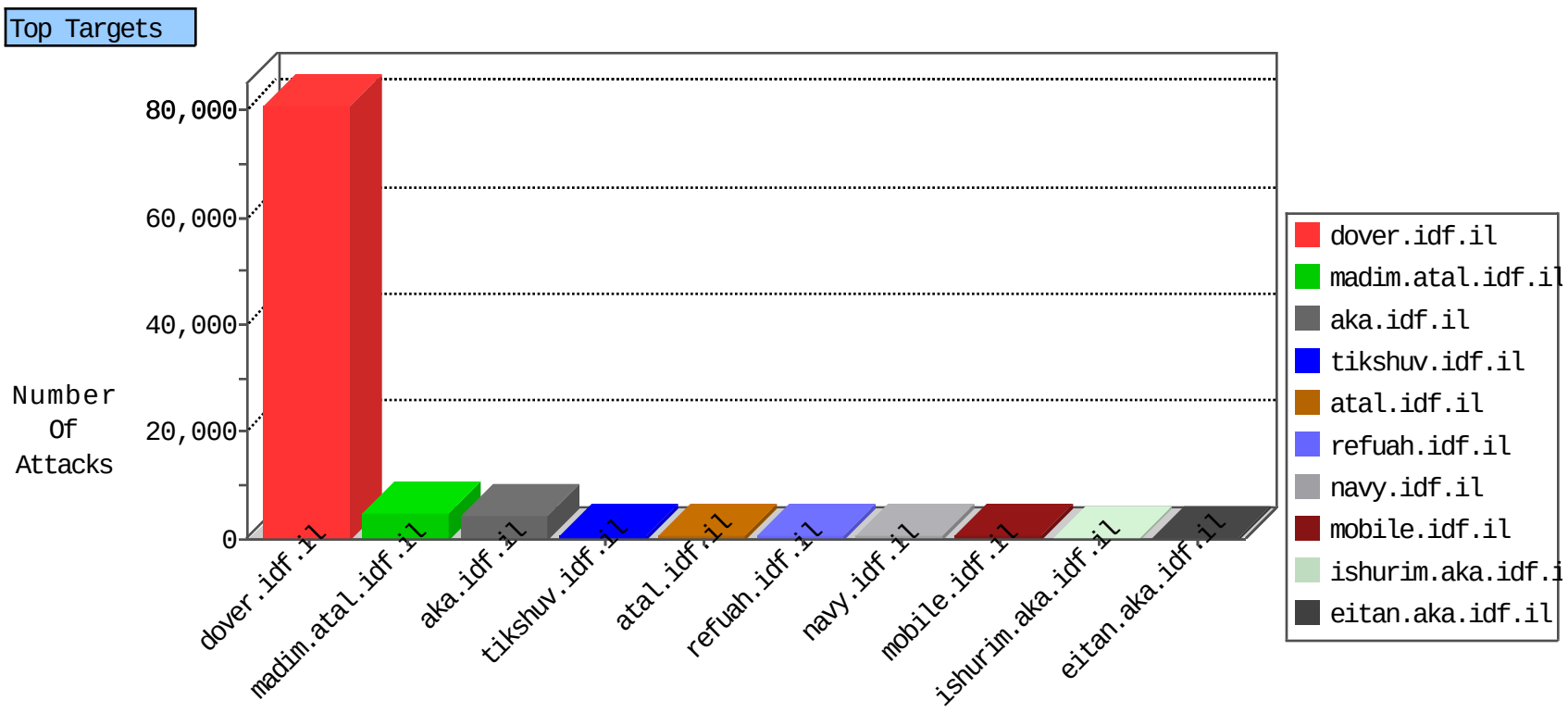
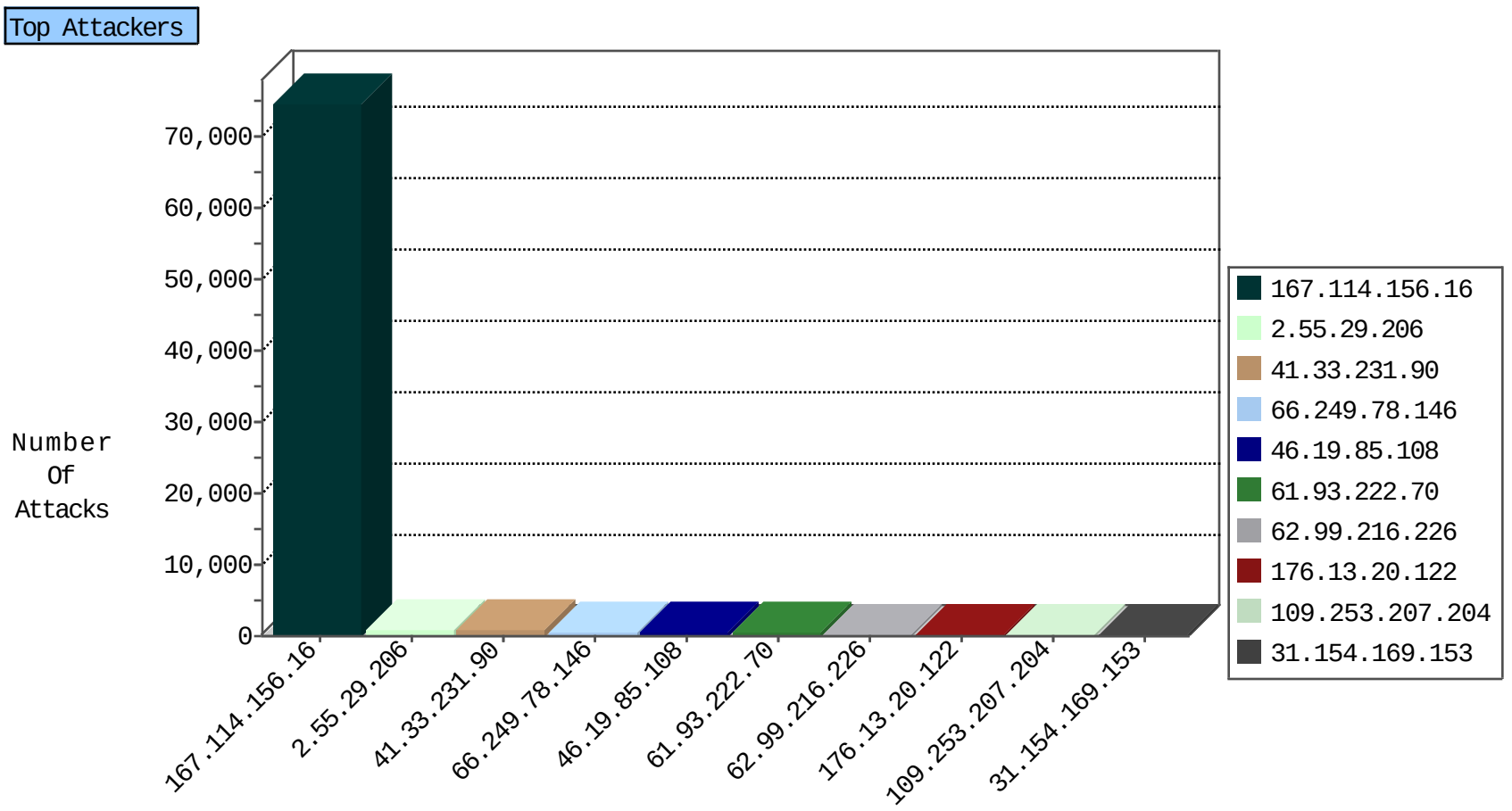
04-14-2016 to 04-15-2016

IDF Under Attack
Daily Report

Top Targets



Top Attackers



04-14-2016 to 04-15-2016

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	Block_Ip_Web_In	drop	74702
46.116.137.190	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3206
197.41.61.60	Egypt	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	651
197.41.92.240	Egypt	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	622
197.41.93.176	Egypt	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	619
197.41.93.29	Egypt	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	613
197.41.120.111	Egypt	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	609
197.41.86.35	Egypt	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	591
197.41.84.42	Egypt	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	585
197.41.10.47	Egypt	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	568
197.41.11.71	Egypt	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	530
185.32.179.209	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	61
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	51
176.13.14.49	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	51
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	42
197.6.36.60	Tunisia	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	37
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	19
80.178.95.33	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	11
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	10
80.246.133.225	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
120.132.50.135	China	147.237.77.233	atal.idf.il	block-sp-traf1	forward	8
192.116.232.69	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
82.145.209.190	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	7
79.178.163.130	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	5
109.65.71.4	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
123.59.59.52	China	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	4
123.59.59.52	China	147.237.77.216	dover.idf.il	block-sp-traf1	forward	4
123.59.59.52	China	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	4
212.199.233.127	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
79.178.23.64	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
192.118.132.185	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
42.156.241.248	China	147.237.8.45	e.eitan.idf.il	Block_Udp_All_Nets	drop	3
82.81.90.118	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
192.118.132.185	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
109.253.204.199	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
31.210.185.218	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
79.178.205.207	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
8.37.231.156	United States	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
79.177.180.227	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
222.186.58.188	China	147.237.0.15	kosher-kravi.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
79.181.127.93	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
8.37.231.156	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
101.201.147.32	China	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	forward	2
80.82.78.38	Netherlands	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	2
80.82.78.38	Netherlands	147.237.76.31	nakchal.idf.il	block-sp-traf1	forward	2
101.201.147.32	China	147.237.77.176	matpash.idf.il	block-sp-traf1	forward	2
80.82.78.38	Netherlands	147.237.77.74	law.idf.il	block-sp-traf1	forward	2
123.59.59.52	China	147.237.77.170	maarachot.idf.il	block-sp-traf1	forward	2
80.82.78.38	Netherlands	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	2
82.145.209.90	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	2

04-14-2016 to 04-15-2016

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
207.241.237.222	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	57
106.38.241.144	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	42
79.180.198.191	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	31
5.29.122.103	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	23
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	20
106.38.241.106	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	20
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	18
213.8.204.61	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	17
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	16
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	13
98.19.222.133	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	12
61.135.189.114	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	11
66.249.66.154	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
176.13.18.172	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
94.159.152.231	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
66.249.66.158	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
213.8.204.71	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
83.143.81.94	Norway	147.237.76.31	nakchal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
213.57.205.145	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
87.69.144.214	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
79.183.59.115	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
123.126.113.101	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	7
82.166.148.243	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
82.81.96.41	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
87.71.87.207	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
213.57.82.58	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
87.71.94.110	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
213.8.10.16	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
79.178.52.195	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
192.118.78.199	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
10.0.0.3		147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
79.176.138.27	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
177.185.194.47	Brazil	147.237.77.176	matpash.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
66.135.63.82	United States	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
41.185.31.40	South Africa	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
212.235.119.230	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
70.89.127.78	United States	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
63.143.34.37	United States	147.237.76.86	navy.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
109.253.215.206	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
177.185.194.138	Brazil	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
185.106.92.47	Russian Federation	147.237.76.39	mobile.meitav.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	4
77.126.24.168	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
63.143.34.37	United States	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
194.88.154.138	Poland	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
177.185.194.138	Brazil	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
162.210.196.97	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	4
209.15.196.170	Canada	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
87.106.179.116	Germany	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
5.28.169.13	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
213.8.145.99	Israel	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4

04-14-2016 to 04-15-2016

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	513
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	68
98.19.222.133	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	25
37.46.42.188	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	24
83.143.81.94	147.237.76.31	Norway	nakchal.idf.il	SQL Injection - Select From	19
63.143.34.37	147.237.77.216	United States	dover.idf.il	SQL Injection - Select From	16
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	16
63.143.34.37	147.237.76.86	United States	navy.idf.il	SQL Injection - Select From	15
194.88.154.138	147.237.76.42	Poland	refuah.idf.il	SQL Injection - Select From	14
66.135.63.82	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	13
70.89.127.78	147.237.77.216	United States	dover.idf.il	SQL Injection - Select From	12
31.154.41.17	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	11
213.8.145.99	147.237.77.74	Israel	law.idf.il	SQL Injection - Select From	11
177.185.194.138	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	10
82.165.24.123	147.237.76.42	Germany	refuah.idf.il	SQL Injection - Select From	10
209.15.196.170	147.237.77.233	Canada	atal.idf.il	SQL Injection - Select From	9
209.173.241.141	147.237.77.226	United States	www.chamatz.aka.idf.il	SQL Injection - Select From	9
177.185.194.138	147.237.77.233	Brazil	atal.idf.il	SQL Injection - Select From	9
197.41.11.71	147.237.77.216	Egypt	dover.idf.il	ET SCAN NMAP -sS window 1024	9
87.106.179.116	147.237.72.166	Germany	aka.idf.il	SQL Injection - Select From	7
41.185.31.40	147.237.77.74	South Africa	law.idf.il	SQL Injection - Select From	7
197.41.93.176	147.237.77.216	Egypt	dover.idf.il	ET SCAN NMAP -sS window 1024	6
197.41.92.240	147.237.77.216	Egypt	dover.idf.il	ET SCAN NMAP -sS window 1024	6
197.41.120.111	147.237.77.216	Egypt	dover.idf.il	ET SCAN NMAP -sS window 1024	6
177.185.194.47	147.237.77.176	Brazil	matpash.idf.il	SQL Injection - Select From	6
197.41.10.47	147.237.77.216	Egypt	dover.idf.il	ET SCAN NMAP -sS window 1024	5
197.41.61.60	147.237.77.216	Egypt	dover.idf.il	ET SCAN NMAP -sS window 1024	5
66.249.66.12	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	5
197.41.93.29	147.237.77.216	Egypt	dover.idf.il	ET SCAN NMAP -sS window 1024	5
197.41.86.35	147.237.77.216	Egypt	dover.idf.il	ET SCAN NMAP -sS window 1024	5
82.205.4.135	147.237.77.176	Palestinian Territory, Occupied	matpash.idf.il	ET SCAN NMAP -sA (2)	4
96.47.2.10	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	4
197.41.84.42	147.237.77.216	Egypt	dover.idf.il	ET SCAN NMAP -sS window 1024	4
212.235.98.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	3
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	3
66.249.78.158	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
66.249.66.1	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	2
77.124.241.188	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
59.45.79.103	147.237.8.14	China	e.orchot.idf.il	ET SCAN Potential SSH Scan	2
80.82.78.38	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	2
5.22.135.246	147.237.72.167	Israel	ishurim.aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
66.249.83.209	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
212.106.76.162	147.237.77.176	Palestinian Territory, Occupied	matpash.idf.il	ET SCAN NMAP -sA (2)	2
192.114.5.10	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
80.246.133.222	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
79.176.74.203	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	2
122.141.236.69	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	2
217.21.7.11	147.237.77.176	Palestinian Territory, Occupied	matpash.idf.il	ET SCAN NMAP -sA (2)	2
95.211.70.193	147.237.77.74	Netherlands	law.idf.il	SQL Injection - Select From	2
59.45.79.103	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	2

04-14-2016 to 04-15-2016

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	738
62.99.216.226	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	308
61.93.222.70	Hong Kong	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	250
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	218
80.246.133.167	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	187
194.90.83.233	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	90
61.93.222.70	Hong Kong	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	89
109.65.162.115	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	78
176.13.10.111	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
51.36.16.28	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	70
176.13.4.200	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	69
109.186.169.154	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	68
46.116.162.187	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	57
2.53.173.1	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	51
46.116.162.187	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	50
87.70.52.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
109.67.101.24	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
130.154.3.250	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
195.160.242.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
212.179.21.194	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	38
93.172.155.203	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	37
188.120.154.2	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	36
79.180.5.107	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
212.150.7.37	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	36
37.142.68.60	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
81.218.172.111	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	32
5.22.135.246	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	28
46.116.162.187	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	26
176.13.3.226	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	26
93.173.63.93	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	25
80.178.189.185	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
90.213.180.255	United Kingdom	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
109.253.158.208	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
2.55.41.96	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
107.167.112.198	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	23
201.179.168.61	Argentina	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	23
2.53.181.88	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	23
46.19.85.4	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
80.246.133.65	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
79.177.183.4	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
2.53.181.88	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
80.230.62.178	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
46.116.42.255	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
93.173.63.93	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
176.13.11.152	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
87.70.90.253	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18

04-14-2016 to 04-15-2016

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
2.53.133.166	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
79.182.142.234	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
176.13.14.49	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.55.29.206	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	798
46.19.85.108	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	429
176.13.20.122	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	290
109.253.207.204	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	253
31.154.169.153	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	247
95.86.106.179	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	232
46.19.85.35	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	209
2.53.48.181	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	203
2.53.183.16	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	138
109.253.221.87	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	111
2.55.62.48	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	105
46.19.86.197	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	101
109.253.224.21	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	97
37.26.149.239	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	94
94.159.166.36	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	93
176.13.20.219	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	81
46.19.86.52	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	74
176.13.3.28	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	71
46.19.85.246	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	66
95.175.35.73	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	64
176.13.16.219	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	62
5.189.190.212	Germany	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	60
176.13.3.226	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	57
80.246.139.113	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	54
2.53.53.233	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	41
46.19.85.180	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	40
176.13.6.34	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	39
109.253.224.110	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	37
149.88.225.172	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	35
109.253.157.174	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	34
2.53.172.189	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	33
2.53.2.196	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	28
109.253.204.245	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	27
82.102.136.69	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 82.102.136.69	Block	26
109.253.224.112	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	24
2.55.132.146	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	24
176.13.19.65	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	23
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	23
2.55.15.93	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	21
2.53.29.78	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	21
109.64.30.143	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	20
109.253.224.109	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	19
84.109.215.153	Israel	147.237.0.34	tikshuv.idf.il	Automated Vulnerability Scanning V1	Block	18
2.53.130.179	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	16
62.219.21.30	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/	Block	13
2.53.175.113	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	11
46.188.30.189	Russian Federation	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.188.30.189	Block	10
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	10
91.228.248.251	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	10
2.55.172.149	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9

04-14-2016 to 04-15-2016