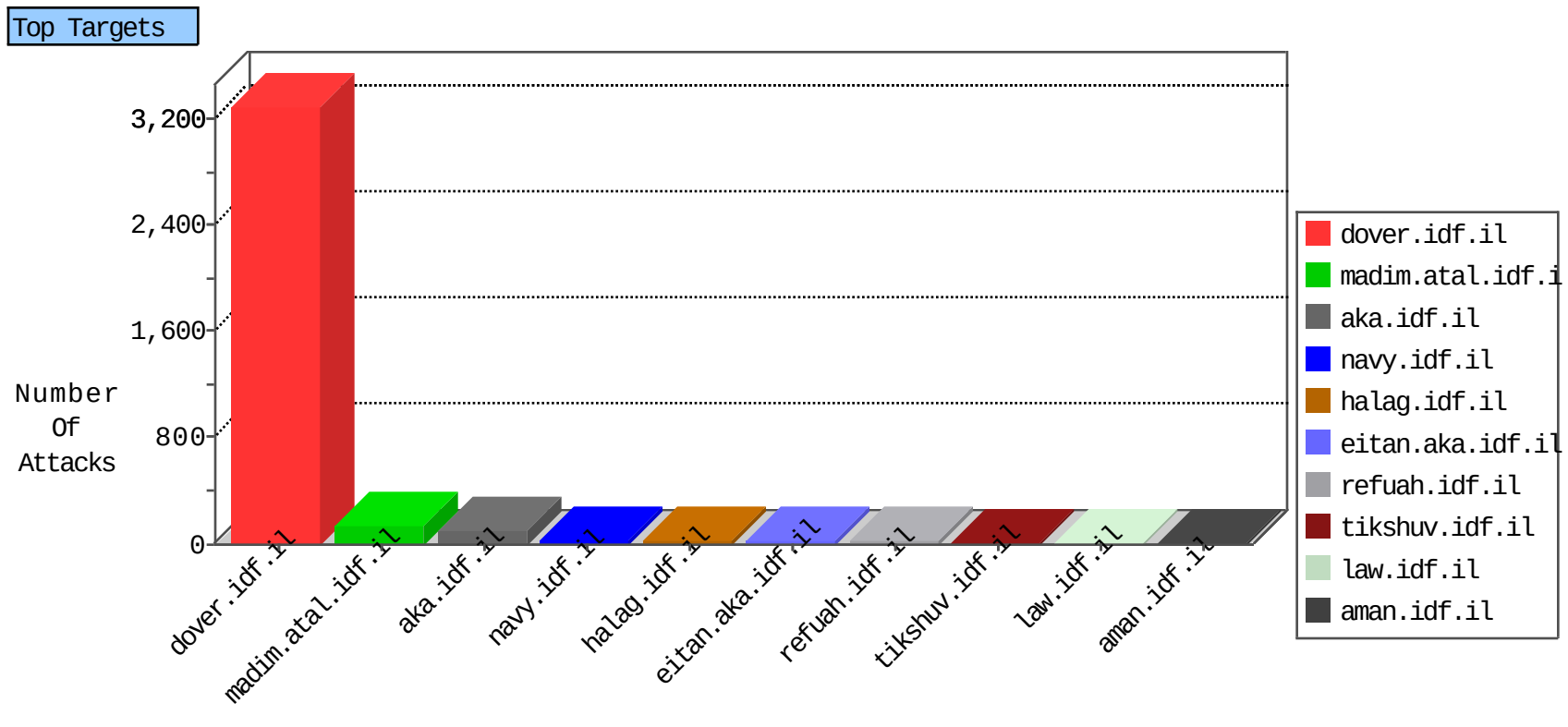
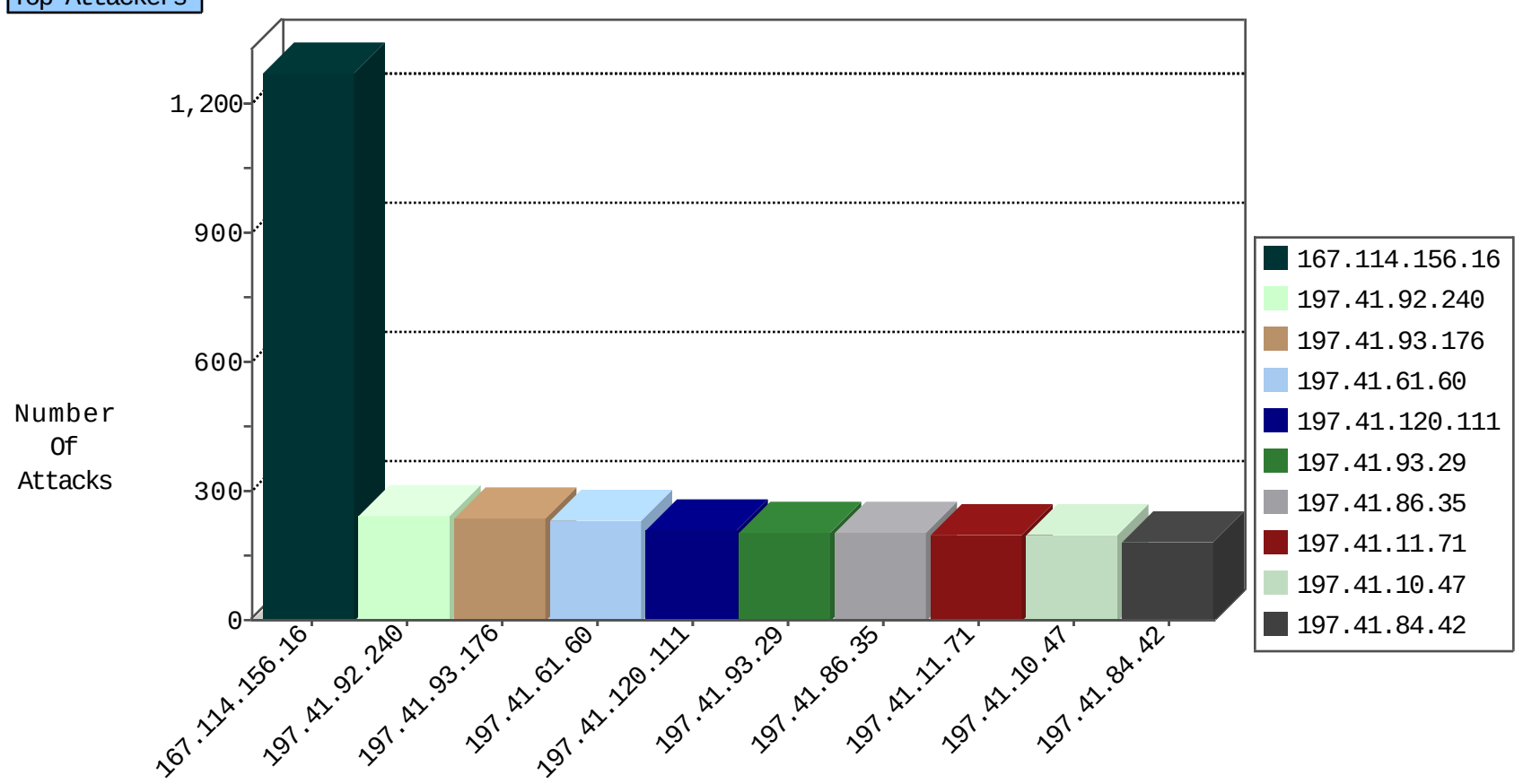
04-14-2016-23:04:04 to 04-15-2016-00:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-14-2016-23:04:04 to 04-15-2016-00:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	1273
197.41.61.60	Egypt	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	651
197.41.92.240	Egypt	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	622
197.41.93.176	Egypt	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	619
197.41.93.29	Egypt	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	613
197.41.120.111	Egypt	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	609
197.41.86.35	Egypt	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	591
197.41.84.42	Egypt	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	585
197.41.10.47	Egypt	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	568
197.41.11.71	Egypt	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	530
79.181.127.93	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
89.248.160.138	Netherlands	147.237.77.205	prisha.idf.il	Block_Ntp_All_Net	drop	1
89.248.160.138	Netherlands	147.237.0.34	tikshuv.idf.il	Block_Ntp_All_Net	drop	1
89.248.160.138	Netherlands	147.237.72.217	e.idf.il	Block_Ntp_All_Net	drop	1

04-14-2016-23:04:04 to 04-15-2016-00:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
144.76.30.236	Germany	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Block	2
144.76.30.236	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
149.78.168.201	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
79.176.138.27	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
199.30.25.97	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
144.76.30.236	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
62.98.17.225	Italy	147.237.77.216	dover.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.66.154	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
115.73.177.112	Vietnam	147.237.77.74	law.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1
123.126.113.101	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-14-2016-23:04:04 to 04-15-2016-00:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
197.41.11.71	147.237.77.216	Egypt	dover.idf.il	ET SCAN NMAP -sS window 1024	9
197.41.120.111	147.237.77.216	Egypt	dover.idf.il	ET SCAN NMAP -sS window 1024	6
197.41.93.176	147.237.77.216	Egypt	dover.idf.il	ET SCAN NMAP -sS window 1024	6
197.41.92.240	147.237.77.216	Egypt	dover.idf.il	ET SCAN NMAP -sS window 1024	6
197.41.61.60	147.237.77.216	Egypt	dover.idf.il	ET SCAN NMAP -sS window 1024	5
197.41.93.29	147.237.77.216	Egypt	dover.idf.il	ET SCAN NMAP -sS window 1024	5
197.41.86.35	147.237.77.216	Egypt	dover.idf.il	ET SCAN NMAP -sS window 1024	5
197.41.10.47	147.237.77.216	Egypt	dover.idf.il	ET SCAN NMAP -sS window 1024	5
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
197.41.84.42	147.237.77.216	Egypt	dover.idf.il	ET SCAN NMAP -sS window 1024	4
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
197.41.84.42	147.237.77.216	Egypt	dover.idf.il	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	1
197.41.10.47	147.237.77.216	Egypt	dover.idf.il	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	1
183.60.252.84	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN NMAP -sS window 3072	1
220.132.95.204	147.237.0.33	Taiwan	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
180.97.106.37	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
183.60.252.84	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN NMAP -sS window 4096	1
180.97.106.37	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.74	147.237.76.34	United States	yohalan.idf.il	ET DROP Dshield Block Listed Source	1
106.186.113.132	147.237.8.46	Japan	e.chinuch.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
65.181.123.161	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1

04-14-2016-23:04:04 to 04-15-2016-00:04:04

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
87.70.90.253	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
5.28.189.51	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	13
5.28.189.51	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
87.71.78.167	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.183.197.204	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
109.64.93.42	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
2.53.155.237	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
197.41.11.71	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
5.102.254.90	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.16	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.16	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
197.41.10.47	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.90	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
123.126.113.101	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
192.115.60.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
197.41.120.111	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
195.60.232.57	Israel	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
188.36.120.189	Hungary	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
77.126.215.16	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.242.155	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
62.210.254.123	France	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
87.71.104.169	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
197.41.86.35	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
109.65.197.49	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.182.170	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.191	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
31.210.187.203	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.179.70	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.189.94	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.146.158	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.147.175	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.237	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
197.41.93.176	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
82.81.53.201	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
37.26.149.191	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
82.81.53.201	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
79.182.153.159	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
5.22.135.113	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.167	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
82.81.53.201	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
128.232.110.29	United Kingdom	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
82.81.53.201	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
128.232.110.29	United Kingdom	147.237.8.24	e.lifestyle.idf.	Geo-location enforcement	Geo-location inbound enforcement	drop	2
5.22.135.113	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
68.180.230.155	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.85.167	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
197.41.92.240	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
82.81.53.201	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
109.186.5.19	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

04-14-2016-23:04:04 to 04-15-2016-00:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
31.154.169.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	137
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	19
130.193.50.33	Russian Federation	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 130.193.50.33	Block	4
80.246.136.9	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.134.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
82.166.153.125	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 82.166.153.125	Block	2
157.55.39.217	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
79.180.120.34	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
31.168.201.169	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/tfasim.aspx'	Block	2
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
195.60.232.57	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/5/112335.pdf	Block	1
131.253.25.151	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
31.210.187.203	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
83.54.3.19	Spain	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
197.41.86.35	Egypt	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/sachar/resources/images/malshab-over.jpg	Block	1
62.210.181.15	France	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
176.13.23.188	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	1
5.29.72.179	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 5.29.72.179	Block	1
109.64.93.42	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
79.183.197.204	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
217.69.136.208	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy	Block	1
66.249.64.179	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/sachar/resources/images/sidebar/bulletorange.gif	Block	1
197.41.10.47	Egypt	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	1
131.253.25.248	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
37.26.146.158	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
87.69.224.109	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/960.css	Block	1
5.28.130.226	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/resources/styles/recruitlane.css	Block	1
62.210.254.52	France	147.237.72.166	aka.idf.il	Unknown Parameter amp;rnd in www.aka.idf.il/main/giyus/captcha.ashx	None	1
176.213.185.90	Russian Federation	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/unit.aspx	Block	1
5.29.72.179	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/	Block	1
111.56.13.150	China	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
197.41.10.47	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-16449-he/dover.aspx	Block	1
157.55.39.107	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
40.77.167.16	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	1
5.28.189.51	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
87.71.23.156	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/eitan/listpage/	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-he/dover.aspx	Block	1
62.210.254.123	France	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
188.36.120.189	Hungary	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 188.36.120.189 (Open Mode)	None	1
197.41.10.47	Egypt	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/sachar/resources/images/icons/favicon.png	Block	1
5.29.24.197	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 5.29.24.197 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english	Block	1
213.151.38.132	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
62.210.254.123	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1

04-14-2016-23:04:04 to 04-15-2016-00:04:04