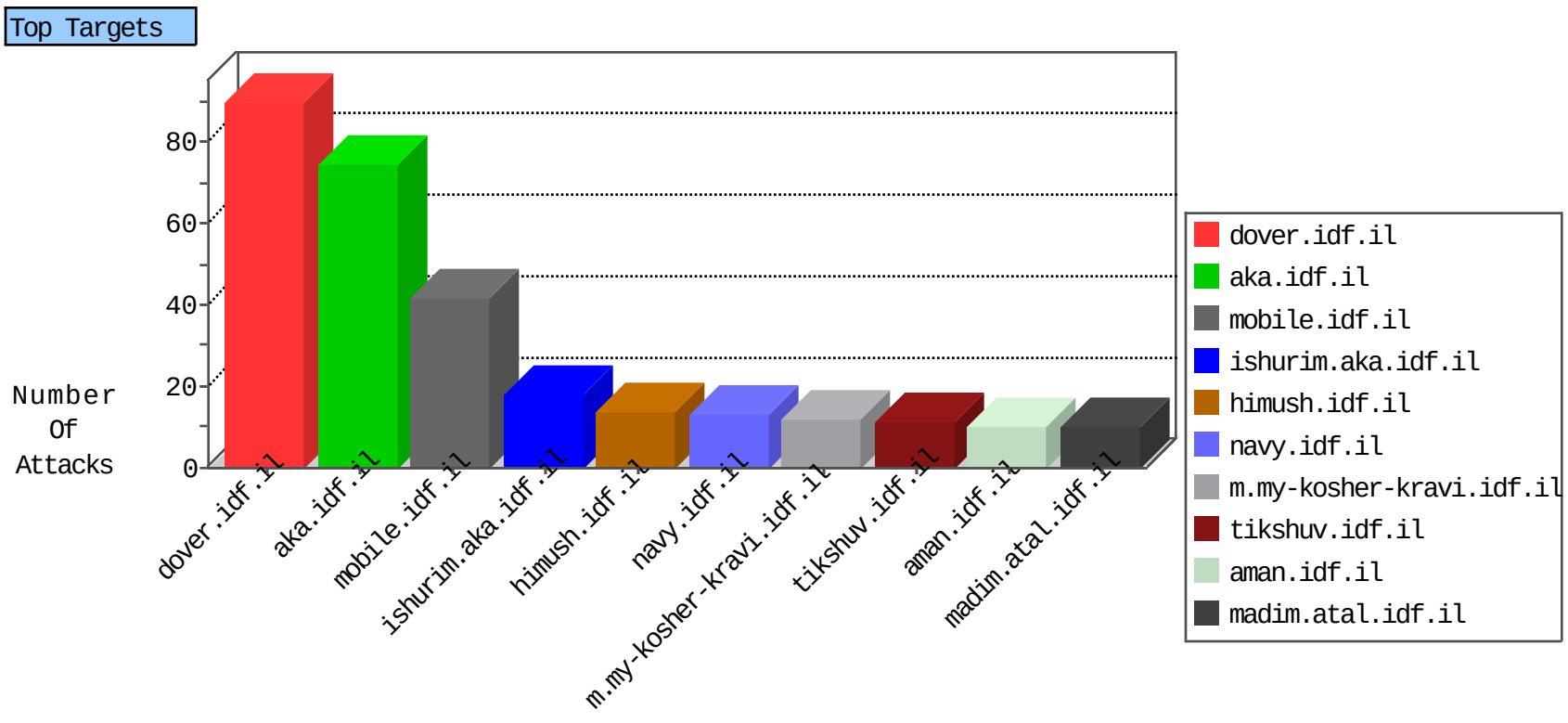
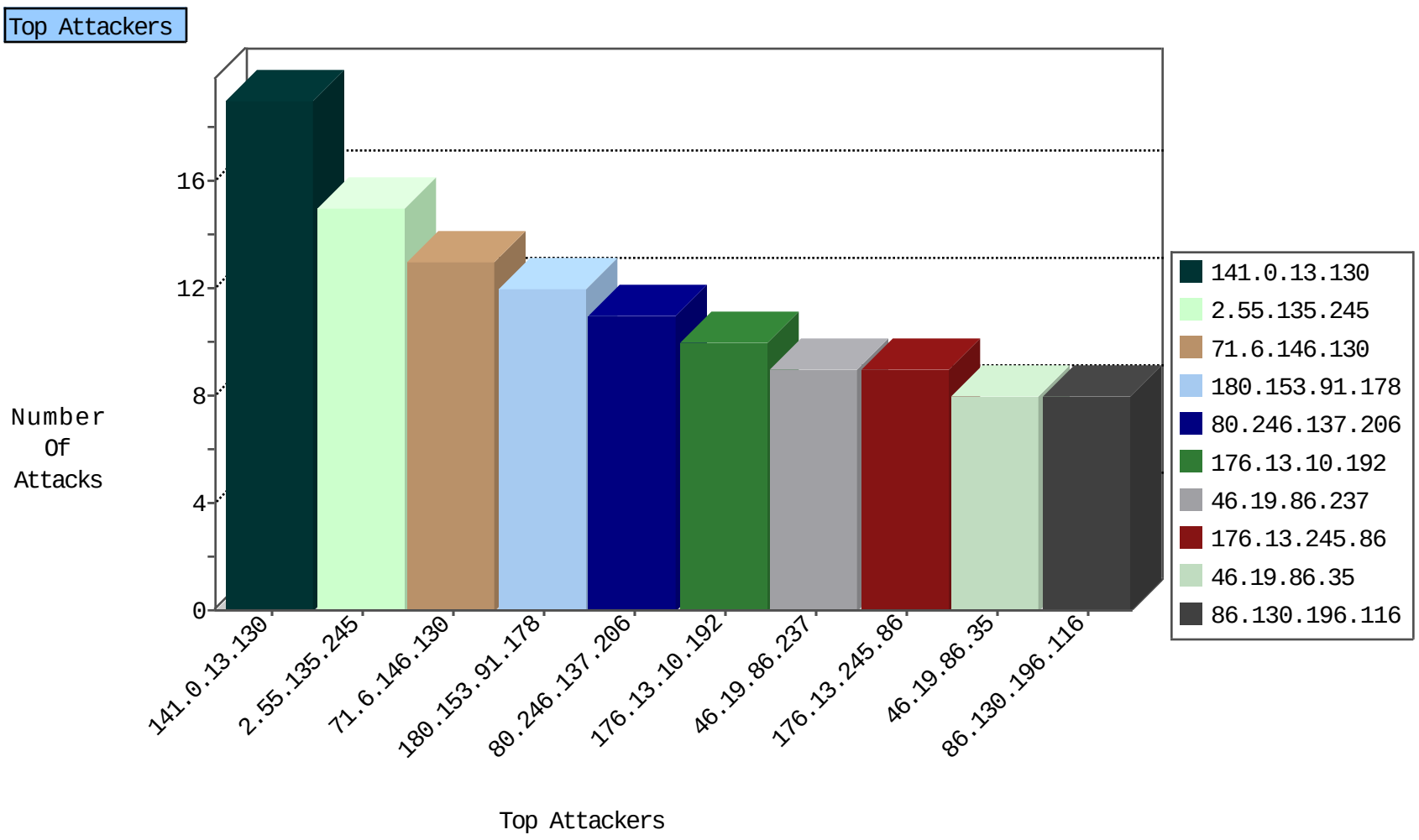
09-30-2016-00:04:05 to 09-30-2016-01:04:05

IDF Under Attack Daily Report





09-30-2016-00:04:05 to 09-30-2016-01:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
71.6.146.130	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	213
180.153.91.178	China	147.237.76.30	himush.idf.il	Black List	drop	12
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
42.112.10.70	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1
42.112.10.81	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1
42.112.10.73	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1
42.112.10.85	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1
42.112.10.66	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1
42.112.10.74	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1
42.112.10.69	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1
42.112.10.75	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1

09-30-2016-00:04:05 to 09-30-2016-01:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.183.223.232	Latvia	147.237.77.216	dover.idf.i	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	1

09-30-2016-00:04:05 to 09-30-2016-01:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
5.255.90.133	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
194.106.166.123	147.237.8.46		e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
163.172.129.15	147.237.76.147	United Kingdom	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
144.0.1.12	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
144.0.1.12	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
78.129.171.173	147.237.8.50	United Kingdom	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
46.172.91.20	147.237.8.28	Ukraine	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
5.255.90.133	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
194.106.166.123	147.237.8.50		e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
165.215.209.15	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	1
144.0.1.12	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
144.0.1.12	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.194	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.200.137	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
42.114.119.161	147.237.76.147	Vietnam	chinuch.aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

09-30-2016-00:04:05 to 09-30-2016-01:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
141.0.13.130	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	19
176.13.10.192	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	10
46.19.86.237	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
80.246.137.206	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
86.130.196.116	United Kingdom	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.85.251	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
79.179.30.42	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.245.86	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.248.125	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.216.70	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
2.55.135.245	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
2.55.135.245	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
2.55.135.245	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.75	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
66.249.66.129	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.8.204.62	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
176.13.14.11	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
206.173.106.22	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
157.55.39.71	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
5.22.134.194	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
84.108.144.22	Israel	147.237.77.121	e.navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
37.75.215.141	Palestinian Territory, Occupied	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	2
79.180.165.221	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
77.125.23.10	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.86.35	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
85.65.49.103	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
37.26.147.210	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	2
79.178.220.9	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
109.253.208.117	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.127	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
66.249.64.183	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
176.13.20.174	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
212.199.218.246	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.212.30	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
31.210.188.21	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.92	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
176.13.250.219	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.19.86.215	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
176.13.18.235	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid sequence number	monitor	1
46.19.86.35	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
169.229.3.91	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
195.62.53.168	Russian Federation	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
37.26.149.130	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.95	United States	147.237.77.61	e.cogat.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
183.129.160.229	China	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.86	United States	147.237.0.35	akaws.idf.il	drop		drop	1
176.13.245.86	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
46.19.86.35	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1

09-30-2016-00:04:05 to 09-30-2016-01:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
80.179.184.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
31.168.75.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.245.86	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
79.180.165.221	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
80.246.137.206	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
169.229.3.91	United States	147.237.76.86	navy.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
79.179.28.24	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.69.228	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
192.243.55.135	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=59331&docid=64441	Block	1
2.53.129.0	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.111.39.248	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
68.180.231.60	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1934-he/cogat.aspx	Block	1
46.183.223.232	Latvia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/phppath/php	Block	1
79.179.30.42	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.76.54	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	1
192.243.55.138	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/general.aspx	Block	1
2.53.191.249	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
85.64.8.125	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
77.138.200.171	France	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.102.9.3	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
176.13.248.125	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.76.108	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/iturim/asp/search.asp	None	1
206.173.106.22	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.60.32.94	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/atudalane.aspx	Block	1
85.64.107.198	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
79.178.143.14	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.185	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
180.76.15.161	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9724-he/refuah.aspx	Block	1
66.249.79.172	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1409-he/atal.aspx	Block	1
212.199.57.206	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
85.65.49.103	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.178.252.210	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
66.249.66.103	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
192.243.55.130	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=59391&docid=68135	Block	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1397-en/dover.aspx	Block	1

09-30-2016-00:04:05 to 09-30-2016-01:04:05