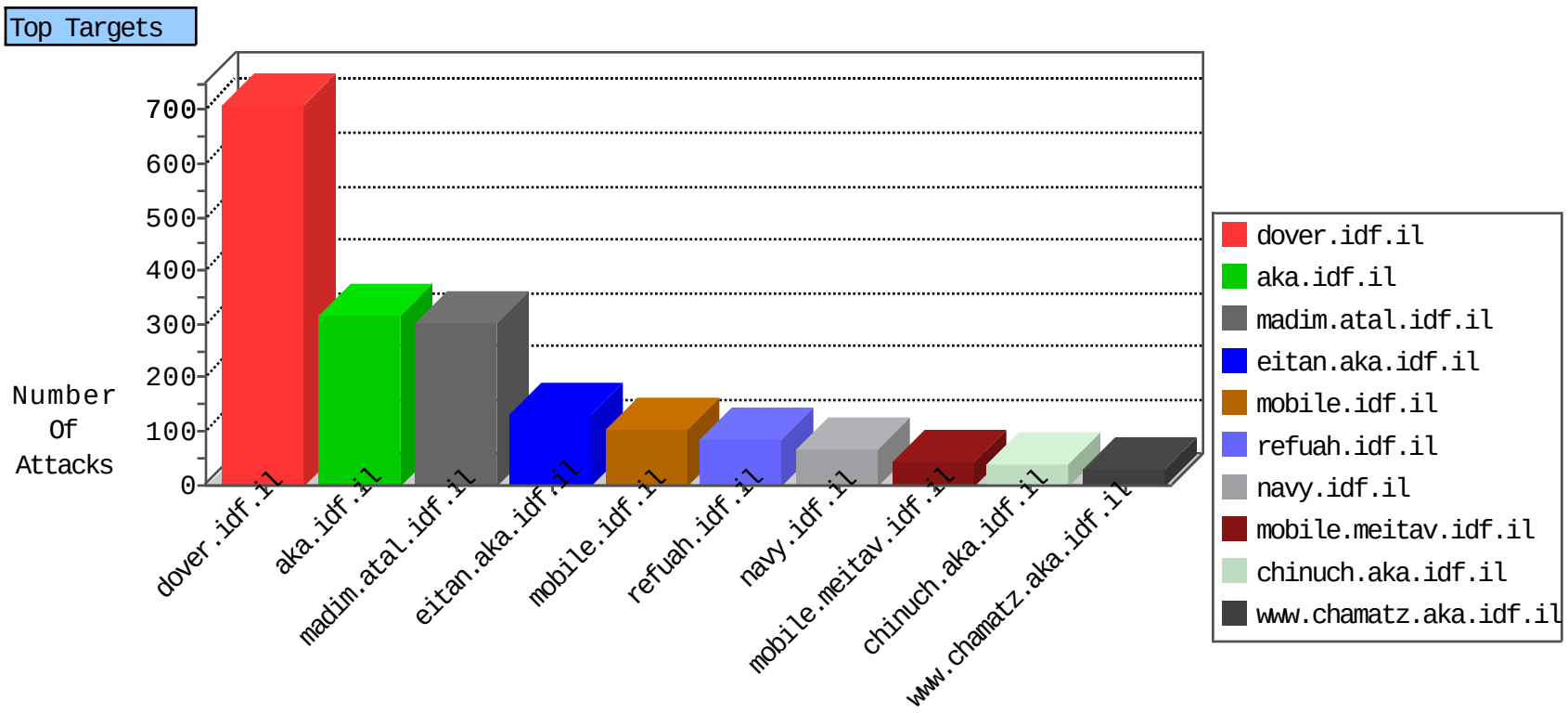
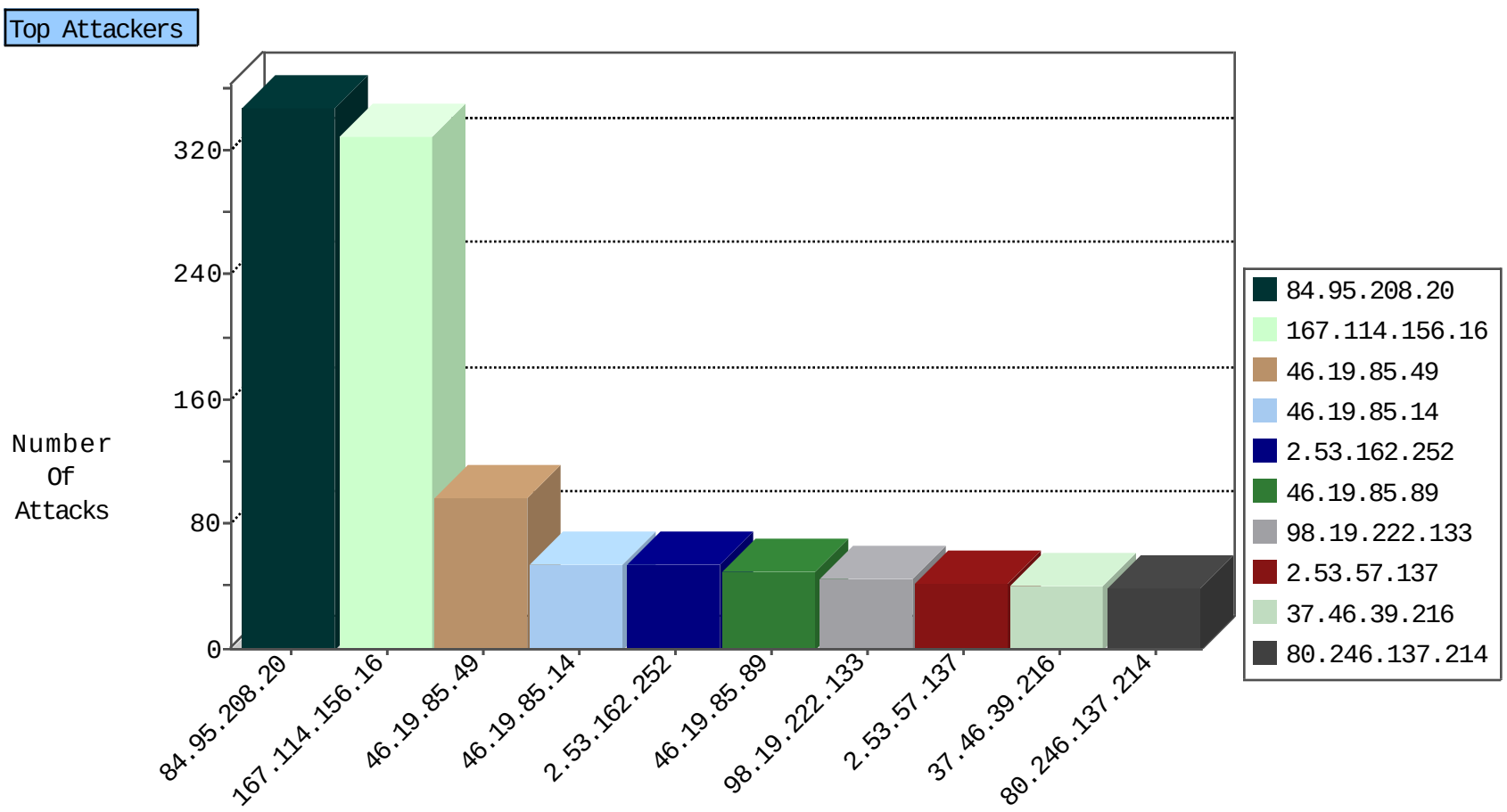
04-20-2016-10:04:02 to 04-20-2016-11:04:02

IDF Under Attack
Daily Report



Top Target



Top Attackers

04-20-2016-10:04:02 to 04-20-2016-11:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	20596
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9207
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	7168
192.115.83.5	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	202
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	121
46.117.78.159	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	102
5.102.198.58	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	101
180.160.115.173	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	13
183.36.65.153	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	6
140.250.2.136	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	6
111.36.3.238	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3
113.14.4.120	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
1.80.115.164	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	3
183.141.22.226	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	2
111.40.27.97	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	2
79.176.124.194	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	2
59.57.245.40	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	2
71.6.165.200	United States	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
71.6.167.142	United States	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
180.109.32.165	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1

04-20-2016-10:04:02 to 04-20-2016-11:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
98.19.222.133	United States	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	16
92.249.104.63	Ukraine	147.237.72.166	aka.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	8
98.19.222.133	United States	147.237.76.86	navy.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
82.165.24.123	Germany	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4

04-20-2016-10:04:02 to 04-20-2016-11:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
98.19.222.133	147.237.76.86	United States	navy.idf.il	SQL Injection - Select From	23
82.165.24.123	147.237.76.86	Germany	navy.idf.il	SQL Injection - Select From	5
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
66.249.78.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
132.74.7.49	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.183.141.92	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.147.206	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.248.33	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.34.0.141	147.237.0.200	Germany	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
109.66.1.123	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.250.216.11	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.179.118.203	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

04-20-2016-10:04:02 to 04-20-2016-11:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	108
46.19.86.119	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
79.181.226.136	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
37.46.39.216	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	34
2.55.163.142	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
176.13.18.195	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	25
46.19.85.89	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
107.167.104.59	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
95.35.77.241	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
62.219.194.115	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	12
46.19.86.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.21.242	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.253.144.84	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
80.246.137.214	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
188.120.154.187	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
109.253.145.60	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
80.246.137.214	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
46.19.85.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.13	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.32.179.49	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
72.82.254.23	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.137.214	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	6
192.118.30.102	Israel	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
192.118.30.102	Israel	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
192.118.30.102	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
80.246.137.214	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
192.118.30.102	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.52	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.94.114.160	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.148.142	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.118.30.102	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.13	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.89	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.89	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.46.39.216	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.89	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
87.69.247.34	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
126.175.37.197	Japan	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
80.246.137.214	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
82.81.101.124	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
80.246.137.214	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.85.89	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
2.55.14.26	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.184	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	124
46.19.85.49	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	97
2.53.162.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	54
46.19.85.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	52
2.53.57.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	42
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	30
2.53.175.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	20
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	12
46.19.85.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
46.19.85.89	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	8
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	8
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.154.19.5	Block	7
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	6
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	5
176.13.7.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
109.253.131.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.147.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	3
37.26.148.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.55.163.142	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
2.53.41.73	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
81.218.70.243	Israel	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.mag.idf.il/images/trans.gif	Block	3
109.253.192.184	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.21.242	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
72.82.254.23	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	2
109.253.144.84	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.109	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
185.3.147.181	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
141.212.122.161	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
46.19.85.213	Israel	147.237.77.216	dover.idf.il	Distributed Abnormally Long Request	Block	1
212.199.244.112	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/requestpayslipexplanation.aspx	None	1
194.28.115.230	Netherlands	147.237.77.235	sviva.idf.il	Unauthorized URL Access to www.hagnas.atal.idf.il/hnap1/	Block	1
176.13.1.248	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/1340-he/navi.aspx	Block	1
82.80.80.33	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/scriptresource.axd	Block	1
110.89.60.108	China	147.237.77.176	matpash.idf.il	Distributed Unauthorized HTTP Method	Block	1
46.19.85.51	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
212.199.198.113	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.95.208.20	Israel	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
192.116.94.110	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/894-he/nakhal.aspx	Block	1
149.88.195.82	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/	Block	1
79.183.222.21	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl09 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
46.19.85.213	Israel	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	1
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	1
207.46.13.94	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/yohalan/main/main.asp	Block	1
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
66.249.75.118	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.75.118	Block	1

04-20-2016-10:04:02 to 04-20-2016-11:04:02