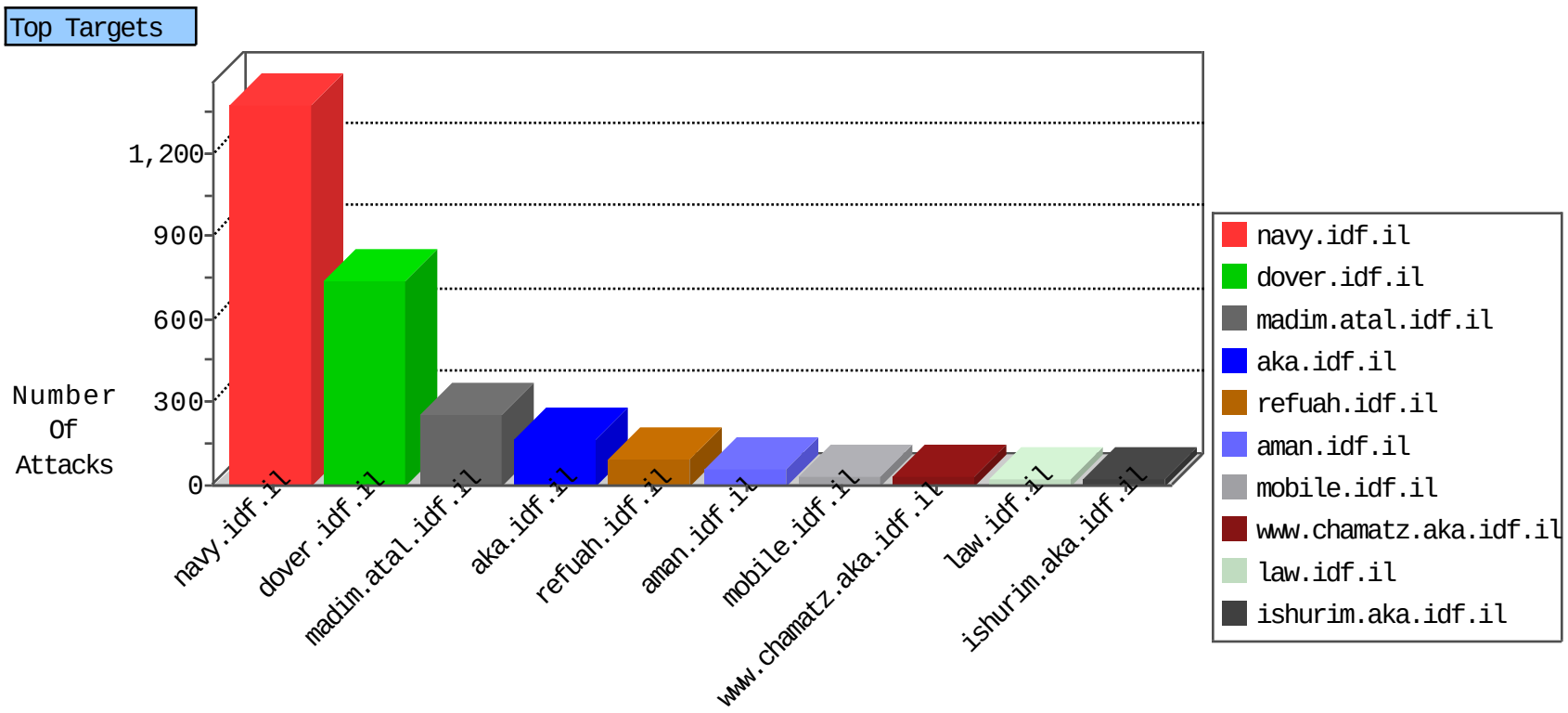
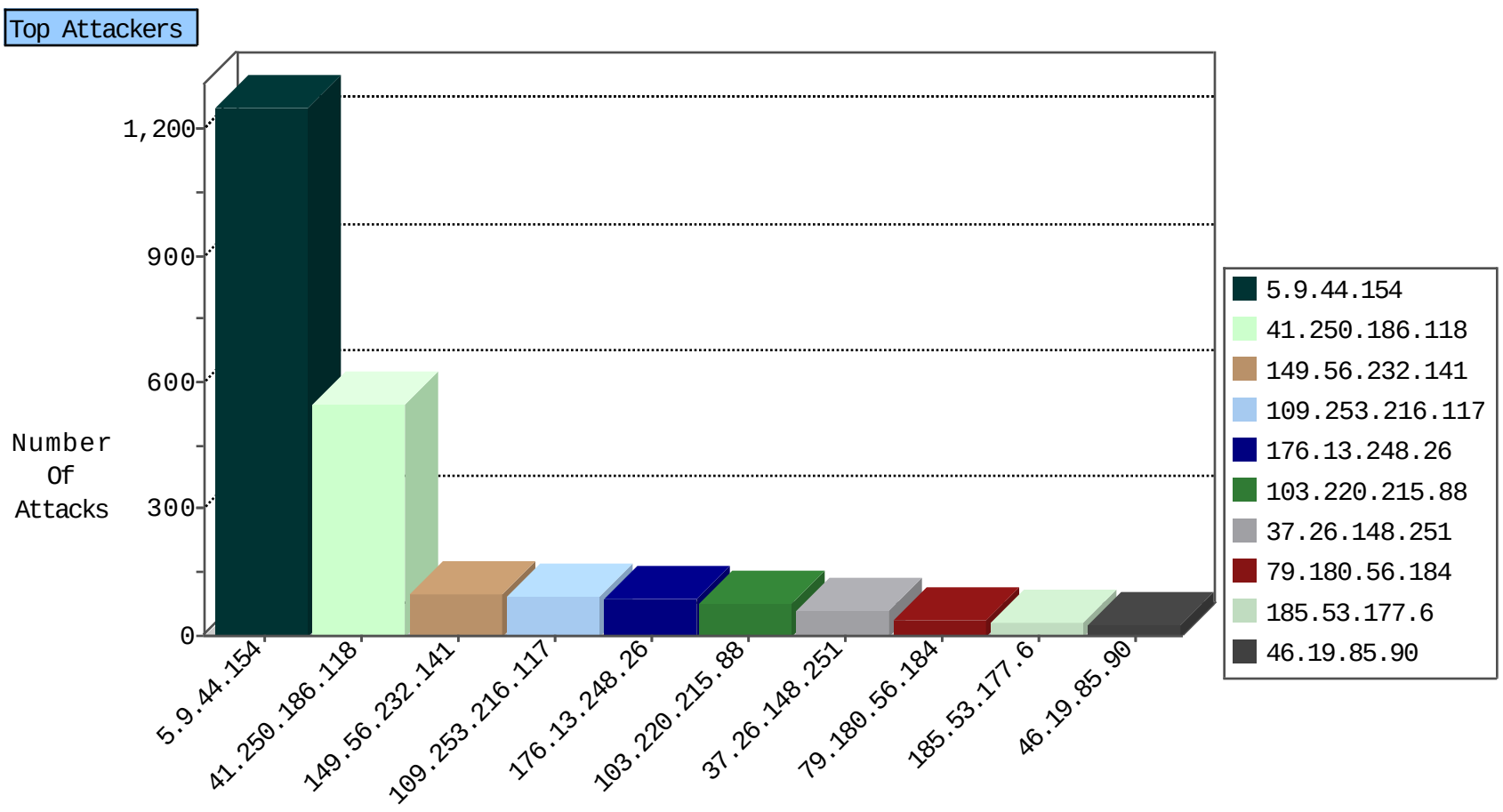
09-11-2016-19:04:06 to 09-11-2016-20:04:06

IDF Under Attack
Daily Report





09-11-2016-19:04:06 to 09-11-2016-20:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.250.186.118	Morocco	147.237.77.216	dover.idf.il	DOS-HTTP-torshammer	forward	406
41.250.186.118	Morocco	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	340
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
194.29.178.14	Poland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
129.93.229.138	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
131.247.2.241	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
156.56.250.226	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	2
130.194.252.8	Australia	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
141.22.213.34	Germany	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
153.90.1.34	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
134.197.113.3	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.82	Czech Republic	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
139.78.141.243	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.42.142.45	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
204.85.191.11	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
170.140.119.70	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
82.81.90.13	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.114	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-11-2016-19:04:06 to 09-11-2016-20:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
162.210.196.129	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2

09-11-2016-19:04:06 to 09-11-2016-20:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
45.79.71.122	147.237.72.167	United States	ishurim.aka.idf.il	WEB-MISC Chunked-Encoding transfer attempt	2
83.20.39.39	147.237.77.216	Poland	dover.idf.il	Xenu Link Sleuth User Agent	2
79.180.56.184	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sA (2)	2
175.142.131.240	147.237.77.216	Malaysia	dover.idf.il	Xenu Link Sleuth User Agent	2
79.181.105.42	147.237.76.86	Israel	navy.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
66.249.93.69	147.237.76.42	Europe	refuah.idf.il	ET SCAN NMAP -sA (2)	1
202.170.80.40	147.237.76.177	Mongolia	ncore.idf.il	ET SCAN Potential SSH Scan	1
1.32.43.154	147.237.76.42	Malaysia	refuah.idf.il	ET SCAN NMAP -sS window 4096	1
163.172.129.15	147.237.76.42	United Kingdom	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
109.60.153.178	147.237.77.19	Russian Federation	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
109.60.153.178	147.237.76.42	Russian Federation	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
95.211.144.96	147.237.77.234	Netherlands	halag.idf.il	ET WEB_SERVER Poison Null Byte	1
46.172.71.251	147.237.0.35	Ukraine	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
5.255.90.133	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
1.32.43.154	147.237.76.42	Malaysia	refuah.idf.il	ET SCAN NMAP -sS window 3072	1
162.213.1.246	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	1
109.60.153.178	147.237.76.148	Russian Federation	gqcenter.aka.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
103.207.39.11	147.237.76.30	Vietnam	himush.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.8.28	Netherlands	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1

09-11-2016-19:04:06 to 09-11-2016-20:04:06

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		monitor	657
5.9.44.154	Germany	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	569
41.250.186.118	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	458
103.220.215.88		147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	74
79.180.56.184	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	32
5.9.44.154	Germany	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	27
46.19.85.244	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
79.33.130.153	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
46.19.85.10	Israel	147.237.76.42	refuah.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	13
46.19.85.90	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
109.253.209.5	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
46.19.86.144	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
46.19.86.144	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
141.226.162.23	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
81.218.57.230	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
2.53.13.32	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.247	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.85	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
185.32.179.159	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.90	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
5.22.134.222	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.90	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
149.56.232.141	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
74.208.230.195	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
158.85.253.245	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
87.106.184.160	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
176.13.250.78	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.229.25.35	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
149.56.232.141	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
149.56.232.141	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
91.135.102.183	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
2.55.20.118	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
149.56.232.141	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
31.25.73.184	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
149.56.232.141	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
37.26.148.231	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
2.53.50.92	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
149.56.232.141	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
91.135.102.183	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
41.250.186.118	Morocco	147.237.77.216	dover.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	4
185.53.177.6	Germany	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
109.253.216.146	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
149.56.232.141	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.19.85.148	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
84.94.170.66	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
149.56.232.141	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
149.56.232.141	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
185.53.177.6	Germany	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4

09-11-2016-19:04:06 to 09-11-2016-20:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.216.117	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	93
176.13.248.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	87
37.26.148.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	56
109.65.49.141	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
141.226.243.47	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	3
80.246.136.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.179.179.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.146.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.53.2.24	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
66.102.8.217	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
95.211.144.96	Netherlands	147.237.77.234	halag.idf.il	Illegal HTTP Version	Block	1
2.53.45.148	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
79.180.130.214	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/homepage.aspx	Block	1
141.226.162.23	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
77.125.85.56	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
95.211.144.96	Netherlands	147.237.77.234	halag.idf.il	Multiple NULL Character in Method from 95.211.144.96	Block	1
93.172.158.17	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
77.138.234.231	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
204.79.180.238	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	1
109.65.150.51	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international_training	Block	1
66.249.66.174	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.66.174	Block	1
95.211.144.96	Netherlands	147.237.77.234	halag.idf.il	Malformed HTTP Header Line 2	Block	1
2.55.42.206	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.180.136.146	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
77.138.51.133	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
46.19.85.156	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
95.211.144.96	Netherlands	147.237.77.234	halag.idf.il	NULL Character in Header Name at [[#0]]œ[[#0]]•[[#0]]/[[#0]]5À[[#18]][[#0]]	Block	1
95.211.144.96	Netherlands	147.237.77.234	halag.idf.il	Abnormally Long Request method	Block	1
77.139.105.211	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/	Block	1
207.46.13.59	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/tizmoret/gallery/	None	1
109.66.141.63	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
66.249.66.176	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
95.211.144.96	Netherlands	147.237.77.234	halag.idf.il	Malformed URL ¸[[#20]]¸	Block	1
31.154.81.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/giyus	Block	1
77.138.68.62	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/yohalan/	Block	1
174.44.65.2	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/	Block	1
95.211.144.96	Netherlands	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/changelog.txt	Block	1
95.211.144.96	Netherlands	147.237.77.234	halag.idf.il	Illegal Byte Code Character in Header Name [[#0]]œ[[#0]]•[[#0]]/[[#0]]5À[[#18]][[#0]]	Block	1
213.8.204.33	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
109.253.208.3	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.76.70	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/.well-known/apple-app-site-association	Block	1
95.211.144.96	Netherlands	147.237.77.234	halag.idf.il	Multiple Illegal Byte Code Character in Method from 95.211.144.96	Block	1
80.246.138.98	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.138.121.97	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	1
95.211.144.96	Netherlands	147.237.77.234	halag.idf.il	Unknown HTTP Request Method [[#22]][[#3]][[#1]][[#0]]•[[#1]][[#0]][[#0]]{[[#3]][[#3]]¹•K½C<žl[[#6]]LA†ÏT[[#7]]¿"¶(ˆð[[#0]]r}Ê°[[#23]]7Š‘-[[#25]][[#0]][[#0]][[#28]]À/À+À0À,À[[#19]]À in URL ¸[[#20]]¸	Block	1
95.211.144.96	Netherlands	147.237.77.234	halag.idf.il	Illegal Byte Code Character in URL ¸[[#20]]¸	Block	1
79.180.56.184	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1

09-11-2016-19:04:06 to 09-11-2016-20:04:06