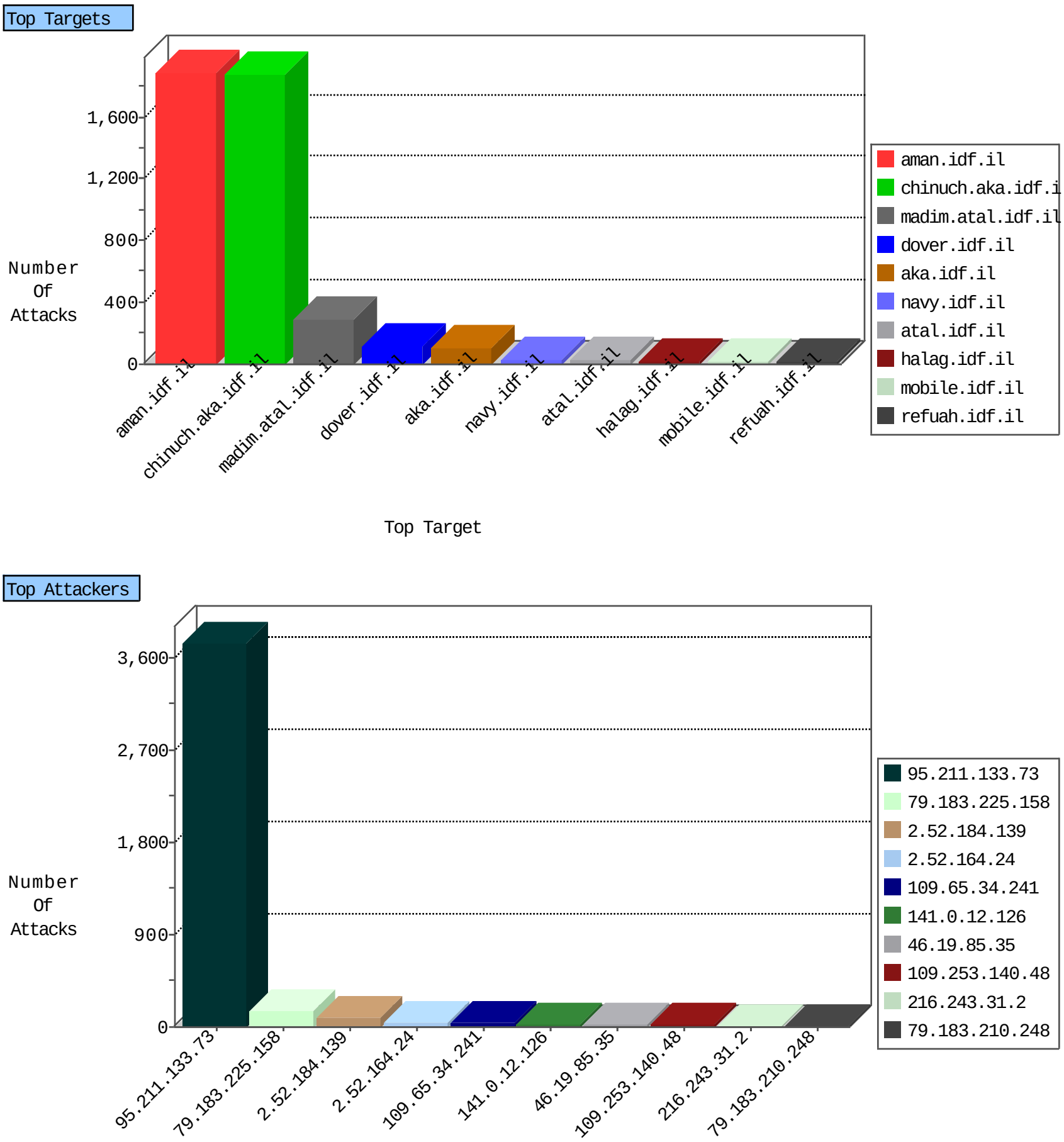
03-05-2016-16:04:01 to 03-05-2016-17:04:01

IDF Under Attack Daily Report



03-05-2016-16:04:01 to 03-05-2016-17:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
52.31.84.220	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
178.32.137.188	Italy	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
52.31.84.220	United States	147.237.0.34	tikshuv.idf.il	Block_Ntp_All_Net	drop	1
178.32.137.188	Italy	147.237.77.179	e.mazi.idf.il	Block_Ntp_All_Net	drop	1

03-05-2016-16:04:01 to 03-05-2016-17:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.136.246	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
5.29.107.7	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
46.116.208.172	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-05-2016-16:04:01 to 03-05-2016-17:04:01

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
199.101.186.245	147.237.0.33	United States	idf.il	ET SCAN NMAP -f -sS	1
159.122.220.108	147.237.72.166	Netherlands	aka.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.193	147.237.72.166	Netherlands	aka.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.76.201	China	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
91.236.74.6	147.237.8.45	Poland	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
213.136.91.26	147.237.77.234	Germany	halag.idf.il	ET SCAN Potential SSH Scan	1
82.166.184.187	147.237.76.198	Israel	e.yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
213.136.91.26	147.237.77.179	Germany	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
82.166.184.187	147.237.76.198	Israel	e.yohalan.idf.il	ET SCAN NMAP -f -sS	1
213.136.91.26	147.237.8.50	Germany	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
209.126.116.147	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -sS window 1024	1
199.101.186.245	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 1024	1
113.176.83.10	147.237.0.19	Vietnam	madim.atal.idf.il	WEB-CGI redirect access	1
94.102.48.193	147.237.72.166	Netherlands	aka.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.76.198	China	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
82.200.142.180	147.237.76.198	Kazakstan	e.yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
213.136.91.26	147.237.77.227	Germany	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
82.166.184.187	147.237.76.198	Israel	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
213.136.91.26	147.237.76.31	Germany	nakchal.idf.il	ET SCAN Potential SSH Scan	1
213.136.91.26	147.237.8.14	Germany	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
199.101.186.245	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 2048	1

03-05-2016-16:04:01 to 03-05-2016-17:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
95.211.133.73	Netherlands	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1291
95.211.133.73	Netherlands	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	931
95.211.133.73	Netherlands	147.237.76.147	chinuch.aka.idf.il	SYN Attack		reject	919
95.211.133.73	Netherlands	147.237.72.156	aman.idf.il	SYN Attack		reject	567
141.0.12.126	Norway	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
109.253.140.48	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
46.117.175.126	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
79.183.210.248	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
109.65.34.241	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
213.8.204.31	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
109.64.123.38	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
85.250.20.4	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
176.13.21.148	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
95.211.133.73	Netherlands	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.230	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.70.41.120	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.2.22	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.35	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.52.164.24	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.35	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.35	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
95.211.133.73	Netherlands	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
91.200.12.106	Ukraine	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	4
91.200.12.106	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
46.19.86.111	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.35	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
79.180.139.116	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.210.63	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
5.28.159.138	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
95.211.133.73	Netherlands	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
77.125.161.178	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.125.26		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.147.226	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.153.124	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.9.242	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
80.178.168.22	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.176.178.208	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
54.147.176.220	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.85.151	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
109.66.23.127	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
95.211.133.73	Netherlands	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
193.33.148.6	Denmark	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
46.19.86.35	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
84.108.86.101	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
79.182.208.36	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
5.102.195.94	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
176.13.9.242	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
46.19.86.35	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
109.66.17.167	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2

03-05-2016-16:04:01 to 03-05-2016-17:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.183.225.158	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	152
2.52.184.139	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	91
2.52.164.24	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	38
157.55.2.139	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
213.8.204.64	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
168.63.137.102	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
199.30.25.106	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
37.142.64.94	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
46.19.86.132	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
109.65.34.241	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 109.65.34.241	Block	2
109.65.34.241	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 109.65.34.241	Block	2
37.59.29.19	France	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/general.aspx	Block	2
109.65.34.241	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 109.65.34.241	Block	2
109.65.34.241	Israel	147.237.72.166	aka.idf.il	Multiple Malformed HTTP Header Line from 109.65.34.241	Block	2
109.65.34.241	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 109.65.34.241	Block	2
109.65.34.241	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 109.65.34.241	Block	2
66.249.64.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.65.34.241	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 109.65.34.241	Block	2
109.253.130.119	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
109.65.34.241	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 109.65.34.241	Block	2
109.65.34.241	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 109.65.34.241	Block	2
109.65.34.241	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name Õ³¤E[çW?Äªyë-*„;[[#22]]ý[[#20]]‰ÆDt¡¤šw[[#23]]Cá¬Þ(+=³Í•Eàºr^/ëƒ¯ÿpw 1àÊPÓº„^F¿vo}[[#24]]KL•«[[#30]]zíQ&‡ý®¼Ï^[[#18]]X»ò”ñ	Block	1
185.89.217.231		147.237.77.74	law.idf.il	URL is Above Root Directory www.law.idf.il/../images/1.he/navigation/navigation_arrow.gif	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1380-he/dover.aspx	Block	1
65.55.210.250	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
37.26.146.173	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
109.65.34.241	Israel	147.237.72.166	aka.idf.il	Malformed URL	Block	1
173.20.245.205	United States	147.237.76.86	navy.idf.il	NULL Character in Method ,[[#0]][[#0]][[#0]]@¥X”ÛÏ`[[#30]]6Kßbo§‰[[#27]]án›ê9¼Ê–GÐ•ÄÉáÛ§•Ÿœ ÿ<3Í™º¹4NfÂÜ*ÜòJ![[#26]]×-@Œ¥Í¸ÌÆÜGú=U	Block	1
109.64.123.38	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
66.249.64.233	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
109.65.34.241	Israel	147.237.72.166	aka.idf.il	Too Many Headers per Request - 31 Headers	Block	1
46.120.68.255	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	1
109.65.34.241	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Value	Block	1
188.247.73.231	Jordan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1361-13185-ar	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9628-he/refuah.aspx	Block	1
109.65.34.241	Israel	147.237.72.166	aka.idf.il	NULL Character in Header Name at Õ³¤E[çW?Äªyë-*„;[[#22]]ý[[#20]]‰ÆDt¡¤šw[[#23]]Cá¬Þ(+=³Í•Eàºr^/ëƒ¯ÿpw 1àÊPÓº„^F¿vo}[[#24]]KL•«[[#30]]zíQ&‡ý®¼Ï^[[#18]]X»ò”ñ	Block	1
66.249.64.37	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list7.htm	Block	1
219.94.129.86	Japan	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/blog/wp-admin/	Block	1
109.65.34.241	Israel	147.237.72.166	aka.idf.il	Abnormally Long Header Line request header name	Block	1
173.20.245.205	United States	147.237.76.86	navy.idf.il	Unknown HTTP Request Method ,[[#0]][[#0]][[#0]]@¥X”ÛÏ`[[#30]]6Kßbo§‰[[#27]]án›ê9¼Ê–GÐ•ÄÉáÛ§•Ÿœ ÿ<3Í™º¹4NfÂÜ*ÜòJ![[#26]]×-@Œ¥Í¸ÌÆÜGú=U in URL	Block	1
66.249.64.235	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
109.65.34.241	Israel	147.237.72.166	aka.idf.il	Unknown HTTP Request Method Œ•ÑTsí#012ŸZRPH¬dS,¥•ÿ[[#4]][[#29]]{…•BšI[[#5]]L[[#26]]”¹Ñ¹€k¬W[[#18]][[#8]][[#5]]ñ[[#1]][[#22]]È[[#0]]R¨é$#012±q[[#26]]¢™VKÆø[[#2]]•[[#24]]%x¼‹	Block	1
46.120.68.255	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/xmlrpc.php	Block	1
109.65.34.241	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Method Œ•ÑTsí#012ŸZRPH¬dS,¥•ÿ[[#4]][[#29]]{…•BšI[[#5]]L[[#26]]”¹Ñ¹€k¬W[[#18]][[#8]][[#5]]ñ[[#1]][[#22]]È[[#0]]R¨é$#012±q[[#26]]¢™VKÆø[[#2]]•[[#24]]%x¼‹	Block	1
173.20.245.205	United States	147.237.76.86	navy.idf.il	Abnormally Long Request method	Block	1
76.237.90.77	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.64.42	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
109.65.34.241	Israel	147.237.72.166	aka.idf.il	NULL Character in Method Œ•ÑTsí#012ŸZRPH¬dS,¥•ÿ[[#4]][[#29]]{…•BšI[[#5]]L[[#26]]”¹Ñ¹€k¬W[[#18]][[#8]][[#5]]ñ[[#1]][[#22]]È[[#0]]R¨é$#012±q[[#26]]¢™VKÆø[[#2]]•[[#24]]%x¼‹	Block	1
109.65.34.241	Israel	147.237.72.166	aka.idf.il	Abnormally Long Request method	Block	1
176.9.58.227	Germany	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/shared/usercontrols/headerupper/	Block	1

03-05-2016-16:04:01 to 03-05-2016-17:04:01