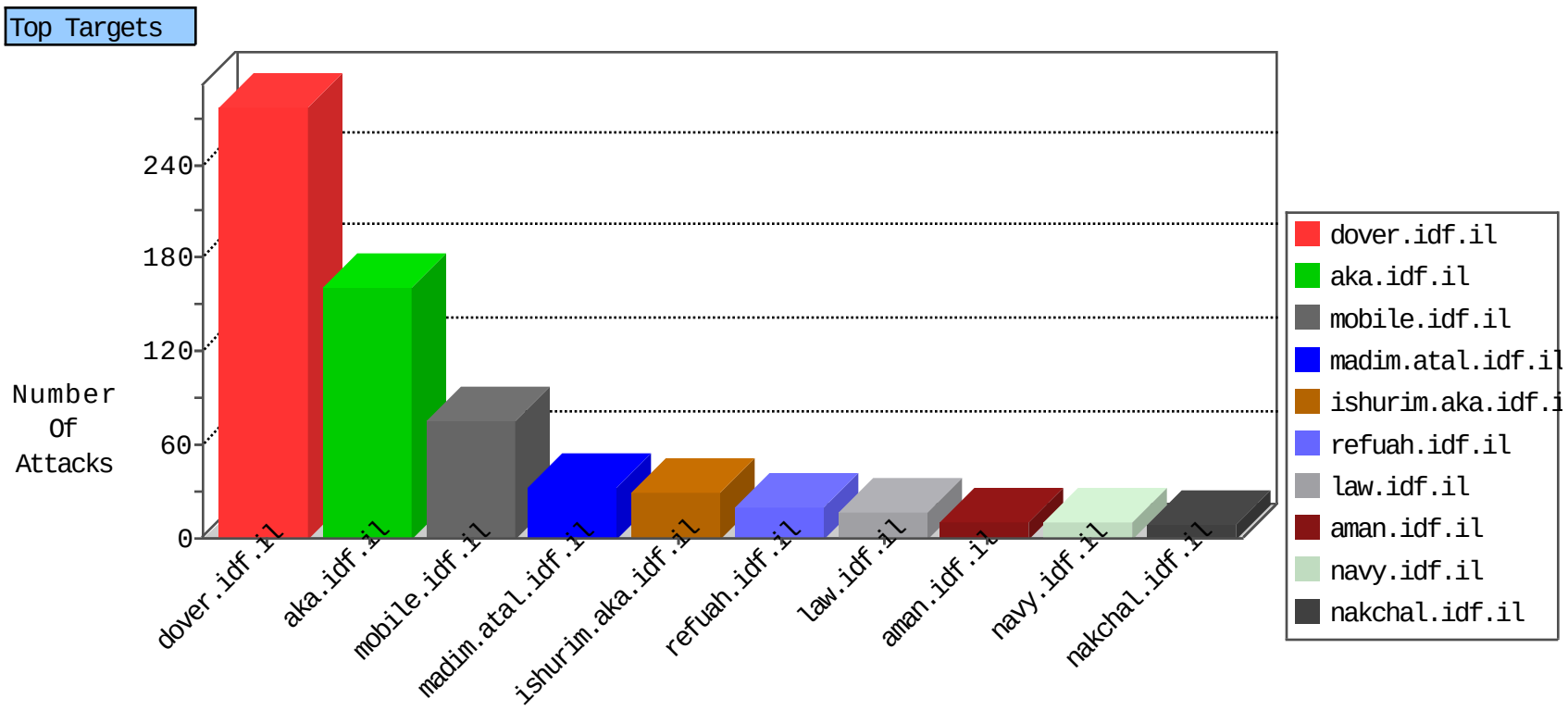
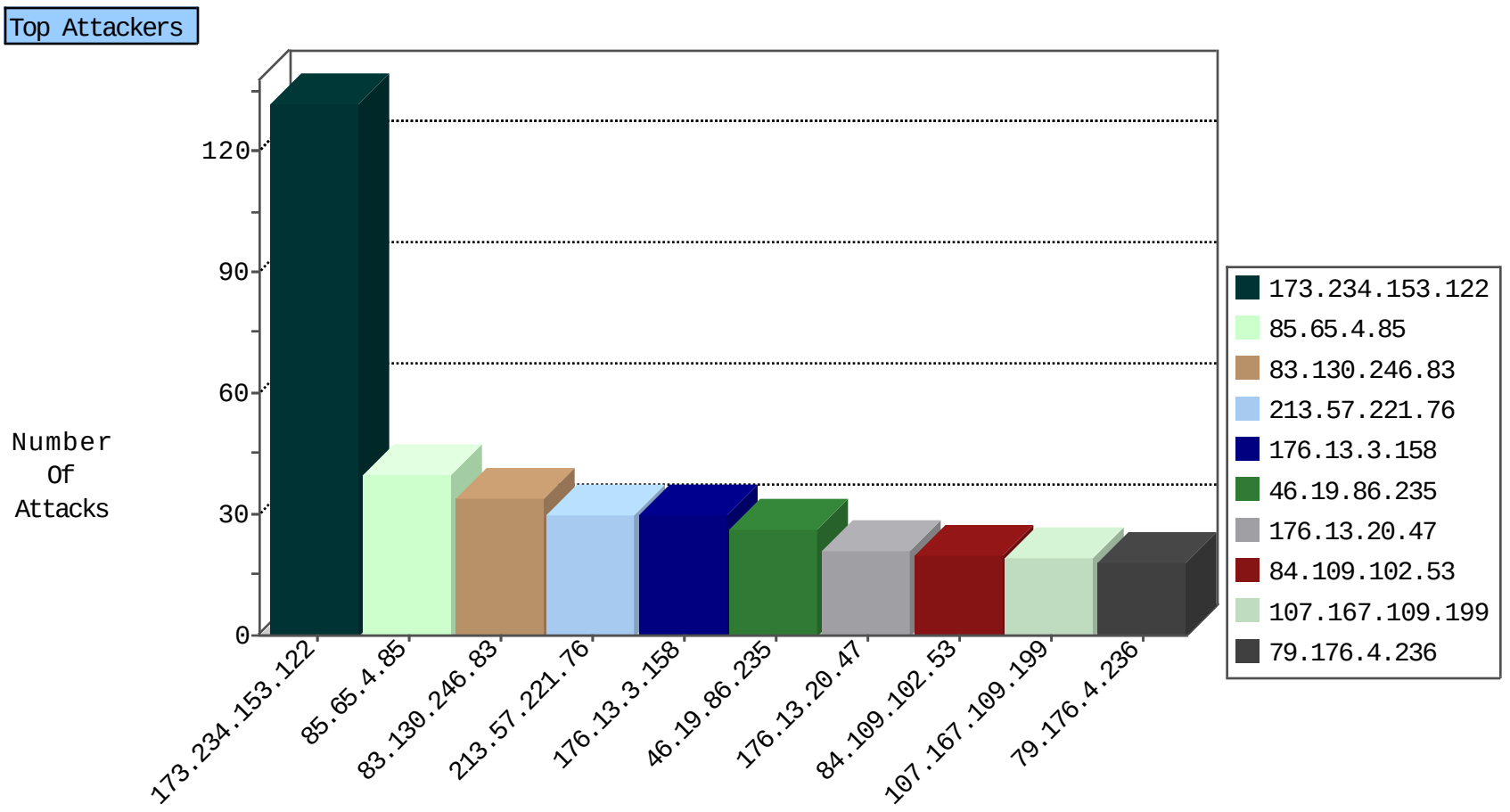
10-04-2016-18:04:01 to 10-04-2016-19:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-04-2016-18:04:01 to 10-04-2016-19:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
85.250.214.228	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
46.19.86.166	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
93.174.93.210	Netherlands	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	forward	2
93.174.93.210	Netherlands	147.237.76.86	navy.idf.il	block-sp-traf1	forward	2
93.172.104.68	Israel	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.31	nakchal.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.201	e.atal.idf.il	Black List	drop	1
77.124.7.15	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
183.60.48.25	China	147.237.0.200	m4u.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1

10-04-2016-18:04:01 to 10-04-2016-19:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
173.234.153.122	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	125
173.234.153.122	United States	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	4
173.234.153.122	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
62.210.250.212	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
198.245.49.215	Canada	147.237.76.42	refuah.idf.il	C1000074: HTTP: majestic bot	Permit	2
91.209.51.22	Ukraine	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
198.245.49.215	Canada	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

10-04-2016-18:04:01 to 10-04-2016-19:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
180.250.191.154	147.237.77.176	Indonesia	matpash.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.201.236.50	147.237.72.14	Ukraine	dover.idf.il(old)	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.199.41.16	147.237.72.166	Netherlands	aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
58.218.200.137	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
109.236.86.32	147.237.77.243	Netherlands	mobile.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
58.218.200.137	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
109.236.86.32	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
54.147.7.228	147.237.76.201	United States	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
220.233.79.180	147.237.77.179	Australia	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
109.236.86.32	147.237.72.217	Netherlands	e.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
208.100.26.228	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 1024	1
23.91.75.231	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
109.236.86.32	147.237.72.156	Netherlands	aman.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
195.154.53.146	147.237.76.31	France	nakchal.idf.il	ET SCAN Potential SSH Scan	1
23.91.75.231	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
195.154.53.146	147.237.0.35	France	akaws.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.50	147.237.72.14	Ukraine	dover.idf.il(old)	ET SCAN NMAP -sS window 4096	1
183.129.160.229	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.50	147.237.72.14	Ukraine	dover.idf.il(old)	ET SCAN NMAP -f -sS	1
163.172.129.15	147.237.76.198	United Kingdom	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.200.137	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
113.23.54.240	147.237.77.176	Vietnam	matpash.idf.il	ET SCAN NMAP -sS window 3072	1
58.218.200.137	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
109.236.86.32	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
58.218.200.137	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
109.236.86.32	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
217.23.6.58	147.237.72.217	Netherlands	e.idf.il	ET SCAN NMAP -sS window 1024	1
40.114.15.49	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 1024	1
109.236.86.32	147.237.72.167	Netherlands	ishurim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
195.154.53.146	147.237.77.170	France	maarachot.idf.il	ET SCAN Potential SSH Scan	1
23.91.75.231	147.237.76.86	United States	navy.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
104.128.144.131	147.237.77.19	Canada	law-forum.idf.il	ET SCAN NMAP -sS window 3072	1
195.154.53.146	147.237.72.166	France	aka.idf.il	ET SCAN Potential SSH Scan	1
5.255.90.133	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
93.174.93.210	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
195.154.53.146	147.237.0.15	France	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.50	147.237.72.14	Ukraine	dover.idf.il(old)	ET SCAN NMAP -sS window 2048	1

10-04-2016-18:04:01 to 10-04-2016-19:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
85.65.4.85	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	40
83.130.246.83	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	34
107.167.109.199	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	19
46.19.86.235	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
176.13.3.158	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
79.176.4.236	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	10
213.57.221.76	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	10
176.13.3.158	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
176.13.3.158	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.86.235	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.19.86.28	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
79.176.4.236	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
77.126.58.14	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.133.65	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.116.65.231	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.57.221.76	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
31.210.186.54	Israel	147.237.0.15	kosher-kravi.idf.i	drop	First packet isn't SYN	drop	5
217.132.33.43	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
213.57.221.76	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
193.239.221.230	Switzerland	147.237.77.74	law.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
213.57.221.76	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
109.67.52.204	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
213.57.221.76	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.253.196.65	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
85.65.203.32	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
199.30.25.125	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
131.253.27.172	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
91.202.128.7	Ukraine	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.108.96.164	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
93.174.93.210	Netherlands	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
79.177.33.178	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
141.226.218.17	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.108.96.164	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.143	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.65.145	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
91.202.128.7	Ukraine	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
109.253.196.65	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
93.174.93.210	Netherlands	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
177.74.154.97	Brazil	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
192.115.83.5	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
176.13.15.45	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
5.22.134.203	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
85.64.45.73	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.26.148.134	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
104.197.229.243	United States	147.237.77.216	dover.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
109.253.212.61	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
37.26.148.195	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
77.138.141.202	France	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
5.22.134.168	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.20.47	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
84.109.102.53	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 84.109.102.53	Block	19
77.125.65.145	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	11
5.22.134.165	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	4
79.178.82.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
46.19.86.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.153.108	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.120.125.131	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
67.245.1.115	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-he/	Block	1
66.249.64.118	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/apple-app-site-association	Block	1
173.234.153.122	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-17275-he/חיל האוויר קף שלוש מטרות טרור ברצועה בתגובה לירי הרקטות.aspx	Block	1
37.142.9.207	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
80.246.136.91	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.76.79	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/6/71566.pdf	Block	1
66.249.64.33	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8974-he/refuah.aspx	Block	1
94.230.86.149	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/894-he/dover.aspx	Block	1
68.224.169.101	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/pniotanswer.aspx	Block	1
66.249.66.23	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
66.249.76.80	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/5/71575.pdf	Block	1
94.230.86.149	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
5.22.134.165	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 5.22.134.165	Block	1
66.249.66.26	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
46.116.65.231	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
84.109.102.53	Israel	147.237.72.166	aka.idf.il	Unknown HTTP Request Method undefined in URL www.aka.idf.il/main/giyus/api/api/professiondescription/5797	Block	1
66.249.76.81	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/6/70476.pdf	Block	1
66.249.64.43	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/1/71761.pdf	Block	1
94.230.86.149	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl55 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
5.22.134.165	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/sip_storage/files/2/	Block	1
77.138.141.202	France	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/favicon.ico	Block	1
66.249.66.210	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-17802-he/dover.aspx	Block	1
66.102.8.158	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1008-he/+navmenu.qc+	Block	1
204.79.180.112	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/templates/home.asp	Block	1
2.53.145.196	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
84.111.171.47	Israel	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	1
67.245.1.115	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	1
66.249.64.45	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/5/69385.pdf	Block	1
157.55.39.104	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
5.29.181.69	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.77	Block	1
66.249.64.30	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9724-he/refuah.aspx	Block	1
204.79.180.226	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
84.111.171.47	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp-login.php	Block	1