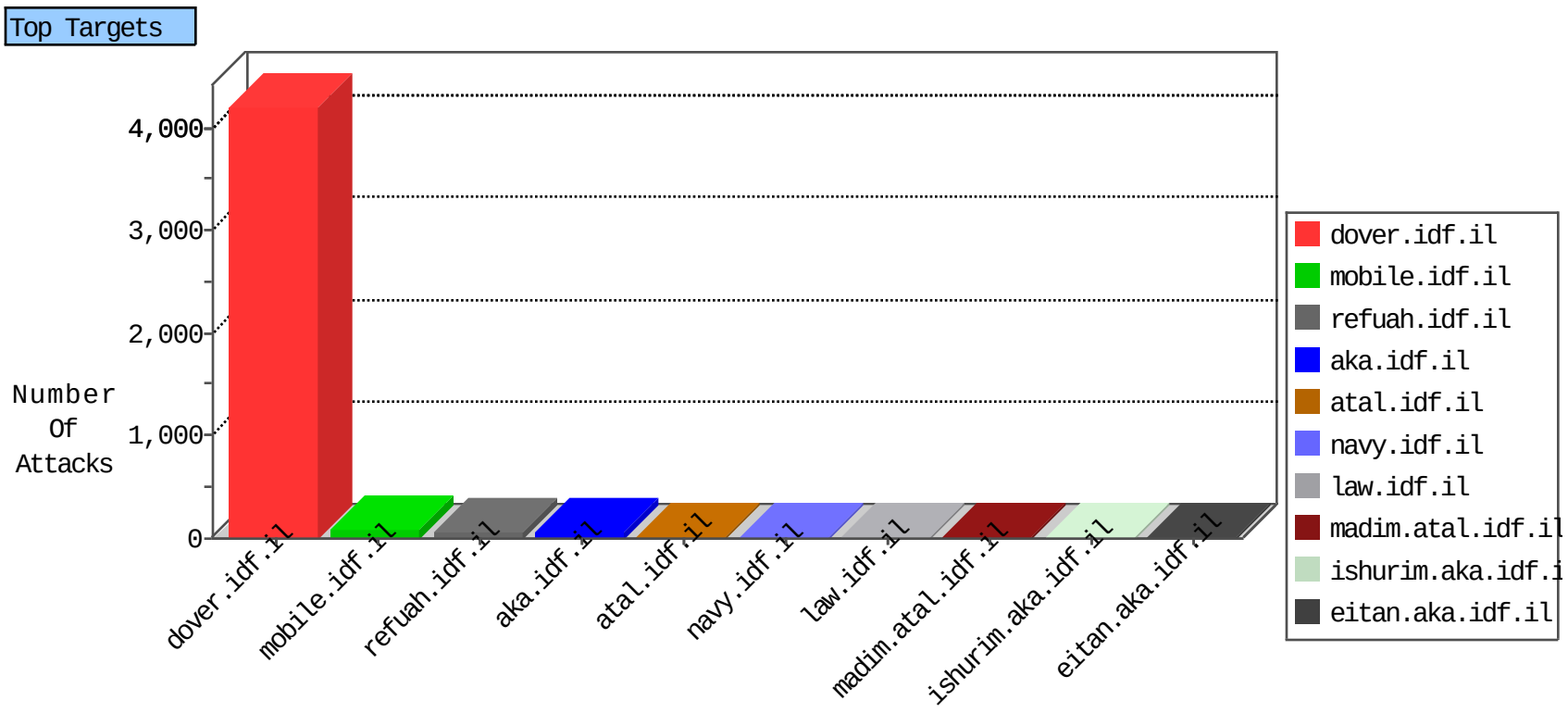
04-18-2016-06:04:03 to 04-18-2016-07:04:03

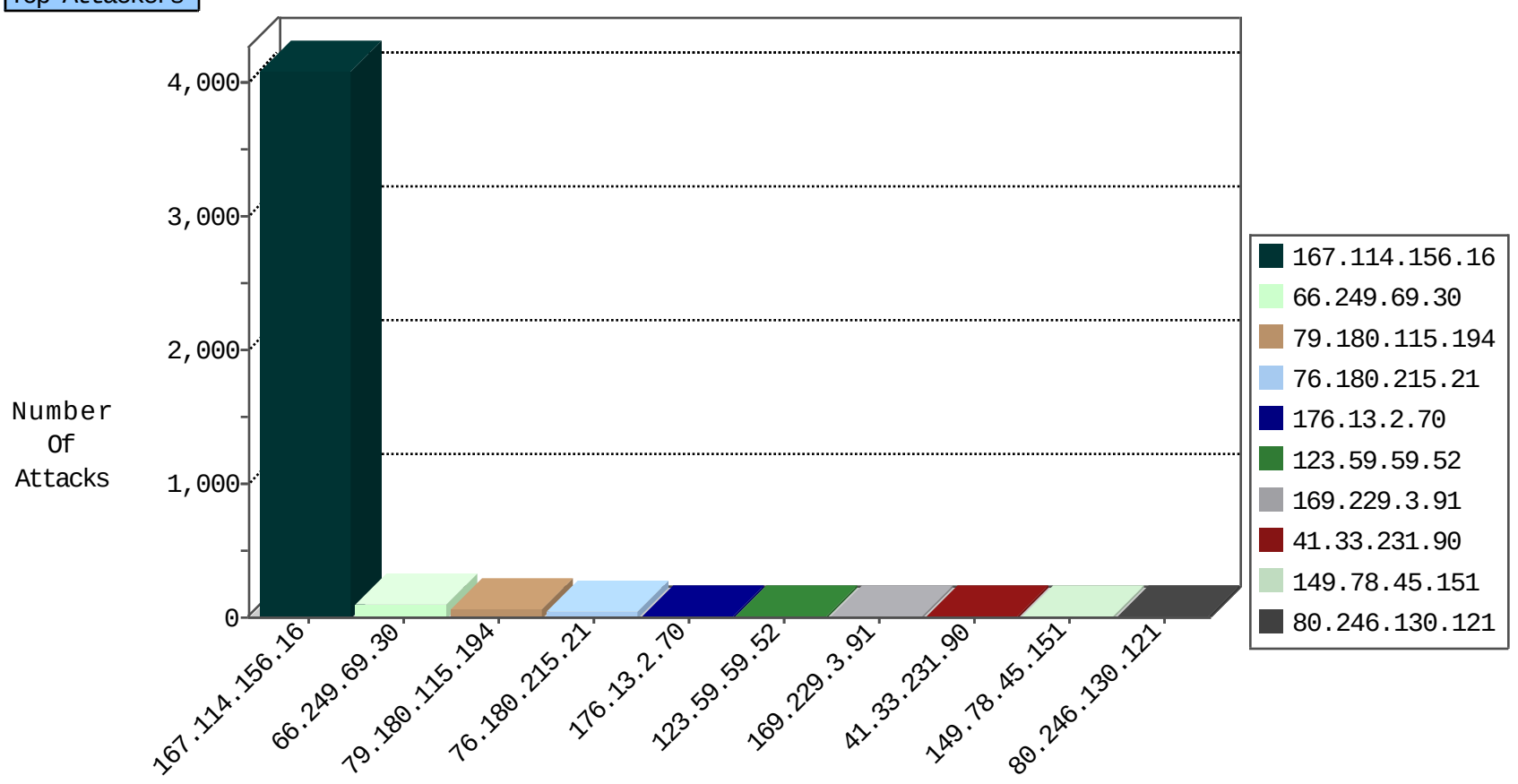
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

04-18-2016-06:04:03 to 04-18-2016-07:04:03

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	Block_Ip_Web_In	drop	4074
79.180.115.194	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	48
79.180.115.194	Israel	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	15
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
123.59.59.52	China	147.237.72.166	aka.idf.il	block-sp-traf1	forward	4
123.59.59.52	China	147.237.77.74	law.idf.il	block-sp-traf1	forward	4
120.132.50.135	China	147.237.77.205	prisha.idf.il	block-sp-traf1	forward	2
184.105.139.92	United States	147.237.77.234	halag.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.124	United States	147.237.0.19	madim.atal.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.76	United States	147.237.8.28	e.mobile-ks.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.104	United States	147.237.8.50	e.tikshuv.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.68	United States	147.237.77.178	e.matpash.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.124	United States	147.237.0.33	idf.il	Block_Ntp_All_Net	drop	1
184.105.139.84	United States	147.237.8.14	e.orchot.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.112	United States	147.237.72.167	ishurim.aka.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.68	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.84	United States	147.237.77.205	prisha.idf.il	Block_Ntp_All_Net	drop	1
159.122.220.135	United States	147.237.77.179	e.mazi.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.112	United States	147.237.72.217	e.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.72	United States	147.237.0.200	m4u.idf.il	Block_Ntp_All_Net	drop	1

04-18-2016-06:04:03 to 04-18-2016-07:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
69.197.177.50	United States	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	2
69.197.177.50	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-18-2016-06:04:03 to 04-18-2016-07:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	10
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
66.249.93.109	147.237.76.86	Europe	navy.idf.il	ET SCAN NMAP -sA (2)	2
80.246.130.121	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
212.129.15.245	147.237.76.34	France	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
186.49.175.148	147.237.0.33	Uruguay	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
124.83.57.31	147.237.0.33	Philippines	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.219.238.10	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
173.65.154.27	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
104.238.82.190	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
46.151.52.139	147.237.77.226	Ukraine	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
40.114.42.13	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1

04-18-2016-06:04:03 to 04-18-2016-07:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.69.30	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
76.180.215.21	United States	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	40
176.13.2.70	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
80.179.78.185	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.17.133	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.97.153	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	5
82.80.168.133	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
84.108.57.88	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
173.60.226.137	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
207.46.13.103	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.53.25.76	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.130.121	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.86.214	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.71.197.9	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.130.121	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
62.90.180.145	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.55.155.44	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.22.115	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.69.46	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
38.81.65.42	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
38.111.147.86	United States	147.237.77.216	dover.idf.il	drop		drop	2
118.173.142.96	Thailand	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
157.55.2.151	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
2.53.55.197	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
109.67.194.8	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP anomaly detected	Non-compliant TCP packets coming from multiple external sources were detected. This may result from potential network configuration problem.	drop	1
216.218.206.103	United States	147.237.8.46	e.chinuch.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.228	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.85.194	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
169.229.3.91	United States	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
136.243.11.18	Germany	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
72.173.225.170	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.103	United States	147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.230	United States	147.237.76.148	gqcenter.aka.idf.i	drop		drop	1
2.53.55.197	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
216.218.206.74	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.79	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
169.229.3.91	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.90	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
120.132.67.62	China	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
218.22.211.69	China	147.237.0.35	akaws.idf.il	drop		drop	1
184.105.247.240	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
176.13.2.70	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
162.144.41.122	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
106.186.113.132	Japan	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

04-18-2016-06:04:03 to 04-18-2016-07:04:03

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
216.218.206.75	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
79.180.115.194	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.139.83	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.78.45.151	United States	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	9
50.59.104.18	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 50.59.104.18	Block	4
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/site/unselecatble.aspx	Block	2
17.142.156.109	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	2
2.53.25.76	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/1231-he/miluim.aspx	Block	1
131.253.25.206	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
76.180.215.21	United States	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in URL t…₪´¿„ˆnz3„g:ע6°,ÿסצ„¸oך=]]62#[[€¡e¨™•f¦ט<„[[61#]]מ¶[[52#]]lÊ[[#17]]¸€ü]]#25[[¶מ]]#16[[„<ט	Block	1
50.240.82.133	United States	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
169.229.3.91	United States	147.237.77.243	mobile.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
109.127.65.242	Iraq	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	1
76.180.215.21	United States	147.237.76.42	refuah.idf.il	Abnormally Long Request method	Block	1
76.180.215.21	United States	147.237.76.42	refuah.idf.il	Malformed URL t…₪´¿„ˆnz3„g:ע6°,ÿסצ„¸oך=]]62#[[€¡e¨™•f¦ט<„[[61#]]מ¶[[#25]]lÊ[[#17]]¸€ü	Block	1
65.55.210.90	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
176.13.2.70	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
109.253.197.212	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/general/mobile	Block	1
76.180.215.21	United States	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in Method ¬[[#0]][[#0]][[#0]]B¦#012•ÝÀbXdïMRìþn•Í¬£[[#27]]•{tÇ^Ý[[#5]]§*óõ¦p±\ï Àœ"ó[[#14]]¸¿-[[#22]]'ôI¹@Rƒ‹ñÄbEÖ…¸Õ	Block	1
38.81.65.42	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
157.55.39.1	United States	147.237.77.216	dover.idf.il	Abnormally Long Request URL	Block	1
76.180.215.21	United States	147.237.76.42	refuah.idf.il	NULL Character in Method ¬[[#0]][[#0]][[#0]]B¦#012•ÝÀbXdïMRìþn•Í¬£[[#27]]•{tÇ^Ý[[#5]]§*óõ¦p±\ï Àœ"ó[[#14]]¸¿-[[#22]]'ôI¹@Rƒ‹ñÄbEÖ…¸Õ	Block	1
66.249.79.169	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	1
199.47.81.13	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1503-	Block	1
123.59.59.52	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.ctrip.com/main/home/default.aspx	Block	1
76.180.215.21	United States	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in Parameter Name ₪[[†'#18[[]]#15ˆ„¿´₪….t ni]] nz3„g:ע6°,ÿסצ„¸oך=]]62#[[€¡e¨™•f¦ט<„[[61#]]מ¶[[52#]]lÊ[[#17]]¸€ü	Block	1
157.55.39.1	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
76.180.215.21	United States	147.237.76.42	refuah.idf.il	Unauthorized Method POST for 147.237.76.42/	Block	1
66.249.79.183	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 208.115.113.82	Block	1
123.59.59.52	China	147.237.77.74	law.idf.il	Unauthorized URL Access to www.ctrip.com/14-he/patzar.aspx	Block	1
76.180.215.21	United States	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in Query String ₪[[†'#18[[]]#15„3znˆ„¿´₪….t no]] g:ע6°,ÿסצ„¸oך=]]62#[[€¡e¨™•f¦ט<„[[61#]]מ¶[[52#]]lÊ[[#17]]¸€ü	Block	1
50.59.104.18	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/mobile	Block	1
169.229.3.91	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
76.180.215.21	United States	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method ¬[[#0]][[#0]][[#0]]B¦#012•ÝÀbXdïMRìþn•Í¬£[[#27]]•{tÇ^Ý[[#5]]§*óõ¦p±\ï Àœ"ó[[#14]]¸¿-[[#22]]'ôI¹@Rƒ‹ñÄbEÖ…¸Õ	Block	1
68.180.229.89	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/chamatz/home/d...sp	Block	1

04-18-2016-06:04:03 to 04-18-2016-07:04:03