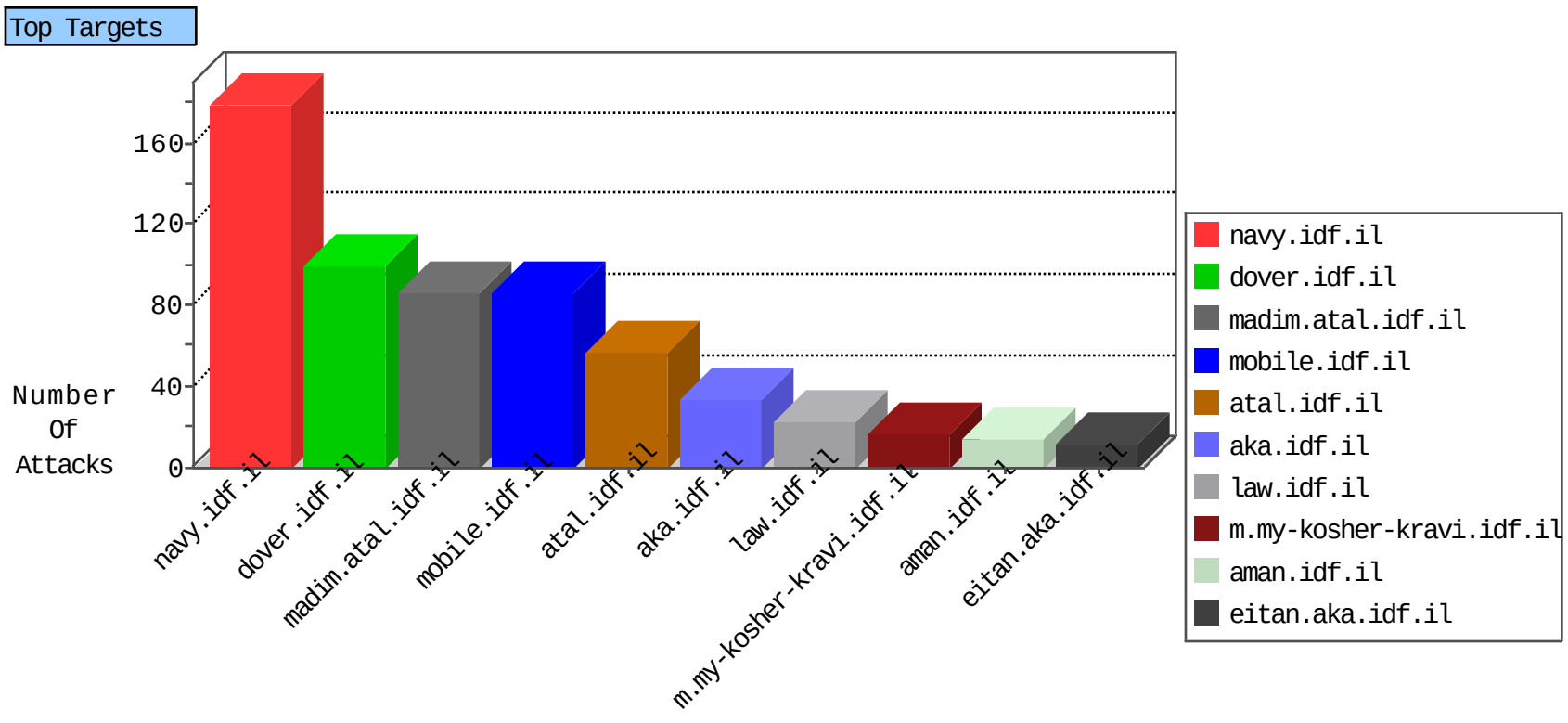
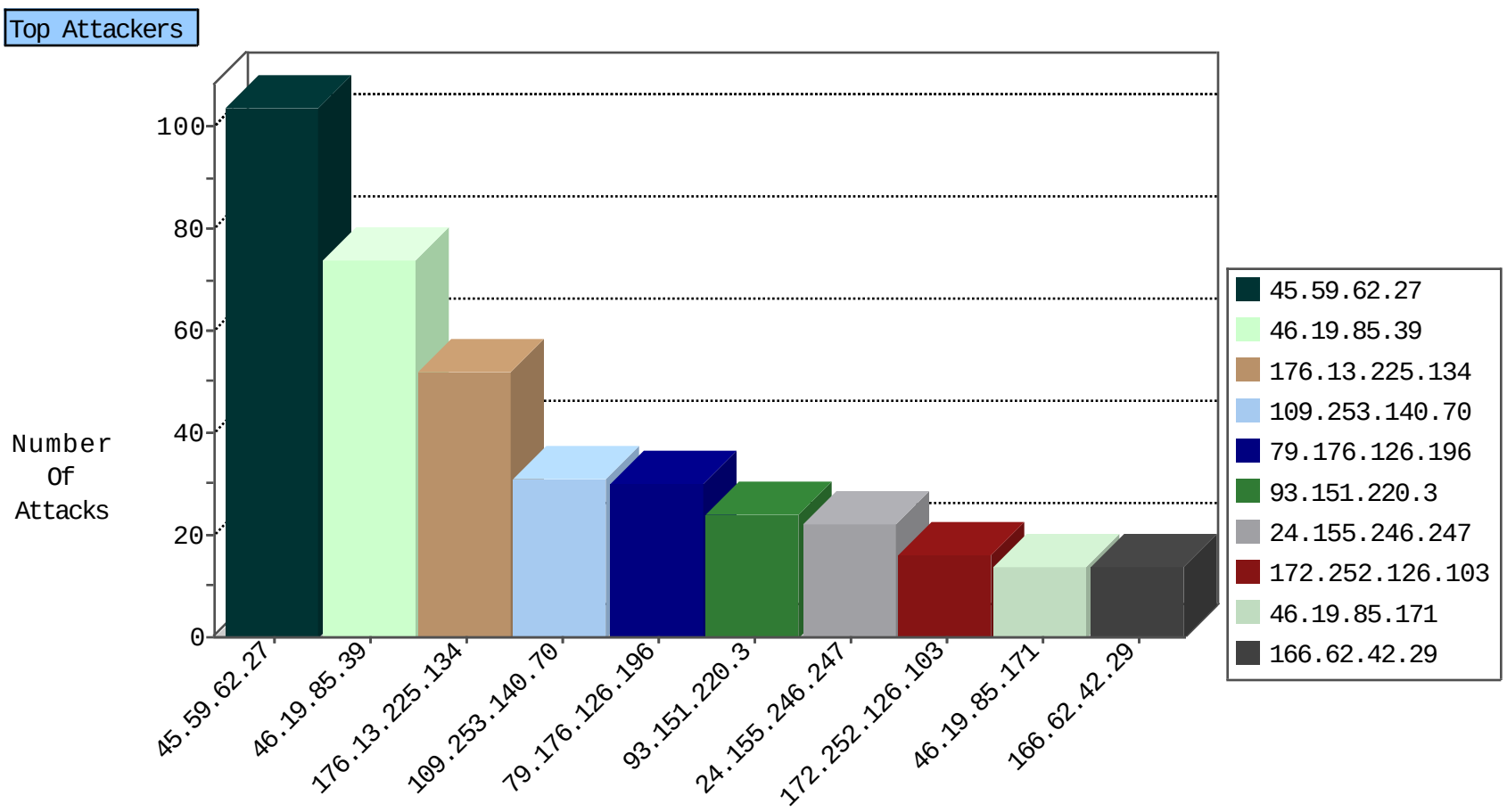
09-22-2016-00:04:04 to 09-22-2016-01:04:04

IDF Under Attack
Daily Report





09-22-2016-00:04:04 to 09-22-2016-01:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
42.112.10.89	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1
42.112.10.73	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1
185.94.111.1	Russian Federation	147.237.76.31	nakchal.idf.il	Black List	drop	1
42.112.10.81	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1
42.112.10.66	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1
42.112.10.74	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1
185.94.111.1	Russian Federation	147.237.76.38	e.e.meitav.idf.il	Black List	drop	1
42.112.10.83	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1
42.112.10.69	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1
122.224.153.109	China	147.237.76.39	mobile.meitav.idf.il	JLM_Purple_Con_Limit_Http	drop	1
42.112.10.75	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1
42.112.10.85	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1
42.112.10.70	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1
122.224.153.109	China	147.237.76.39	mobile.meitav.idf.il	JLM_Under_Attack_Con_Http	drop	1
42.112.10.80	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1

09-22-2016-00:04:04 to 09-22-2016-01:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
166.62.42.29	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
195.8.208.130	Netherlands	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

09-22-2016-00:04:04 to 09-22-2016-01:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.8.208.130	147.237.77.74	Netherlands	law.idf.il	SQL Injection - Select From	8
166.62.42.29	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
80.15.154.133	147.237.77.205	France	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
164.52.227.101	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
77.252.26.51	147.237.8.27	Poland	e.madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1
118.217.223.25	147.237.76.196	Korea, Republic of	e.sviva.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
58.244.234.106	147.237.0.200	China	m4u.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
100.13.130.4	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
47.88.4.204	147.237.77.121	Canada	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.49.92	147.237.77.216	Netherlands	dover.idf.il	ET SCAN NMAP -sS window 1024	1
23.91.75.231	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
85.244.226.214	147.237.76.148	Portugal	gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
23.91.75.231	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
206.246.150.226	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
85.244.226.214	147.237.76.39	Portugal	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
2.235.174.164	147.237.8.27	Italy	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
206.246.150.226	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
85.244.226.214	147.237.0.34	Portugal	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
200.241.137.4	147.237.0.33	Brazil	idf.il	ET SCAN NMAP -sS window 1024	1
80.15.154.133	147.237.77.233	France	atal.idf.il	ET SCAN NMAP -sS window 1024	1
80.15.154.133	147.237.0.19	France	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
139.162.13.205	147.237.0.15	Singapore	kosher-kravi.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
77.252.26.51	147.237.8.27	Poland	e.madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1
118.103.126.194	147.237.0.35	Japan	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
58.220.2.5	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
100.13.130.4	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 1024	1
31.24.228.20	147.237.76.31	United Kingdom	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
89.139.114.189	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
23.91.75.231	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 1024	1
218.27.1.174	147.237.72.166	China	aka.idf.il	ET SCAN NMAP -sS window 1024	1
85.244.226.214	147.237.76.44	Portugal	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
2.235.174.164	147.237.8.50	Italy	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
206.246.150.226	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
85.244.226.214	147.237.76.31	Portugal	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
2.235.174.164	147.237.8.14	Italy	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
200.241.137.4	147.237.0.35	Brazil	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
85.244.226.214	147.237.0.19	Portugal	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

09-22-2016-00:04:04 to 09-22-2016-01:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
45.59.62.27	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	103
176.13.225.134	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	51
79.176.126.196	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	29
93.151.220.3	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
172.252.126.103	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
46.19.85.39	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.85.171	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.85.171	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.39	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.55.145.226	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.39	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.39	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
31.210.187.86	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.39	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
24.155.246.247	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	5
24.155.246.247	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	5
46.117.76.103	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
24.155.246.247	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
195.239.16.40	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
24.155.246.247	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
195.239.16.53	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
24.155.246.247	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
66.249.64.85	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.39.49	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.195.226	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.218.21	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
24.4.50.221	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	2
24.4.50.221	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.251	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
213.77.24.132	Poland	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
79.179.168.66	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2
109.253.140.251	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
24.208.186.108	United States	147.237.76.86	navy.idf.il	SYN Attack		alert	2
141.226.218.113	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
79.180.159.88	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
77.139.74.146	France	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
149.56.106.186	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	2
109.253.140.251	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
24.208.186.108	United States	147.237.76.86	navy.idf.il	SYN Attack		monitor	2
24.4.50.221	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
149.56.106.186	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.26.148.153	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
161.18.72.175	Colombia	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
85.64.103.217	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
24.4.50.221	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	2
46.19.85.136	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	2
79.167.136.251	Greece	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
109.253.140.251	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
66.90.218.69	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	1

09-22-2016-00:04:04 to 09-22-2016-01:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	34
109.253.140.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31
213.8.204.13	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.86.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
2.53.173.31	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1432	Block	3
109.253.221.75	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.173.31	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 2.53.173.31	Block	2
79.178.129.123	Israel	147.237.72.156	aman.idf.il	Distributed Double URL Encoding	Block	2
213.151.46.98	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	2
66.249.64.131	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
139.162.13.205	Singapore	147.237.0.15	kosher-kravi.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	2
79.176.126.196	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
66.248.219.109	United States	147.237.76.147	chinuch.aka.idf.il	PHP Attempt	Block	1
176.13.225.134	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.76.53	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	1
46.19.85.39	Israel	147.237.0.19	madim.atal.idf.il	Double URL Encoding - parameter: ReturnUrl in madim.atal.idf.il/login.aspx	Block	1
180.97.106.162	China	147.237.0.16	my-kosher-kravi.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
157.55.39.161	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
66.248.219.109	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to chinuch.aka.idf.il/blogs/wp-login.php	Block	1
176.13.243.184	Israel	147.237.72.167	ishurim.aka.idf.il	Double URL Encoding - parameter: rdfrom in www.ishurim.aka.idf.il/1050-he/pickcertificates.aspx	Block	1
77.138.162.100	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
180.97.106.162	China	147.237.76.39	mobile.meitav.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
157.55.39.226	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/tizmoret/home/default.asp	None	1
80.179.54.68	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 80.179.54.68	Block	1
31.154.81.28	Israel	147.237.0.15	kosher-kravi.idf.il	PHP Attempt	Block	1
180.97.106.37	China	147.237.0.15	kosher-kravi.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
77.139.69.182	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.139.69.182	Block	1
180.97.106.162	China	147.237.76.200	eitan.aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
62.90.35.177	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
80.179.54.68	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.249.64.131	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Byte Code Character in Parameter Name Gb&T907@)DKd&f^z^H!1kR[[#28]]{	Block	1
31.154.81.28	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/xmlrpc.php	Block	1
180.97.106.37	China	147.237.0.34	tikshuv.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
157.55.39.99	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/index-files/list1.xls	Block	1
77.139.69.182	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/kiosk/	Block	1
207.46.13.31	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
66.102.9.24	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
95.143.213.229	Russian Federation	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
66.249.64.137	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding /BPv^_V*oD^ in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
180.97.106.37	China	147.237.77.176	matpash.idf.il	Multiple Untraceable SSL Sessions from 180.97.106.37 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
157.55.39.161	United States	147.237.77.216	dover.idf.il	PHP Attempt	Block	1

09-22-2016-00:04:04 to 09-22-2016-01:04:04