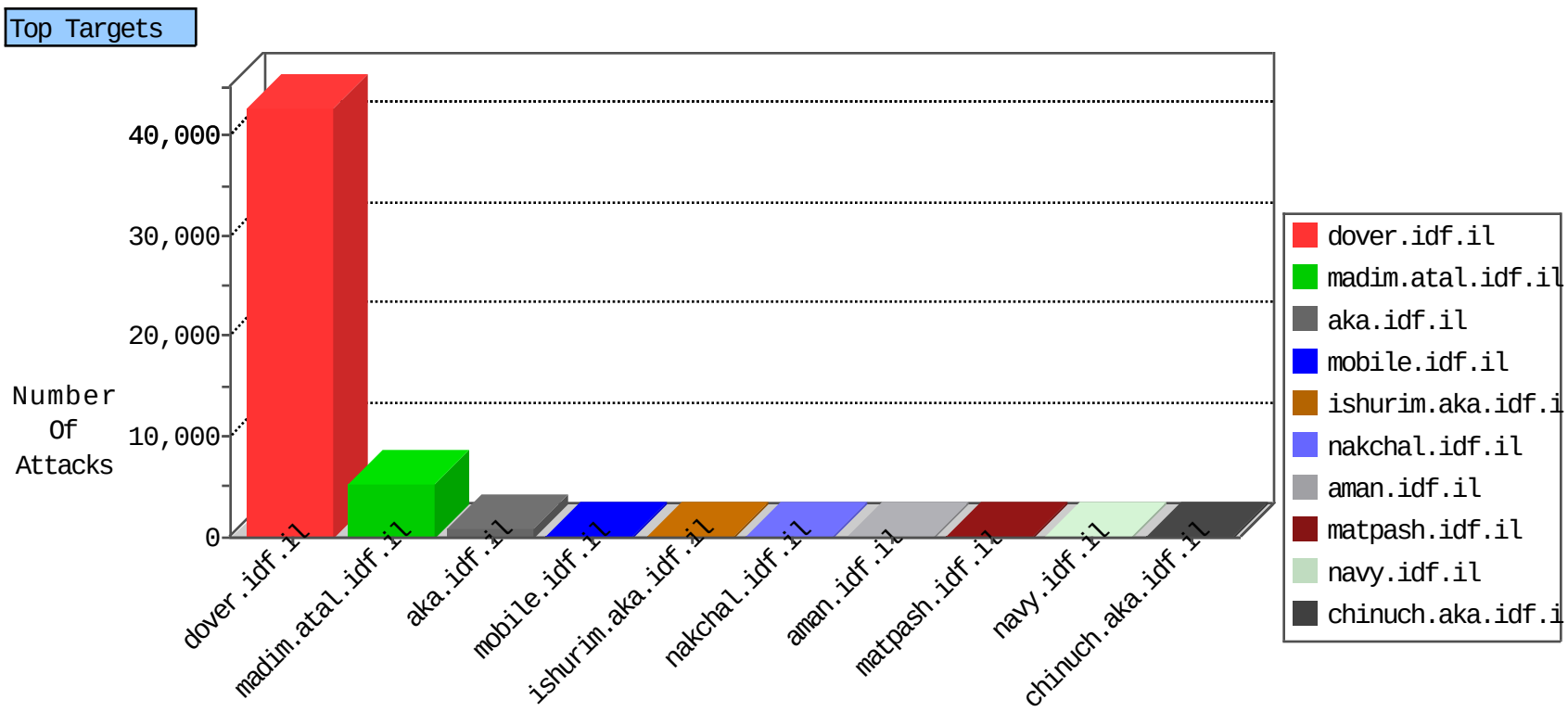
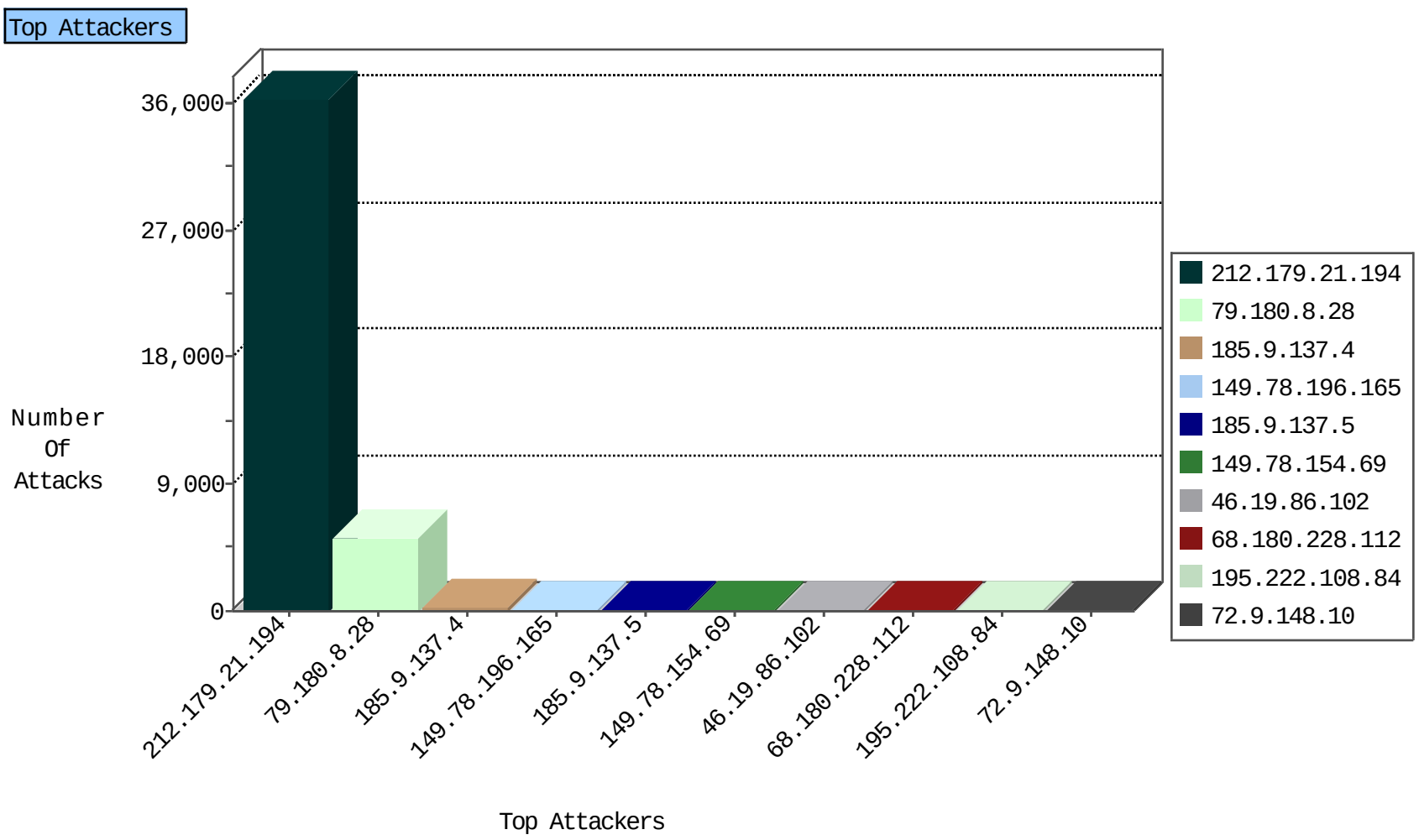
10-20-2015-19:04:08 to 10-20-2015-20:04:08

IDF Under Attack
Daily Report

Top Targets



Top Attackers



10-20-2015-19:04:08 to 10-20-2015-20:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
104.159.221.135	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	640
37.26.149.237	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	103
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	81
46.116.230.0	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	77
37.142.68.128	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	35
77.127.184.111	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
5.102.241.43	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
79.177.144.116	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
212.76.101.129	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
46.120.140.184	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
112.133.229.114	India	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
2.54.59.171	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
79.179.33.64	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
188.120.148.226	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
82.81.6.85	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
149.78.196.165	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
79.177.199.121	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
212.179.21.194	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
80.246.136.182	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
37.26.148.240	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
37.8.3.180	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
2.54.169.78	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
109.252.38.122	Russian Federation	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	4
84.109.36.246	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
80.246.139.189	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
77.125.114.6	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.13.1.122	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
85.250.220.207	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
188.120.148.226	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
185.120.126.22		147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
172.56.26.253	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
45.33.4.186		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
67.101.225.138	United States	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
82.136.239.71	Netherlands	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
46.19.86.83	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
185.9.137.4	Lebanon	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
93.174.93.146	Netherlands	147.237.76.86	navy.idf.il	Invalid TCP Flags	drop	1
80.246.136.182	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
67.101.225.138	United States	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
190.104.20.141	Bolivia	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
37.19.137.17	Ukraine	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
85.140.118.78	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
37.26.148.181	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1

10-20-2015-19:04:08 to 10-20-2015-20:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.219.209.176	Israel	147.237.77.176	matpash.idf.il	14170: HTTP: Blank User-Agent (descriptor but no string)	Block	4
149.88.229.142	Israel	147.237.0.34	tikshuv.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
5.22.130.135	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.121.235.25	Israel	147.237.76.86	navy.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2

10-20-2015-19:04:08 to 10-20-2015-20:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	3
31.154.9.150	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.111.38.242	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
209.41.67.92	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
84.108.40.24	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.240.155.234	147.237.76.201	United States	e.atal.idf.il	ET SCAN Potential SSH Scan	1
80.179.102.94	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
120.150.29.211	147.237.76.31	Australia	nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
79.181.37.40	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.66.41.57	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.121.94.24	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.49.122	147.237.72.166	Netherlands	aka.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.240	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.69.159.140	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.38	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
86.98.11.74	147.237.8.46	United Arab Emirates	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
31.211.102.129	147.237.77.212	Russian Federation	e.dover.idf.il	ET SCAN NMAP -sS window 4096	1
85.65.161.3	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
209.56.132.253	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
84.108.220.25	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
199.203.215.1	147.237.76.86	Israel	navy.idf.il	SQL Injection - Paranoid	1
82.102.169.210	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.240.155.234	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
79.181.109.126	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
120.150.29.211	147.237.76.31	Australia	nakchal.idf.il	ET SCAN NMAP -f -sS	1
79.143.180.44	147.237.8.28	Germany	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
94.159.216.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.117.11.149	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.69.235.43	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.249	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.68.59.236	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
86.98.11.74	147.237.8.45	United Arab Emirates	e.eitan.idf.il	ET SCAN Potential SSH Scan	1

10-20-2015-19:04:08 to 10-20-2015-20:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36251
185.9.137.4	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	264
149.78.196.165	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	137
185.9.137.5	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	125
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	122
46.19.86.102	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	115
195.222.108.84	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	98
109.65.211.39	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	78
46.19.85.151	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	69
37.142.136.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
167.63.37.210	Uruguay	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	62
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
79.179.128.87	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
156.111.111.81	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
66.249.93.196	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
131.92.84.144	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
151.80.31.115	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
176.58.77.179	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
198.254.230.9	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
46.19.85.121	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
84.109.36.246	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
87.68.18.28	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
113.255.125.242	Hong Kong	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
66.249.93.192	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
66.249.93.200	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
46.19.86.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
93.172.184.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
31.154.92.164	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
100.100.29.21		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	38
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
37.142.68.128	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
80.179.9.7	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
82.102.169.113	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
172.56.26.253	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
100.100.13.91		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	36
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
100.100.109.19		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	33
80.179.9.115	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
173.209.212.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
149.88.229.142	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
91.135.102.176	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
84.228.243.79	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
109.65.141.198	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
100.100.32.216		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	27

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.180.8.28	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 79.180.8.28	Block	5204
68.180.230.167	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in nakhal.idf.il/1117-he/nakhal.aspx	Block	78
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1927-he/cogat.aspx	Block	76
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	52
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	52
189.203.217.246	Mexico	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1744	Block	39
79.180.143.11	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	39
65.55.210.93	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	26
2.54.186.43	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	26
176.12.139.88	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	26
207.46.13.187	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	26
81.218.135.68	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on aka.idf.il/https:/aka.idf.il/	Block	13
37.26.146.157	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	13
79.176.226.181	Israel	147.237.72.166	aka.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 79.176.226.181	Block	13
180.97.106.37	China	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	13
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_text.asp	Block	13
62.0.101.185	Israel	147.237.77.216	dover.idf.il	NULL Character in Method	Block	13
87.69.241.92	Israel	147.237.72.156	aman.idf.il	Multiple Abnormally Long Request from 87.69.241.92	Block	13
2.52.163.163	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
79.182.195.243	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	13
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
109.65.80.118	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	13
84.108.71.220	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
46.116.171.172	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	13
79.179.55.119	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/giyus	Block	13
185.32.179.63	Israel	147.237.76.39	mobile.meitav.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtContent in mobile.meitav.idf.il/1494-he/meitav.aspx	Block	13
66.249.93.154	Israel	147.237.72.166	aka.idf.il	Unknown Parameter modul.GoTo in www.aka.idf.il/main/giyus/default.aspx	None	13
89.139.161.186	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	13
2.54.160.248	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/favicon.ico	Block	13
79.182.216.115	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	13
77.125.100.102	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	13
109.160.164.50	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	13
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.59	Block	13
87.68.251.114	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	13
46.117.125.190	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/home/giyus	Block	13
79.180.8.28	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	13
66.249.64.244	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	13
95.86.86.171	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on aka.idf.il/https:/aka.idf.il/	Block	13
80.246.130.164	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
77.127.246.188	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/faq.aspxhttps:/www.aka.idf.il/main/giyus/faq.aspx	Block	13
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
87.69.191.117	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
46.117.162.162	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	13
66.249.67.41	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	13
95.86.86.171	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	13
80.246.139.185	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
17.138.59.144	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/apple-app-site-association	Block	13
79.176.19.24	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	13
176.12.139.243	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.65	Block	13