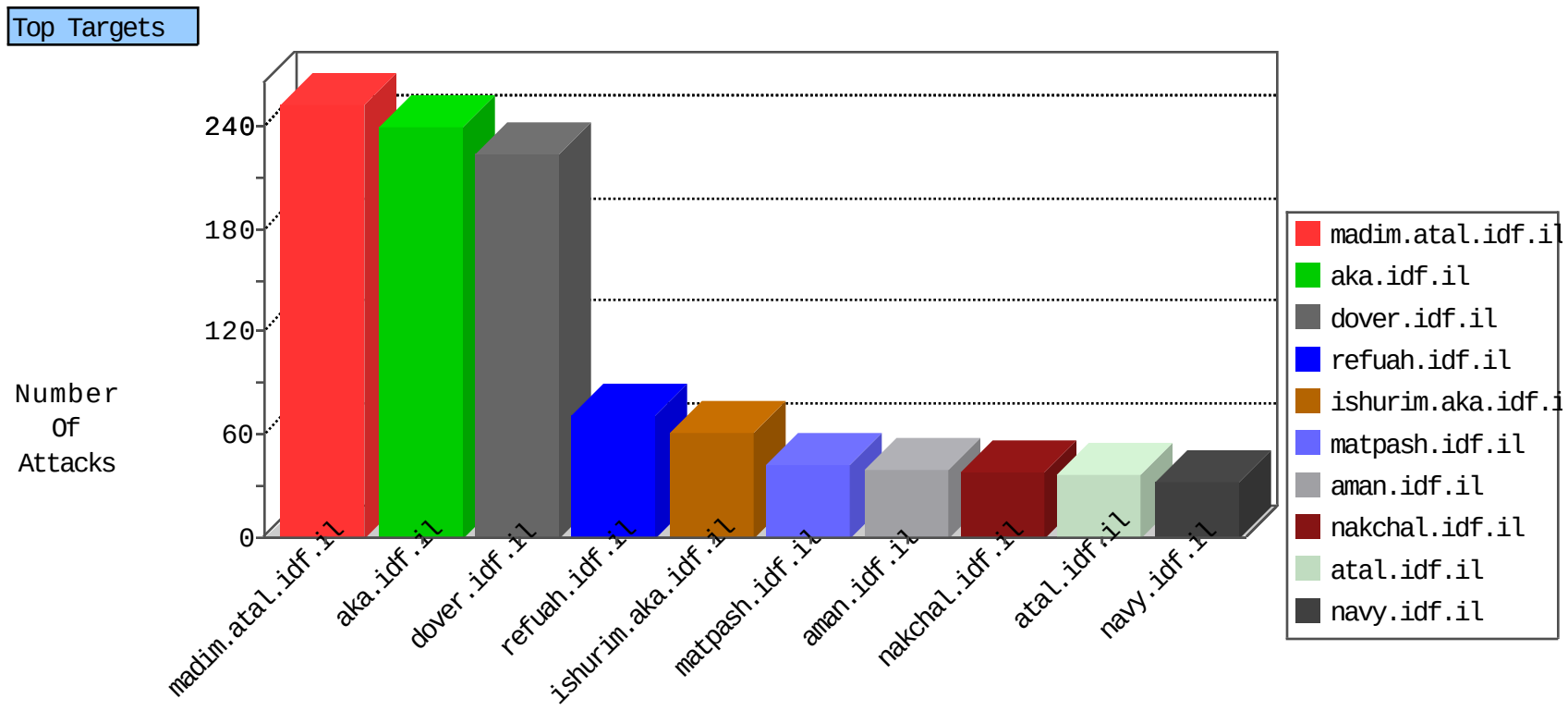
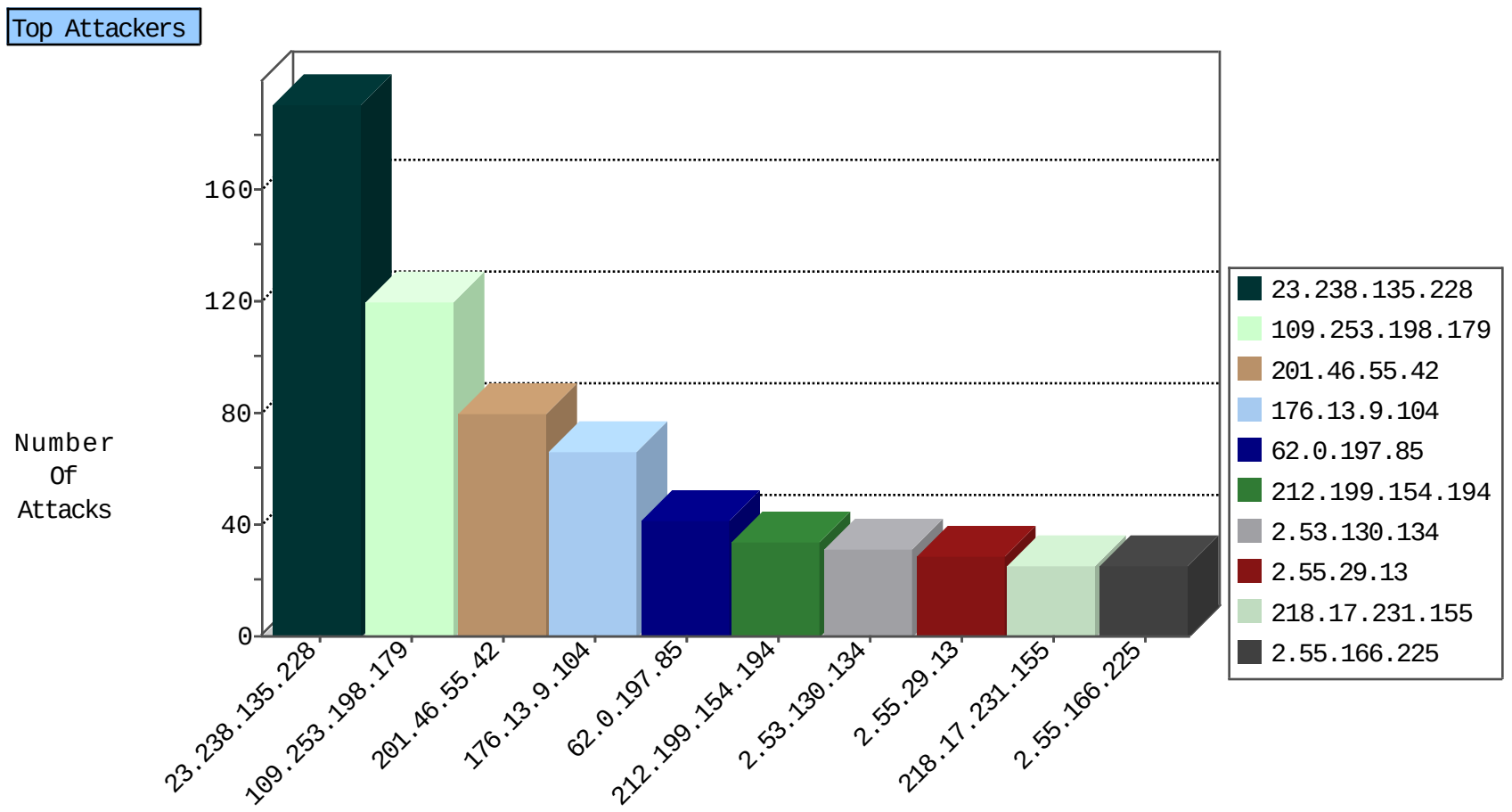
09-08-2016-10:04:08 to 09-08-2016-11:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-08-2016-10:04:08 to 09-08-2016-11:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.199.154.194	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	215
120.132.50.135	China	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	4
213.244.82.139	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
209.126.136.2	United States	147.237.76.201	e.atal.idf.il	Black List	drop	1

09-08-2016-10:04:08 to 09-08-2016-11:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.202.48.246	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
149.202.48.246	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
176.31.7.241	France	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1

09-08-2016-10:04:08 to 09-08-2016-11:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.19.85.207	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sA (2)	2
79.177.238.90	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
212.235.98.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
147.236.232.254	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
199.203.123.201	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.195	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
185.110.132.201	147.237.77.243	Ukraine	mobile.idf.il	ET SCAN Potential SSH Scan	1
81.218.116.129	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.201	147.237.76.202	Ukraine	e.halag.idf.il	ET SCAN Potential SSH Scan	1
79.183.103.196	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.201	147.237.76.38	Ukraine	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
72.252.157.188	147.237.76.197	Jamaica	e.himush.idf.il	ET SCAN NMAP -sS window 4096	1
185.110.132.201	147.237.0.35	Ukraine	akaws.idf.il	ET SCAN Potential SSH Scan	1
185.110.132.201	147.237.0.16	Ukraine	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
2.53.177.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.20.70	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.129.15	147.237.77.121	United Kingdom	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
212.199.9.181	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.23.92	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.201.225.149	147.237.0.15	Ukraine	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
89.187.217.67	147.237.77.216	Lebanon	dover.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.201	147.237.77.121	Ukraine	e.navy.idf.il	ET SCAN Potential SSH Scan	1
80.179.201.185	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.201	147.237.76.44	Ukraine	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
185.110.132.201	147.237.8.45	Ukraine	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
72.252.157.188	147.237.76.197	Jamaica	e.himush.idf.il	ET SCAN NMAP -sS window 3072	1
185.110.132.201	147.237.0.19	Ukraine	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.2	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
180.62.176.6	147.237.77.216	Japan	dover.idf.il	ET SCAN Suspicious User-Agent Containing Web Scan/er, Likely Web Scanner	1
2.53.11.8	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.169.150	147.237.0.17	United Kingdom	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1

09-08-2016-10:04:08 to 09-08-2016-11:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
62.0.197.85	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	41
2.55.29.13	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	29
23.238.135.228	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	20
23.238.135.228	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	20
23.238.135.228	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	20
23.238.135.228	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
23.238.135.228	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
212.199.154.194	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	19
23.238.135.228	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
23.238.135.228	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	18
23.238.135.228	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
100.92.190.168		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
2.53.130.134	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	15
84.95.201.5	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.55.166.225	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
2.53.130.134	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
201.46.55.42	Brazil	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
201.46.55.42	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
201.46.55.42	Brazil	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
82.166.125.198	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
37.26.148.219	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
37.26.148.219	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
172.58.73.171	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
2.53.130.134	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
46.19.86.36	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	8
201.46.55.42	Brazil	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
46.19.86.201	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
109.253.223.167	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
213.244.82.139	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
62.0.197.69	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.126	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.225	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	6
178.62.224.34	Netherlands	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	6
62.0.197.69	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.48	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.48	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.201	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.66.147.170	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
201.46.55.42	Brazil	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.85.206	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
66.102.9.1	United States	147.237.77.235	sviva.idf.il	drop	First packet isn't SYN	drop	5
2.53.146.20	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
37.26.147.164	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
37.26.147.164	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
2.55.166.225	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.81	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
82.166.125.198	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.249	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
109.253.223.167	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
201.46.55.42	Brazil	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4

09-08-2016-10:04:08 to 09-08-2016-11:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.198.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	120
176.13.9.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	65
37.26.147.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
2.55.145.73	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	20
218.17.231.155	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 218.17.231.155	Block	18
185.27.106.217	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on aka.idf.il/main/sachar/viewpayslip.aspx	Block	16
113.71.255.4	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 113.71.255.4	Block	15
37.26.147.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
218.17.231.155	China	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	6
113.71.255.4	China	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	6
194.114.146.227	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/	Block	5
85.64.219.23	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/general.aspx	Block	3
192.117.107.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
62.219.99.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
185.27.105.82	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	2
176.13.230.28	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
89.248.172.16	Netherlands	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	1
216.244.66.243	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/bamachane	Block	1
194.114.146.227	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 194.114.146.227	Block	1
2.53.186.52	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
84.109.124.18	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
46.19.85.62	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
207.46.13.93	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19645-he/dover	Block	1
66.249.66.251	Israel	147.237.72.166	aka.idf.il	Unknown Parameter utm_content in www.aka.idf.il/ishurim/main	None	1
176.13.9.104	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in madim.atal.idf.il/mobile/login.aspx	Block	1
84.229.7.3	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
46.19.85.95	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	1
207.46.13.111	United States	147.237.72.166	aka.idf.il	Unknown Parameter 4f9c0c80 in www.aka.idf.il/main/home/default.aspx	None	1
79.181.149.219	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
195.160.242.40	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
10.125.50.10		147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1
46.19.86.90	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
212.179.73.106	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
218.17.231.155	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.asp	Block	1
81.218.118.126	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/nav.css	Block	1
199.203.136.183	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/1070-he/nakhal.aspx	Block	1
176.13.230.92	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
85.64.219.23	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
213.151.32.163	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
194.114.146.227	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 194.114.146.227	Block	1
113.71.255.4	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/index.asp	Block	1
81.255.155.161	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	1
207.46.13.57	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
185.22.224.96	United Kingdom	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/6/4616.jpg	Block	1

09-08-2016-10:04:08 to 09-08-2016-11:04:08