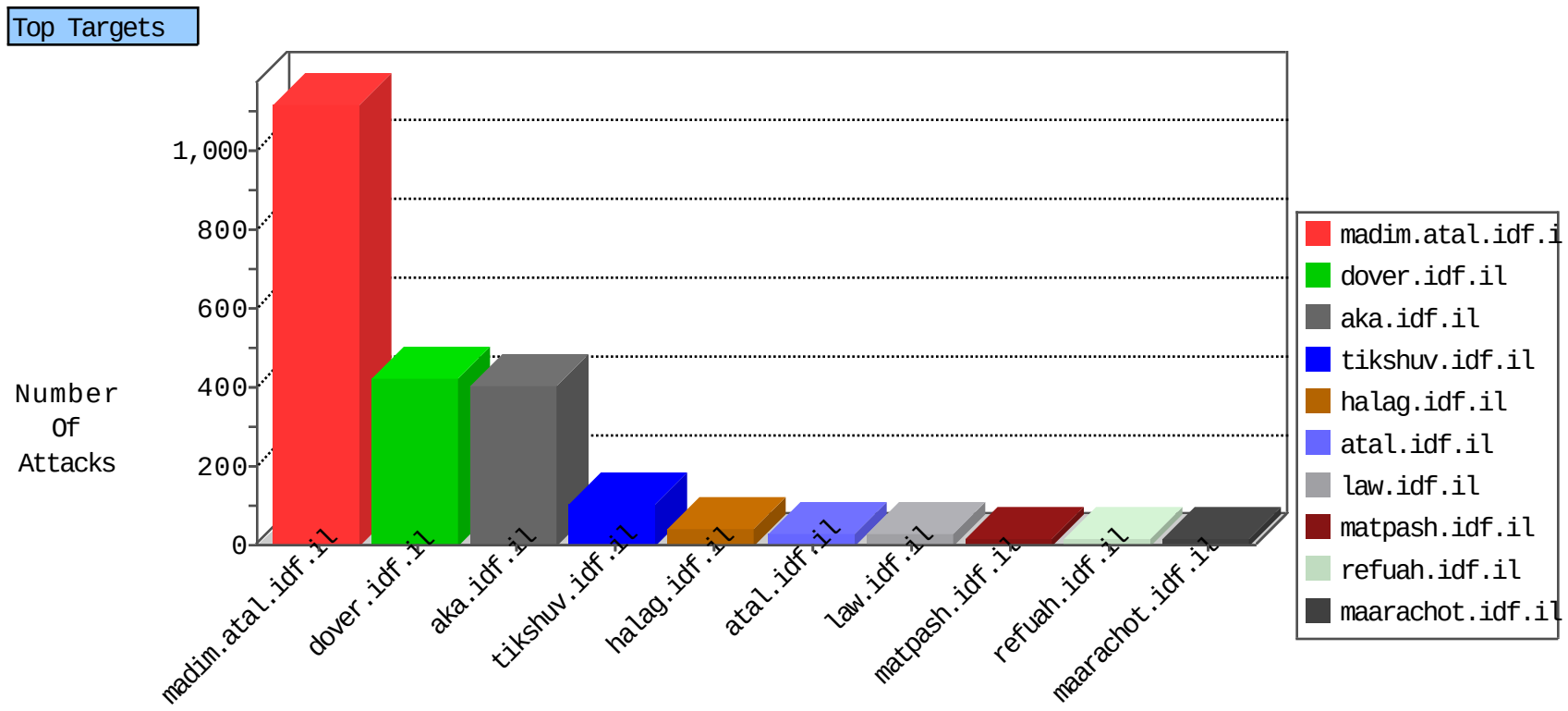
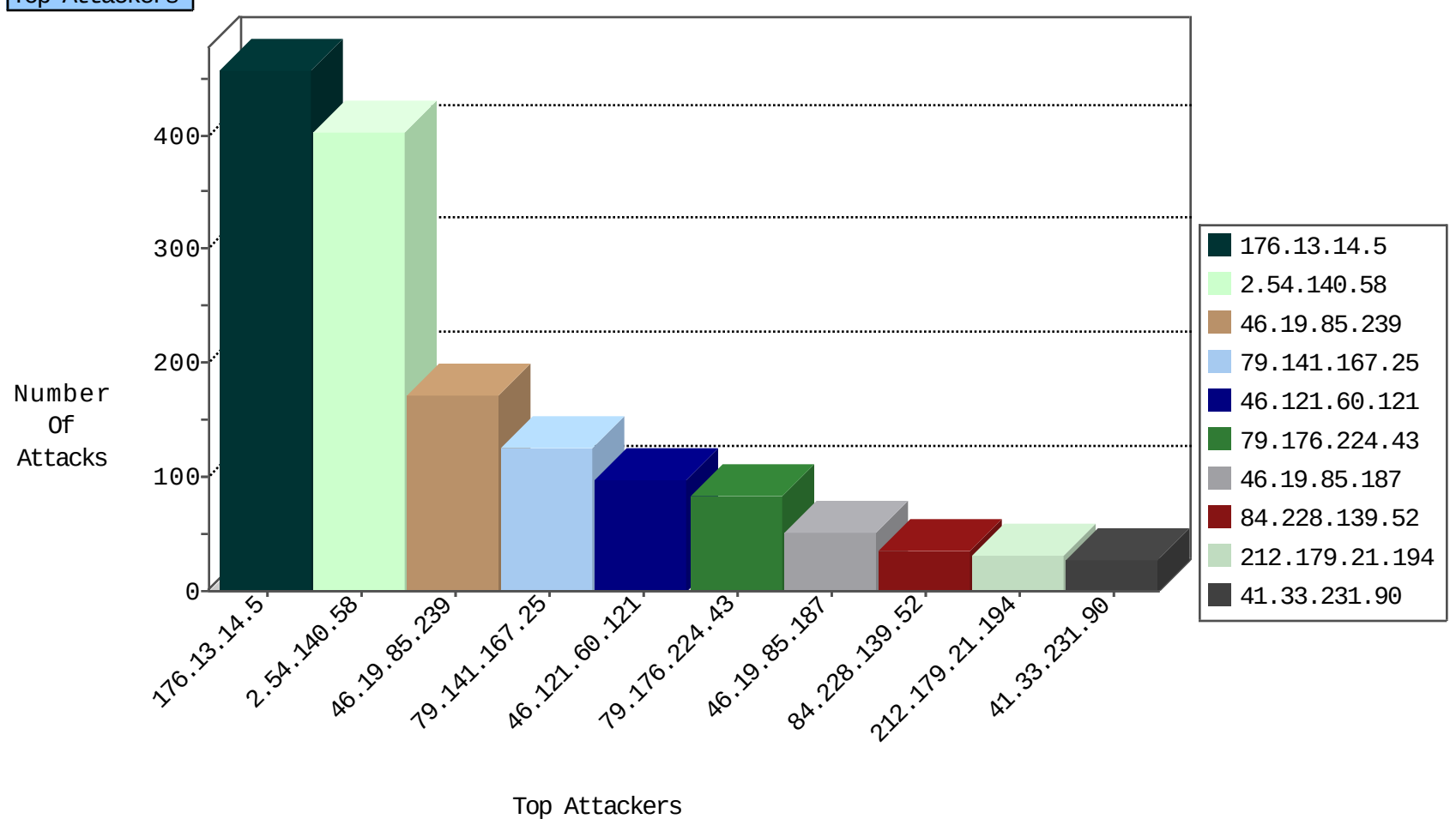
02-17-2016-16:04:03 to 02-17-2016-17:04:03

IDF Under Attack
Daily Report

Top Targets



Top Attackers



02-17-2016-16:04:03 to 02-17-2016-17:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.141.167.25	Switzerland	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-cat	dest-reset	93
207.232.36.181	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	66
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	4
212.179.54.237	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
31.168.240.21	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
185.94.111.1		147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
104.238.129.180		147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1		147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1

02-17-2016-16:04:03 to 02-17-2016-17:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
65.111.169.4	United States	147.237.77.216	dover.idf.il	3886: HTTP: Cross Site Scripting in POST Request	Block	2
69.30.215.142	United States	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	1

02-17-2016-16:04:03 to 02-17-2016-17:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
79.141.167.25	147.237.77.216	Switzerland	dover.idf.il	ET CURRENT_EVENTS Inbound Low Orbit Ion Cannon LOIC DDOS Tool desu string	2
65.111.169.4	147.237.77.216	United States	dover.idf.il	GPL WEB_SERVER /etc/passwd	2
65.111.169.4	147.237.77.216	United States	dover.idf.il	SQL Injection - Select From	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
176.13.23.55	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.103	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.66.112.245	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.179.71	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
103.224.167.30	147.237.8.24	Singapore	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
2.54.5.247	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.138.172.120	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.200.142.180	147.237.76.86	Kazakstan	navy.idf.il	ET SCAN NMAP -sS window 3072	1
79.177.163.189	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
208.115.111.73	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
192.116.166.66	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.117.129.162	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.67.102.70	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.28.154.89	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.255.65.207	147.237.76.39		mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
2.54.158.86	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
103.224.167.30	147.237.8.14	Singapore	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
2.52.32.203	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.111.70.5	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.179.9.115	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.176.227.245	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
50.118.172.244	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1

02-17-2016-16:04:03 to 02-17-2016-17:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.176.224.43	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	84
2.54.140.58	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	26
212.179.21.194	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	24
79.141.167.25	Switzerland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	24
31.168.83.233	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
89.139.49.84	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
212.199.34.114	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
46.19.85.188	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
72.9.148.10	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	13
2.54.37.84	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
82.80.28.245	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
84.228.139.52	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	11
82.80.51.115	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
66.249.79.6	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.85.111	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.153	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
77.127.230.232	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
109.253.131.93	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.228.139.52	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
194.250.161.45	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
87.68.243.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.253.106	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.129	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
84.228.139.52	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
84.228.139.52	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
82.81.44.151	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
212.235.72.108	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.228.139.52	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.95.217.4	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.131.93	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
122.170.157.40	India	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
188.120.148.10	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.193	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
66.249.93.60	Israel	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	5
122.170.157.40	India	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.193	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.253.215.100	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
66.249.93.248	Israel	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	5
122.170.157.40	India	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
46.19.85.108	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.224	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
66.249.66.95	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.54.176.232	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.54.135.212	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
31.210.186.156	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.108	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4

02-17-2016-16:04:03 to 02-17-2016-17:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.14.5	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.14.5	Block	268
2.54.140.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	249
176.13.14.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	186
46.19.85.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	168
2.54.140.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	113
46.121.60.121	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 46.121.60.121	Block	97
46.19.85.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	52
37.26.146.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
2.54.140.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	15
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	11
65.111.169.4	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 65.111.169.4	Block	9
85.64.191.131	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 85.64.191.131	Block	9
85.65.47.130	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 85.65.47.130	Block	5
85.64.191.131	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	5
83.130.121.112	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	3
176.13.14.5	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 176.13.14.5	Block	3
109.66.163.55	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.66.163.55	Block	3
85.65.47.130	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	3
65.55.210.203	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
176.13.1.106	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
212.117.143.250	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	2
109.66.163.55	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.154.19.5	Block	2
193.227.170.194	Lebanon	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	2
80.246.133.219	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.253.131.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	2
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
5.29.227.158	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/xmlrpc.php	Block	1
85.65.47.130	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/updatestatus.php	Block	1
46.19.85.239	Israel	147.237.0.19	madim.atal.idf.il	Cookie Tampering on cookie Login: Expected , Observed ********** ********** **********	None	1
77.6.149.78	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
31.168.114.111	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on www.chamatz.aka.idf.il/xmlrpc.php	Block	1
66.249.66.67	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	1
213.8.204.24	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	1
37.142.68.9	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
192.243.55.136	Dominica	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/5/112435.pdf).	Block	1
80.246.133.196	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.69.58	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.58	Block	1
176.13.7.38	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
65.111.169.4	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/abc123/	Block	1
85.93.89.74	Germany	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/templates/shared/usercontrols/headerupper/	Block	1
84.94.199.153	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
212.199.224.24	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 212.199.224.24	Block	1
37.26.146.131	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
79.178.206.98	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
66.249.66.126	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/5/110485.pdf	Block	1
52.16.137.212	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on /	Block	1
85.64.191.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/updatestatus.php	Block	1

02-17-2016-16:04:03 to 02-17-2016-17:04:03