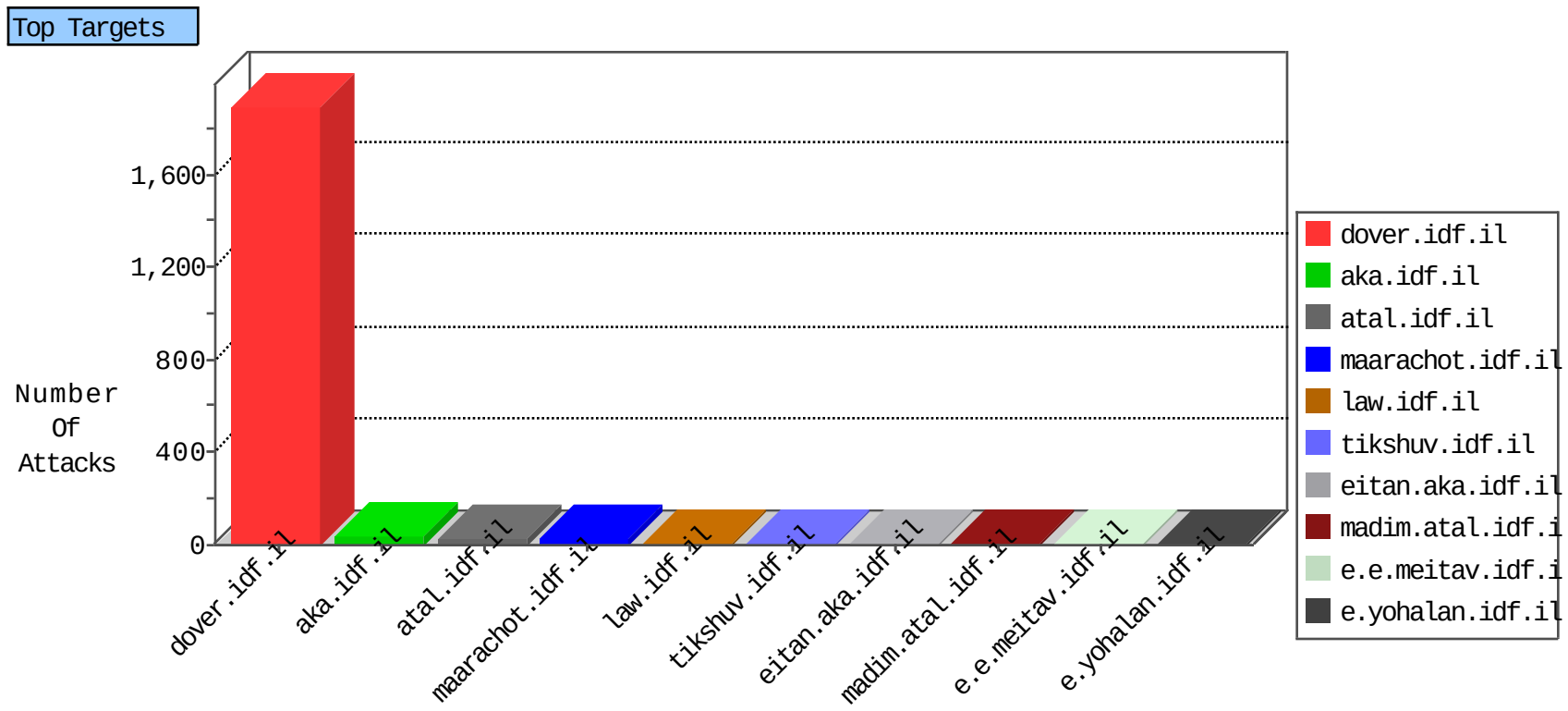
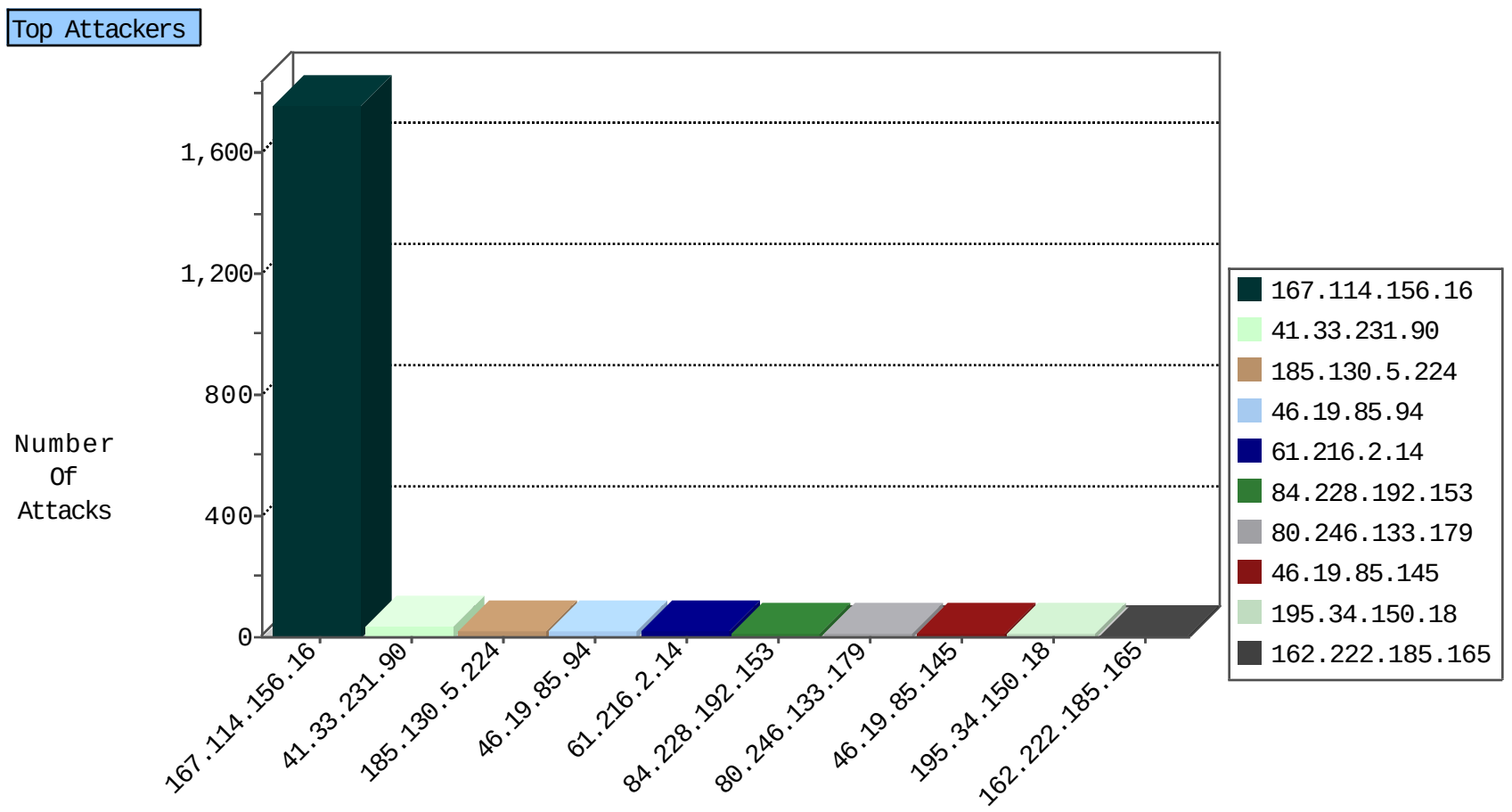
01-04-2016-02:04:05 to 01-04-2016-03:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-04-2016-02:04:05 to 01-04-2016-03:04:05

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	3216
76.75.126.81	Canada	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
107.150.98.131	United States	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1

01-04-2016-02:04:05 to 01-04-2016-03:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-04-2016-02:04:05 to 01-04-2016-03:04:05

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
180.150.177.188	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
162.222.185.165	147.237.76.177	United States	ncore.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.76.30	United States	himush.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
95.218.131.95	147.237.72.217	Romania	e.idf.il	ET SCAN NMAP -sS window 1024	1
80.246.133.179	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
209.126.116.147	147.237.72.166	United States	aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.216.2.14	147.237.76.177	Taiwan	ncore.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
185.130.5.224	147.237.77.212		e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
180.150.177.188	147.237.76.196	China	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
162.222.185.165	147.237.76.196	United States	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.0.34	United States	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.203	147.237.77.234	Netherlands	halag.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
61.216.2.14	147.237.77.179	Taiwan	e.mazi.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
185.130.5.224	147.237.8.50		e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1

01-04-2016-02:04:05 to 01-04-2016-03:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
84.228.192.153	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
61.216.2.14	Taiwan	147.237.77.233	atal.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	9
46.19.85.94	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.145	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.178.119.65	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.19.85.145	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.246.133.179	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
217.132.6.46	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
194.90.89.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.133.179	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.94	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.204	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
93.172.3.107	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
37.26.149.168	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
98.252.51.195	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
79.178.33.193	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
157.55.39.69	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
85.177.83.219	Germany	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
68.180.229.121	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
185.130.5.224		147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	2
203.127.96.218	Singapore	147.237.77.216	dover.idf.il	SYN Attack		reject	2
185.130.5.224		147.237.77.233	atal.idf.il	drop	SAM rule	drop	2
61.216.2.14	Taiwan	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
185.3.144.97	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
82.81.45.133	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
185.130.5.224		147.237.76.148	gqcenter.aka.idf.il	drop	SAM rule	drop	2
208.115.113.89	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
61.216.2.14	Taiwan	147.237.77.179	e.mazi.idf.il	drop	First packet isn't SYN	drop	1
185.130.5.224		147.237.8.24	e.lifestyle.idf.il	drop	SAM rule	drop	1
203.127.96.216	Singapore	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
84.108.61.199	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
185.130.5.224		147.237.76.201	e.atal.idf.il	drop	SAM rule	drop	1
65.55.218.57	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
185.130.5.224		147.237.76.34	yohalan.idf.il	drop	SAM rule	drop	1
46.19.86.211	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
203.127.96.221	Singapore	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
195.154.38.230	France	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
185.130.5.224		147.237.76.196	e.sviva.idf.il	drop	SAM rule	drop	1
61.216.2.14	Taiwan	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
185.130.5.224		147.237.8.27	e.madim.atal.idf.il	drop	SAM rule	drop	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
203.127.96.216	Singapore	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
37.26.149.168	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
84.108.61.199	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.130.5.224		147.237.77.212	e.dover.idf.il	drop	SAM rule	drop	1
61.216.2.14	Taiwan	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
167.114.156.16	Canada	147.237.77.216	dover.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
2.54.25.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
79.182.221.233	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
68.191.69.219	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en	Block	2
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
66.230.230.230	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
46.19.85.94	Israel	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 46.19.85.94	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.93.99	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
46.43.185.41	United Kingdom	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
150.70.173.54	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
46.19.85.94	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
79.176.73.236	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
46.19.85.94	Israel	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 46.19.85.94	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
109.201.154.230	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.112	Block	1
46.43.185.41	United Kingdom	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
187.60.107.77	Brazil	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/general.aspx	Block	1
46.19.85.94	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
46.19.85.94	Israel	147.237.77.216	dover.idf.il	Multiple Malformed URL from 46.19.85.94	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
150.70.97.85	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1362-he/dover.aspx	Block	1
54.152.151.136	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;list in www.aka.idf.il/chinuch/klali/default.asp	None	1
187.60.107.77	Brazil	147.237.0.34	tikshuv.idf.il	Parameter Type Violation docId in www.tikshuv.idf.il/site/general.aspx	Block	1
46.19.85.94	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp	Block	1
46.19.85.94	Israel	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 46.19.85.94	Block	1
150.70.97.85	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
23.251.86.72	United States	147.237.77.74	law.idf.il	PHP Attempt	Block	1
61.216.2.14	Taiwan	147.237.77.233	atal.idf.il	Unauthorized URL Access to 8.8.8.8/404	Block	1
192.99.41.217	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
46.19.85.94	Israel	147.237.77.216	dover.idf.il	Malformed URL http/1.1	Block	1
66.249.79.28	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/shared/usercontrols/headerupper/	Block	1
46.19.85.94	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method /Shared/ClientScripts/SideBar/sideBar.js in URL www.idf.ilhttp/1.1	Block	1
150.70.173.54	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
23.251.86.72	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/xmlrpc.php	Block	1
69.171.228.117	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

01-04-2016-02:04:05 to 01-04-2016-03:04:05