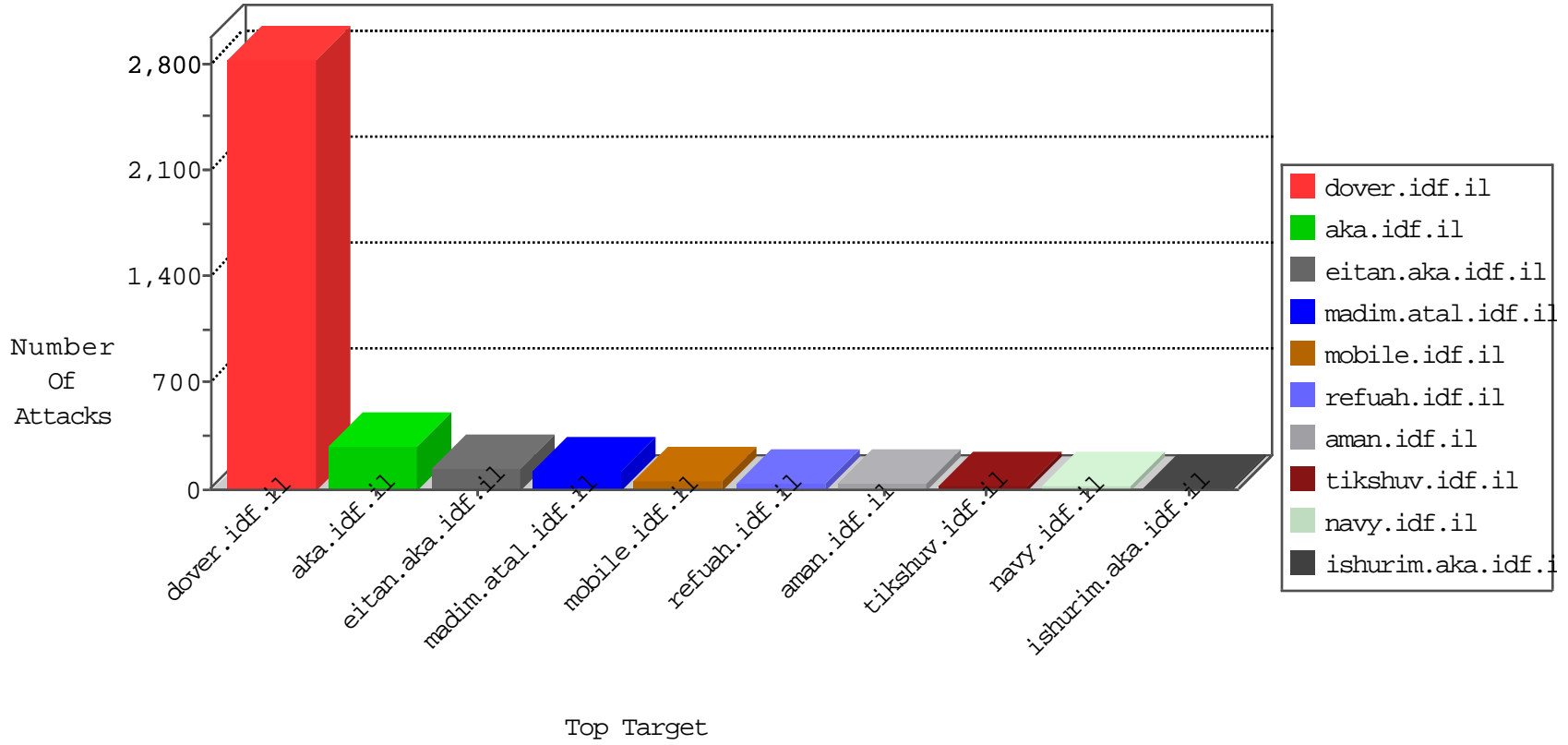


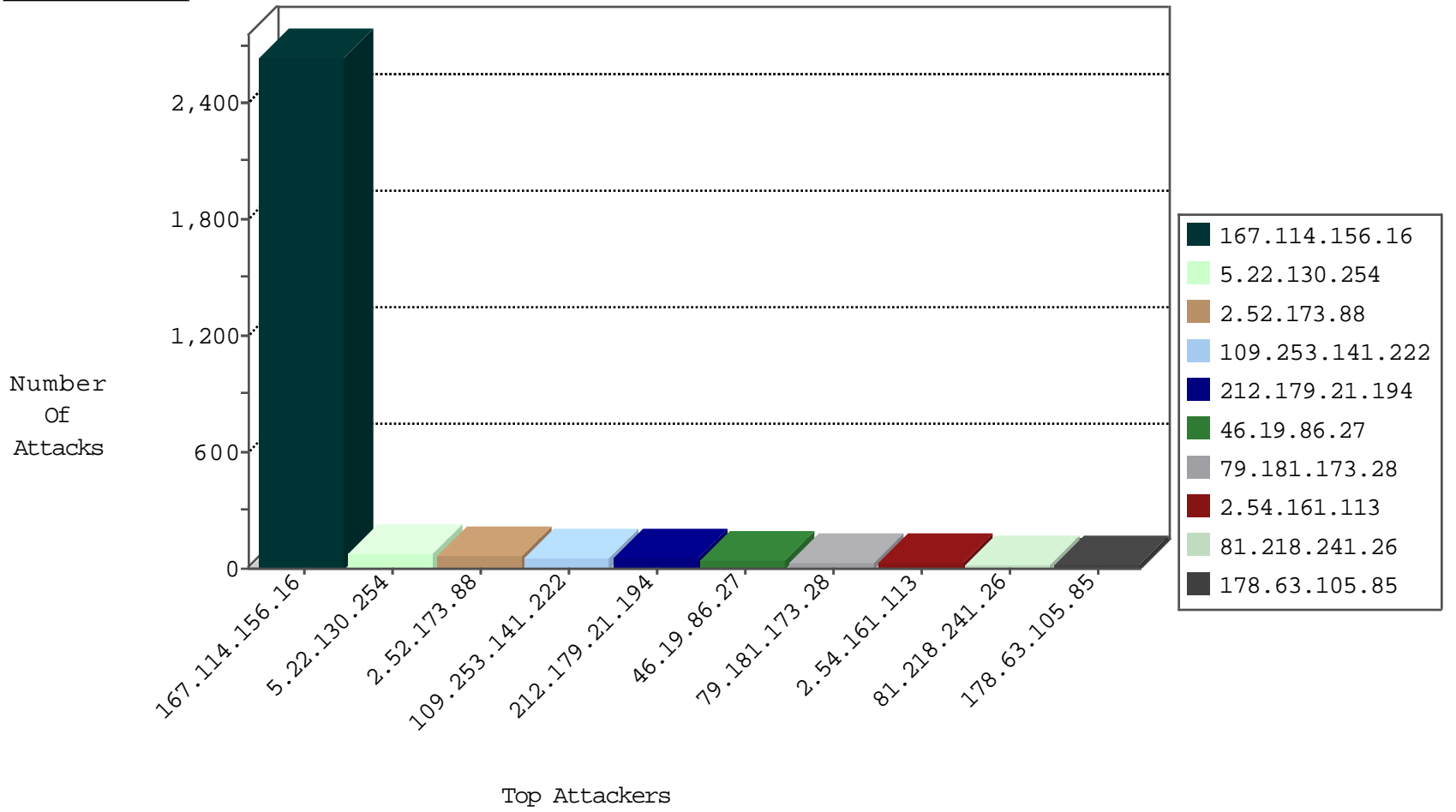
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3406
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	126
81.218.65.210	Israel	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
184.105.139.110	United States	147.237.8.50	e.tikshuv.idf.il	Block_Ntp_All_Net	drop	1
50.30.37.38	United States	147.237.8.24	e.lifestyle.idf.il	Block_Udp_All_Nets	drop	1
199.58.80.184	Canada	147.237.8.14	e.orchot.idf.il	I4 Source or Dest Port Zero	drop	1
184.105.139.82	United States	147.237.8.14	e.orchot.idf.il	Block_Ntp_All_Net	drop	1
218.57.11.7	China	147.237.76.199	e.nakchal.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
184.105.139.106	United States	147.237.77.243	mobile.idf.il	Block_Ntp_All_Net	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.28	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	5
79.180.171.223	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	5
82.80.152.34	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	2
62.0.118.10	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
60.49.72.184	Malaysia	147.237.77.216	dover.idf.il	12347: HTTP: PHP-CGI Query String Parameter Information Disclosure Vulnerability	Block	1

## 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	2
185.72.179.226	147.237.72.166		aka.idf.il	ET SCAN NMAP -f -sS	1
109.65.85.48	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.76.44	China	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
218.57.11.7	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
212.235.34.70	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.105.134.220	147.237.72.167	Sweden	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
185.72.179.226	147.237.72.166		aka.idf.il	ET SCAN NMAP -sS window 2048	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.34.63	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.57.11.7	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
218.57.11.7	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
193.105.134.220	147.237.8.24	Sweden	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.22.130.254	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	81
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	79
2.52.173.88	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	60
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	25
79.181.173.28	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
132.68.43.124	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack		reject	16
84.95.3.101	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
84.95.217.170	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	12
176.13.22.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.19.85.77	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.159	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	8
212.179.214.113	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
37.26.149.138	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
212.179.214.113	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
80.246.130.93	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.19.85.190	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.195.92.148	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.77	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.201	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
149.78.230.179	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.36	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.52.129.72	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.96.211	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.201	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.138.107	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.54.161.113	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.161.113	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.190	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.168.173.102		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
132.68.47.19	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
199.203.63.167	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
193.43.245.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
157.55.39.202	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
85.130.216.49	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
178.63.105.85	Germany	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	4
2.54.161.113	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
80.246.137.76	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
178.63.105.85	Germany	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	4
2.54.161.113	Israel	147.237.77.216	dover.idf.il	SYN Attack		reject	4
80.179.22.148	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
132.65.125.40	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.240.69	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.171.223	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
2.54.161.113	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
62.90.164.101	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.235	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.141.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	51
46.19.86.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
176.13.9.75	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	15
109.253.223.5	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter CurrentPassword	Block	12
80.246.136.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
2.54.63.45	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
2.54.161.216	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
195.95.183.254	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 195.95.183.254	Block	5
2.52.33.38	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.217.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.54.165.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
147.235.8.61	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter CurrentPassword	Block	2
109.253.156.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.9.121	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
62.219.137.5	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
176.13.23.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
81.218.199.148	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 81.218.199.148	Block	1
207.46.13.105	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.105	Block	1
173.208.136.114	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
93.169.81.239	Romania	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
217.194.207.24	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
79.180.150.131	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$ct151 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
81.218.199.148	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/8/	Block	1
66.249.78.216	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/authentication/index	Block	1
207.46.13.105	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	1
173.208.136.114	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
5.29.231.149	Israel	147.237.76.200	eitan.aka.idf.il	Cookie Tampering on cookie __atssc: Expected facebook;2, Observed facebook;3	None	1
79.180.150.131	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$ct171 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
195.154.73.222	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
46.19.86.244	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
2.52.34.51	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/0/70610.pdf	Block	1
207.46.13.160	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
37.26.148.194	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
62.105.140.248	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage	Block	1
197.7.172.18	Tunisia	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
157.55.39.116	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
93.115.95.204	Anonymous Proxy	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/./shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
68.180.228.167	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1035-ar/cogat.aspx	Block	1
207.241.229.224	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/faq/faq.aspx	Block	1
37.26.148.241	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
1.132.96.199	Australia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
80.246.137.76	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
207.46.13.70	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/	Block	1
157.55.39.202	United States	147.237.72.166	aka.idf.il	Unknown Parameter tm in www.aka.idf.il/main/giyus/	None	1
93.169.81.239	Romania	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
210.187.26.2	Malaysia	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1