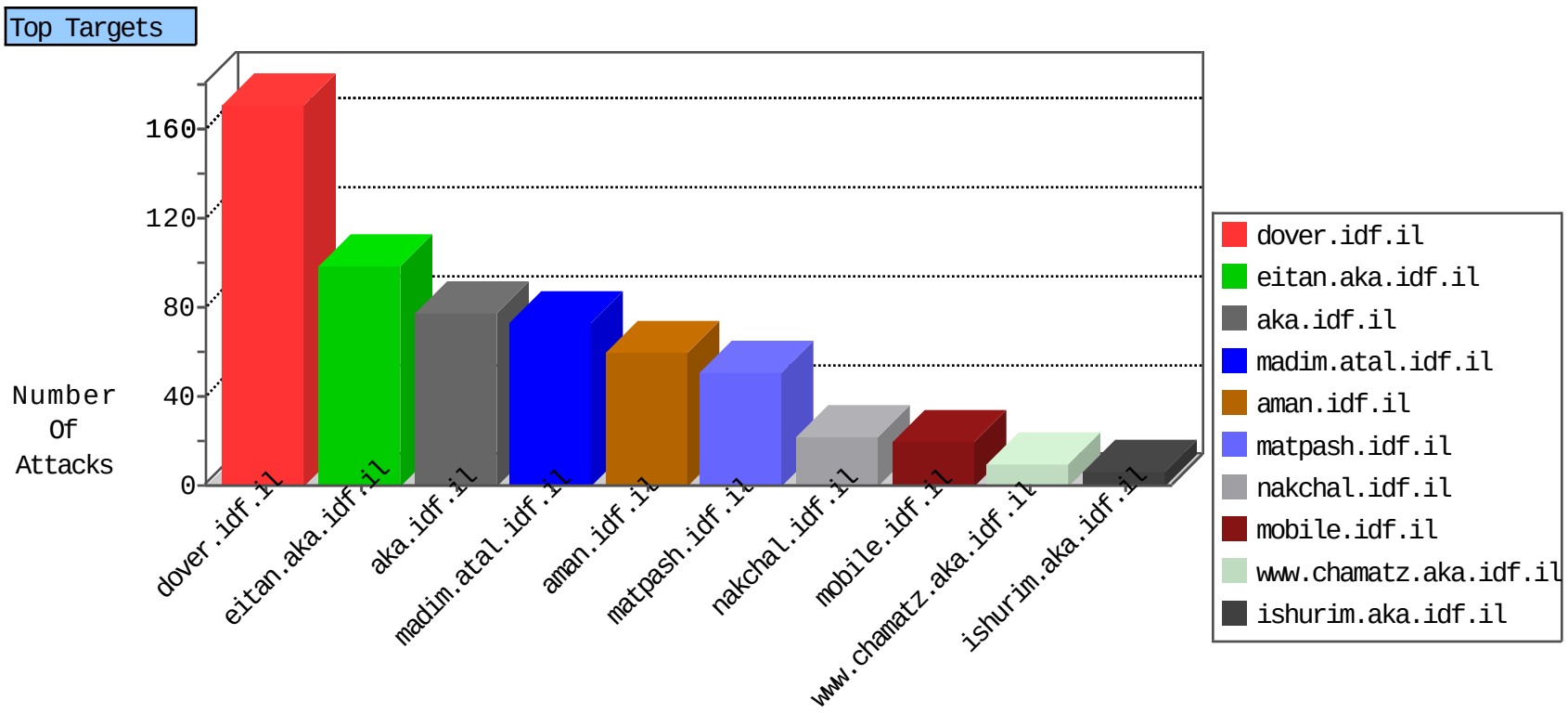
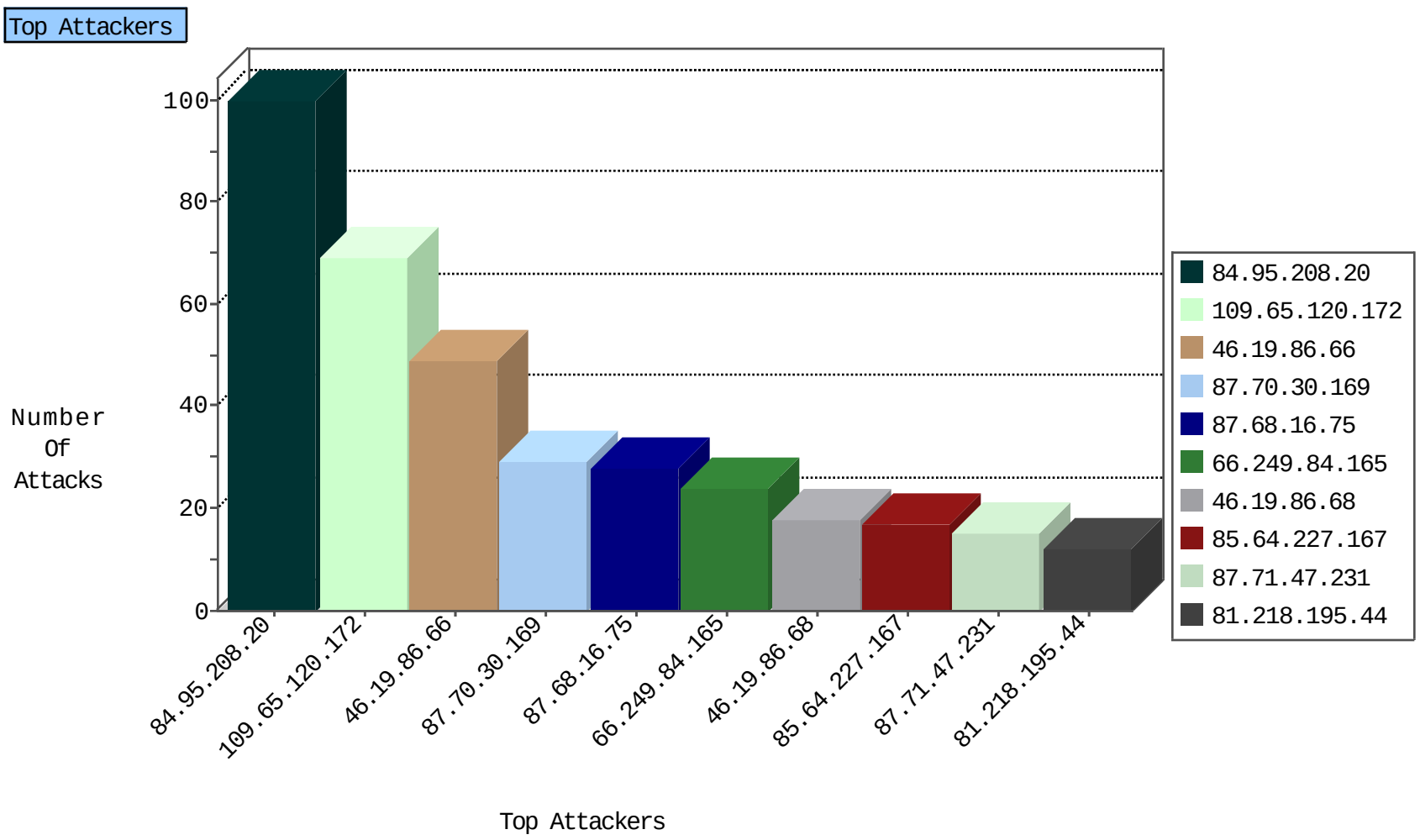
09-17-2016-10:04:02 to 09-17-2016-11:04:02

IDF Under Attack
Daily Report





09-17-2016-10:04:02 to 09-17-2016-11:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
208.94.63.194	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
139.78.141.243	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
31.168.240.21	Israel	147.237.72.166	aka.idf.il	Black List	drop	3
198.82.160.221	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	2
216.48.80.12	Canada	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	2
200.19.159.34	Brazil	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	2
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
221.1.118.195	China	147.237.77.61	e.cogat.idf.il	Invalid TCP Flags	drop	1
123.59.59.52	China	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	forward	1
221.1.118.195	China	147.237.77.235	sviva.idf.il	Invalid TCP Flags	drop	1
221.1.118.195	China	147.237.77.121	e.navy.idf.il	Invalid TCP Flags	drop	1
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.32.84.160	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
141.22.213.34	Germany	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
221.1.118.195	China	147.237.77.205	prisha.idf.il	Invalid TCP Flags	drop	1
129.97.74.14	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
143.225.229.236	Italy	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
221.1.118.195	China	147.237.77.233	atal.idf.il	Invalid TCP Flags	drop	1
130.194.252.8	Australia	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-17-2016-10:04:02 to 09-17-2016-11:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
144.76.8.132	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	3
87.68.16.75	Israel	147.237.72.156	aman.idf.il	3886: HTTP: Cross Site Scripting in POST Request	Block	2

09-17-2016-10:04:02 to 09-17-2016-11:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
87.68.16.75	147.237.72.156	Israel	aman.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	8
87.68.16.75	147.237.72.156	Israel	aman.idf.il	SERVER-WEBAPP DELETE attempt	2
87.68.16.75	147.237.72.156	Israel	aman.idf.il	GPL WEB_SERVER /etc/passwd	2
218.24.171.223	147.237.76.31	China	nakchal.idf.il	GPL SCAN nmap TCP	2
59.46.193.114	147.237.76.31	China	nakchal.idf.il	GPL SCAN nmap TCP	2
185.110.132.201	147.237.8.28	Ukraine	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
5.255.90.133	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
185.110.132.201	147.237.0.19	Ukraine	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
133.208.21.66	147.237.77.234	Japan	halag.idf.il	ET SCAN NMAP -sS window 1024	1
203.235.199.167	147.237.0.35	Korea, Republic of	akaws.idf.il	ET SCAN Potential SSH Scan	1
202.155.58.28	147.237.77.121	Indonesia	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.74	147.237.76.177	United States	ncore.idf.il	ET DROP Dshield Block Listed Source	1
85.65.176.195	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.201	147.237.77.170	Ukraine	maarachot.idf.il	ET SCAN Potential SSH Scan	1
63.225.115.84	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
185.110.132.201	147.237.76.147	Ukraine	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
61.178.42.242	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
185.110.132.201	147.237.76.34	Ukraine	yohalan.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
185.110.132.201	147.237.0.33	Ukraine	idf.il	ET SCAN Potential SSH Scan	1
5.255.90.133	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
185.110.132.201	147.237.0.16	Ukraine	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
133.208.21.66	147.237.8.14	Japan	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
203.235.199.167	147.237.0.17	Korea, Republic of	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
202.155.58.28	147.237.8.46	Indonesia	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
85.93.5.70	147.237.72.167	United Arab Emirates	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
185.110.132.201	147.237.77.226	Ukraine	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
66.249.66.238	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
185.110.132.201	147.237.76.176	Ukraine	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
61.178.42.242	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
185.110.132.201	147.237.76.44	Ukraine	e.refuah.idf.il	ET SCAN Potential SSH Scan	1

09-17-2016-10:04:02 to 09-17-2016-11:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
46.19.86.68	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.86.66	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	16
46.19.86.66	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
87.71.47.231	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
81.218.195.44	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	12
185.32.179.138	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.66	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
87.70.30.169	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
100.92.217.95		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
85.164.132.227	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	10
87.70.30.169	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
87.70.30.169	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	9
78.73.129.54	Sweden	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
66.249.84.167	United States	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	6
66.249.84.165	United States	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
66.249.84.165	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
66.249.84.165	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
66.249.84.165	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.66	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
141.226.218.56	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.176.10.196	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.84.165	United States	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	4
66.249.84.166	United States	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	4
85.64.227.167	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
199.30.24.111	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
109.253.193.2	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
176.13.22.165	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.29.116.151	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
84.95.208.20	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.253.198.204	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
195.154.230.187	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3
2.53.153.247	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
5.29.81.196	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.105	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
5.102.242.241	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
87.68.59.57	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.198.204	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
49.34.30.56	India	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
5.102.195.141	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.130.227.133	United Kingdom	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
213.57.189.33	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
156.204.167.74	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
46.19.85.33	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
85.64.227.167	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

09-17-2016-10:04:02 to 09-17-2016-11:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	79
109.65.120.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	69
85.64.227.167	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/homepage/homepage.aspx	Block	11
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	7
87.68.16.75	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 87.68.16.75	Block	6
87.69.119.245	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 87.69.119.245	Block	4
5.102.253.235	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	4
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
87.68.16.75	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	2
77.139.202.204	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/kapatz/	Block	2
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
79.181.105.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.64.9	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
87.68.16.75	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	1
79.181.216.85	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
89.138.107.11	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.76.31	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/apple-app-site-association	Block	1
37.26.147.160	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
87.68.16.75	Israel	147.237.72.156	aman.idf.il	Multiple Illegal HTTP Version from 87.68.16.75	Block	1
77.138.7.168	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1
204.79.180.179	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/default.aspx	Block	1
66.249.64.43	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/1/70011.doc	Block	1
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/templates/news/piwik.php	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
89.139.218.201	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.84.167	Israel	147.237.77.216	dover.idf.il	Distributed URL is Above Root Directory	Block	1
46.19.85.18	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
207.46.13.30	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
87.68.16.75	Israel	147.237.72.156	aman.idf.il	Unknown HTTP Request Method TEST in URL www.aman.idf.il/	Block	1
66.249.64.134	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/apple-app-site-association	Block	1
84.111.180.212	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl57 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
68.180.228.58	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/1093-7963-he/מאי-ר שחמו|.aspx	Block	1
46.19.86.94	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
87.68.16.75	Israel	147.237.72.156	aman.idf.il	Multiple Unknown HTTP Request Method from 87.68.16.75	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation aspxerrorpath in www.idf.il/error.htm	Block	1
79.179.141.178	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/watch	Block	1
212.179.229.29	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.64.163	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/.well-known/apple-app-site-association	Block	1
84.95.208.20	Israel	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
68.180.229.223	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1397-en/dover.aspx	Block	1
114.98.244.254	China	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 114.98.244.254	Block	1
54.161.51.139	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
87.68.16.75	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 87.68.16.75 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
87.69.119.245	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	1
66.249.76.31	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.76.31	Block	1
31.154.81.73	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1
87.68.16.75	Israel	147.237.72.156	aman.idf.il	Illegal HTTP Version HTTP/9.8	Block	1
77.127.57.60	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	1

09-17-2016-10:04:02 to 09-17-2016-11:04:02