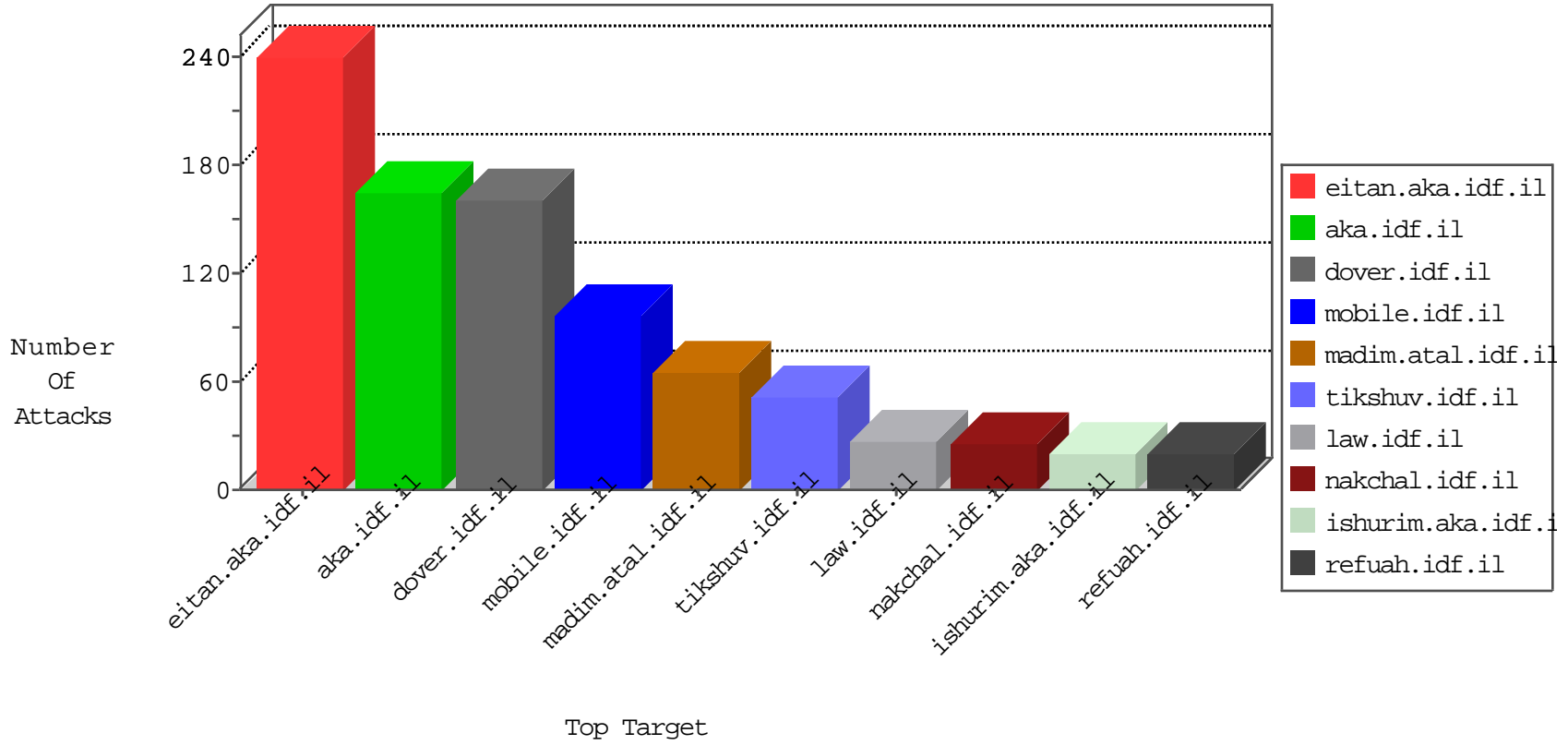


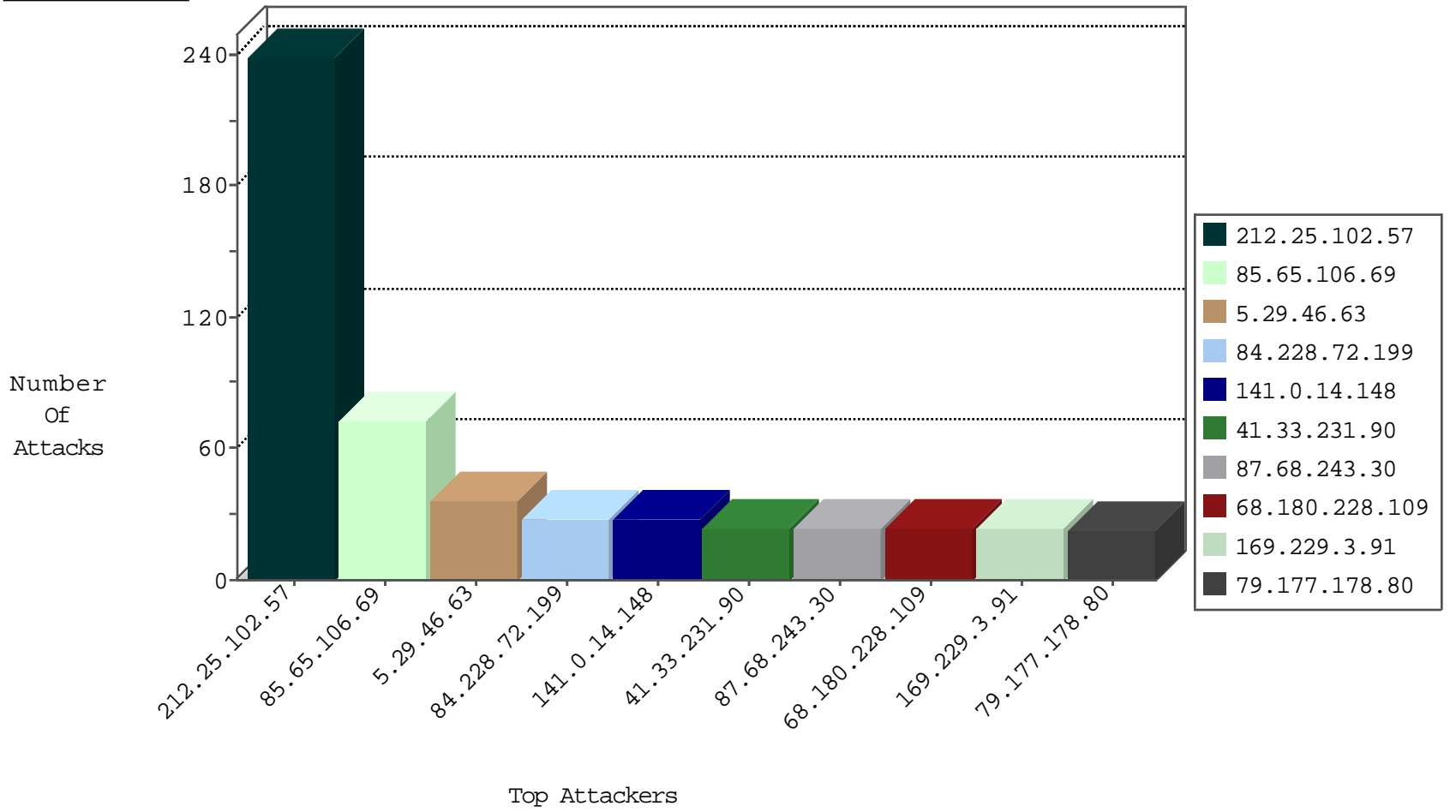
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
217.26.171.188	Moldova, Republic of	147.237.77.176	matpash.idf.il	L4 Source or Dest Port Zero	drop	4
212.179.54.237	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
109.65.49.86	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
183.2.172.4	China	147.237.76.30	himush.idf.il	L4 Source or Dest Port Zero	drop	1
192.187.120.162	United States	147.237.72.217	e.idf.il	Block_Udp_All_Nets	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.120.190.202	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	13
109.65.49.86	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
65.55.210.222	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
94.230.93.179	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
188.120.148.150	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
207.46.13.145	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

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	9
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
37.142.118.230	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	2
176.13.15.28	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
183.61.109.189	147.237.77.243	China	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
167.0.64.9	147.237.76.30	Colombia	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
114.108.128.65	147.237.0.200	Korea, Republic of	m4u.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.144	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
183.61.109.189	147.237.77.243	China	mobile.idf.il	ET SCAN NMAP -sS window 4096	1
120.55.90.163	147.237.77.227	China	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
95.86.123.213	147.237.77.216	Israel	dover.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.25.102.57	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	234
141.0.14.148	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	28
68.180.228.109	United States	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	24
87.68.243.30	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
84.228.72.199	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
2.54.161.98	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
82.80.52.100	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
85.65.63.187	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
54.173.113.175	United States	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	10
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	10
5.102.222.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.52.19.188	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
2.52.174.211	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
185.3.144.71	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
52.5.133.46	United States	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	7
157.55.39.178	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.178.80	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
84.228.72.199	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.66.173.20	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	6
46.19.85.2	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
5.28.167.208	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.2	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.181.32.69	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
176.13.15.28	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
176.13.15.28	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
185.24.206.51	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
37.142.72.86	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.117.179.188	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.85.45	Israel	147.237.72.156	aman.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
54.152.77.211	United States	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
213.57.75.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.28.178.94	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.173.4	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.18.69	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.117.176	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
64.46.23.242	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.54.62.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
176.13.5.58	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.137.241	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.19.86.238	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.65.182.146	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
188.120.154.241	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.65.49.86	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.244.118.251	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
46.19.86.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.80.96.166	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.131.195	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.65.106.69	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	73
5.29.46.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
176.13.5.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
157.55.39.211	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
104.236.207.30		147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 104.236.207.30	Block	4
176.13.15.28	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	4
212.25.102.57	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/1091-he/eitan/asp.	Block	4
46.19.85.72	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
46.120.51.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.1.198	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.130.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.137.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
87.71.9.13	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/controls/atuda/	Block	2
188.29.165.213	United Kingdom	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
176.13.15.28	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
85.65.63.187	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
54.152.77.211	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/checksite/custom-error-page-test	Block	2
77.125.159.105	Israel	147.237.77.170	maarachot.idf.il	Unauthorized HTTP Method	Block	2
169.229.3.91	United States	147.237.76.39	mobile.meitav.idf.il	Unknown HTTP Request Method ?-lcMh"e/Üæd%\$¶+ÅEã?há81@úí%ö6"pè[[#25]] in URL +[[#21]]j6Ú Û[[#17[[[*]]#4[[,]]#4]]#012 ¶e çŠr[[#22]]&t	Block	1
79.177.178.80	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Value	Block	1
54.173.113.175	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/news	Block	1
199.119.139.3	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.177.178.80	Israel	147.237.72.166	aka.idf.il	Illegal HTTP Version	Block	1
169.229.3.91	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Malformed URL	Block	1
77.125.159.105	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/sip_storage/files/4/	Block	1
213.244.118.245	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
169.229.3.91	United States	147.237.76.39	mobile.meitav.idf.il	Abnormally Long Request method	Block	1
46.19.86.153	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
79.177.178.80	Israel	147.237.72.166	aka.idf.il	NULL Character in Query String [[#31]][[#3]]Y[[#17 ~]]2[[#2p]]0#[[c]] u'<üM on æ ¶]]v[[#6]]I[[#1]]#11[[3 ~]]#31[[]]	Block	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
169.229.3.91	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Illegal Byte Code Character in Header Name	Block	1
79.177.178.80	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Method gGU=/ [[#19]]F¥+æü-ãE(Z[[#5]]äfæ°Ei+)%b[[#25]][[#29]]ÓM[[#11]]f•)XS [[#28]]è5@ð1çü[[#29]]äÖL%Y>1B+gH~,EtèÜmì)ðè+[[#18]]1[[#6]]Ä* !ÄÇg•hš"µ>[[#26]]İ3[[#6]]\$øö/xðf1šX•R[[#25]]+?[[#22]]eİ%4[[#19]]][•eNcd-tù^[[#1]]øÑct[[#31]][[#3]].Ü[[#5]]/!&ÇSiè-ø)+sø'8E	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation pageNum in www.idf.il/1393-en/dover.aspx	Block	1
207.46.13.162	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Untraceable SSL Sessions from 207.46.13.162 (Unknown Server Certificate)	None	1
141.212.122.177	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
84.228.72.199	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
79.177.178.80	Israel	147.237.72.166	aka.idf.il	Malformed HTTP Header Line 3	Block	1
169.229.3.91	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unknown HTTP Request Method	Block	1
79.177.178.80	Israel	147.237.72.166	aka.idf.il	Abnormally Long Header Line request header name	Block	1
216.218.206.68	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
169.229.3.91	United States	147.237.76.39	mobile.meitav.idf.il	Illegal Byte Code Character in Method ?-lcMh"e/Üæd%\$¶+ÅEã?há81@úí%ö6"pè[[#25]]	Block	1
192.117.138.210	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
173.208.136.114	United States	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
79.177.178.80	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
169.229.3.91	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
79.177.178.80	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Parameter Name [[#31]][[#3]]Y[[#17 ~]] 2[[#2]]c[[#0]]p[[]] #31~]] 3[[#11]]v[[#6]]I[[#1]]¶ æ u'<üM in	Block	1
74.82.47.2	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
207.46.13.162	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
149.78.103.2	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/console/core/doc_mgr/undefined	Block	1