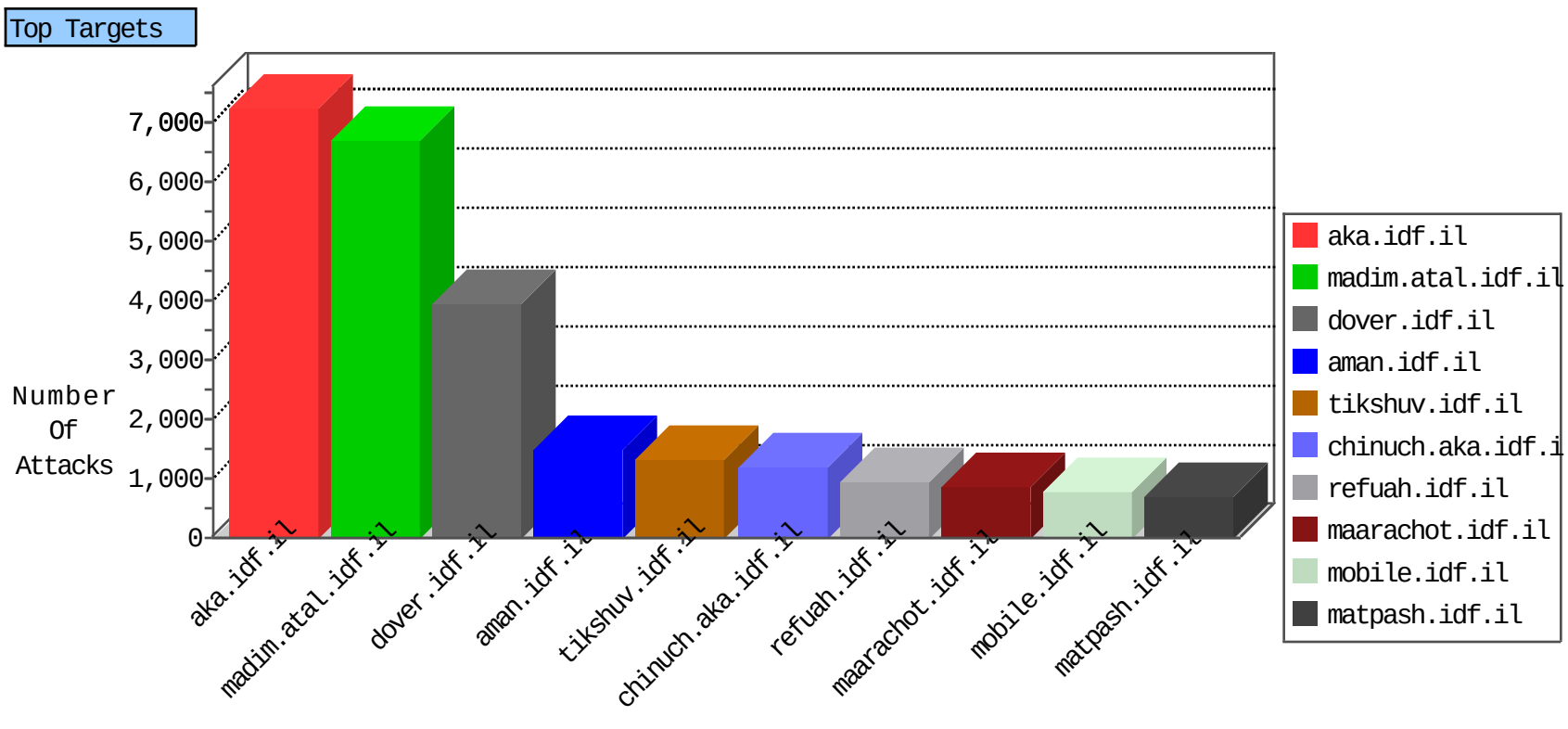
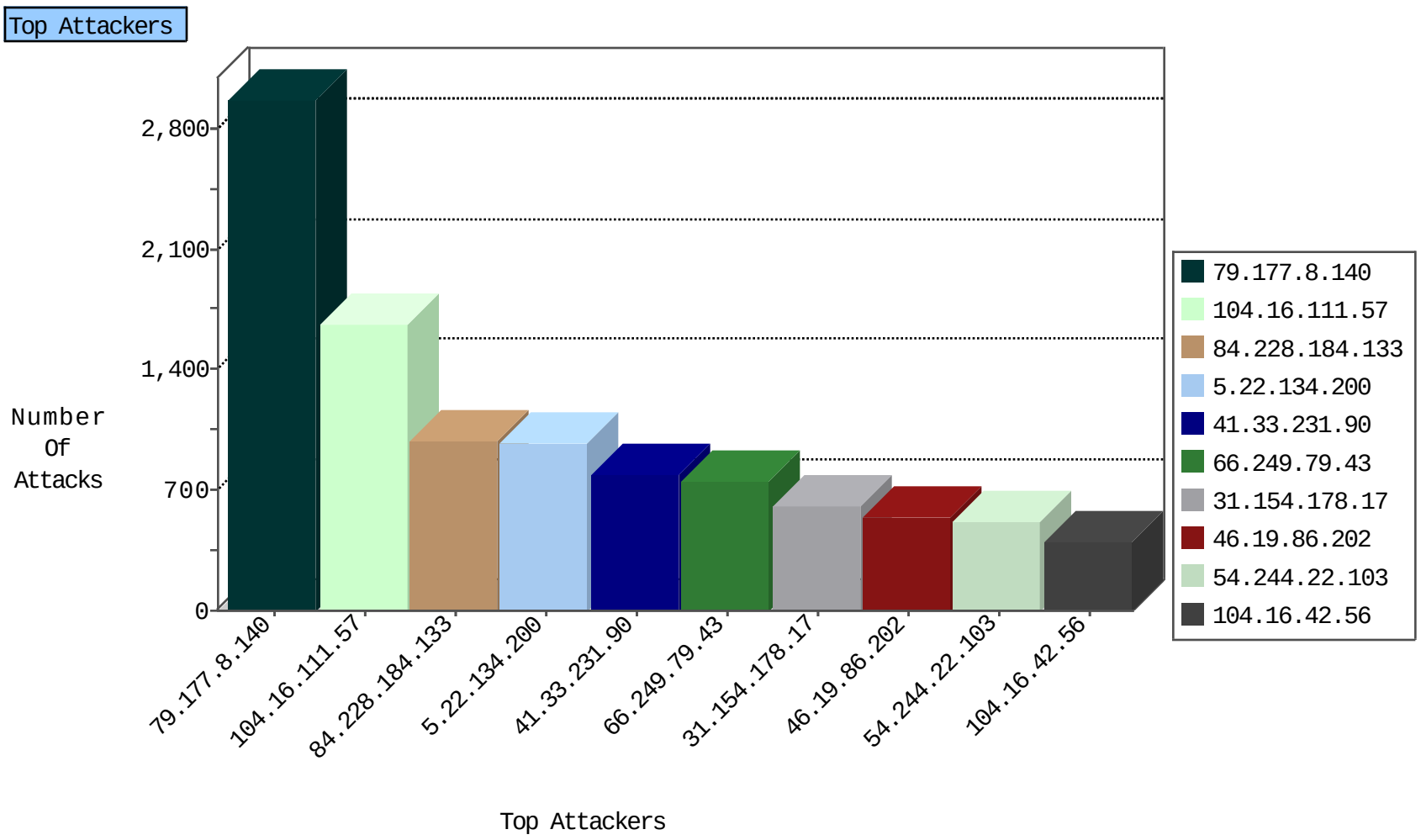
02-05-2016 to 02-06-2016

IDF Under Attack
Daily Report

Top Targets



Top Attackers



02-05-2016 to 02-06-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.78.31	Israel	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	2543
66.249.78.146	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	721
66.249.78.79	Israel	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	716
92.253.91.66	Jordan	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	633
82.163.70.206	United Kingdom	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	221
50.118.172.76	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	199
66.249.78.22	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	70
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	60
187.213.149.164	Mexico	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	50
66.249.78.190	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	26
66.249.78.82	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	25
80.246.136.82	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	18
66.249.78.15	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	10
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	8
82.145.217.212	Europe	147.237.76.147	chinuch.aka.idf.il	Block_Ip_Web_In	drop	7
37.8.86.185	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
79.180.52.13	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
71.83.52.230	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
80.246.136.82	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	4
81.218.206.82	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
46.188.23.221	Russian Federation	147.237.76.42	refuah.idf.il	JLM_Purple_Con_Limit_Http	drop	3
79.176.127.112	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
115.239.228.10	China	147.237.76.39	mobile.meitav.idf.il	JLM_Purple_Con_Limit_Http	drop	3
212.179.54.237	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
109.67.167.16	Israel	147.237.77.233	atal.idf.il	Block_Udp_All_Nets	drop	3
79.178.13.103	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
72.9.148.10	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
81.218.206.82	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
79.182.167.209	Israel	147.237.77.234	halag.idf.il	Block_Udp_All_Nets	drop	3
204.42.253.2	United States	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	2
185.130.5.224		147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	2
204.42.253.2	United States	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	2
134.147.203.115	Germany	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	2
46.188.23.221	Russian Federation	147.237.76.42	refuah.idf.il	JLM_Under_Attack_Con_Http	drop	2
204.42.253.2	United States	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	2
134.147.203.115	Germany	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	2
115.239.228.10	China	147.237.76.39	mobile.meitav.idf.il	JLM_Under_Attack_Con_Http	drop	2
185.130.5.201		147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	2
168.235.196.104	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
94.102.48.195	Netherlands	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	2
204.42.253.2	United States	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	2
123.151.149.222	China	147.237.76.196	e.sviva.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
95.185.96.142	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
204.42.253.2	United States	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	2

02-05-2016 to 02-06-2016

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.254.112.141	United Kingdom	147.237.76.86	navy.idf.il	0543: HTTP: php.cgi Access	Block	2
202.69.240.221	Hong Kong	147.237.77.74	law.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	2
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	2
110.249.142.199	China	147.237.77.216	dover.idf.il	13076: HTTP: Apache Struts 2 OGNL Command Injection Vulnerability	Block	1
202.69.240.221	Hong Kong	147.237.77.226	www.chamatz.aka.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
52.89.170.75	United States	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
202.69.240.221	Hong Kong	147.237.0.34	tikshuv.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
2.54.168.179	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
185.130.5.207		147.237.72.156	aman.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
91.219.122.4	Poland	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
45.63.97.227		147.237.76.42	refuah.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
202.69.240.221	Hong Kong	147.237.76.147	chinuch.aka.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
198.20.69.74	United States	147.237.8.27	e.madim.atal.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
123.125.125.79	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
213.57.240.91	Israel	147.237.0.19	madim.atal.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
69.30.215.142	United States	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	1
202.69.240.221	Hong Kong	147.237.76.30	himush.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
188.165.15.27	France	147.237.0.34	tikshuv.idf.il	C228: HTTP: AhrefBot crawler	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
45.63.97.227		147.237.77.216	dover.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
198.20.69.74	United States	147.237.76.201	e.atal.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
123.126.113.154	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
218.24.91.130	China	147.237.0.17	m.my-kosher-kravi.idf.il	13076: HTTP: Apache Struts 2 OGNL Command Injection Vulnerability	Block	1
78.161.81.201	Turkey	147.237.77.216	dover.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
5.254.112.141	United Kingdom	147.237.77.216	dover.idf.il	0543: HTTP: php.cgi Access	Block	1
202.69.240.221	Hong Kong	147.237.76.31	nakchal.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
188.165.15.43	France	147.237.76.147	chinuch.aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1
109.160.135.255	Israel	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
45.79.193.230		147.237.77.216	dover.idf.il	C104: HTTP: Access to - pageinfo.php	Block	1
202.69.240.221	Hong Kong	147.237.77.170	maarachot.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
198.20.99.130	Netherlands	147.237.77.61	e.cogat.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
151.80.31.141	Italy	147.237.77.74	law.idf.il	C228: HTTP: AhrefBot crawler	Block	1
218.24.91.130	China	147.237.77.216	dover.idf.il	13076: HTTP: Apache Struts 2 OGNL Command Injection Vulnerability	Block	1
86.193.37.134	France	147.237.72.166	aka.idf.il	C008: HTTP: Xenu UserAgent	Block	1
27.154.224.210	China	147.237.0.17	m.my-kosher-kravi.idf.il	13076: HTTP: Apache Struts 2 OGNL Command Injection Vulnerability	Block	1
202.69.240.221	Hong Kong	147.237.76.42	refuah.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
188.165.15.60	France	147.237.72.167	ishurim.aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1
110.249.142.199	China	147.237.0.17	m.my-kosher-kravi.idf.il	13076: HTTP: Apache Struts 2 OGNL Command Injection Vulnerability	Block	1
202.69.240.221	Hong Kong	147.237.77.176	matpash.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
202.69.240.221	Hong Kong	147.237.0.15	kosher-kravi.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
182.50.130.136	Singapore	147.237.77.216	dover.idf.il	C228: HTTP: AhrefBot crawler	Block	1
91.20.12.178	Germany	147.237.72.166	aka.idf.il	C106: HTTP: majestic bot	Block	1
45.63.97.227		147.237.72.166	aka.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
202.69.240.221	Hong Kong	147.237.76.86	navy.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
188.165.15.206	France	147.237.77.233	atal.idf.il	C228: HTTP: AhrefBot crawler	Block	1

02-05-2016 to 02-06-2016

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.79.43	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	754
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	91
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	20
80.246.133.205	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	17
66.249.78.159	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	10
66.249.78.45	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	4
80.246.130.233	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	4
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	4
66.249.78.31	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	4
91.219.122.4	147.237.77.74	Poland	law.idf.il	SQL Injection - Select From	3
66.249.78.15	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
37.26.148.152	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
66.249.69.34	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
59.45.79.117	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	2
66.249.65.18	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
59.45.79.117	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.197	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	2
59.45.79.117	147.237.77.179	China	e.mazi.idf.il	ET SCAN Potential SSH Scan	2
59.45.79.117	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	2
59.45.79.117	147.237.77.176	China	matpash.idf.il	ET SCAN Potential SSH Scan	2
59.45.79.117	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.147	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
193.105.134.220	147.237.77.234	Sweden	halag.idf.il	ET SCAN NMAP -sS window 1024	2
94.230.93.211	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.29	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
73.179.141.155	147.237.8.14	United States	e.orchot.idf.il	ET SCAN Potential SSH Scan	2
66.249.69.122	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sA (2)	2
66.249.66.23	147.237.72.156	United States	aman.idf.il	ET SCAN NMAP -sA (2)	2
66.249.81.198	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.190	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.206	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.187	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sA (2)	2
188.152.234.175	147.237.77.216	Italy	dover.idf.il	ET WEB_SERVER PyCurl Suspicious User Agent Inbound	2
59.45.79.117	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	2
183.60.48.25	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	2
125.212.232.144	147.237.77.216	Vietnam	dover.idf.il	ET SCAN NMAP -sS window 2048	1
91.201.236.114	147.237.0.16	Ukraine	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
61.148.124.38	147.237.77.216	China	dover.idf.il	SERVER-APACHE Apache Tomcat Web Application Manager access	1
218.246.0.97	147.237.77.233	China	atal.idf.il	ET SCAN NMAP -sS window 1024	1
41.228.12.4	147.237.72.166	Tunisia	aka.idf.il	ET SCAN Potential SSH Scan	1
188.6.142.254	147.237.76.196	Hungary	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
107.2.79.150	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sS window 3072	1
73.179.141.155	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
58.56.93.171	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
209.126.116.147	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
59.45.79.117	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
209.126.116.147	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
94.102.49.151	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
46.148.22.26	147.237.76.38	Lithuania	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1

02-05-2016 to 02-06-2016

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
104.16.111.57	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	834
104.16.111.57	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	834
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	740
31.154.178.17	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	612
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	376
94.159.154.240	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	204
87.68.36.38	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	201
104.16.42.56	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	200
104.16.42.56	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	200
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	189
46.19.86.71	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	146
94.100.245.126	Germany	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	137
211.44.8.161	Korea, Republic of	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	107
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	106
211.44.8.161	Korea, Republic of	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	106
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	106
149.154.240.211	Belgium	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	101
93.172.35.9	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	97
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	92
89.249.107.248	Croatia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	89
50.118.172.76	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	88
8.37.237.22	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	79
46.19.85.18	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	76
77.127.209.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
82.80.156.245	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	65
80.246.133.5	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	64
168.235.196.104	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	57
87.68.153.111	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	51
46.19.85.230	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	50
109.67.112.82	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	47
194.150.201.210	United Kingdom	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
176.0.68.242	Germany	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	45
109.67.234.164	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
46.19.86.53	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	44
46.19.86.58	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	44
212.76.127.219	Israel	147.237.76.30	himush.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	42
85.130.217.200	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
85.64.35.119	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	40
109.65.208.97	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
54.172.96.232	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	34
46.19.85.59	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	34
207.241.231.229	United States	147.237.72.166	aka.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	34
185.32.179.235	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	34
176.13.9.244	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	34
185.130.5.207		147.237.77.233	atal.idf.il	drop	SAM rule	drop	30
176.13.20.93	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
89.249.107.248	Croatia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	29
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	28
80.246.136.178	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	28
213.57.240.91	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	28

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.177.8.140	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2769
84.228.184.133	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	619
5.22.134.200	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 5.22.134.200	Block	527
5.22.134.200	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 5.22.134.200	Block	345
46.19.86.202	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	323
176.13.18.29	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	281
84.228.184.133	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 84.228.184.133	Block	259
46.19.86.202	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	221
109.253.204.87	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 109.253.204.87	Block	211
79.177.8.140	Israel	147.237.72.166	aka.idf.il	Too Many of the Same Response Code (404) in Session from 79.177.8.140	Block	203
5.28.136.50	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	166
2.54.25.62	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	162
37.142.228.147	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	142
46.19.86.39	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	135
77.127.32.19	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	129
46.121.97.91	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	127
37.142.228.147	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	117
109.253.192.191	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	116
109.253.204.87	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	114
2.54.25.62	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	112
84.228.184.133	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	110
46.121.37.45	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 46.121.37.45	Block	107
5.22.134.200	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
46.19.86.39	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.86.39	Block	103
109.67.9.200	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	101
176.13.1.111	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	100
2.54.40.89	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	100
2.54.150.224	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	96
109.67.9.200	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	95
176.13.18.29	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	95
2.52.188.210	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	90
84.108.66.42	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	89
46.121.97.91	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.121.97.91	Block	87
46.19.86.190	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	86
37.46.38.98	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 37.46.38.98	Block	82
84.109.212.210	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	82
176.13.1.111	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	82
46.19.86.246	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	81
37.142.215.95	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 37.142.215.95	Block	78
2.54.14.35	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.14.35	Block	73
46.19.85.115	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	70
2.54.20.26	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	67
87.69.246.21	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	64
109.253.192.191	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	63
77.126.26.235	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	61
77.126.92.8	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	56
109.253.204.87	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 109.253.204.87	Block	54
109.253.156.91	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	52
2.54.40.89	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	52
2.52.188.210	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	51