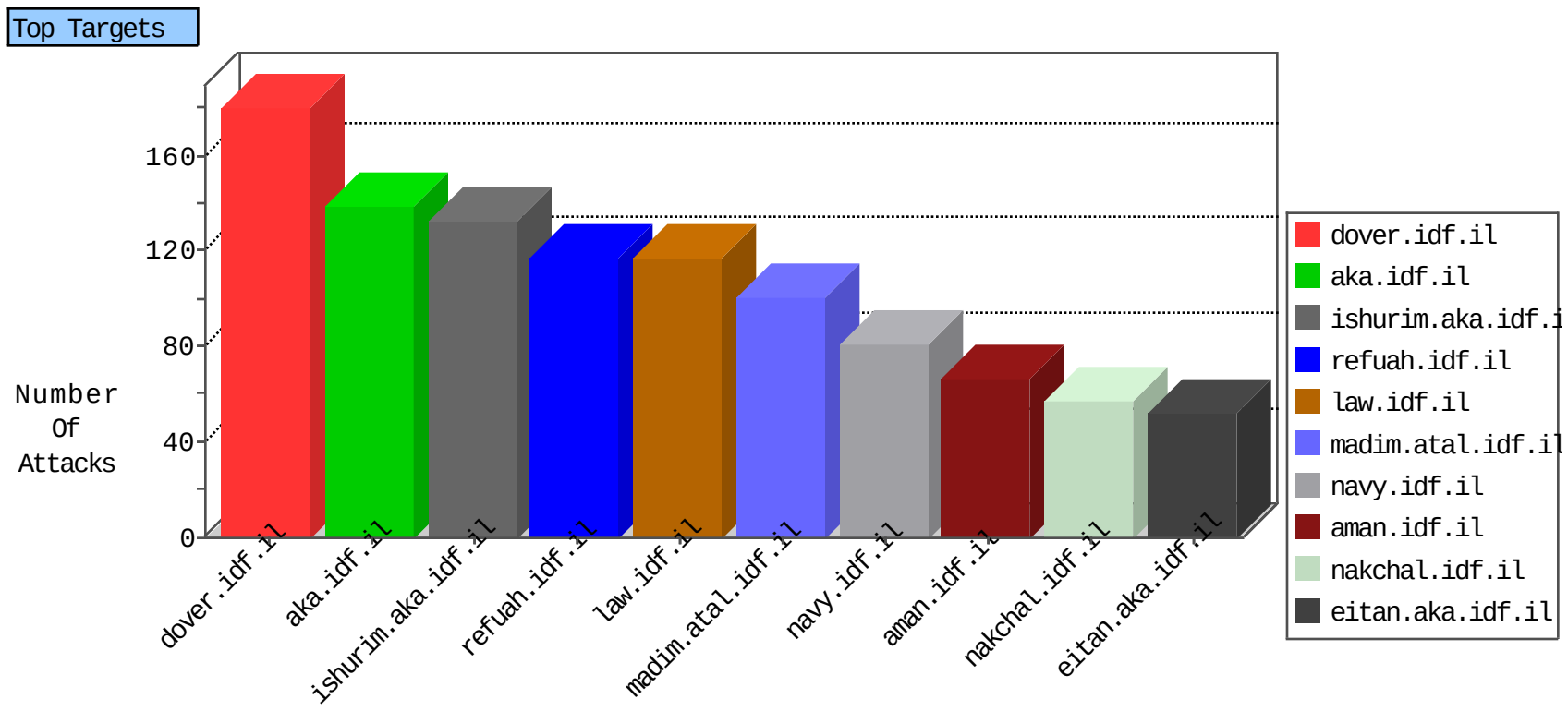
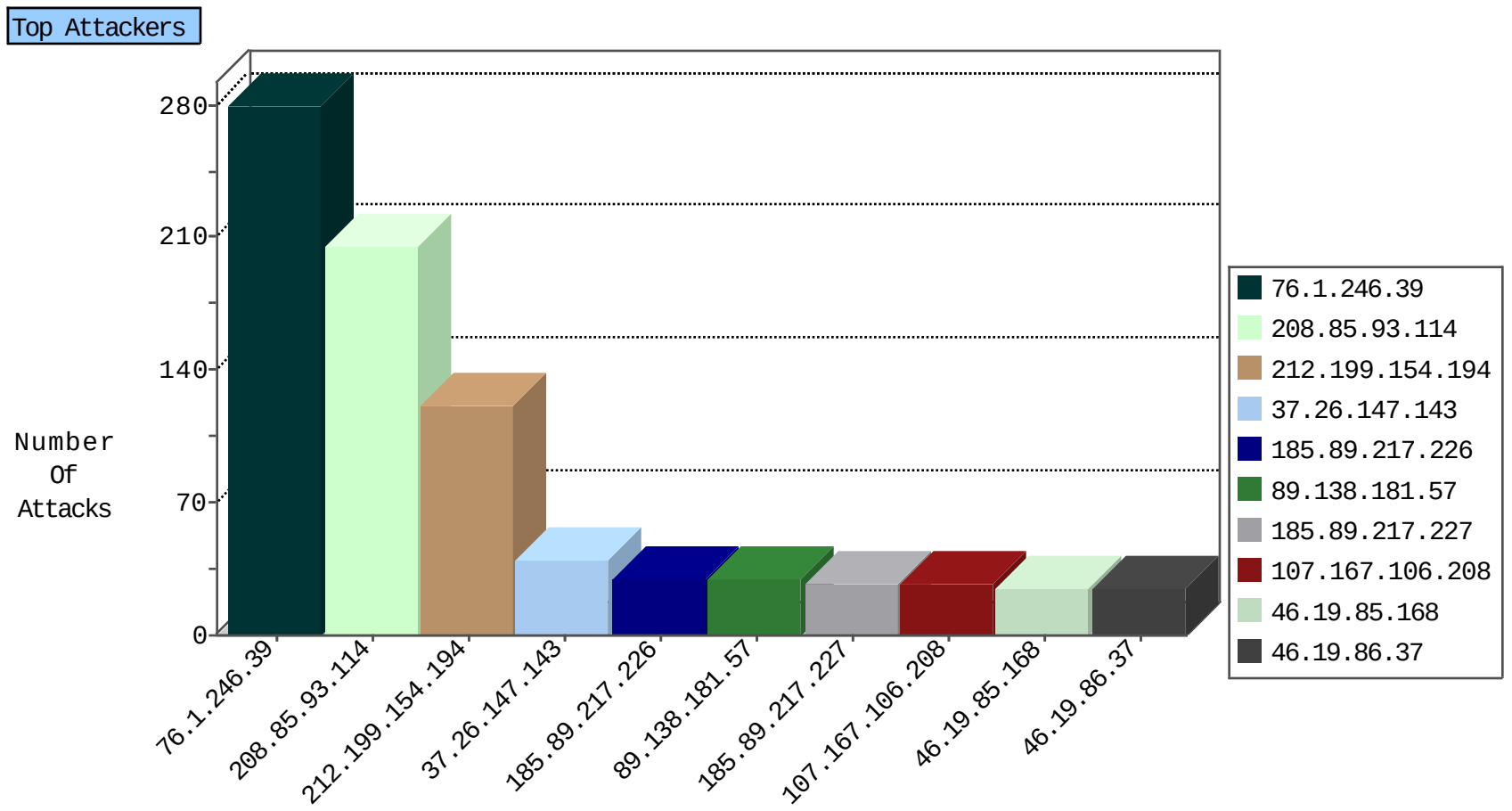
09-06-2016-09:04:03 to 09-06-2016-10:04:03

IDF Under Attack
Daily Report

Top Targets



Top Attackers



09-06-2016-09:04:03 to 09-06-2016-10:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.199.154.194	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	731
185.89.217.229	Netherlands	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	9
2.53.151.138	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
212.179.64.162	Israel	147.237.77.170	maarachot.idf.il	Black List	drop	2
71.6.146.185	United States	147.237.76.31	nakchal.idf.il	Black List	drop	1

09-06-2016-09:04:03 to 09-06-2016-10:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.101.157.16	Russian Federation	147.237.77.176	matpash.idf.il	3630: HTTP: SQL Injection (Boolean Identity)	Block	1
103.199.2.2	Indonesia	147.237.77.176	matpash.idf.il	3630: HTTP: SQL Injection (Boolean Identity)	Block	1

09-06-2016-09:04:03 to 09-06-2016-10:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
62.219.120.45	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
45.79.71.122	147.237.0.34	United States	tikshuv.idf.il	WEB-MISC Chunked-Encoding transfer attempt	1
213.8.38.12	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.154.38.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.130.6.49	147.237.77.121	Lithuania	e.navy.idf.il	ET SCAN Potential SSH Scan	1
2.53.147.155	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.11.135	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.155	147.237.77.234	Ukraine	halag.idf.il	ET SCAN NMAP -sS window 3072	1
80.246.138.134	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.181.166.122	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
64.137.171.55	147.237.77.74	Canada	law.idf.il	ET SCAN Potential SSH Scan	1
62.219.54.250	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.194.193.52	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
41.33.231.86	147.237.77.216	Egypt	dover.idf.il	portscan: TCP Distributed Portscan	1
195.146.61.3	147.237.77.216	Iran, Islamic Republic of	dover.idf.il	portscan: TCP Distributed Portscan	1
5.102.195.103	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.130.6.49	147.237.8.27	Lithuania	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
109.123.101.31	147.237.77.235	United Kingdom	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.8.14	Ukraine	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
79.182.149.153	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.76.75	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1

09-06-2016-09:04:03 to 09-06-2016-10:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.199.154.194	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	54
107.167.106.208	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	27
208.85.93.114	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	26
208.85.93.114	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	26
76.1.246.39	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	26
76.1.246.39	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	26
208.85.93.114	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	26
208.85.93.114	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	26
208.85.93.114	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	26
208.85.93.114	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	26
208.85.93.114	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	26
76.1.246.39	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	25
76.1.246.39	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	25
76.1.246.39	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	25
76.1.246.39	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	25
62.0.227.57	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	24
76.1.246.39	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	24
208.85.93.114	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	24
76.1.246.39	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	23
185.89.217.226	Netherlands	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	22
185.89.217.227	Netherlands	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	18
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
185.89.217.229	Netherlands	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	11
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.19.86.37	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	11
46.19.85.148	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
37.26.148.145	Israel	147.237.77.176	matpash.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.37	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
176.13.11.135	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.193	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.53.173.133	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
76.1.246.39	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.85.168	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.219	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
76.1.246.39	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.85.168	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.129	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
76.1.246.39	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.86.106	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
76.1.246.39	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
176.13.224.7	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.168	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
76.1.246.39	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
76.1.246.39	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.86.106	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
76.1.246.39	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
76.1.246.39	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
185.89.217.234	Netherlands	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.168	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
76.1.246.39	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6

09-06-2016-09:04:03 to 09-06-2016-10:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.147.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
89.138.181.57	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	29
176.13.241.73	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
176.13.4.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
93.172.217.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
2.53.162.128	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	7
2.53.175.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
82.81.78.91	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	4
46.18.17.212	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
194.114.146.227	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 194.114.146.227	Block	3
192.115.64.250	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 192.115.64.250	Block	3
46.19.86.196	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	3
37.26.149.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.224.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.57.70.4	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
185.3.147.64	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
45.79.71.122	United States	147.237.0.34	tikshuv.idf.il	Multiple Malformed HTTP Header Line from 45.79.71.122	Block	2
109.253.147.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
82.80.86.46	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 82.80.86.46	Block	2
192.198.151.43	Europe	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/contactus.aspx	Block	2
46.19.85.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
45.79.71.122	United States	147.237.0.34	tikshuv.idf.il	Multiple Malformed URL from 45.79.71.122	Block	2
45.79.71.122	United States	147.237.0.34	tikshuv.idf.il	Multiple Unknown HTTP Request Method from 45.79.71.122	Block	2
192.198.151.43	Europe	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 192.198.151.43	Block	2
66.249.93.202	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
62.90.35.105	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/894-he/nakhal.aspx	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
176.13.224.7	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
84.95.208.20	Israel	147.237.72.156	aman.idf.il	PHP Attempt	Block	1
5.101.157.16	Russian Federation	147.237.77.176	matpash.idf.il	Parameter Type Violation SortDir in www.cogat.idf.il/1043-en/cogat.aspx	Block	1
66.249.93.205	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
185.89.217.225	Netherlands	147.237.77.74	law.idf.il	URL is Above Root Directory www.law.idf.il/../images/1.he/navigation/navigation_arrow.gif	Block	1
62.219.136.238	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/6/110516.pdf	Block	1
128.68.53.124	Russian Federation	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
2.53.56.230	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 2.53.56.230 (Open Mode)	None	1
82.80.190.84	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/1044-he/ishurim.aspx	Block	1
66.249.79.139	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/3269.jpg	Block	1
46.19.86.28	Israel	147.237.0.19	madim.atal.idf.il	SSL Untraceable Connection - Open Mode	None	1
84.108.36.196	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
5.101.157.16	Russian Federation	147.237.77.176	matpash.idf.il	Parameter Type Violation lang in www.cogat.idf.il/1043-en/cogat.aspx	Block	1
68.180.230.47	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx	Block	1
66.249.69.14	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/6/1066.pdf	Block	1
147.234.241.1	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
66.249.79.143	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/3424.jpg	Block	1
207.232.35.50	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.59.71.224	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
77.139.90.75	France	147.237.72.166	aka.idf.il	Unknown Parameter __EVENTARGUMENT in www.aka.idf.il/main/giyus/	None	1
192.115.64.250	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
66.249.69.208	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/3/69903.pdf	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to www.kosher-kravi.idf.il/default.aspx	Block	1

09-06-2016-09:04:03 to 09-06-2016-10:04:03