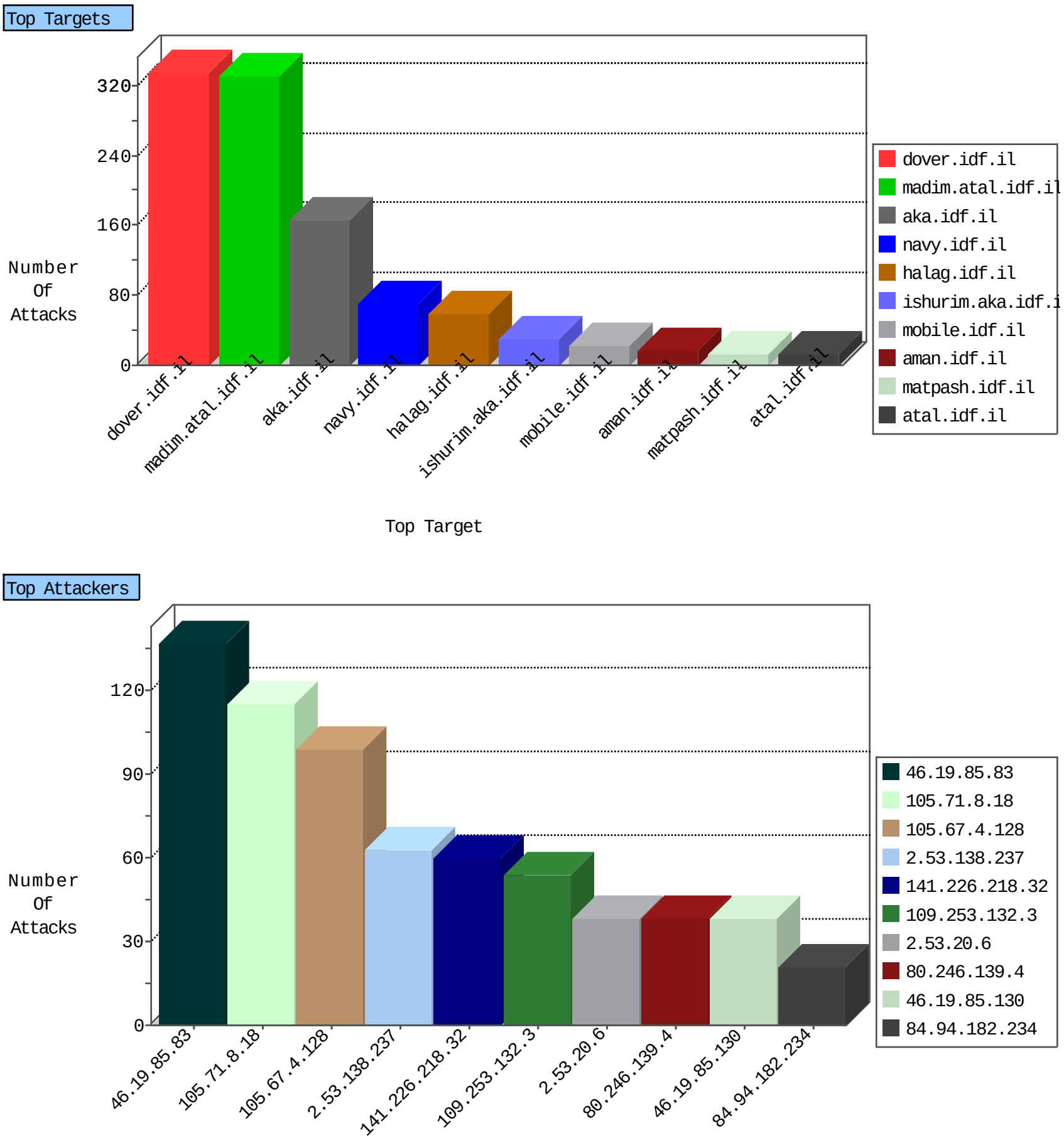
09-21-2016-21:04:09 to 09-21-2016-22:04:09

IDF Under Attack Daily Report



09-21-2016-21:04:09 to 09-21-2016-22:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.137.183	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
173.208.150.116	United States	147.237.76.30	himush.idf.il	block-sp-traf1	forward	2
69.30.193.250	United States	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	2
204.12.220.82	United States	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	1
71.15.85.176	United States	147.237.77.179	e.mazi.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
173.208.197.202	United States	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	forward	1
69.30.193.250	United States	147.237.77.233	atal.idf.il	block-sp-traf1	forward	1
204.12.220.85	United States	147.237.77.216	dover.idf.il	block-sp-traf1	forward	1
142.54.174.82	United States	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	1
176.228.24.49	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1
69.30.226.220	United States	147.237.72.166	aka.idf.il	block-sp-traf1	forward	1
142.54.174.86	United States	147.237.77.235	sviva.idf.il	block-sp-traf1	forward	1
63.141.231.195	United States	147.237.77.170	maarachot.idf.il	block-sp-traf1	forward	1
198.204.224.235	United States	147.237.77.176	matpash.idf.il	block-sp-traf1	forward	1
69.30.226.220	United States	147.237.77.234	halag.idf.il	block-sp-traf1	forward	1

09-21-2016-21:04:09 to 09-21-2016-22:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-21-2016-21:04:09 to 09-21-2016-22:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
79.179.19.77	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	2
115.238.163.174	147.237.77.235	China	sviva.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
5.149.251.149	147.237.77.176	United Kingdom	matpash.idf.il	ET SCAN NMAP -sS window 1024	2
123.142.241.28	147.237.77.216	Korea, Republic of	dover.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
94.102.56.151	147.237.77.74	Netherlands	law.idf.il	ET SCAN Potential SSH Scan	1
94.102.56.151	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.74	147.237.8.45	United States	e.eitan.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
163.172.238.45	147.237.72.156	United Kingdom	aman.idf.il	ET SCAN NMAP -sS window 1024	1
64.137.168.128	147.237.77.74	Canada	law.idf.il	ET SCAN Potential SSH Scan	1
118.103.126.194	147.237.77.179	Japan	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
47.88.4.204	147.237.77.226	Canada	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
109.60.153.178	147.237.77.234	Russian Federation	halag.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.56.151	147.237.77.233	Netherlands	atal.idf.il	ET SCAN Potential SSH Scan	1
94.102.56.151	147.237.77.176	Netherlands	matpash.idf.il	ET SCAN Potential SSH Scan	1
94.102.56.151	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
94.102.56.151	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN Potential SSH Scan	1
176.228.24.49	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
71.15.85.176	147.237.77.235	United States	sviva.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	147.237.77.234	China	halag.idf.il	ET SCAN NMAP -sS window 1024	1
116.26.7.25	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
37.143.82.50	147.237.77.216	Netherlands	dover.idf.il	ET SCAN NMAP -sS window 3072	1
113.105.246.214	147.237.77.176	China	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
105.67.4.128	147.237.77.216	Morocco	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.56.151	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN Potential SSH Scan	1

09-21-2016-21:04:09 to 09-21-2016-22:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
141.226.218.32	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	48
105.71.8.18	Morocco	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	46
105.71.8.18	Morocco	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	39
105.67.4.128	Morocco	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	33
105.67.4.128	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
80.246.139.4	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	17
142.244.5.112	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	12
105.71.8.18	Morocco	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
105.71.8.18	Morocco	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	10
80.246.139.4	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	10
46.19.85.130	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
46.19.85.130	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
109.253.240.157	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
105.71.8.18	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
84.111.38.84	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.85.130	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
105.67.4.128	Morocco	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
105.67.4.128	Morocco	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
66.102.9.147	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
105.67.4.128	Morocco	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
105.67.4.128	Morocco	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	8
109.253.240.157	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
105.67.4.128	Morocco	147.237.77.216	dover.idf.il	Streaming Engine: TCP SYN Modified Retransmission	Data received before SYN-ACK was acknowledged. Stripping all packet data.	drop	6
46.19.86.251	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.32.179.149	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
79.181.58.141	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.94.182.234	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence		monitor	6
176.13.246.88	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.139.4	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
84.94.182.234	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	6
46.19.85.130	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
80.246.139.4	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
207.241.226.144	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	5
2.55.179.142	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
185.32.179.149	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
141.226.218.32	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
141.226.218.32	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.55.191.108	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.46.39.81	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.92	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
37.46.41.214	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	4
37.26.149.137	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.182.147.135	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
66.249.64.169	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.73	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	3
84.94.182.234	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	3
176.13.19.64	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
5.149.251.149	United Kingdom	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
84.94.182.234	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	3
37.26.147.161	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3

09-21-2016-21:04:09 to 09-21-2016-22:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.83	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	137
2.53.138.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	62
109.253.132.3	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	54
2.53.20.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	38
77.125.87.136	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	17
2.53.135.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
176.13.247.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
185.120.126.29	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	6
185.120.126.29	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	3
46.19.85.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.179.25.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.22.134.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.166.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
217.132.44.28	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/kiosk/kiosk.aspx	Block	2
109.253.201.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.126.39.25	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
217.132.116.109	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$emailUpdate$rptEmailSubjectsList$ctl00$cbEmailSubject in www.aka.idf.il/main/giyus/faq.aspx	None	1
180.97.106.162	China	147.237.76.30	himush.idf.il	Unauthorized URL Access to 180.163.113.82/check_proxy	Block	1
46.19.86.140	Israel	147.237.77.216	dover.idf.il	Malformed URL like	Block	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
46.19.85.73	Israel	147.237.76.86	navy.idf.il	Malformed URL	Block	1
2.53.138.237	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
87.69.67.177	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/	Block	1
66.240.192.138	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/robots.txt	Block	1
46.19.85.89	Israel	147.237.76.86	navy.idf.il	Illegal HTTP Version	Block	1
180.97.106.161	China	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 180.163.113.82/check_proxy	Block	1
110.170.10.178	Thailand	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
5.149.251.149	United Kingdom	147.237.77.176	matpash.idf.il	Unauthorized Method OPTIONS for /	Block	1
77.139.226.111	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
217.132.165.113	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/	Block	1
180.97.106.162	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to 180.163.113.82/check_proxy	Block	1
46.19.86.140	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method (KHTML, in URL like	Block	1
46.19.85.73	Israel	147.237.76.86	navy.idf.il	Unknown HTTP Request Method /en_US;FBOP/5] in URL	Block	1
2.53.140.189	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
89.237.114.86	France	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.139	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8876-he/refuah.aspx	Block	1
198.20.87.98	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
180.97.106.161	China	147.237.0.19	madim.atal.idf.il	Distributed Unauthorized URL Access on 180.163.113.82/check_proxy	Block	1
141.226.218.32	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
5.149.251.149	United Kingdom	147.237.77.176	matpash.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
185.27.105.74	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/watch	Block	1
46.19.86.251	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
180.97.106.37	China	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on 180.163.113.82/check_proxy	Block	1
89.248.172.16	Netherlands	147.237.76.30	himush.idf.il	Unauthorized URL Access to 147.237.76.30/robots.txt	Block	1
66.249.65.14	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on www.chamatz.aka.idf.il/404.aspx	Block	1
216.244.66.236	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	Block	1
180.97.106.161	China	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on 180.163.113.82/check_proxy	Block	1
46.19.86.140	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request request version	Block	1
157.55.39.153	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
37.46.39.223	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1

09-21-2016-21:04:09 to 09-21-2016-22:04:09