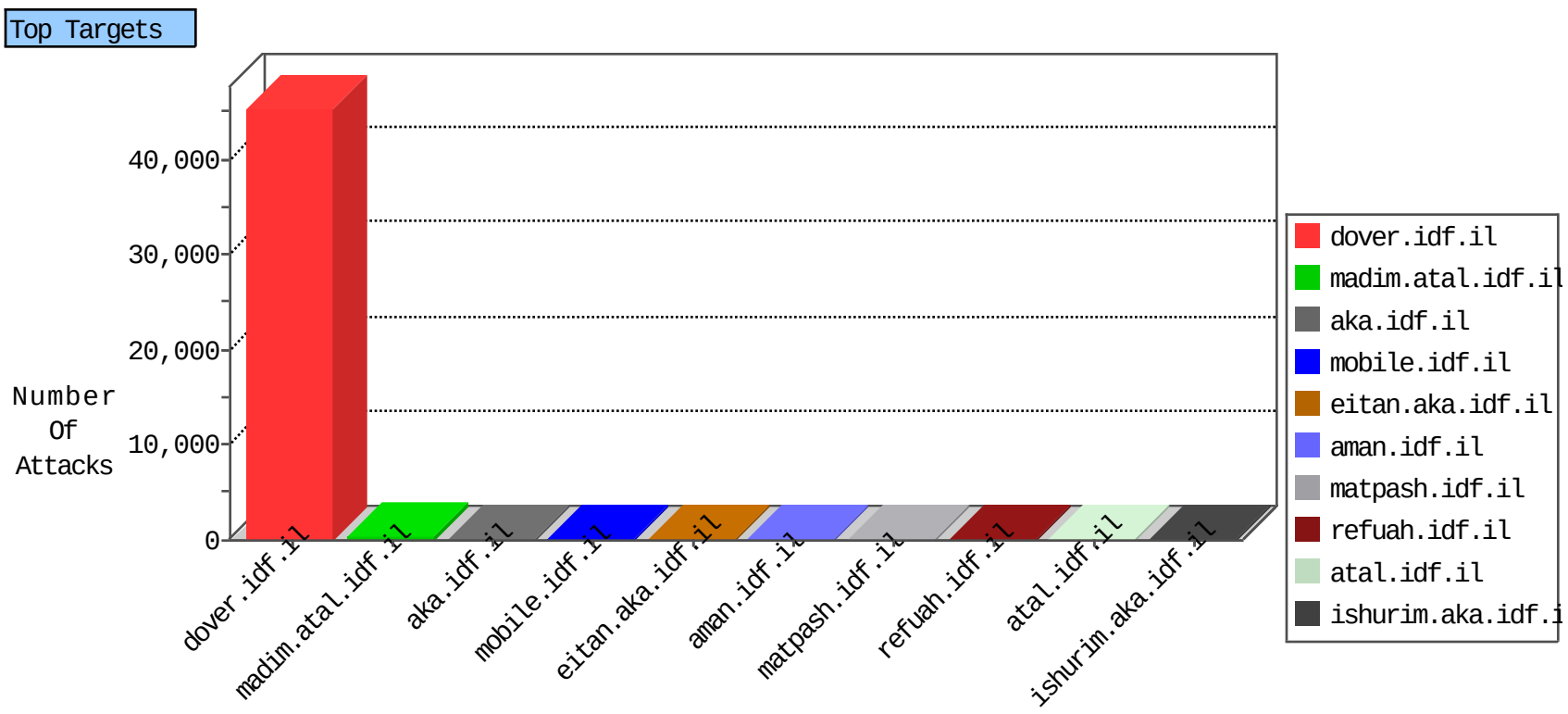
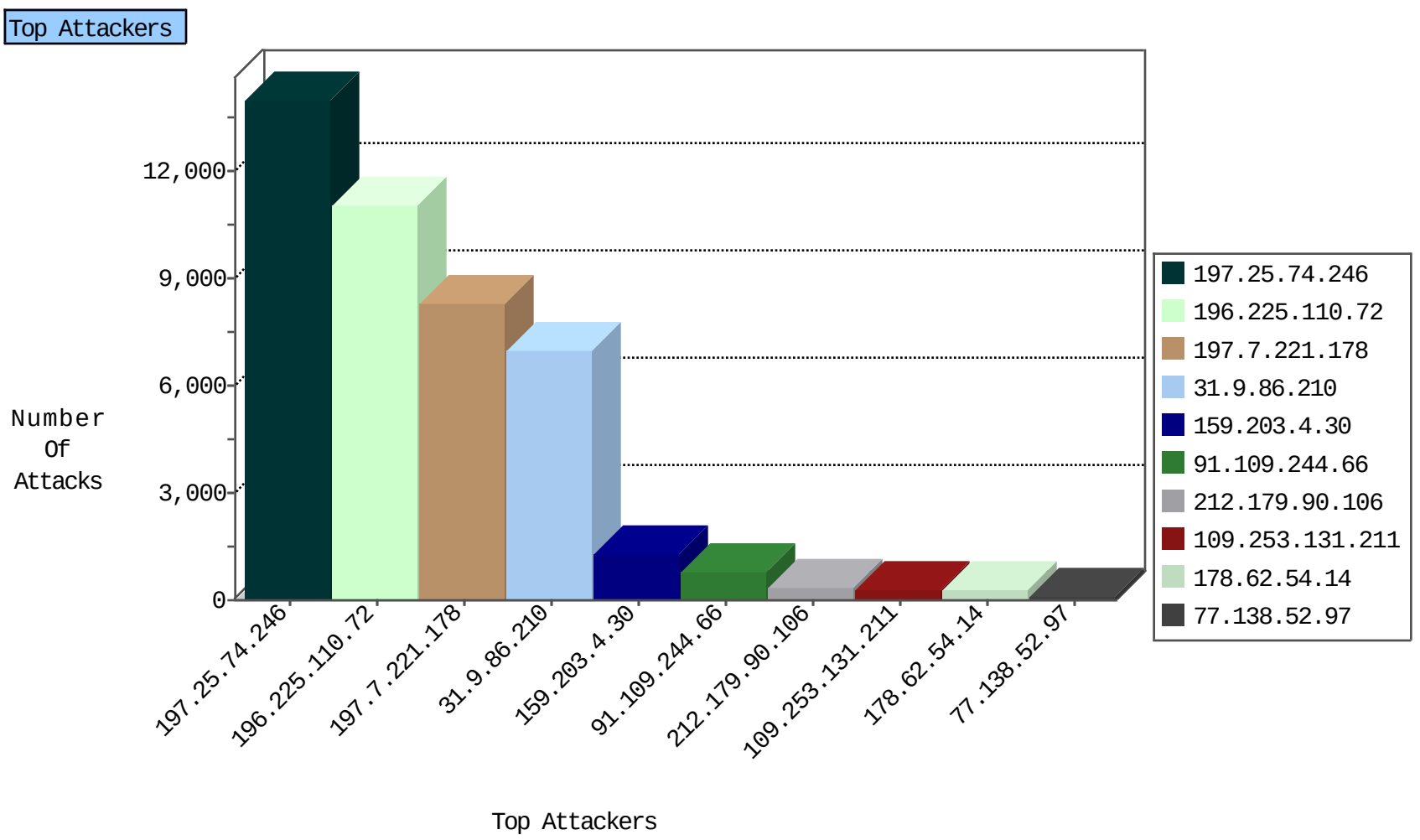
09-17-2016-23:04:07 to 09-18-2016-00:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-17-2016-23:04:07 to 09-18-2016-00:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
197.7.221.178	Tunisia	147.237.77.216	dover.idf.il	DOS-HTTP-torshammer	forward	7439
197.7.221.178	Tunisia	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2810
197.7.221.178	Tunisia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	174
197.25.74.246	Tunisia	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	9
159.203.4.30	Canada	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	6
194.254.215.12	France	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	5
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	4
178.62.54.14	United Kingdom	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	3
193.1.13.14	Ireland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
51.255.218.57	France	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	3
147.83.29.234	Spain	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
153.90.1.34	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.223.8.114	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
130.206.158.138	Spain	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
200.19.159.34	Brazil	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
193.166.167.4	Finland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
139.78.141.243	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
204.85.191.10	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
130.194.252.8	Australia	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
42.112.10.73	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1
198.82.160.221	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
42.112.10.66	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1
42.112.10.74	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
216.48.80.14	Canada	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
42.112.10.69	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1
165.242.90.128	Japan	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.97.74.14	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
42.112.10.70	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
194.29.178.14	Poland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.112	United States	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1

09-17-2016-23:04:07 to 09-18-2016-00:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.119.115.28	Ukraine	147.237.77.216	dover.idf.il	15323: HTTP: User-Agent (MRSPUTNIK)	Block	5
199.58.86.206	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3
162.210.196.97	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

09-17-2016-23:04:07 to 09-18-2016-00:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
192.81.133.226	147.237.76.148	United States	gqcenter.aka.idf.il	GPL SCAN superscan echo	1
91.197.232.15	147.237.8.28	Russian Federation	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
183.25.248.90	147.237.76.197	China	e.himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.197.232.15	147.237.0.33	Russian Federation	idf.il	ET SCAN Potential SSH Scan	1
139.162.13.205	147.237.76.200	Singapore	eitan.aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
88.249.106.23	147.237.8.45	Turkey	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
91.197.232.15	147.237.77.179	Russian Federation	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
91.197.232.15	147.237.77.19	Russian Federation	law-forum.idf.il	ET SCAN Potential SSH Scan	1
91.197.232.15	147.237.76.44	Russian Federation	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
91.197.232.15	147.237.76.30	Russian Federation	himush.idf.il	ET SCAN Potential SSH Scan	1
91.197.232.15	147.237.72.14	Russian Federation	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
91.197.232.15	147.237.8.45	Russian Federation	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
192.81.133.226	147.237.76.147	United States	chinuch.aka.idf.il	GPL SCAN superscan echo	1
91.197.232.15	147.237.8.27	Russian Federation	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
179.43.141.228	147.237.8.28	Switzerland	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
91.197.232.15	147.237.0.15	Russian Federation	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
109.236.80.12	147.237.72.167	Netherlands	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
62.210.189.248	147.237.77.243	France	mobile.idf.il	ET SCAN Potential SSH Scan	1
91.197.232.15	147.237.77.178	Russian Federation	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
91.197.232.15	147.237.76.199	Russian Federation	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
91.197.232.15	147.237.76.39	Russian Federation	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
91.197.232.15	147.237.72.217	Russian Federation	e.idf.il	ET SCAN Potential SSH Scan	1
91.197.232.15	147.237.8.46	Russian Federation	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1

09-17-2016-23:04:07 to 09-18-2016-00:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
197.25.74.246	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12469
196.225.110.72	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9207
31.9.86.210	Syrian Arab Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6997
197.7.221.178	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4795
197.25.74.246	Tunisia	147.237.77.216	dover.idf.il	drop		drop	1375
196.225.110.72	Tunisia	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1301
159.203.4.30	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1174
91.109.244.66	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	766
196.225.110.72	Tunisia	147.237.77.216	dover.idf.il	drop		drop	540
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	357
197.7.221.178	Tunisia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	288
178.62.54.14	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	257
197.25.74.246	Tunisia	147.237.77.216	dover.idf.il	drop	SAM rule	drop	156
197.7.221.178	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	92
197.7.221.178	Tunisia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	80
62.16.72.250	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	69
197.7.221.178	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	66
159.203.4.30	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	64
37.26.147.207	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
109.226.40.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
159.203.4.30	Canada	147.237.77.216	dover.idf.il	Streaming Engine: TCP SYN Modified Retransmission	Data received before SYN-ACK was acknowledged. Stripping all packet data.	drop	36
77.138.52.97	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	35
79.178.240.247	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
197.7.221.178	Tunisia	147.237.77.216	dover.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	34
68.180.229.223	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
197.7.221.178	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	27
185.110.108.52	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
128.177.161.146	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
46.120.222.245	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
197.7.221.178	Tunisia	147.237.77.216	dover.idf.il	Web Server Enforcement Violation	Torshammer Denial of Service Tool	reject	22
156.204.16.63	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
46.19.85.41	Israel	147.237.77.243	mobile.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
84.95.133.162	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	20
85.250.214.228	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
80.226.24.12	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
84.95.133.162	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	18
109.253.147.14	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
109.253.215.11	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
197.7.221.178	Tunisia	147.237.77.216	dover.idf.il	SYN Attack		monitor	16
197.25.74.246	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	16
5.0.176.229	Syrian Arab Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
141.226.218.29	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
84.95.133.162	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	15
77.138.124.172	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
157.55.39.20	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
77.138.52.97	France	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
84.85.214.91	Netherlands	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
109.253.150.222	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15

09-17-2016-23:04:07 to 09-18-2016-00:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.131.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	288
46.19.86.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
159.203.4.30	Canada	147.237.77.216	dover.idf.il	Distributed Abnormally Long Request	Block	6
159.203.4.30	Canada	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	6
159.203.4.30	Canada	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	6
217.132.31.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.124.11.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.64.108	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/moreinfo/tichnun.yosh@gmail.com	Block	1
37.26.148.222	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
157.55.39.123	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
77.138.121.47	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/kamlar/home/default.asp	Block	1
46.19.85.149	Israel	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method 9258cc8a.1454353725.6.1472983483.1472983483.; in URL asp.net_sessionid=nglebp55m0baa2551lt0km45	Block	1
93.172.107.65	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$passwordUpdate$txtPasswordRepeat in www.aka.idf.il/main/giyus/faq.aspx	None	1
66.249.64.183	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/main	Block	1
40.77.167.62	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1
77.139.51.45	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/haredim/general.aspx	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
46.19.85.149	Israel	147.237.76.42	refuah.idf.il	Abnormally Long Request method	Block	1
79.179.116.9	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/homepage.aspx	Block	1
46.120.18.206	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
139.162.13.205	Singapore	147.237.76.200	eitan.aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/nakha	Block	1
46.19.85.149	Israel	147.237.76.42	refuah.idf.il	Illegal HTTP Version	Block	1
84.108.35.41	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/.well-known/assetlinks.json	Block	1
5.28.144.189	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
139.162.13.205	Singapore	147.237.77.176	matpash.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
46.19.85.149	Israel	147.237.76.42	refuah.idf.il	Malformed URL asp.net_sessionid=nglebp55m0baa2551lt0km45	Block	1
213.205.194.243	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/brothers/skira/default.asp	Block	1
85.64.16.218	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1

09-17-2016-23:04:07 to 09-18-2016-00:04:07