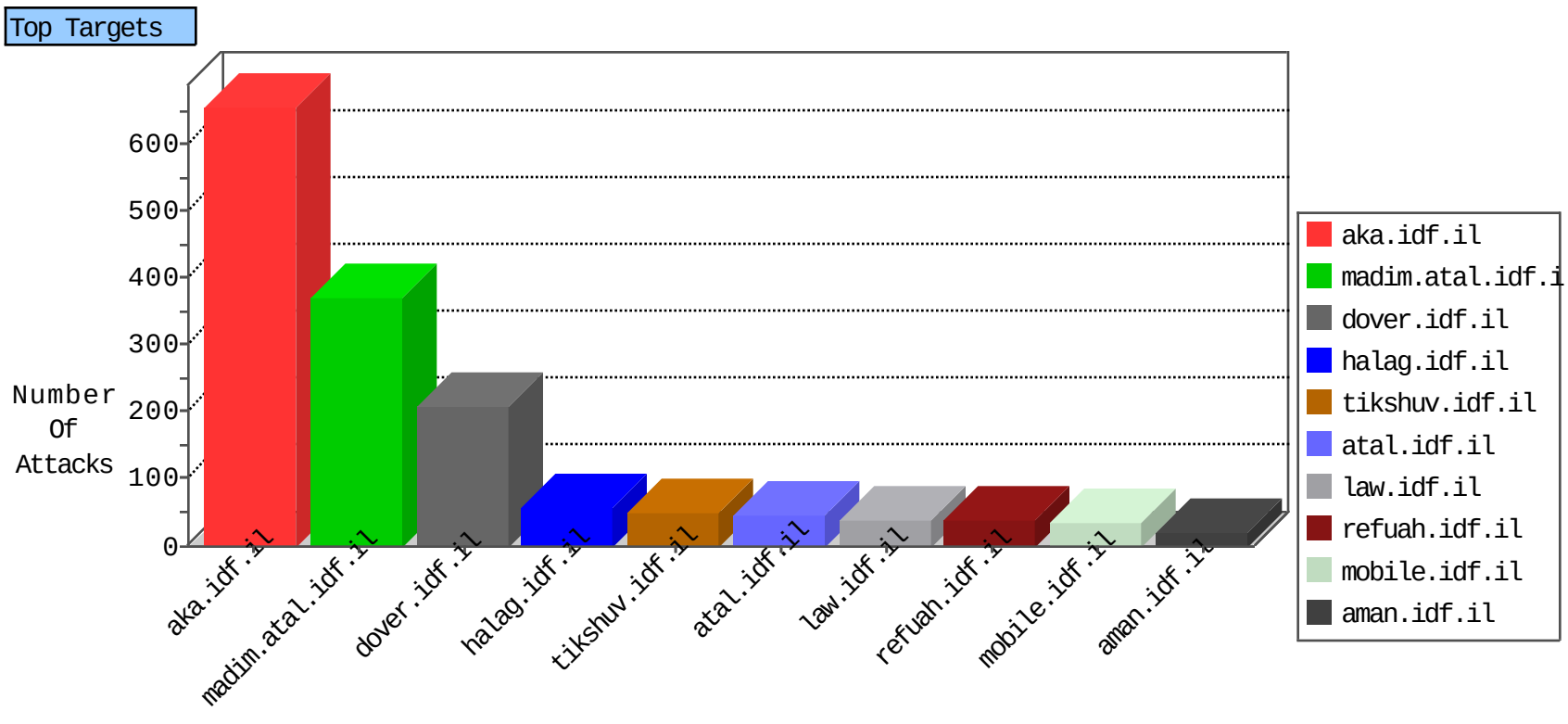
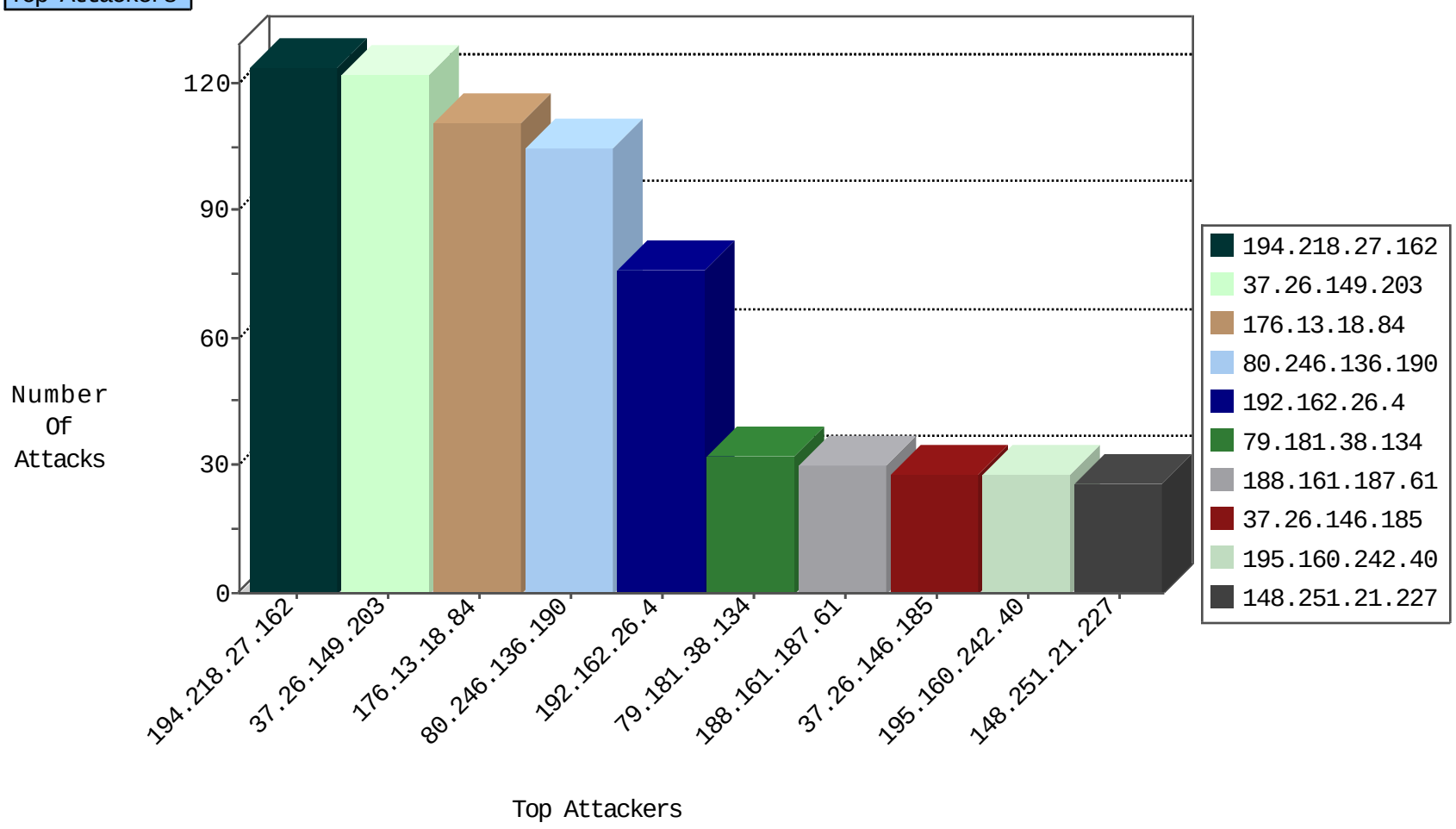
02-29-2016-15:04:06 to 02-29-2016-16:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-29-2016-15:04:06 to 02-29-2016-16:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.145.220.26	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	9
217.26.171.188	Moldova, Republic of	147.237.76.176	test.ncore.idf.il	L4 Source or Dest Port Zero	drop	4
82.145.219.82	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4
197.165.136.193	Egypt	147.237.77.216	dover.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	2
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
74.82.47.29	United States	147.237.77.170	maarachot.idf.il	Block_Udp_All_Nets	drop	1

02-29-2016-15:04:06 to 02-29-2016-16:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
31.154.41.13	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	20
37.142.68.31	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
173.234.153.122	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	6
79.179.11.211	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
85.65.167.150	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
212.235.64.137	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
79.178.181.61	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
69.30.213.18	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	2
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
92.169.26.13	France	147.237.77.216	dover.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1
77.248.12.153	Netherlands	147.237.77.170	maarachot.idf.il	14331: HTTP: Suspicious User-Agent (My Session)	Block	1

02-29-2016-15:04:06 to 02-29-2016-16:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
84.109.12.29	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
37.142.241.89	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.172.235.215	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
14.187.188.202	147.237.0.35	Vietnam	akaws.idf.il	ET SCAN NMAP -sS window 2048	1
87.68.71.18	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.28.171.5	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.76.196	China	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
84.109.12.29	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.182.105	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.106.50	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.182.107.134	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.150.189.2	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.121.77.59	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
46.117.34.25	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.183	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
40.113.118.99	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 2048	1
178.255.215.87	147.237.72.166	France	aka.idf.il	portscan: TCP Distributed Portscan	1
40.76.204.123	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
95.9.82.247	147.237.8.28	Turkey	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
37.26.146.221	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.71.29.4	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
14.187.188.202	147.237.0.35	Vietnam	akaws.idf.il	ET SCAN NMAP -f -sS	1
85.250.71.12	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.22.131.10	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.163.241	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.8.204.38	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.126.215.151	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.143.71.203	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.121.61.153	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.115.177.203	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.103	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.3.147.227	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
40.113.118.99	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -f -sS	1
121.141.225.10	147.237.72.166	Korea, Republic of	aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

02-29-2016-15:04:06 to 02-29-2016-16:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	83
192.162.26.4	Spain	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	51
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	41
37.26.146.185	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
79.181.38.134	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	26
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	23
84.111.66.15	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
148.251.21.227	Germany	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	19
195.160.242.40	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
109.66.157.22	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
188.161.187.61	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
188.161.187.61	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
212.143.71.203	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
195.160.242.40	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
82.114.168.158	Yemen	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
212.29.202.226	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
105.106.143.247	Algeria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	8
212.29.202.226	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	8
46.19.85.9	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
212.29.202.226	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	7
64.237.232.209	Puerto Rico	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
79.176.185.186	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.166.93.85	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.179.21.194	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.177	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.215.42	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.66.13	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.0.119	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.38.134	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.19.86.252	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.236.120	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.178.123.227	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
2.52.0.228	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
84.110.37.105	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.167	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.168.112	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
104.232.181.118		147.237.77.74	law.idf.il	Header Rejection	header rejection pattern found in request	monitor	5
104.232.181.118		147.237.77.176	matpash.idf.il	Header Rejection	header rejection pattern found in request	monitor	5
213.244.119.251	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.198	Israel	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
148.251.21.227	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
64.237.232.209	Puerto Rico	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.86.198	Israel	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
37.46.39.125	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
188.161.187.61	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.52.173.56	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.3	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.86.198	Israel	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4

02-29-2016-15:04:06 to 02-29-2016-16:04:06

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
80.246.139.173	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
138.134.192.10	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4

02-29-2016-15:04:06 to 02-29-2016-16:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.149.203	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	122
176.13.18.84	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	111
80.246.136.190	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	105
79.178.209.43	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.178.209.43	Block	15
79.176.133.18	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.176.133.18	Block	13
80.246.136.151	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 80.246.136.151	Block	13
80.246.136.218	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
79.178.209.43	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	8
79.176.133.18	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	7
46.39.36.65	Russian Federation	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	5
37.46.35.163	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 37.46.35.163	Block	5
217.132.47.149	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 217.132.47.149	Block	5
37.46.35.163	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	3
80.246.137.72	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
217.132.47.149	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	3
2.54.38.159	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.178.52.79	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.178	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
192.162.26.4	Spain	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
85.65.127.79	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 85.65.127.79	Block	2
176.13.3.50	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
82.166.93.85	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/	Block	2
85.65.127.79	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/default.aspx	Block	2
192.162.26.4	Spain	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Method	Block	2
176.13.13.9	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
84.94.84.124	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/console/core/doc_mgr/undefined	Block	2
46.39.36.65	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/faq.aspx	Block	2
209.88.157.203	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/scripts/css3pie.htc	Block	2
192.162.26.4	Spain	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
46.19.85.21	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.85.186	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	2
2.54.147.223	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
213.244.119.251	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
212.117.136.7	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
80.246.136.151	Israel	147.237.72.166	aka.idf.il	Unknown Parameter c in www.aka.idf.il/main/giyus/general.aspx	None	1
213.57.175.209	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
192.115.248.2	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl73 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
114.112.90.54	China	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
79.178.39.60	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.178.39.60	Block	1
2.54.184.111	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.69.32	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
192.162.26.4	Spain	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 192.162.26.4	Block	1
66.249.64.119	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
192.162.26.4	Spain	147.237.72.166	aka.idf.il	Abnormally Long Request method	Block	1
216.218.206.68	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
212.117.136.7	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;t in www.aka.idf.il/main/kapatz/scriptresource.axd	None	1
37.142.64.88	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	1
192.162.26.4	Spain	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 192.162.26.4	Block	1
37.19.119.62	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar	Block	1
89.107.186.233	Germany	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1

02-29-2016-15:04:06 to 02-29-2016-16:04:06