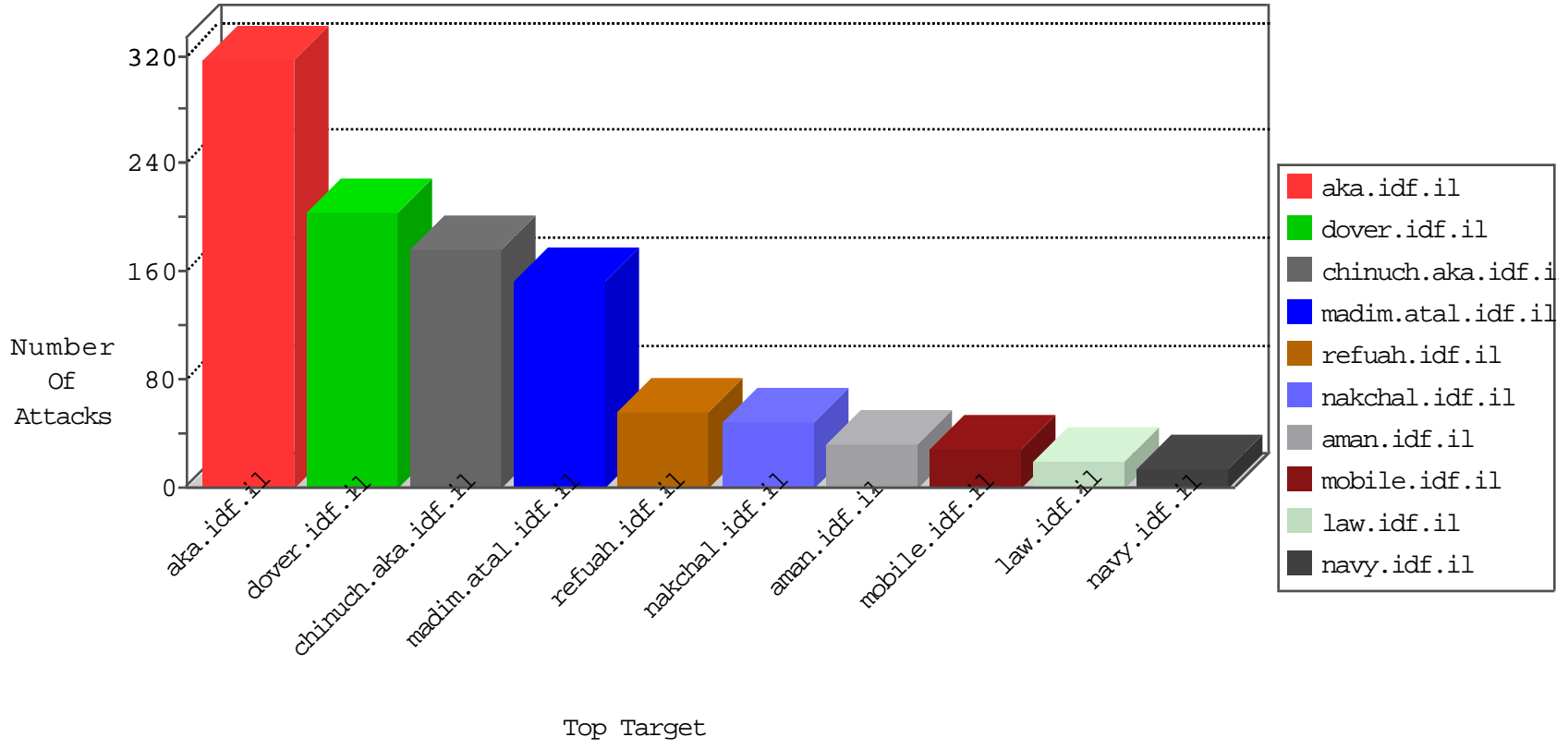


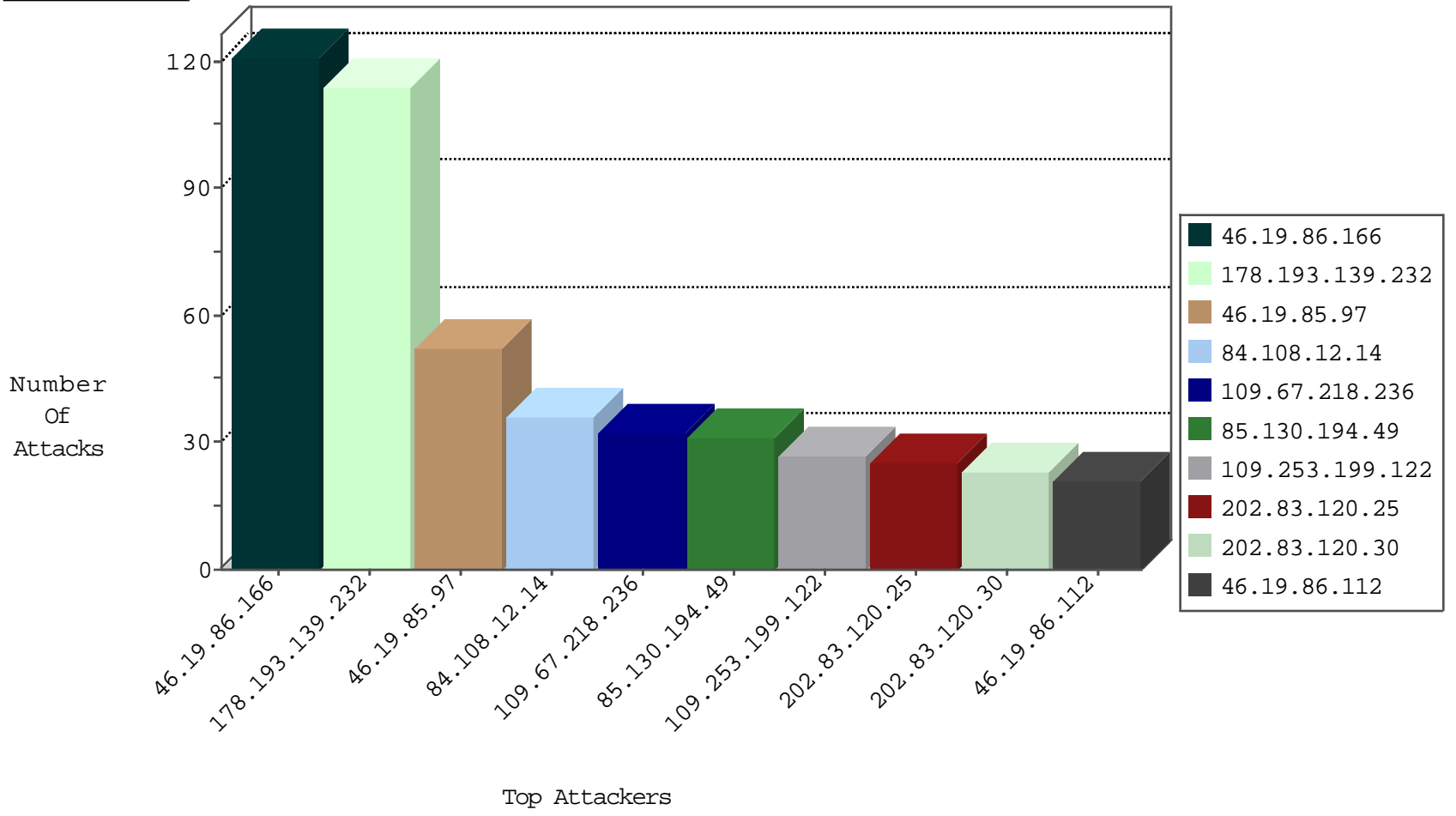
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.238.23	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
110.249.208.86	China	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
93.174.94.235	Netherlands	147.237.76.201	e.atal.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1
110.249.208.86	China	147.237.0.15	kosher-kravi.idf.il	TCP Scan (vertical)	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
75.75.210.162	United States	147.237.0.15	kosher-kravi.idf.il	10993: HTTP: Morfeus Scanner Scanning Attempt	Block	1
75.75.210.162	United States	147.237.0.19	madim.atal.idf.il	10993: HTTP: Morfeus Scanner Scanning Attempt	Block	1
75.75.210.162	United States	147.237.77.216	dover.idf.il	10993: HTTP: Morfeus Scanner Scanning Attempt	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
146.200.148.0	147.237.77.216	United Kingdom	dover.idf.il	Tehila - Perl LWP with fake user agent	2
46.33.34.16	147.237.8.46	Ukraine	e.chinuch.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
14.41.15.12	147.237.76.42	Korea, Republic of	refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
185.129.148.230	147.237.76.199	Latvia	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.69.228	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	1
23.91.75.231	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
218.5.244.35	147.237.72.14	China	dover.idf.il(ol	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
163.172.129.15	147.237.0.200	United Kingdom	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
78.129.171.173	147.237.76.34	United Kingdom	yohalan.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.67.218.236	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	32
178.193.139.232	Switzerland	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	27
178.193.139.232	Switzerland	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	25
178.193.139.232	Switzerland	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	23
178.193.139.232	Switzerland	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	22
141.0.15.74	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	20
178.193.139.232	Switzerland	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
46.19.85.97	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
46.19.85.97	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
46.19.85.97	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
46.19.85.97	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
37.26.146.145	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.199.122	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	11
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
109.66.176.197	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	9
46.19.86.112	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
185.32.179.158	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
109.64.182.70	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
109.253.199.122	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.112	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
109.253.134.206	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
46.19.85.64	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
85.130.194.49	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.112	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
202.83.120.30	Indonesia	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
85.130.194.49	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
81.218.175.8	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
202.83.120.30	Indonesia	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	6
109.201.133.100	Netherlands	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
202.83.120.30	Indonesia	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	6
109.253.130.238	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
202.83.120.25	Indonesia	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
85.130.194.49	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
80.246.136.25	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
202.83.120.25	Indonesia	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	5
46.19.85.127	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
80.246.136.25	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.85.68	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
202.83.120.25	Indonesia	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	5
79.181.235.197	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.85.64	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
85.130.194.49	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
80.246.136.25	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.55	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
202.83.120.25	Indonesia	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.64	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
176.13.21.127	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
85.130.194.49	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
147.235.8.74	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
2.53.63.123	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	117
84.108.12.14	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.108.12.14	Block	17
46.19.86.98	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
109.253.211.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
109.65.183.147	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	5
95.35.137.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
46.19.86.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
132.72.174.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
194.90.128.185	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 194.90.128.185	Block	4
37.26.146.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.229.78.215	Israel	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/1065-he/dover.aspx parameter SearchText	Block	2
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atall/izkor/view_imgtop.asp	Block	2
84.108.12.14	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/	Block	2
37.26.146.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.13	Israel	147.237.77.243	mobile.idf.il	Untraceable SSL Sessions: Open Mode	None	2
213.151.35.214	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/gyius/news.aspx	Block	2
37.26.147.220	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
188.120.148.92	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/	Block	2
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atall/izkor/view_img.asp	Block	2
77.139.108.213	France	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
66.249.64.89	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter lang in www.eitan.aka.idf.il/1103-en/eitan.aspx	None	1
84.108.12.14	Israel	147.237.72.166	aka.idf.il	Unknown Parameter Slip in www.aka.idf.il/main/sachar/viewpayslip.aspx	None	1
84.108.12.14	Israel	147.237.72.166	aka.idf.il	Unknown Parameter IsPDF in www.aka.idf.il/main/sachar/viewpayslip.aspx	None	1
217.132.9.222	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
79.181.1.178	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
37.8.40.143	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.13.5.53	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.108.12.14	Israel	147.237.72.166	aka.idf.il	Unknown Parameter IsPDFForma in www.aka.idf.il/main/sachar/viewpayslip.aspx	None	1
66.102.9.5	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 66.102.9.5	Block	1
40.77.167.41	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
194.90.128.185	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/trigger.png	Block	1
84.108.12.14	Israel	147.237.72.166	aka.idf.il	Unknown Parameter IsM in www.aka.idf.il/main/sachar/viewpayslip.aspx	None	1
77.139.116.159	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https://www.aman.idf.il/	Block	1
2.53.2.118	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
109.65.183.147	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakchal.idf.il/sip_storage/files/2/	Block	1
66.249.64.141	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/sip_storage/files/8/638.pds	Block	1
84.108.12.14	Israel	147.237.72.166	aka.idf.il	Unknown Parameter SlipI in www.aka.idf.il/main/sachar/viewpayslip.aspx	None	1
84.108.12.14	Israel	147.237.72.166	aka.idf.il	Unknown Parameter IsPDF in www.aka.idf.il/main/sachar/viewpayslip.aspx	None	1
185.32.179.62	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
85.130.234.154	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.75.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19667-he/idfgdover.aspx	Block	1
66.102.9.5	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/gyius/pniot.aspx	Block	1
84.108.12.14	Israel	147.237.72.166	aka.idf.il	Unknown Parameter S in www.aka.idf.il/main/sachar/viewpayslip.aspx	None	1
46.19.85.218	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.151.35.214	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 213.151.35.214	Block	1
84.108.12.14	Israel	147.237.72.166	aka.idf.il	Unknown Parameter IsMu in www.aka.idf.il/main/sachar/viewpayslip.aspx	None	1
77.139.212.159	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	1
2.53.46.119	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/gyius/null	Block	1
66.249.69.18	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atall/izkor/view_img.asp	Block	1
84.108.108.202	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1