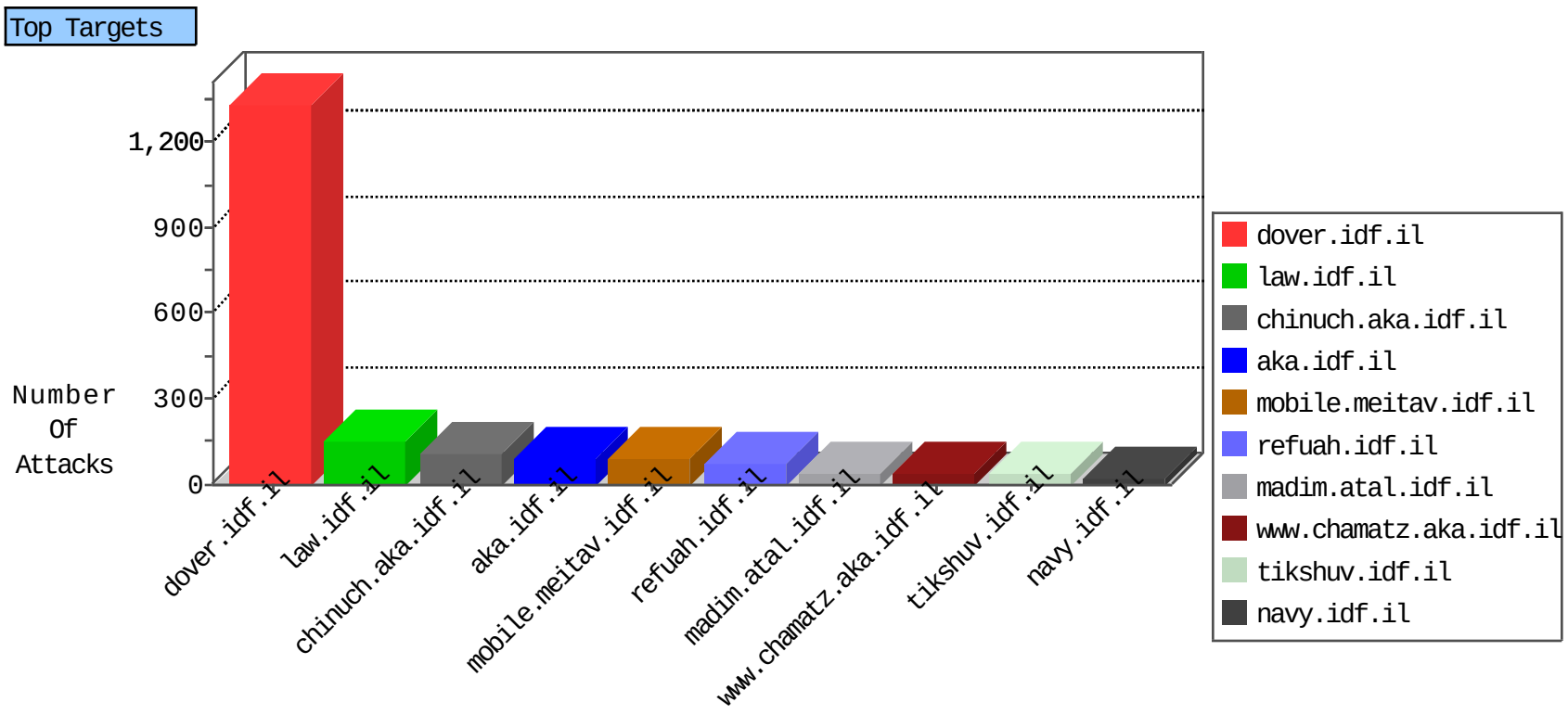
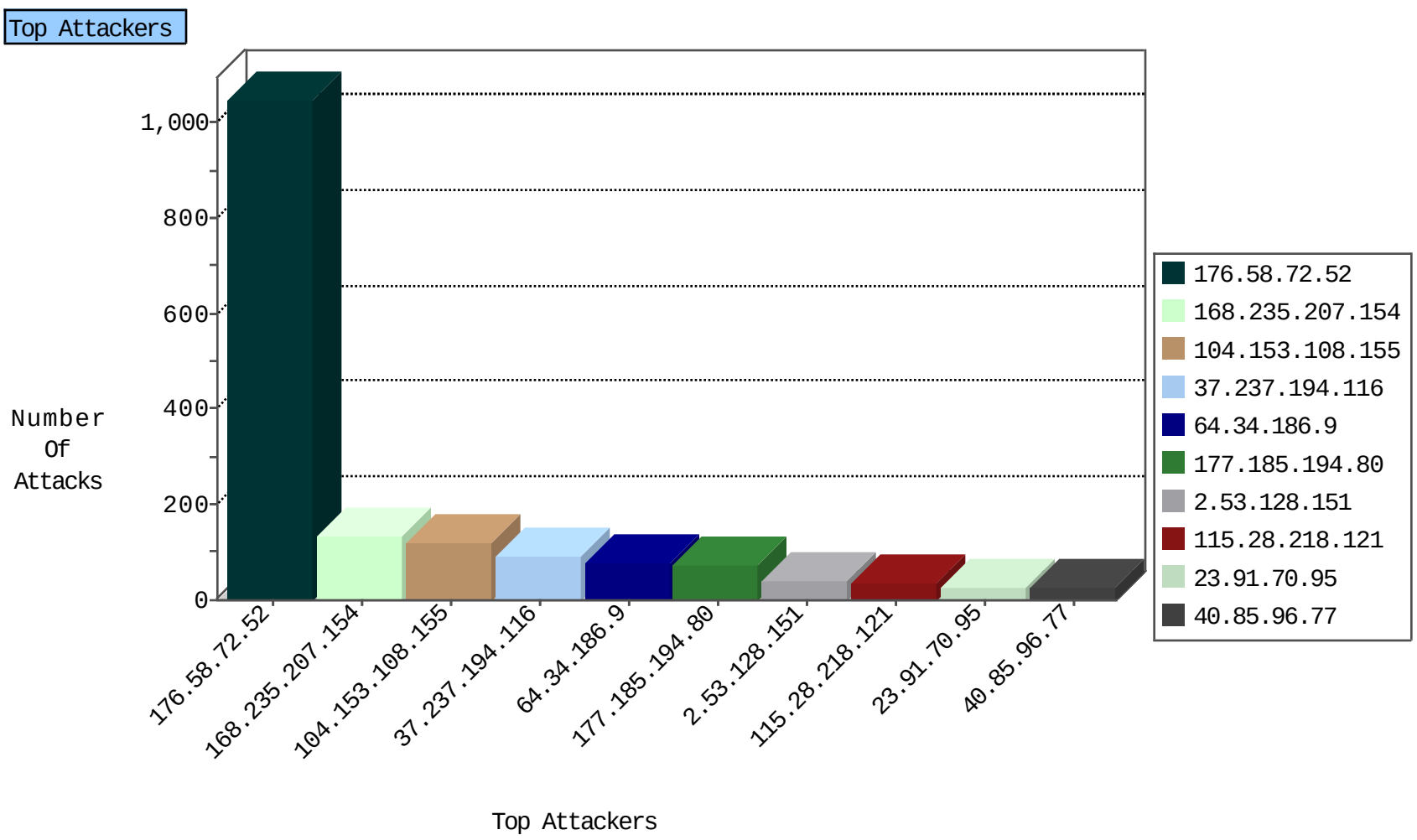
09-25-2016-03:04:01 to 09-25-2016-04:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-25-2016-03:04:01 to 09-25-2016-04:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
168.235.207.154	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
168.235.207.154	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	3
222.186.34.141	China	147.237.76.42	refuah.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
168.235.207.154	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
191.96.249.37	Chile	147.237.76.197	e.himush.idf.il	Black List	drop	1
31.204.128.22	Netherlands	147.237.76.176	test.ncore.idf.il	Black List	drop	1
192.249.66.247	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
45.32.193.80	Netherlands	147.237.76.197	e.himush.idf.il	Black List	drop	1
45.32.195.0	Netherlands	147.237.76.38	e.e.meitav.idf.il	Black List	drop	1
104.238.147.7	United States	147.237.76.31	nakchal.idf.il	Black List	drop	1

09-25-2016-03:04:01 to 09-25-2016-04:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
64.34.186.9	United States	147.237.0.34	tikshuv.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
202.124.242.10	Australia	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	12
64.34.186.9	United States	147.237.77.226	www.chamatz.aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
166.62.42.29	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
91.219.122.4	Poland	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
40.85.96.77	Ireland	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
177.185.194.80	Brazil	147.237.76.42	refuah.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
64.34.186.9	United States	147.237.77.226	www.chamatz.aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
23.91.70.95	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
209.147.117.51	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
50.63.196.35	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
177.185.194.80	Brazil	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
50.63.197.140	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
177.185.194.80	Brazil	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
74.208.154.12	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
24.86.161.214	Canada	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
64.34.186.9	United States	147.237.0.34	tikshuv.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
184.172.106.100	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
91.219.122.2	Poland	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
40.85.96.77	Ireland	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
23.91.70.95	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	5
144.76.4.148	Germany	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	2
144.76.8.132	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
144.76.8.132	Germany	147.237.76.147	chinuch.aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
23.91.70.95	United States	147.237.77.74	law.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	1

09-25-2016-03:04:01 to 09-25-2016-04:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
177.185.194.80	147.237.76.42	Brazil	refuah.idf.il	SQL Injection - Select From	54
64.34.186.9	147.237.77.226	United States	www.chamatz.aka.idf.il	SQL Injection - Select From	20
64.34.186.9	147.237.0.34	United States	tikshuv.idf.il	SQL Injection - Select From	20
184.172.106.100	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	18
209.147.117.51	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	18
40.85.96.77	147.237.77.74	Ireland	law.idf.il	SQL Injection - Select From	14
23.91.70.95	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	14
202.124.242.10	147.237.72.166	Australia	aka.idf.il	SQL Injection - Select From	12
50.63.197.140	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
166.62.42.29	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
91.219.122.4	147.237.77.74	Poland	law.idf.il	SQL Injection - Select From	8
50.63.196.35	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
24.86.161.214	147.237.77.74	Canada	law.idf.il	SQL Injection - Select From	8
91.219.122.2	147.237.72.166	Poland	aka.idf.il	SQL Injection - Select From	8
74.208.154.12	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	8
91.121.220.181	147.237.72.166	France	aka.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	5
183.60.48.25	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
47.23.146.194	147.237.76.31	United States	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
212.159.137.130	147.237.77.61	United Kingdom	e.cogat.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
125.77.28.26	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1
106.51.226.59	147.237.77.233	India	atal.idf.il	ET SCAN NMAP -sS window 2048	1
201.73.83.242	147.237.76.31	Brazil	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
194.60.242.6	147.237.77.61	Ukraine	e.cogat.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
185.129.148.230	147.237.77.170	Latvia	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
84.94.198.81	147.237.76.201	Israel	e.atal.idf.il	ET SCAN NMAP -sS window 3072	1
66.102.6.18	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
163.172.129.15	147.237.72.166	United Kingdom	aka.idf.il	ET SCAN NMAP -sS window 1024	1
46.161.40.17	147.237.76.31	Russian Federation	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
106.51.226.59	147.237.77.233	India	atal.idf.il	ET SCAN NMAP -sS window 4096	1
201.73.83.242	147.237.76.31	Brazil	nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
106.51.226.59	147.237.77.233	India	atal.idf.il	ET SCAN NMAP -f -sS	1
196.47.173.21	147.237.8.28	Cote D'Ivoire	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 4096	1
5.255.90.133	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
185.129.148.230	147.237.77.227	Latvia	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
84.94.198.81	147.237.76.201	Israel	e.atal.idf.il	ET SCAN NMAP -sS window 4096	1
185.93.185.10	147.237.72.166	Ukraine	aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

09-25-2016-03:04:01 to 09-25-2016-04:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
176.58.72.52	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	787
168.235.207.154	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	106
37.237.194.116	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	90
168.235.207.154	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
104.153.108.155	United States	147.237.76.39	mobile.meitav.idf.i	Bad TCP sequence	Invalid ACK number	monitor	18
104.153.108.155	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
73.73.148.148	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
66.249.69.30	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
104.153.108.155	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	15
104.153.108.155	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	14
104.153.108.155	United States	147.237.76.39	mobile.meitav.idf.i	Bad TCP sequence	SYN retransmit with different sequence	monitor	14
104.153.108.155	United States	147.237.76.39	mobile.meitav.idf.i	Bad TCP sequence	SYN retransmit with different sequence	alert	12
104.153.108.155	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
176.58.72.52	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
104.153.108.155	United States	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
46.133.60.186	Ukraine	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	8
104.153.108.155	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	7
184.168.192.134	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
85.94.76.17	Croatia	147.237.77.74	law.idf.il	drop	SAM rule	drop	6
66.249.69.26	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.58.72.52	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Web Server Enforcement Violation	Anonymous DoSer Denial of Service Tool	reject	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
115.28.218.121	China	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	5
115.28.218.121	China	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	5
115.28.218.121	China	147.237.76.39	mobile.meitav.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
115.28.218.121	China	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
96.224.230.17	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
115.28.218.121	China	147.237.76.39	mobile.meitav.idf.i	Bad TCP sequence	SYN retransmit with different sequence	monitor	3
199.30.24.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
85.190.155.48	Germany	147.237.76.39	mobile.meitav.idf.i	Bad TCP sequence	SYN retransmit with different sequence	monitor	3
85.190.155.48	Germany	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	3
85.190.155.48	Germany	147.237.76.39	mobile.meitav.idf.i	Bad TCP sequence	Invalid ACK number	monitor	3
66.249.76.108	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
106.39.60.184	China	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
79.183.96.191	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
85.190.155.48	Germany	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
115.28.218.121	China	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
85.190.155.48	Germany	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
115.28.218.121	China	147.237.76.39	mobile.meitav.idf.i	Bad TCP sequence	SYN retransmit with different sequence	alert	3
85.190.155.48	Germany	147.237.76.39	mobile.meitav.idf.i	Bad TCP sequence	SYN retransmit with different sequence	alert	2
85.190.155.48	Germany	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	2
176.58.72.52	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
37.76.218.213	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
144.76.8.132	Germany	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	2
142.134.20.232	Canada	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
85.190.155.48	Germany	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
178.20.231.251	Turkey	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	alert	2
144.76.8.132	Germany	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2

09-25-2016-03:04:01 to 09-25-2016-04:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.58.72.52	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 176.58.72.52	Block	245
2.53.128.151	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	40
157.55.39.233	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-18537-he/dover	Block	1
66.249.76.70	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/apple-app-site-association	Block	1
94.249.15.134	Jordan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
54.70.57.110	United States	147.237.72.167	ishurim.aka.idf.i	Unauthorized URL Access to 147.237.72.167/web-console/serverinfo.jsp	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/9/69039.pdf	Block	1
98.138.223.156	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized Method HEAD for www.eitan.aka.idf.il/1103-8363-he/eitan.aspx	None	1
66.249.64.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
185.27.106.169	Israel	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
99.225.105.145	Canada	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/giyus/general/default.asp	Block	1
66.249.69.102	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
185.27.106.169	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/wp-login.php	Block	1
84.108.87.238	Israel	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	1
108.44.36.226	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.75.12	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/2370.jpg	Block	1
84.108.87.238	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/wp-login.php	Block	1

09-25-2016-03:04:01 to 09-25-2016-04:04:01