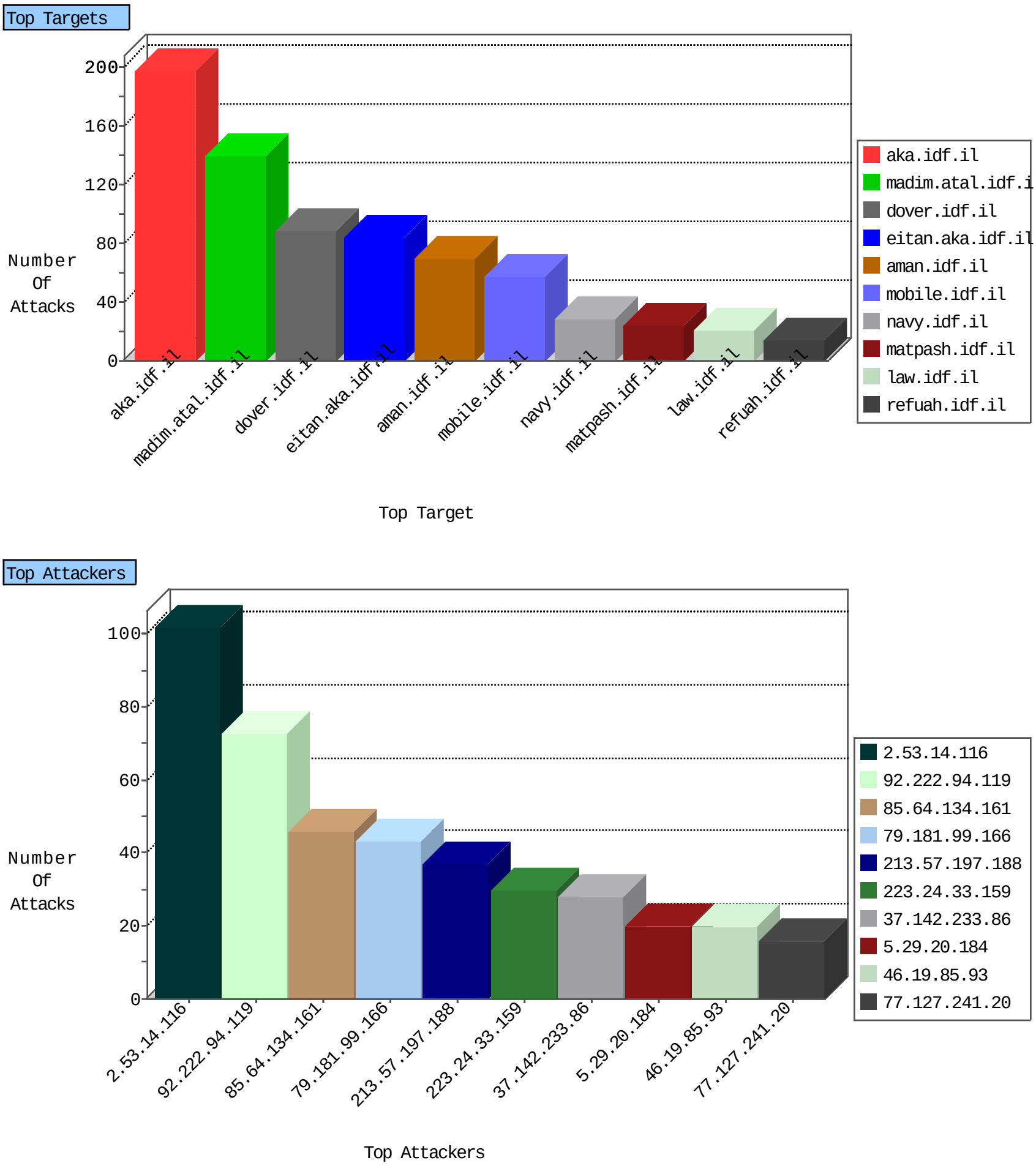
09-30-2016-17:04:09 to 09-30-2016-18:04:09

IDF Under Attack
Daily Report



09-30-2016-17:04:09 to 09-30-2016-18:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
180.104.45.221	China	147.237.76.86	navy.idf.il	Black List	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
71.6.216.49	United States	147.237.76.202	e.halag.idf.il	Black List	drop	1
220.191.57.124	China	147.237.76.86	navy.idf.il	Black List	drop	1
71.6.216.44	United States	147.237.76.197	e.himush.idf.il	Black List	drop	1

09-30-2016-17:04:09 to 09-30-2016-18:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
92.222.94.119	France	147.237.76.200	eitan.aka.idf.il	C1000074: HTTP: majestic bot	Permit	28
92.222.94.119	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	25
92.222.94.119	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	8
92.222.94.119	France	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	7
92.222.94.119	France	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	5
106.38.241.106	China	147.237.77.170	maarachot.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	4
220.181.125.23	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	4
74.208.230.195	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	3
106.38.241.106	China	147.237.76.200	eitan.aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
106.38.241.106	China	147.237.77.74	law.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2

09-30-2016-17:04:09 to 09-30-2016-18:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
74.208.230.195	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
79.177.125.76	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	3
121.103.242.121	147.237.72.156	Japan	aman.idf.il	ET SCAN Potential SSH Scan	2
115.237.73.191	147.237.72.14	China	dover.idf.il(old)	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.224.161.69	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
207.179.59.33	147.237.8.14	United States	e.orchot.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
66.249.75.12	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	1
163.172.11.244	147.237.77.235	United Kingdom	sviva.idf.il	ET SCAN NMAP -sS window 2048	1
58.220.2.5	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.11.244	147.237.0.34	United Kingdom	tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
46.120.122.219	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	1
163.172.11.244	147.237.0.34	United Kingdom	tikshuv.idf.il	ET SCAN NMAP -f -sS	1
27.12.211.101	147.237.0.15	China	kosher-kravi.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
121.103.242.121	147.237.72.167	Japan	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
121.103.242.121	147.237.72.14	Japan	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
91.224.161.69	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN Potential SSH Scan	1
79.182.127.157	147.237.76.86	Israel	navy.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
163.172.11.244	147.237.77.235	United Kingdom	sviva.idf.il	ET SCAN NMAP -sS window 3072	1
62.210.189.248	147.237.8.14	France	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
163.172.11.244	147.237.77.235	United Kingdom	sviva.idf.il	ET SCAN NMAP -f -sS	1
46.161.40.17	147.237.0.34	Russian Federation	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.11.244	147.237.0.34	United Kingdom	tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
40.121.139.43	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
121.103.242.121	147.237.72.217	Japan	e.idf.il	ET SCAN Potential SSH Scan	1

09-30-2016-17:04:09 to 09-30-2016-18:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
85.64.134.161	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	46
223.24.33.159	Thailand	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
79.181.99.166	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	19
79.181.99.166	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	18
213.57.197.188	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	9
213.57.197.188	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
176.13.229.21	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	8
213.57.197.188	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
5.29.20.184	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.84	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.93	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.93	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.95	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
2.55.19.168	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.97.123	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.227.45	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	5
79.181.99.166	Israel	147.237.72.156	aman.idf.il	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	5
46.19.86.102	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
109.253.209.50	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.84	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.93	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
84.108.248.21	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.1	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
176.13.225.111	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
213.57.197.188	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.85.84	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
185.89.217.229	Netherlands	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.1	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
213.57.197.188	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
5.29.20.184	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
46.133.111.232	Ukraine	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.93	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
213.57.197.188	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.29.20.184	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.176.75.32	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.29.20.184	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.19.85.192	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
217.132.101.40	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
85.64.92.24	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.85.102	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.133.111.232	Ukraine	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
84.108.85.8	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
185.3.147.233	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
109.253.199.71	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
93.169.182.218	Saudi Arabia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
176.13.19.160	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
5.29.20.184	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
80.246.139.193	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
109.253.128.218	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2

09-30-2016-17:04:09 to 09-30-2016-18:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.14.116	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	102
37.142.233.86	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	28
109.253.209.65	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
79.178.1.179	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	4
192.243.55.136	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.136	Block	4
80.246.136.241	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
80.252.37.124	Austria	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/sachar	Block	3
77.139.13.144	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	Block	3
77.138.119.144	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	Block	2
46.19.86.237	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
82.81.40.246	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
216.244.66.236	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 216.244.66.236	Block	2
31.154.81.11	Israel	147.237.76.42	refuah.idf.il	PHP Attempt	Block	2
176.13.230.51	Israel	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/894-ar	Block	2
77.127.241.20	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Method from 77.127.241.20	Block	2
31.154.81.11	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	2
176.13.230.51	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	2
208.51.63.37	United States	147.237.77.216	dover.idf.il	PHP Attempt	Block	2
77.127.241.20	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 77.127.241.20 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	2
77.127.241.20	Israel	147.237.72.156	aman.idf.il	Multiple Abnormally Long Request from 77.127.241.20	Block	2
5.29.177.217	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	1
180.76.15.147	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9023-he/refuah.aspx	Block	1
105.105.187.192	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/'	Block	1
77.127.241.20	Israel	147.237.72.156	aman.idf.il	Multiple Malformed HTTP Header Line from 77.127.241.20	Block	1
79.181.99.166	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.79.169	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1486-he/atal.aspx	Block	1
217.132.125.22	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 217.132.125.22	Block	1
192.243.55.136	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/327-he/patzar.aspx?pagenum=2	Block	1
77.139.37.100	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
176.13.12.11	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
77.127.241.20	Israel	147.237.72.156	aman.idf.il	NULL Character in Method	Block	1
77.127.241.20	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Header Name from 77.127.241.20	Block	1
79.177.125.76	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/patzar	Block	1
66.249.65.51	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
77.138.121.222	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
192.243.55.130	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.130	Block	1
77.127.241.20	Israel	147.237.72.156	aman.idf.il	Multiple Malformed URL from 77.127.241.20	Block	1
66.249.79.172	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1232-he/atal.aspx	Block	1
220.181.125.23	China	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 220.181.125.23	Block	1
66.102.9.5	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
199.212.86.112	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
77.139.88.53	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/pniot.aspx	Block	1
77.127.241.20	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
84.108.248.21	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.65.58	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8859-he/refuah.aspx	Block	1
216.244.66.236	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/site/unselecatble.aspx	Block	1
77.138.204.196	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.138.204.196	Block	1
192.243.55.130	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/kadatz	Block	1
141.226.218.85	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
77.127.241.20	Israel	147.237.72.156	aman.idf.il	Multiple NULL Character in Method from 77.127.241.20	Block	1

09-30-2016-17:04:09 to 09-30-2016-18:04:09