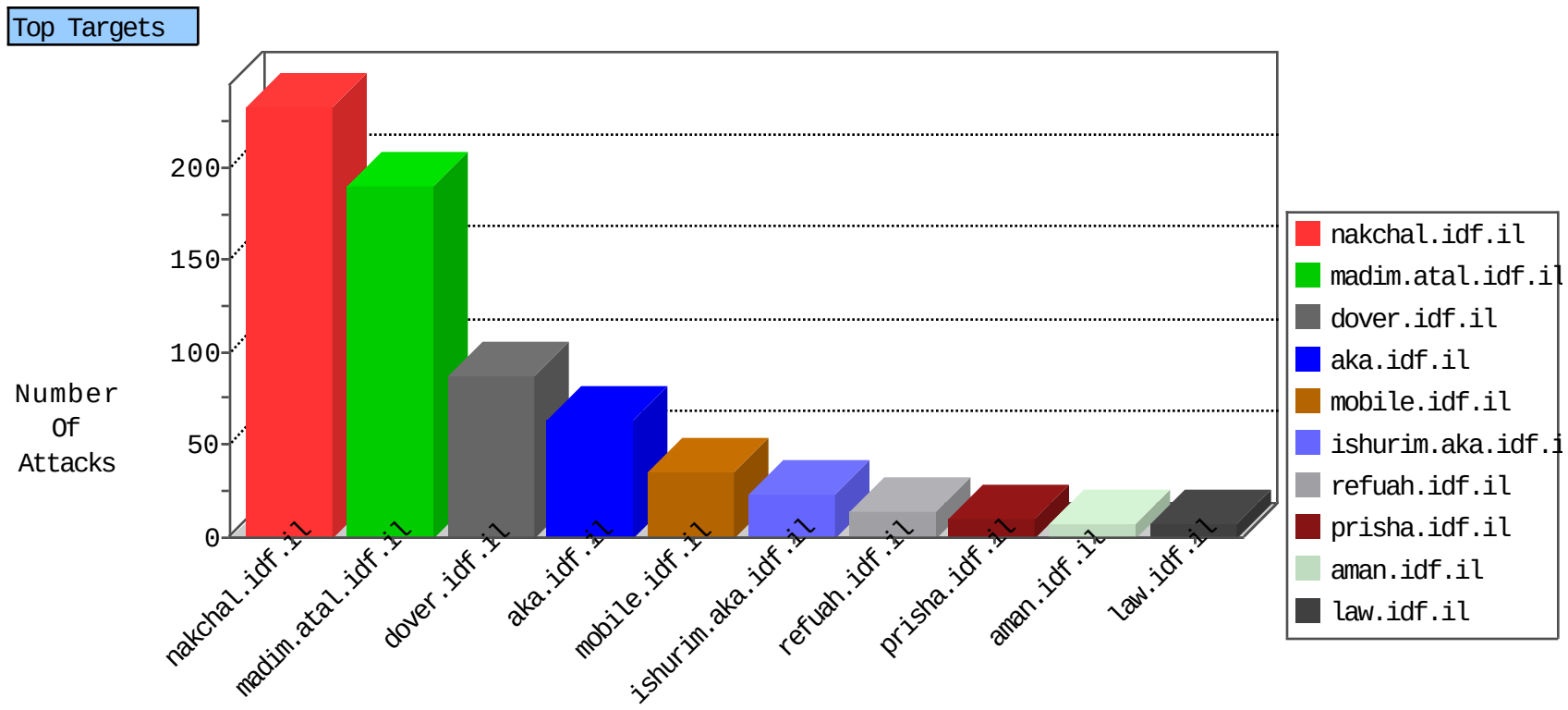
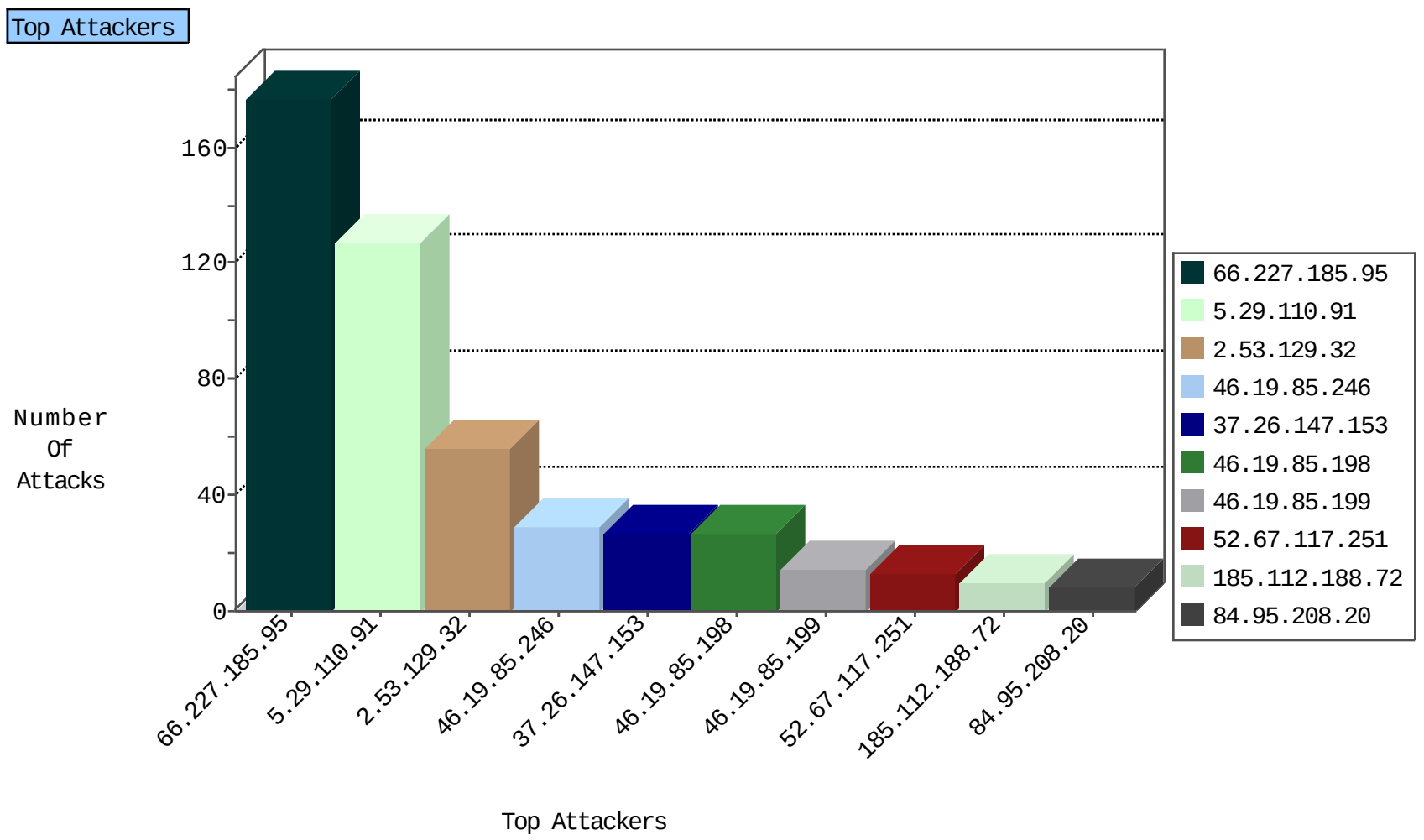
09-28-2016-07:04:09 to 09-28-2016-08:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-28-2016-07:04:09 to 09-28-2016-08:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.203.172	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	16
60.212.47.99	China	147.237.76.201	e.atal.idf.il	Invalid TCP Flags	drop	1
60.212.47.99	China	147.237.76.196	e.sviva.idf.il	Invalid TCP Flags	drop	1
93.158.200.206	Netherlands	147.237.76.198	e.yohalan.idf.il	Black List	drop	1
60.212.47.99	China	147.237.76.38	e.e.meitav.idf.i	Invalid TCP Flags	drop	1
60.212.47.99	China	147.237.76.197	e.himush.idf.il	Invalid TCP Flags	drop	1
93.174.94.235	Netherlands	147.237.76.196	e.sviva.idf.il	Black List	drop	1
60.212.47.99	China	147.237.76.176	test.ncore.idf.i	Invalid TCP Flags	drop	1
60.212.47.99	China	147.237.76.198	e.yohalan.idf.il	Invalid TCP Flags	drop	1
60.212.47.99	China	147.237.76.177	ncore.idf.il	Invalid TCP Flags	drop	1

09-28-2016-07:04:09 to 09-28-2016-08:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-28-2016-07:04:09 to 09-28-2016-08:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.210.166.214	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.146.171	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
209.126.230.71	147.237.0.19	United States	madim.atal.idf.i	ET SCAN NMAP -sS window 1024	1
149.255.108.192	147.237.76.177	United Kingdom	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
95.163.144.203	147.237.76.86	Russian Federation	navy.idf.il	ET SCAN NMAP -sS window 1024	1
72.229.6.66	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
58.218.200.137	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
37.26.147.238	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
209.126.230.71	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
180.213.5.205	147.237.77.243	China	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
149.255.108.192	147.237.0.33	United Kingdom	idf.il	ET SCAN NMAP -sS window 1024	1
89.248.163.3	147.237.0.19	Netherlands	madim.atal.idf.i	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
58.218.200.137	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1

09-28-2016-07:04:09 to 09-28-2016-08:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
66.227.185.95	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	176
46.19.85.246	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	25
46.19.85.198	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
46.19.85.198	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
46.19.85.199	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.199	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
37.26.147.153	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
185.112.188.72	Iraq	147.237.77.205	prisha.idf.il	drop	First packet isn't SYN	drop	6
79.181.151.174	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.243	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.49	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.5.25	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
62.0.212.209	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
37.26.147.153	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
111.248.108.57	Taiwan	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
185.120.124.46	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
52.67.117.251	Brazil	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	3
5.22.134.238	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
66.249.76.31	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.138.229	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.153	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
52.67.117.251	Brazil	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
52.67.117.251	Brazil	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
212.179.63.66	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.26.146.195	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.153	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
52.67.117.251	Brazil	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	3
66.249.69.152	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.153	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	2
37.26.147.153	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.85.18	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
185.112.188.72	Iraq	147.237.77.205	prisha.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	2
46.19.85.246	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
77.124.2.3	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
176.13.226.152	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.85.18	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.120.240.183	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	2
185.112.188.72	Iraq	147.237.77.205	prisha.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
46.19.85.246	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.99	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
131.253.25.149	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
37.26.147.153	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
185.27.105.93	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
176.13.17.6	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.85.99	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.22	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
85.65.93.243	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
176.13.18.85	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2

09-28-2016-07:04:09 to 09-28-2016-08:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.29.110.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	127
2.53.129.32	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	56
84.95.208.20	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	4
31.154.81.10	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on www.refua.atal.idf.il/xmlrpc.php	Block	3
46.19.86.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.156.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.95.208.20	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	3
31.154.81.10	Israel	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	3
176.13.245.130	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	3
37.26.147.153	Israel	147.237.72.167	ishurim.aka.idf.i	Untraceable SSL Sessions: Open Mode	None	2
79.181.151.174	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.64.12	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/brothers/gallery/showpicture.asp	Block	1
85.64.12.183	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.76.81	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
180.76.15.7	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9694-he/refuah.aspx	Block	1
80.246.138.229	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.66.197	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1779-21525-he/idfgdover.aspx	Block	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1153-he/dover.aspx	Block	1
46.19.86.49	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
2.55.190.147	Israel	147.237.72.166	aka.idf.il	Multiple Extremely Long Parameter from 2.55.190.147	Block	1
213.8.204.57	Israel	147.237.76.31	nakchal.idf.il	PHP Attempt	Block	1
66.249.69.72	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8847-he/refuah.aspx	Block	1
37.26.147.153	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
141.226.144.36	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
77.139.236.27	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/miyun/miyunsummary.aspx	Block	1
66.102.9.2	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
213.8.204.57	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/xmlrpc.php	Block	1
66.249.69.139	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9711-he/refuah.aspx	Block	1
37.26.147.239	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/894-he/nakhal.aspx	Block	1
157.55.39.111	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
79.180.203.170	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/yahash2017אורט lobby.aspx/ערד	Block	1
66.249.64.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/forums/asp/showforum.asp	Block	1
217.132.136.23	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/default.aspx	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
37.26.149.254	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1

09-28-2016-07:04:09 to 09-28-2016-08:04:09