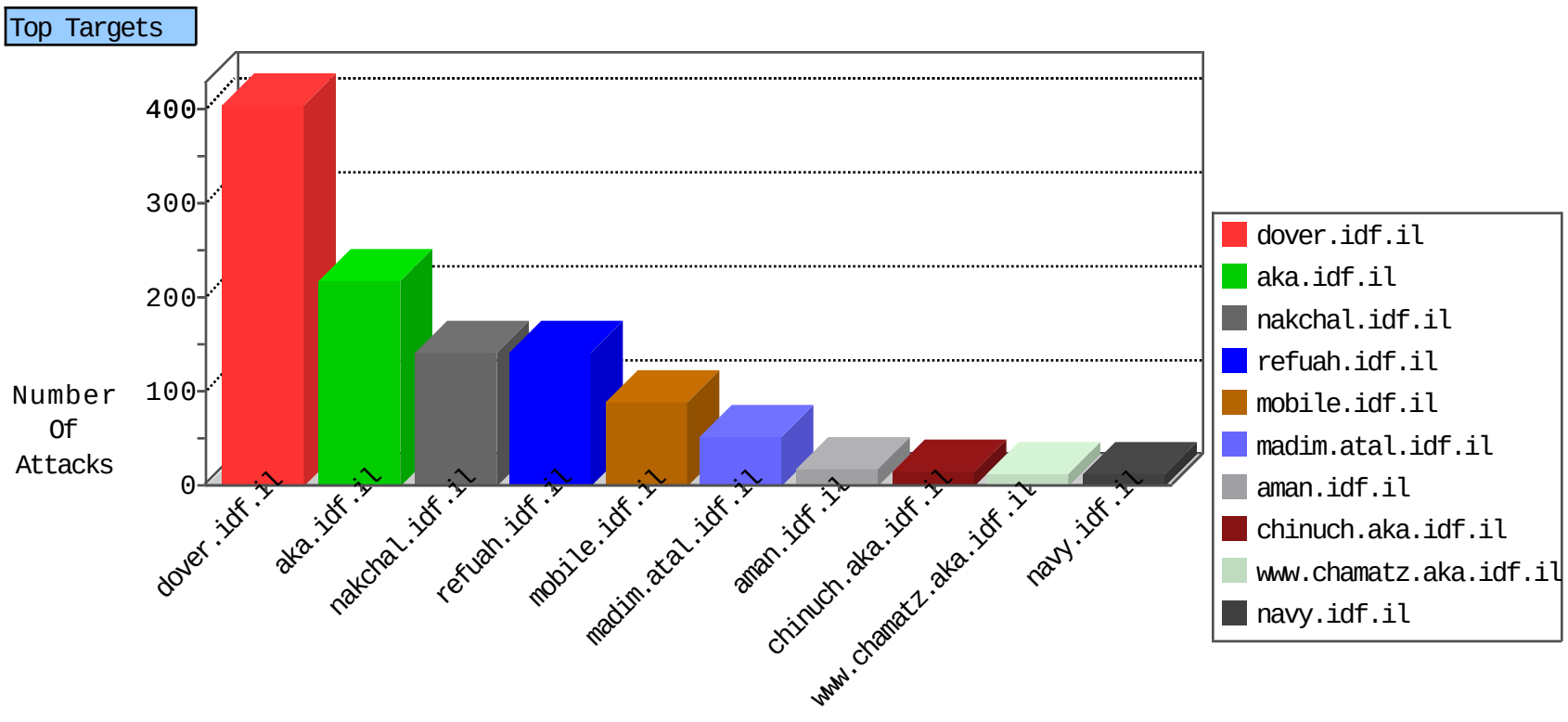
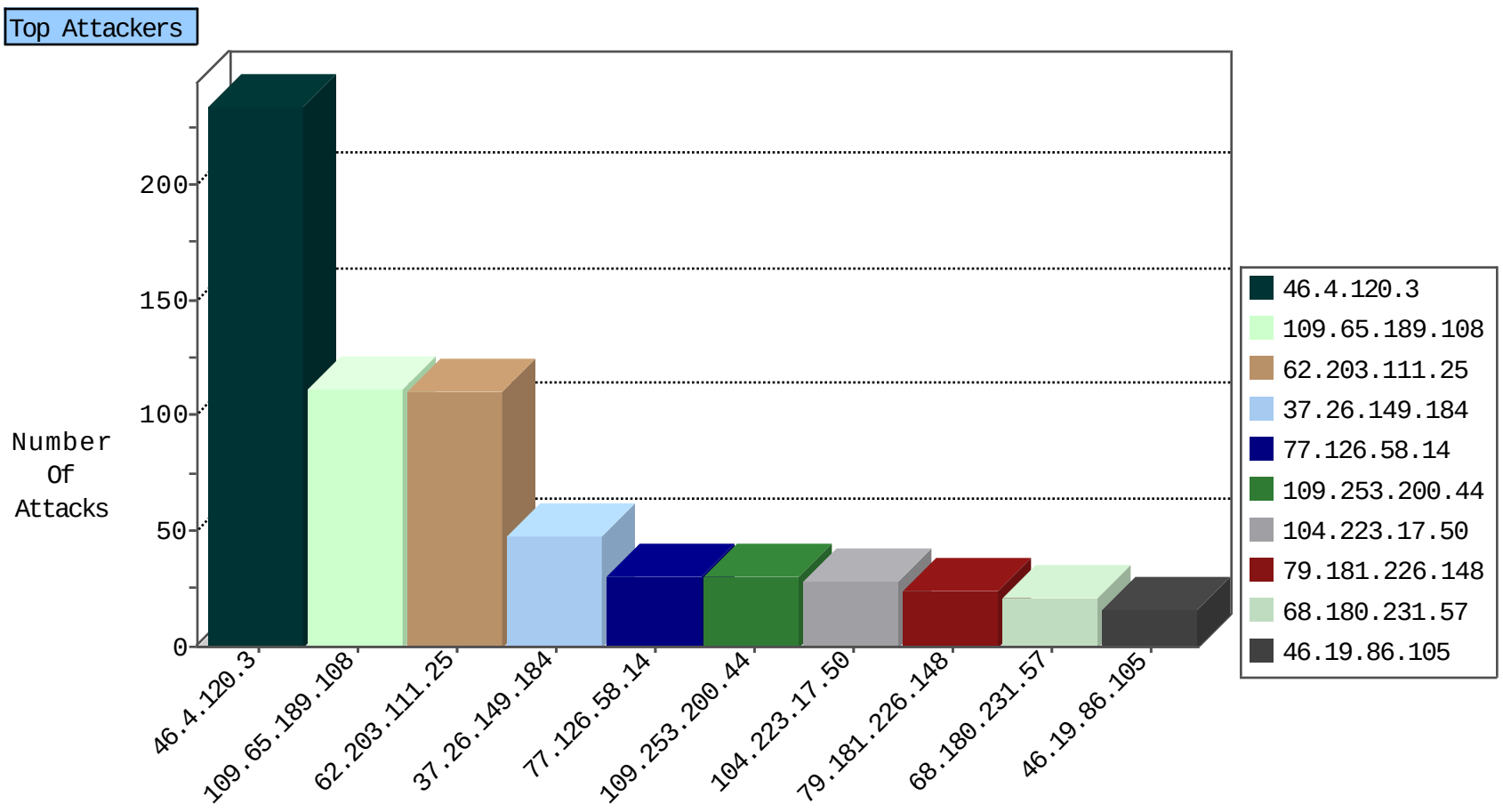
09-28-2016-21:04:00 to 09-28-2016-22:04:00

IDF Under Attack
Daily Report





09-28-2016-21:04:00 to 09-28-2016-22:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
68.180.231.57	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1224002
2.53.41.180	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4308
5.102.195.141	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1368
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
185.94.111.1	Russian Federation	147.237.76.201	e.atal.idf.il	Black List	drop	1
5.29.96.42	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
185.94.111.1	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1

09-28-2016-21:04:00 to 09-28-2016-22:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.4.120.3	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	199
46.4.120.3	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	18
46.4.120.3	Germany	147.237.76.31	nakchal.idf.il	C1000074: HTTP: majestic bot	Permit	12
5.189.190.238	Germany	147.237.72.167	ishurim.aka.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
46.4.120.3	Germany	147.237.76.147	chinuch.aka.idf.il	C1000074: HTTP: majestic bot	Permit	3
46.4.120.3	Germany	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	2
104.223.17.50	United States	147.237.77.216	dover.idf.il	19791: HTTP: WordPress N-Media PHP File Upload	Block	2
104.223.17.50	United States	147.237.77.216	dover.idf.il	22611: HTTP: WordPress LoginWall Fake Plugin Usage	Block	1
151.80.31.175	France	147.237.77.170	maarachot.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
5.189.190.238	Germany	147.237.72.167	ishurim.aka.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1

09-28-2016-21:04:00 to 09-28-2016-22:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
128.30.52.96	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	3
79.177.37.76	147.237.77.233	Israel	atal.idf.il	ET SCAN NMAP -sA (2)	3
86.60.212.121	147.237.76.42	Finland	refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
46.161.40.17	147.237.77.74	Russian Federation	law.idf.il	ET SCAN NMAP -sS window 1024	1
154.16.199.242	147.237.76.44	United States	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
2.53.181.123	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
151.11.201.3	147.237.76.31	Italy	nakchal.idf.il	ET SCAN NMAP -sS window 3072	1
151.11.201.3	147.237.76.31	Italy	nakchal.idf.il	ET SCAN NMAP -f -sS	1
213.151.32.163	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
117.21.248.87	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.37	147.237.76.197	Lithuania	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
117.21.248.87	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.37	147.237.76.38	Lithuania	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
94.60.121.232	147.237.76.86	Portugal	navy.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
163.172.238.45	147.237.77.227	United Kingdom	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
154.16.199.242	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
5.189.190.238	147.237.72.167	Germany	ishurim.aka.idf.il	ET WEB_SERVER Muieblackcat scanner	1
154.16.199.242	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential SSH Scan	1
151.11.201.3	147.237.76.31	Italy	nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
128.30.52.134	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	1
128.30.52.73	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	1
212.116.72.226	147.237.8.46	Sweden	e.chinuch.idf.il	ET SCAN NMAP -sS window 4096	1
117.21.248.87	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.37	147.237.76.147	Lithuania	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
113.190.120.233	147.237.0.16	Vietnam	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
185.130.5.37	147.237.76.30	Lithuania	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
163.172.129.15	147.237.0.33	United Kingdom	idf.il	ET SCAN NMAP -sS window 1024	1

09-28-2016-21:04:00 to 09-28-2016-22:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.65.189.108	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	111
109.253.200.44	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
77.126.58.14	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
62.203.111.25	Switzerland	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	26
62.203.111.25	Switzerland	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	25
79.181.226.148	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	24
62.203.111.25	Switzerland	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	21
62.203.111.25	Switzerland	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	21
62.203.111.25	Switzerland	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
86.95.185.112	Netherlands	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
79.179.185.155	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
2.55.42.18	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
141.226.162.96	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
79.177.63.230	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
37.26.149.204	Israel	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
46.19.85.148	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.85.42	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.105	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	7
46.120.199.77	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
217.132.102.179	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
79.182.51.23	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.41	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.253.219.70	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.41	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
100.92.231.131		147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	6
2.53.189.209	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.69.123.12	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
46.19.85.42	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.53.45.68	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.86.105	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.87	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.120.199.77	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
185.27.106.108	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.85.54	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.253.194.112	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.86.105	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.86.87	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
104.223.17.50	United States	147.237.77.216	dover.idf.il	Command Injection	command injection detected in request: 'echo"'	monitor	4
46.19.85.87	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
84.108.170.236	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.87	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
78.102.111.94	Czech Republic	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.148	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.121.94.210	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
176.13.229.255	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.19.85.9	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.176.54.156	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.178.38	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
185.3.147.72	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

09-28-2016-21:04:00 to 09-28-2016-22:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.149.184	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	46
104.223.17.50	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 104.223.17.50	Block	9
104.223.17.50	United States	147.237.77.216	dover.idf.il	PHP Attempt	Block	9
77.139.223.214	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	5
176.13.239.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
37.142.241.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
109.65.138.229	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.65.138.229	Block	2
79.178.129.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.229.73.160	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	2
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.177	Block	2
77.138.128.113	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
66.249.66.210	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1362-9916-he/dover.aspx	Block	1
141.226.162.96	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
104.223.17.50	United States	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
79.182.52.201	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
180.97.106.162	China	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 180.163.113.82/check_proxy	Block	1
77.125.51.155	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
66.102.8.213	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
2.53.187.147	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/null	Block	1
85.64.16.101	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/promotioncube/	Block	1
66.249.75.4	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9738-he/refuah.aspx	Block	1
104.223.17.50	United States	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 104.223.17.50	Block	1
46.19.86.165	Israel	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	1
84.109.70.218	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
204.79.180.210	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/templates/home.asp	Block	1
77.125.67.102	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
109.65.189.108	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
66.102.9.2	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/sitemap.aspx	Block	1
5.102.242.91	Israel	147.237.72.166	aka.idf.il	Unknown Parameter x in www.aka.idf.il/main/sachar/payslips.aspx	None	1
85.250.190.7	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	1
66.249.75.8	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/3/2613.pdf	Block	1
180.76.15.136	China	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/994-9738-he/refuah.aspx	Block	1
46.19.86.165	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method 3t3kr5by in URL	Block	1
84.229.73.160	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 84.229.73.160	Block	1
207.46.13.176	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/...	Block	1
77.138.10.182	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	Block	1
109.253.197.209	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
66.249.64.157	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/m/	Block	1
89.139.101.74	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl25 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
79.180.207.2	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/6/71706.pdf	Block	1
180.97.106.37	China	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on 180.163.113.82/check_proxy	Block	1
46.116.125.9	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
213.151.35.212	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz	Block	1
77.138.89.242	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	Block	1
109.253.219.70	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
37.142.72.152	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
93.172.128.143	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.181.179.176	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
66.249.76.79	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/0/70000.jpg	Block	1

09-28-2016-21:04:00 to 09-28-2016-22:04:00