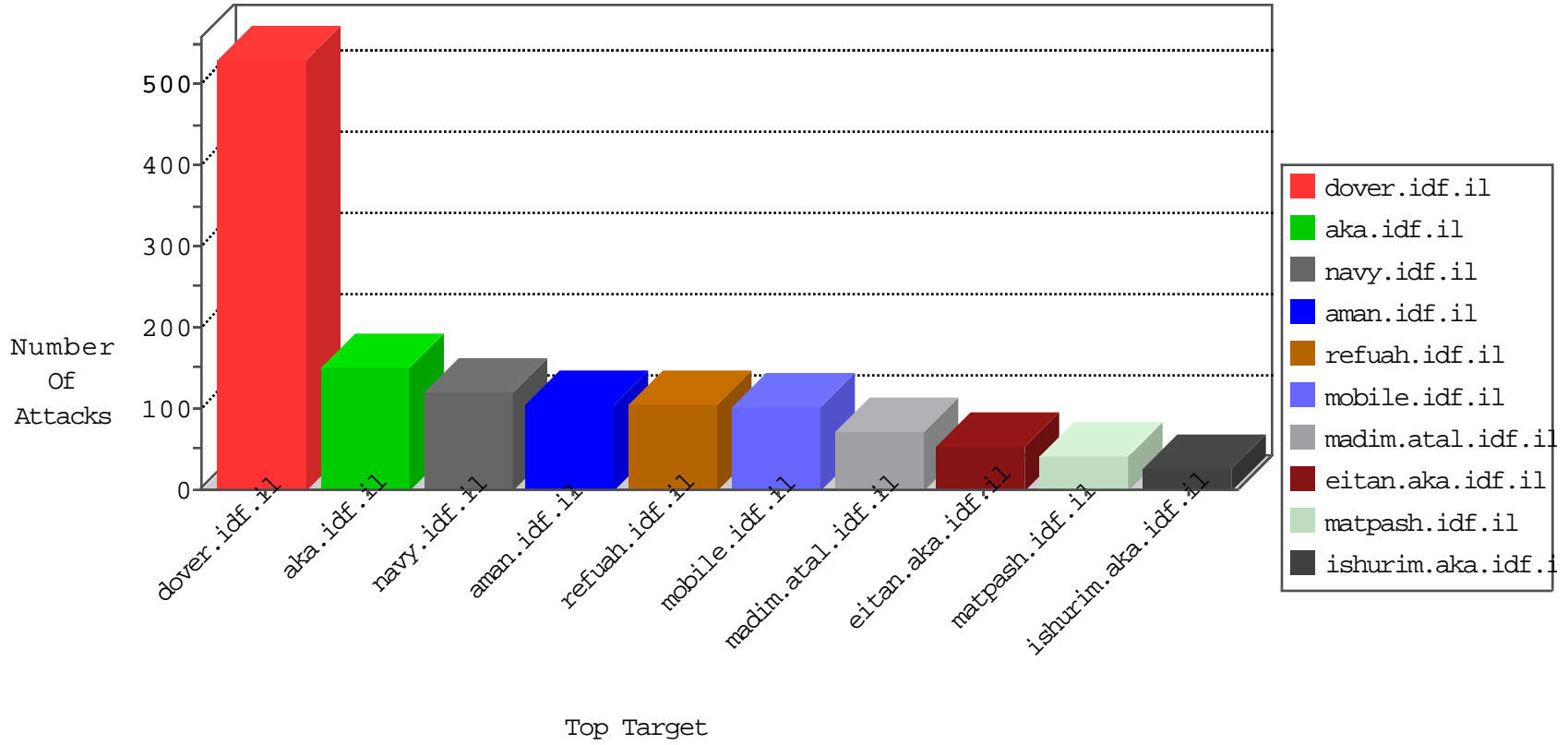


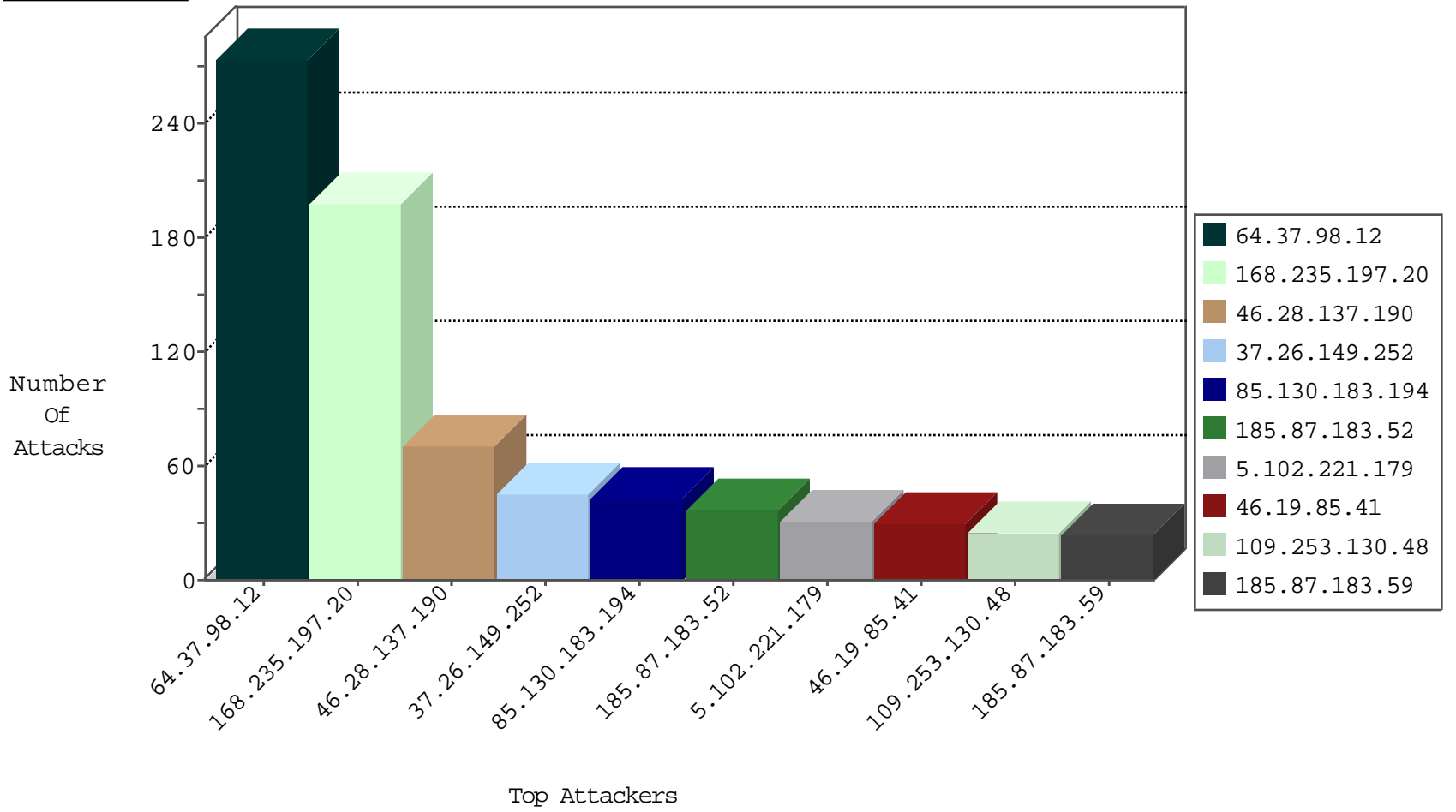
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
168.235.197.20	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	51
168.235.197.20	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	31
157.55.39.74	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
168.235.197.20	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	3
71.6.216.45	United States	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1
208.67.1.32	United States	147.237.76.86	navy.idf.il	Black List	drop	1
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
71.6.216.37	United States	147.237.76.31	nakchal.idf.il	Black List	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
198.27.100.198	Canada	147.237.77.216	dover.idf.il	C1000026: HTTP: Access to - index.php?option=com_jce	Permit	6
151.80.31.183	France	147.237.72.156	aman.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1
198.27.100.198	Canada	147.237.77.216	dover.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
45.56.108.106	147.237.76.39	United States	mobile.meitav.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
62.210.113.216	147.237.77.74	France	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
31.168.13.78	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.241.253	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.65.90.207	147.237.77.226	Israel	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	1
84.109.29.18	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.178.149.52	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
203.86.3.66	147.237.0.34	China	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
43.245.183.109	147.237.8.45	Indonesia	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.98	147.237.77.178	United States	e.matpash.idf.il	ET DROP Dshield Block Listed Source	1
43.245.183.109	147.237.8.24	Indonesia	e.lifestyle.idf.il	ET SCAN NMAP -sS window 2048	1
185.27.106.249	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.149.155	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.129.15	147.237.77.170	United Kingdom	maarachot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
109.66.141.88	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.69.234.47	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.94.91.220	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
43.245.183.109	147.237.8.45	Indonesia	e.eitan.idf.il	ET SCAN NMAP -sS window 4096	1
201.211.125.189	147.237.77.216	Venezuela	dover.idf.il	portscan: TCP Distributed Portscan	1
43.245.183.109	147.237.8.24	Indonesia	e.lifestyle.idf.il	ET SCAN NMAP -sS window 4096	1
194.56.215.218	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
43.245.183.109	147.237.8.24	Indonesia	e.lifestyle.idf.il	ET SCAN NMAP -f -sS	1
168.235.197.20	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
168.235.197.20	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	96
168.235.197.20	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	70
46.28.137.190	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
46.28.137.190	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	30
5.102.221.179	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
109.253.130.48	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
66.249.66.6	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
141.0.13.223	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	19
141.0.14.106	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	19
109.253.200.197	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.85.236	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
85.130.183.194	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
46.19.85.41	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
85.130.183.194	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	15
64.37.98.12	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
64.37.98.12	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
64.37.98.12	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
64.37.98.12	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
64.37.98.12	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
46.19.85.41	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
64.37.98.12	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
64.37.98.12	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
64.37.98.12	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
64.37.98.12	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
64.37.98.12	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
64.37.98.12	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
64.37.98.12	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
64.37.98.12	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
64.37.98.12	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
64.37.98.12	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
64.37.98.12	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
185.87.183.52	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
64.37.98.12	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
64.37.98.12	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
85.130.183.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
64.37.98.12	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
64.37.98.12	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
185.87.183.52	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	10
185.87.183.52	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	10
64.37.98.12	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
93.172.206.23	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
2.53.5.102	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
64.37.98.12	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
46.19.85.201	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
45.74.1.194	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
185.87.183.59	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	7
37.26.149.252	Israel	147.237.0.19	madim.atal.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.72	Israel	147.237.76.200	eitan.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	alert	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.111.41.50	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	22
37.26.149.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
46.120.38.133	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	9
198.27.100.198	Canada	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 198.27.100.198	Block	8
198.27.100.198	Canada	147.237.77.216	dover.idf.il	PHP Attempt	Block	8
84.229.86.113	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	6
176.13.227.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
2.53.132.242	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	5
79.181.8.173	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	4
109.253.130.48	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
109.253.200.197	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
2.53.5.102	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.121.210.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.125.58.60	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
84.229.86.113	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	2
176.13.9.153	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
89.139.185.139	Israel	147.237.76.42	refuah.idf.il	Distributed Parameter Type Violation on www.refua.atal.idf.il/1518-he/refuah.aspx parameter ct100\$ContentPlaceHolder1\$txtLastName	Block	2
5.29.31.30	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
77.138.196.195	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
37.142.211.152	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
207.232.21.105	Israel	147.237.72.156	aman.idf.il	Unauthorized Method HEAD for list.ips.gov.il/	Block	1
66.249.65.12	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/faq/faq.aspx	Block	1
109.253.241.174	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
85.65.170.118	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/resources/images/favicon/favicon.png	Block	1
46.19.86.130	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version _pk_id.20.8afc=c3a48bad8d5a45e0.1472997452.2.1473253980.1473253980.; _pk_ses.20.8afc=*	Block	1
45.56.108.106	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized Method OPTIONS for /	Block	1
216.1.128.60	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
79.179.28.253	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
5.102.221.179	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/homepage/homepage.aspx	Block	1
185.120.125.71	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
46.121.253.55	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$tfasimSignAll in www.aka.idf.il/main/sachar/payslips.aspx	None	1
109.64.39.26	Israel	147.237.76.42	refuah.idf.il	Distributed Parameter Type Violation on www.refua.atal.idf.il/1518-he/refuah.aspx parameter ct100\$ContentPlaceHolder1\$txtLastName	Block	1
46.19.85.148	Israel	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
77.138.206.194	France	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.142.211.152	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1
212.76.99.52	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/sachar/faq.aspx	Block	1
157.55.39.49	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.65.51	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.51	Block	1
85.65.186.161	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
46.19.86.214	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
46.19.85.118	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
37.26.146.157	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
68.180.230.47	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-he/dover.aspx	Block	1
46.252.244.150	Russian Federation	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
109.67.33.235	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
46.19.86.130	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
77.139.65.61	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/cityofficers/	Block	1
45.56.108.106	United States	147.237.76.39	mobile.meitav.idf.il	Distributed Unauthorized HTTP Method	Block	1
212.76.99.52	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$ct109 in aka.idf.il/main/sachar/payslips.aspx	None	1