54.5.187	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	1
66.249.66.93	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/shared/ajax/setivgallerycontrol.aspx	Block	1
46.117.110.137	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
132.66.222.158	Israel	147.237.72.156	aman.idf.il	Illegal Byte Code Character in Method Â®Â¾ZFt	Block	1
84.94.41.184	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
79.183.6.26	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
207.46.13.169	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/miktzoa/	Block	1
46.19.85.212	Israel	147.237.77.216	dover.idf.il	Distributed Abnormally Long Request	Block	1
109.64.217.236	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 109.64.217.236 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
173.252.120.110	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
31.168.30.155	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
95.86.111.58	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 95.86.111.58	Block	1
2.52.132.78	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.65.71.158	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/tmuna/	Block	1
132.66.222.158	Israel	147.237.72.156	aman.idf.il	Illegal URL Path Encoding v[ÃŠ[[#20]]×€Â¹ÂŠf[Ë†[[#25]]Â¼[Ö¶[[#3]]&×Ÿ`Ö²[[#20]]Ã¼×¥×ƒ×'×€ÂŒv×žu&rfÂžÖ¼Â¸×ªÂžpiÂšÂ¼Ö·Ã¼mÂ©6[[#21]]Ãœ}f[[#31]]bÃšsÖ·k[[#8]]lâ€ 2cr>>u!×´6×´×™ÃœcÂ¨Ãžâ€"g%u[[#30]]~[[#3]]Â§â€™@×°×´kÂš,Â¿×,h{[[#27]]Ã¿ÂŠ_Ã–Â´[[#19]]cgu	Block	1
132.66.222.158	Israel	147.237.72.156	aman.idf.il	Abnormally Long Header Line request header name	Block	1
80.246.137.77	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.96	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
107.178.195.171	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
79.179.99.94	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/xmlrpc.php	Block	1
199.30.24.152	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-he/dover.aspx	Block	1
149.78.185.32	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
94.249.60.127	Jordan	147.237.77.74	law.idf.il	E-mail collector robots 14	Block	1

12-13-2015-21:04:00 to 12-13-2015-22:04:00