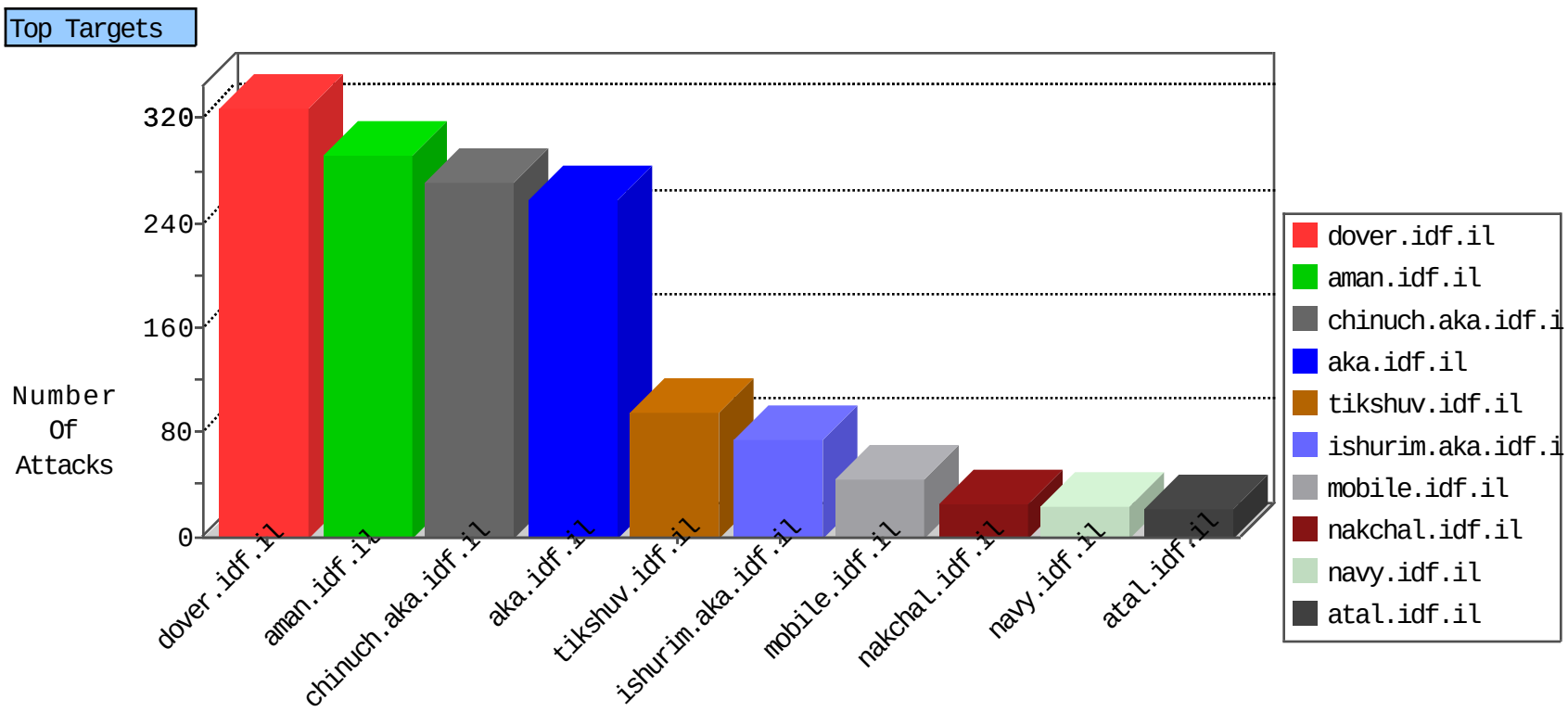
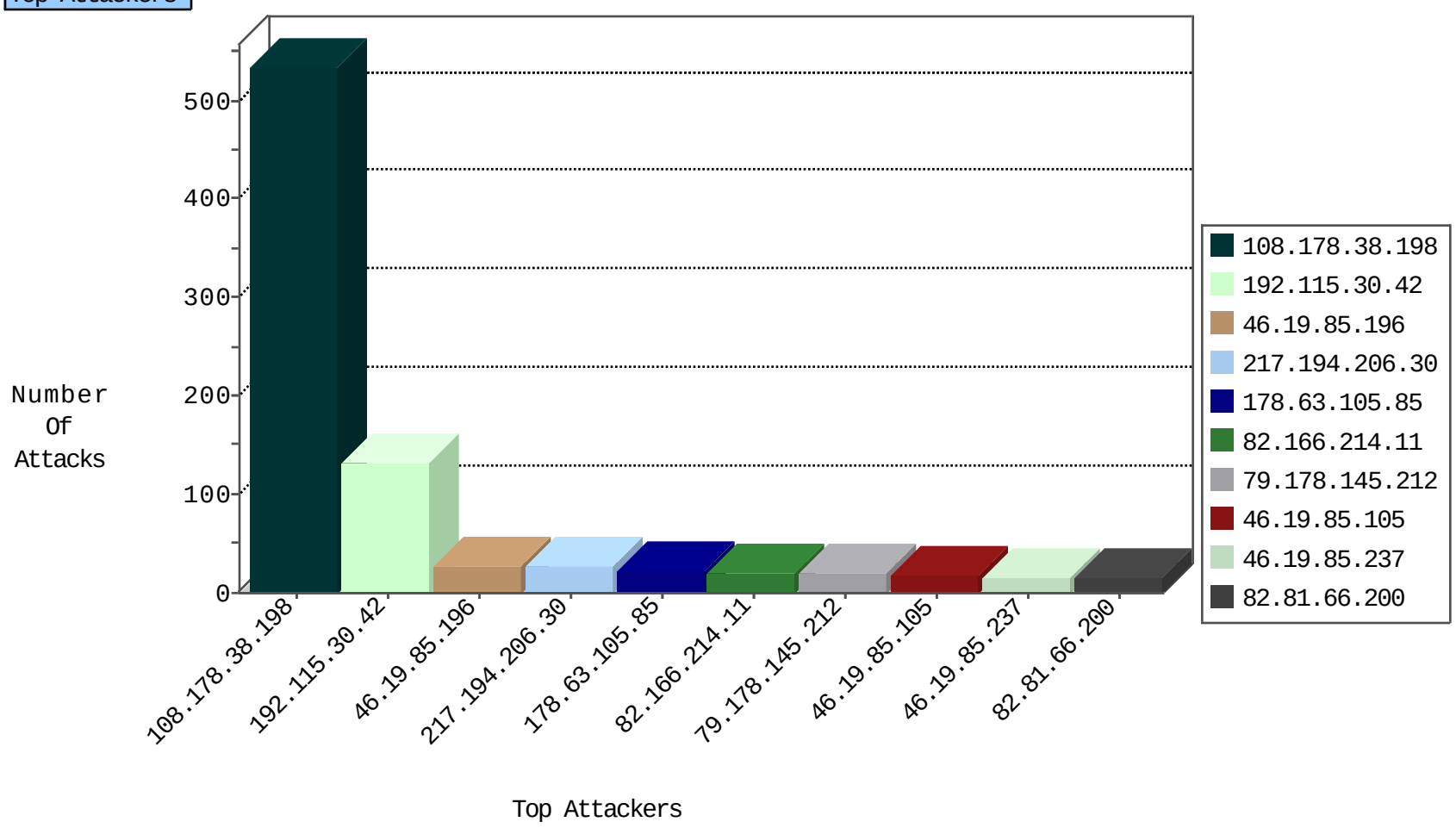
03-07-2016-17:04:08 to 03-07-2016-18:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-07-2016-17:04:08 to 03-07-2016-18:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
198.48.92.104	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
5.29.88.246	Israel	147.237.77.234	halag.idf.il	Invalid TCP Flags	drop	1
89.248.174.4	Netherlands	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
209.126.105.33	United States	147.237.8.45	e.eitan.idf.il	Block_Ntp_All_Net	drop	1
188.138.1.218	Germany	147.237.8.24	e.lifestyle.idf.il	Block_Udp_All_Nets	drop	1
209.126.105.33	United States	147.237.77.19	law-forum.idf.il	Block_Ntp_All_Net	drop	1
72.166.89.99	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
198.48.92.104	United States	147.237.0.33	idf.il	Block_Udp_All_Nets	drop	1

03-07-2016-17:04:08 to 03-07-2016-18:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.178.145.212	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	19
85.250.183.55	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
84.109.0.63	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
46.117.34.25	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
176.13.23.248	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
5.29.231.40	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
84.228.147.208	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
151.80.31.140	Italy	147.237.76.31	nakchal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
66.249.69.87	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
175.10.210.214	China	147.237.77.216	dover.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
79.176.195.217	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-07-2016-17:04:08 to 03-07-2016-18:04:08

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
66.102.9.17	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sA (2)	2
77.125.72.214	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.120.126.39	147.237.77.216		dover.idf.il	portscan: TCP Distributed Portscan	1
61.163.231.229	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
109.253.134.176	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
40.77.103.52	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
108.178.38.198	147.237.72.156	United States	aman.idf.il	portscan: TCP Distributed Portscan	1
23.96.109.87	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 1024	1
104.192.0.226	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
5.22.129.254	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.192.0.226	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
89.138.185.11	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
82.81.56.152	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.127.219.196	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
189.202.241.84	147.237.77.179	Mexico	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
140.242.217.2	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.120.51.143	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.65.54.75	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
23.96.109.87	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 2048	1
104.192.0.226	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
23.96.109.87	147.237.0.33	United States	idf.il	ET SCAN NMAP -f -sS	1
104.192.0.226	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
213.57.106.142	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.139.234.167	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
87.69.230.235	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
204.10.221.47	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.136.142	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
194.90.229.225	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

03-07-2016-17:04:08 to 03-07-2016-18:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
108.178.38.198	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	265
108.178.38.198	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	264
192.115.30.42	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
217.194.206.30	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
82.166.214.11	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
192.115.30.42	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
82.81.66.200	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
192.115.30.42	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
192.115.30.42	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
46.19.85.196	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
192.115.30.42	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.172	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
192.115.30.42	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.19.85.105	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
2.54.140.200	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.67.158.246	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.196	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.105	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
79.180.27.178	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.85.237	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.115.30.42	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.231	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.95	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
37.26.146.164	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.116	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.54.46.3	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.119	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.13.12.40	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.219.137.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.64.191.246	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.25.112	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.119	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.232	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.196	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.29	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
87.71.102.77	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.128.134	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	6
46.19.85.112	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.125	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.13	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.121.40.12	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.80	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.237	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
85.130.227.205	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
85.130.227.205	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
178.63.105.85	Germany	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	5
46.19.85.13	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
85.130.227.205	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
31.9.185.176	Syrian Arab Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5

03-07-2016-17:04:08 to 03-07-2016-18:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.209.150	Israel	147.237.76.39	mobile.meitav.idf.il	Cookie Tampering on cookie .ASPNETAUTH: Expected 0102556FCB1D9F46D308FE55E70CE9A146D308000933003100380037003500310037003600350000012F00FF, Observed 010215CF7B199F46D308FE1547BDE4A146D308000933003100380037003500310037003600350000012F00FF	None	14
65.208.151.117	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1008-he/+navmenu.qc+	Block	5
89.138.123.72	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
65.208.151.118	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1008-he/+navmenu.qc+	Block	3
2.54.161.121	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
65.208.151.119	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 65.208.151.119	Block	2
65.208.151.115	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1008-he/+navmenu.qc+	Block	2
66.249.69.63	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 66.249.69.63	Block	2
2.54.3.138	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
65.208.151.115	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
37.26.146.175	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
40.77.167.82	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/site- øªø§ø±ùšø® ø§ù„ ø¯ø®ùˆù„ 2-12-2004	Block	1
69.64.43.159	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to chinuch.aka.idf.il/old/wp-admin/	Block	1
2.54.42.3	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/gitus	Block	1
185.82.200.91		147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/	Block	1
65.208.151.114	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.108.186.33	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1
81.25.53.135	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1395-en/dover.aspx	Block	1
46.19.85.13	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	1
37.26.148.142	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.66.23	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1244-he/atal.aspx	Block	1
109.184.156.190	Russian Federation	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
65.208.151.112	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.108.186.33	Israel	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
46.19.85.0	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request request version	Block	1
69.147.248.190	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/592-6584-en/patzar.aspx',	Block	1
66.249.64.51	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/3251.pdf	Block	1
2.54.46.3	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
185.89.217.233		147.237.76.86	navy.idf.il	URL is Above Root Directory www.navy.idf.il/../images/shared/home.png	Block	1
84.108.186.33	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
81.25.53.135	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation lang in www.idf.il/1395-en/dover.aspx	Block	1
46.19.85.13	Israel	147.237.77.216	dover.idf.il	Malformed URL gzip,deflate	Block	1
37.46.38.125	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
65.208.151.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/clientscripts/{1}	Block	1
84.108.186.33	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1
81.25.53.135	Russian Federation	147.237.77.74	law.idf.il	Parameter Type Violation FileName in www.law.idf.il/templates/getfile/getfile.aspx	Block	1
46.19.85.0	Israel	147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	1
66.249.64.137	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
200.158.221.62	Brazil	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.108.186.33	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
82.81.40.156	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
46.19.85.13	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method : in URL gzip,deflate	Block	1
37.60.43.227	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ved in www.aka.idf.il/main/haredim/general.aspx	None	1
66.249.69.63	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/shared/usercontrols/headerupper/	Block	1
65.208.151.118	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
2.54.24.42	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
141.212.122.145	United States	147.237.76.39	mobile.meitav.idf.il	Untraceable SSL Sessions: Open Mode	None	1
65.208.151.113	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1008-he/+navmenu.qc+	Block	1
84.108.186.33	Israel	147.237.76.147	chinuch.aka.idf.il	PHP Attempt	Block	1
81.25.53.135	Russian Federation	147.237.77.74	law.idf.il	Parameter Type Violation InfoCenterItem in www.law.idf.il/templates/getfile/getfile.aspx	Block	1

03-07-2016-17:04:08 to 03-07-2016-18:04:08