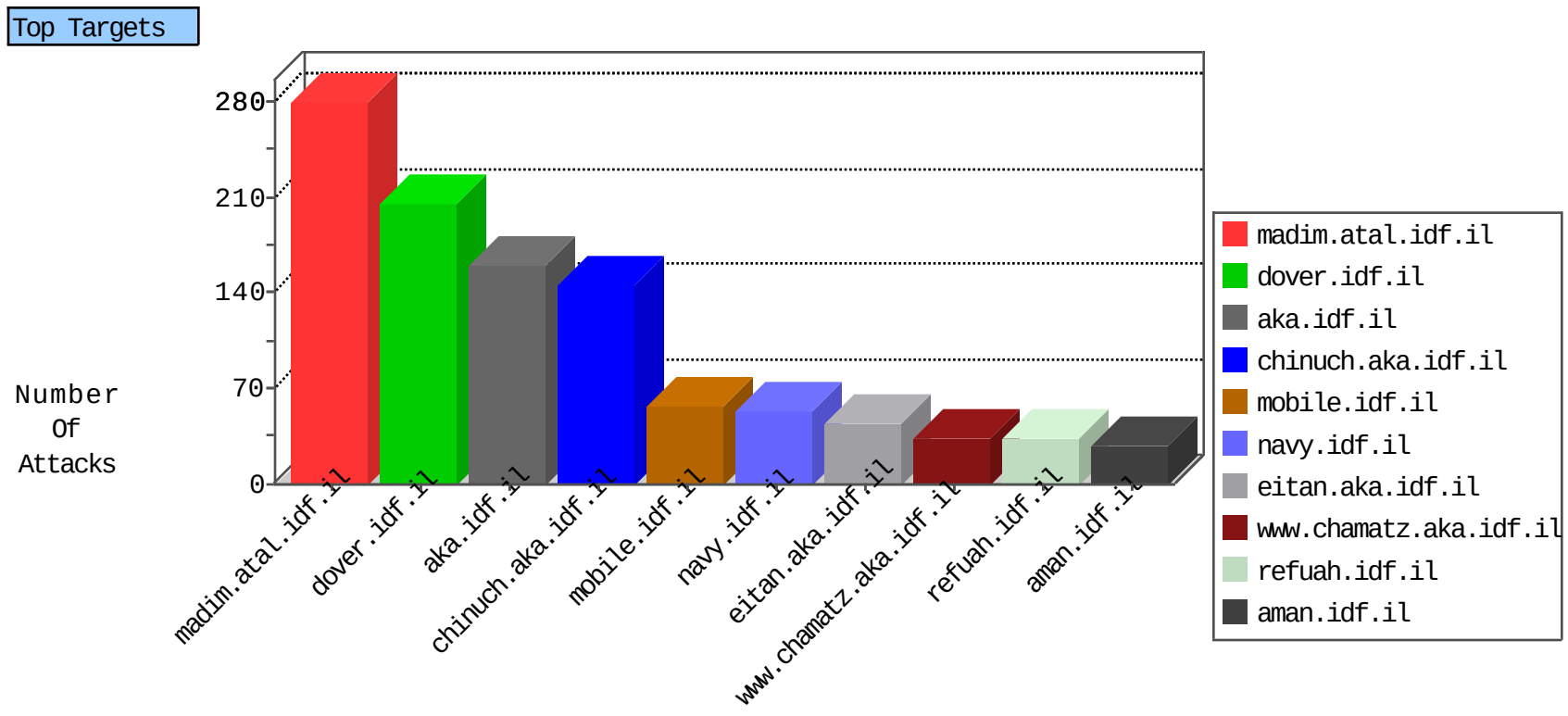
09-27-2016-21:04:08 to 09-27-2016-22:04:08

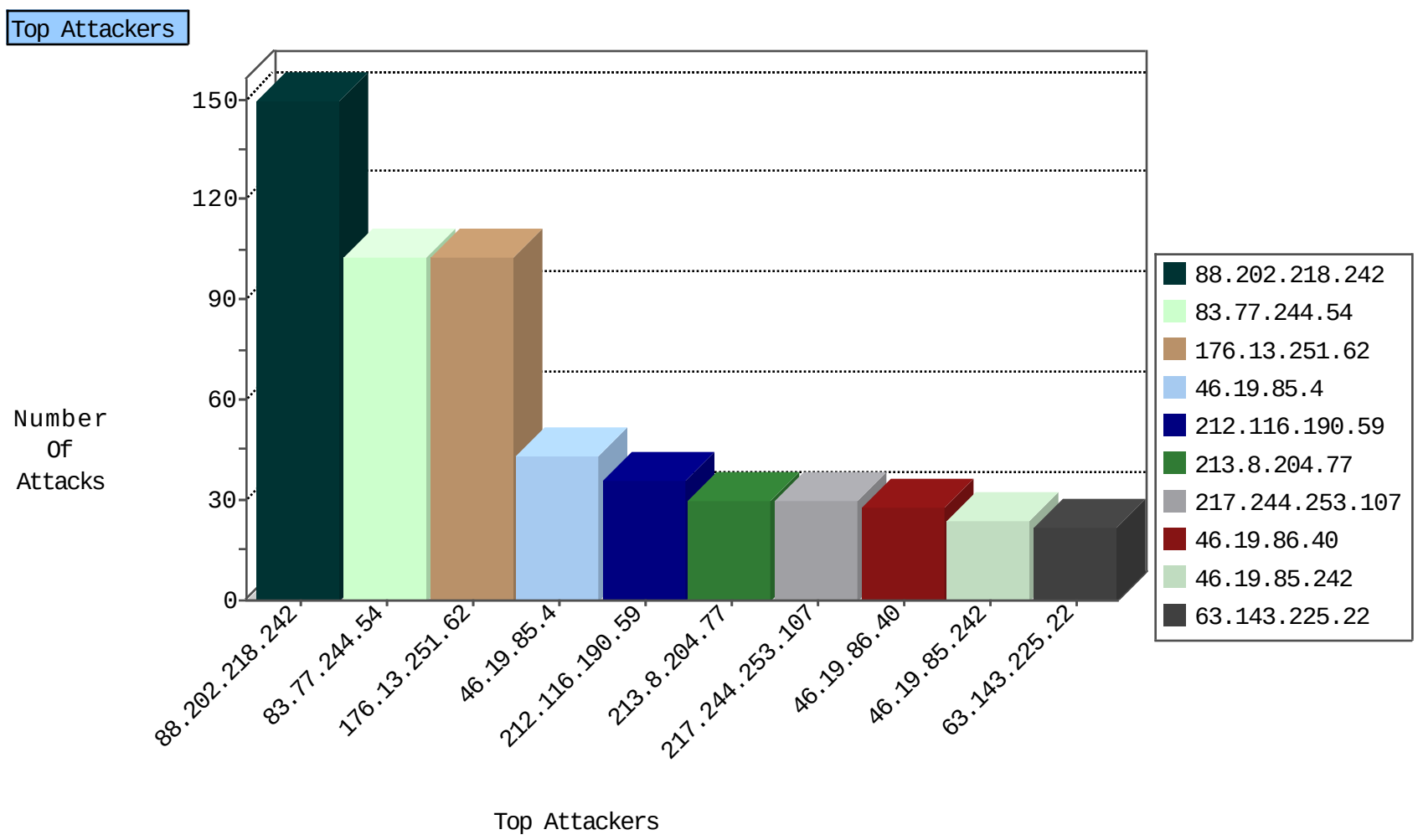
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

09-27-2016-21:04:08 to 09-27-2016-22:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.120.126.32	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
176.13.232.229	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
46.19.86.58	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
77.138.52.97	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
79.179.56.139	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
212.92.127.172	Russian Federation	147.237.0.35	akaws.idf.il	Frk_Under_Attack_Con_Http	drop	1
212.92.127.172	Russian Federation	147.237.0.35	akaws.idf.il	Frk_Purple_Con_Limit_Http	drop	1
79.181.240.150	Israel	147.237.72.156	aman.idf.il	Black List	drop	1

09-27-2016-21:04:08 to 09-27-2016-22:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.189.190.238	Germany	147.237.77.170	maarachot.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
62.212.73.211	Netherlands	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3
94.154.239.69	Ukraine	147.237.76.42	refuah.idf.il	C1000074: HTTP: majestic bot	Permit	2
94.154.239.69	Ukraine	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	2
94.154.239.69	Ukraine	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
123.126.113.101	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1
5.189.190.238	Germany	147.237.77.170	maarachot.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
94.154.239.69	Ukraine	147.237.76.200	eitan.aka.idf.il	C1000074: HTTP: majestic bot	Permit	1
94.154.239.69	Ukraine	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	1
123.125.125.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

09-27-2016-21:04:08 to 09-27-2016-22:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
87.68.26.174	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.87.109.253	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1
79.183.97.188	147.237.76.86	Israel	navy.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
218.87.109.253	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	147.237.77.74	China	law.idf.il	ET SCAN NMAP -sS window 1024	1
218.87.109.253	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	1
46.161.40.17	147.237.77.226	Russian Federation	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
218.87.109.253	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
41.39.177.14	147.237.77.212	Egypt	e.dover.idf.il	ET SCAN NMAP -sS window 2048	1
218.87.109.253	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
31.168.104.195	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	1
163.172.169.150	147.237.76.86	United Kingdom	navy.idf.il	ET SCAN NMAP -sS window 1024	1
139.59.28.44	147.237.77.226	Singapore	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
95.71.127.188	147.237.77.170	Russian Federation	maarachot.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
86.121.105.226	147.237.72.156	Romania	aman.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
218.87.109.253	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
66.249.76.117	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
218.87.109.253	147.237.77.179	China	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
46.161.40.17	147.237.77.243	Russian Federation	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
218.87.109.253	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
41.39.177.14	147.237.77.212	Egypt	e.dover.idf.il	ET SCAN NMAP -sS window 4096	1
218.87.109.253	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
41.39.177.14	147.237.77.212	Egypt	e.dover.idf.il	ET SCAN NMAP -f -sS	1
163.172.169.150	147.237.76.201	United Kingdom	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
5.189.190.238	147.237.77.170	Germany	maarachot.idf.il	ET WEB_SERVER Muieblackcat scanner	1
163.172.169.150	147.237.76.42	United Kingdom	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
109.60.153.178	147.237.8.50	Russian Federation	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1

09-27-2016-21:04:08 to 09-27-2016-22:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.116.190.59	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
217.244.253.107	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
213.8.204.77	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
83.77.244.54	Switzerland	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	26
83.77.244.54	Switzerland	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	25
46.19.85.4	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	24
83.77.244.54	Switzerland	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	22
63.143.225.22	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
83.77.244.54	Switzerland	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	20
46.19.85.4	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	19
31.13.167.141	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
85.250.122.216	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
79.180.230.182	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
83.77.244.54	Switzerland	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
188.120.154.7	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.36	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
46.19.86.40	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.86.40	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
178.216.76.98	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.165	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
176.13.15.178	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.40	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.242	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.242	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.120.126.32	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.40	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
141.226.218.4	Israel	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.242	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.29	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
5.144.63.5	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.242	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
202.83.120.30	Indonesia	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
202.83.120.30	Indonesia	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	5
84.108.20.61	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
95.35.135.80	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
109.253.156.76	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.113	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
31.154.81.20	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
2.55.55.164	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.85.113	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
77.138.146.46	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
85.130.234.154	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.19.85.36	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
66.249.64.148	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.110	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
188.120.148.45	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.26.149.149	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.142	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
85.130.234.120	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3

09-27-2016-21:04:08 to 09-27-2016-22:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
88.202.218.242	United Kingdom	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	150
176.13.251.62	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	103
2.53.57.46	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
46.19.86.221	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
87.70.241.253	Israel	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	4
2.55.167.142	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 2.55.167.142	Block	3
37.142.224.121	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.55.167.142	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	3
31.154.81.21	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
81.18.206.13	Poland	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	Block	2
89.139.177.4	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
77.139.69.119	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	2
66.249.69.14	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	2
107.77.161.3	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/haredim/maslulimlist.aspx	Block	2
79.183.11.148	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.253.197.25	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
77.125.35.208	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
180.76.15.33	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/ui/i18n/jquery-ui-i18n.js	Block	1
66.102.6.21	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
37.26.148.193	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
79.180.230.182	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
141.226.161.53	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.108.20.197	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
77.138.185.180	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	Block	1
207.46.13.176	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/sachar/faq.aspx	None	1
66.102.9.2	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
79.181.62.217	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.76.101	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/m/	Block	1
176.13.15.178	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
46.116.93.28	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.241.215.219	Netherlands	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
213.8.204.38	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.64.141	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/templates/templatecontrols/news/sip_storage/files/7/1437.pdf/	Block	1
46.19.85.137	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	1
93.172.216.173	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.181.235.199	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
66.249.76.117	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
46.117.232.79	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/tikshuv/site/templates/controller.asp	Block	1
85.65.220.142	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
5.29.213.220	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
77.139.237.125	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	Block	1
213.8.204.64	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.85.137	Israel	147.237.77.216	dover.idf.il	Malformed URL en-us,en;q=0.8,he;q=0.6	Block	1
77.124.27.32	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012ources/images/innerpage/goback.gif	Block	1
176.195.174.8	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
46.120.242.148	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtContent in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1
77.139.237.125	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
66.249.69.127	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9688-he/refuah.aspx	Block	1
217.158.205.113	United Kingdom	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1

09-27-2016-21:04:08 to 09-27-2016-22:04:08