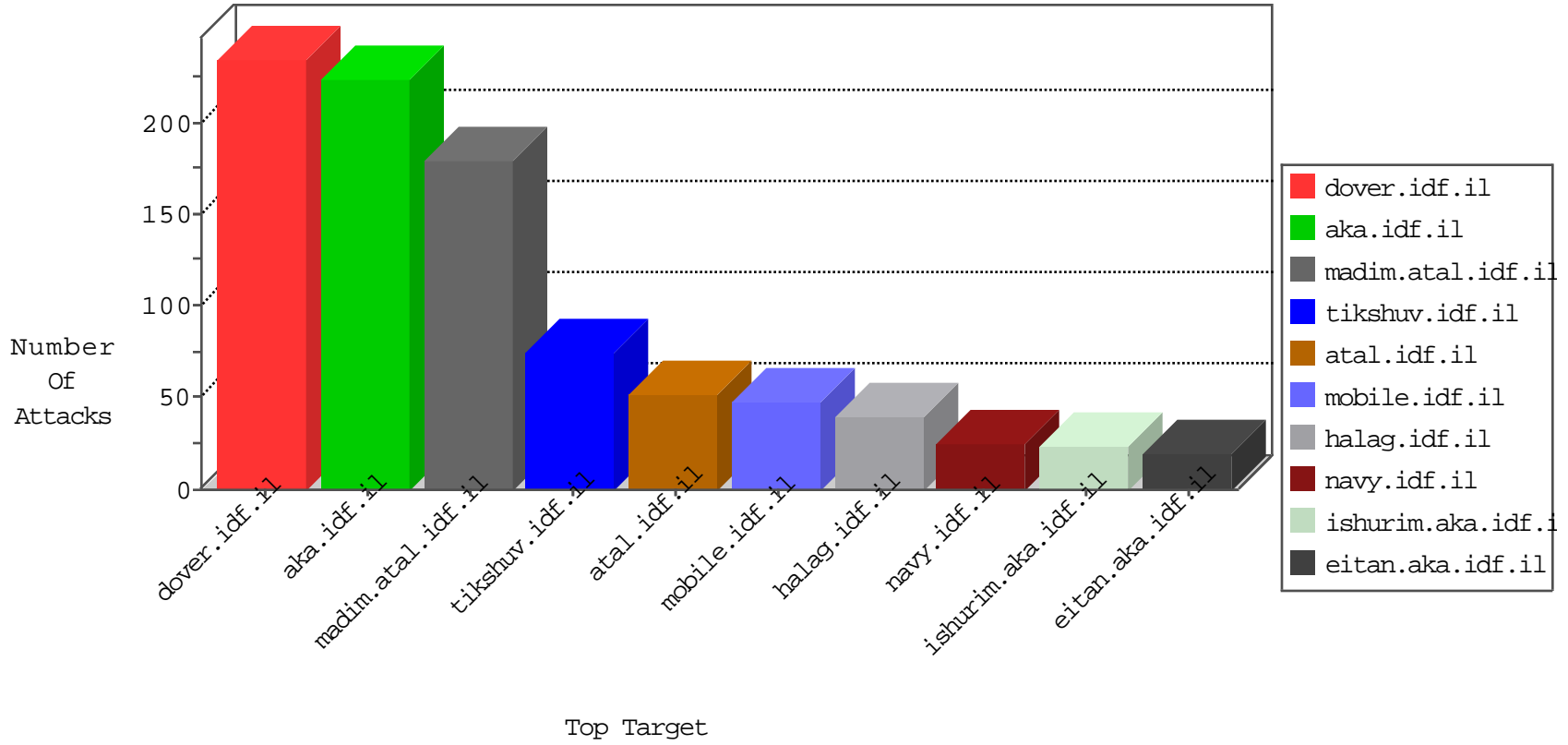


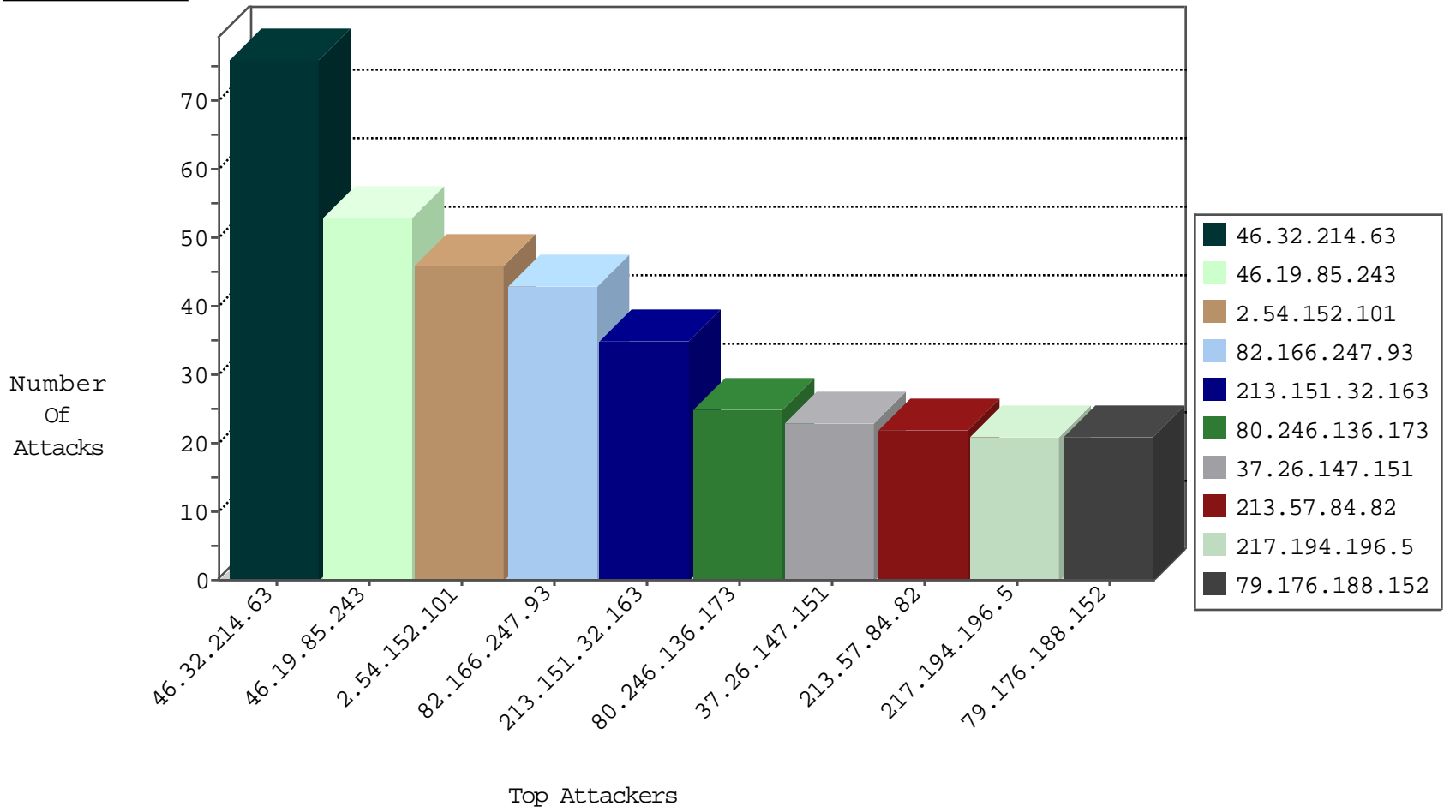
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.32.214.63	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SQL-Inj-Pang-GMSSQLInt1	dest-reset	57
41.137.23.30	Morocco	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-Url	dest-reset	3
82.145.217.21	Europe	147.237.72.167	ishurim.aka.idf.il	Block_Ip_Web_In	drop	3
184.105.247.223	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Udp_All_Nets	drop	1
64.21.147.6	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
216.47.169.70	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
89.248.172.207	Netherlands	147.237.77.243	mobile.idf.il	Block_Ntp_All_Net	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
217.194.196.5	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	19
79.183.211.18	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
199.30.24.159	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
69.30.198.186	United States	147.237.72.156	aman.idf.il	C1000074: HTTP: majestic bot	Block	2
109.64.125.21	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
192.118.12.102	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
198.20.69.74	United States	147.237.8.27	e.madim.atal.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
207.46.13.70	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.102.6.251	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sA (2)	1
46.19.85.84	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.72.166	China	aka.idf.il	ET SCAN NMAP -sS window 1024	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
89.139.131.113	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.179.192.157	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.32.214.63	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	SQL 1 = 1 - possible sql injection attempt	1
217.156.163.145	147.237.77.216	United Kingdom	dover.idf.il	portscan: TCP Distributed Portscan	1
104.44.133.108	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -sS window 4096	1
81.218.178.50	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.54.152.101	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	38
82.166.247.93	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	29
31.168.3.26	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
213.57.84.82	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
82.166.247.93	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
46.32.214.63	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
176.13.7.243	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.176.152.205	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.179.199.166	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.149.141	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
46.19.85.206	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.49	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
79.183.211.18	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.26.147.151	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
80.246.130.250	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
95.35.166.215	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
95.35.166.215	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
37.26.147.151	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
95.35.166.215	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
212.179.21.194	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	7
212.179.21.194	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
80.246.136.173	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.2	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.49	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.23.231	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.107	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.64	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.27.105.137	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.7.1	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.206	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
207.232.28.213	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.123	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
85.130.240.165	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
207.232.28.213	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
64.233.172.209	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.123	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
213.57.84.82	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
188.161.17.235	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
147.236.50.70	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.86.33	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.58.126	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.60.34	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.187.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.89	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.130.240.165	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.253.141.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

03-10-2016-13:04:08 to 03-10-2016-14:04:08

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.86.49	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.137.83	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
141.8.132.112	Russian Federation	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
46.19.85.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	53
213.151.32.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
79.176.188.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
80.246.136.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	19
46.19.86.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	17
46.19.86.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
176.13.7.1	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
31.168.116.1	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 31.168.116.1	Block	6
46.32.214.63	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.32.214.63	Block	4
176.13.7.243	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.147.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.148.138	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 37.26.148.138	Block	2
37.26.148.138	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
2.54.169.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal HTTP Version	Block	1
80.246.137.91	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
5.29.36.156	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/giyos	Block	1
66.249.64.253	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	Illegal Byte Code Character in Method Å3I':İ¶0g'NŞ[[#21]]Ş6[[#19]]ozúŞ>İ@H	Block	1
40.77.167.10	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
94.185.83.100	Sweden	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to testpl.piwo.pila.pl/testproxy.php	Block	1
37.26.146.144	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
2.54.52.214	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
185.120.126.10		147.237.77.74	law.idf.il	PHP Attempt	Block	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Malformed URL Ýz	Block	1
82.102.169.113	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
5.29.119.39	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ctl00\$cphMain\$cphSachar\$cb14490455 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8910-he/refuah.aspx	Block	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	Malformed URL	Block	1
46.19.85.64	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
37.26.146.217	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
157.55.39.112	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
2.54.152.107	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.180.150.131	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ctl00\$cphMain\$cphSachar\$ctl155 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
185.120.126.10		147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/xmlrpc.php	Block	1
37.26.148.196	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unknown HTTP Request Method ošá_•X[[#30]]ŞNÅ in URL Ýz	Block	1
82.166.247.93	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
74.82.47.2	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	Unknown HTTP Request Method Å3I':İ¶0g'NŞ[[#21]]Ş6[[#19]]ozúŞ>İ@H in URL	Block	1
46.19.85.160	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
37.26.146.234	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Byte Code Character in Header Name	Block	1
79.182.186.210	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to ww.idf.il/https://ww.idf.il/	Block	1
207.232.21.105	Israel	147.237.72.167	ishurim.aka.idf.il	Admin Blocking	Block	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	Abnormally Long Request method	Block	1
37.26.149.141	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
87.69.36.210	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
31.184.238.200	Russian Federation	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1