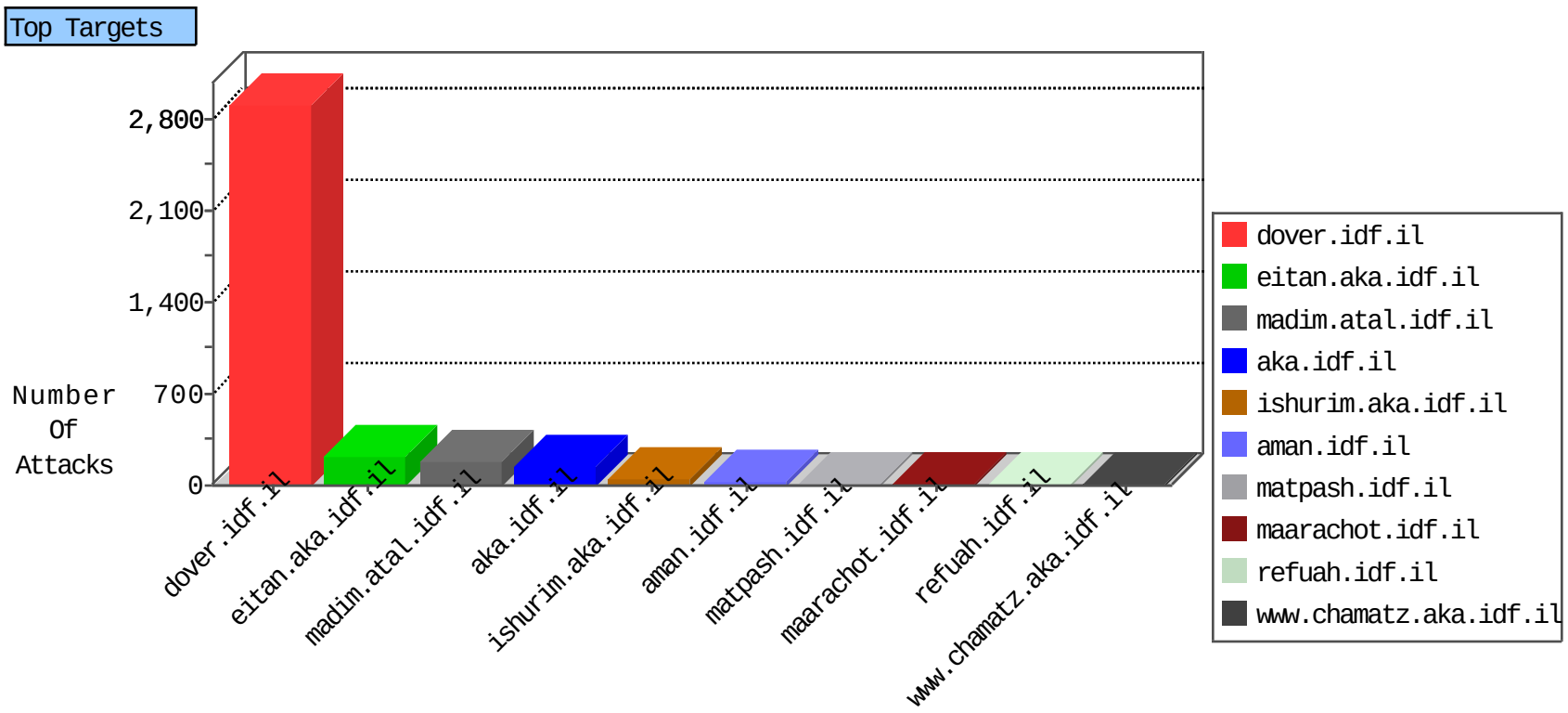
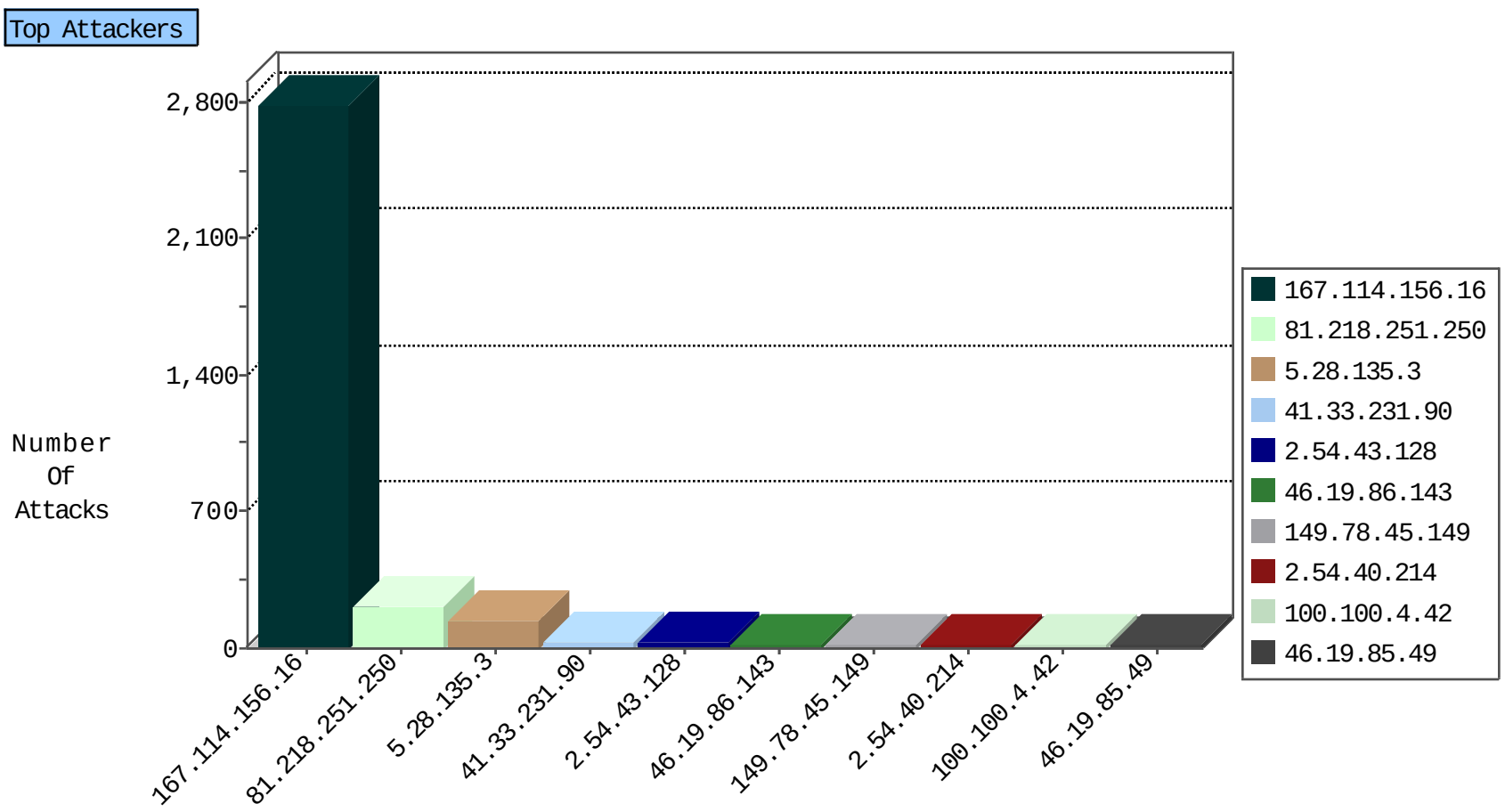
12-04-2015-08:04:04 to 12-04-2015-09:04:04

IDF Under Attack Daily Report





12-04-2015-08:04:04 to 12-04-2015-09:04:04

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	3447
198.20.69.98	United States	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
180.97.106.37	China	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
198.20.70.114	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
180.97.106.36	China	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
180.97.106.37	China	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
202.112.51.96	China	147.237.77.19	law-forum.idf.il	block-sp-traf1	drop	1
180.97.106.36	China	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
180.97.106.162	China	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
218.104.207.11	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
180.97.106.37	China	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1

12-04-2015-08:04:04 to 12-04-2015-09:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.113.80	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

12-04-2015-08:04:04 to 12-04-2015-09:04:04

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	3
66.249.64.233	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
110.77.213.245	147.237.8.27	Thailand	e.madim.atal.idf.i	ET SCAN NMAP -sS window 2048	1
110.77.213.245	147.237.8.27	Thailand	e.madim.atal.idf.i	ET SCAN NMAP -f -sS	1
85.17.156.69	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
82.117.208.243	147.237.77.179		e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
183.33.202.102	147.237.0.33	China	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
110.77.213.245	147.237.8.27	Thailand	e.madim.atal.idf.i	ET SCAN NMAP -sS window 1024	1
85.17.156.69	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN Potential SSH Scan	1
85.17.156.69	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	1

12-04-2015-08:04:04 to 12-04-2015-09:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
81.218.251.250	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
46.19.86.143	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	22
149.78.45.149	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
2.54.147.50	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
100.100.4.42		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.49	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.49	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
212.179.218.166	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.255.253.188	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.32.55	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.40.214	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
85.130.253.120	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.40.214	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
212.179.218.166	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.173	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.218	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
27.50.90.106	Australia	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	4
46.19.86.88	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.144.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.37.18	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
95.104.138.199	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.15.122	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.88.5.105	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.80.196.44	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
2.54.40.214	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
2.54.43.34	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
100.100.4.42		147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	3
188.120.148.234	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
185.3.144.164	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.54.122	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.64.6.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
89.138.233.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.120.150.157	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.88	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.26.148.249	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
80.246.139.252	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
66.249.64.98	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.86.88	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
46.19.86.228	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
79.183.53.230	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
5.29.60.218	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
46.19.86.228	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
89.138.223.216	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
37.142.68.109	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
82.80.196.44	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	2
46.19.85.10	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

12-04-2015-08:04:04 to 12-04-2015-09:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.251.250	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 81.218.251.250	Block	181
5.28.135.3	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	80
5.28.135.3	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 5.28.135.3	Block	62
2.54.43.128	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
46.19.85.229	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	6
176.12.145.143	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
198.1.68.234	United States	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	3
176.13.18.16	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
116.12.55.118	Singapore	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
95.108.158.144	Russian Federation	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.121.46.202	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
198.1.68.234	United States	147.237.77.170	maarachot.idf.il	Distributed Admin Blocking	Block	2
176.12.140.37	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
116.12.55.118	Singapore	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/index.php	Block	2
116.12.55.118	Singapore	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	2
198.1.68.234	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/index.php	Block	2
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
5.29.101.29	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gius	Block	2
185.3.144.78	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
45.35.71.179		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
213.57.215.159	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.179.116.220	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
2.54.180.139	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dover/site/mainpage.asp	Block	1
207.46.13.72	United States	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
173.254.202.145	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/	Block	1
66.249.64.235	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18858-he/dover.aspx	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
31.210.189.252	Israel	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
85.154.206.179	Oman	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
69.132.108.222	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
2.54.40.214	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.60	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/×©×§×•×¤×™×ª 10	Block	1
116.12.55.118	Singapore	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 116.12.55.118	Block	1
107.130.122.243	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 107.130.122.243	Block	1
46.19.85.134	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
81.218.251.250	Israel	147.237.76.200	eitan.aka.idf.il	Too Many 404: Response Code per Session	Block	1
207.46.13.72	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/w/load.php	Block	1
66.249.64.243	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.243	Block	1
58.59.237.168	China	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1
109.64.131.189	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	1
31.210.189.252	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
93.172.141.56	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
79.179.99.94	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
66.249.64.98	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
107.130.122.243	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	1
66.249.64.243	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-20896-he/dover.aspx×″ ×ž×©×™×›×•	Block	1

12-04-2015-08:04:04 to 12-04-2015-09:04:04