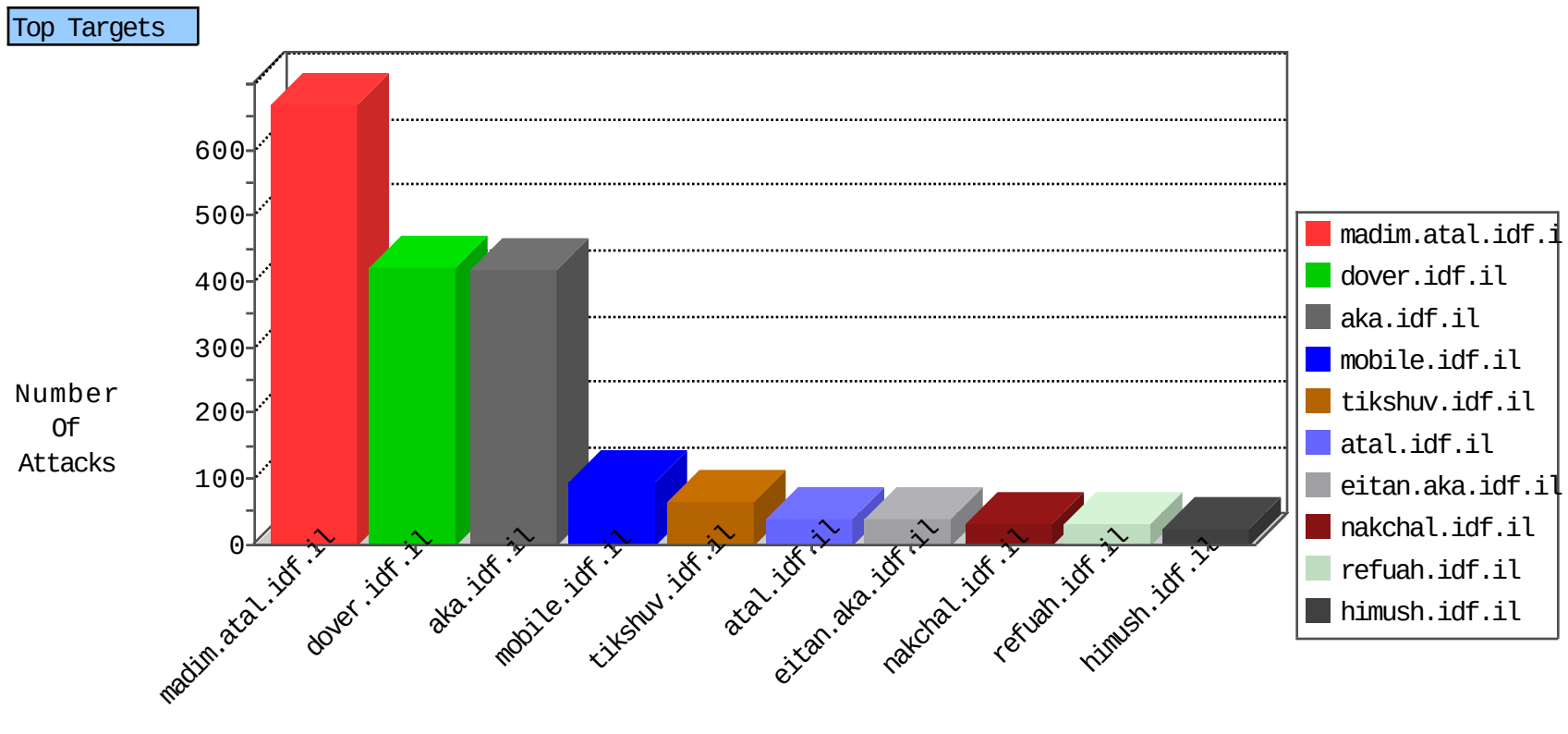
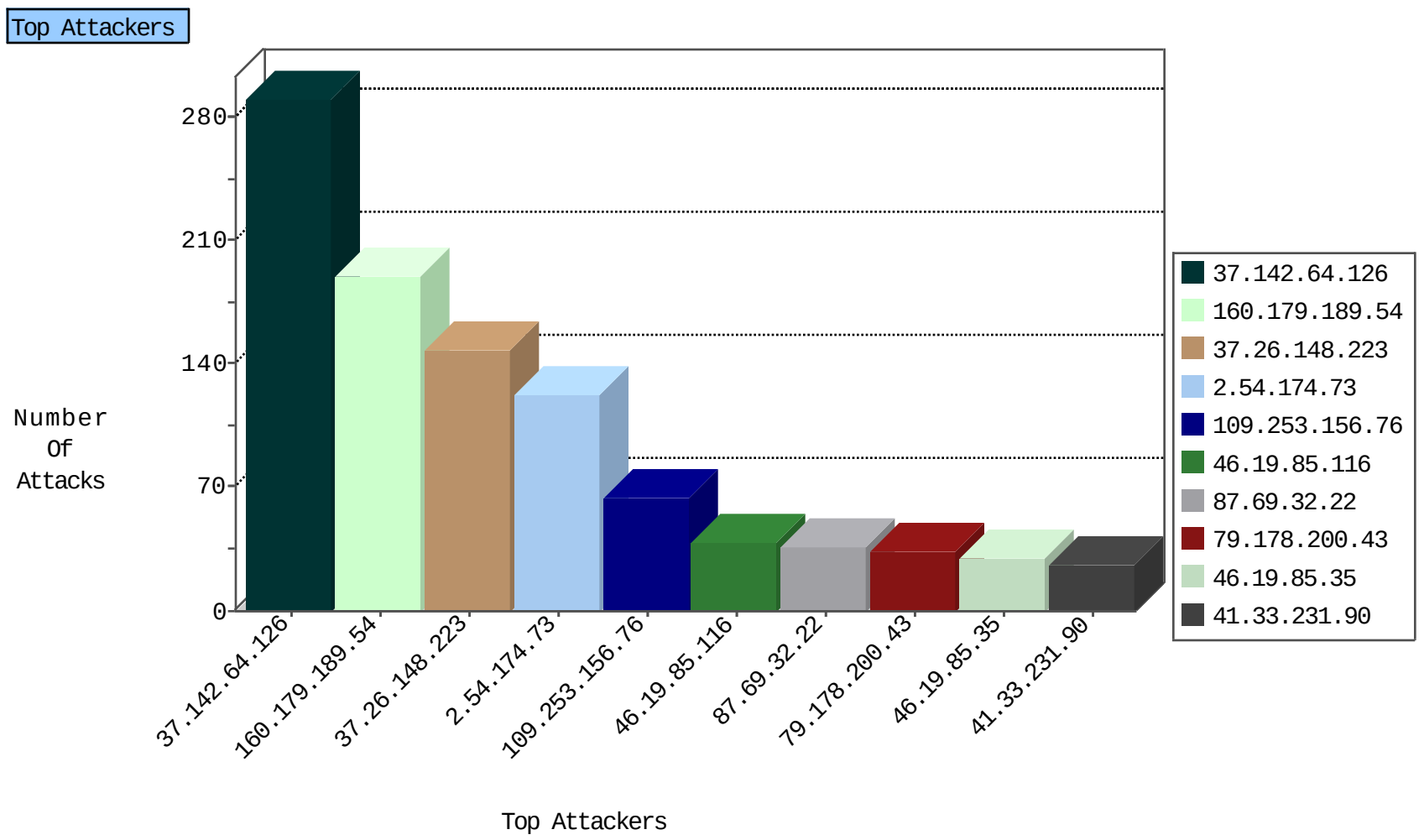
02-28-2016-16:04:03 to 02-28-2016-17:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-28-2016-16:04:03 to 02-28-2016-17:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
193.104.77.4	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
79.180.120.16	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
115.239.228.10	China	147.237.0.200	m4u.idf.il	JLM_Under_Attack_Con_Http	drop	2
198.20.70.114	United States	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
185.112.102.166		147.237.76.176	test.ncore.idf.il	JLM_Purple_Con_Limit_Http	drop	1
185.130.5.224		147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
115.239.228.10	China	147.237.0.200	m4u.idf.il	JLM_Purple_Con_Limit_Http	drop	1

02-28-2016-16:04:03 to 02-28-2016-17:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.138.169.64	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
37.26.147.230	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
84.111.163.138	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
46.19.86.172	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
46.116.172.85	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
79.182.180.207	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
185.3.147.196	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
79.177.135.127	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
91.121.211.59	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
5.9.111.70	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
213.251.184.38	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
136.243.103.165	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
79.183.145.211	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
149.78.253.223	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
51.255.65.69	United Kingdom	147.237.77.170	maarachot.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
160.179.189.54		147.237.77.216	dover.idf.il	3630: HTTP: SQL Injection (Boolean Identity)	Block	1
66.249.64.190	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
51.255.65.77	United Kingdom	147.237.77.170	maarachot.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.8	United Kingdom	147.237.77.170	maarachot.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.79	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.9	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.85	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.41	United Kingdom	147.237.77.170	maarachot.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.90	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

02-28-2016-16:04:03 to 02-28-2016-17:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
160.179.189.54	147.237.77.216		dover.idf.il	SERVER-WEBAPP admin.php access	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
93.172.23.50	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.146.249	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.109.115.135	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.139.232	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.114.23.18	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.176.230.165	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.106	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
151.11.201.3	147.237.77.61	Italy	e.cogat.idf.il	ET SCAN NMAP -sS window 3072	1
2.54.25.242	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.255.65.207	147.237.8.46		e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
98.119.105.221	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 4096	1
94.102.48.193	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
217.132.62.252	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.228.185.62	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.118.67	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.81.57.208	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.182.155.90	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
160.179.189.54	147.237.77.216		dover.idf.il	portscan: TCP Distributed Portscan	1
62.219.229.9	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
160.179.189.54	147.237.77.216		dover.idf.il	OS-WINDOWS Microsoft Forefront UAG javascript handler in URI XSS attempt	1
37.26.149.179	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.67.222.125	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.255.65.207	147.237.8.24		e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
95.86.124.117	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

02-28-2016-16:04:03 to 02-28-2016-17:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.85.116	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
79.178.200.43	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	20
46.19.85.35	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
77.127.209.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
77.126.220.231	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
132.74.44.166	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.178.200.43	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
176.13.4.64	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
87.69.32.22	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
46.19.85.35	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
199.203.215.1	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
87.69.32.22	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	10
62.219.130.248	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
99.60.110.103	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
185.3.147.196	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
79.178.182.205	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.140	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
199.203.215.1	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
212.25.105.8	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.85.112	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.180.178.162	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
46.120.73.224	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
46.19.85.105	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
176.13.15.109	Israel	147.237.72.166	aka.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
46.19.85.161	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
80.179.235.210	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
87.68.72.235	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.112	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.132.191	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.105	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.246.138.88	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.132.191	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.22.12	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
176.13.11.130	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.131.24	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
87.68.248.250	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.0	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.168	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.69.32.22	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
31.154.154.188	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
87.69.32.22	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
87.69.32.22	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
5.102.254.210	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
188.120.154.228	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
80.246.137.123	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4

02-28-2016-16:04:03 to 02-28-2016-17:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.142.64.126	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	291
37.26.148.223	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	144
2.54.174.73	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	123
160.179.189.54		147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 160.179.189.54	Block	98
109.253.156.76	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	64
160.179.189.54		147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1362-he/dover.aspx	Block	31
160.179.189.54		147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1362-he/dover.aspx	Block	18
109.253.221.61	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
160.179.189.54		147.237.77.216	dover.idf.il	Multiple Admin Blocking from 160.179.189.54	Block	13
160.179.189.54		147.237.77.216	dover.idf.il	PHP Attempt	Block	10
160.179.189.54		147.237.77.216	dover.idf.il	Parameter Type Violation lang in www.idf.il/1362-he/dover.aspx	Block	10
46.19.85.162	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
109.253.223.15	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
66.249.69.38	United States	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.69.38	Block	6
66.249.69.30	United States	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.69.30	Block	5
46.118.114.75	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi/	Block	5
66.249.66.69	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.66.69	Block	4
66.249.79.75	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.75	Block	4
66.249.64.185	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 66.249.64.185	Block	3
160.179.189.54		147.237.77.216	dover.idf.il	Multiple signatures from 160.179.189.54	Block	3
176.13.12.8	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.116	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/authentication/index	Block	3
46.19.85.130	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.147.156	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
66.249.69.46	United States	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.69.46	Block	2
46.19.85.15	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
79.179.27.232	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.179.27.232	Block	2
62.0.34.177	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	2
37.26.148.223	Israel	147.237.0.19	madim.atal.idf.i	Untraceable SSL Sessions: Open Mode	None	2
66.249.64.190	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 66.249.64.190	Block	2
5.22.131.24	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
79.177.6.184	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
66.249.64.180	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/searchresultsidf/searchresultsidf.aspx	Block	1
185.89.217.227		147.237.76.42	refuah.idf.il	URL is Above Root Directory www.refua.atal.idf.il/../images/shared/home.png	Block	1
95.86.99.8	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ved in www.aka.idf.il/rights/asp/info.asp	None	1
81.218.190.43	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 81.218.190.43 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Header Name	Block	1
2.54.150.146	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
109.67.127.206	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/0/	Block	1
66.249.64.212	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/templates/searchresults/searchresults.aspx	Block	1
176.13.11.130	Israel	147.237.77.243	mobile.idf.il	Suspicious Response Code	Block	1
87.69.134.153	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/	Block	1
46.120.73.224	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
160.179.189.54		147.237.77.216	dover.idf.il	Parameter Type Violation __EVENTTARGET in www.idf.il/1133-he/dover.aspx	Block	1
37.26.148.188	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
141.212.122.64	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to /x	Block	1
193.16.147.2	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/3/size338x0/1613.jpg	Block	1
95.86.99.8	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 95.86.99.8	Block	1
81.218.190.43	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
46.19.86.95	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1

02-28-2016-16:04:03 to 02-28-2016-17:04:03