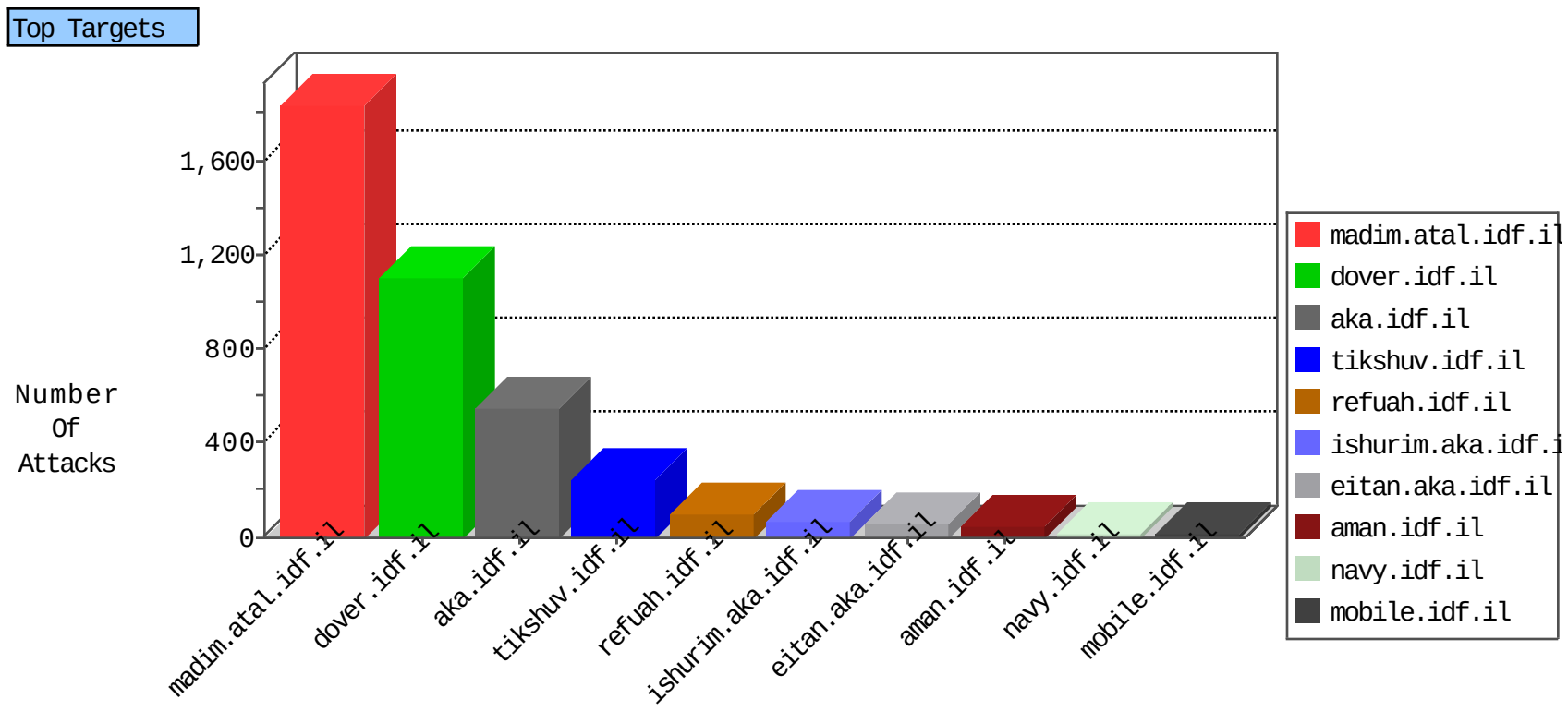
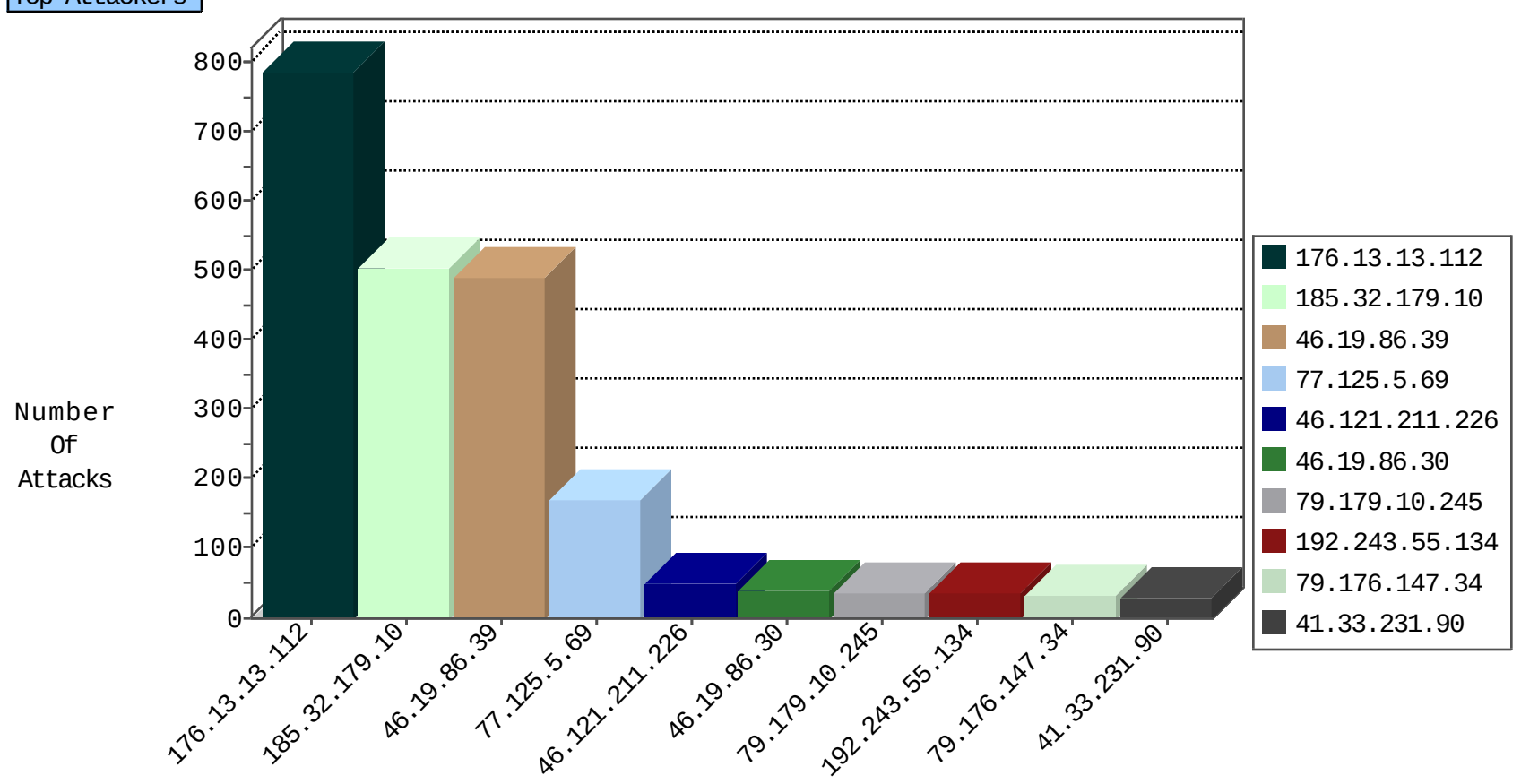
02-21-2016-18:04:04 to 02-21-2016-19:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-21-2016-18:04:04 to 02-21-2016-19:04:04

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	33
85.65.188.110	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	19
185.120.125.41		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
109.160.147.207	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
87.69.106.238	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
46.19.85.186	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
46.19.85.226	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
2.54.55.230	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
213.8.204.70	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
109.64.104.75	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
109.66.121.166	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
84.94.74.231	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
46.19.85.167	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
46.19.85.176	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
5.29.79.115	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
79.176.198.1	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
37.26.147.132	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
80.246.133.201	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
37.142.180.6	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
149.78.154.69	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
2.54.36.154	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
185.3.144.12	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	2
134.147.203.115	Germany	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	2
185.130.5.201		147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
141.212.122.220	United States	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
2.54.160.167	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
185.130.5.201		147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
109.66.123.213	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
192.168.1.13		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
89.248.174.4	Netherlands	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.201		147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
37.142.180.6	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
10.0.0.5		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
185.130.5.201		147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1

02-21-2016-18:04:04 to 02-21-2016-19:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.111.209.100	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
87.71.42.114	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
79.176.99.193	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
80.246.133.206	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
149.202.47.161	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
69.30.205.218	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
149.202.47.161	Germany	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Block	2
188.165.15.55	France	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
198.20.69.74	United States	147.237.76.202	e.halag.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
66.249.66.190	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

02-21-2016-18:04:04 to 02-21-2016-19:04:04

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	3
188.120.148.141	147.237.77.216	Israel	dover.idf.il	ET SCAN NMAP -sA (2)	2
109.65.62.59	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	2
79.176.120.143	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.8.204.54	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.148.29.148	147.237.0.33	Hong Kong	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.117.127.177	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
125.212.232.146	147.237.76.86	Vietnam	navy.idf.il	ET SCAN NMAP -sS window 1024	1
5.29.198.38	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.143.199.164	147.237.8.45	Kyrgyzstan	e.eitan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
2.54.171.127	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.228.6.54	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.94.188.216	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.81.97.178	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.183.7	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
74.201.85.87	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.74	147.237.76.202	United States	e.halag.idf.il	ET DROP Dshield Block Listed Source	1
58.176.160.211	147.237.0.34	Hong Kong	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
37.60.44.180	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.29.152.243	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.193	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
84.108.64.31	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.94.46.149	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.178.195.147	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

02-21-2016-18:04:04 to 02-21-2016-19:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.121.211.226	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
79.179.10.245	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
79.176.147.34	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	31
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
109.253.144.155	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	26
192.115.248.2	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
94.159.179.127	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
107.167.107.153	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	23
109.64.139.29	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
212.117.154.242	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
2.54.16.219	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
149.88.220.111	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
84.94.74.231	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
37.26.146.237	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
2.54.177.139	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.179.213.153	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
87.71.54.149	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.179.213.153	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.116.21.156	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
37.26.146.237	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
46.19.85.226	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
188.120.134.181	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
46.19.85.152	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.179.196.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.85.121	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.127.202.190	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
109.67.68.63	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.107	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
31.168.116.240	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.58	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.176	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
82.81.66.189	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
79.182.59.23	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.127.202.190	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
37.26.149.219	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.112	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.26.148.179	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.6	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.46.41.243	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.149.219	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.100	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.192	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
66.249.79.86	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.54	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.173	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6

02-21-2016-18:04:04 to 02-21-2016-19:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.13.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	550
185.32.179.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	375
46.19.86.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	351
176.13.13.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	238
77.125.5.69	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	168
46.19.86.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	139
185.32.179.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	129
46.19.86.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	40
77.125.115.24	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.125.115.24	Block	20
109.65.159.157	Israel	147.237.77.216	dover.idf.il	Distributed Too Many of the Same Response Code (404)	Block	10
85.250.136.247	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 85.250.136.247	Block	10
77.125.115.24	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	6
109.186.144.171	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	6
85.250.136.247	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	6
109.186.144.171	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.186.144.171	Block	6
188.228.38.48	Denmark	147.237.77.216	dover.idf.il	Distributed Too Many of the Same Response Code (404)	Block	4
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
197.36.250.183	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	4
79.177.180.63	Israel	147.237.76.31	nakchal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	4
199.30.25.48	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
80.246.130.182	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
157.55.12.67	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
197.36.250.183	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	4
80.246.130.194	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
66.249.81.218	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
109.186.144.171	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/updatestatus.php	Block	4
85.64.6.109	Israel	147.237.76.31	nakchal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	4
199.30.24.77	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
85.64.153.59	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtContent in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	4
46.121.37.72	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	4
199.30.24.196	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
176.13.20.134	Israel	147.237.76.31	nakchal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3
2.54.182.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.41.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
80.246.133.104	Israel	147.237.76.31	nakchal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3
66.249.81.212	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
80.246.133.188	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	2
2.54.173.126	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
93.172.244.231	Israel	147.237.72.166	aka.idf.il	Unknown Parameter gws_rd in www.aka.idf.il/giyus/	None	2
85.250.136.247	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
46.19.85.5	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version like Gecko) Version/10.3.2.2876 Mobile Safari/537.35+	Block	2
128.232.110.28	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	2
213.8.204.83	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
5.15.204.76	Romania	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	2
157.55.39.215	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	2
141.212.122.129	United States	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to /x	Block	2

02-21-2016-18:04:04 to 02-21-2016-19:04:04