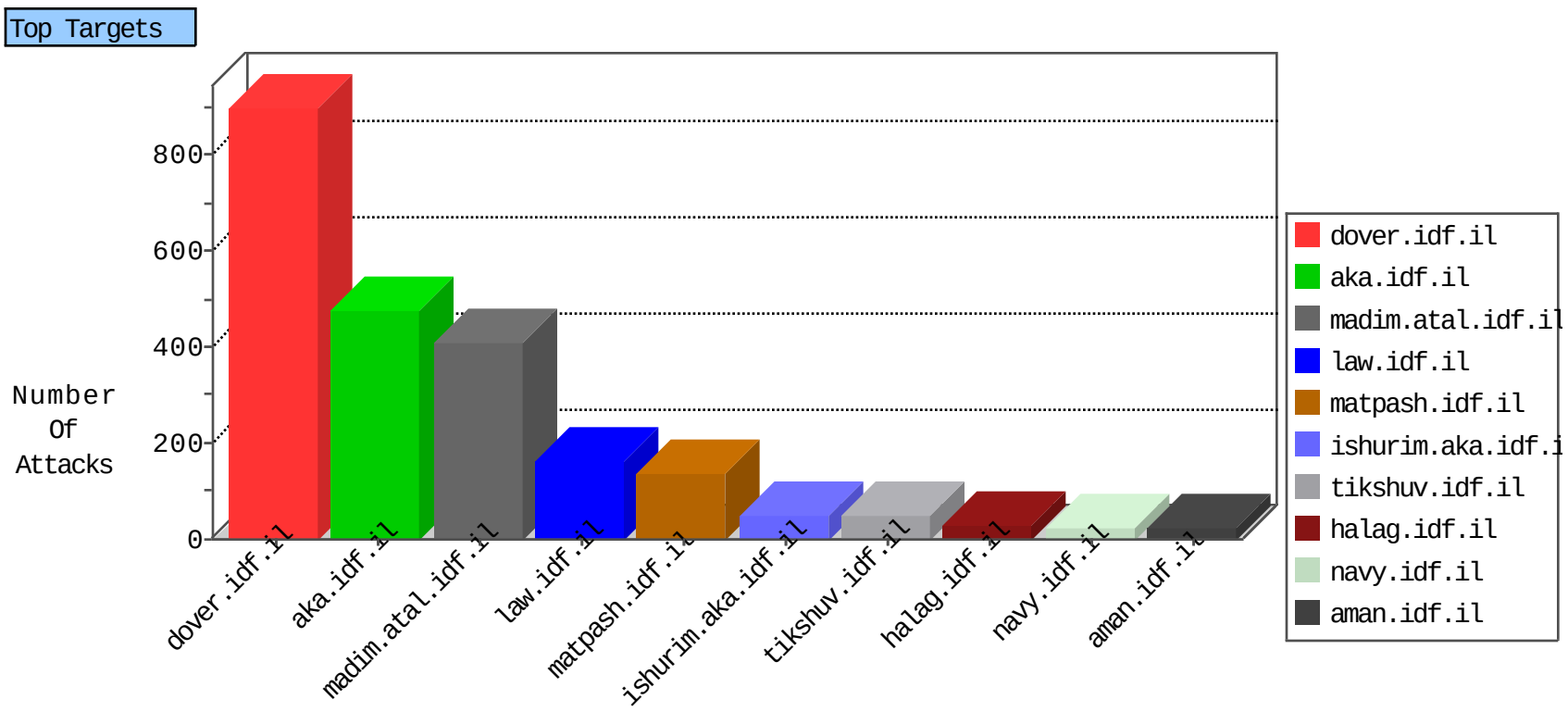
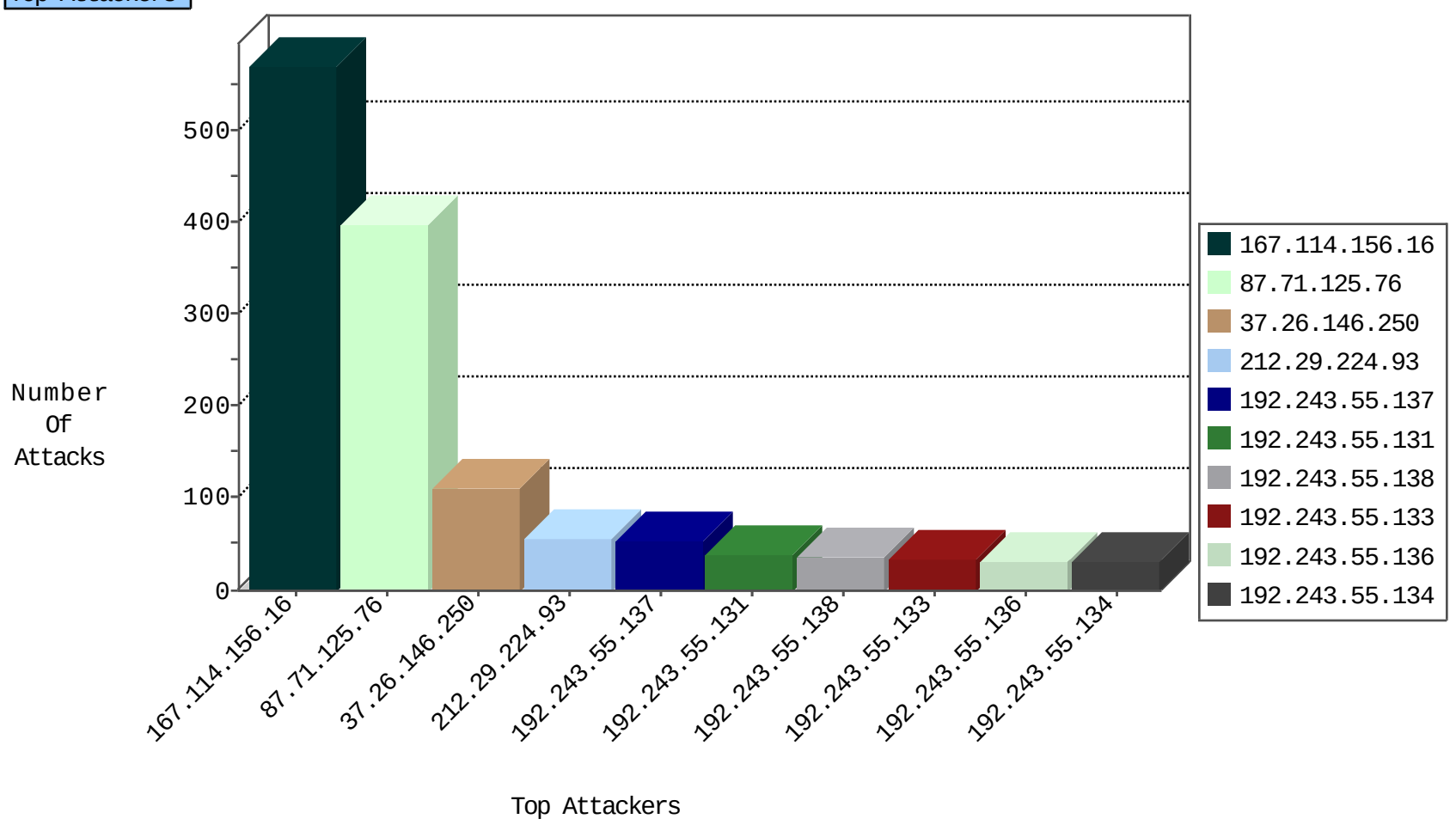
03-10-2016-18:04:05 to 03-10-2016-19:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-10-2016-18:04:05 to 03-10-2016-19:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	4000
2.52.149.49	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	74
79.183.98.143	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	21
82.145.216.142	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	5
221.0.95.227	China	147.237.76.148	gqcenter.aka.idf.il	JLM_Purple_Con_Limit_Tcp	drop	2
89.248.172.207	Netherlands	147.237.77.212	e.dover.idf.il	Block_Ntp_All_Net	drop	1
221.0.95.227	China	147.237.76.198	e.yohalan.idf.il	JLM_Purple_Con_Limit_Https	drop	1
89.248.172.207	Netherlands	147.237.0.16	my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
89.248.172.207	Netherlands	147.237.77.233	atal.idf.il	Block_Ntp_All_Net	drop	1
79.183.98.143	Israel	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
89.248.172.207	Netherlands	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
89.248.172.207	Netherlands	147.237.77.178	e.matpash.idf.il	Block_Ntp_All_Net	drop	1

03-10-2016-18:04:05 to 03-10-2016-19:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.109.32.144	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	18
79.181.56.133	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
87.71.37.242	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
123.126.113.154	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
84.108.245.193	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
46.19.86.216	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
84.94.38.118	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-10-2016-18:04:05 to 03-10-2016-19:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
212.199.57.193	147.237.72.166	Israel	aka.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	4
199.101.186.238	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 2048	1
1.52.59.143	147.237.8.45	Vietnam	e.eitan.idf.il	ET SCAN NMAP -f -sS	1
93.189.26.18	147.237.8.50	Austria	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
199.101.186.238	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -f -sS	1
87.70.61.56	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.230.182.133	147.237.76.34	France	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
180.97.215.116	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
80.246.136.103	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
178.63.11.208	147.237.76.44	Germany	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
46.116.150.253	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
178.62.94.12	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.149.237	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
162.213.37.21	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -f -sS	1
220.231.195.122	147.237.76.200	China	eitan.aka.idf.il	ET SCAN NMAP -sS window 3072	1
2.54.147.44	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.129.80	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
1.52.59.143	147.237.8.45	Vietnam	e.eitan.idf.il	ET SCAN NMAP -sS window 2048	1
98.119.105.221	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 3072	1
199.101.186.238	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
89.139.251.80	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.74	147.237.77.226	United States	www.chamatz.aka.idf.il	ET DROP Dshield Block Listed Source	1
83.130.105.203	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.243.55.136	147.237.77.216	Dominica	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.137.55	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
180.97.106.37	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
178.63.11.208	147.237.76.39	Germany	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
46.116.114.154	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
162.213.37.21	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 2048	1
5.22.135.140	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.140.211	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
220.231.195.122	147.237.76.200	China	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
2.54.56.185	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.65.201.84	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

03-10-2016-18:04:05 to 03-10-2016-19:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.26.146.250	Israel	147.237.77.176	matpash.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	111
212.29.224.93	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	45
128.54.236.94	United States	147.237.77.176	matpash.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
176.13.16.117	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
77.125.12.177	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
109.253.150.95	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
2.52.12.50	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
79.181.229.213	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.29.224.93	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid sequence number	monitor	12
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.180.66.139	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
37.26.149.237	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
79.179.20.128	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.137	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.9	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
5.22.131.63	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.228.148.72	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.102.195.96	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.32.179.54	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.30.137	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.27.117	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.237	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
80.246.137.239	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.189	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.136	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.67.118.38	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.133	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
2.52.181.11	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
81.4.163.106	Cyprus	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.131	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	5
192.243.55.137	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.136	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.128	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
192.243.55.137	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
5.22.131.76	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
192.243.55.138	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.71.125.76	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	398
80.246.130.249	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 80.246.130.249	Block	15
2.54.13.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
109.253.129.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
87.70.45.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.116.150.253	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
79.180.35.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.117.112.46	Israel	147.237.72.166	aka.idf.il	Redundant HTTP Headers from 46.117.112.46	Block	2
79.180.66.139	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
2.54.208.2	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
109.65.201.84	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	2
185.89.217.227		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
5.22.131.123	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/	Block	1
130.193.51.62	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
86.25.96.54	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
68.180.228.109	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation PageNum in www.tikshuv.idf.il/901-he/tikshuv.aspx	Block	1
197.96.66.125	South Africa	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
185.25.148.240	Poland	147.237.72.166	aka.idf.il	Unauthorized URL Access to testp3.pospr.waw.pl/testproxy.php	Block	1
80.246.130.249	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1500-en/dover.asp	Block	1
185.89.217.232		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.143	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/sachar/resources/images/logo.jpg	Block	1
31.172.191.135	Poland	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
141.8.184.13	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
69.198.205.18	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
198.20.69.74	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
185.25.151.159	Poland	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to testp5.mielno.lubin.pl/testproxy.php	Block	1
46.117.112.46	Israel	147.237.72.166	aka.idf.il	Redundant HTTP Headers Referer	Block	1
109.253.150.95	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
2.54.146.212	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.255.192.237	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/wp-content/themes/antioch/lib/scripts/download.php	Block	1
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/history/entebbe1.stm<p>	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-he	Block	1
36.33.6.61	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to z-h-e-n-111.appspot.com/	Block	1
157.55.39.12	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
218.10.51.70	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to 323.yui87x20.appspot.com/	Block	1
185.25.151.159	Poland	147.237.77.233	atal.idf.il	Unauthorized URL Access to testp5.mielno.lubin.pl/testproxy.php	Block	1
115.200.238.156	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
2.54.187.42	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
82.102.169.113	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.224	Block	1
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.243.55.135	Block	1
37.26.146.203	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
173.13.178.34	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-en/dover.aspx	Block	1
88.250.44.10	Turkey	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	1
185.89.217.225		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.121.158.234	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl105 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
116.113.49.19	China	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
86.25.96.54	United Kingdom	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-18863-en/dover.aspx.	Block	1
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-13885-en/dov.	Block	1