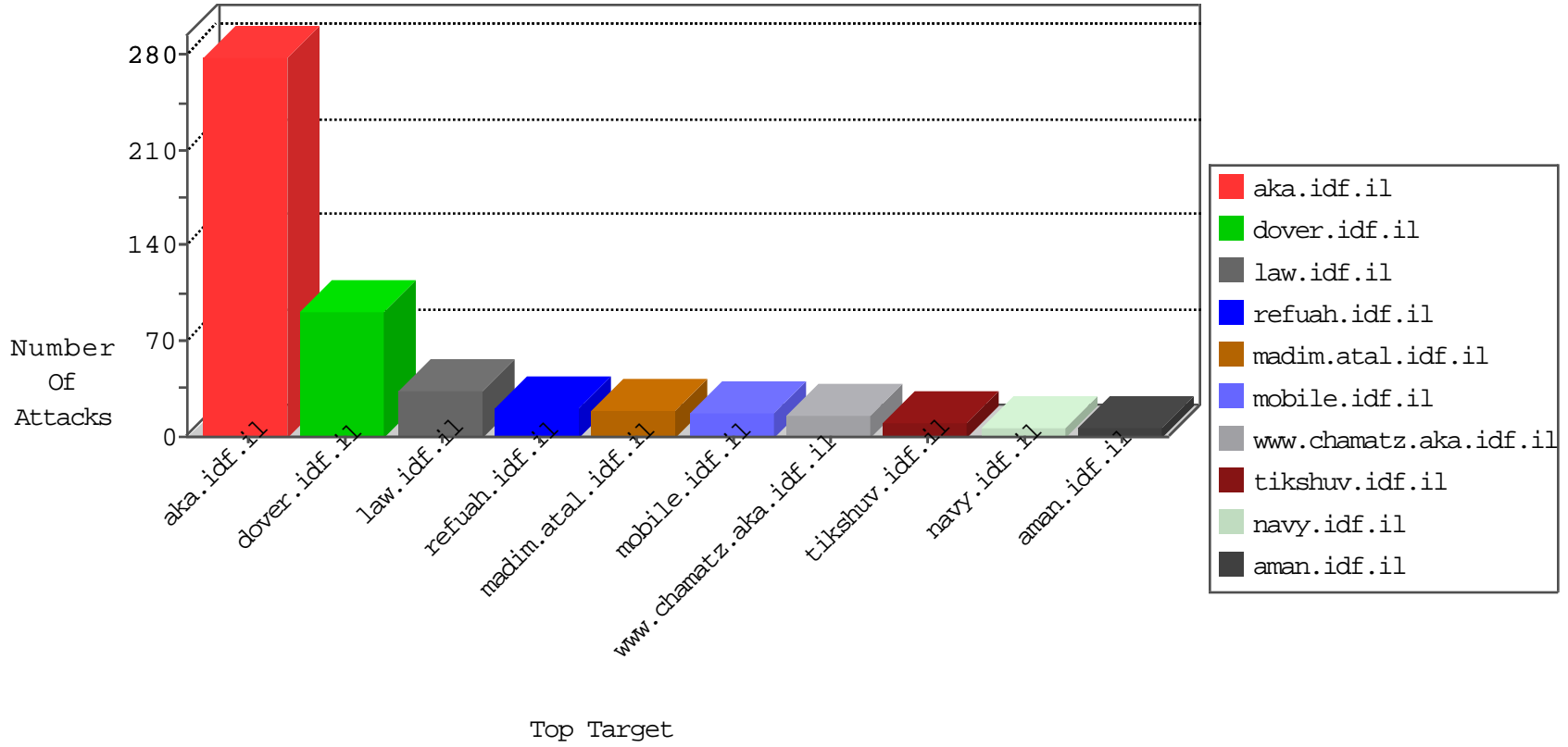


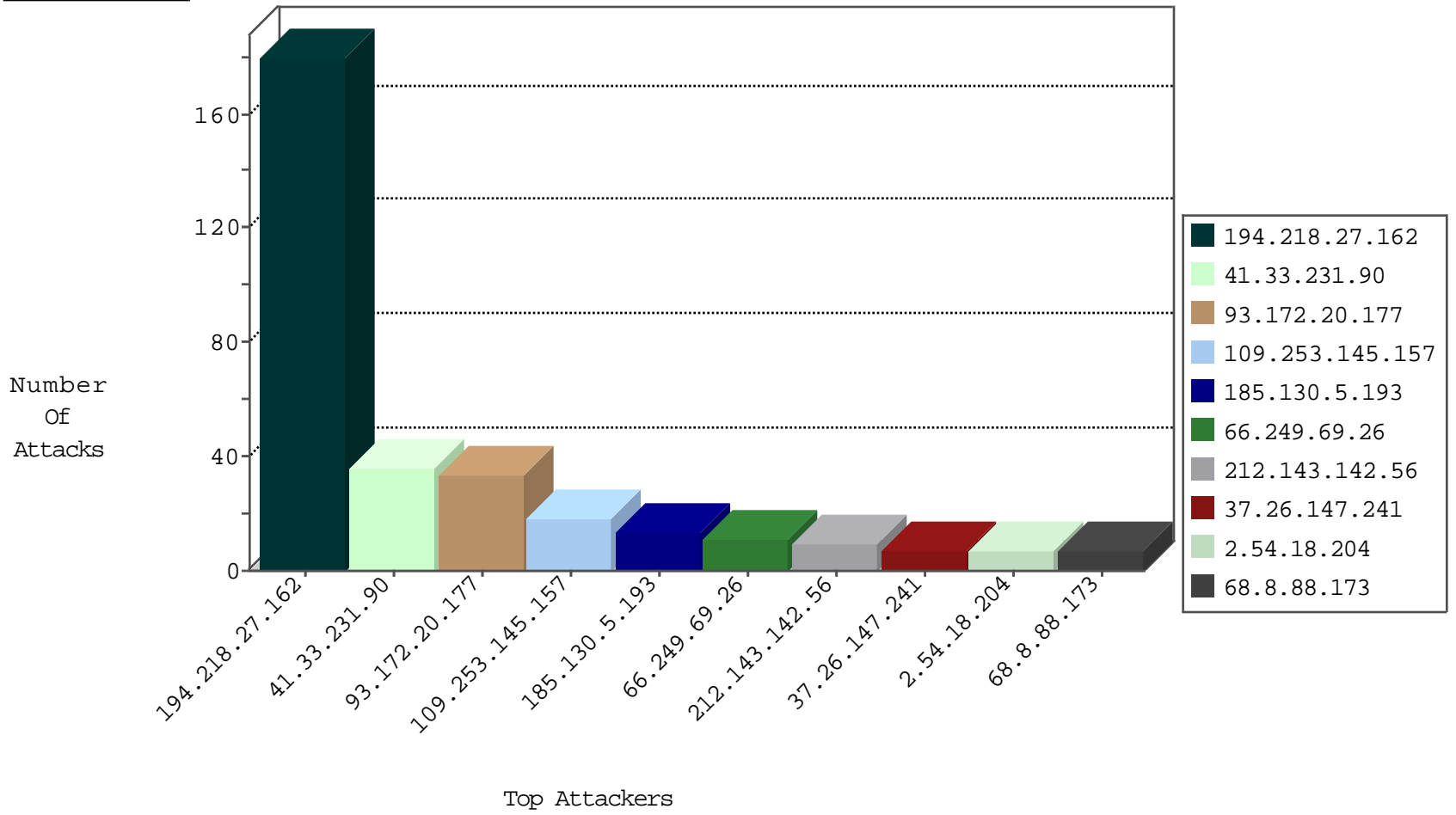
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
217.26.171.188	Moldova, Republic of	147.237.77.176	matpash.idf.il	I4 Source or Dest Port Zero	drop	4
79.181.110.220	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
159.220.78.113	India	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
184.105.139.84	United States	147.237.0.19	madim.atal.idf.il	Block_Ntp_All_Net	drop	1
159.220.78.114	India	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
184.105.139.104	United States	147.237.77.61	e.cogat.idf.il	Block_Ntp_All_Net	drop	1
89.248.172.207	Netherlands	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.80	United States	147.237.0.16	my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
217.26.171.188	Moldova, Republic of	147.237.76.176	test.ncore.idf.il	I4 Source or Dest Port Zero	drop	1
159.203.25.95	United States	147.237.0.35	akaws.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.80	United States	147.237.77.170	maarachot.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.212.127	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
108.59.8.70	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	4
162.210.196.100	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
51.255.65.64	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.96	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.97	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.26	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
104.232.98.38	147.237.0.34		tikshuv.idf.il	ET SCAN NMAP -f -sS	1
85.93.5.66	147.237.77.121	Germany	e.navy.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
212.227.89.173	147.237.76.42	Germany	refuah.idf.il	ET SCAN Potential SSH Scan	1
195.216.176.244	147.237.0.15	Latvia	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
121.99.220.125	147.237.72.166	New Zealand	aka.idf.il	ET SCAN NMAP -sS window 1024	1
104.232.98.38	147.237.0.34		tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
94.102.48.193	147.237.77.176	Netherlands	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.77.74	China	law.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
195.216.176.244	147.237.0.19	Latvia	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
104.232.98.38	147.237.0.34		tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	120
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	60
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
109.253.145.157	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
185.130.5.193		147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
68.8.88.173	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
37.26.147.241	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.18.204	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.66.93	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
5.102.242.89	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.90	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.184.177	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.171.103	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.32.39	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.210.136	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.46.144	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.198.103	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.146.170	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.5.11	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
188.120.148.17	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
66.249.78.230	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.162.6.255	France	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
109.67.24.3	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.205.13	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.146.217	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.22.235	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.15.9	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.137.8	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.25.233	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.214.135	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.201	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.38.182	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
70.199.214.176	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.21.89	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.141.161	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.31.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.171.90	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.110.211.249	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
172.98.86.188		147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
216.190.59.150	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2

03-01-2016-06:04:08 to 03-01-2016-07:04:08

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
77.126.66.168	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
106.38.241.106	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
106.38.241.106	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
212.29.246.78	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
216.218.206.118	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.228.63.238	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.48	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.91	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.172.20.177	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 93.172.20.177	Block	21
93.172.20.177	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	11
66.249.69.26	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	8
2.54.47.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.69.26	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
109.253.129.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.148.184	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.139.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.136.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
108.196.83.66	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.182.31.191	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/updatestatus.php	Block	1
40.77.167.24	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/jeninkilled/stn	Block	1
157.55.39.39	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
91.199.69.254	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
74.64.46.22	United States	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$ct163 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
37.26.146.138	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.67.24.3	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/matash	Block	1
188.165.15.132	France	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
74.82.47.4	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
37.26.147.241	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
80.246.137.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
207.46.13.80	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/scripts.aspx/getjs	Block	1
79.182.31.191	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
109.253.145.157	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.249.78.248	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/3251.pdf	Block	1
2.54.18.204	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/authentication/index	Block	1
93.172.20.177	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/ajax/updatestatus.php	Block	1
79.182.31.191	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.182.31.191	Block	1
40.77.167.5	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
84.228.232.101	Israel	147.237.72.166	aka.idf.il	Double URL Encoding - parameter: search in www.aka.idf.il/main/gyus/pniohandler1.aspx/search	Block	1