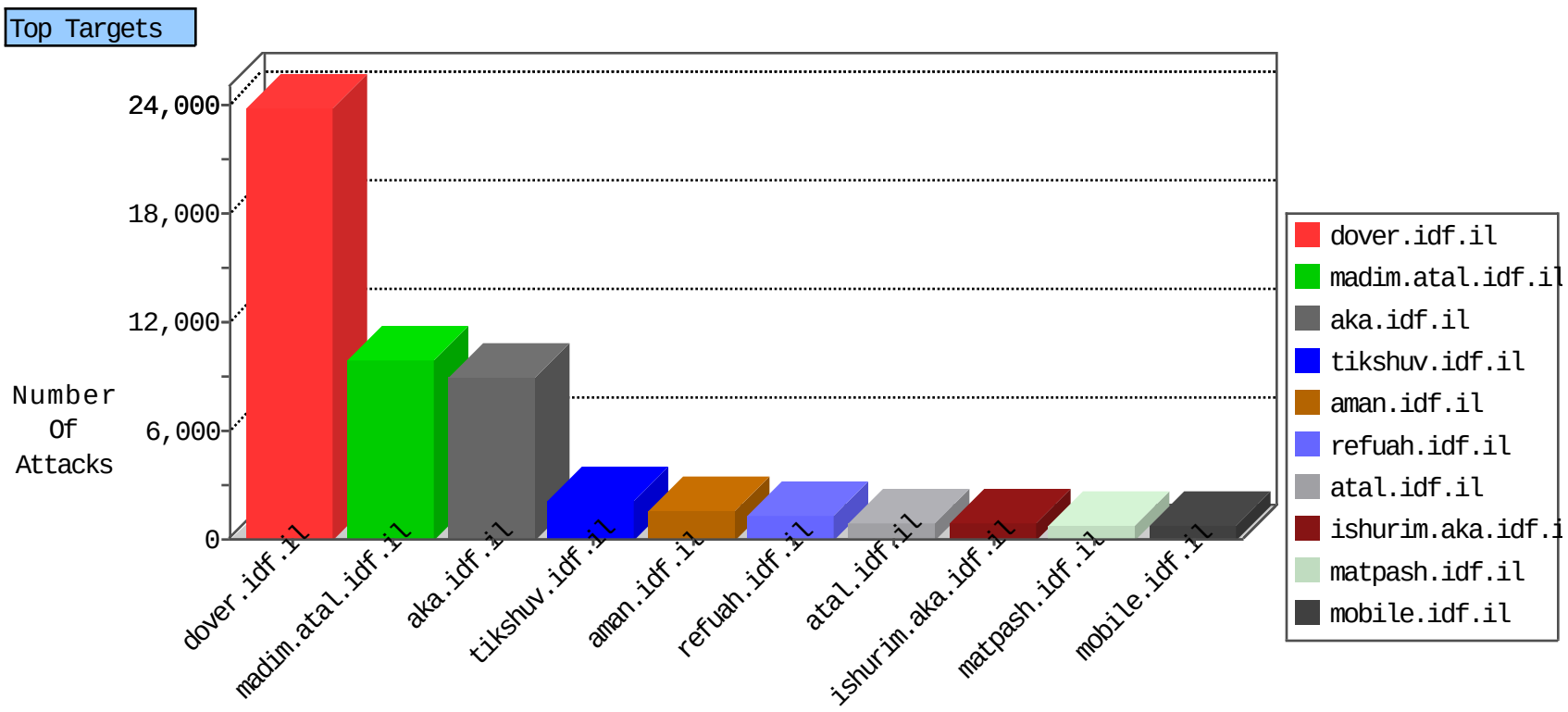
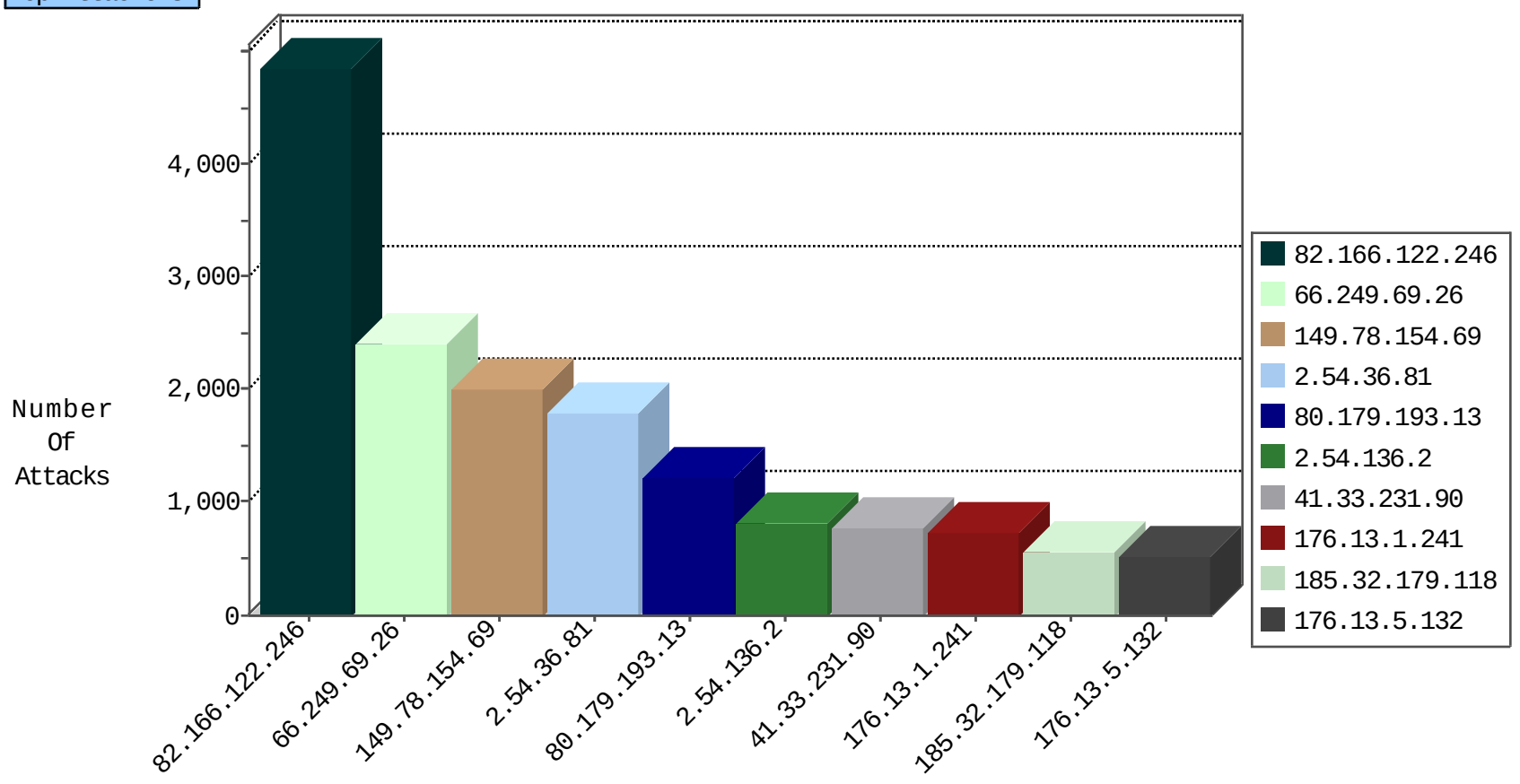
02-14-2016 to 02-15-2016

IDF Under Attack
Daily Report

Top Targets



Top Attackers



02-14-2016 to 02-15-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
207.232.36.181	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	343
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	327
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	196
192.118.30.102	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	150
212.199.112.144	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	148
212.199.154.194	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	115
81.218.241.26	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	109
81.218.241.26	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	97
192.118.30.102	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	91
79.183.21.158	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	65
37.26.148.146	Israel	147.237.77.233	atal.idf.il	Invalid TCP Flags	drop	26
82.145.216.77	Europe	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	22
66.249.69.26	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	11
31.168.232.150	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	11
85.250.161.178	Israel	147.237.77.226	www.chamatz.aka.idf.il	L4 Source or Dest Port Zero	drop	8
84.228.143.250	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	6
31.168.240.21	Israel	147.237.72.166	aka.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
134.147.203.115	Germany	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	4
84.108.85.95	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
185.130.5.224		147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	3
168.235.197.204	United States	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Http	drop	3
212.179.54.237	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
95.86.109.248	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
192.118.132.185	Israel	147.237.77.216	dover.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
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
178.69.38.230	Russian Federation	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	3
222.186.130.223	China	147.237.76.39	mobile.meitav.idf.il	JLM_Purple_Con_Limit_Http	drop	3
212.179.46.189	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
185.130.5.224		147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	3
149.78.154.69	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
185.130.5.224		147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	3
79.182.23.89	Israel	147.237.0.34	tikshuv.idf.il	L4 Source or Dest Port Zero	drop	3
212.179.46.189	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
157.55.39.19	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
91.197.207.192	Russian Federation	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	2
134.147.203.115	Germany	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	2
201.48.16.165	Brazil	147.237.72.167	ishurim.aka.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
185.94.111.1		147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	2
183.11.122.177	China	147.237.76.147	chinuch.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
115.239.228.10	China	147.237.0.34	tikshuv.idf.il	Frk_Under_Attack_Con_Http	drop	2
185.130.5.224		147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	2
134.147.203.115	Germany	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	2
123.151.42.61	China	147.237.76.30	himush.idf.il	Block_Udp_All_Nets_Con_Limit	drop	2
115.230.124.164	China	147.237.76.30	himush.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
157.55.39.147	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
185.130.5.224		147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	2
134.147.203.115	Germany	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	2

02-14-2016 to 02-15-2016

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.166.122.246	Israel	147.237.77.216	dover.idf.il	3886: HTTP: Cross Site Scripting in POST Request	Block	7
85.251.251.9	Spain	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	2
210.1.218.60	Australia	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	2
106.120.173.159	China	147.237.77.233	atal.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
51.254.103.60	United Kingdom	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	1
188.165.15.191	France	147.237.76.147	chinuch.aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1
155.94.254.143	United States	147.237.77.170	maarachot.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1
198.20.69.74	United States	147.237.8.46	e.chinuch.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
41.234.7.141	Egypt	147.237.77.216	dover.idf.il	3886: HTTP: Cross Site Scripting in POST Request	Block	1
180.251.137.58	Indonesia	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
115.42.137.250	Singapore	147.237.77.216	dover.idf.il	12347: HTTP: PHP-CGI Query String Parameter Information Disclosure Vulnerability	Block	1
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
188.165.15.195	France	147.237.0.15	kosher-kravi.idf.il	C228: HTTP: AhrefBot crawler	Block	1
155.94.254.143	United States	147.237.77.234	halag.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1
83.97.83.125	Switzerland	147.237.76.42	refuah.idf.il	14331: HTTP: Suspicious User-Agent (My Session)	Block	1
198.20.69.74	United States	147.237.76.177	ncore.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
42.236.200.105	China	147.237.77.216	dover.idf.il	15324: HTTP: CNC Dialer User-Agent (CNCDialer)	Block	1
185.3.147.188	Israel	147.237.77.74	law.idf.il	C008: HTTP: Xenu UserAgent	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
79.177.19.35	Israel	147.237.72.166	aka.idf.il	C008: HTTP: Xenu UserAgent	Block	1
40.115.22.29	United States	147.237.0.15	kosher-kravi.idf.il	10711: HTTP: ZmEu Vulnerability Scanner	Block	1
188.165.15.223	France	147.237.72.156	aman.idf.il	C228: HTTP: AhrefBot crawler	Block	1
155.94.254.143	United States	147.237.77.235	sviva.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1
198.20.87.98	United States	147.237.76.38	e.e.meitav.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
45.43.221.55		147.237.72.166	aka.idf.il	C008: HTTP: Xenu UserAgent	Block	1
188.165.15.61	France	147.237.72.166	aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1
155.94.254.143	United States	147.237.76.42	refuah.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1
79.177.19.35	Israel	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
40.115.22.29	United States	147.237.0.17	m.my-kosher-kravi.idf.il	10711: HTTP: ZmEu Vulnerability Scanner	Block	1
188.165.15.231	France	147.237.77.176	matpash.idf.il	C228: HTTP: AhrefBot crawler	Block	1
162.210.196.98	United States	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	1
104.167.211.3	Pakistan	147.237.77.216	dover.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
49.246.230.40	China	147.237.77.74	law.idf.il	8479: HTTP: Suspicious HTTP Request	Block	1
188.165.15.160	France	147.237.76.31	nakchal.idf.il	C228: HTTP: AhrefBot crawler	Block	1
155.94.254.143	United States	147.237.77.19	law-forum.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1
79.181.103.246	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
198.20.69.74	United States	147.237.8.28	e.mobile-ks.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
40.115.22.29	United States	147.237.0.19	madim.atal.idf.il	10711: HTTP: ZmEu Vulnerability Scanner	Block	1
162.250.190.142	Canada	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1

02-14-2016 to 02-15-2016

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	36
82.166.122.246	147.237.77.216	Israel	dover.idf.il	SERVER-WEBAPP WEB-INF access	34
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	31
82.166.122.246	147.237.77.216	Israel	dover.idf.il	POLICY-OTHER script tag in URI - likely cross-site scripting attempt	27
82.166.122.246	147.237.77.216	Israel	dover.idf.il	ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attempt	27
66.249.93.91	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	24
82.166.122.246	147.237.77.216	Israel	dover.idf.il	tehila expiremental XSS in POST	14
82.166.122.246	147.237.77.216	Israel	dover.idf.il	SERVER-WEBAPP cross-site scripting attempt via form data attempt	14
82.166.122.246	147.237.77.216	Israel	dover.idf.il	SERVER-WEBAPP /etc/passwd file access attempt	14
82.166.122.246	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	3
180.251.137.58	147.237.77.216	Indonesia	dover.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	3
221.139.14.120	147.237.77.216	Korea, Republic of	dover.idf.il	Tehila - Perl LWP with fake user agent	3
66.249.81.230	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	2
132.252.173.4	147.237.77.216	Germany	dover.idf.il	GPL SCAN nmap TCP	2
66.249.69.26	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
59.45.79.117	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	2
66.249.66.15	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
109.253.205.21	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
79.176.165.67	147.237.72.156	Israel	aman.idf.il	ET SCAN NMAP -sA (2)	2
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
59.45.79.117	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	2
94.188.248.70	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
85.250.124.73	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sA (2)	2
94.102.48.193	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.88.187	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
94.102.48.193	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	2
212.235.98.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
59.45.79.117	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	2
132.74.95.21	147.237.77.170	Israel	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
59.45.79.117	147.237.77.233	China	atal.idf.il	ET SCAN Potential SSH Scan	2
69.197.145.242	147.237.77.178	United States	e.matpash.idf.il	ET SCAN Potential SSH Scan	2
59.45.79.117	147.237.77.74	China	law.idf.il	ET SCAN Potential SSH Scan	2
64.233.172.163	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
94.102.48.193	147.237.76.198	Netherlands	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
80.246.130.47	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
222.170.70.222	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.147.103.155	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
182.234.150.46	147.237.8.46	Taiwan	e.chinuch.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
37.26.147.198	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.66.208.131	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.250.200.41	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.125.98.56	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
200.188.147.131	147.237.76.34	Mexico	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.120.20.83	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
125.27.179.82	147.237.76.39	Thailand	mobile.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.45.79.117	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
149.50.87.208	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.33.174	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
105.226.175.208	147.237.76.196	South Africa	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
192.115.97.253	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

02-14-2016 to 02-15-2016

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2057
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	678
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Command Injection		monitor	423
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	195
46.117.255.151	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	192
23.27.220.137	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	180
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	175
212.76.127.44	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	159
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	158
80.246.133.197	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	157
31.210.187.242	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	150
212.179.155.129	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	127
212.76.127.111	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	126
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	111
64.237.46.194	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	94
64.237.46.194	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	94
77.126.68.197	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
208.109.97.62	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	84
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	83
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	73
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	61
46.19.85.121	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
213.57.143.236	Israel	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	59
80.246.133.148	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	57
212.76.127.219	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	57
80.178.100.167	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	57
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	55
168.235.197.204	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	53
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	53
2.54.170.191	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	53
79.67.165.140	United Kingdom	147.237.76.42	refuah.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	53
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	52
212.179.21.194	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	50
82.166.122.246	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
80.246.130.141	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	48
168.235.197.144	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	48
46.121.82.102	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
37.26.149.237	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
46.19.85.82	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	43
85.65.151.232	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	40
79.182.203.168	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
2.52.137.213	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	38
176.13.16.217	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	37
2.52.137.213	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	37
46.19.85.191	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
84.108.124.64	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	36
81.218.241.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	36
212.179.172.219	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	36
84.111.180.57	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	35
85.65.151.232	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	35

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2357
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1956
80.179.193.13	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1216
2.54.36.81	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	1112
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 82.166.122.246	Block	682
52.16.5.197	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	481
2.54.136.2	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	441
2.54.36.81	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	429
176.13.1.241	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	421
157.55.39.19	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	408
208.109.97.62	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	380
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	356
2.54.136.2	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	331
157.55.39.159	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	315
185.32.179.118	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	309
40.77.167.100	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	308
176.13.5.132	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	272
79.180.13.226	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 79.180.13.226	Block	266
2.54.36.81	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	258
50.87.144.145	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	239
192.249.66.247	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	233
176.13.1.241	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 176.13.1.241	Block	211
46.19.85.159	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.85.159	Block	208
46.19.85.159	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	198
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	192
87.69.211.140	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 87.69.211.140	Block	169
185.32.179.118	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	155
46.19.86.199	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	143
37.26.149.183	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	131
52.33.66.29	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	129
176.13.5.132	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	127
185.32.179.32	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	127
109.253.208.125	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	124
2.54.49.28	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	124
46.19.86.109	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	124
79.180.13.226	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 79.180.13.226	Block	121
176.13.12.4	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	120
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	117
87.69.211.140	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	117
2.54.168.158	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	114
84.110.33.22	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	113
2.54.31.77	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	112
176.13.12.4	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	111
79.180.13.226	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	110
2.52.48.96	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	108
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	108
176.13.1.241	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
84.110.33.22	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
176.13.5.132	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
185.32.179.118	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104