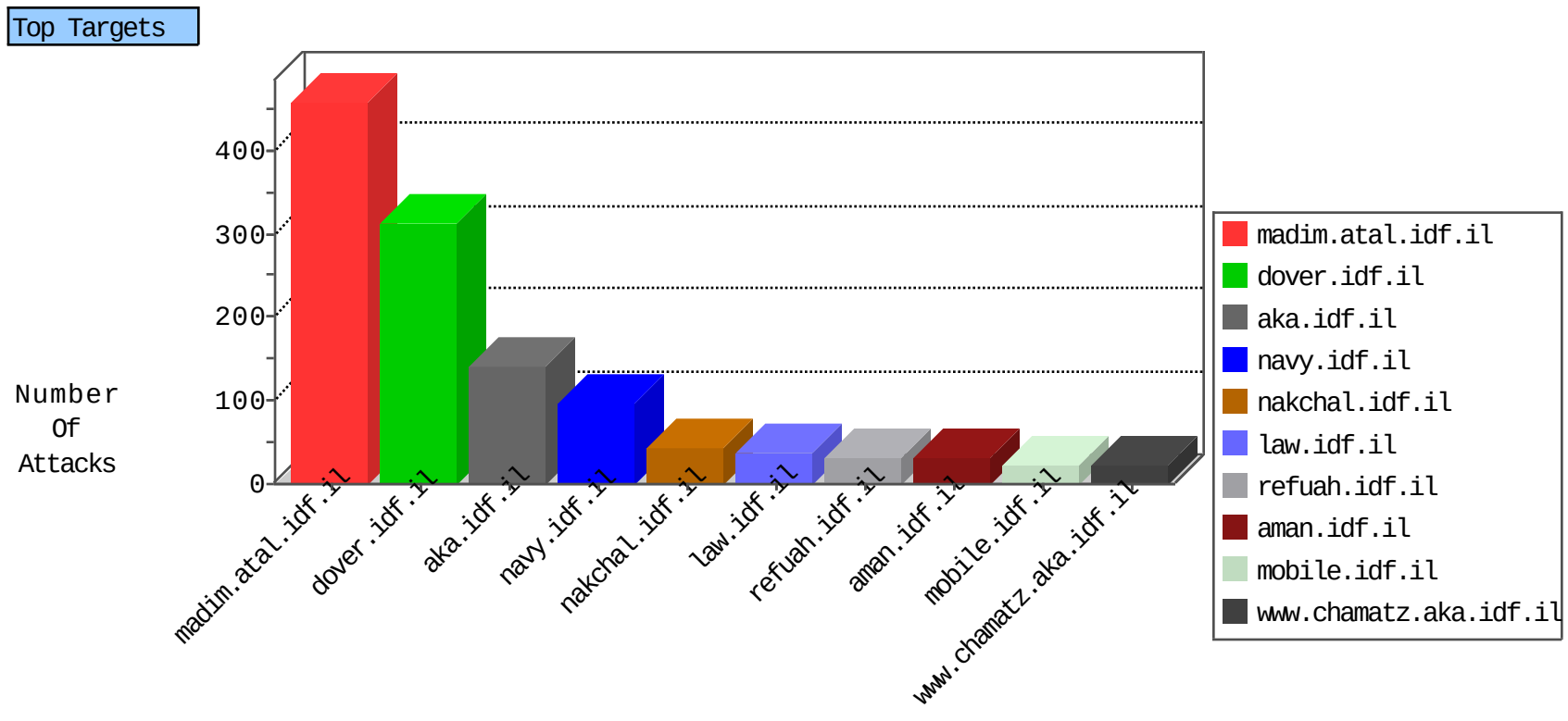
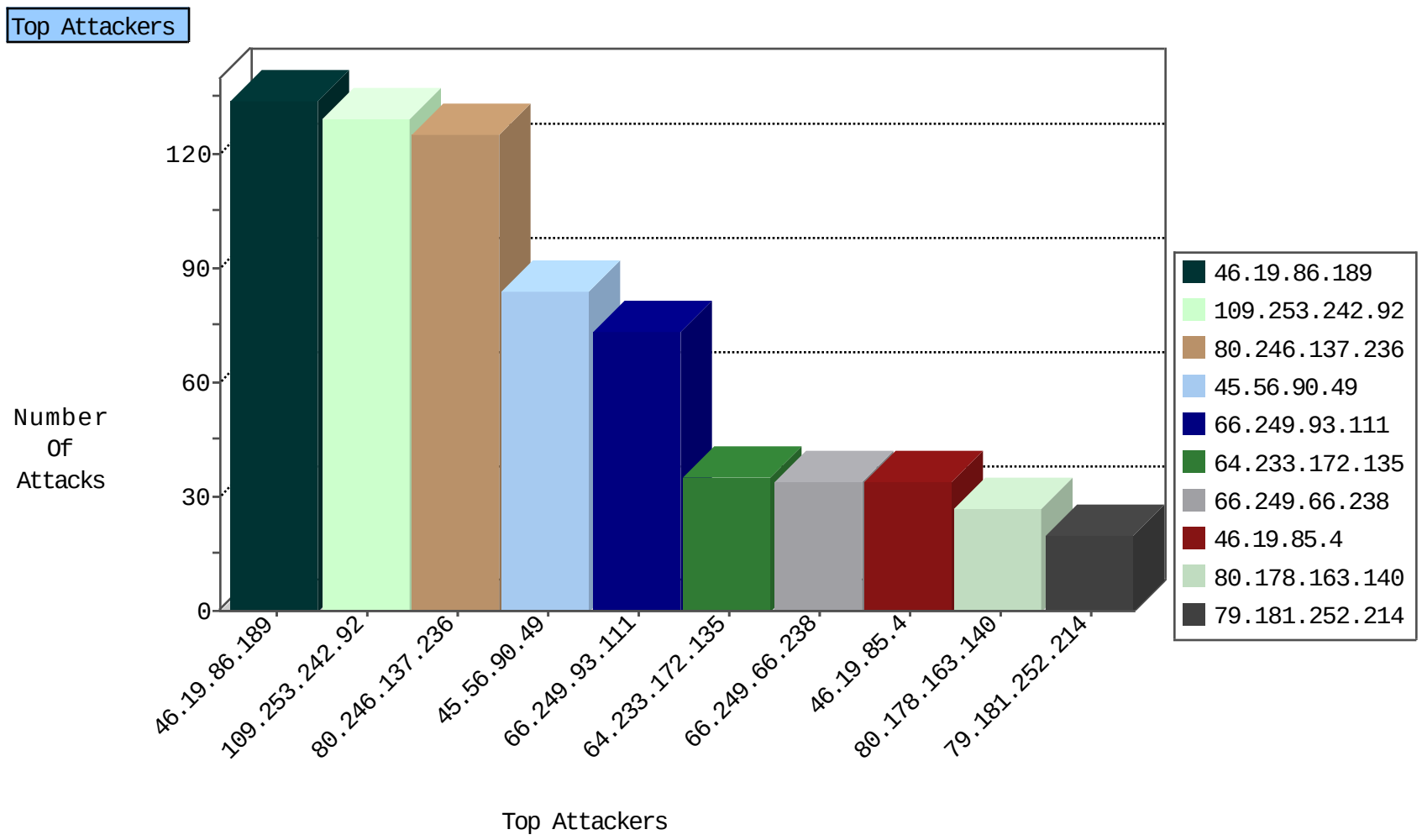
09-04-2016-15:04:08 to 09-04-2016-16:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-04-2016-15:04:08 to 09-04-2016-16:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.139.156.151	France	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
134.147.203.115	Germany	147.237.76.201	e.atal.idf.il	Black List	drop	2
31.168.133.226	Israel	147.237.77.216	dover.idf.il	Black List	drop	1
199.203.37.52	Israel	147.237.76.42	refuah.idf.il	Black List	drop	1
82.81.37.46	Israel	147.237.77.216	dover.idf.il	Black List	drop	1
123.56.204.28	China	147.237.76.44	e.refuah.idf.i	Black List	drop	1

09-04-2016-15:04:08 to 09-04-2016-16:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
199.58.86.206	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

09-04-2016-15:04:08 to 09-04-2016-16:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
64.233.172.135	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	35
66.249.66.238	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	34
84.93.84.77	147.237.77.176	United Kingdom	matpash.idf.il	Tehila - Perl LWP with fake user agent	2
195.54.210.203	147.237.72.166	Russian Federation	aka.idf.il	ET SCAN NMAP -sA (2)	2
163.172.238.38	147.237.8.46	United Kingdom	e.chinuch.idf.i	ET SCAN NMAP -sS window 1024	1
124.83.33.119	147.237.76.196	Philippines	e.sviva.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.19.86.113	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.211.114	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.168.197.233	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.195	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
31.154.81.29	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
221.226.31.210	147.237.8.24	China	e.lifestyle.idf	ET SCAN NMAP -sS window 2048	1
87.71.52.18	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
221.6.32.82	147.237.8.24	China	e.lifestyle.idf	ET SCAN NMAP -sS window 2048	1
5.29.150.244	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.132.18.62	147.237.8.46	Azerbaijan	e.chinuch.idf.i	ET SCAN NMAP -sS window 1024	1
217.132.53.222	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.153.157	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.32.23	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
198.52.97.91	147.237.77.74	United States	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
79.178.52.182	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.87.160.1	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
146.185.56.162	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
50.116.123.135	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
115.72.188.60	147.237.76.38	Vietnam	e.e.meitav.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
45.79.103.178	147.237.72.156	United States	aman.idf.il	WEB-MISC Chunked-Encoding transfer attempt	1
109.64.38.110	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.168.104.85	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
91.121.78.198	147.237.77.74	France	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
5.102.253.136	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
221.226.31.210	147.237.8.24	China	e.lifestyle.idf	ET SCAN NMAP -f -sS	1
85.132.18.62	147.237.8.46	Azerbaijan	e.chinuch.idf.i	ET SCAN NMAP -sS window 4096	1
221.6.32.82	147.237.8.24	China	e.lifestyle.idf	ET SCAN NMAP -f -sS	1
5.28.153.215	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
208.100.26.228	147.237.76.198	United States	e.yohalan.idf.i	ET SCAN NMAP -sS window 1024	1
2.53.40.241	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.179.205.36	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.139.25.164	147.237.77.216	France	dover.idf.il	portscan: TCP Distributed Portscan	1

09-04-2016-15:04:08 to 09-04-2016-16:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
66.249.93.111	Europe	147.237.77.216	dover.idf.il	drop	SAM rule	drop	40
45.56.90.49	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
82.176.200.133	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
45.56.90.49	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	18
45.56.90.49	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
45.56.90.49	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	17
66.249.93.111	Europe	147.237.77.216	dover.idf.il	drop		drop	15
45.56.90.49	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	12
46.19.86.3	Israel	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	12
46.117.215.217	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
79.181.252.214	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
80.178.163.140	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
79.181.252.214	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
66.249.93.111	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
89.139.151.92	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
66.249.93.111	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	8
85.65.176.193	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.235.98.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.89	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
89.139.180.182	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.243	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.86.12	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.178.198.242	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.52.172	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.107	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
66.249.76.106	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.12	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
195.60.232.57	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
80.178.163.140	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	5
46.19.85.153	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.253.199.73	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
37.26.147.146	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.117.215.217	Israel	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.139	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.205	Israel	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	4
176.13.241.114	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.65	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
80.178.163.140	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.19.85.154	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.85.139	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
80.178.163.140	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
80.246.136.216	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
212.117.150.179	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
80.178.163.140	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.85.185	Israel	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	2
109.253.158.39	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
176.13.22.120	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
176.13.232.237	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.85.65	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2

09-04-2016-15:04:08 to 09-04-2016-16:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	134
109.253.242.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	127
80.246.137.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	125
46.19.85.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	34
176.13.241.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
192.116.233.90	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on www.nakhal.idf.il/sip_storage/files/2/	Block	10
192.116.233.90	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	10
84.94.235.121	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.94.235.121	Block	7
199.203.173.198	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	5
176.13.228.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
157.55.39.36	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
176.13.235.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
109.253.216.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.178.184.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
194.177.16.3	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	3
80.246.130.221	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
88.202.218.246	United Kingdom	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	2
159.122.159.28	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 159.122.159.28	Block	2
2.53.13.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
94.230.86.41	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
5.29.120.2	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
2.53.51.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
185.46.137.18	Germany	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	2
2.53.52.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/watch	Block	1
2.53.13.8	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 2.53.13.8	Block	1
84.94.235.121	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
46.19.86.5	Israel	147.237.76.42	refuah.idf.il	Distributed Unknown HTTP Request Method	Block	1
192.243.55.132	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/chinuch/contact	Block	1
31.168.49.178	Israel	147.237.72.166	aka.idf.il	Unknown Parameter doc in www.aka.idf.il/main/giyus/general.aspx	None	1
2.55.17.250	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.141	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/m/	Block	1
45.79.111.169	United States	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 45.79.111.169	Block	1
77.125.13.104	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
31.168.49.178	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ca in www.aka.idf.il/main/giyus/general.aspx	None	1
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Unknown Parameter newsItem in www.aka.idf.il/megurim/news/	None	1
84.94.235.121	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/index.php	Block	1
46.19.86.111	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/resources/images/favicon/favicon.png	Block	1
192.243.55.134	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/chinuch/gallery	Block	1
79.180.211.240	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
31.168.49.178	Israel	147.237.72.166	aka.idf.il	Unknown Parameter doci in www.aka.idf.il/main/giyus/general.aspx	None	1
185.3.147.254	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
2.55.189.125	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
157.55.39.36	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/mpqlw-8vpxs	Block	1
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.76.47	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/iturim/asp/list.asp	Block	1
199.203.173.198	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on www.nakhal.idf.il/sip_storage/files/2/	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=59334&docid=68033	Block	1
82.166.76.90	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 82.166.76.90	Block	1

09-04-2016-15:04:08 to 09-04-2016-16:04:08