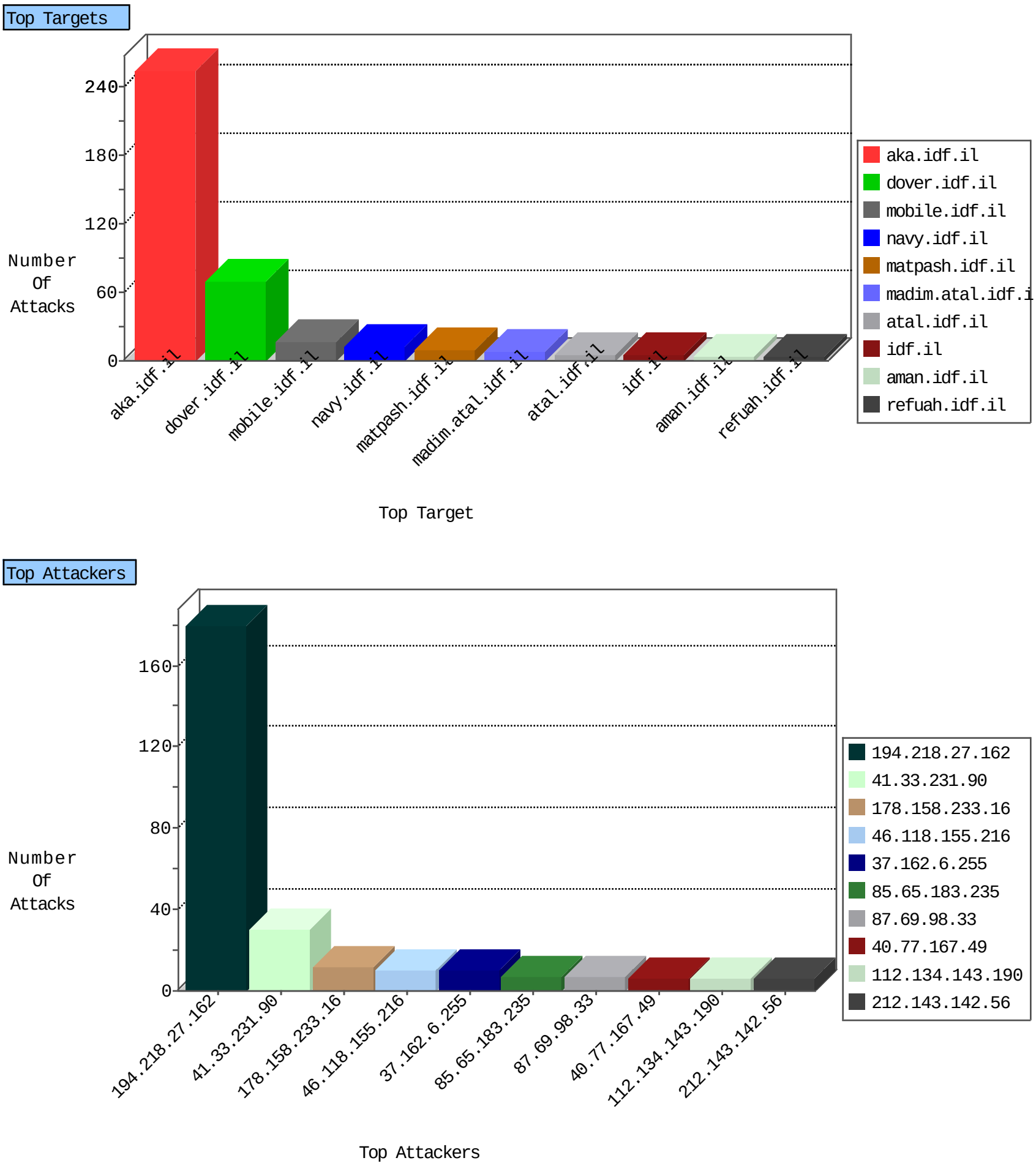
03-01-2016-05:04:05 to 03-01-2016-06:04:05

IDF Under Attack Daily Report



03-01-2016-05:04:05 to 03-01-2016-06:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
184.105.139.120	United States	147.237.77.234	halag.idf.il	Block_Ntp_All_Net	drop	1
78.36.187.12	Russian Federation	147.237.77.74	law.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.92	United States	147.237.72.167	ishurim.aka.idf.il	Block_Ntp_All_Net	drop	1
185.35.62.87	Switzerland	147.237.77.178	e.matpash.idf.il	Block_Udp_All_Nets	drop	1
104.158.24.81	Canada	147.237.77.61	e.cogat.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.104	United States	147.237.77.205	prisha.idf.il	Block_Ntp_All_Net	drop	1
23.239.64.15	United States	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.224		147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.68	United States	147.237.8.46	e.chinuch.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.116	United States	147.237.8.28	e.mobile-ks.idf.il	Block_Ntp_All_Net	drop	1
23.239.64.15	United States	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.224		147.237.77.234	halag.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.68	United States	147.237.77.179	e.mazi.idf.il	Block_Ntp_All_Net	drop	1

03-01-2016-05:04:05 to 03-01-2016-06:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
119.74.148.71	Singapore	147.237.77.216	dover.idf.il	C1000008: HTTP: Xenu UserAgent	Block	2
62.210.148.246	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
66.249.66.184	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
51.255.65.32	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.63	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.77	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

03-01-2016-05:04:05 to 03-01-2016-06:04:05

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
37.162.6.255	147.237.76.86	France	navy.idf.il	ET SCAN NMAP -sA (2)	4
94.102.48.193	147.237.77.216	Netherlands	dover.idf.il	ET SCAN NMAP -sS window 1024	1
46.130.112.6	147.237.76.31	Armenia	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
5.104.111.218	147.237.76.38	Germany	e.e.meitav.idf.il	ET SCAN NMAP -sS window 2048	1
5.104.111.218	147.237.76.38	Germany	e.e.meitav.idf.il	ET SCAN NMAP -f -sS	1
193.201.227.57	147.237.0.19	Ukraine	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
189.254.90.133	147.237.0.33	Mexico	idf.il	ET SCAN NMAP -sS window 2048	1
188.191.21.221	147.237.72.166	Ukraine	aka.idf.il	ET SCAN NMAP -sS window 1024	1
104.232.98.38	147.237.0.33		idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.114	147.237.76.39	Ukraine	mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
5.104.111.218	147.237.76.38	Germany	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.227.57	147.237.0.34	Ukraine	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
189.254.90.133	147.237.0.33	Mexico	idf.il	ET SCAN NMAP -sS window 3072	1
189.254.90.133	147.237.0.33	Mexico	idf.il	ET SCAN NMAP -f -sS	1
104.232.98.38	147.237.0.33		idf.il	ET SCAN NMAP -sS window 4096	1

03-01-2016-05:04:05 to 03-01-2016-06:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	119
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	59
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
46.19.85.223	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
40.77.167.49	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.182.15.77	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.131.95	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.72.8	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.162.6.255	France	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
5.144.58.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.2.73	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.127.205.11	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
112.134.143.190	Sri Lanka	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
79.177.153.145	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.63.238	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
73.3.77.56	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.178.183.107	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
157.55.39.253	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
106.38.241.106	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
66.249.66.96	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
119.74.148.71	Singapore	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
85.65.188.111	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.159	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.18	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.151	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
37.26.147.239	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
137.116.71.170	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.104	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
106.38.241.106	China	147.237.77.233	atal.idf.il	drop	SAM rule	drop	1
184.105.247.231	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.156	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.26	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.149	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
113.76.90.199	China	147.237.77.234	halag.idf.il	drop	SAM rule	drop	1
94.230.86.61	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.152	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
141.212.122.144	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
112.134.143.190	Sri Lanka	147.237.76.34	yohalan.idf.il	drop		drop	1
185.106.92.164		147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
79.182.17.72	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
141.212.122.157	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.150	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
114.112.90.54	China	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.152	United States	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.145	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.106.92.164		147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
84.108.16.40	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.158	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.150	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.65.183.235	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 85.65.183.235	Block	6
178.158.233.16	Ukraine	147.237.72.166	aka.idf.il	PHP Attempt	Block	6
178.158.233.16	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 178.158.233.16	Block	5
87.69.98.33	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 87.69.98.33	Block	4
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	4
87.69.98.33	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1514	Block	3
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	3
46.119.127.64	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi/	Block	3
131.253.25.144	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
82.81.21.169	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.120.125.41		147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
180.189.144.220	Australia	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
66.249.78.236	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
185.112.248.32		147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
128.151.150.25	United States	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
64.41.200.105	United States	147.237.72.156	aman.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	1
178.158.233.16	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/index.php	Block	1
93.173.232.206	Israel	147.237.77.243	mobile.idf.il	SSL Untraceable Connection - Open Mode	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1381-he/dover.aspx	Block	1
85.65.183.235	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
66.249.66.96	United States	147.237.72.166	aka.idf.il	Unknown Parameter KEY in www.aka.idf.il/valtam/asp/default.asp	None	1
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
108.84.128.238	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
73.3.77.56	United States	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$employmentStatesMonth in www.aka.idf.il/main/sachar/payslips.aspx	None	1
187.36.16.13	Brazil	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/home/default.aspxhot	Block	1
64.41.200.105	United States	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 64.41.200.105 (Protocol violation (SSL_CONN_CLIENT_KEY_EXCHANGE))	None	1
174.70.103.251	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
85.250.175.199	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/926-he/refuah.aspx	Block	1
66.249.66.125	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/m/templates/getfile/getfile.aspx	Block	1
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
184.105.139.70	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
112.134.143.190	Sri Lanka	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to 147.237.0.15/1phpmyadmin/	Block	1
77.75.77.101	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
192.162.26.46	Spain	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 192.162.26.46 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
64.41.200.105	United States	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.69.26	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	1
184.105.247.196	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
112.134.143.190	Sri Lanka	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/1phpmyadmin/	Block	1
64.41.200.105	United States	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_KEY_EXCHANGE)	None	1