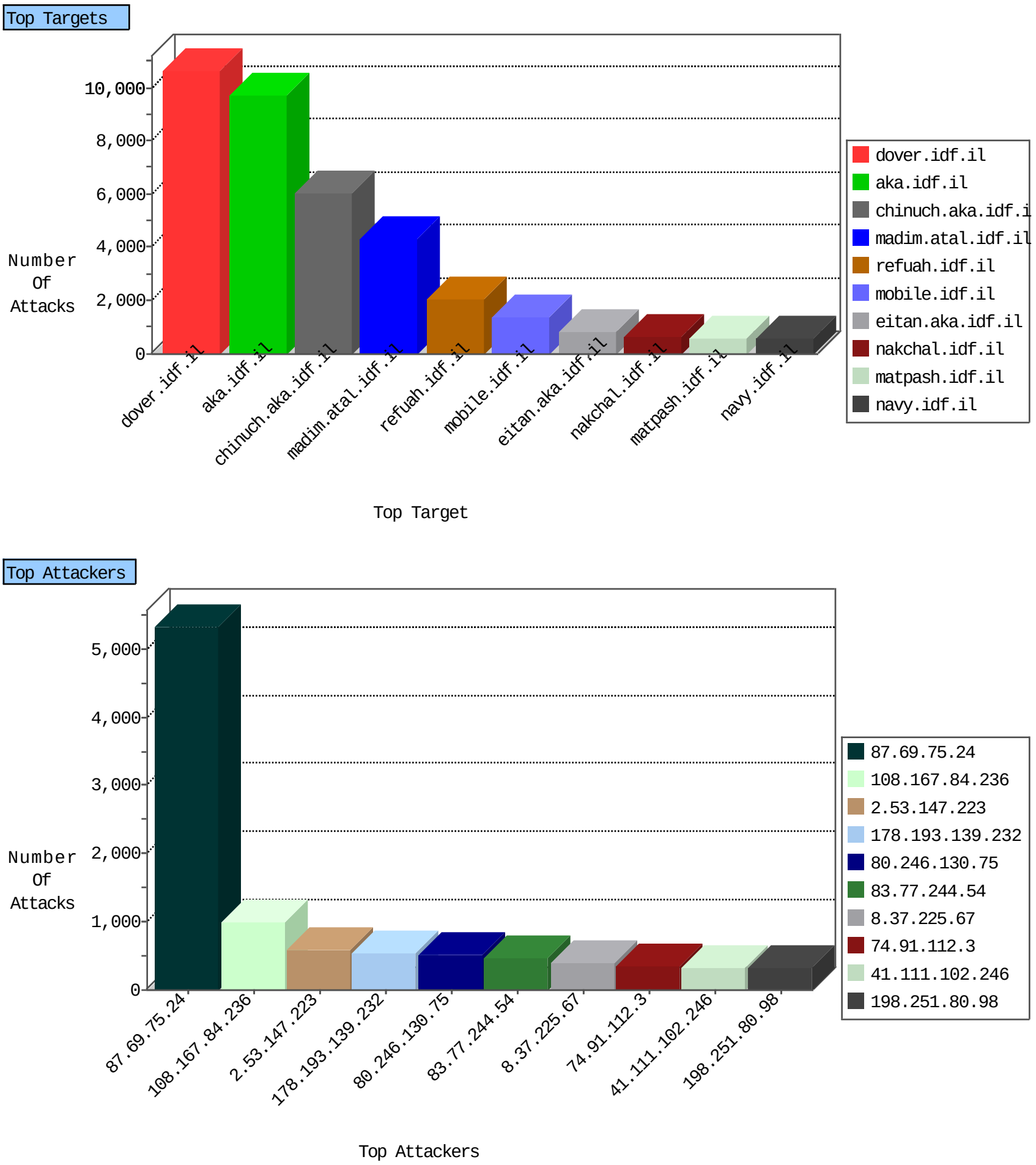
09-27-2016 to 09-28-2016

IDF Under Attack Daily Report



09-27-2016 to 09-28-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
10.3.36.100		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8747
37.26.146.234	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5929
2.55.128.146	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5042
62.219.226.69	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4855
216.172.142.204	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	4006
109.253.141.165	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3434
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3395
176.13.10.187	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3168
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3140
5.102.242.141	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3118
141.0.15.52	Norway	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3013
62.44.134.113	Denmark	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3011
212.179.90.106	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2971
8.37.225.67	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2952
2.53.41.78	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2913
91.227.164.5	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2767
46.19.86.223	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2565
62.0.201.1	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2509
84.111.120.9	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2504
62.90.153.76	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2503
2.55.142.137	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2332
46.19.86.193	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2084
81.218.57.61	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1869
212.25.84.200	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1866
37.46.41.54	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1624
109.253.212.111	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1538
85.130.139.108	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1307
46.19.85.208	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1253
66.249.69.228	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1179
2.53.149.34	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1106
62.0.217.1	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1019
77.138.52.97	France	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	633
68.180.231.57	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	585
79.177.140.120	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	567
46.19.86.173	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	558
2.53.9.139	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	516
109.253.205.29	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	483
132.64.212.159	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	293
46.19.86.24	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	289
176.13.237.102	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	285
138.134.102.15	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	262
79.178.212.124	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	224
85.255.7.155	Poland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	201
37.26.147.245	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	185
2.53.128.24	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	182
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	108
37.26.148.155	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	98
2.53.43.67	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	84
213.57.68.251	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	73
84.108.109.37	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	51

09-27-2016 to 09-28-2016

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
178.203.120.68	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	77
91.121.109.55	France	147.237.76.200	eitan.aka.idf.il	C1000074: HTTP: majestic bot	Permit	52
149.202.48.240	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	35
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	32
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	23
178.203.120.68	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	19
91.121.109.55	France	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	16
149.202.48.240	France	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	14
149.202.48.240	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	11
148.251.190.162	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	8
91.121.109.55	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	8
178.203.120.68	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	6
5.189.190.238	Germany	147.237.0.15	kosher-kravi.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
178.203.120.68	Germany	147.237.76.42	refuah.idf.il	C1000074: HTTP: majestic bot	Permit	5
5.189.190.238	Germany	147.237.77.170	maarachot.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
69.30.213.138	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	5
109.253.211.21	Israel	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	4
69.30.213.138	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3
62.212.73.211	Netherlands	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3
92.238.226.245	United Kingdom	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3
51.254.215.140	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	3
51.254.215.140	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
149.202.48.240	France	147.237.0.34	tikshuv.idf.il	C1000074: HTTP: majestic bot	Permit	2
144.76.30.236	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
94.154.239.69	Ukraine	147.237.76.42	refuah.idf.il	C1000074: HTTP: majestic bot	Permit	2
178.203.120.68	Germany	147.237.76.30	himush.idf.il	C1000074: HTTP: majestic bot	Permit	2
149.202.48.240	France	147.237.77.226	www.chamatz.aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
69.30.213.202	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
148.251.190.162	Germany	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	2
83.149.126.98	Germany	147.237.72.156	aman.idf.il	C1000074: HTTP: majestic bot	Permit	2
149.202.48.240	France	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	2
91.121.109.55	France	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	2
148.251.190.162	Germany	147.237.77.74	law.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
88.198.16.153	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
149.202.48.240	France	147.237.76.200	eitan.aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
68.135.8.175	United States	147.237.77.216	dover.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
75.75.210.162	United States	147.237.77.216	dover.idf.il	10993: HTTP: Morfeus Scanner Scanning Attempt	Block	1
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	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
151.80.31.171	France	147.237.76.31	nakchal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
71.6.146.185	United States	147.237.0.17	m.my-kosher-kravi.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
123.125.125.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1
75.75.210.162	United States	147.237.0.15	kosher-kravi.idf.il	10993: HTTP: Morfeus Scanner Scanning Attempt	Block	1
156.211.51.34	Egypt	147.237.77.216	dover.idf.il	3886: HTTP: Cross Site Scripting in POST Request	Block	1
123.126.113.101	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1
94.154.239.69	Ukraine	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	1
75.75.210.162	United States	147.237.0.19	madim.atal.idf.il	10993: HTTP: Morfeus Scanner Scanning Attempt	Block	1

09-27-2016 to 09-28-2016

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.19.86.207	147.237.77.176	Israel	matpash.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	58
66.102.6.207	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	22
58.218.200.137	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	3
80.246.130.54	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
82.80.196.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	3
109.75.43.41	147.237.72.14	Armenia	dover.idf.il(old)	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	3
84.94.140.177	147.237.77.226	Israel	www.chamatz.aka.idf.il	LOCAL_RULES - HTTP Request with OPTIONS method to a .doc file	3
66.249.93.137	147.237.77.233	Europe	atal.idf.il	ET SCAN NMAP -sA (2)	3
66.249.93.83	147.237.77.216	Europe	dover.idf.il	ET SCAN NMAP -sA (2)	2
91.201.236.50	147.237.76.198	Ukraine	e.yohalan.idf.il	ET SCAN NMAP -sS window 4096	2
79.181.244.133	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
124.8.223.198	147.237.76.39	Taiwan	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	2
58.218.200.137	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	2
82.81.76.144	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	2
121.32.129.130	147.237.76.30	China	himush.idf.il	GPL SCAN nmap TCP	2
37.220.31.10	147.237.77.226	United Kingdom	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	2
194.90.178.37	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
146.200.148.0	147.237.77.74	United Kingdom	law.idf.il	Tehila - Perl LWP with fake user agent	2
66.249.64.160	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
46.183.223.228	147.237.8.50	Latvia	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	2
124.197.95.73	147.237.76.86	Singapore	navy.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
46.183.223.228	147.237.0.16	Latvia	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
124.8.223.198	147.237.76.177	Taiwan	ncore.idf.il	ET SCAN Potential SSH Scan	2
163.172.129.15	147.237.0.200	United Kingdom	m4u.idf.il	ET SCAN NMAP -sS window 1024	2
52.33.211.238	147.237.77.61	United States	e.cogat.idf.il	ET SCAN Potential SSH Scan	2
58.218.200.137	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	2
222.186.56.200	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
213.57.177.33	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
58.218.200.137	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	2
80.246.139.213	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
58.218.200.137	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
146.200.148.0	147.237.77.216	United Kingdom	dover.idf.il	Tehila - Perl LWP with fake user agent	2
80.246.133.48	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
91.201.236.50	147.237.77.121	Ukraine	e.navy.idf.il	ET SCAN NMAP -sS window 3072	2
66.102.9.149	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
163.172.129.15	147.237.76.38	United Kingdom	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
46.116.64.164	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
115.47.12.162	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.76.196	China	e.sviva.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
91.201.236.50	147.237.8.50	Ukraine	e.tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
196.47.173.21	147.237.76.199	Cote D'Ivoire	e.nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
78.129.171.173	147.237.76.86	United Kingdom	navy.idf.il	ET SCAN Potential SSH Scan	1
179.43.144.18	147.237.76.38	Switzerland	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
52.33.211.238	147.237.77.205	United States	prisha.idf.il	ET SCAN Potential SSH Scan	1
139.162.187.89	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 1024	1
40.121.139.43	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
93.172.123.51	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
211.149.222.5	147.237.77.227	China	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
2.53.53.201	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-27-2016 to 09-28-2016

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
108.167.84.236	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	997
87.69.75.24	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	936
80.246.130.75	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	524
8.37.225.67	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	327
66.169.8.29	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	311
75.138.220.53	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	289
75.255.124.13	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	278
41.111.102.246	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	242
148.177.168.117	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	209
8.37.225.186	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	163
27.55.45.165	Thailand	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	150
213.151.52.217	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	148
79.179.15.6	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
5.151.46.12	United Kingdom	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	127
178.193.139.232	Switzerland	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	126
178.193.139.232	Switzerland	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	123
2.53.177.12	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	114
178.193.139.232	Switzerland	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	106
82.145.222.119	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	104
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	104
83.77.244.54	Switzerland	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	103
178.193.139.232	Switzerland	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	100
83.77.244.54	Switzerland	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	99
2.55.177.206	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	99
83.77.244.54	Switzerland	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	88
212.116.190.59	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	84
84.93.36.200	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	84
5.82.101.175	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	83
83.77.244.54	Switzerland	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	80
178.193.139.232	Switzerland	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	78
62.0.230.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	72
106.188.26.113	Japan	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	69
109.63.151.105	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	66
74.91.112.3	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	65
80.81.23.7	Germany	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	63
8.37.225.186	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	62
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	61
46.19.86.207	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	60
79.176.13.237	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	56
74.91.112.3	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	56
185.10.125.63	Hungary	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	55
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	55
66.249.76.30	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
109.67.218.236	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	54
74.91.112.3	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	54
64.94.238.88	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	52
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
62.0.236.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	50
100.92.97.43		147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	50

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.69.75.24	Israel	147.237.72.166	aka.idf.il	Automated Vulnerability Scanning V1	Block	3084
87.69.75.24	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 87.69.75.24	Block	1325
2.53.147.223	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	581
2.53.165.210	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	241
80.246.138.223	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	205
46.19.86.26	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	154
88.202.218.242	United Kingdom	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	150
46.19.86.166	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	135
46.19.86.37	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	133
2.53.136.211	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	126
37.26.147.166	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	122
2.55.191.102	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	116
109.253.199.45	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	113
46.19.86.221	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
109.253.129.143	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
176.13.251.62	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	103
37.26.146.165	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	96
109.253.196.23	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	88
109.253.222.113	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	87
2.55.165.164	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	83
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	81
2.53.4.167	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	81
46.19.86.134	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	78
2.55.23.138	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	74
109.253.147.238	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	66
80.246.137.93	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	63
109.67.131.62	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	62
89.138.254.248	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	57
2.53.52.255	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	57
41.111.102.246	Algeria	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 41.111.102.246	Block	57
46.19.86.14	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	53
2.53.40.136	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	53
46.210.206.25	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	45
109.253.143.4	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	43
46.19.85.220	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	38
176.13.16.59	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	37
95.35.137.176	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	35
95.35.75.113	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	34
176.13.228.255	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
176.13.238.188	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	27
82.166.240.204	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	26
195.189.193.1	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 195.189.193.1	Block	25
109.253.136.94	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	25
2.53.160.79	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	23
37.26.148.149	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	22
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	21
37.26.148.252	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	21
37.26.147.182	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	20
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.224	Block	19
46.19.86.201	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	18

09-27-2016 to 09-28-2016