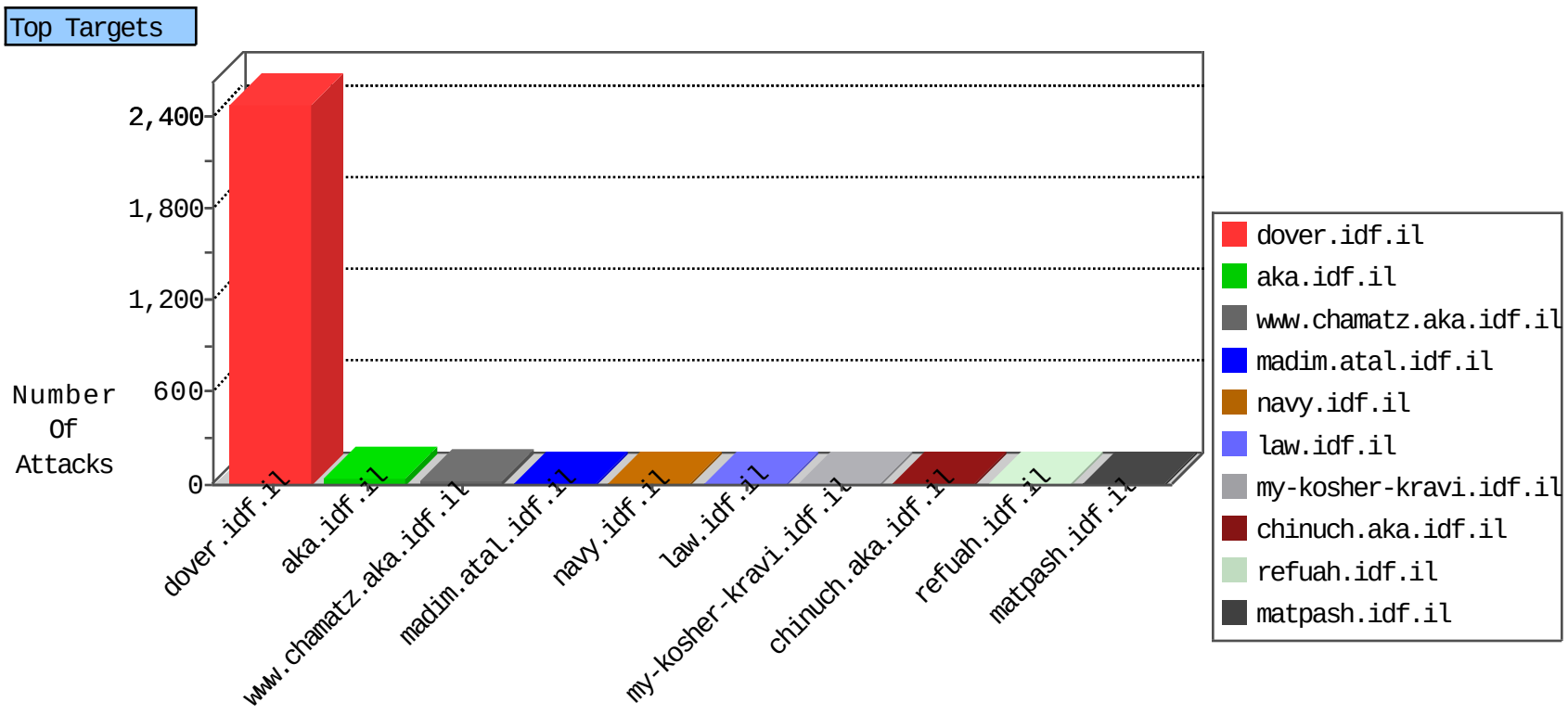
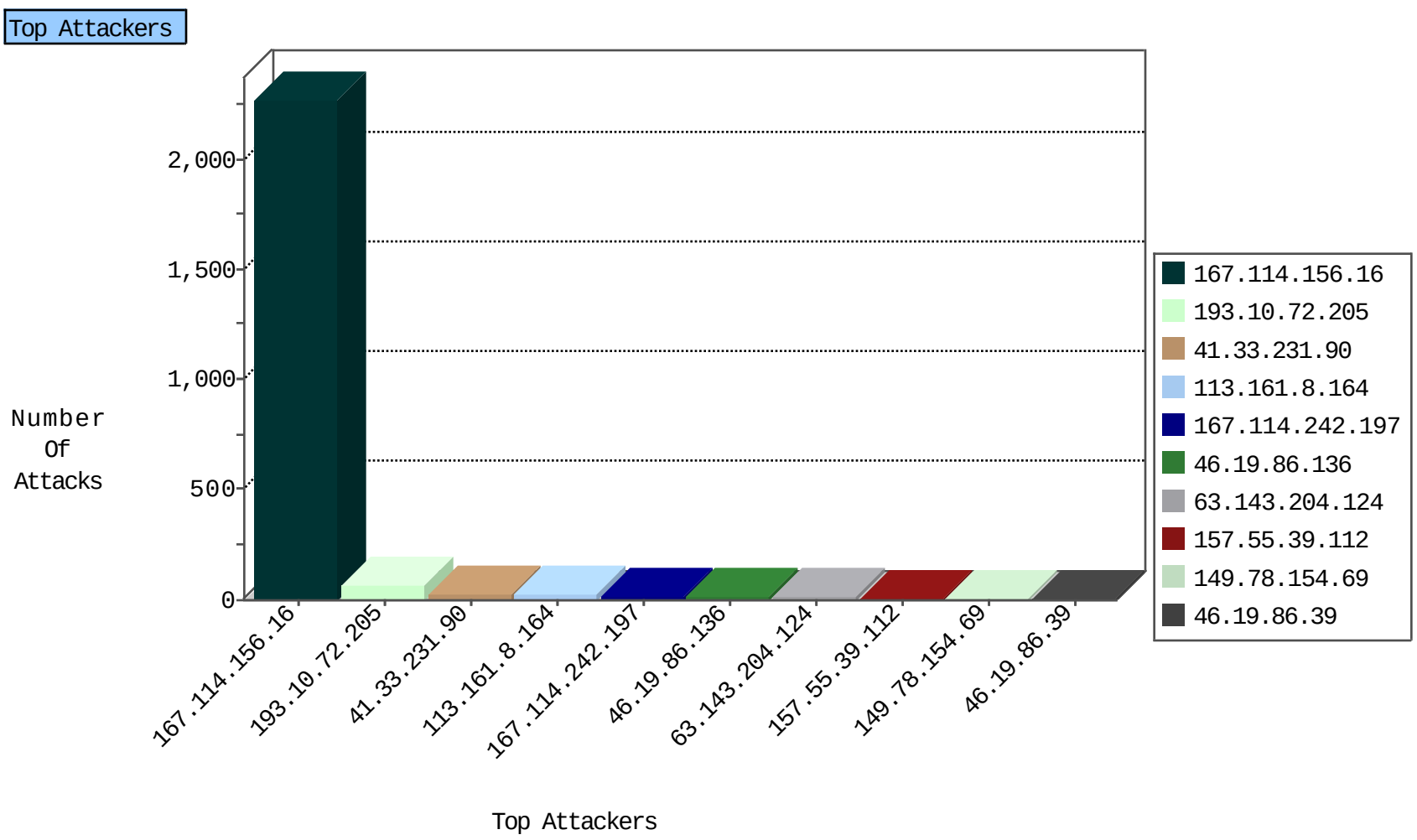
12-08-2015-05:04:00 to 12-08-2015-06:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



12-08-2015-05:04:00 to 12-08-2015-06:04:00

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	3551
66.249.78.29	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	93
167.114.242.197	Canada	147.237.77.226	www.chamatz.aka.idf.il	Frk_Under_Attack_Con_Https	drop	2
185.35.62.85	Switzerland	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
71.6.165.200	United States	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1

12-08-2015-05:04:00 to 12-08-2015-06:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.242.197	Canada	147.237.77.226	www.chamatz.aka.idf.il	13891: TLS: OpenSSL Encrypted/Unencrypted Heartbeat Packet	Permit	1

12-08-2015-05:04:00 to 12-08-2015-06:04:00

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
172.36.3.24	147.237.0.34	United States	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
98.119.105.221	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sS window 4096	1
61.240.144.64	147.237.0.34	China	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
201.173.133.175	147.237.77.176	Mexico	matpash.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
199.168.136.165	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
185.56.82.14	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
180.153.104.125	147.237.72.156	China	aman.idf.il	ET SCAN NMAP -sS window 4096	1
180.153.104.125	147.237.72.156	China	aman.idf.il	ET SCAN NMAP -f -sS	1
172.36.3.24	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
98.119.105.221	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
201.173.133.175	147.237.77.216	Mexico	dover.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
199.168.136.165	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
195.54.209.148	147.237.72.166	Russian Federation	aka.idf.il	ET SCAN NMAP -sS window 1024	1
185.56.82.14	147.237.0.33	Netherlands	idf.il	ET SCAN NMAP -sS window 1024	1
183.60.252.84	147.237.77.234	China	halag.idf.il	ET SCAN NMAP -sS window 4096	1
180.153.104.125	147.237.72.156	China	aman.idf.il	ET SCAN NMAP -sS window 2048	1

12-08-2015-05:04:00 to 12-08-2015-06:04:00

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	28
113.161.8.164	Vietnam	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
63.143.204.124	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
167.114.242.197	Canada	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	8
167.114.242.197	Canada	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.55	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
157.55.39.112	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
113.161.8.164	Vietnam	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
213.57.128.172	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
113.161.8.164	Vietnam	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.14	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
80.246.133.75	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
157.55.39.112	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
149.78.19.151	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
2.54.50.0	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
80.246.133.75	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
66.249.66.1	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
40.77.167.65	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
77.75.76.169	Czech Republic	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.39	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.134	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
207.46.13.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
68.191.34.27	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
50.87.144.145	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.153	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.86.39	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
131.253.24.142	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
216.218.206.104	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
77.237.138.51	Czech Republic	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
184.105.247.216	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
65.55.218.54	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.135	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
69.64.105.142	United States	147.237.77.216	dover.idf.il	Header Rejection	header rejection pattern found in request	monitor	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.156	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.39	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
131.253.26.238	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
216.218.206.104	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
193.10.72.205	Sweden	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
66.249.65.37	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
157.55.39.6	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.86.109	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.140	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
212.199.182.150	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

12-08-2015-05:04:00 to 12-08-2015-06:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
193.10.72.205	Sweden	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 193.10.72.205	Block	66
46.19.86.136	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	13
199.30.24.39	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	2
199.30.25.250	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.12.146.181	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.66.40	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
157.55.39.145	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.145	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	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
77.237.138.51	Czech Republic	147.237.77.74	law.idf.il	Unauthorized URL Access to /	Block	1
46.19.86.39	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
188.143.232.14	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1283-en/dover.aspx	Block	1
130.193.50.11	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
98.195.130.182	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
66.249.66.69	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/about/memorial/pages/ehudtal.aspx	Block	1
157.55.39.145	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/_ajax/setplugin/taleswords	Block	1
5.255.253.151	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
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	1
85.250.46.163	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
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	1
136.243.36.96	Germany	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/228-he/faq.aspx	Block	1
107.77.77.226	United States	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
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	1
69.64.105.142	United States	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1
5.255.253.166	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/templates/login/login.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
95.108.158.173	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
213.8.204.15	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.65.112	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/6/size100x0/2796.jpg	Block	1
193.10.72.205	Sweden	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
141.212.122.129	United States	147.237.77.226	www.chamatz.aka.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
107.77.77.226	United States	147.237.77.216	dover.idf.il	Malformed URL	Block	1
207.46.13.132	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/8/638.pdf	Block	1
69.64.105.142	United States	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
37.140.141.35	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19779-he/kkkkkkk=34d19df9kkkkkkk_34d19df9	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
95.108.158.191	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
66.249.66.16	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
193.10.72.205	Sweden	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/piwik.php	Block	1
157.55.39.112	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/news/<a href=	Block	1
107.77.77.226	United States	147.237.77.216	dover.idf.il	Unknown HTTP Request Method ssionId=4lcjbr45fqccwkectziysi55 in URL	Block	1
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	1
77.75.76.162	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/page/28/	Block	1
40.77.167.65	United States	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
184.105.247.196	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
109.66.29.108	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
98.195.130.182	United States	147.237.77.74	law.idf.il	PHP Attempt	Block	1

12-08-2015-05:04:00 to 12-08-2015-06:04:00