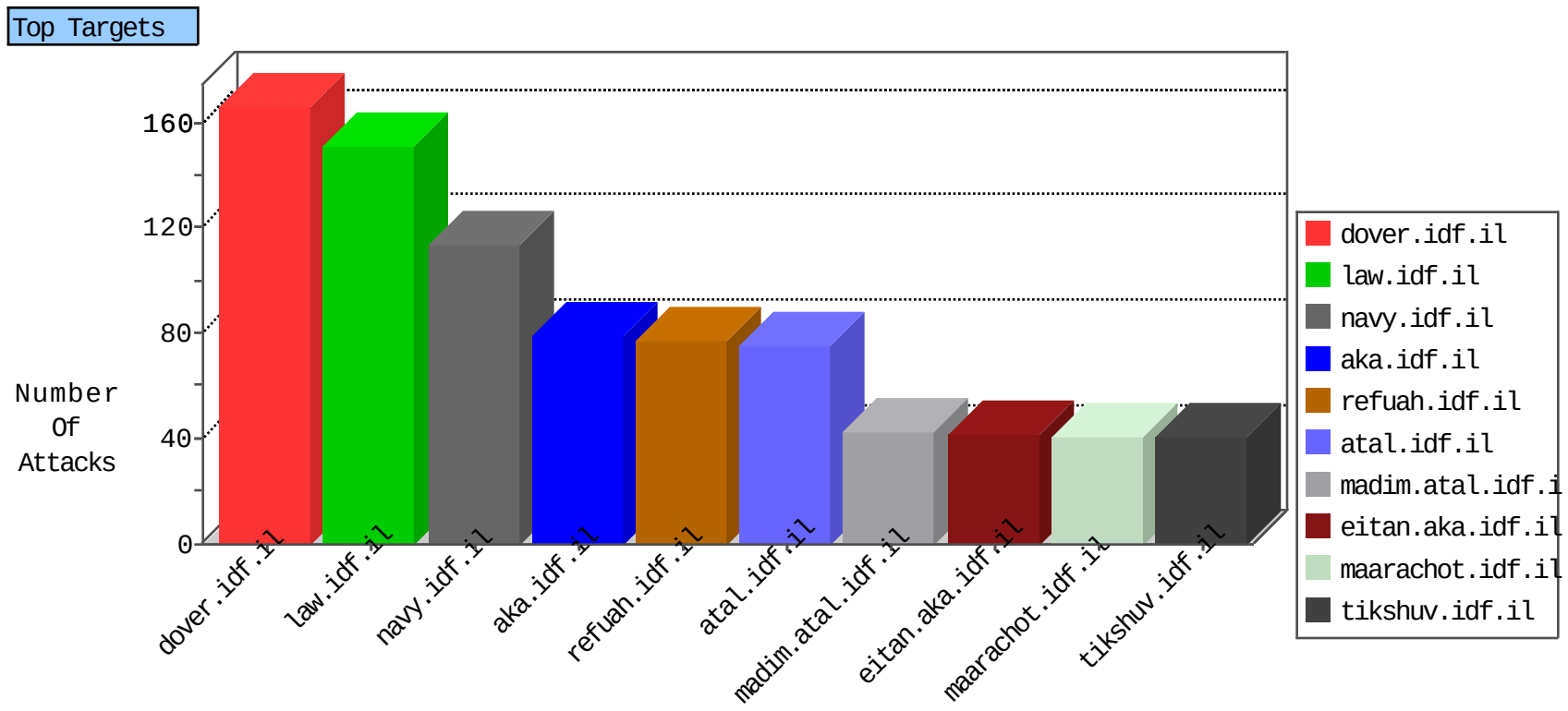
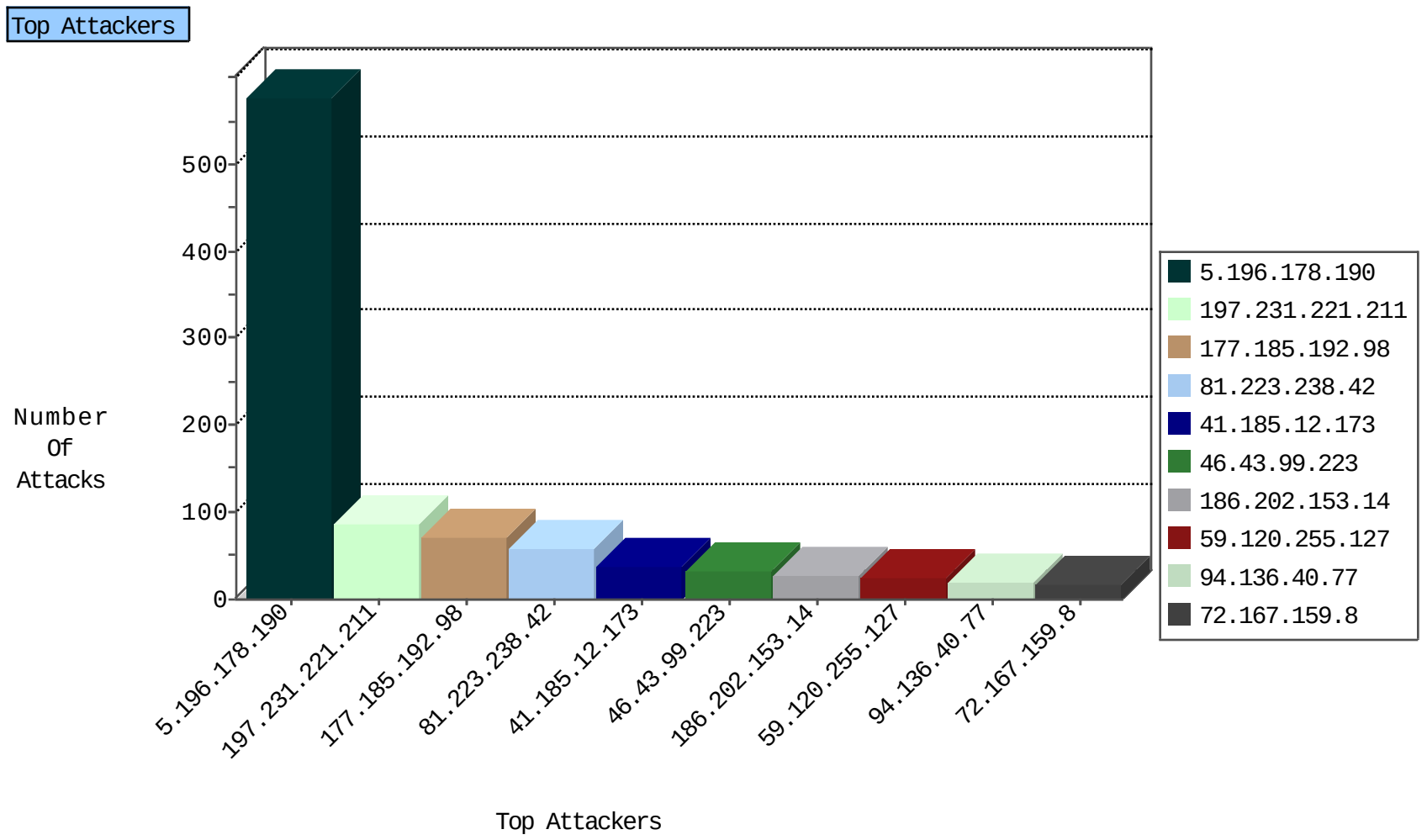
09-12-2016-02:04:01 to 09-12-2016-03:04:01

IDF Under Attack
Daily Report

Top Targets



Top Attackers



09-12-2016-02:04:01 to 09-12-2016-03:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
131.247.2.241	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
129.10.120.193	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
204.85.191.11	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
87.68.49.168	Israel	147.237.72.166	aka.idf.il	Black List	drop	2
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
164.107.127.12	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
139.78.141.243	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
129.32.84.160	United States	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	2
134.197.113.3	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.93.229.138	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
115.47.12.162	China	147.237.0.16	my-kosher-kravi.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
198.133.224.147	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
134.197.113.3	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.114	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.217.77.4	New Zealand	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
200.19.159.35	Brazil	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
139.78.141.243	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.42.142.45	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-12-2016-02:04:01 to 09-12-2016-03:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
94.136.40.77	United Kingdom	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	12
81.223.238.42	Austria	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	11
41.185.12.173	South Africa	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
177.185.192.98	Brazil	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
69.10.156.44	Canada	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
91.219.122.2	Poland	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
72.167.131.22	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
50.77.136.81	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
210.169.203.81	Japan	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
177.185.192.98	Brazil	147.237.76.86	navy.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
212.147.60.96	Switzerland	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
81.223.238.42	Austria	147.237.77.216	dover.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
177.185.192.98	Brazil	147.237.76.86	navy.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
59.120.255.127	Taiwan	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
41.185.12.173	South Africa	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	2
216.119.125.34	United States	147.237.77.216	dover.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	2
210.169.203.81	Japan	147.237.76.86	navy.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	2
51.255.51.25	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
216.119.125.34	United States	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	2
81.223.238.42	Austria	147.237.77.216	dover.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	1

09-12-2016-02:04:01 to 09-12-2016-03:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
177.185.192.98	147.237.76.86	Brazil	navy.idf.il	SQL Injection - Select From	54
81.223.238.42	147.237.77.216	Austria	dover.idf.il	SQL Injection - Select From	40
41.185.12.173	147.237.76.42	South Africa	refuah.idf.il	SQL Injection - Select From	28
59.120.255.127	147.237.77.74	Taiwan	law.idf.il	SQL Injection - Select From	18
94.136.40.77	147.237.77.74	United Kingdom	law.idf.il	SQL Injection - Select From	8
69.10.156.44	147.237.77.74	Canada	law.idf.il	SQL Injection - Select From	8
50.77.136.81	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
91.219.122.2	147.237.77.74	Poland	law.idf.il	SQL Injection - Select From	8
72.167.131.22	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	6
66.249.66.12	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	6
212.147.60.96	147.237.77.74	Switzerland	law.idf.il	SQL Injection - Select From	5
46.120.122.219	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	3
46.120.122.219	147.237.76.147	Israel	chinuch.aka.idf.il	Xenu Link Sleuth User Agent	2
93.174.91.29	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
37.48.77.131	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
191.96.249.18	147.237.76.176	Chile	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
163.172.129.15	147.237.76.200	United Kingdom	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
163.172.129.15	147.237.76.44	United Kingdom	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
50.245.143.138	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN NMAP -sS window 2048	1
115.47.12.162	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
103.207.39.82	147.237.76.197	Vietnam	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
46.227.67.158	147.237.76.42	Sweden	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
93.174.91.29	147.237.76.197	Netherlands	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
45.79.103.178	147.237.72.167	United States	ishurim.aka.idf.il	WEB-MISC Chunked-Encoding transfer attempt	1
37.48.77.131	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN Potential SSH Scan	1
210.169.203.81	147.237.76.86	Japan	navy.idf.il	SQL Injection - Select From	1
66.249.66.238	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
37.48.77.131	147.237.8.14	Netherlands	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
66.249.65.19	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	1
163.172.129.15	147.237.76.197	United Kingdom	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.200.137	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
116.71.128.85	147.237.72.217	Pakistan	e.idf.il	ET SCAN NMAP -sS window 1024	1
50.245.143.138	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN NMAP -f -sS	1
114.40.234.49	147.237.77.227	Taiwan	e.hamaz.idf.il	GPL SCAN PING CyberKit 2.2 Windows	1
46.227.67.158	147.237.76.147	Sweden	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1

09-12-2016-02:04:01 to 09-12-2016-03:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.196.178.190	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	30
5.196.178.190	France	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	29
5.196.178.190	France	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	28
46.43.99.223	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
5.196.178.190	France	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	27
5.196.178.190	France	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	27
5.196.178.190	France	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	27
5.196.178.190	France	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	27
5.196.178.190	France	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	27
5.196.178.190	France	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	27
5.196.178.190	France	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	26
5.196.178.190	France	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	26
5.196.178.190	France	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	26
5.196.178.190	France	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	26
5.196.178.190	France	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	26
5.196.178.190	France	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	25
5.196.178.190	France	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	25
5.196.178.190	France	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	25
5.196.178.190	France	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	25
5.196.178.190	France	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	24
5.196.178.190	France	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	24
5.196.178.190	France	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	24
5.196.178.190	France	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	24
72.167.159.8	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	18
195.74.38.14	Sweden	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
74.208.192.137	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
158.85.253.245	United States	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	6
66.249.76.67	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
158.85.253.245	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	6
197.231.221.211	Liberia	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
197.231.221.211	Liberia	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.43.99.223	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
197.231.221.211	Liberia	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
186.202.153.14	Brazil	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
197.231.221.211	Liberia	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
197.231.221.211	Liberia	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
197.231.221.211	Liberia	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
113.210.188.153	Malaysia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
186.202.153.14	Brazil	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
186.202.153.14	Brazil	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
197.231.221.211	Liberia	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
197.231.221.211	Liberia	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
197.231.221.211	Liberia	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
192.169.7.223	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
197.231.221.211	Liberia	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
197.231.221.211	Liberia	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
197.231.221.211	Liberia	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
128.232.110.28	United Kingdom	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
197.231.221.211	Liberia	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2

09-12-2016-02:04:01 to 09-12-2016-03:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
83.220.236.132	Russian Federation	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.120.122.219	Block	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1086-he/dover.aspx	Block	1
109.253.216.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
46.120.122.219	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized Method HEAD for www.chinuch.aka.idf.il/	None	1
66.249.79.59	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.9	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
66.249.66.111	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/m/main/giyus/general.aspx	Block	1
68.180.229.181	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-he/cogat.aspx	Block	1
66.249.66.174	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/8/71518.pdf	Block	1
68.180.229.181	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1927-he/cogat.aspx	Block	1
46.4.74.42	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/iturim/asp/displayonesoldier.asp	Block	1
66.249.66.176	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1

09-12-2016-02:04:01 to 09-12-2016-03:04:01