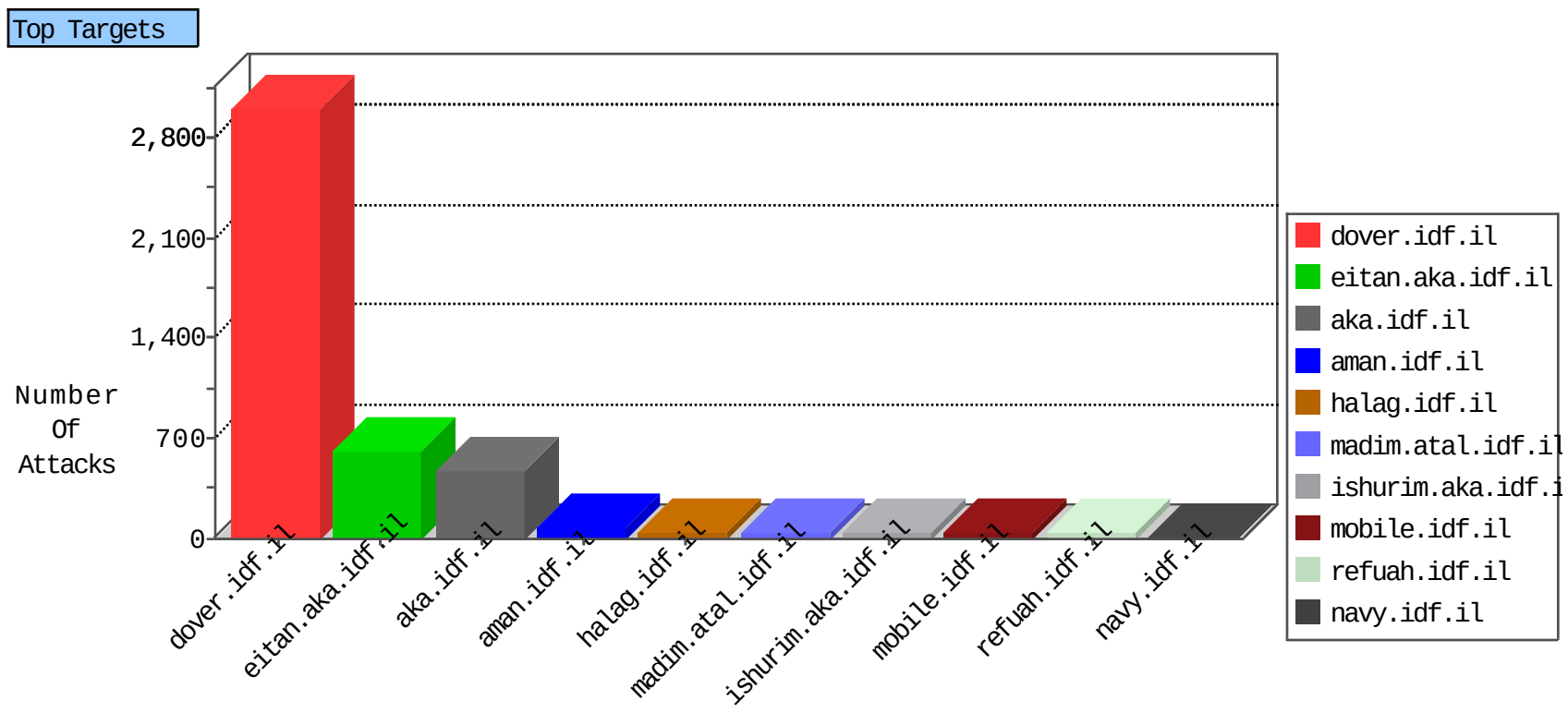
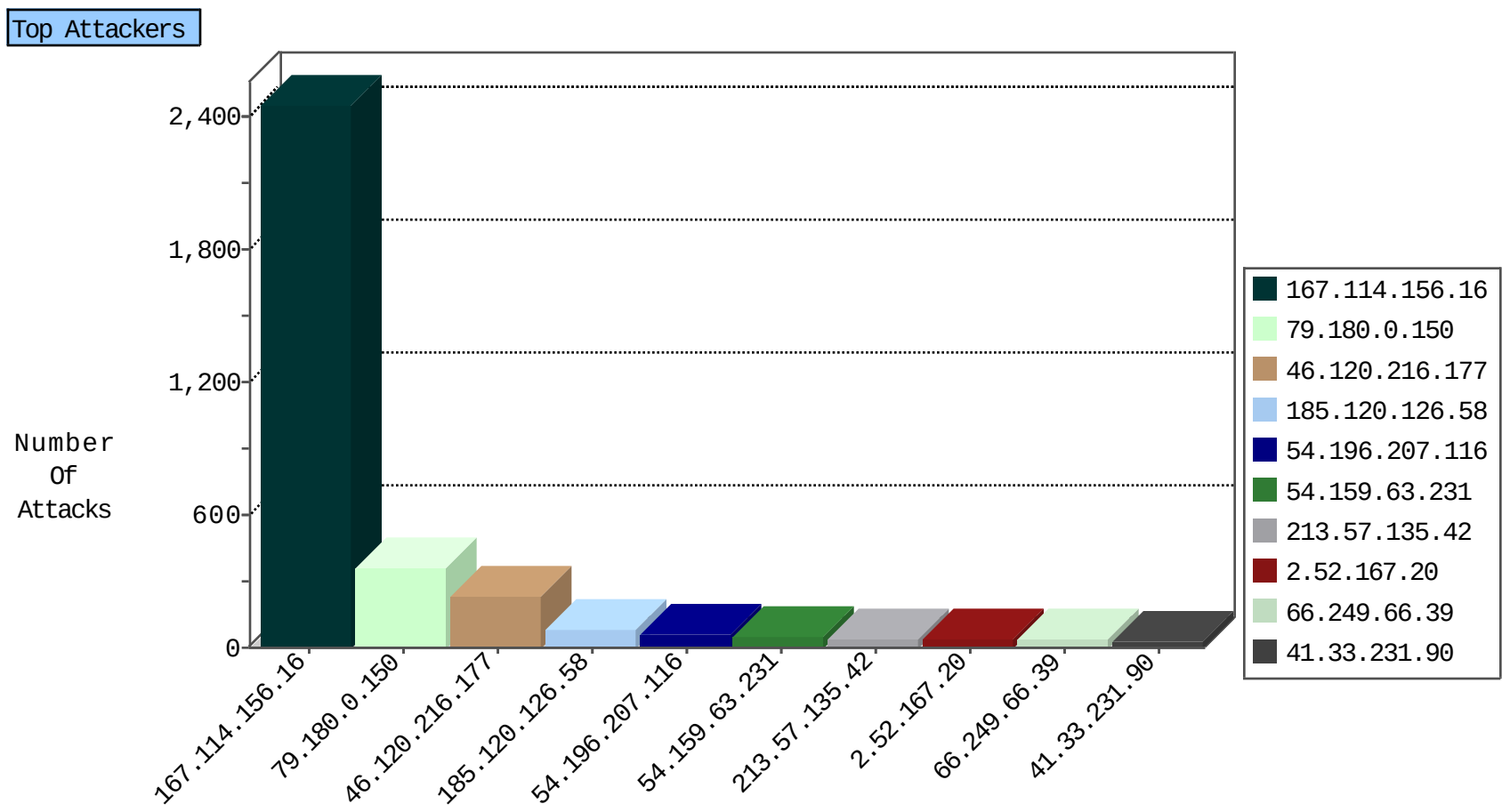
12-16-2015-18:04:08 to 12-16-2015-19:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



12-16-2015-18:04:08 to 12-16-2015-19:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3590
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	572
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	486
54.196.207.116	United States	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	29
54.196.207.116	United States	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	28
54.159.63.231	United States	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	23
54.159.63.231	United States	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	22
54.83.98.217	United States	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	7
54.197.86.71	United States	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	6
107.22.127.154	United States	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	5
107.20.119.96	United States	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	3
54.83.98.217	United States	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	3
54.145.63.46	United States	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
54.234.76.114	United States	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2

12-16-2015-18:04:08 to 12-16-2015-19:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.181.26.181	Israel	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
109.64.33.218	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
123.126.113.154	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

12-16-2015-18:04:08 to 12-16-2015-19:04:08

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	4
109.64.136.94	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.152.190.84	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
84.94.170.23	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
73.17.14.46	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sS window 1024	1
73.17.14.46	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.225	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
141.105.160.161	147.237.72.166	Satellite Provider	aka.idf.il	portscan: TCP Distributed Portscan	1
123.196.116.11	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
123.196.116.11	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
104.152.190.84	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.172.140.240	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.102.253.52	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.90.106	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
73.17.14.46	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
192.162.100.148	147.237.0.34	Russian Federation	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
60.177.195.87	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
149.78.154.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
27.8.249.165	147.237.76.44	China	e.refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
123.196.116.11	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
123.196.116.11	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1

12-16-2015-18:04:08 to 12-16-2015-19:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.180.0.150	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	351
185.120.126.58		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	54
213.57.135.42	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	40
66.249.66.39	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
46.19.85.9	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	26
185.120.126.58		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	26
192.114.105.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
84.94.38.200	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
107.167.108.129	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
207.241.226.40	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	17
172.56.15.246	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	17
185.27.105.185	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
213.57.140.129	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	15
66.249.66.45	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.146.252	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	12
79.183.202.108	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
94.230.86.147	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.120.216.177	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
84.94.38.200	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
91.201.242.130	Ukraine	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
2.52.167.20	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
91.201.242.130	Ukraine	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
2.52.167.20	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
2.52.167.20	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
84.228.87.186	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
54.145.63.46	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.52.167.20	Israel	147.237.72.156	aman.idf.il	SYN Attack		reject	7
46.116.160.8	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.149.134	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.137.150	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
93.172.140.240	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.102.254.103	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.161	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.160.242	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.120.44.219	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
149.78.96.53	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
37.26.146.201	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.116.160.8	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.26.147.226	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
130.207.203.56	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	6
176.13.1.230	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.167.20	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.245	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
54.234.76.114	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
84.228.26.102	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
213.8.204.60	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
172.56.15.246	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.245	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5

12-16-2015-18:04:08 to 12-16-2015-19:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.120.216.177	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	222
46.19.85.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	27
79.180.0.150	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	13
59.40.119.109	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 59.40.119.109	Block	4
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
176.13.20.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
46.19.86.207	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
2.52.16.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.54.151	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.120.92.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.4.145	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 176.13.4.145	Block	3
94.230.86.147	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
59.40.119.109	China	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
149.78.171.86	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.66.16	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
37.26.146.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.4.145	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1432	Block	2
79.182.70.126	Israel	147.237.72.166	aka.idf.il	NULL Character in Header Name at Â¨Ã¦Â‹Ã‹EÂ´VÃ¢Â”Ã± SÃžC!lÂ?ÃŠhÂ‘Â®Â®Â‡Ã¬Â°<ÃšÂ²Â?g"Ã?Ã“Â¡ZÂ´(IÂ•Ã¡Ã^ ;[[#28]]Ã¥Â-Ã'[[#19]]-gÃ'rfÃž\Ã?mÂœÂµÂ“eX,Â?)Ã– [[#21]]Ã?Ã¹,[[#5]]BÂ›xÃ«Ã¾Ã£	Block	1
109.160.243.152	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.44	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/tfasim.aspx.	Block	1
79.181.128.195	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
77.126.40.222	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.25	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
87.68.82.245	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
176.12.138.251	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	1
5.29.66.60	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
79.183.147.149	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
79.182.70.126	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Value	Block	1
46.116.160.8	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.178.187.10	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
212.150.245.250	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/8/109978.pdf	Block	1
46.19.85.105	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method 1f05rb in URL	Block	1
89.139.182.189	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
37.26.148.239	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.109.18.75	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.64.200	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/asp/giyus.asp	Block	1
176.13.5.193	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
149.78.110.220	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
2.54.19.121	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
79.182.70.126	Israel	147.237.72.166	aka.idf.il	NULL Character in Method Ã¸[[#30]]Â»[[#3]][[#1]]	Block	1
46.121.211.67	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.114	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
95.12.112.96	Turkey	147.237.72.166	aka.idf.il	Unknown Parameter docid in www.aka.idf.il/iturim/asp/diploma.asp	None	1
79.181.149.146	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.113.56.149	Romania	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
46.19.85.54	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
88.80.197.74	Germany	147.237.77.216	dover.idf.il	Admin Blocking	Block	1

12-16-2015-18:04:08 to 12-16-2015-19:04:08