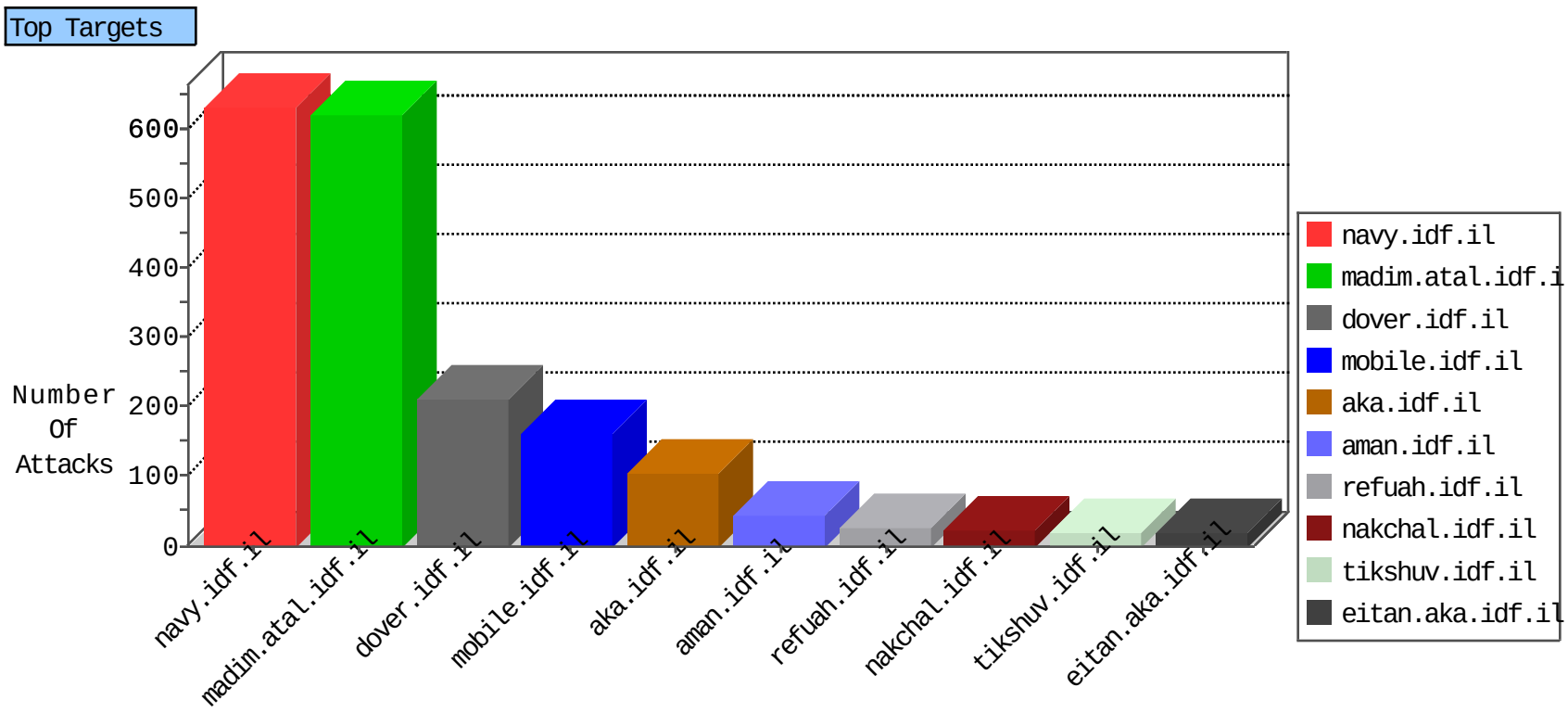
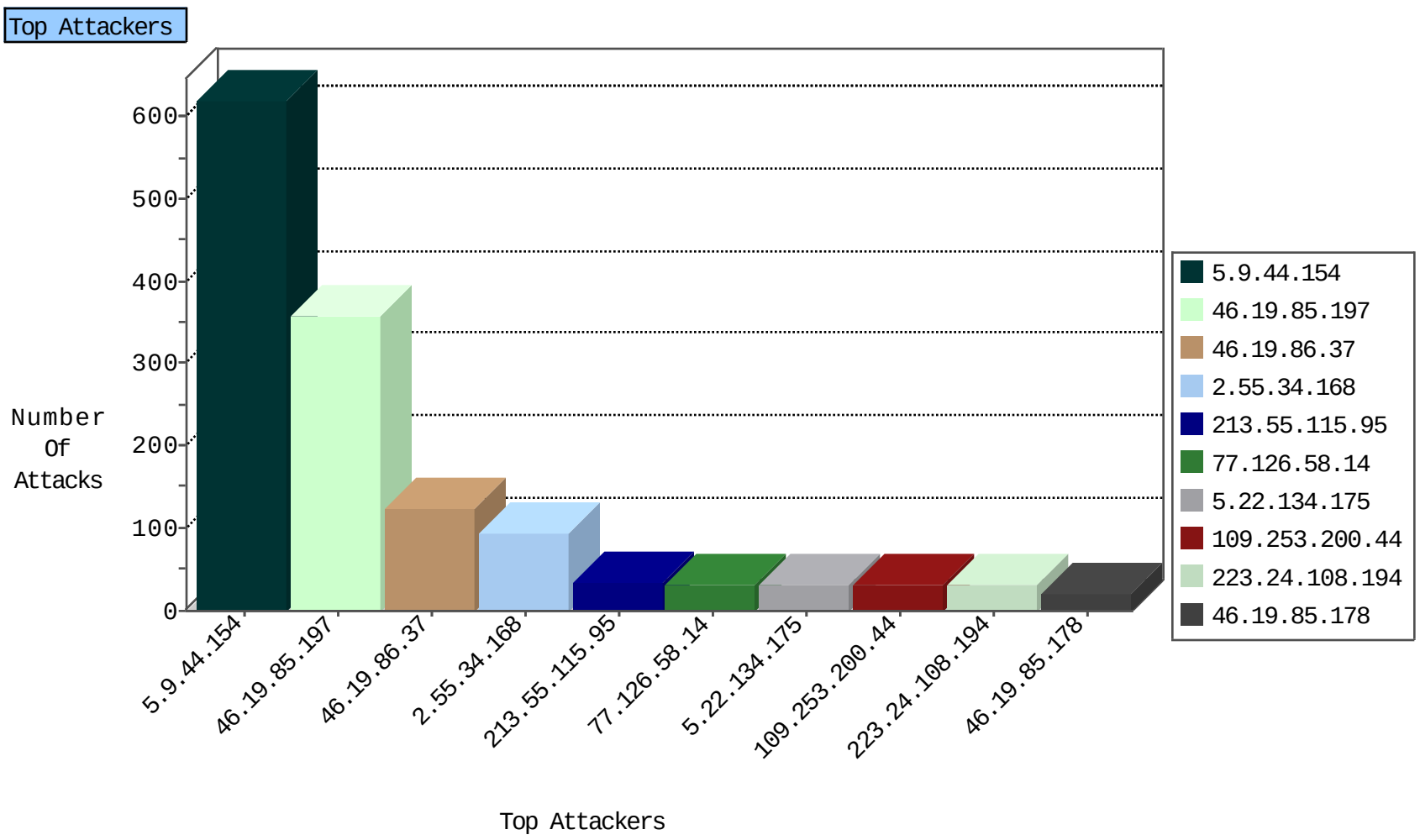
09-22-2016-18:04:05 to 09-22-2016-19:04:05

IDF Under Attack
Daily Report





09-22-2016-18:04:05 to 09-22-2016-19:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.80.52.119	Israel	147.237.72.166	aka.idf.il	Black List	drop	2
167.114.210.17	Canada	147.237.76.177	ncore.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
167.114.210.17	Canada	147.237.76.201	e.atal.idf.il	JLM_Purple_Con_Limit_Http	drop	1
185.94.111.1	Russian Federation	147.237.76.34	yohalan.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.42	refuah.idf.il	Black List	drop	1

09-22-2016-18:04:05 to 09-22-2016-19:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
198.20.69.74	United States	147.237.76.39	mobile.meitav.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

09-22-2016-18:04:05 to 09-22-2016-19:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
218.87.109.253	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.35	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.98	147.237.76.177	United States	ncore.idf.il	ET DROP Dshield Block Listed Source	1
218.87.109.253	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
195.70.44.28	147.237.77.74	Hungary	law.idf.il	ET SCAN NMAP -sS window 1024	1
218.87.109.253	147.237.77.74	China	law.idf.il	ET SCAN Potential SSH Scan	1
163.172.129.15	147.237.77.227	United Kingdom	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
218.87.109.253	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
128.127.0.45	147.237.72.217	Italy	e.idf.il	ET SCAN NMAP -sS window 3072	1
218.87.109.253	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
117.21.248.87	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
117.21.248.87	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
117.21.248.87	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
46.183.223.228	147.237.8.50	Latvia	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
198.199.89.155	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
14.41.15.12	147.237.77.226	Korea, Republic of	www.chamatz.aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
218.87.109.253	147.237.77.243	China	mobile.idf.il	ET SCAN Potential SSH Scan	1
195.70.44.28	147.237.77.179	Hungary	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
218.87.109.253	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	1
163.172.169.150	147.237.77.227	United Kingdom	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
218.87.109.253	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
139.162.187.89	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 1024	1
218.87.109.253	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
128.127.0.45	147.237.72.217	Italy	e.idf.il	ET SCAN NMAP -sS window 1024	1
218.87.109.253	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
117.21.248.87	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
117.21.248.87	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
91.242.217.191	147.237.77.216	United Arab Emirates	dover.idf.il	ET WEB_SERVER PyCurl Suspicious User Agent Inbound	1

09-22-2016-18:04:05 to 09-22-2016-19:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.9.44.154	Germany	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	620
213.55.115.95	Ethiopia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
77.126.58.14	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
223.24.108.194	Thailand	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
109.253.200.44	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
46.19.85.178	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
37.26.149.191	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
2.53.17.186	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
79.179.97.60	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.60	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.60	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
109.253.213.128	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.117	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.86.37	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.0.230.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.112	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.126.66.37	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
77.124.42.97	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.58.33	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.231.56	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.8.49	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
89.139.117.173	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.86.137	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
66.102.9.149	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
46.19.86.86	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.86.137	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.86	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
79.179.28.97	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
46.19.86.183	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
176.13.226.91	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
141.0.12.30	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
2.53.188.81	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.33	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
176.13.231.132	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
185.3.147.217	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.120.124.171	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.26.147.182	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.146.145	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.86.62	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
37.26.146.145	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
2.55.21.81	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
37.26.147.250	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
79.181.172.70	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
176.13.241.217	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.26.146.145	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.53.188.81	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	3

09-22-2016-18:04:05 to 09-22-2016-19:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.197	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	359
46.19.86.37	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	117
2.55.34.168	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	94
5.22.134.175	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	30
119.128.121.252	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 119.128.121.252	Block	12
212.199.57.195	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
113.109.27.69	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 113.109.27.69	Block	4
113.109.25.47	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 113.109.25.47	Block	4
46.19.85.201	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	4
113.109.26.108	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 113.109.26.108	Block	4
119.128.121.252	China	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	4
46.19.86.248	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
113.109.24.217	China	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
113.109.24.217	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 113.109.24.217	Block	3
46.19.85.117	Israel	147.237.76.31	nakchal.idf.il	Multiple Abnormally Long Request from 46.19.85.117	Block	2
185.32.179.84	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.19.85.117	Israel	147.237.76.31	nakchal.idf.il	Multiple Illegal HTTP Version from 46.19.85.117	Block	2
2.55.47.220	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
113.109.26.108	China	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
77.138.210.129	France	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.85.117	Israel	147.237.76.31	nakchal.idf.il	Multiple Malformed URL from 46.19.85.117	Block	2
46.19.85.117	Israel	147.237.76.31	nakchal.idf.il	Multiple Unknown HTTP Request Method from 46.19.85.117	Block	2
5.29.148.123	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
89.237.117.101	France	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	2
176.13.11.139	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
113.109.25.242	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 113.109.25.242	Block	2
84.109.241.213	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/matash	Block	1
5.29.181.69	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/	Block	1
157.55.39.1	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
66.249.76.115	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1153-22231-he/dover.aspx	Block	1
113.109.27.69	China	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
113.109.24.217	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/default.php	Block	1
213.57.243.74	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
93.158.152.34	Russian Federation	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
185.32.179.45	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
79.179.28.97	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
113.109.25.242	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/main.aspx	Block	1
66.102.9.6	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
194.187.170.107	France	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il./robots.txt	Block	1
113.65.21.108	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 113.65.21.108	Block	1
84.111.172.88	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
5.29.181.69	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/עסוד	Block	1
157.55.39.43	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/sitemap/sitemap.aspx	Block	1
74.82.4.76	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.86.46	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
95.86.126.37	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
119.128.121.252	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.asp	Block	1
79.179.28.97	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
66.102.9.8	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/pniotanswer.aspx	Block	1
200.49.168.250	Guatemala	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	Block	1

09-22-2016-18:04:05 to 09-22-2016-19:04:05