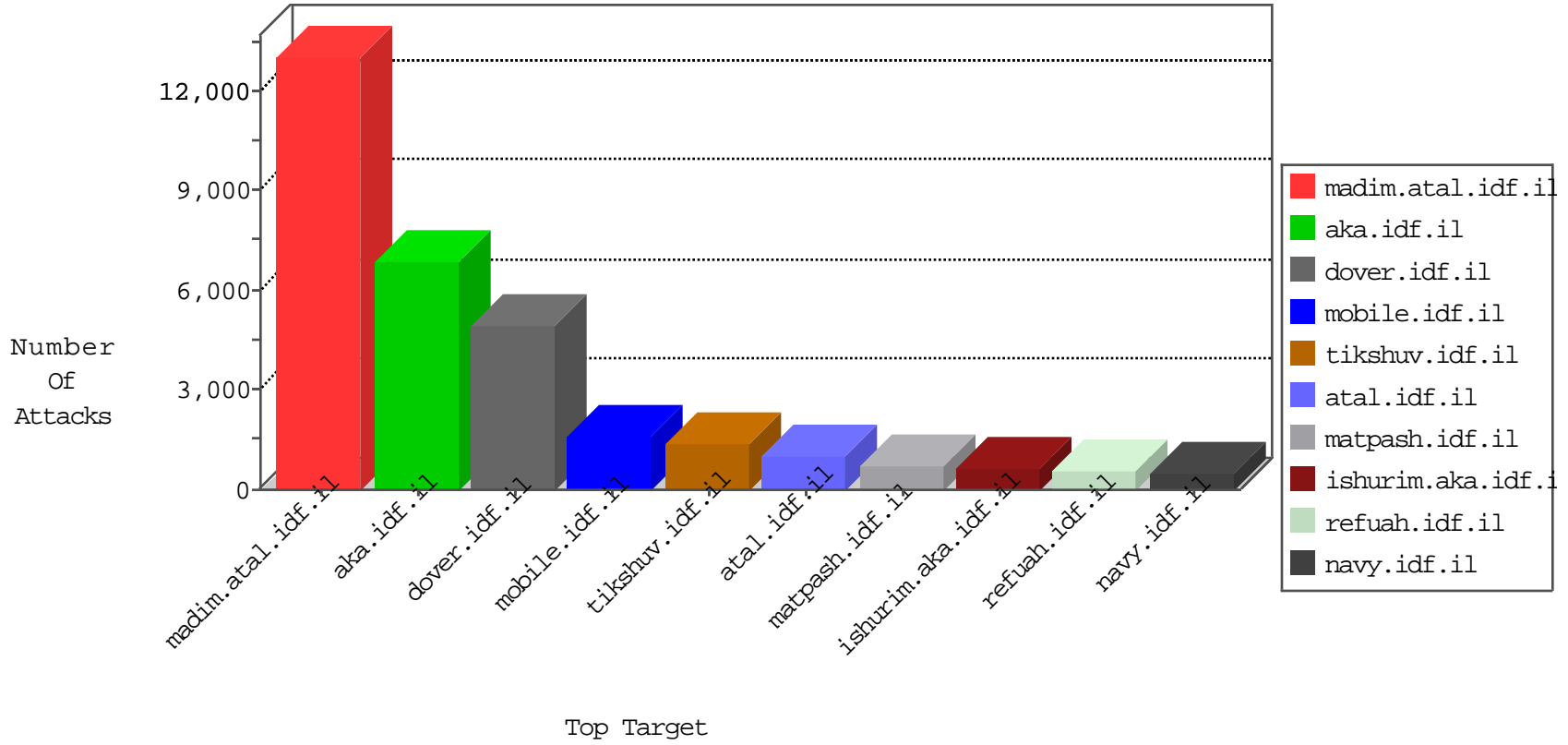


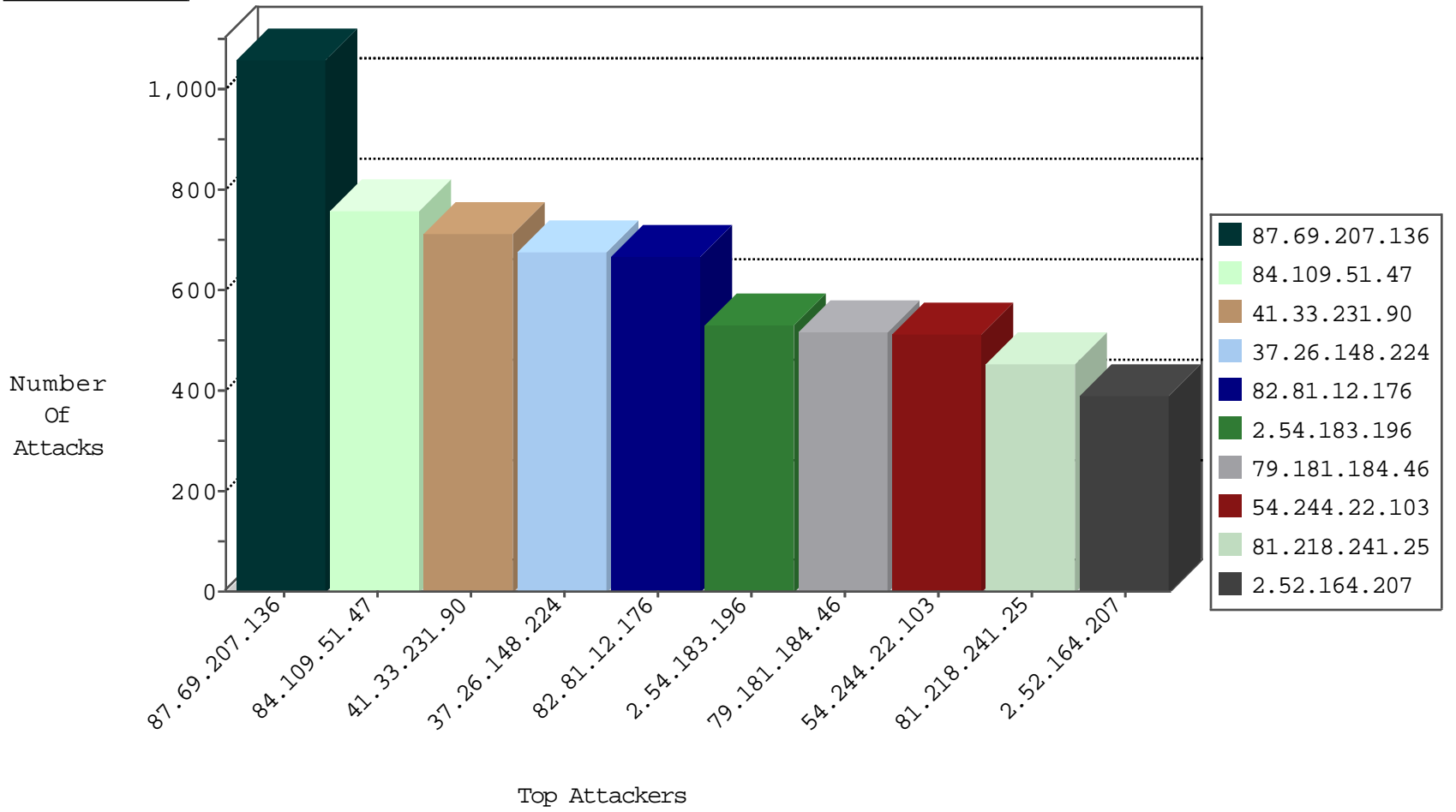
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.78.254	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3211
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1667
207.232.36.181	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1052
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	662
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	511
212.199.154.194	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	407
81.218.241.25	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	89
46.19.85.140	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	71
109.67.179.166	Israel	147.237.76.86	navy.idf.il	IA Source or Dest Port Zero	drop	30
77.125.96.130	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	20
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	18
185.32.179.217	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	14
31.223.191.72	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	13
46.19.86.63	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	11
212.179.54.237	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	11
2.54.135.246	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	9
82.132.223.85	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
109.67.179.166	Israel	147.237.77.216	dover.idf.il	IA Source or Dest Port Zero	drop	9
87.68.154.207	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
109.66.55.173	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	6
109.66.55.173	Israel	147.237.77.166	aka.idf.il	Block_Udp_All_Nets	drop	6
212.199.182.150	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
79.176.58.6	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
115.230.124.164	China	147.237.77.216	dover.idf.il	block-sp-traf1	drop	4
185.120.126.37		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
173.252.112.102	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
149.78.154.69	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
192.0.100.226	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
109.64.23.204	Israel	147.237.0.19	madim.atal.idf.il	Block_Udp_All_Nets	drop	3
31.168.146.45	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
81.218.56.245	Israel	147.237.72.167	ishurim.aka.idf.i	Block_Udp_All_Nets	drop	3
109.64.23.204	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
81.218.151.130	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
149.78.47.74	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
192.118.132.185	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
212.179.64.162	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
79.183.131.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
109.64.23.204	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
37.142.182.119	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
82.166.20.226	Israel	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
82.81.12.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
207.46.13.163	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
81.218.206.82	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
183.60.48.25	China	147.237.76.176	test.ncore.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
60.169.79.173	China	147.237.76.201	e.atal.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
115.239.228.10	China	147.237.76.202	e.halag.idf.il	JLM_Under_Attack_Con_Http	drop	2

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
159.253.145.150	United States	147.237.76.86	navy.idf.il	C095: Suspicious Addresses MFA	Permit	23
159.253.145.150	United States	147.237.77.216	dover.idf.il	C095: Suspicious Addresses MFA	Permit	14
104.236.201.28		147.237.72.166	aka.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	12
202.69.240.159	Hong Kong	147.237.77.74	law.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	4
202.69.240.159	Hong Kong	147.237.77.170	maarachot.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	4
202.69.240.192	Hong Kong	147.237.77.74	law.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	4
199.255.210.41	Anonymous Proxy	147.237.77.74	law.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	4
159.253.145.150	United States	147.237.77.170	maarachot.idf.il	C095: Suspicious Addresses MFA	Permit	2
212.225.165.62	Spain	147.237.77.176	matpash.idf.il	C008: HTTP: Xenu UserAgent	Block	2
94.76.13.228	Bahrain	147.237.0.34	tikshuv.idf.il	C107: DDOS-Spoofed HTTP Packets	Block	2
217.80.196.237	Germany	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	1
71.13.87.122	United States	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	1
188.165.15.210	France	147.237.77.234	halag.idf.il	C228: HTTP: AhrefBot crawler	Block	1
46.119.121.146	Ukraine	147.237.76.200	eitan.aka.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
188.165.15.15	France	147.237.76.86	navy.idf.il	C228: HTTP: AhrefBot crawler	Block	1
123.149.205.53	China	147.237.72.166	aka.idf.il	3630: HTTP: SQL Injection (Boolean Identity)	Block	1
78.165.93.125	Turkey	147.237.77.74	law.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
5.9.73.227	Germany	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	1
192.240.106.106	United States	147.237.76.86	navy.idf.il	0543: HTTP: php.cgi Access	Block	1
106.38.241.106	China	147.237.77.233	atal.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
51.255.48.154	United Kingdom	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	1
188.165.15.66	France	147.237.72.156	aman.idf.il	C228: HTTP: AhrefBot crawler	Block	1
149.255.59.146	United Kingdom	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	1
83.136.249.162	United Kingdom	147.237.77.176	matpash.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
5.9.111.70	Germany	147.237.72.166	aka.idf.il	C106: HTTP: majestic bot	Block	1
192.240.106.106	United States	147.237.77.216	dover.idf.il	0543: HTTP: php.cgi Access	Block	1
106.120.173.127	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
51.255.194.33	United Kingdom	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	1
188.165.15.121	France	147.237.72.156	aman.idf.il	C228: HTTP: AhrefBot crawler	Block	1
151.80.31.128	Italy	147.237.0.34	tikshuv.idf.il	C228: HTTP: AhrefBot crawler	Block	1
94.76.10.91	Bahrain	147.237.77.19	law-forum.idf.il	C107: DDOS-Spoofed HTTP Packets	Block	1
198.20.69.74	United States	147.237.76.38	e.e.meitav.idf.i	13840: TLS: OpenSSL Heartbeat Packet	Block	1
37.229.252.191	Ukraine	147.237.77.74	law.idf.il	C008: HTTP: Xenu UserAgent	Block	1
171.8.152.200	China	147.237.72.166	aka.idf.il	3630: HTTP: SQL Injection (Boolean Identity)	Block	1
108.59.8.80	United States	147.237.77.233	atal.idf.il	C106: HTTP: majestic bot	Block	1
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
188.165.15.193	France	147.237.77.170	maarachot.idf.il	C228: HTTP: AhrefBot crawler	Block	1
151.80.31.142	Italy	147.237.72.166	aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1
46.119.121.146	Ukraine	147.237.72.166	aka.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
188.165.15.13	France	147.237.76.31	nakchal.idf.il	C228: HTTP: AhrefBot crawler	Block	1
123.126.113.154	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	69
46.19.85.128	147.237.77.216	Israel	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	48
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	33
104.236.201.28	147.237.72.166		aka.idf.il	Tehila - Perl LWP with fake user agent	11
66.249.81.201	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	10
37.26.148.224	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	6
66.249.78.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	5
66.249.78.2	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	4
212.199.57.207	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	4
66.249.64.92	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
172.58.224.73	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.159	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
61.149.161.186	147.237.76.147	China	chinuch.aka.idf.il	GPL SCAN nmap TCP	2
59.45.79.117	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.157	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sA (2)	2
93.172.43.16	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	2
59.45.79.117	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	2
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
59.45.79.117	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	2
193.201.227.10	147.237.77.205	Ukraine	prisha.idf.il	ET SCAN Potential SSH Scan	2
81.21.67.189	147.237.77.216	United Kingdom	dover.idf.il	Tehila - Perl LWP with fake user agent	2
66.249.78.97	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
183.60.48.25	147.237.77.216	China	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
94.76.14.46	147.237.0.16	Bahrain	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
59.45.79.117	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential SSH Scan	2
84.108.98.134	147.237.72.156	Israel	aman.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.44	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
94.76.11.99	147.237.0.34	Bahrain	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.64.102	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
192.115.67.2	147.237.72.166	Israel	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
193.201.227.10	147.237.8.50	Ukraine	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	2
59.45.79.117	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.153	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
81.218.241.25	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
66.249.78.111	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
59.45.79.117	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.96	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
59.45.79.117	147.237.77.74	China	law.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.67	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.15	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
193.201.227.10	147.237.76.39	Ukraine	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	2
66.249.93.29	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.73.206	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
218.246.0.97	147.237.72.156	China	aman.idf.il	ET SCAN NMAP -sS window 1024	2
40.122.124.70	147.237.77.216	United States	dover.idf.il	ET SCAN Potential SSH Scan	1
108.4.143.45	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
88.249.106.23	147.237.77.74	Turkey	law.idf.il	ET SCAN NMAP -sS window 1024	1
207.232.46.170	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.81.198	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	1
185.56.82.22	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

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	627
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	423
188.161.48.127	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	255
212.76.127.10	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	195
5.22.129.251	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	174
81.218.241.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	159
2.54.162.93	Israel	147.237.77.226	www.chamatz.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	118
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	115
212.76.127.219	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	114
50.118.162.210	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	102
94.76.10.201	Bahrain	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	94
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	91
2.52.60.242	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	87
84.95.134.199	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	78
176.13.5.169	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	66
5.34.160.178	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	64
212.76.127.219	Israel	147.237.76.30	himush.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	60
62.90.193.203	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	56
176.58.77.73	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	53
84.228.245.88	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	49
13.21.125.9	United Kingdom	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	48
79.182.64.11	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	47
81.218.241.25	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	46
213.34.206.38	Kuwait	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	43
176.13.2.0	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	41
176.13.21.8	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	40
212.76.127.44	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	40
85.250.159.179	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	39
94.76.14.202	Bahrain	147.237.77.19	law-forum.idf.il	drop	SAM rule	drop	38
213.57.178.72	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	38
85.65.111.84	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
176.13.10.186	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
109.253.203.153	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
79.177.16.23	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	33
176.58.77.73	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	33
2.52.0.105	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
77.125.97.9	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	32
190.247.171.130	Argentina	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	31
31.154.150.95	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	31
31.154.150.95	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	31
82.166.97.26	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	31
188.161.48.127	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	31
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	31

01-28-2016 to 01-29-2016

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.121.123.18	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
89.138.171.77	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
185.120.125.55		147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
176.13.13.167	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.69.207.136	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 87.69.207.136	Block	631
84.109.51.47	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	396
37.26.148.224	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	382
84.109.51.47	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	351
2.54.183.196	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	316
87.69.207.136	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 87.69.207.136	Block	304
79.181.184.46	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	300
176.13.17.20	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	225
2.52.164.207	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	215
79.176.53.235	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	204
176.13.22.233	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	189
46.19.86.224	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	171
185.32.179.99	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	167
109.253.150.71	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	166
37.26.148.224	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 37.26.148.224	Block	159
185.32.179.99	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	158
31.168.115.178	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 31.168.115.178	Block	158
216.72.40.185	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	152
213.151.32.163	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 213.151.32.163	Block	149
109.253.157.238	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	139
109.253.214.162	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	128
46.19.86.221	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	126
37.26.148.224	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	126
213.151.32.163	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	122
87.69.207.136	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	122
176.13.13.120	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	119
2.52.3.52	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	117
46.19.86.224	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	114
46.19.86.243	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	114
79.181.184.46	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 79.181.184.46	Block	113
2.52.164.207	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	113
79.176.53.235	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	111
80.246.136.111	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	111
2.54.183.196	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	110
31.168.115.178	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
109.253.150.71	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
2.52.3.52	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	106
2.54.183.196	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	105
109.253.199.158	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
79.181.184.46	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
79.177.9.111	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
192.117.101.230	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	100
176.13.13.120	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	100
109.253.194.127	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	98
2.52.23.201	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	98
79.179.107.15	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	96
46.19.85.186	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	96
109.253.131.11	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	92
46.19.86.246	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	90
109.253.214.162	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	89