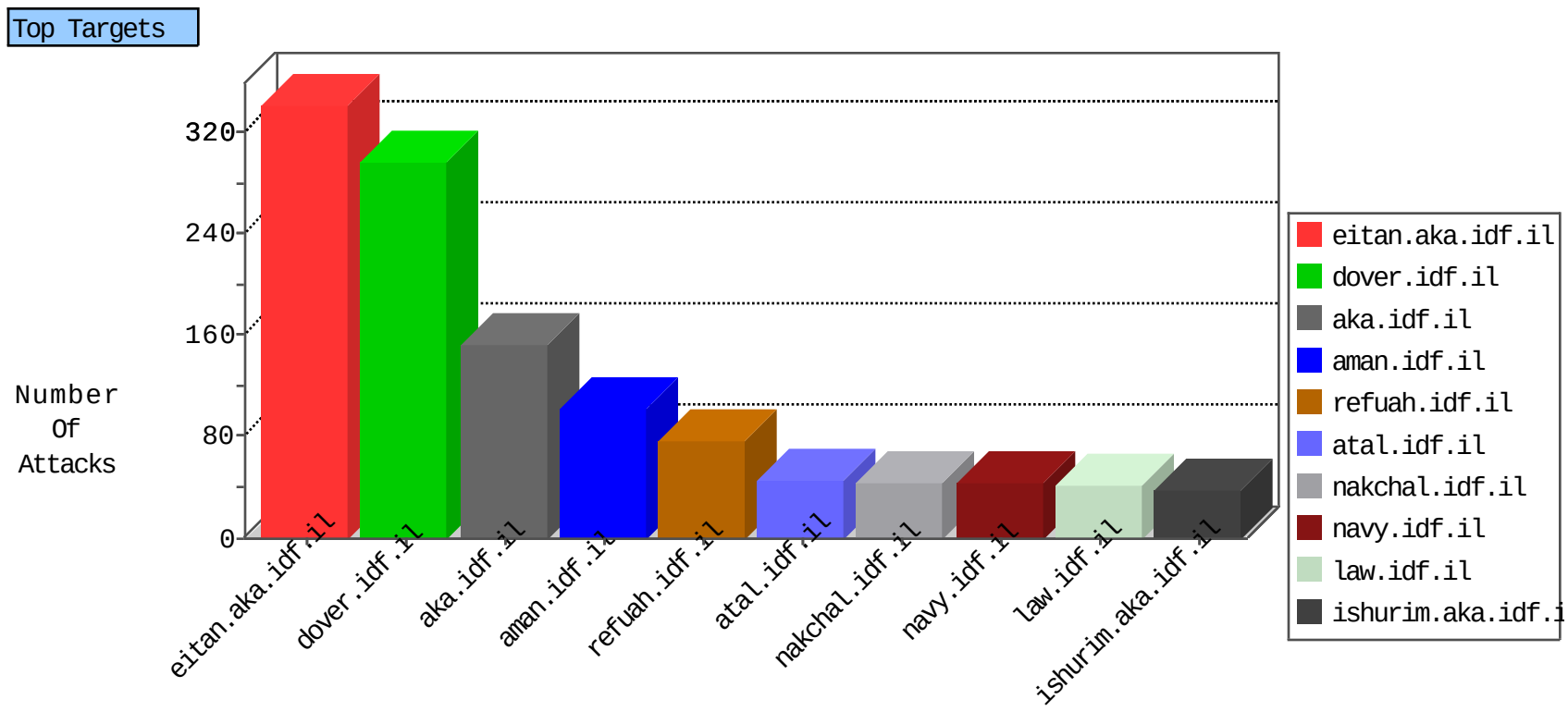
09-12-2016-16:04:02 to 09-12-2016-17:04:02

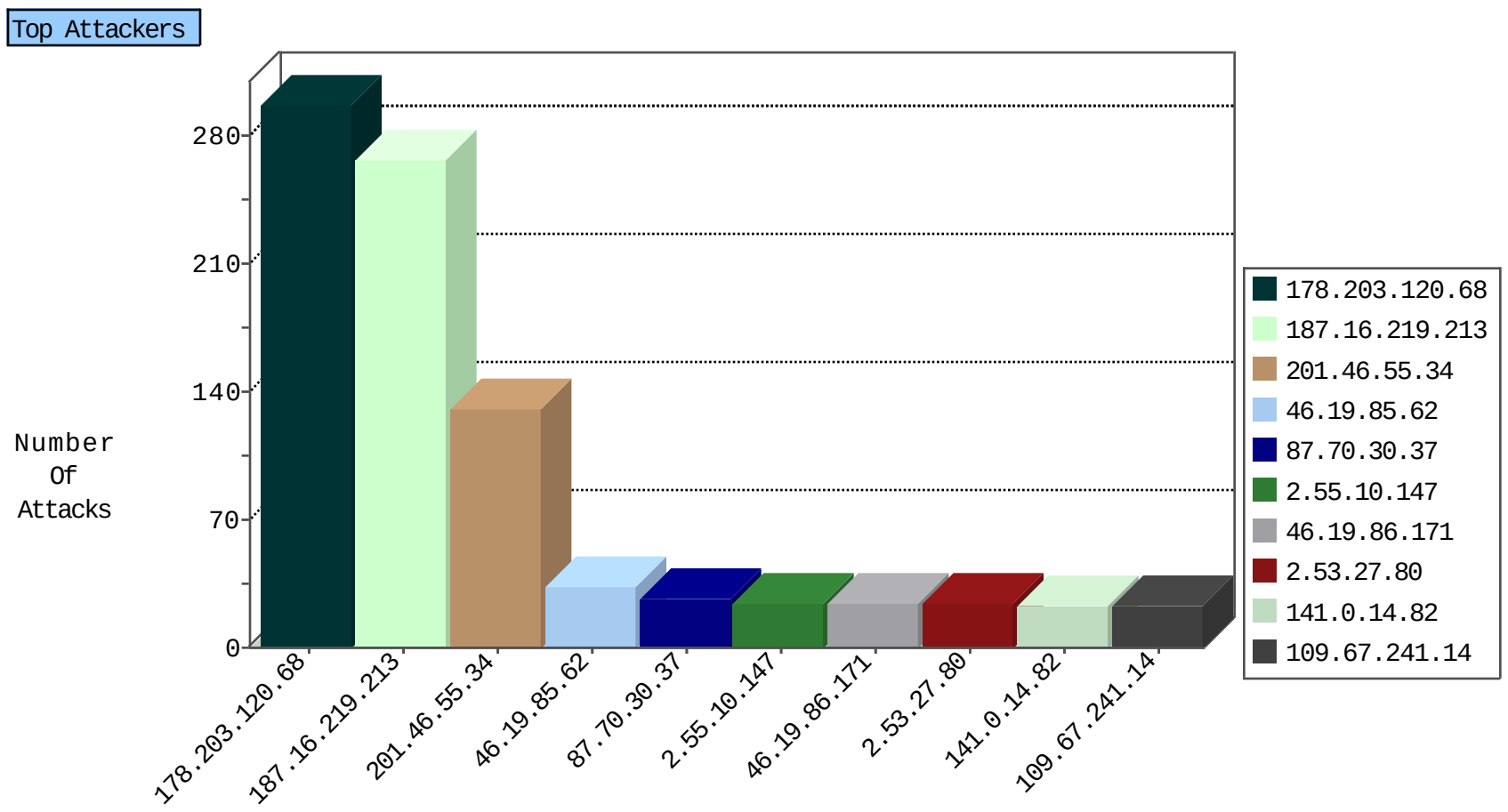
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

09-12-2016-16:04:02 to 09-12-2016-17:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	36
80.178.89.55	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
46.19.85.62	Israel	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	6
131.247.2.241	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
195.113.161.83	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.22.150.78	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.93.229.138	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
153.90.1.34	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
164.107.127.12	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.195.4.69	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-12-2016-16:04:02 to 09-12-2016-17:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
178.203.120.68	Germany	147.237.76.200	eitan.aka.idf.il	C1000074: HTTP: majestic bot	Permit	293
178.203.120.68	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	4
188.40.95.70	Germany	147.237.76.42	refuah.idf.il	C1000074: HTTP: majestic bot	Permit	2
106.38.241.105	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

09-12-2016-16:04:02 to 09-12-2016-17:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.77.170	Israel	maarachot.idf.il	Xenu Link Sleuth User Agent	2
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	2
95.35.85.16	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
201.73.83.242	147.237.77.216	Brazil	dover.idf.il	ET SCAN NMAP -sS window 4096	1
46.117.105.16	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.174.93.50	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
192.116.83.2	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.184.195.114	147.237.76.44	Russian Federation	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
93.158.203.147	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
31.184.195.114	147.237.72.166	Russian Federation	aka.idf.il	ET SCAN Potential SSH Scan	1
163.172.129.15	147.237.76.38	United Kingdom	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
87.71.20.169	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.53.164.104	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
163.172.129.15	147.237.0.35	United Kingdom	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
85.64.176.234	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
125.212.235.111	147.237.0.19	Vietnam	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
77.127.36.225	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
116.12.175.233	147.237.8.14	Singapore	e.orchot.idf.il	ET SCAN NMAP -f -sS	1
50.84.213.146	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 3072	1
109.66.150.60	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
50.84.213.146	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -f -sS	1
109.64.1.212	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.115.20	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.174.93.50	147.237.77.243	Netherlands	mobile.idf.il	ET SCAN Potential SSH Scan	1
201.73.83.242	147.237.77.216	Brazil	dover.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.116	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.174.93.50	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN Potential SSH Scan	1
31.184.195.114	147.237.76.30	Russian Federation	himush.idf.il	ET SCAN Potential SSH Scan	1
176.13.250.32	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
89.248.172.140	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
5.102.195.227	147.237.77.216	Israel	dover.idf.il	ET SCAN HTTP OPTIONS invalid method case	1
163.172.129.15	147.237.76.30	United Kingdom	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
87.69.127.198	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.157.38	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
125.212.235.111	147.237.0.33	Vietnam	idf.il	ET SCAN Potential SSH Scan	1
79.178.37.236	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
116.12.175.233	147.237.8.14	Singapore	e.orchot.idf.il	ET SCAN NMAP -sS window 2048	1
62.219.131.74	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.123.101.31	147.237.0.17	United Kingdom	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
50.84.213.146	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 2048	1
109.66.25.169	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-12-2016-16:04:02 to 09-12-2016-17:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
2.55.10.147	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
141.0.14.82	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	23
141.0.15.207	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	19
193.43.246.250	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	18
46.19.85.62	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
187.16.219.213	Brazil	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
187.16.219.213	Brazil	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
187.16.219.213	Brazil	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
187.16.219.213	Brazil	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
187.16.219.213	Brazil	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
187.16.219.213	Brazil	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
187.16.219.213	Brazil	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
187.16.219.213	Brazil	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
187.16.219.213	Brazil	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
2.53.27.80	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
187.16.219.213	Brazil	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
187.16.219.213	Brazil	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
187.16.219.213	Brazil	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
187.16.219.213	Brazil	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
187.16.219.213	Brazil	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
187.16.219.213	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
187.16.219.213	Brazil	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
187.16.219.213	Brazil	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
187.16.219.213	Brazil	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
187.16.219.213	Brazil	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
84.94.65.88	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
187.16.219.213	Brazil	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
87.70.30.37	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
87.70.30.37	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
109.66.25.169	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
187.16.219.213	Brazil	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
187.16.219.213	Brazil	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
46.120.102.72	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
2.53.145.148	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.62	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
46.19.86.177	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
5.22.134.69	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.167	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
201.46.55.34	Brazil	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
201.46.55.34	Brazil	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
201.46.55.34	Brazil	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
201.46.55.34	Brazil	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
201.46.55.34	Brazil	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
201.46.55.34	Brazil	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.86.171	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
201.46.55.34	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
201.46.55.34	Brazil	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
2.53.27.80	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
201.46.55.34	Brazil	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.86.171	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6

09-12-2016-16:04:02 to 09-12-2016-17:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.67.241.14	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	23
218.87.63.144	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 218.87.63.144	Block	17
85.64.157.76	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	10
46.19.85.127	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	9
218.87.63.144	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	6
192.115.86.17	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 192.115.86.17	Block	5
109.253.222.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
79.178.8.83	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
212.199.118.19	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 212.199.118.19	Block	2
46.19.86.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
89.138.163.196	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.120.113.100	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
217.194.198.145	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.53.142.131	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
176.13.15.119	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
82.166.76.90	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 82.166.76.90	Block	1
77.138.232.58	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
212.25.79.133	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
89.139.169.212	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
79.178.82.68	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main kapatz	Block	1
62.0.101.97	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/trigger.png	Block	1
2.53.169.241	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
176.13.17.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
84.108.138.120	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.138.240.25	France	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
79.179.50.204	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
66.249.66.174	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
2.53.174.39	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
84.109.160.43	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 84.109.160.43	Block	1
77.139.56.173	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
212.199.118.19	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/back.png	Block	1
46.116.119.176	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.116.119.176	Block	1
80.246.130.42	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/nakha	Block	1
192.115.86.17	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/8/size338x0/1808.jpg	Block	1
5.22.134.69	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
77.139.135.45	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
213.151.32.163	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 213.151.32.163	Block	1
46.120.102.72	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
2.53.52.147	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
157.55.39.241	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/dynamic_map/dynamic_map.aspx	Block	1
80.246.137.87	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.76.53	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
192.243.55.131	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=59390&docid=76111	Block	1
38.111.147.88	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1

09-12-2016-16:04:02 to 09-12-2016-17:04:02