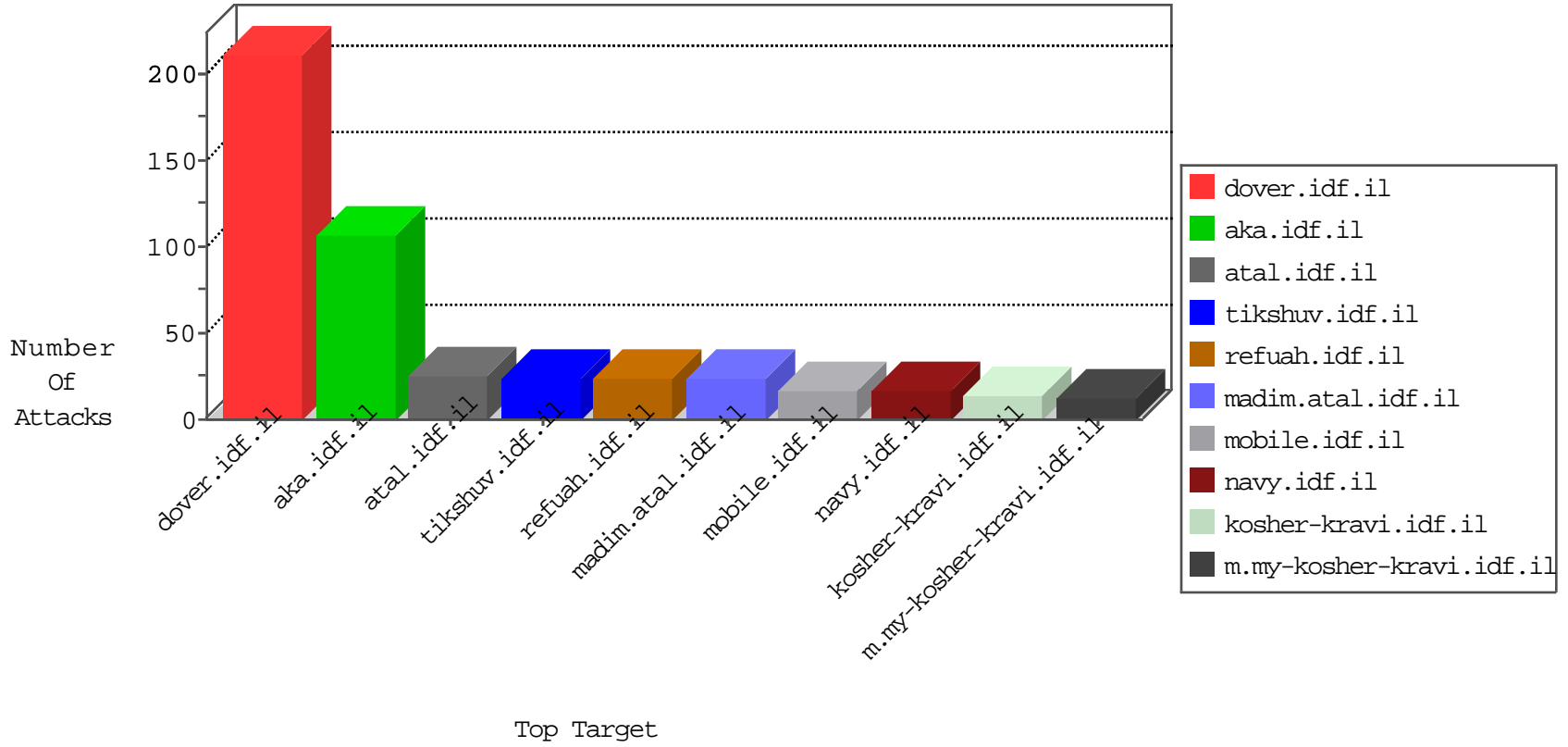


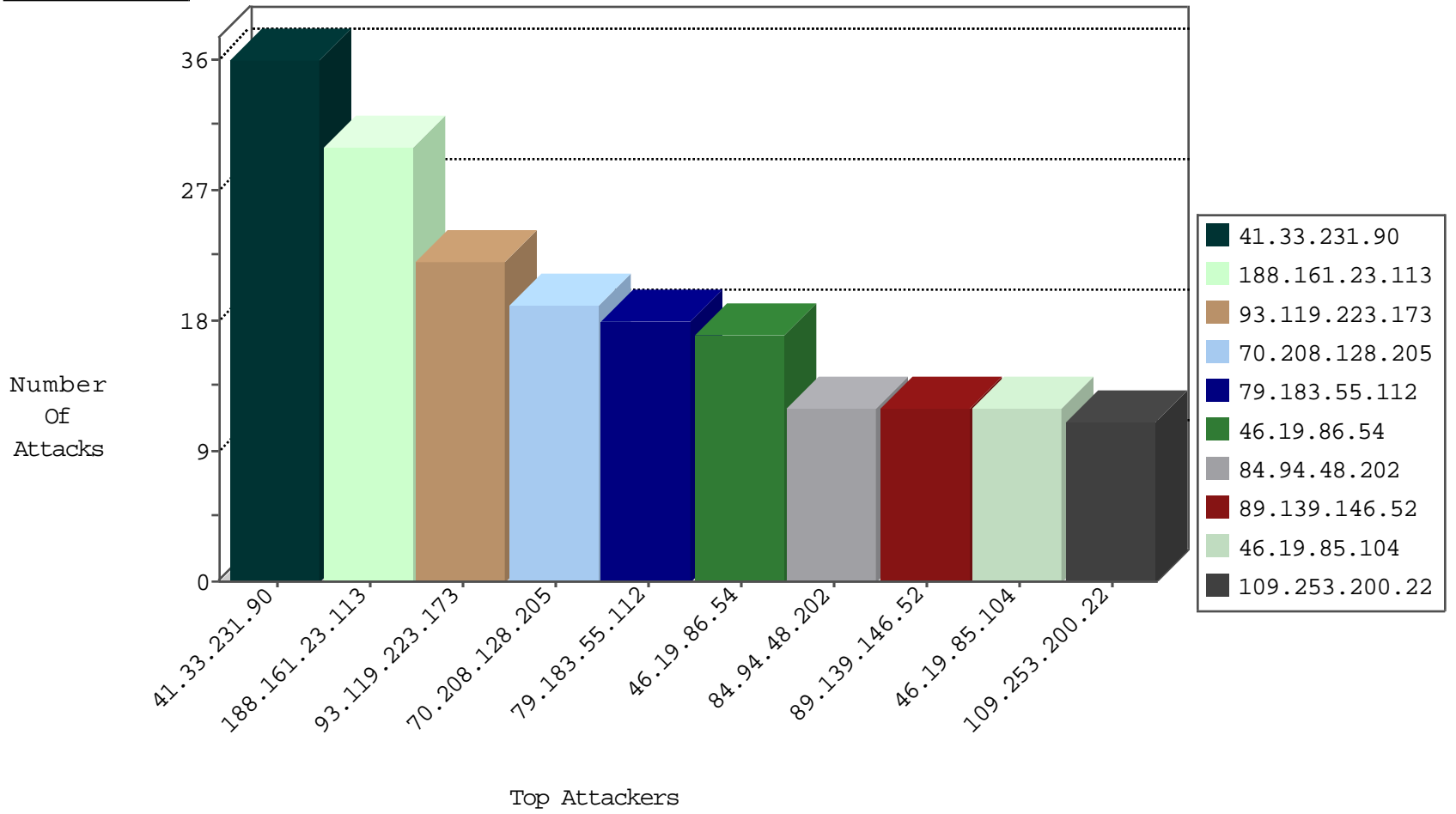
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
220.181.108.155	China	147.237.72.156	aran.idf.il	TCP handshake violation, first packet not syn	drop	2834
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	4
79.179.49.39	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
134.147.203.115	Germany	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	2
185.130.5.200		147.237.76.176	test.ncore.idf.i	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.94.48.202	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	12
77.127.221.29	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	5
162.210.196.130	United States	147.237.77.216	doover.idf.il	C1000106: HTTP: majestic bot	Block	2
199.58.86.206	United States	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	2
5.9.85.4	Germany	147.237.77.216	doover.idf.il	C1000106: HTTP: majestic bot	Block	2
199.58.86.206	United States	147.237.77.216	doover.idf.il	C1000106: HTTP: majestic bot	Block	2
111.202.102.69	China	147.237.77.216	doover.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	1
80.246.133.222	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	1
187.38.150.123	Brazil	147.237.77.176	matpash.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	doover.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	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	4
218.246.0.97	147.237.0.200	China	m4u.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.66.125	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
175.146.162.167	147.237.76.30	China	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.255.65.207	147.237.0.15		kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
98.119.105.221	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
59.45.79.117	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.74	147.237.77.226	United States	www.chamatz.aka.idf.il	ET DROP Dshield Block Listed Source	1
185.130.5.200	147.237.8.27		e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
104.255.65.207	147.237.0.34		tikshuv.idf.il	ET SCAN Potential SSH Scan	1
98.119.105.221	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
95.211.184.107	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.176	China	test.ncoore.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
89.139.146.52	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
93.119.223.173	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
93.119.223.173	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
70.208.128.205	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
109.253.210.178	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
46.19.86.54	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	9
79.183.55.112	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
104.148.71.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
104.148.71.83	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
46.19.86.54	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
85.130.254.145	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
188.161.23.113	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
188.161.23.113	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	7
188.161.23.113	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
152.248.150.72	Brazil	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
188.161.23.113	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
104.148.71.90	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.104	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
77.125.143.85	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.104	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.200.22	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.20.33	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.148.191	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
188.120.154.102	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.253.200.22	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.172	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
212.14.140.2	Italy	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
66.249.66.95	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
212.14.140.2	Italy	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
94.230.86.123	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
37.46.39.51	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
85.130.254.145	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.19.86.26	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.54.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
70.208.128.205	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
188.161.23.113	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
79.183.60.125	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.229.214	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
185.3.147.232	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
193.238.188.56	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.231.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.133.0	Israel	147.237.77.170	maarachot.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
176.13.7.73	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-19-2016-21:04:09 to 02-19-2016-22:04:09

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.181.63.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	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
79.183.55.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
5.102.215.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.8.121.198	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$txtEmail in www.idf.il/1038-en/dover.aspx	Block	3
149.78.63.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.182	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/	Block	2
110.141.139.71	Australia	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
157.55.39.164	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
89.139.146.52	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/894-he/atal.aspx	Block	1
68.180.231.40	United States	147.237.77.74	law.idf.il	Suspicious Response Code	Block	1
110.141.139.71	Australia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
82.81.40.156	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https://www.aman.idf.il/	Block	1
66.249.65.40	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/894-he	Block	1
188.138.1.218	Germany	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
95.160.59.28	Poland	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/1593-he/refuah.aspx+help+get+things+started+by+asking+a+question+	Block	1
79.179.170.184	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestion\$26 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
128.232.110.28	United Kingdom	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	1
84.94.155.121	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
213.57.38.75	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestion\$14 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
109.253.210.178	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 109.253.210.178	Block	1
79.179.170.184	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestion\$39 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
130.193.218.90	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
84.200.45.165	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
213.57.38.75	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestion\$7 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
109.253.210.178	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/960.css	Block	1
79.180.250.122	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
85.64.37.209	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/galeryfs.html	Block	1