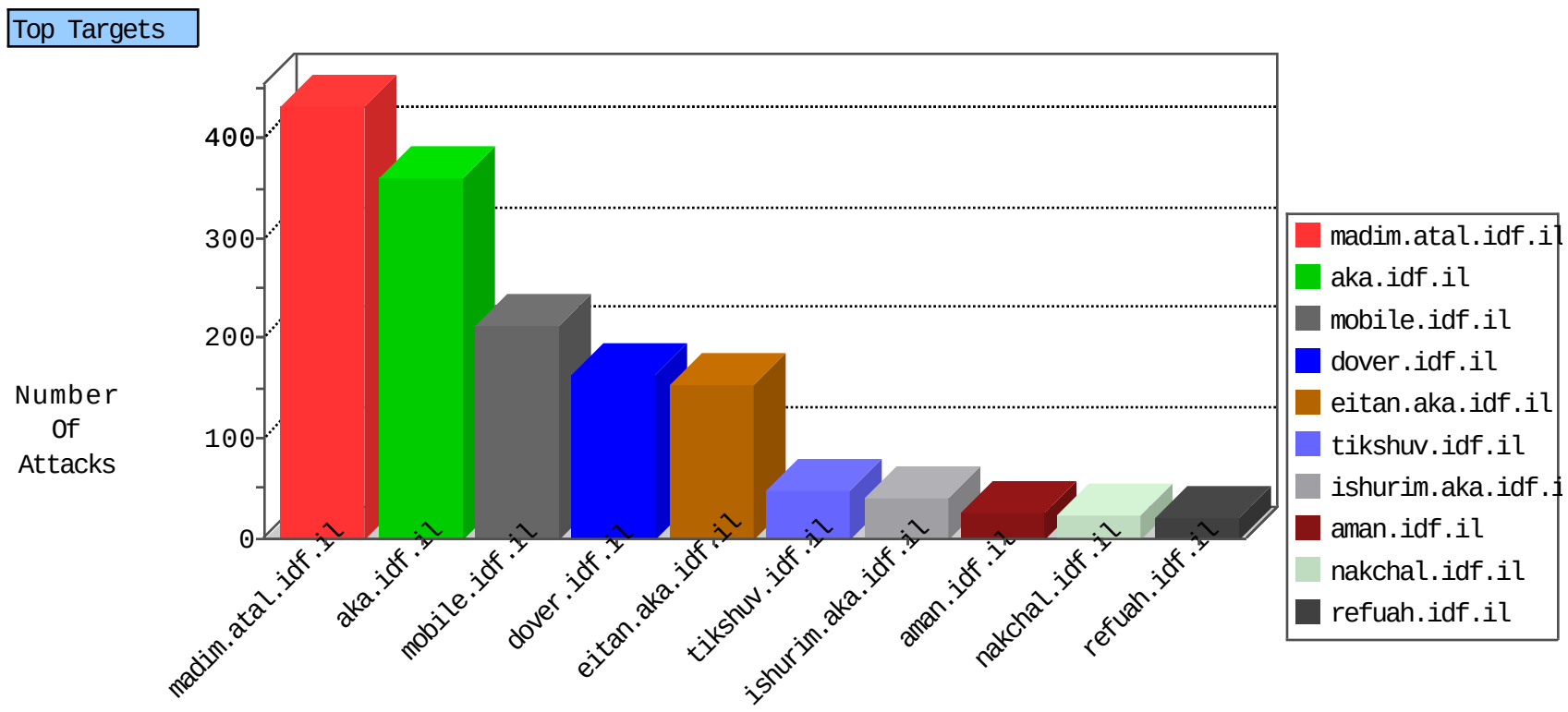
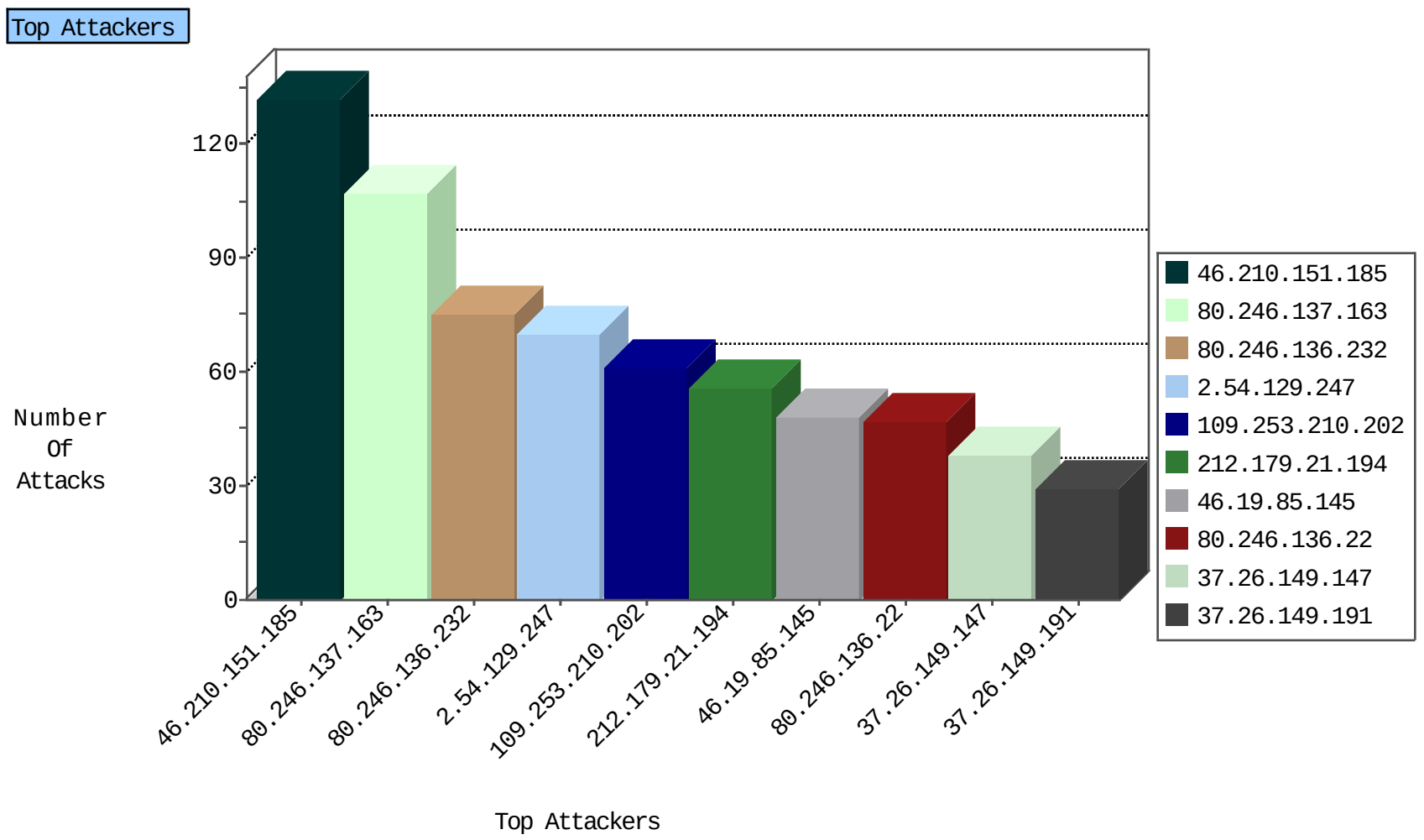
02-28-2016-12:04:00 to 02-28-2016-13:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-28-2016-12:04:00 to 02-28-2016-13:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
208.109.97.62	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	187633
109.65.104.164	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	2
134.147.203.115	Germany	147.237.72.166	aka.idf.il	Block_Ntp_All_Net	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
185.94.111.1		147.237.77.74	law.idf.il	Block_Udp_All_Nets	drop	1
14.211.52.35	China	147.237.8.14	e.orchot.idf.il	Block_Udp_All_Nets	drop	1
179.43.144.33	Switzerland	147.237.77.179	e.mazi.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.224		147.237.8.14	e.orchot.idf.il	Block_Udp_All_Nets	drop	1
182.140.167.188	China	147.237.8.27	e.madim.atal.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.72.14	dover.idf.il(old)	Block_Udp_All_Nets	drop	1
184.105.139.85	United States	147.237.8.24	e.lifestyle.idf.il	Block_Udp_All_Nets	drop	1
179.43.144.33	Switzerland	147.237.0.19	madim.atal.idf.il	Block_Ntp_All_Net	drop	1

02-28-2016-12:04:00 to 02-28-2016-13:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.65.93.236	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	22
85.130.131.61	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
51.254.129.87	United Kingdom	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Block	2
51.254.129.87	United Kingdom	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
176.13.11.220	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
2.54.52.121	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
84.94.41.65	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
51.254.129.87	United Kingdom	147.237.76.31	nakchal.idf.il	C1000074: HTTP: majestic bot	Block	2
51.255.65.78	United Kingdom	147.237.77.170	maarachot.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.88	United Kingdom	147.237.77.170	maarachot.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
66.249.64.185	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
51.255.65.30	United Kingdom	147.237.77.170	maarachot.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.38	United Kingdom	147.237.77.170	maarachot.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

02-28-2016-12:04:00 to 02-28-2016-13:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.i	Tehila - Perl LWP with fake user agent	2
176.13.10.243	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
164.39.11.198	147.237.0.33	United Kingdom	idf.il	ET SCAN NMAP -sS window 1024	1
109.67.26.231	147.237.77.216	Israel	dover.idf.i	portscan: TCP Distributed Portscan	1
91.197.61.250	147.237.77.216	Israel	dover.idf.i	portscan: TCP Distributed Portscan	1
212.117.143.194	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.108.145.172	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
199.203.111.231	147.237.77.216	Israel	dover.idf.i	portscan: TCP Distributed Portscan	1
82.80.58.58	147.237.77.216	Israel	dover.idf.i	portscan: TCP Distributed Portscan	1
192.116.91.200	147.237.77.216	Israel	dover.idf.i	portscan: TCP Distributed Portscan	1
80.246.140.97	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.12.24.237	147.237.77.216	Iraq	dover.idf.i	OS-WINDOWS Microsoft Forefront UAG javascript handler in URI XSS attempt	1
79.177.57.156	147.237.77.216	Israel	dover.idf.i	portscan: TCP Distributed Portscan	1
176.13.13.222	147.237.77.216	Israel	dover.idf.i	portscan: TCP Distributed Portscan	1
31.210.188.64	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.6.201	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.160.178.129	147.237.77.216	Israel	dover.idf.i	portscan: TCP Distributed Portscan	1
95.86.102.53	147.237.77.216	Israel	dover.idf.i	portscan: TCP Distributed Portscan	1
213.57.152.246	147.237.77.216	Israel	dover.idf.i	portscan: TCP Distributed Portscan	1
87.69.104.67	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.25.82.123	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.80.126.182	147.237.77.216	Israel	dover.idf.i	portscan: TCP Distributed Portscan	1
82.76.46.25	147.237.77.216	Romania	dover.idf.i	portscan: TCP Distributed Portscan	1
185.32.179.13	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.182.37.95	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.21.74	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
62.90.131.46	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

02-28-2016-12:04:00 to 02-28-2016-13:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.210.151.185	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	132
46.19.85.145	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
212.179.21.194	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	28
212.179.21.194	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	28
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	25
109.67.49.215	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
185.32.179.170	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
2.54.3.21	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
81.218.241.26	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	16
37.26.149.191	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
2.54.139.59	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
81.218.178.243	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	12
185.32.179.110	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
80.246.137.26	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.149.191	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	10
81.218.178.243	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid sequence number	monitor	10
80.246.137.66	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
195.60.232.57	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
2.54.143.178	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.203	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
164.138.124.7	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.250	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.73	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
91.240.235.225	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.6.132	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.161	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.136.132	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.145.59	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.13.85	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.139.110	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.232	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.219.47.150	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
81.218.195.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.138.153	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
176.13.19.73	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.147.133	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	5
31.210.188.64	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.150.245.250	Israel	147.237.76.31	nakchal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
84.108.6.189	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
132.74.215.241	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
81.218.251.252	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
176.13.4.218	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
2.54.163.115	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
176.13.2.199	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
194.114.146.227	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.176	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4

02-28-2016-12:04:00 to 02-28-2016-13:04:00

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
79.177.190.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.22.34	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-28-2016-12:04:00 to 02-28-2016-13:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.137.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
80.246.136.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	75
2.54.129.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	70
109.253.210.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	61
80.246.136.22	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	47
37.26.149.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	38
46.19.86.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
109.67.14.59	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 109.67.14.59	Block	12
46.19.85.145	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	12
5.29.43.253	Israel	147.237.0.34	tikshuv.idf.il	Automated Vulnerability Scanning V1	Block	8
212.150.245.250	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 212.150.245.250	Block	6
212.150.245.250	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	5
66.249.79.75	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.75	Block	4
185.32.179.110	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
2.54.3.21	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
185.32.179.170	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
2.54.45.46	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.18.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.12.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.183.129	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
79.183.16.12	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
176.13.8.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.0.37	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
134.191.232.69	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.54.139.59	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
176.13.10.72	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
134.191.232.70	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.54.143.178	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
109.253.145.59	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
176.13.19.73	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
176.13.12.218	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
95.153.129.233	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	2
80.246.136.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.13.85	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
109.67.14.59	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/trigger.png"	Block	1
40.77.167.3	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
31.168.17.15	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	1
176.13.15.78	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
79.176.120.170	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.64.170	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
37.26.148.233	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
192.117.101.169	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/atuda	Block	1
85.65.125.129	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/716	Block	1
79.183.169.121	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl83 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
157.55.39.39	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
37.26.146.138	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
2.54.51.255	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
176.13.2.199	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1

02-28-2016-12:04:00 to 02-28-2016-13:04:00