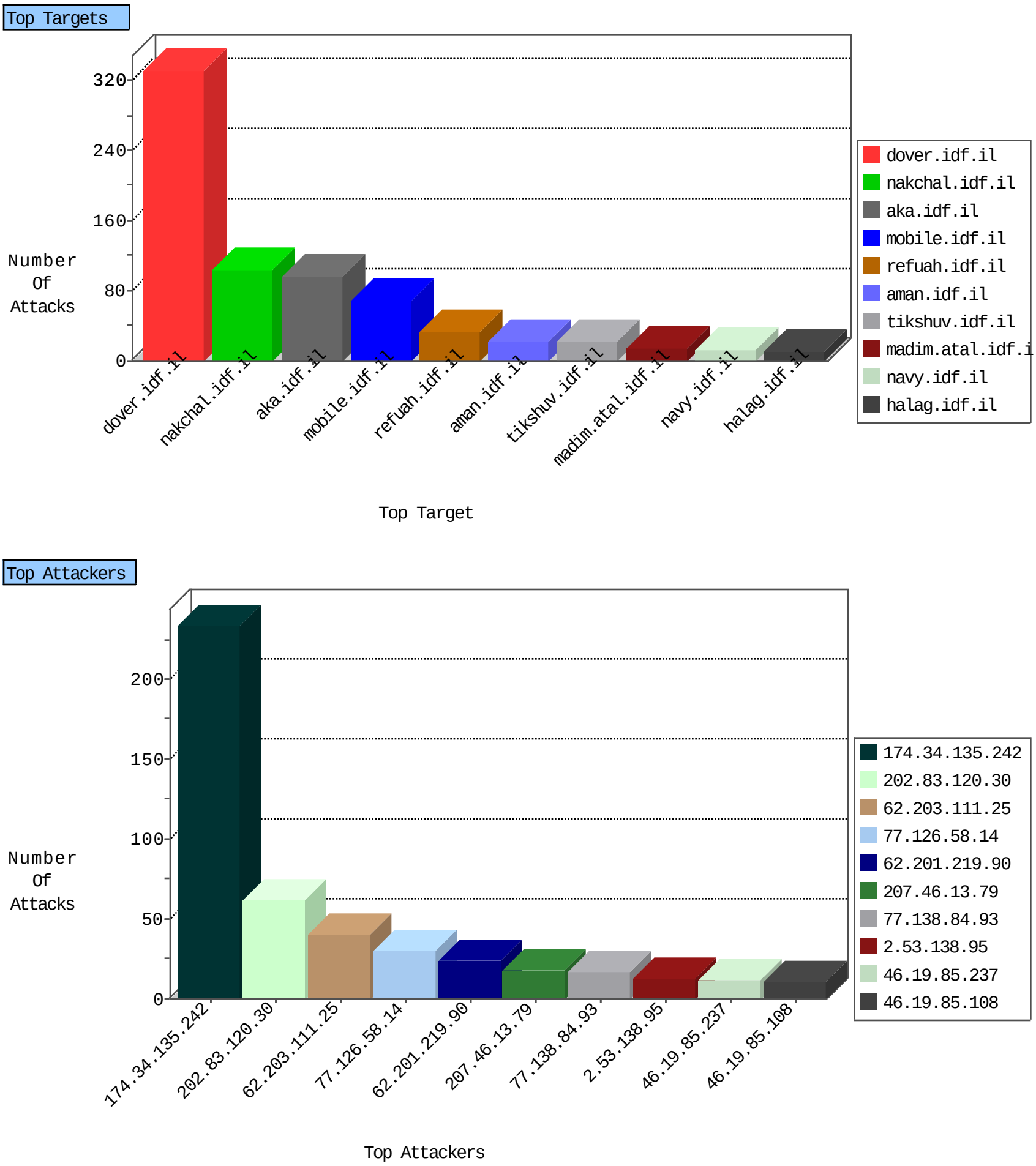
09-28-2016-23:04:07 to 09-29-2016-00:04:07

IDF Under Attack
Daily Report



09-28-2016-23:04:07 to 09-29-2016-00:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.22.134.165	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	10
198.44.110.25	United States	147.237.76.30	himush.idf.il	Black List	drop	1

09-28-2016-23:04:07 to 09-29-2016-00:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
174.34.135.242	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	223
174.34.135.242	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	7
174.34.135.242	United States	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	4
69.30.213.202	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2

09-28-2016-23:04:07 to 09-29-2016-00:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
123.31.35.23	147.237.77.179	Vietnam	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
119.147.84.8	147.237.77.227	China	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
84.109.36.223	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
61.147.247.161	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
61.147.247.161	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
58.220.2.5	147.237.77.234	China	halag.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.129.15	147.237.77.234	United Kingdom	halag.idf.il	ET SCAN NMAP -sS window 1024	1
46.97.58.78	147.237.76.199	Romania	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
123.31.35.23	147.237.77.233	Vietnam	atal.idf.il	ET SCAN NMAP -sS window 1024	1
123.31.35.23	147.237.77.179	Vietnam	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
123.31.35.23	147.237.77.178	Vietnam	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
93.172.213.165	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
61.147.247.161	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
61.147.247.161	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
61.147.247.161	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
46.161.40.17	147.237.0.34	Russian Federation	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
125.77.28.26	147.237.76.197	China	e.himush.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
42.247.4.164	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
123.31.35.23	147.237.77.226	Vietnam	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1

09-28-2016-23:04:07 to 09-29-2016-00:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
77.126.58.14	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
62.201.219.90	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
207.46.13.79	United States	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	18
77.138.84.93	France	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
202.83.120.30	Indonesia	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	16
202.83.120.30	Indonesia	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
202.83.120.30	Indonesia	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	14
202.83.120.30	Indonesia	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
62.203.111.25	Switzerland	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	10
62.203.111.25	Switzerland	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
109.253.144.180	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
62.203.111.25	Switzerland	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	9
62.203.111.25	Switzerland	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	7
2.53.138.95	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.117.40.37	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
207.232.5.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.120.29.26	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.237	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.237	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
202.83.120.30	Indonesia	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
2.53.2.107	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.86.134	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
62.203.111.25	Switzerland	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.53.8.14	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
79.177.111.167	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.186	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.163	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
77.125.5.251	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
5.28.164.36	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
2.53.183.254	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
89.237.115.245	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
79.180.95.242	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.221.97	Israel	147.237.72.166	aka.idf.il	SYN Attack		monitor	3
109.64.114.95	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.170	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.74	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
176.13.237.116	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
79.182.139.15	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
5.102.195.90	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.108	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
31.223.181.102	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
31.223.181.102	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2
79.176.101.85	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
2.55.189.83	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
71.198.173.115	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
185.27.106.243	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2
84.109.192.191	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
37.26.148.193	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		alert	2
188.120.148.54	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

09-28-2016-23:04:07 to 09-29-2016-00:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.166.240.201	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
2.53.138.95	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
140.147.146.194	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/	Block	3
176.13.246.65	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
77.139.102.129	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.139.102.129	Block	2
2.53.138.95	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 2.53.138.95	Block	2
2.53.138.95	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1541	Block	2
46.120.29.26	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
108.231.240.75	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 108.231.240.75	Block	2
46.19.85.108	Israel	147.237.76.86	navy.idf.il	Distributed Malformed URL	Block	2
5.29.21.43	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
209.94.232.130	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	2
46.19.85.108	Israel	147.237.76.86	navy.idf.il	Distributed Unknown HTTP Request Method	Block	2
66.249.66.23	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
180.97.106.161	China	147.237.0.19	madim.atal.idf.i	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
46.19.85.63	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
140.147.146.194	United States	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/	Block	1
66.249.75.8	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9757-he/refuah.aspx	Block	1
180.97.106.37	China	147.237.0.34	tikshuv.idf.il	Multiple Untraceable SSL Sessions from 180.97.106.37 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
46.19.86.206	Israel	147.237.77.243	mobile.idf.il	SSL Untraceable Connection - Open Mode	None	1
31.154.81.1	Israel	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1
84.109.69.39	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main.giyus	Block	1
77.138.56.72	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/	Block	1
66.249.66.29	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
180.97.106.161	China	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
46.19.85.108	Israel	147.237.76.86	navy.idf.il	Distributed Abnormally Long Request	Block	1
77.139.102.129	France	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/home/default.aspx	Block	1
66.249.76.72	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 66.249.76.72	Block	1
180.97.106.37	China	147.237.76.42	refuah.idf.il	Multiple Untraceable SSL Sessions from 180.97.106.37 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
46.117.40.37	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
31.154.81.1	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1
85.64.26.54	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	1
77.138.84.93	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
180.97.106.162	China	147.237.76.86	navy.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
176.13.233.200	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
46.19.85.108	Israel	147.237.76.86	navy.idf.il	Distributed Illegal HTTP Version	Block	1
79.177.150.138	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
66.249.76.72	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/.well-known/apple-app-site-association	Block	1
180.97.106.37	China	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
42.96.177.34	China	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
77.139.56.6	France	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$emailUpdate$txtEmail in www.aka.idf.il/main/giyus/faq.aspx	None	1
66.249.66.180	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
180.97.106.162	China	147.237.76.200	eitan.aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
79.177.168.13	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.76.112	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.112	Block	1
180.97.106.37	China	147.237.77.234	halag.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.64.105	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/.well-known/assetlinks.json	Block	1
42.96.177.34	China	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/wp-login.php	Block	1
108.231.240.75	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	1

09-28-2016-23:04:07 to 09-29-2016-00:04:07