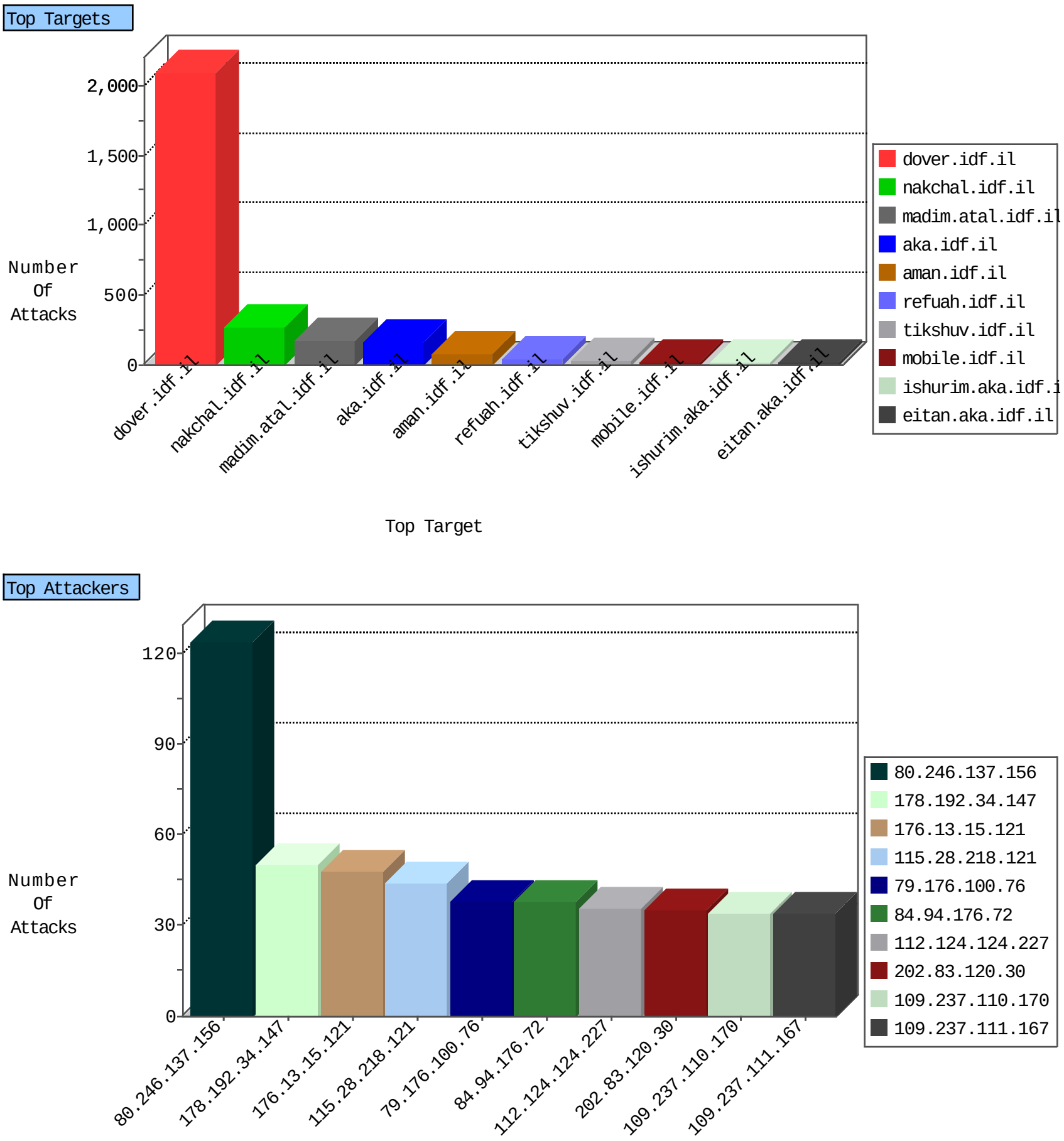
09-28-2016-13:04:01 to 09-28-2016-14:04:01

IDF Under Attack Daily Report



09-28-2016-13:04:01 to 09-28-2016-14:04:01

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	15
79.176.100.76	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
2.53.131.0	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9
207.232.5.113	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
109.253.136.112	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
109.64.118.73	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
2.53.169.108	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
2.53.5.85	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
2.53.147.88	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
185.24.207.96	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
176.13.22.76	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
2.53.182.42	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
199.203.83.190	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
2.55.50.129	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
2.53.6.188	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
84.95.21.211	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
2.55.27.152	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
37.26.149.174	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
185.32.179.214	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
2.55.32.190	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
2.53.44.244	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
37.46.41.127	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
93.158.200.206	Netherlands	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1
176.13.250.254	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
37.142.223.188	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
2.55.1.99	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
31.168.240.21	Israel	147.237.72.166	aka.idf.il	Black List	drop	1

09-28-2016-13:04:01 to 09-28-2016-14:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.29.217.24	Israel	147.237.72.156	aman.idf.il	32390: HTTP: Suspicious User-Agent (Mozilla)	Block	2
203.219.204.56	Australia	147.237.76.148	gqcenter.aka.idf.il	2226: Backdoor: TCP Window Size 55808 Trojan	Block	1

09-28-2016-13:04:01 to 09-28-2016-14:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
59.67.64.13	147.237.76.148	China	gqcenter.aka.idf.il	GPL SCAN nmap TCP	1
52.91.97.47	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.162	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.154.12.158	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.28.134.152	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
177.16.113.80	147.237.76.30	Brazil	himush.idf.il	ET SCAN NMAP -sS window 4096	1
106.120.209.154	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN NMAP -f -sS	1
80.246.137.47	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.125.90.126	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	1
52.91.97.47	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.89	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.142.40.142	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.102.253.115	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
179.43.141.198	147.237.0.200	Switzerland	m4u.idf.il	ET SCAN Potential SSH Scan	1
2.55.157.176	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
106.120.209.154	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN NMAP -sS window 2048	1
82.81.108.146	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.176.92	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-28-2016-13:04:01 to 09-28-2016-14:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.93.83	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
212.235.98.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
62.0.229.154	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	25
141.0.14.146	Europe	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	24
199.203.63.211	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
62.219.138.226	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
176.13.15.121	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
109.66.4.113	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
109.253.129.176	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
109.253.214.127	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.14	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
176.13.6.111	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
178.192.34.147	Switzerland	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	12
37.26.148.163	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
178.192.34.147	Switzerland	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	11
194.90.99.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
2.53.156.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
84.229.33.20	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
115.28.218.121	China	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
176.13.22.76	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
178.192.34.147	Switzerland	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	10
115.28.218.121	China	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	9
178.192.34.147	Switzerland	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
79.176.59.71	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.105	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
115.28.218.121	China	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	9
185.32.176.24	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
46.19.85.105	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
202.83.120.30	Indonesia	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	9
46.19.86.143	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
31.168.231.141	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
109.253.201.236	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
185.46.214.59	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.90	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.237.111.167	Russian Federation	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	8
176.13.7.156	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
2.53.163.43	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
176.228.33.78	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
109.253.199.180	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
202.83.120.30	Indonesia	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	8
109.237.110.170	Russian Federation	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	8
109.237.111.167	Russian Federation	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	8
82.80.103.126	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
202.83.120.30	Indonesia	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
212.25.107.145	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
199.203.179.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
115.28.218.121	China	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
112.124.124.227	China	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	7

09-28-2016-13:04:01 to 09-28-2016-14:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.137.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	124
109.253.200.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
132.72.86.150	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	7
2.53.163.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
141.0.15.214	Norway	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 141.0.15.214	Block	7
197.211.57.26	Nigeria	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	7
197.211.57.26	Nigeria	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	7
197.211.57.26	Nigeria	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 197.211.57.26	Block	6
84.94.176.72	Israel	147.237.72.156	aman.idf.il	Distributed Illegal Byte Code Character in Method	Block	5
84.94.176.72	Israel	147.237.72.156	aman.idf.il	Distributed Unknown HTTP Request Method	Block	5
80.246.139.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
176.13.227.84	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
84.94.176.72	Israel	147.237.72.156	aman.idf.il	Distributed Malformed URL	Block	5
84.94.176.72	Israel	147.237.72.156	aman.idf.il	Distributed Abnormally Long Request	Block	5
109.253.201.236	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
84.94.176.72	Israel	147.237.72.156	aman.idf.il	Distributed Illegal Byte Code Character in Header Name	Block	4
2.55.178.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.197.33	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.147.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
62.219.147.212	Israel	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	2
197.211.57.26	Nigeria	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.idf.il/1038-en/dover.aspx	Block	2
84.94.176.72	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Header Value from 84.94.176.72	Block	2
157.55.39.177	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/robots.txt	Block	2
84.94.176.72	Israel	147.237.72.156	aman.idf.il	Distributed Malformed HTTP Header Line	Block	2
77.138.195.95	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/	Block	2
91.112.220.66	Austria	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 91.112.220.66	Block	2
46.158.128.221	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	2
80.246.137.232	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
2.53.35.243	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
91.199.99.36	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;t in www.aka.idf.il/main/sachar/scriptresource.axd	None	1
66.249.76.43	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/shared/usercontrols/headeruppe r/	Block	1
84.94.176.72	Israel	147.237.72.156	aman.idf.il	Multiple Abnormally Long Header Line from 84.94.176.72	Block	1
62.219.147.212	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 62.219.147.212	Block	1
157.55.39.164	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1
77.125.90.126	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/giyus/main/	Block	1
66.102.9.22	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	1
84.95.252.83	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.86.67	Israel	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
194.90.200.70	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 194.90.200.70	Block	1
138.134.192.10	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	1
109.253.129.28	Israel	147.237.72.167	ishurim.aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 109.253.129.28	Block	1
66.249.76.57	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/iturim/asp/list.asp	Block	1
109.253.199.180	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.66.162	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.162	Block	1
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/nakhal	Block	1
85.64.144.223	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il./favicon.ico	Block	1
84.94.176.72	Israel	147.237.72.156	aman.idf.il	Illegal Byte Code Character in Header Value	Block	1
46.121.83.201	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl17 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
197.211.57.26	Nigeria	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1

09-28-2016-13:04:01 to 09-28-2016-14:04:01