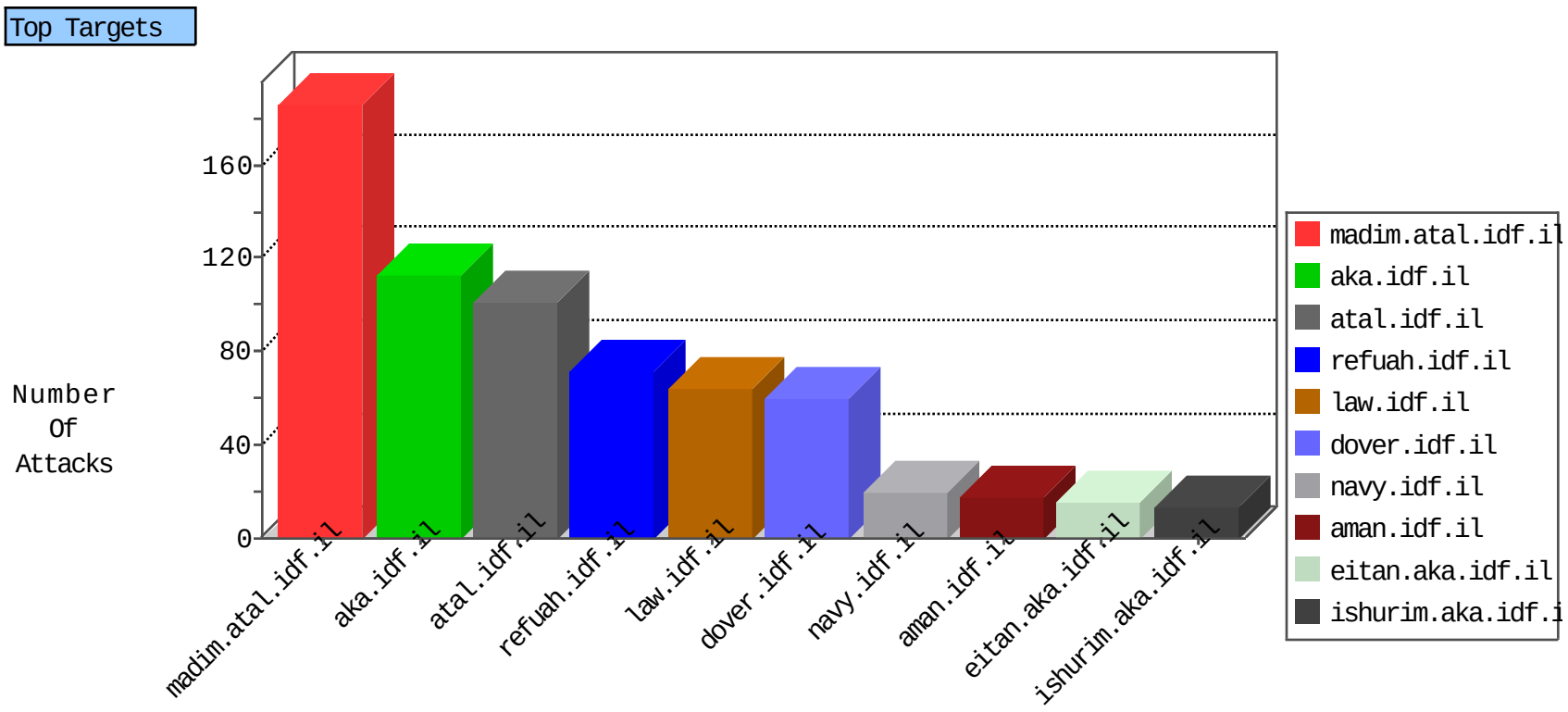
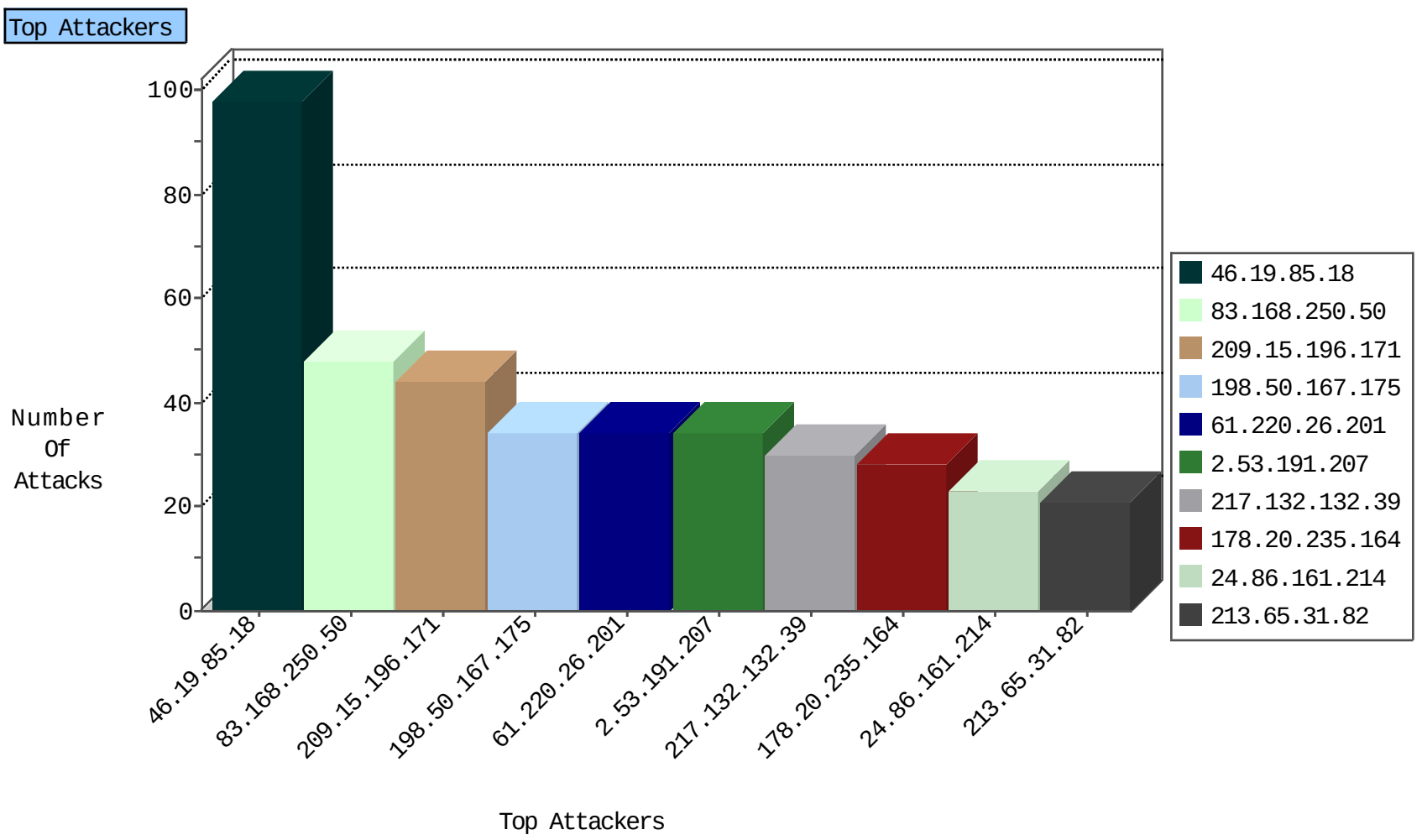
09-12-2016-11:19:56 to 09-12-2016-12:19:56

IDF Under Attack Daily Report





09-12-2016-11:19:56 to 09-12-2016-12:19:56

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	6
128.223.8.114	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	5
141.22.213.34	Germany	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	5
130.217.77.2	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
131.247.2.241	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
212.179.64.162	Israel	147.237.72.166	aka.idf.il	Black List	drop	3
31.168.133.226	Israel	147.237.72.167	ishurim.aka.idf.il	Black List	drop	3
141.212.113.178	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	2
193.1.13.14	Ireland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
211.1.156.90	Japan	147.237.72.167	ishurim.aka.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
194.29.178.14	Poland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
139.78.141.243	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
186.235.129.29	Brazil	147.237.76.147	chinuch.aka.idf.il	JLM_Purple_Con_Limit_Http	drop	1
130.206.158.138	Spain	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
192.243.55.129	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
200.19.159.34	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-12-2016-11:19:56 to 09-12-2016-12:19:56

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
61.220.26.201	Taiwan	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	11
209.15.196.171	Canada	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	9
209.15.196.171	Canada	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	9
106.38.241.105	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	8
83.168.250.50	Sweden	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	7
83.168.250.50	Sweden	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
24.86.161.214	Canada	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
213.65.31.82	Sweden	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
83.168.250.50	Sweden	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	5
178.20.235.164	Russian Federation	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	5
178.20.235.164	Russian Federation	147.237.77.74	law.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	1

09-12-2016-11:19:56 to 09-12-2016-12:19:56

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
83.168.250.50	147.237.77.233	Sweden	atal.idf.il	SQL Injection - Select From	30
209.15.196.171	147.237.76.42	Canada	refuah.idf.il	SQL Injection - Select From	26
61.220.26.201	147.237.77.74	Taiwan	law.idf.il	SQL Injection - Select From	23
178.20.235.164	147.237.77.74	Russian Federation	law.idf.il	SQL Injection - Select From	22
24.86.161.214	147.237.77.233	Canada	atal.idf.il	SQL Injection - Select From	17
213.65.31.82	147.237.77.233	Sweden	atal.idf.il	SQL Injection - Select From	15
151.80.41.176	147.237.72.166	France	aka.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	3
46.120.122.219	147.237.76.200	Israel	eitan.aka.idf.il	Xenu Link Sleuth User Agent	2
79.181.206.187	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.138.66.137	147.237.77.216	France	dover.idf.il	portscan: TCP Distributed Portscan	1
201.73.83.242	147.237.0.15	Brazil	kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
199.203.215.1	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.75	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
190.153.238.58	147.237.76.34	Chile	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
31.168.133.168	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.44.131.203	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
103.207.37.81	147.237.77.74	Vietnam	law.idf.il	ET SCAN NMAP -sS window 1024	1
2.53.45.94	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.250.8.103	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.106.13.240	147.237.76.38	Albania	e.e.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
201.73.83.242	147.237.0.15	Brazil	kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
46.19.86.165	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.98	147.237.77.170	United States	maarachot.idf.il	ET DROP Dshield Block Listed Source	1
37.26.146.253	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
190.153.238.58	147.237.0.17	Chile	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
31.168.99.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.158.203.149	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
84.108.130.125	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-12-2016-11:19:56 to 09-12-2016-12:19:56

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
132.64.217.139	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
217.132.132.39	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
217.132.132.39	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
62.0.227.33	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
79.176.24.164	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
62.0.237.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
66.249.66.6	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.32.179.32	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
79.176.24.164	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.19.86.237	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.237	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.215	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
46.19.85.151	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	5
46.19.85.12	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
176.13.236.249	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
198.50.167.175	Canada	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
198.50.167.175	Canada	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
62.0.200.38	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.46	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.151	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.215	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
185.27.105.66	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.236.249	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
198.50.167.175	Canada	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
198.50.167.175	Canada	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
195.189.193.1	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
176.13.234.60	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
2.53.146.204	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
198.50.167.175	Canada	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
176.13.251.213	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.53	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
37.142.82.120	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
2.53.191.207	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
46.19.86.14	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
198.50.167.175	Canada	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
2.53.1.105	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
2.53.38.243	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
198.50.167.175	Canada	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
31.154.23.73	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
198.50.167.175	Canada	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
2.53.1.105	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	2
198.50.167.175	Canada	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
46.19.86.21	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.18	United States	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
198.50.167.175	Canada	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
37.46.41.109	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
109.226.40.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
2.53.29.208	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
128.232.110.28	United Kingdom	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
198.50.167.175	Canada	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1

09-12-2016-11:19:56 to 09-12-2016-12:19:56

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	98
2.53.191.207	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
176.13.21.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
80.246.136.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
109.253.223.96	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
2.53.45.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
31.154.81.75	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	4
79.178.168.236	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	3
185.32.179.21	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.0.117	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
199.203.226.21	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl50.x in www.aka.idf.il/main/sachar/payslips.aspx	None	1
109.67.131.149	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
52.30.171.229	Ireland	147.237.72.166	aka.idf.il	Unauthorized URL Access to /	Block	1
2.53.55.190	Israel	147.237.72.167	ishurim.aka.idf.i	Illegal Parameter Encoding __EVENTVALIDATION in www.ishurim.aka.idf.il/1052-he/ordermilitarycertificates.aspx	None	1
79.180.35.233	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	1
46.19.85.94	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	1
66.102.9.22	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
192.243.55.129	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=58625&docid=68481	Block	1
80.178.192.19	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.86.26	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	1
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/nakhal	Block	1
2.53.38.63	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
69.171.230.108	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/sip_storage/files/9/size220x0/2019.jpg	Block	1
192.243.55.135	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/tizmoret/printpreview/default.asp	Block	1
46.19.86.26	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method =0.8 in URL	Block	1
213.57.27.134	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/default.as.px	Block	1
77.127.71.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	1
37.26.148.172	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
192.243.55.135	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/1132-8613-he/navy.aspx.aspx	Block	1
81.131.221.61	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il./favicon.ico	Block	1
46.19.86.105	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl51 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
213.251.182.110	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/blog/wp-admin/	Block	1
2.53.45.94	Israel	147.237.0.19	madim.atal.idf.il	SSL Untraceable Connection - Open Mode	None	1
176.13.241.4	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1

09-12-2016-11:19:56 to 09-12-2016-12:19:56