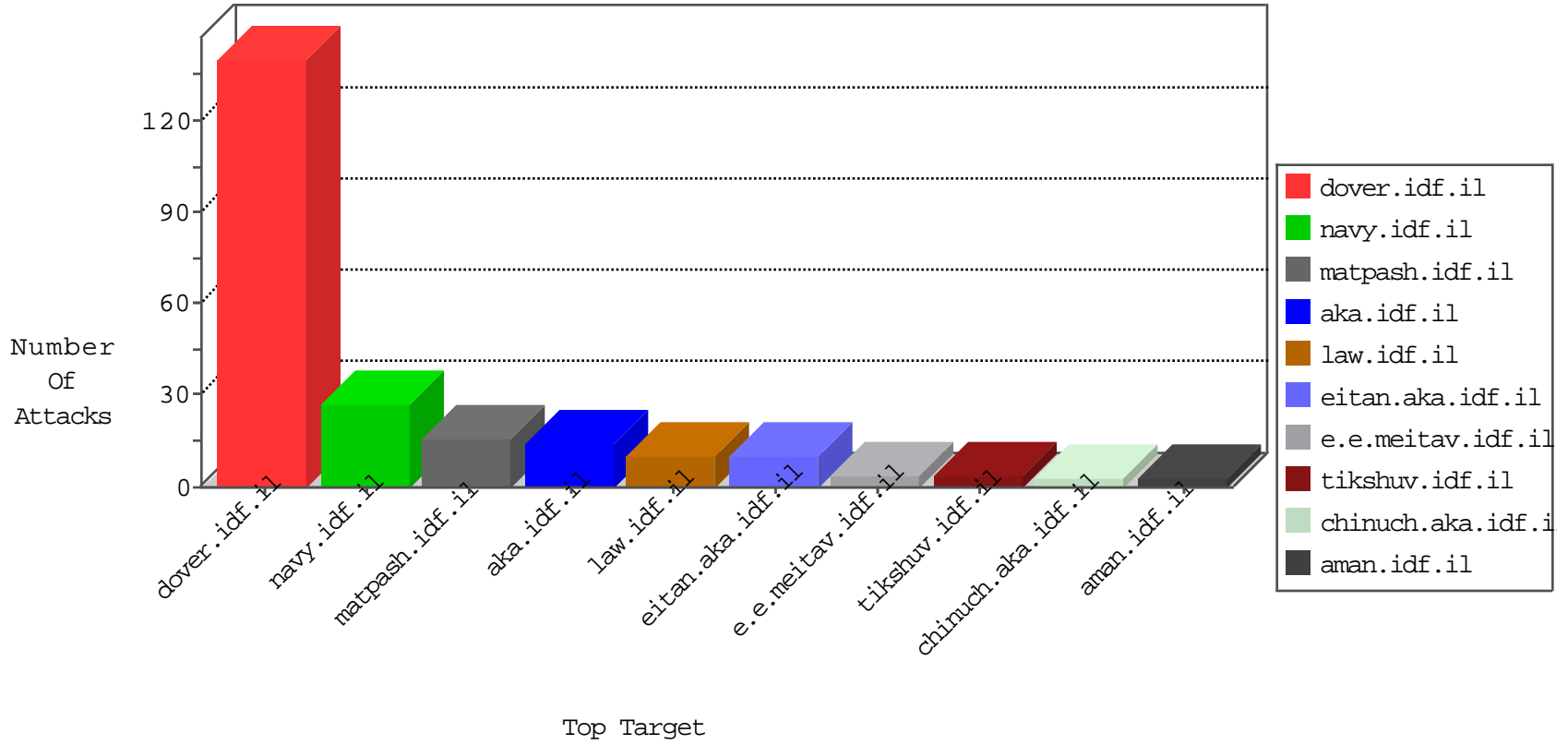


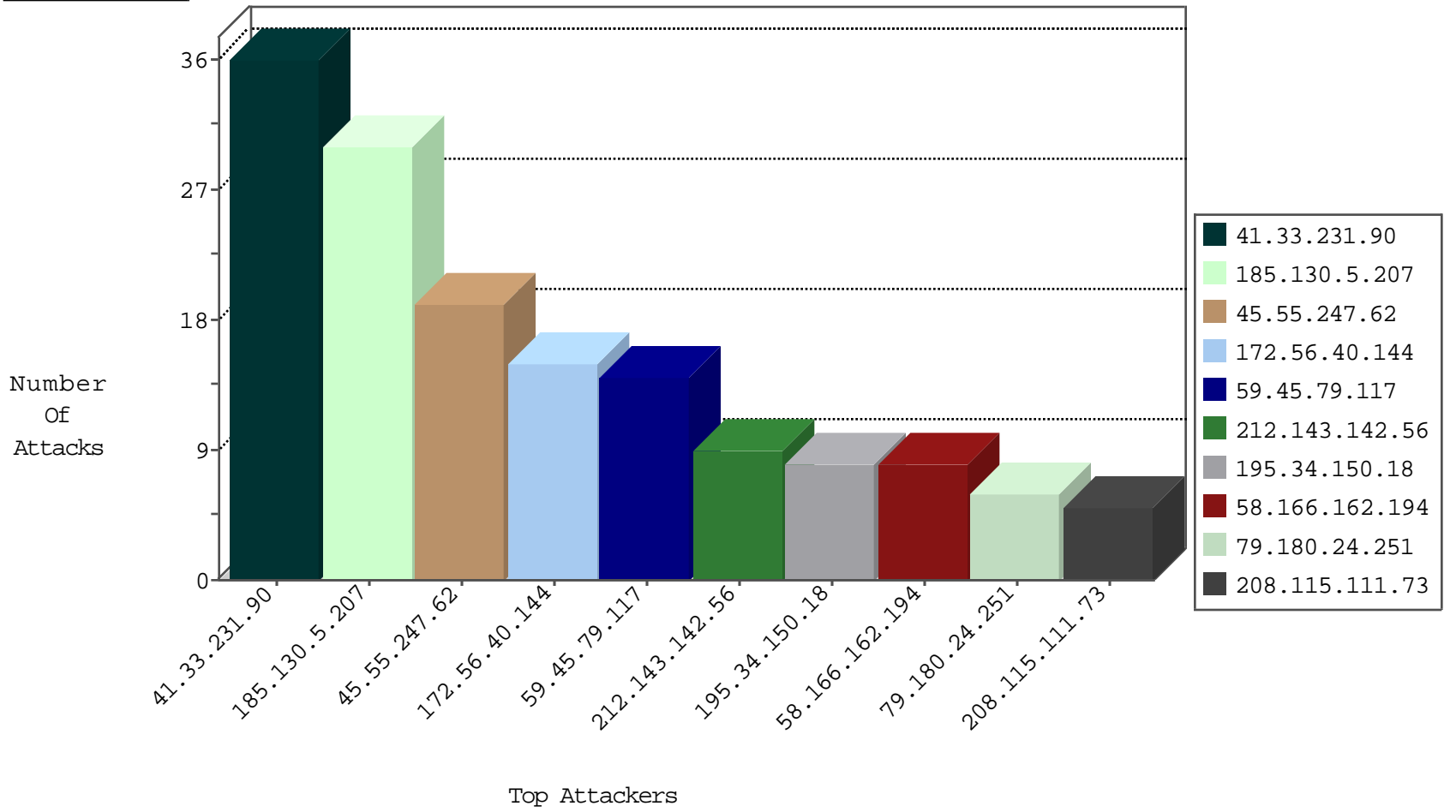
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
72.69.189.184	United States	147.237.76.147	chinuch.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	1

02-06-2016-04:04:01 to 02-06-2016-05:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

Top Attackers In IDF

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
202.106.54.203	147.237.76.38	China	e.e.meitav.idf.il	GPL SCAN nmap TCP	2
219.142.79.3	147.237.76.38	China	e.e.meitav.idf.il	GPL SCAN nmap TCP	2
59.45.79.117	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
112.171.173.85	147.237.8.50	Korea, Republic of	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
112.171.173.85	147.237.8.28	Korea, Republic of	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
112.171.173.85	147.237.8.24	Korea, Republic of	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.233	China	atal.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.205	China	prisha.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.74	China	law.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
209.126.116.147	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.14	China	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
112.171.173.85	147.237.8.46	Korea, Republic of	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
112.171.173.85	147.237.8.27	Korea, Republic of	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.243	China	mobile.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.179	China	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.148	China	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
185.130.5.207		147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
172.56.40.144	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	15
45.55.247.62		147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
138.134.102.16	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
91.200.12.143	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
91.200.12.7	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
104.131.115.180	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	3
85.250.165.181	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.252.234	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
91.200.12.106	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
66.249.78.177	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
208.115.111.73	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
66.249.78.245	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
157.55.39.79	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
65.55.210.192	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
66.249.65.122	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
79.178.127.134	Israel	147.237.77.170	maarachot.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
184.105.139.124	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.187.114.171	France	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
136.243.67.234	Germany	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
84.228.252.234	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
74.82.47.19	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.121.96.204	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
182.118.20.173	China	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
80.246.136.94	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.96	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.228.252.234	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
74.82.47.23	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
208.115.111.73	United States	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	1
182.118.20.173	China	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
101.226.168.243	China	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1
81.218.163.108	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
216.218.206.106	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
73.244.226.177	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
74.82.47.42	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
208.115.111.73	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
184.105.139.100	United States	147.237.8.46	e.chimuch.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
101.226.168.243	China	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
81.218.163.108	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
73.244.226.177	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
198.1.101.123	United States	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
75.126.221.55	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
184.105.139.124	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.101.218.65	Russian Federation	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
45.55.247.62		147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 45.55.247.62	Block	4
79.180.24.251	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	3
79.180.24.251	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	3
66.249.65.145	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
91.189.41.165	Sweden	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 91.189.41.165	Block	2
73.22.155.10	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/	Block	2
45.55.247.62		147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	1
213.163.66.185	Netherlands	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/links/links.aspx	Block	1
107.20.255.148	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	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
58.166.162.194	Australia	147.237.76.86	navy.idf.il	Illegal Byte Code Character in Method Å,[[#0]][[#0]][[#0]]\$<[[#16]]Åœ Å„mSÅ"Å<[[#1]]Å"m[[#18]]OÅ„BYÅ;[[#24]]y[[#12]]Å~!rc[[#18]]Å'Å< [[#12]]Å?[[#1]]g: [[#5]]Å±Å-Åž[[#4]]J8I3JÅ\$g/Å"JÅfÅ-	Block	1
192.243.55.135	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.135	Block	1
41.239.187.186	Egypt	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
66.249.66.137	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
58.166.162.194	Australia	147.237.76.86	navy.idf.il	Abnormally Long Header Line request header name	Block	1
216.218.206.66	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
157.55.39.209	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/newsite/english/	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation pageNum in www.cogat.idf.il/901-he/cogat.aspx	Block	1
58.166.162.194	Australia	147.237.76.86	navy.idf.il	Malformed URL	Block	1
45.35.104.98		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.asp	Block	1
199.16.128.53	Canada	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to chinuch.aka.idf.il/wp/wp-admin/	Block	1
87.69.245.216	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
66.249.66.142	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/favicon.ico	Block	1
58.166.162.194	Australia	147.237.76.86	navy.idf.il	Abnormally Long Request method	Block	1
157.55.39.211	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
68.180.230.244	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
58.166.162.194	Australia	147.237.76.86	navy.idf.il	NULL Character in Method Å,[[#0]][[#0]][[#0]]\$<[[#16]]Åœ Å„mSÅ"Å< [[#1]]Å"m[[#18]]OÅ„BYÅ;[[#24]]y[[#12]]Å~!rc[[#18]]Å'Å< [[#12]]Å?[[#1]]g: [[#5]]Å±Å-Åž[[#4]]J8I3JÅ\$g/Å"JÅfÅ-	Block	1
45.35.104.99		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.asp>hebrew 	Block	1
207.46.13.192	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/robots.txt	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 4d9c6f40 in www.aka.idf.il/main/kapatz/contactus.aspx	None	1
58.166.162.194	Australia	147.237.76.86	navy.idf.il	Illegal Byte Code Character in Header Name kÅ;ÅŠÅ"Å"AAÅ?Å?ÅtÅ„•Å, Å„[[#20]][[#18]]qÅµ>'Åœ[[#16]]Åf [[#15]]-Å½Å¾Å"[[#22]]Å²<6fÅ¾tÅ?QjÅ<ÅžÅ„Å¥Åžb/,Å, ÅœÅ?Å»[[#28]][[#6]]T[[#19]]`mTrtÅ>Å~-Å,	Block	1
172.82.175.167		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
40.77.167.70	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/authentication/	Block	1
58.166.162.194	Australia	147.237.76.86	navy.idf.il	Unknown HTTP Request Method Å,[[#0]][[#0]][[#0]]\$<[[#16]]Åœ Å„mSÅ"Å< [[#1]]Å"m[[#18]]OÅ„BYÅ;[[#24]]y[[#12]]Å~!rc[[#18]]Å'Å< [[#12]]Å?[[#1]]g: [[#5]]Å±Å-Åž[[#4]]J8I3JÅ\$g/Å"JÅfÅ- in URL	Block	1
213.163.66.185	Netherlands	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 213.163.66.185	Block	1
104.247.216.212		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp>israeli	Block	1
66.249.78.239	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter pageNum in eitan.aka.idf.il/938-en/eitan.aspx	None	1
58.166.162.194	Australia	147.237.76.86	navy.idf.il	Illegal Byte Code Character in Header Value	Block	1
184.168.46.5	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/	Block	1
41.239.187.186	Egypt	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1