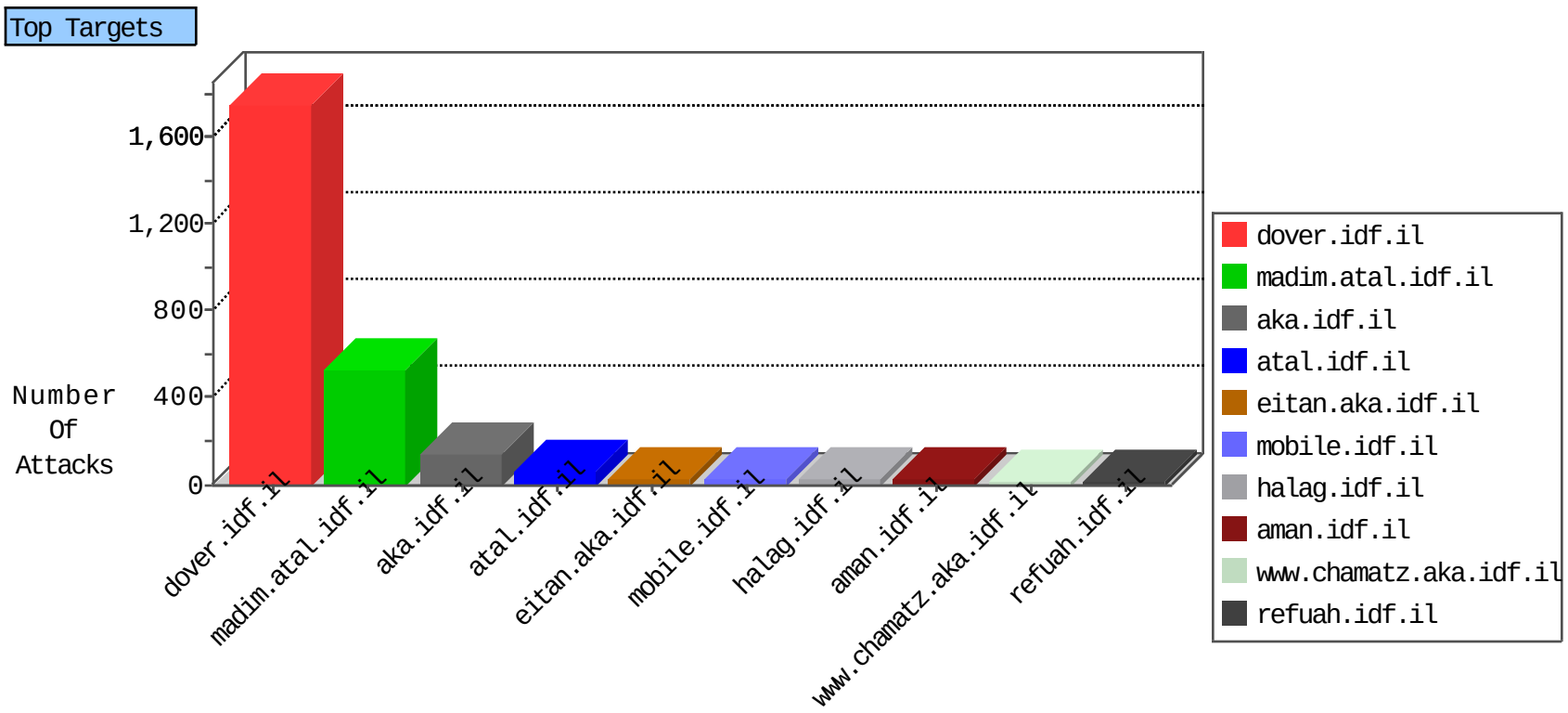
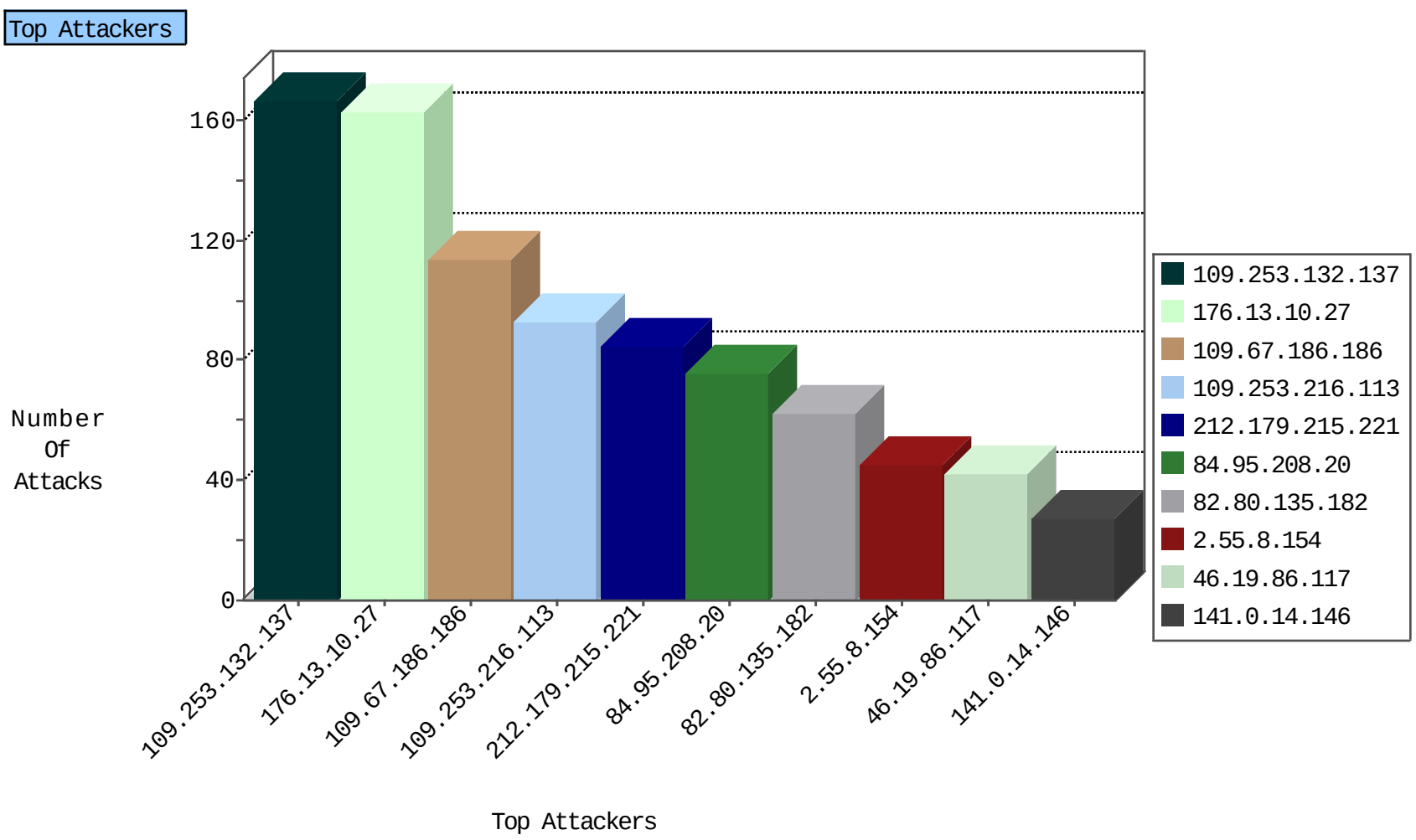
09-21-2016-11:04:02 to 09-21-2016-12:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-21-2016-11:04:02 to 09-21-2016-12:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.55.8.154	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	30
185.32.179.45	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	15
37.26.149.176	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	13
192.117.14.255	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
109.67.176.155	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
141.226.161.92	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
185.32.179.44	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
2.55.44.202	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
79.177.92.17	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
2.55.131.87	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
109.253.217.52	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
2.53.28.42	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
176.13.17.223	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
212.179.215.221	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	3
2.53.52.114	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
192.117.14.255	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
179.99.200.39	Brazil	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	2
2.53.190.222	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
5.102.242.178	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
94.188.158.74	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
37.142.11.242	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
37.26.146.227	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
2.53.155.46	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
185.94.111.1	Russian Federation	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1
45.32.205.133	Netherlands	147.237.76.86	navy.idf.il	Black List	drop	1
85.250.101.50	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
185.94.111.1	Russian Federation	147.237.76.196	e.sviva.idf.il	Black List	drop	1
46.121.132.200	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
37.26.146.169	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
109.67.35.72	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
45.32.201.228	Netherlands	147.237.76.176	test.ncore.idf.il	Black List	drop	1

09-21-2016-11:04:02 to 09-21-2016-12:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.120.188.146	China	147.237.77.74	law.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1
123.126.68.99	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

09-21-2016-11:04:02 to 09-21-2016-12:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
24.173.213.138	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
93.172.110.200	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
88.26.246.198	147.237.72.166	Spain	aka.idf.il	portscan: TCP Distributed Portscan	1
206.246.150.226	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
82.80.196.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
81.218.135.161	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
132.72.20.142	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.202.128	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
118.103.126.194	147.237.77.205	Japan	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.200.137	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
112.35.1.167	147.237.76.176	China	test.ncore.idf.i	ET SCAN Potential SSH Scan	1
46.183.223.228	147.237.76.31	Latvia	nakchal.idf.il	ET SCAN Potential SSH Scan	1
109.253.221.74	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.114.88	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.198.46	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.151.42.63	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.138.4.144	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
211.197.201.106	147.237.8.14	Korea, Republic of	e.orchot.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
82.81.49.185	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
206.246.150.226	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
81.218.138.222	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
79.178.233.105	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
125.212.247.129	147.237.76.198	Vietnam	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
72.241.62.254	147.237.76.38	United States	e.e.meitav.idf.i	ET SCAN NMAP -sS window 3072	1
112.35.1.167	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
57.66.185.4	147.237.77.216	Germany	dover.idf.il	portscan: TCP Distributed Portscan	1
112.35.1.167	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.70	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.201.220	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-21-2016-11:04:02 to 09-21-2016-12:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
82.80.135.182	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	61
141.0.14.146	Europe	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	27
194.90.66.9	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
212.179.215.221	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
109.253.216.113	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
212.179.215.221	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
82.80.190.84	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
212.179.215.221	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	19
109.253.216.113	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	18
212.179.215.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
46.19.86.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
109.253.216.113	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
62.0.224.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
176.123.58.10	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
109.253.216.113	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	11
100.92.136.11		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
109.253.216.113	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
79.178.210.5	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
5.22.134.89	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.34	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
2.53.186.229	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.213	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
109.67.123.82	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
62.0.224.1	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	8
2.55.8.154	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
2.53.186.165	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
37.26.147.207	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
109.253.213.77	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
212.150.128.10	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
37.26.147.207	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
46.19.85.27	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
109.253.216.113	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
2.55.173.188	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.53.36.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.55.8.154	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
193.242.218.25	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.140	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.102	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
156.205.235.64	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.126	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.55.47.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.53.165.152	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.55.36.41	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.100	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.179	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
95.35.35.22	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.53.130.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6

09-21-2016-11:04:02 to 09-21-2016-12:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.132.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	167
176.13.10.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	163
109.67.186.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	111
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	32
46.19.86.117	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
109.253.199.13	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
46.19.85.51	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
213.57.243.74	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	11
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	7
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	7
77.138.210.91	France	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	6
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	6
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	5
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	5
2.53.5.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.50.31	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.147.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.228.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.145.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
82.80.196.44	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	2
46.19.86.124	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	2
196.6.235.1		147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/contactus.aspx	Block	2
87.255.31.189	Russian Federation	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	2
46.19.85.114	Israel	147.237.0.34	tikshuv.idf.il	Distributed Unknown HTTP Request Method	Block	2
196.6.235.1		147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/kapatz/	Block	2
2.55.51.181	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
169.229.3.91	United States	147.237.77.233	atal.idf.il	NULL Character in Method	Block	1
79.182.2.134	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/resources/images/favicon/favicon.png	Block	1
169.229.3.91	United States	147.237.0.15	kosher-kravi.idf.il	Abnormally Long Request method	Block	1
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	1
169.229.3.91	United States	147.237.72.167	ishurim.aka.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
80.246.130.216	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.66.100	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
46.19.85.114	Israel	147.237.0.34	tikshuv.idf.il	Multiple Malformed URL from 46.19.85.114	Block	1
31.168.3.188	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
82.81.22.202	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation aspxerrorpath in www.idf.il/error.htm	Block	1
80.178.204.62	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
169.229.3.91	United States	147.237.0.15	kosher-kravi.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/templates/homepage/piwik.php	Block	1
46.19.86.191	Israel	147.237.76.42	refuah.idf.il	Distributed Parameter Type Violation on www.refua.atal.idf.il/1518-he/refuah.aspx parameter ctl00$ContentPlaceHolder1$txtContent	Block	1
46.19.85.114	Israel	147.237.0.34	tikshuv.idf.il	Distributed Abnormally Long Request	Block	1
169.229.3.91	United States	147.237.72.167	ishurim.aka.idf.il	Unknown HTTP Request Method Éó•Qe–[[#8]]ùÌ«!û6[[#12]]j®“À[[#23]]’Kó@™÷¾§•2òQìç+£’7nQ^åq[[#25]]ÈRÔãg„[[#11]]’[[#6]]ëË[[#12]] in URL	Block	1
80.246.130.242	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
77.138.124.87	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	1
46.19.86.61	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	1
84.94.73.174	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$cb13900030 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
31.168.23.60	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 31.168.23.60	Block	1
176.13.10.169	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtContent in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1
80.230.228.18	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1

09-21-2016-11:04:02 to 09-21-2016-12:04:02