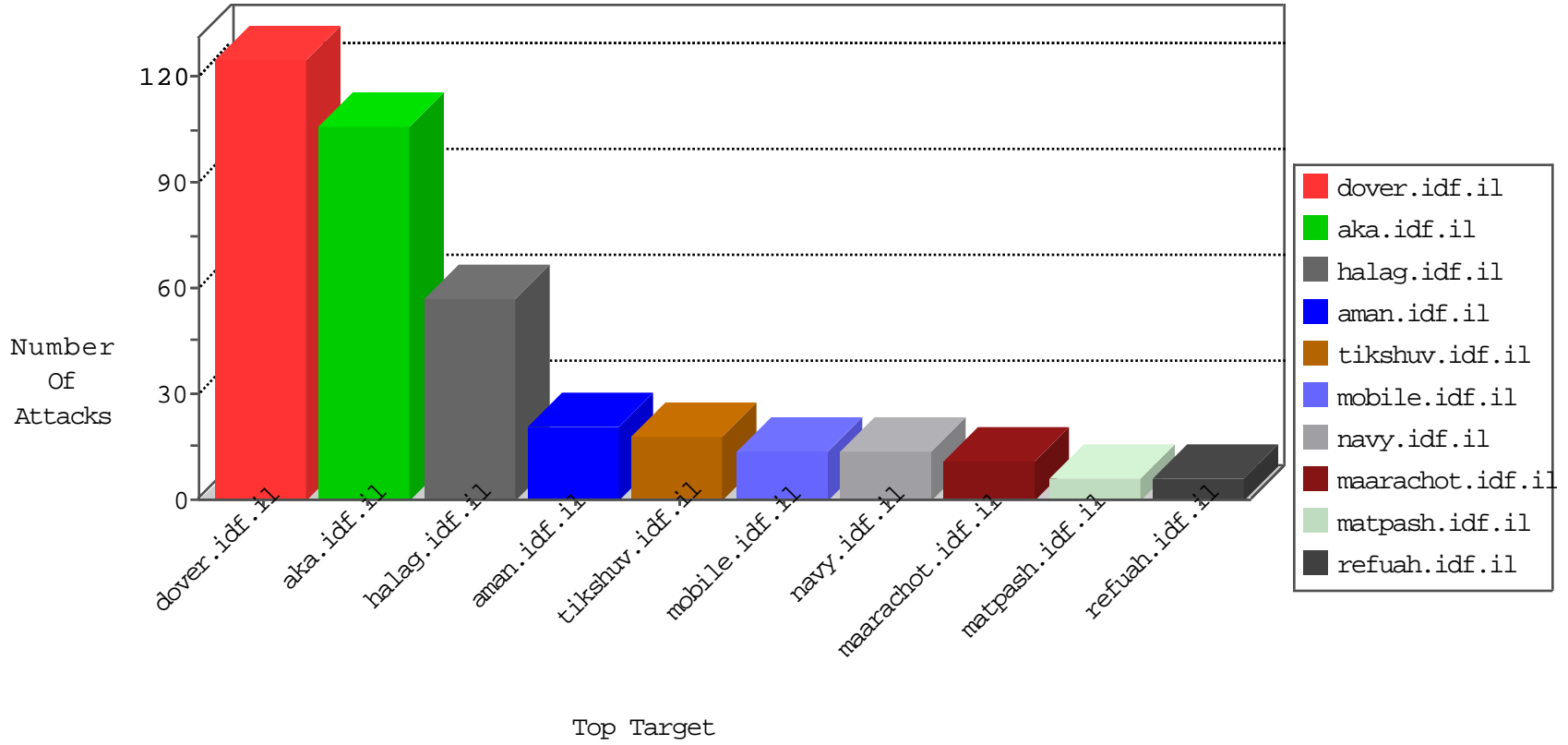


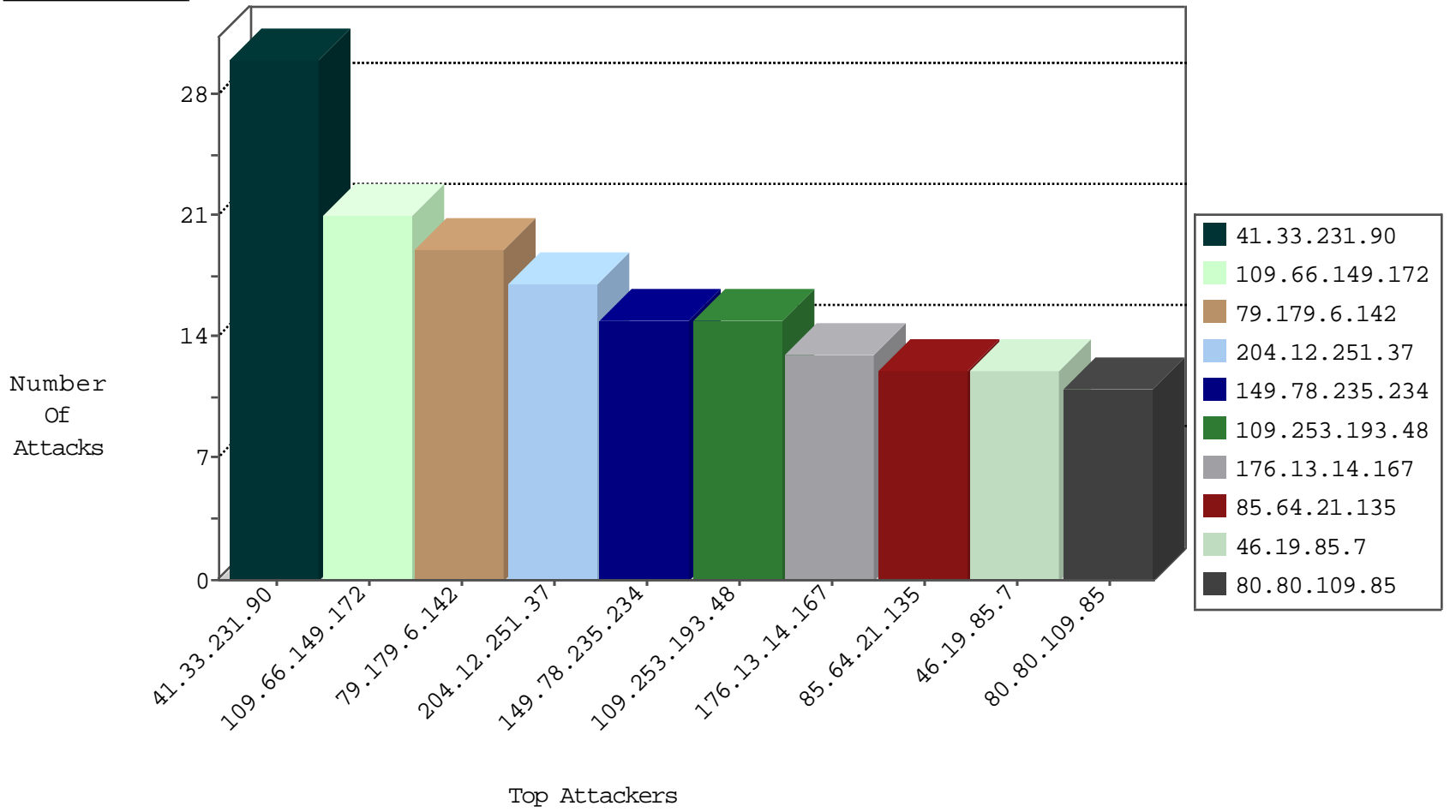
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
198.23.190.39	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ntp_All_Net	drop	1
163.44.112.118	Japan	147.237.72.217	e.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.179		147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	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
85.64.21.135	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
61.135.189.103	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	2
151.80.31.154	Italy	147.237.76.42	refuah.idf.il	C1000146: HTTP: AhrefBot crawler	Block	2
51.255.65.51	United Kingdom	147.237.77.170	maarachot.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
151.80.31.117	Italy	147.237.77.170	maarachot.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.73	United Kingdom	147.237.77.170	maarachot.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
151.80.31.151	Italy	147.237.76.42	refuah.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.97	United Kingdom	147.237.77.170	maarachot.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
151.80.31.152	Italy	147.237.76.42	refuah.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.39	United Kingdom	147.237.77.170	maarachot.idf.il	C1000146: HTTP: AhrefBot crawler	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
80.80.109.85	147.237.0.200	Russian Federation	m4u.idf.il	ET SCAN Potential SSH Scan	2
80.80.109.85	147.237.77.178	Russian Federation	e.matpash.idf.il	ET SCAN Potential SSH Scan	2
180.150.177.188	147.237.72.156	China	aman.idf.il	ET SCAN NMAP -sS window 1024	1
80.80.109.85	147.237.0.19	Russian Federation	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
104.255.65.207	147.237.77.170		maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
40.113.118.99	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
104.44.133.108	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 2048	1
95.67.249.243	147.237.76.176	Russian Federation	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
222.223.153.136	147.237.76.31	China	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.201.236.113	147.237.0.200	Ukraine	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
220.178.78.138	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN NMAP -sS window 2048	1
80.80.109.85	147.237.77.176	Russian Federation	matpash.idf.il	ET SCAN Potential SSH Scan	1
218.57.11.7	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
80.80.109.85	147.237.77.121	Russian Federation	e.navy.idf.il	ET SCAN Potential SSH Scan	1
218.57.11.7	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
80.80.109.85	147.237.76.196	Russian Federation	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
191.251.103.120	147.237.76.30	Brazil	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
117.21.248.87	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
40.113.118.99	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 2048	1
104.44.133.108	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 4096	1
40.113.118.99	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -f -sS	1
104.44.133.108	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -f -sS	1
95.67.249.243	147.237.8.14	Russian Federation	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
220.178.78.138	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN NMAP -sS window 3072	1
220.178.78.138	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN NMAP -f -sS	1
80.80.109.85	147.237.77.170	Russian Federation	maarachot.idf.il	ET SCAN Potential SSH Scan	1
218.57.11.7	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
80.80.109.85	147.237.76.202	Russian Federation	e.halag.idf.il	ET SCAN Potential SSH Scan	1
80.80.109.85	147.237.76.147	Russian Federation	chinuch.aka.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	30
109.66.149.172	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
79.179.6.142	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
204.12.251.37	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
109.253.193.48	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
176.13.14.167	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
2.55.66.40	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.71.51.157	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.7	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.7	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
109.186.184.92	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.86.112	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
88.198.44.2	Germany	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
79.180.149.49	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.7.172	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.211.189	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.239	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.50.192	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.90.146	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
79.181.142.85	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.56	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.19.132	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
88.198.44.2	Germany	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
5.102.242.170	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.180.52.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.99	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
88.198.44.2	Germany	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
2.52.168.177	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	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
46.19.85.88	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
87.69.192.154	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.102.242.115	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.117.1.49	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
185.3.147.140	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.129	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
95.67.249.243	Russian Federation	147.237.8.46	e.chinuch.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.82.200.91		147.237.0.34	tikshuv.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
141.212.122.195	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
31.154.31.187	Israel	147.237.77.170	maarachot.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
141.212.122.132	United States	147.237.0.35	akaws.idf.il	drop		drop	1
2.54.1.143	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.121.121.167	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
195.228.75.121	Hungary	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.228	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
95.67.249.243	Russian Federation	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.78.235.234	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 149.78.235.234	Block	14
80.246.130.49	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	11
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	8
65.55.210.182	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	8
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
66.249.81.212	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
62.219.137.5	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 62.219.137.5	Block	5
62.219.137.5	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	3
109.67.191.38	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
93.170.253.196	Czech Republic	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 93.170.253.196	Block	3
66.249.81.218	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
157.55.39.105	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.116.33.91	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
37.26.149.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.66.149.172	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
46.19.86.59	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
31.154.31.187	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/71929-he/ctl00_ucsidebar_rptcategories_ctl01_innerlevelcontainer	Block	1
68.180.229.239	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/	Block	1
176.13.14.167	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
93.170.253.196	Czech Republic	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/404.aspx'	Block	1
148.251.21.227	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/en	Block	1
77.127.188.73	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/2/1712.pdf	Block	1
46.121.75.19	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 46.121.75.19 (Open Mode)	None	1
185.82.200.91		147.237.0.34	tikshuv.idf.il	Unauthorized Method HEAD for 147.237.0.34/	Block	1
40.77.167.92	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/901-10307-he/cogat.aspx	Block	1
79.177.178.80	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
46.121.75.19	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
2.54.47.207	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestion\$79 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
204.12.251.37	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/eitan/shared/usercontrols/headerupper/	Block	1
95.86.84.70	Israel	147.237.72.166	aka.idf.il	Unknown Parameter sa in www.aka.idf.il/main/sachar/klali.aspx	None	1
46.19.85.217	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
149.78.235.234	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https://www.aman.idf.il/modiin/general.aspx	Block	1
79.179.6.142	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
24.13.241.54	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
208.115.111.68	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/8/638.pdf	Block	1