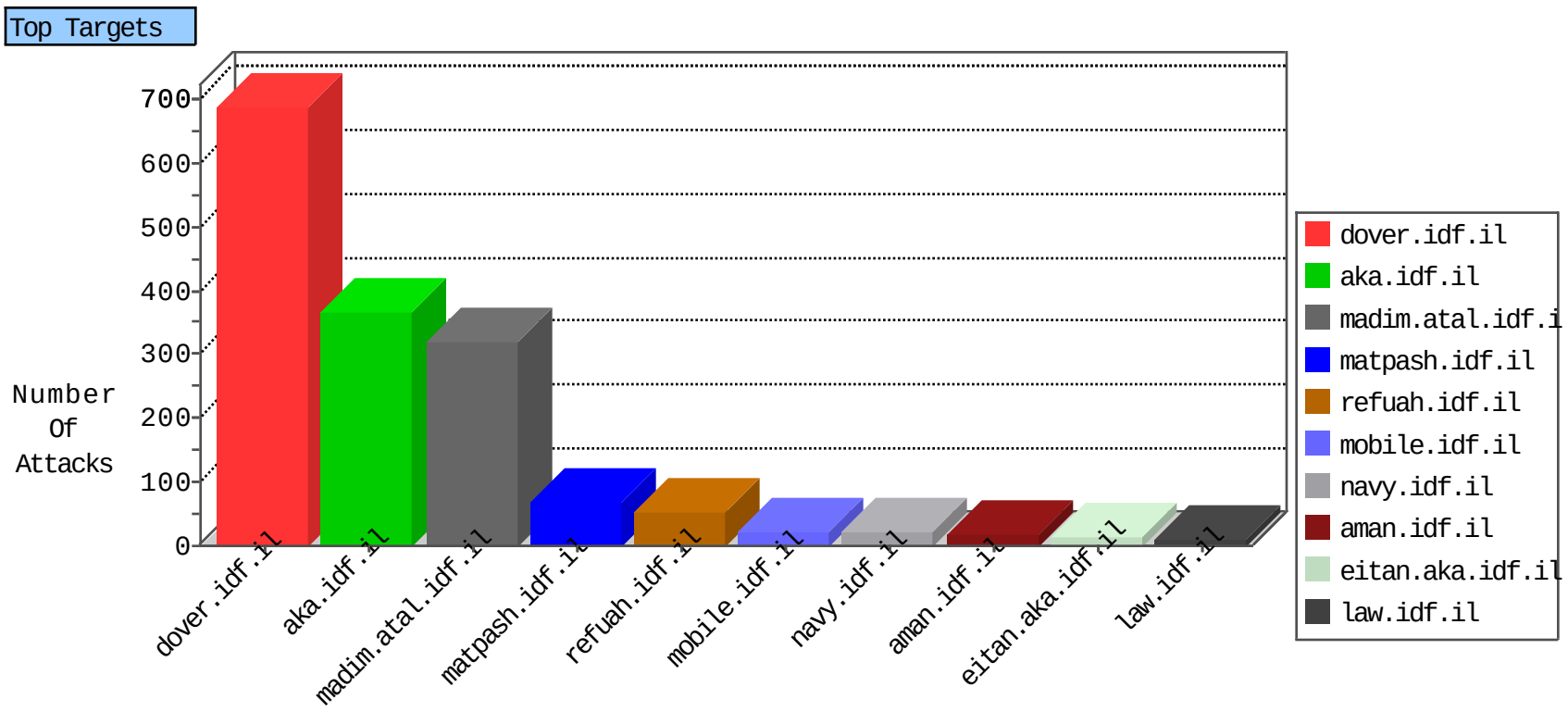
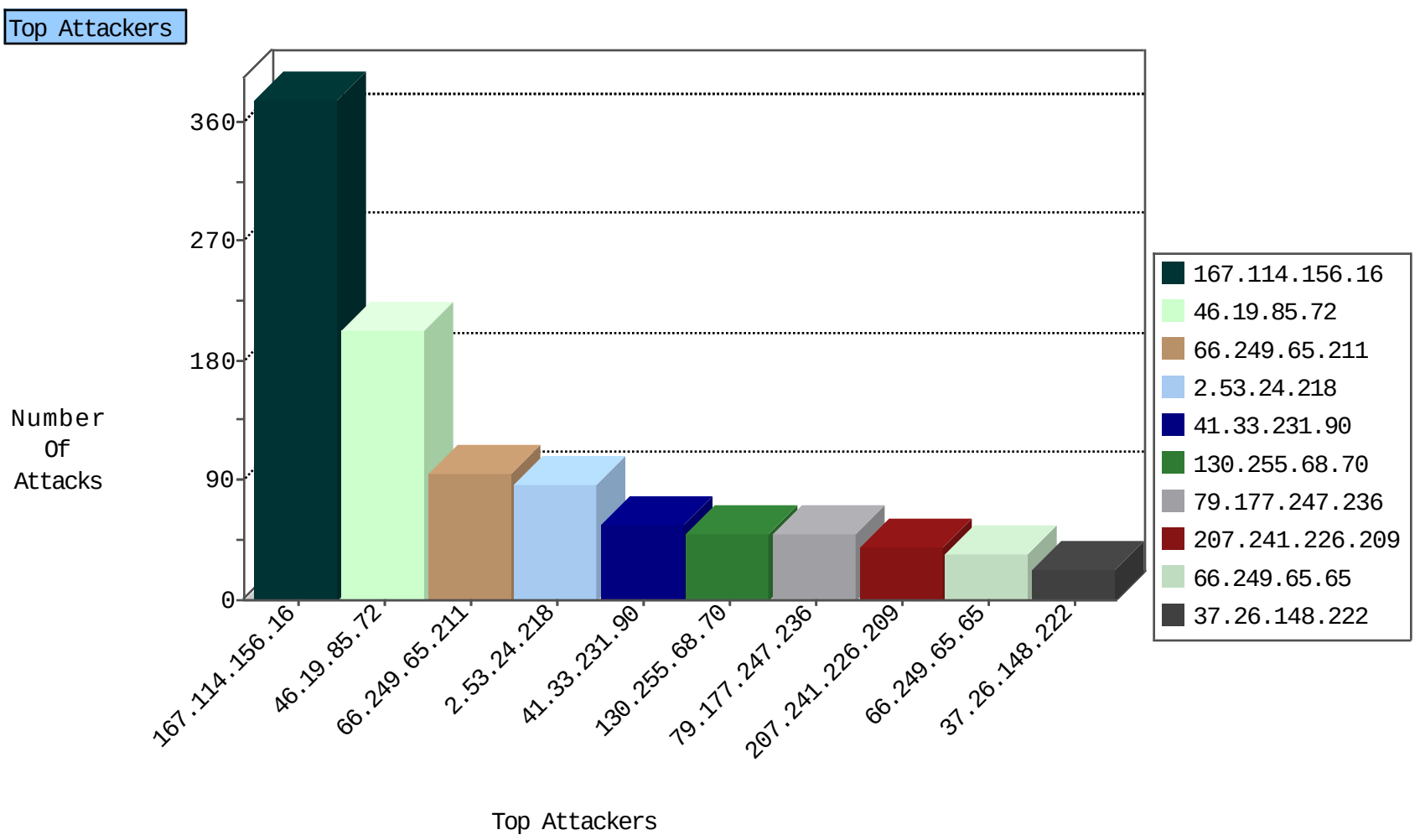
04-21-2016-20:04:08 to 04-21-2016-21:04:08

IDF Under Attack
Daily Report

Top Targets



Top Attackers



04-21-2016-20:04:08 to 04-21-2016-21:04:08

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	15665
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	4348
109.186.63.192	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	205
79.179.164.162	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	105
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	1
115.193.15.11	China	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
94.102.52.10	Netherlands	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
94.102.52.10	Netherlands	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1

04-21-2016-20:04:08 to 04-21-2016-21:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-21-2016-20:04:08 to 04-21-2016-21:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
188.138.25.228	147.237.8.24	France	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	3
100.38.47.218	147.237.76.30	United States	himush.idf.il	ET SCAN Potential SSH Scan	2
100.38.47.218	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN Potential SSH Scan	2
188.214.249.151	147.237.77.216	Romania	dover.idf.il	Xenu Link Sleuth User Agent	2
100.38.47.218	147.237.76.201	United States	e.atal.idf.il	ET SCAN Potential SSH Scan	2
100.38.47.218	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN Potential SSH Scan	2
100.38.47.218	147.237.76.44	United States	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
188.138.25.228	147.237.8.24	France	e.lifestyle.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
100.38.47.218	147.237.76.34	United States	yohalan.idf.il	ET SCAN Potential SSH Scan	1
180.153.151.102	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.8.46	Ukraine	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
151.80.82.44	147.237.76.30	France	himush.idf.il	ET SCAN NMAP -sS window 1024	1
23.96.109.87	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 4096	1
100.38.47.218	147.237.76.197	United States	e.himush.idf.il	ET SCAN Potential SSH Scan	1
100.38.47.218	147.237.76.176	United States	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
203.197.205.118	147.237.0.15	India	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
100.38.47.218	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
100.38.47.218	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
188.138.25.228	147.237.8.24	France	e.lifestyle.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
100.38.47.218	147.237.76.31	United States	nakchal.idf.il	ET SCAN Potential SSH Scan	1
180.153.151.102	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.8.46	Ukraine	e.chinuch.idf.il	ET SCAN NMAP -sS window 4096	1
180.97.106.162	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
85.131.208.140	147.237.76.202	Germany	e.halag.idf.il	ET SCAN Potential SSH Scan	1
23.96.109.87	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 3072	1
100.38.47.218	147.237.76.196	United States	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
100.38.47.218	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1

04-21-2016-20:04:08 to 04-21-2016-21:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.65.211	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	93
130.255.68.70	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	49
79.177.247.236	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	49
207.241.226.209	United States	147.237.72.166	aka.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	39
66.249.65.65	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	33
213.57.38.16	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
213.8.204.37	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
198.58.103.115	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
87.70.52.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
208.181.121.213	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
2.55.0.8	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
37.26.148.222	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
94.230.86.245	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
109.65.143.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.65.172.182	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
79.176.82.150	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	7
46.19.85.155	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.180	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
66.249.64.188	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
8.37.227.81	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.180	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.228.243.87	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.246.130.111	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
80.246.139.185	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
8.37.227.69	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
15.65.244.12	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
79.181.129.17	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
79.176.30.78	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
84.108.240.153	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.26.148.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
84.228.243.87	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
84.108.240.153	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
8.37.227.81	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	4
94.143.60.212	Russian Federation	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
79.176.30.78	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
65.55.210.58	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.163	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.53.24.218	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.164.162	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
89.138.53.153	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.56.156	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
23.97.209.164	Netherlands	147.237.0.15	kosher-kravi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	3

04-21-2016-20:04:08 to 04-21-2016-21:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.72	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	203
2.53.24.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	83
2.53.8.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
176.13.12.13	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
109.253.157.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
164.138.116.29	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.121.128.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.65.225	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
52.87.211.192	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
109.253.150.101	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
78.137.15.204	Ukraine	147.237.77.74	law.idf.il	Parameter Type Violation InfoCenterItem in www.law.idf.il/templates/getfile/getfile.aspx	Block	1
66.249.65.211	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.65.211	Block	1
197.49.72.34	Egypt	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
85.65.197.197	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.65.231	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
66.249.64.3	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/masaiyot04112010.aspx	Block	1
79.177.247.236	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
66.249.65.211	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/main/home/default.aspx	None	1
23.97.209.164	Netherlands	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to 147.237.0.15/	Block	1
207.46.13.98	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/5/109335.pdf¦'¦'½¿¦'½¿¦'¦'½¿¦'½¿¦'-•'½¿	Block	1
95.35.146.236	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
68.180.229.89	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	1
80.246.139.185	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.65.211	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/navy/navy/terms.aspx	None	1
213.8.204.37	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
105.105.127.175	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
68.180.230.45	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
66.249.65.65	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/yohalan.	Block	1
82.166.119.170	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/general/mobile	Block	1
66.249.65.224	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
213.57.38.16	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
109.253.144.251	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
78.137.15.204	Ukraine	147.237.77.74	law.idf.il	Parameter Type Violation FileName in www.law.idf.il/templates/getfile/getfile.aspx	Block	1
66.249.65.65	Israel	147.237.72.166	aka.idf.il	Unknown Parameter newsItem in www.aka.idf.il/megurim/news/	None	1
197.49.72.34	Egypt	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
84.108.240.153	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1

04-21-2016-20:04:08 to 04-21-2016-21:04:08