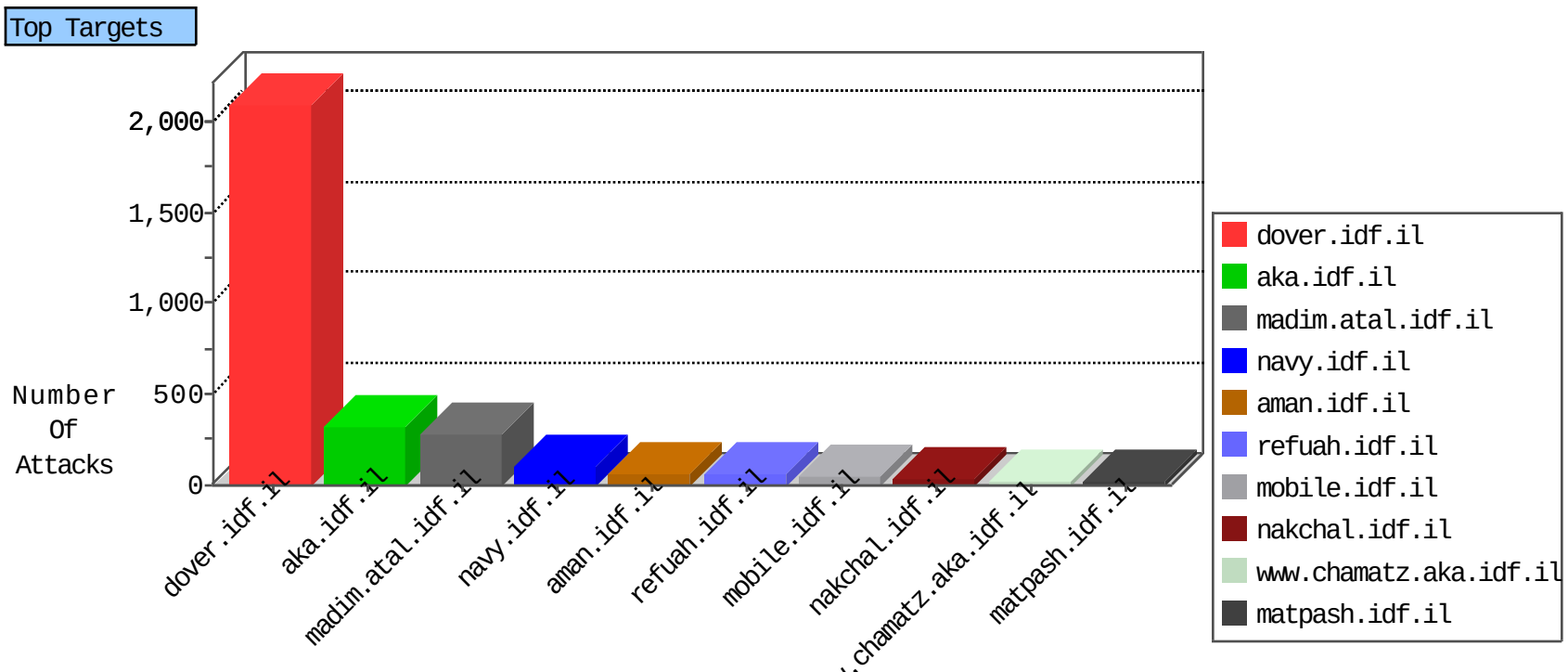
09-20-2016-11:04:03 to 09-20-2016-12:04:03

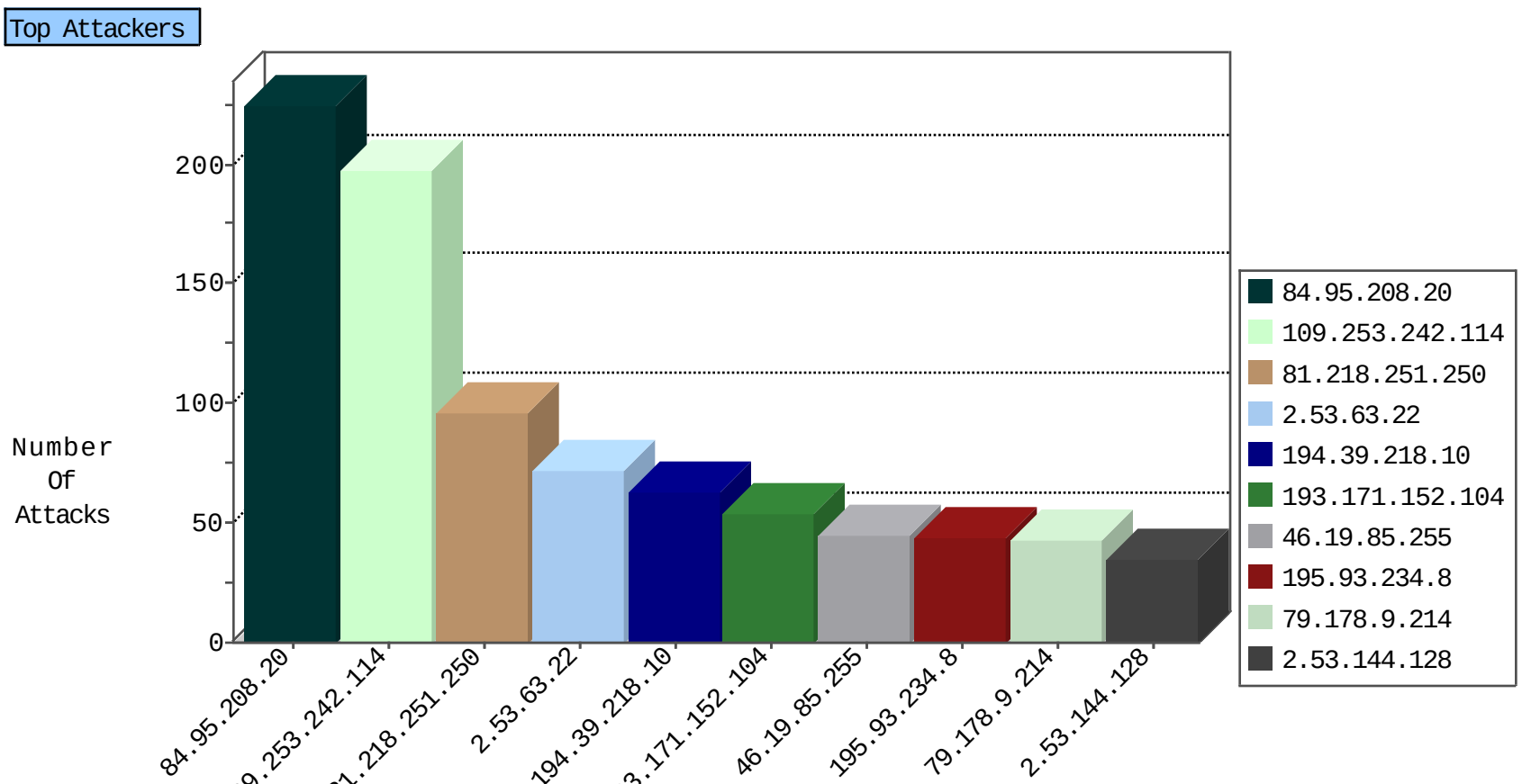
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

09-20-2016-11:04:03 to 09-20-2016-12:04:03

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	SYN Flood out of context	drop	71
46.19.86.116	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	65
0.0.0.0		147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	32
2.53.35.87	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	12
195.93.234.9	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
89.138.199.105	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
46.19.86.36	Israel	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	7
2.55.131.7	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
79.178.9.214	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
176.13.13.173	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
2.53.178.222	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
109.226.44.112	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
2.55.55.245	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
46.117.77.90	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
109.65.72.57	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
80.246.136.60	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
185.32.179.120	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
77.138.52.97	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
141.226.217.252	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
82.166.239.138	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
185.3.147.244	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
31.168.11.194	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	2
132.74.74.170	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
45.32.201.228	Netherlands	147.237.76.30	himush.idf.il	Black List	drop	1
176.13.234.212	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
109.253.194.186	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
149.202.89.123	France	147.237.76.38	e.e.meitav.idf.il	Black List	drop	1
46.19.85.78	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
109.253.213.84	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
80.246.133.120	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
46.19.86.147	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
204.42.253.130	United States	147.237.76.201	e.atal.idf.il	Black List	drop	1
52.53.222.9	United States	147.237.76.177	ncore.idf.il	Black List	drop	1
46.19.85.79	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
46.19.86.172	Israel	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	1
45.32.196.8	United States	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1
212.179.90.106	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
176.13.231.185	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
193.106.54.21	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

09-20-2016-11:04:03 to 09-20-2016-12:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-20-2016-11:04:03 to 09-20-2016-12:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
89.139.198.51	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.132	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.94.159.34	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.82.69.134	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
62.90.107.145	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.235.62.27	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.213	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
202.65.138.2	147.237.72.167	India	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.23	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.224.18	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.14	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
124.106.31.107	147.237.77.216	Philippines	dover.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.19.85.60	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
114.35.149.124	147.237.8.28	Taiwan	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
37.46.38.171	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.229.36.11	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.10.20	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.82.69.134	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
66.249.66.242	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
58.218.200.137	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
211.149.219.167	147.237.72.166	China	aka.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.163	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.70.44.28	147.237.76.200	Hungary	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.15	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.8.222	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.68	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
118.8.27.72	147.237.72.156	Japan	aman.idf.il	ET SCAN NMAP -sA (2)	1
37.142.2.65	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

09-20-2016-11:04:03 to 09-20-2016-12:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
194.39.218.10	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	63
2.53.63.22	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
193.171.152.104	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
195.93.234.8	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
62.0.208.254	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	32
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
192.114.91.230	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
79.178.9.214	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
37.26.146.243	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
31.154.34.246	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
46.19.85.161	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
46.19.85.254	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
126.245.22.156	Japan	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
176.65.22.27	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
46.19.85.254	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	15
77.124.59.189	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
207.241.229.68	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	12
176.13.16.36	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.64	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
109.253.194.186	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
62.0.237.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.86.46	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
109.253.159.19	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
176.13.13.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
84.95.208.20	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
212.199.226.66	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
46.19.86.147	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
80.178.184.37	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
62.16.65.149	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.253	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
5.22.134.211	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.74	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.132	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
46.19.86.188	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
185.89.217.229	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.132	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
85.64.52.168	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
62.0.197.85	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.168	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
66.249.93.87	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
37.26.146.186	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.236	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.121.196.63	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
185.89.217.228	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
82.80.88.153	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
89.138.178.195	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7

09-20-2016-11:04:03 to 09-20-2016-12:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.242.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	190
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	129
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	50
81.218.251.250	Israel	147.237.76.86	navy.idf.il	Unauthorized HTTP Method	Block	48
46.19.85.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	45
81.218.251.250	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/style/shared/	Block	32
2.53.144.128	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	32
46.19.85.82	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	18
81.218.251.250	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 81.218.251.250	Block	16
2.53.56.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	15
46.19.86.249	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	5
62.219.198.6	Israel	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized HTTP Method	Block	4
212.179.64.162	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	4
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	4
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed PHP Attempt	Block	3
176.13.244.71	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.1.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.244.123	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.146.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.21.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
87.70.55.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.169	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
82.166.145.160	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 82.166.145.160	Block	2
62.219.198.6	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/sip_storage/files/0/	Block	2
46.19.85.149	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
2.53.158.38	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	2
62.0.1.30	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	2
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	2
77.127.34.176	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	2
62.0.101.97	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/trigger.png	Block	1
37.26.148.178	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.179.255.94	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
207.46.13.31	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/1/24	Block	1
176.13.226.181	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-9367-he/dover.aspx	Block	1
66.249.64.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
2.55.149.43	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized Method HEAD for www.chinuch.aka.idf.il/1137-he/chinuch.aspx	None	1
217.69.133.242	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/igf	Block	1
185.32.179.119	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.180.109.144	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
109.65.142.78	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
46.19.85.13	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
80.246.137.183	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.53.61.13	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
207.46.13.165	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
176.13.238.146	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1

09-20-2016-11:04:03 to 09-20-2016-12:04:03