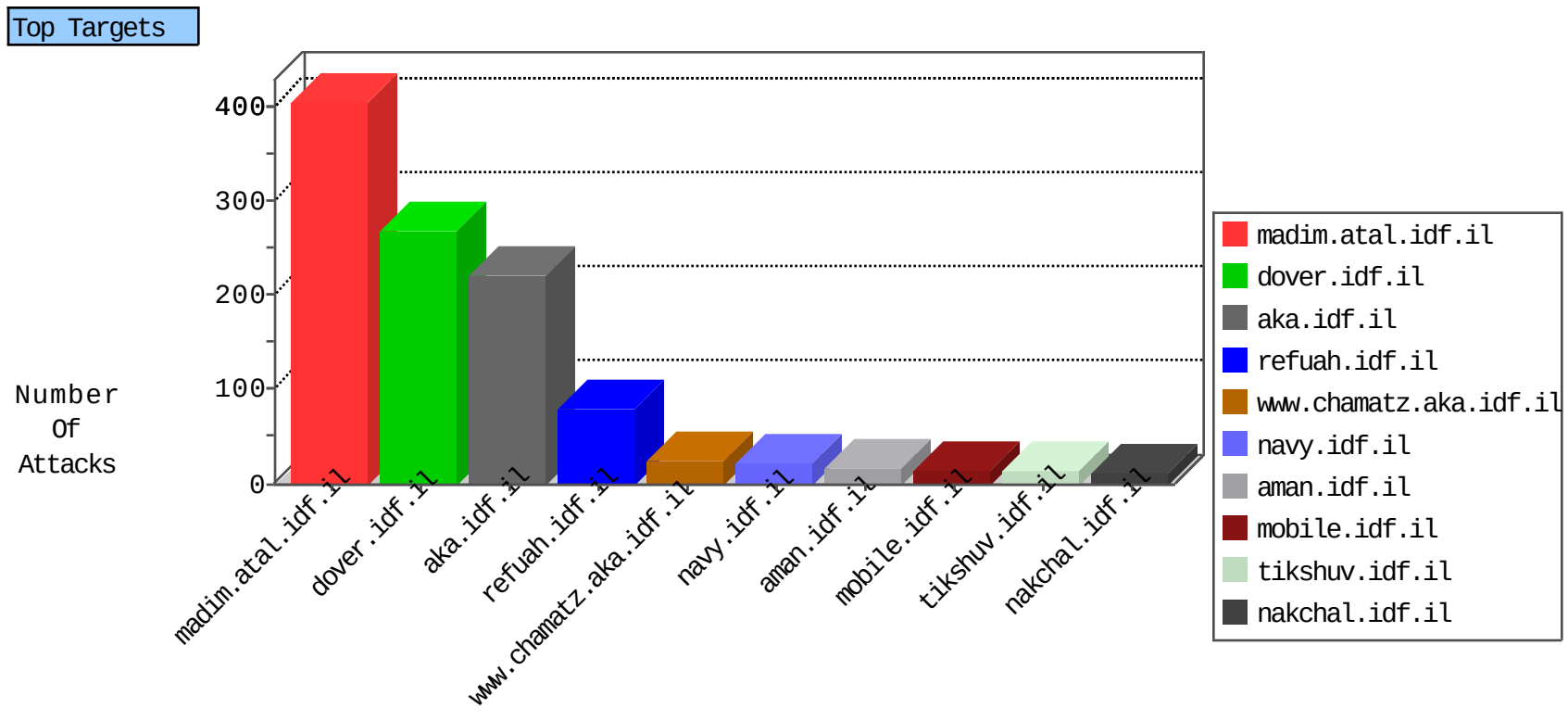
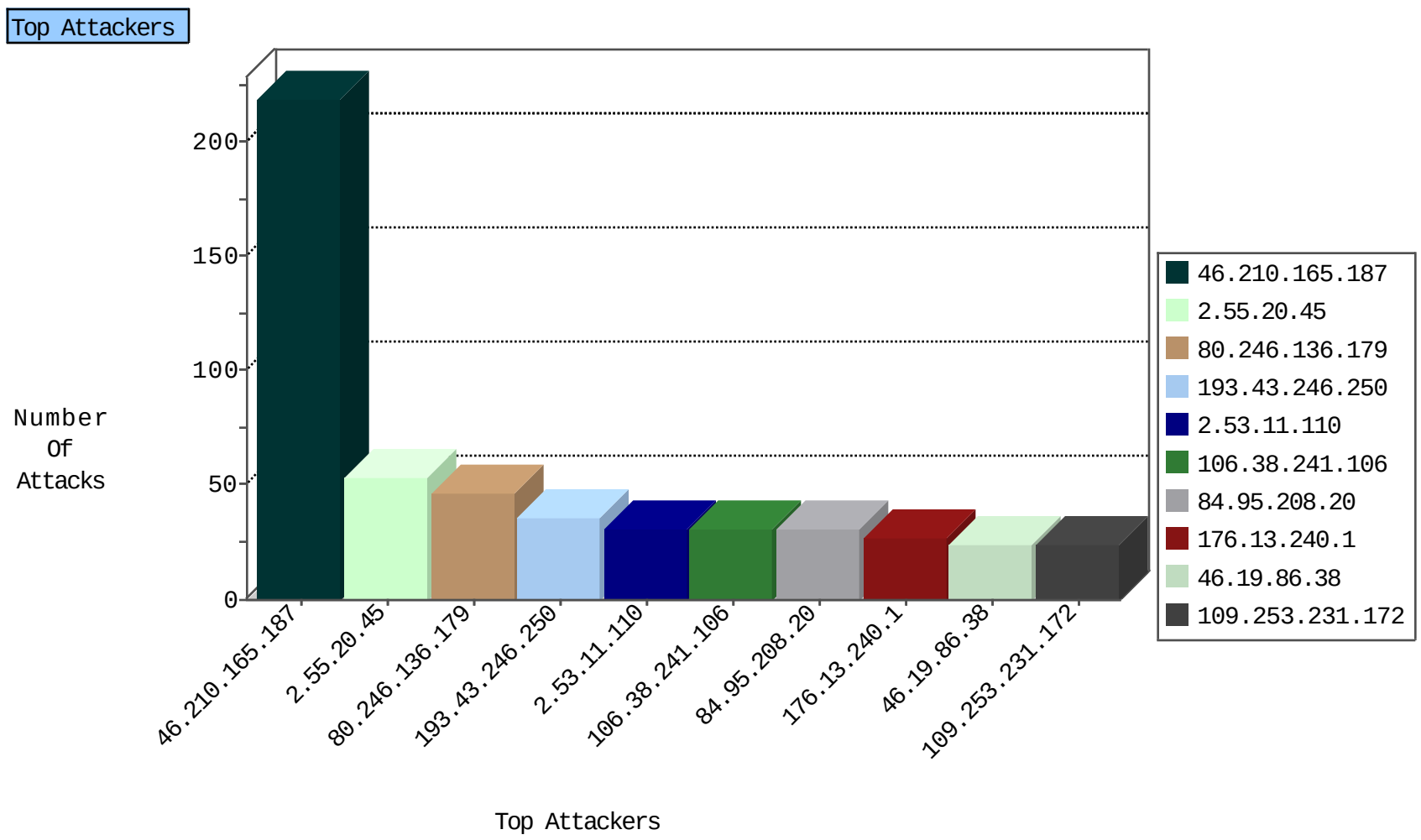
09-26-2016-09:04:04 to 09-26-2016-10:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-26-2016-09:04:04 to 09-26-2016-10:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.102.195.249	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
108.61.204.80	United States	147.237.76.177	ncore.idf.il	Black List	drop	1
210.19.13.209	Malaysia	147.237.76.177	ncore.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
45.63.70.29	United States	147.237.76.176	test.ncore.idf.i	Black List	drop	1

09-26-2016-09:04:04 to 09-26-2016-10:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.216	dover.idf.i	C1000071: HTTP: User Agent Sogou+web+spider	Permit	31
38.110.11.92	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	5
46.4.32.75	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	3
46.4.32.75	Germany	147.237.77.216	dover.idf.i	C1000074: HTTP: majestic bot	Permit	2
115.42.137.250	Singapore	147.237.77.216	dover.idf.i	12347: HTTP: PHP-CGI Query String Parameter Information Disclosure Vulnerability	Block	1
38.110.11.92	United States	147.237.72.166	aka.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	1

09-26-2016-09:04:04 to 09-26-2016-10:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
38.110.11.92	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	8
62.210.97.57	147.237.72.166	France	aka.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	5
141.226.244.49	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.55.190.72	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
128.199.42.73	147.237.77.176	Netherlands	matpash.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
87.71.49.237	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.94.140.177	147.237.77.226	Israel	www.chamatz.aka.idf.il	LOCAL_RULES - HTTP Request with OPTIONS method to a .doc file	1
212.179.1.218	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.182.119.210	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.29.211.62	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
210.19.13.209	147.237.0.16	Malaysia	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.150	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.116.94.67	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.7.125	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.29.182.31	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
139.162.187.89	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
2.53.47.42	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
113.176.215.79	147.237.76.42	Vietnam	refuah.idf.il	portscan: TCP Distributed Portscan	1
84.108.26.184	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.8.105.9	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.179.225.42	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.143.159.118	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.66.12	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
210.19.13.209	147.237.76.34	Malaysia	yohalan.idf.il	ET SCAN Potential SSH Scan	1
62.90.181.97	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
199.203.196.105	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.215	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.129.148.230	147.237.0.33	Latvia	idf.il	ET SCAN NMAP -sS window 1024	1
31.154.92.74	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-26-2016-09:04:04 to 09-26-2016-10:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
46.19.86.13	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
62.0.208.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.154	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
62.0.211.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
80.246.138.65	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
46.19.86.87	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
188.72.103.231	United Arab Emirates	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
176.13.240.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
62.90.193.162	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
62.0.211.1	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	7
62.0.208.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
176.13.1.70	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.32.179.88	Israel	147.237.72.166	aka.idf.il	SYN Attack		monitor	6
46.19.86.87	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.38	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.13.251.171	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.38	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
188.193.78.18	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.14	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.86.38	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.171	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
77.126.6.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.240.1	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.38	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.147.158	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
62.0.207.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.171	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.87	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
62.0.211.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
176.13.240.1	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
84.108.240.62	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
176.13.240.1	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.86.33	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
109.253.204.142	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.86.33	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.53.139.16	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.86.33	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.86.33	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.178.216.96	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.190	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
213.8.242.46	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
80.246.140.209	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
213.57.80.102	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
37.26.149.140	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
46.19.86.35	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
176.13.19.18	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
37.26.148.151	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
176.13.225.128	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.66	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3

09-26-2016-09:04:04 to 09-26-2016-10:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.210.165.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	206
2.55.20.45	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	53
80.246.136.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	45
2.53.11.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31
109.253.231.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
60.181.128.232	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 60.181.128.232	Block	14
176.13.227.127	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
176.13.227.46	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
194.90.151.18	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	6
193.34.57.101	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	6
60.181.128.232	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	5
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	4
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	4
109.253.216.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
176.13.6.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
37.26.149.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.138.13.147	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	2
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	2
185.32.179.33	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.138.232.79	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	2
176.13.228.63	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
84.95.208.20	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
2.55.35.66	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
176.13.225.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
194.114.146.227	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
37.26.148.222	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
194.90.99.193	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	1
84.95.208.20	Israel	147.237.72.156	aman.idf.il	PHP Attempt	Block	1
46.19.85.80	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
195.160.242.40	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/registrationwizard/step4.aspx	Block	1
81.218.57.61	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.53.167.186	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/gius	Block	1
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
212.185.61.13	Germany	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/giyus/	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
46.19.86.227	Israel	147.237.76.42	refuah.idf.il	Malformed URL	Block	1
37.26.148.244	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	PHP Attempt	Block	1
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/div.item	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
46.19.86.48	Israel	147.237.76.42	refuah.idf.il	Abnormally Long Request request version	Block	1
209.88.173.130	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 209.88.173.130	Block	1
81.223.254.34	Austria	147.237.77.216	dover.idf.il	Unauthorized URL Access to /robots.txt	Block	1
2.53.184.211	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.69.228	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_text.asp	Block	1
46.19.86.227	Israel	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method jj4c0v4iu in URL	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/piwik.php	Block	1

09-26-2016-09:04:04 to 09-26-2016-10:04:04