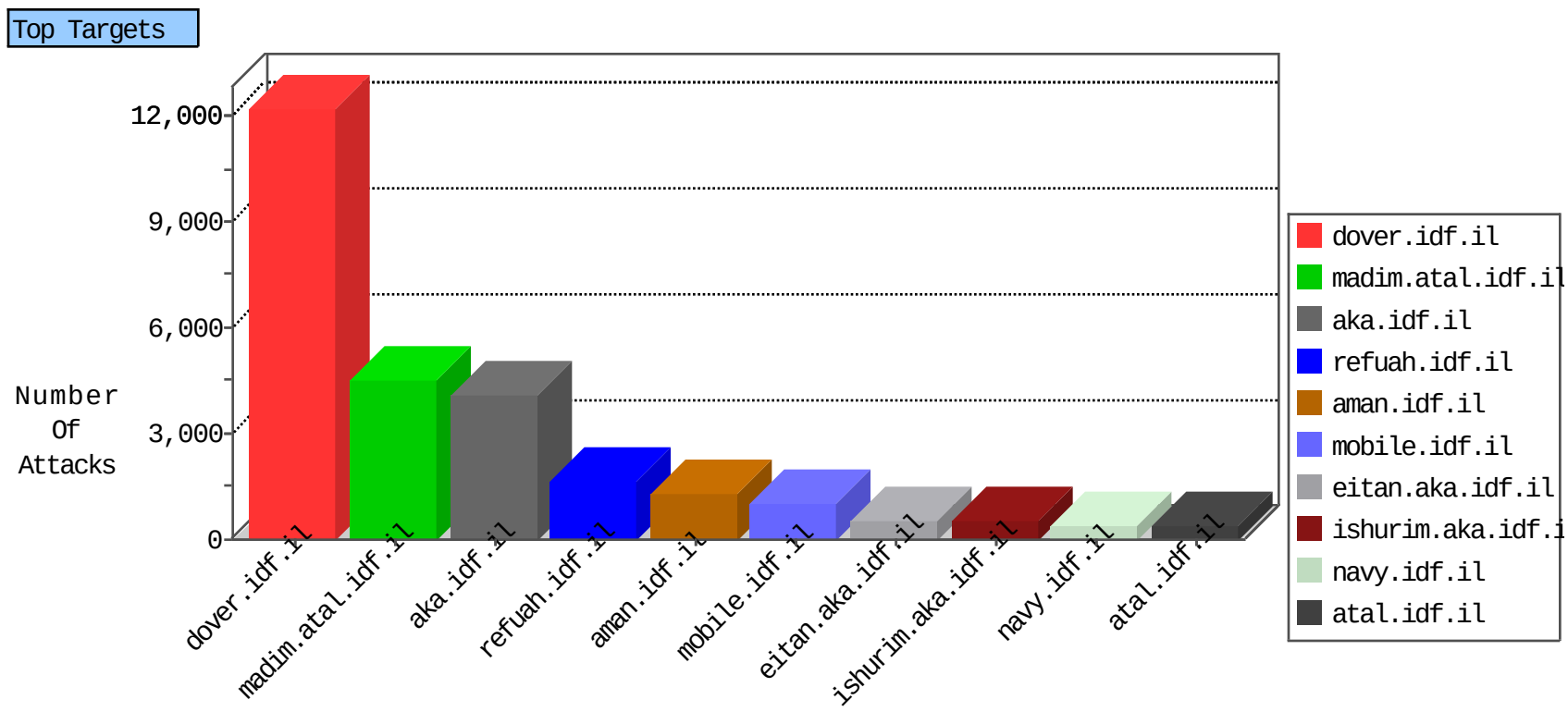
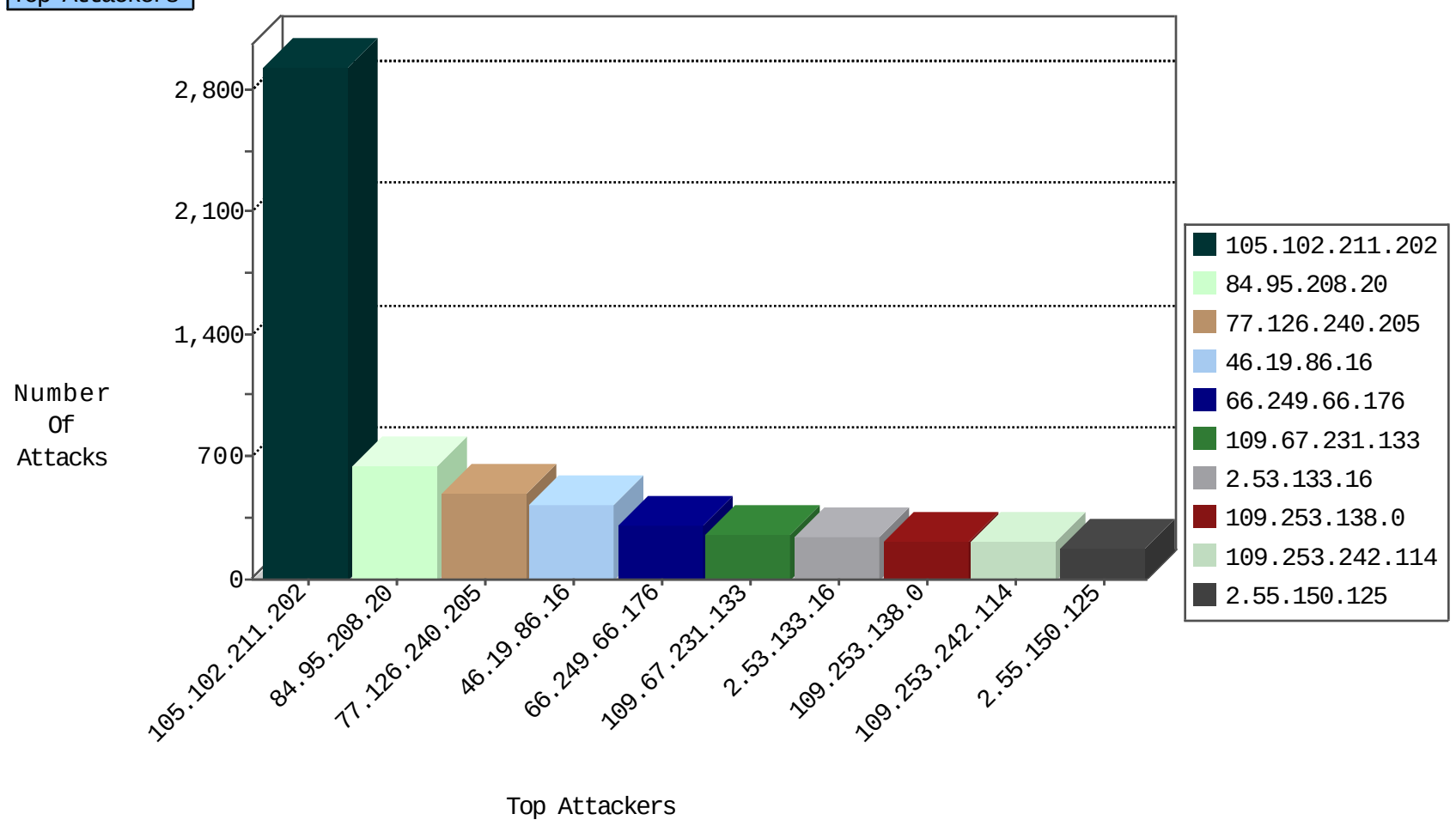
09-20-2016 to 09-21-2016

IDF Under Attack
Daily Report

Top Targets



Top Attackers



09-20-2016 to 09-21-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	89
46.19.86.116	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	65
2.55.134.201	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	54
93.192.105.18	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	42
0.0.0.0		147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	32
46.19.85.99	Israel	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	30
176.13.2.99	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	27
213.57.218.151	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	22
109.66.96.114	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	18
84.108.42.131	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	15
130.195.4.69	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	14
129.10.120.193	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	14
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	13
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	13
200.19.159.34	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	13
2.53.35.87	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	12
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	12
139.78.141.243	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	12
129.93.229.139	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	12
134.197.113.3	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	12
194.29.178.14	Poland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	11
128.223.8.114	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	11
131.247.2.241	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	11
168.235.197.147	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	11
195.93.234.9	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	10
198.133.224.147	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	10
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	9
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	9
89.138.199.105	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
130.206.158.138	Spain	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	9
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	9
2.55.39.26	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9
195.113.161.83	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	8
79.177.151.20	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	8
204.85.191.10	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	8
147.83.29.234	Spain	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	8
2.53.49.74	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
128.42.142.45	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	8
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	8
80.179.10.113	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
185.3.147.70	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
130.194.252.8	Australia	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	8
79.180.173.192	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
194.254.215.12	France	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	8
109.253.135.88	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
193.1.13.14	Ireland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	7
77.138.52.97	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
208.94.63.194	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	7

09-20-2016 to 09-21-2016

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
69.30.198.178	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	110
69.30.211.2	United States	147.237.76.200	eitan.aka.idf.il	C1000074: HTTP: majestic bot	Permit	66
69.30.211.2	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	53
69.30.211.2	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	13
69.30.211.2	United States	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	12
199.58.86.206	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	10
162.210.196.130	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	6
108.59.8.70	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	6
199.58.86.206	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	6
69.30.211.2	United States	147.237.77.226	www.chamatz.aka.idf.il	C1000074: HTTP: majestic bot	Permit	5
144.76.29.162	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3
62.212.73.211	Netherlands	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3
125.64.94.206	China	147.237.77.176	matpash.idf.il	C1000003: HTTP: phpMyAdmin access	Permit	3
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	3
108.59.8.70	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
199.58.86.209	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
62.210.97.48	France	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	2
83.149.126.98	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
69.30.211.2	United States	147.237.76.31	nakchal.idf.il	C1000074: HTTP: majestic bot	Permit	2
46.165.197.142	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
199.58.86.211	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
69.30.211.2	United States	147.237.76.42	refuah.idf.il	C1000074: HTTP: majestic bot	Permit	2
51.254.131.246	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
123.126.68.101	China	147.237.77.74	law.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
162.210.196.100	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
199.58.86.206	United States	147.237.76.42	refuah.idf.il	C1000074: HTTP: majestic bot	Permit	2
51.254.131.246	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
69.30.211.2	United States	147.237.0.34	tikshuv.idf.il	C1000074: HTTP: majestic bot	Permit	2
162.210.196.129	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
62.210.97.48	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
78.166.58.106	Turkey	147.237.72.166	aka.idf.il	C1000018: HTTP: access to administrator/index.php -> Quarantine	Permit	1
36.110.147.80	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1
151.80.31.107	France	147.237.76.86	navy.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
173.31.183.87	United States	147.237.72.167	ishurim.aka.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1
23.228.101.162	United States	147.237.0.19	madim.atal.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	1
151.80.31.160	France	147.237.0.34	tikshuv.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
89.248.172.16	Netherlands	147.237.0.19	madim.atal.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
71.6.146.185	United States	147.237.0.16	my-kosher-kravi.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
210.212.230.170	India	147.237.77.176	matpash.idf.il	12347: HTTP: PHP-CGI Query String Parameter Information Disclosure Vulnerability	Block	1
23.228.101.162	United States	147.237.77.216	dover.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	1
105.98.143.91	Algeria	147.237.77.176	matpash.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
78.166.58.106	Turkey	147.237.72.166	aka.idf.il	C1000016: HTTP: administrator in URI	Permit	1
36.110.147.66	China	147.237.77.74	law.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

09-20-2016 to 09-21-2016

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.66.176	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	312
66.249.64.124	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	142
79.183.92.9	147.237.76.86	Israel	navy.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	23
91.121.222.79	147.237.72.166	France	aka.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	6
66.249.79.103	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	4
105.98.143.91	147.237.77.176	Algeria	matpash.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	4
58.218.200.137	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	3
193.201.227.81	147.237.8.28	Ukraine	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	3
66.249.79.99	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	3
77.126.240.205	147.237.72.156	Israel	aman.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
220.132.224.48	147.237.8.14	Taiwan	e.orchot.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
138.99.12.34	147.237.77.234	Brazil	halag.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
193.201.227.81	147.237.76.86	Ukraine	navy.idf.il	ET SCAN Potential SSH Scan	2
198.52.97.89	147.237.77.74	United States	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
182.255.0.4	147.237.0.200	Indonesia	m4u.idf.il	ET SCAN Potential SSH Scan	2
218.161.81.122	147.237.0.200	Taiwan	m4u.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
105.102.211.202	147.237.77.216	Algeria	dover.idf.il	portscan: TCP Distributed Portscan	2
121.32.129.130	147.237.77.212	China	e.dover.idf.il	GPL SCAN nmap TCP	2
91.224.160.106	147.237.8.27	Netherlands	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	2
193.201.227.81	147.237.72.14	Ukraine	dover.idf.il(old)	ET SCAN Potential SSH Scan	2
213.162.105.152	147.237.77.176	United Kingdom	matpash.idf.il	Tehila - Perl LWP with fake user agent	2
61.72.64.106	147.237.76.148	Korea, Republic of	gqcenter.aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
27.24.237.9	147.237.77.243	China	mobile.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
59.127.162.129	147.237.77.212	Taiwan	e.dover.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
195.154.184.122	147.237.72.166	France	aka.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
109.253.142.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
213.57.87.140	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
41.230.31.128	147.237.76.147	Tunisia	chinuch.aka.idf.il	ET SCAN NMAP -sS window 3072	2
170.149.168.65	147.237.77.74	United States	law.idf.il	Tehila - Perl LWP with fake user agent	2
77.127.35.181	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
91.121.222.79	147.237.77.74	France	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
91.121.220.181	147.237.77.74	France	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
91.224.160.106	147.237.77.74	Netherlands	law.idf.il	ET SCAN Potential SSH Scan	2
193.201.227.81	147.237.0.16	Ukraine	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
193.201.227.81	147.237.77.235	Ukraine	sviva.idf.il	ET SCAN Potential SSH Scan	2
218.239.159.25	147.237.72.167	Korea, Republic of	ishurim.aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	2
182.255.0.6	147.237.0.19	Indonesia	madim.atal.idf.il	ET SCAN Potential SSH Scan	2
50.87.144.145	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	2
91.224.160.106	147.237.0.33	Netherlands	idf.il	ET SCAN Potential SSH Scan	2
125.130.62.100	147.237.0.19	Korea, Republic of	madim.atal.idf.il	ET SCAN Potential SSH Scan	2
27.24.237.9	147.237.77.234	China	halag.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
128.232.110.28	147.237.77.170	United Kingdom	maarachot.idf.il	ET SCAN Potential SSH Scan	2
193.201.227.81	147.237.76.199	Ukraine	e.nakchal.idf.il	ET SCAN Potential SSH Scan	2
58.227.55.118	147.237.0.15	Korea, Republic of	kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
183.60.48.25	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	2
118.103.126.194	147.237.0.19	Japan	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	2
128.232.110.28	147.237.76.38	United Kingdom	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	2
41.230.31.128	147.237.76.147	Tunisia	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	2
128.199.254.234	147.237.76.200	Singapore	eitan.aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1

09-20-2016 to 09-21-2016

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
105.102.211.202	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2931
109.253.200.44	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	150
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	136
81.144.140.102	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	130
188.120.154.153	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	114
80.246.130.211	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	109
147.235.185.74	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	98
168.235.197.147	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	94
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	87
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	82
168.235.196.91	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	78
80.179.255.94	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	78
89.187.217.10	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	73
2.53.63.22	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	70
194.39.218.10	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	63
79.177.107.132	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	62
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
2.53.166.2	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
2.53.46.187	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
5.28.164.51	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	60
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
62.0.221.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
217.132.99.86	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	58
62.0.207.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	55
193.171.152.104	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
2.53.11.180	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
213.8.72.226	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	48
85.64.159.213	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	48
62.0.236.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	45
62.0.214.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	45
195.93.234.8	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
193.43.246.250	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	42
46.19.85.190	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	42
195.229.120.98	United Arab Emirates	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
213.71.171.203	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
109.67.231.133	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
80.246.138.19	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
147.235.185.74	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	35
207.241.229.68	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	35
109.65.92.27	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	34
62.0.244.1	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	33
62.0.208.254	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	32
62.0.235.160	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	32
62.0.221.129	Israel	147.237.76.30	himush.idf.il	drop	First packet isn't SYN	drop	32
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
66.249.93.87	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
176.13.17.211	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	31
46.19.85.52	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	31
2.53.163.26	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
46.19.85.52	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	30

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	401
2.53.133.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	244
109.67.231.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	223
109.253.138.0	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	217
109.253.242.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	208
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	186
2.55.150.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	179
80.246.136.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	152
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	137
2.53.158.38	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	129
109.253.245.151	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	121
109.253.147.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	119
2.53.56.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	108
2.53.50.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
109.253.221.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
46.19.86.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	100
37.26.149.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	100
46.19.85.127	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	99
185.24.204.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	96
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	91
46.19.85.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	82
80.246.139.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	78
46.19.86.9	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	78
176.13.233.135	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	71
77.126.54.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	70
109.253.230.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	69
2.53.191.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	65
79.178.60.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	60
185.32.179.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	59
176.13.234.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	58
2.53.146.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	58
213.57.187.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	53
46.19.85.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	50
81.218.251.250	Israel	147.237.76.86	navy.idf.il	Unauthorized HTTP Method	Block	48
5.29.97.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	47
46.19.85.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	45
46.19.85.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	45
80.246.136.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
46.19.86.249	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	38
109.253.143.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Method from 77.126.240.205	Block	35
46.19.86.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
46.19.86.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
212.199.57.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	34
2.53.144.128	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	33
81.218.251.250	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/style/shared/	Block	32
46.19.86.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31
84.111.30.69	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	28
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Distributed Malformed URL	Block	25
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	25

09-20-2016 to 09-21-2016