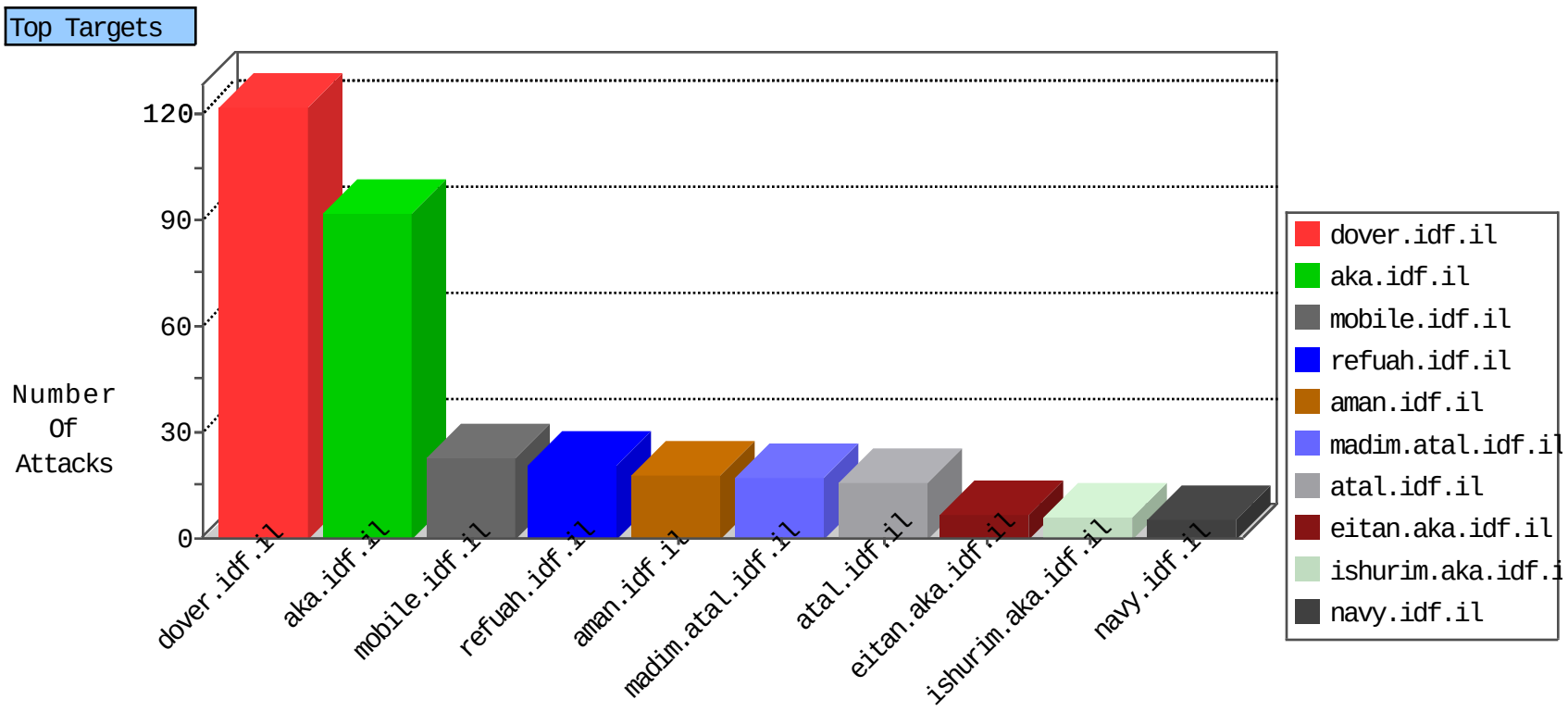
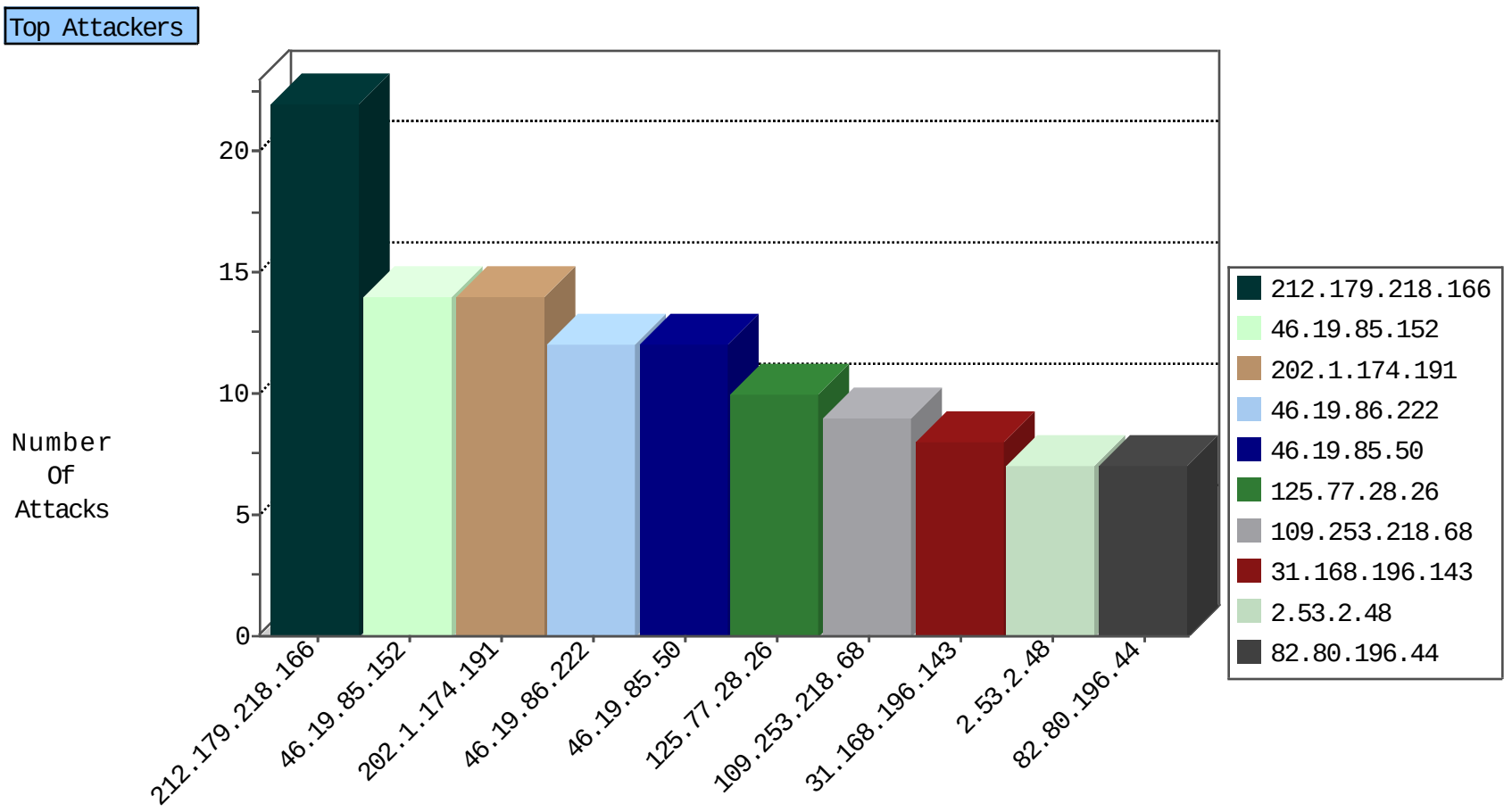
09-30-2016-08:04:03 to 09-30-2016-09:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-30-2016-08:04:03 to 09-30-2016-09:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.228.193	Israel	147.237.72.167	ishurim.aka.idf.il	DOSS-SSL-ClearText	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
71.6.146.185	United States	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1
93.158.200.66	Netherlands	147.237.76.196	e.sviva.idf.il	Black List	drop	1
78.129.171.175	United Kingdom	147.237.76.176	test.ncore.idf.il	Black List	drop	1
78.129.171.175	United Kingdom	147.237.76.197	e.himush.idf.il	Black List	drop	1
58.218.200.137	China	147.237.0.17	m.my-kosher-kravi.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
78.129.171.175	United Kingdom	147.237.76.199	e.nakchal.idf.il	Black List	drop	1

09-30-2016-08:04:03 to 09-30-2016-09:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
220.181.125.23	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	4
36.110.147.67	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

09-30-2016-08:04:03 to 09-30-2016-09:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.19.85.152	147.237.76.42	Israel	refuah.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	8
91.121.81.33	147.237.77.216	France	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
146.200.148.0	147.237.77.216	United Kingdom	dover.idf.il	Tehila - Perl LWP with fake user agent	2
58.218.200.137	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
183.129.160.229	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.93	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.129.15	147.237.77.226	United Kingdom	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.194	147.237.77.19	Netherlands	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
2.50.129.147	147.237.76.86	United Arab Emirates	navy.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.194	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
1.53.224.126	147.237.77.216	Vietnam	dover.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
78.129.171.173	147.237.76.177	United Kingdom	ncore.idf.il	ET SCAN Potential SSH Scan	1
66.249.75.167	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
58.218.200.137	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
192.249.66.247	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
58.218.200.137	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
163.172.129.15	147.237.77.243	United Kingdom	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.247	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.50.129.147	147.237.76.86	United Arab Emirates	navy.idf.il	ET SCAN NMAP -sS window 2048	1
94.102.48.194	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
2.50.129.147	147.237.76.86	United Arab Emirates	navy.idf.il	ET SCAN NMAP -f -sS	1
91.201.236.158	147.237.0.19	Ukraine	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
78.129.171.173	147.237.76.201	United Kingdom	e.atal.idf.il	ET SCAN Potential SSH Scan	1
78.129.171.173	147.237.8.14	United Kingdom	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1

09-30-2016-08:04:03 to 09-30-2016-09:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
31.168.196.143	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
212.179.218.166	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
212.179.218.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
212.179.218.166	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.50	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.50	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.26.147.189	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.2.48	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
132.66.222.47	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.190	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
185.32.179.35	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
87.69.229.218	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
202.1.174.191	Solomon Islands	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.64.51.188	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
109.253.218.68	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
202.1.174.191	Solomon Islands	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
109.253.223.60	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.214	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
46.19.86.222	Israel	147.237.77.216	dover.idf.il	SYN Attack		monitor	3
109.253.218.68	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.86.204	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
141.226.217.115	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
2.53.155.45	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
79.181.255.51	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.222	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
46.19.86.204	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
66.249.64.124	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.214	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
176.13.20.24	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
173.252.123.134	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
202.1.174.191	Solomon Islands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.152	Israel	147.237.76.42	refuah.idf.il	Streaming Engine: TCP Urgent Data Enforcement	TCP segment with urgent pointer (no data). Urgent data indication was stripped. Please refer to sk36869.	drop	2
176.13.8.237	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
80.246.137.234	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
185.58.6.178	Italy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
37.26.147.150	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
109.253.208.18	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
202.1.174.191	Solomon Islands	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
185.3.147.188	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
82.80.196.44	Israel	147.237.72.166	aka.idf.il	SYN Attack		monitor	2
46.121.65.16	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
84.95.208.20	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.73.142.222	Ukraine	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
31.168.134.100	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
46.19.85.152	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.222	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
31.168.134.100	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2

09-30-2016-08:04:03 to 09-30-2016-09:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
108.30.107.143	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 108.30.107.143	Block	4
31.154.3.222	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	4
77.138.144.246	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	3
37.142.251.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.181.255.51	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
31.178.144.59	Poland	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	3
192.243.55.135	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.135	Block	2
109.253.218.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.108.235.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.64.183	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-21744-ar/idfgdover.aspx	Block	1
192.243.55.129	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/tizmoret/gallery	Block	1
37.26.147.189	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
85.64.144.223	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il./favicon.ico	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/tizmoret/gallery/showpicture.asp	Block	1
213.8.204.68	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	1
66.249.64.113	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.113	Block	1
144.76.236.183	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
66.249.75.138	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/.well-known/apple-app-site-association	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/3/61353.jpg	Block	1
66.249.64.113	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/.well-known/apple-app-site-association	Block	1
213.8.204.68	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/xmlrpc.php	Block	1
2.53.2.48	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
176.13.16.153	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.76.52	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding 82G0l3ebf[@G}u@oTlGh8I]nprO in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
192.243.55.135	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/default.aspx	Block	1
46.19.85.84	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
108.30.107.143	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/	Block	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1379-he/dover.aspx	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/apple-app-site-association	Block	1
220.181.125.23	China	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 220.181.125.23	Block	1
185.58.6.178	Italy	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
84.108.144.22	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/894-9030-he	Block	1
66.249.76.61	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.61	Block	1
192.243.55.136	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.136	Block	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp	Block	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1381-he/dover.aspx	Block	1
66.249.64.134	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	1
220.181.125.23	China	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1078-he/atal.aspx	Block	1
192.243.55.129	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.129	Block	1
66.249.76.61	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/.well-known/apple-app-site-association	Block	1
192.243.55.136	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=58563	Block	1
66.249.64.105	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/.well-known/assetlinks.json	Block	1
141.226.161.82	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
77.138.116.235	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	1

09-30-2016-08:04:03 to 09-30-2016-09:04:03