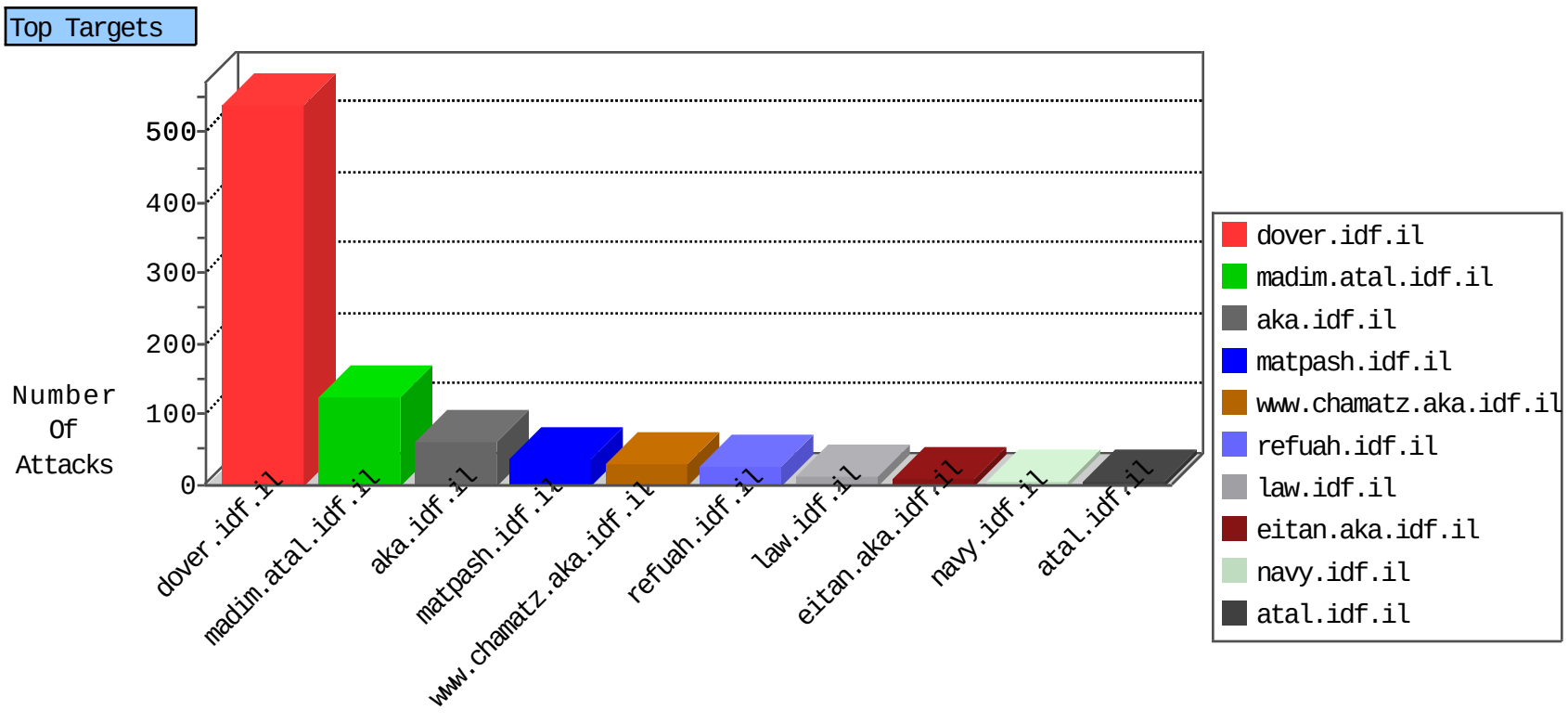
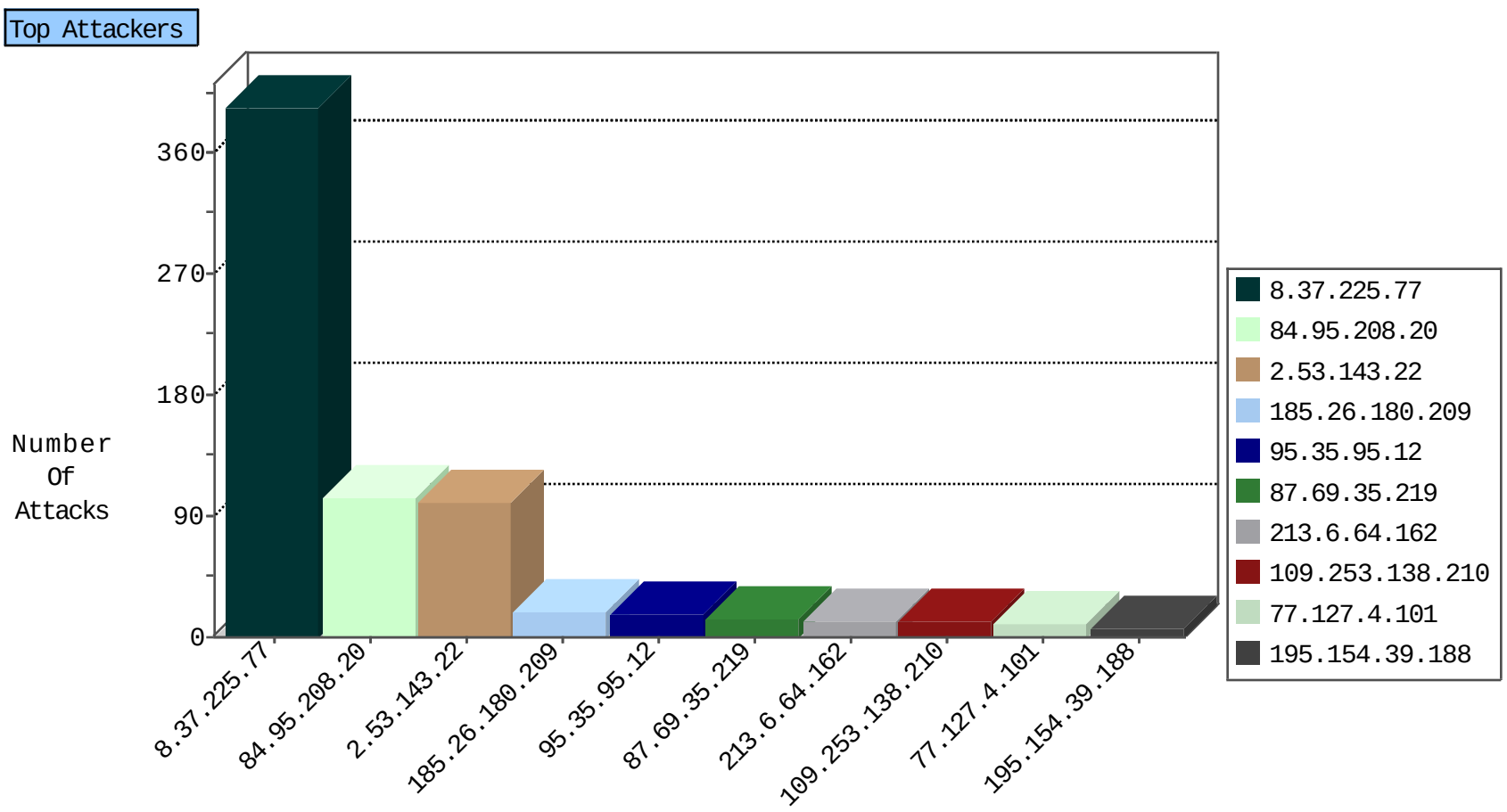
10-04-2016-10:04:02 to 10-04-2016-11:04:02

IDF Under Attack Daily Report





10-04-2016-10:04:02 to 10-04-2016-11:04:02

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	HTTP Page Flood Attack	forward	4
142.54.174.83	United States	147.237.76.30	himush.idf.il	block-sp-traf1	forward	2
69.30.193.254	United States	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	2
173.208.213.196	United States	147.237.76.86	navy.idf.il	block-sp-traf1	forward	2
69.30.193.252	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	2
204.12.217.4	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	2
69.30.193.253	United States	147.237.76.31	nakchal.idf.il	block-sp-traf1	forward	2
63.141.231.196	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	2
192.187.101.237	United States	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	forward	1
63.141.231.198	United States	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	1
198.204.255.76	United States	147.237.77.170	maarachot.idf.il	block-sp-traf1	forward	1
141.226.162.151	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
8.37.225.77	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	1
192.187.109.59	United States	147.237.77.176	matpash.idf.il	block-sp-traf1	forward	1
173.208.198.10	United States	147.237.77.74	law.idf.il	block-sp-traf1	forward	1
71.6.216.42	United States	147.237.76.199	e.nakchal.idf.il	Black List	drop	1
63.141.231.214	United States	147.237.77.233	atal.idf.il	block-sp-traf1	forward	1
173.231.185.150	United States	147.237.0.16	my-kosher-kravi.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
142.54.174.82	United States	147.237.72.156	aman.idf.il	block-sp-traf1	forward	1
8.37.225.77	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
192.187.118.21	United States	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	forward	1
173.208.198.13	United States	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	1
71.6.216.47	United States	147.237.76.176	test.ncore.idf.il	Black List	drop	1
66.240.219.146	United States	147.237.76.38	e.e.meitav.idf.il	Black List	drop	1
183.60.48.25	China	147.237.76.196	e.sviva.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
142.54.174.82	United States	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	forward	1
69.30.193.253	United States	147.237.77.235	sviva.idf.il	block-sp-traf1	forward	1
192.187.118.69	United States	147.237.77.216	dover.idf.il	block-sp-traf1	forward	1
173.208.213.194	United States	147.237.72.166	aka.idf.il	block-sp-traf1	forward	1
94.102.49.193	Netherlands	147.237.76.34	yohalan.idf.il	Black List	drop	1
69.30.193.252	United States	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	1

10-04-2016-10:04:02 to 10-04-2016-11:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.210.250.212	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	3
108.59.8.70	United States	147.237.77.233	atal.idf.il	C1000074: HTTP: majestic bot	Permit	2
62.210.250.212	France	147.237.76.42	refuah.idf.il	C1000074: HTTP: majestic bot	Permit	2
69.30.198.242	United States	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	2
54.187.255.228	United States	147.237.77.176	matpash.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1
69.30.198.242	United States	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	1

10-04-2016-10:04:02 to 10-04-2016-11:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
128.199.176.113	147.237.0.16	Singapore	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
58.220.2.5	147.237.77.227	China	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
212.120.180.188	147.237.76.202	Russian Federation	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.200.137	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
208.100.26.228	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.146.223	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.154.39.188	147.237.76.42	France	refuah.idf.il	ET SCAN Potential SSH Scan	1
195.154.39.188	147.237.72.217	France	e.idf.il	ET SCAN Potential SSH Scan	1
195.154.39.188	147.237.8.14	France	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
195.154.39.188	147.237.0.19	France	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
128.199.176.113	147.237.76.148	Singapore	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
128.127.0.45	147.237.77.74	Italy	law.idf.il	ET SCAN NMAP -sS window 3072	1
58.218.200.137	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
212.120.180.188	147.237.76.201	Russian Federation	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
54.147.8.50	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
202.65.138.2	147.237.76.30	India	himush.idf.il	ET SCAN NMAP -sS window 1024	1
27.64.25.231	147.237.76.196	Vietnam	e.sviva.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
195.154.39.188	147.237.76.39	France	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
195.154.39.188	147.237.8.24	France	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
195.154.39.188	147.237.0.34	France	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
183.63.152.98	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

10-04-2016-10:04:02 to 10-04-2016-11:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
8.37.225.77	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	343
8.37.225.77	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	49
185.26.180.209	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	18
213.6.64.162	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	12
77.127.4.101	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
109.253.138.210	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
87.69.35.219	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.218	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
87.69.35.219	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
157.55.39.92	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.138.210	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
141.226.162.151	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
79.177.28.63	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
213.6.135.50	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
78.181.92.11	Turkey	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
85.250.80.160	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.51	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.95.251.156	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
110.138.238.63	Indonesia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.19.86.51	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
79.178.235.131	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.148.202	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
5.43.195.145	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
66.249.64.105	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
109.64.90.31	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
46.19.85.124	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
141.226.162.13	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
87.69.35.219	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
66.249.64.105	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
79.180.226.47	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
176.13.1.45	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
79.176.63.248	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
141.226.162.13	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
74.82.47.45	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.37	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.120.122.219	Israel	147.237.77.74	law.idf.il	Command Injection	command injection detected in URL: 'label'	monitor	1
184.105.139.87	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.93	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.33	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.19.86.215	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
5.22.134.110	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.58	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.86	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.121.159.209	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
184.105.247.246	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
5.102.242.59	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
79.177.28.63	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
141.212.122.94	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
66.249.64.105	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1

10-04-2016-10:04:02 to 10-04-2016-11:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.143.22	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	100
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	78
95.35.95.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	16
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	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	5
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	5
37.26.148.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.177.161.75	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.64.32.204	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	3
85.132.77.12	Azerbaijan	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	2
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
85.132.77.12	Azerbaijan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/images/	Block	2
188.120.154.90	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	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
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
66.249.66.180	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-18124-he/	Block	1
213.57.236.94	Israel	147.237.72.166	aka.idf.il	Unauthorized Request Content Type text/ping	Block	1
77.138.193.58	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/drushim/general.aspx	Block	1
46.116.57.58	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
123.125.71.114	China	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	PHP Attempt	Block	1
66.249.69.67	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/3/1903.doc	Block	1
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
77.139.223.105	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	Block	1
46.120.122.219	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/726-en/patzar.aspx200oktext/html34445 idf law review 3200:00.359utf-8	Block	1
141.8.183.16	Russian Federation	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1039-he/idfg.asp	Block	1
84.108.88.175	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
66.249.69.72	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9740-he/refuah.aspx	Block	1
46.19.86.87	Israel	147.237.76.86	navy.idf.il	Abnormally Long Request method	Block	1
54.187.255.228	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	1
157.55.39.145	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
85.64.136.102	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
66.249.69.127	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/1902.doc	Block	1
46.19.86.87	Israel	147.237.76.86	navy.idf.il	Malformed URL	Block	1
79.180.226.47	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.64.43	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
85.64.145.193	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.53.48.253	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
77.124.243.146	Israel	147.237.72.167	ishurim.aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
109.64.90.31	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
46.19.86.87	Israel	147.237.76.86	navy.idf.il	Unknown HTTP Request Method xmlfjkojms0r0b0ygiprc in URL	Block	1

10-04-2016-10:04:02 to 10-04-2016-11:04:02