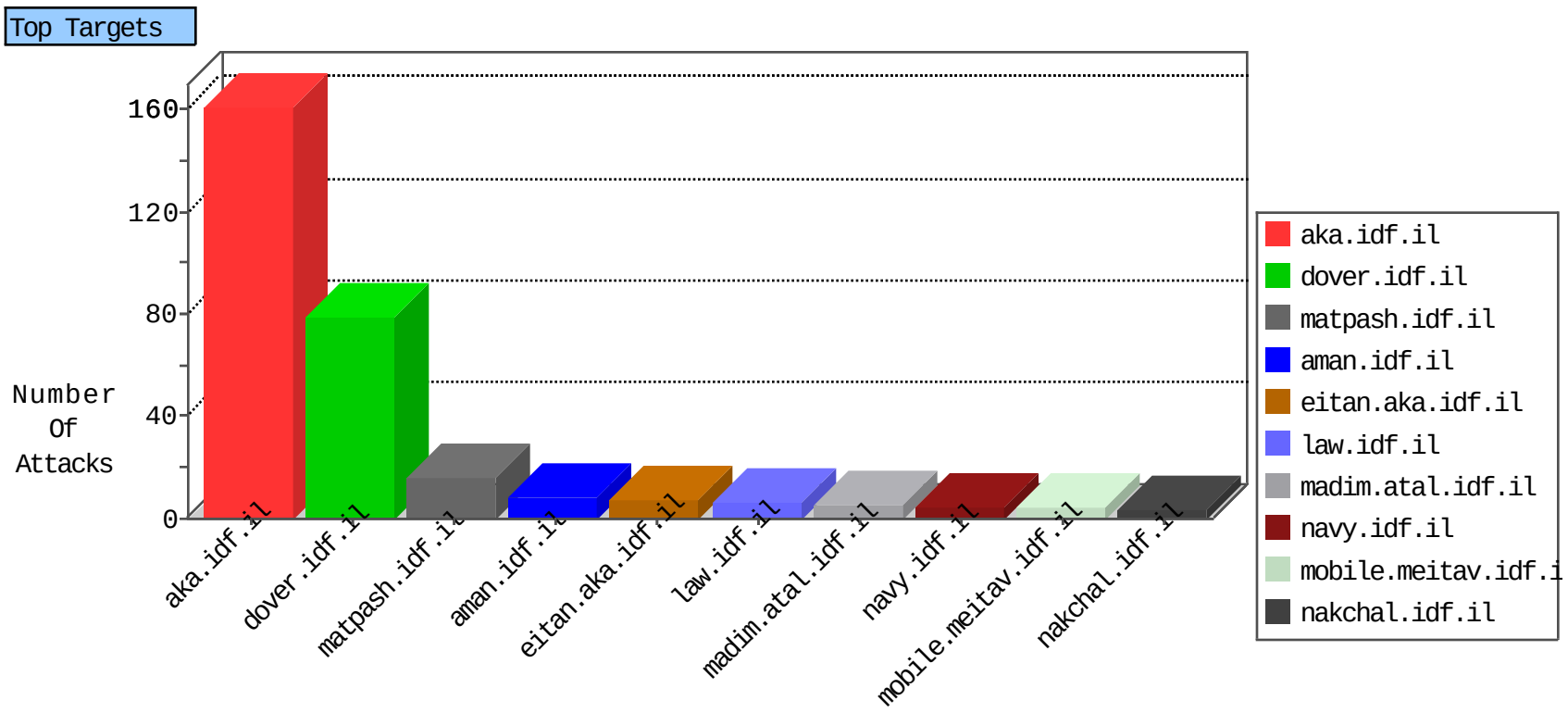
01-31-2016-04:04:07 to 01-31-2016-05:04:07

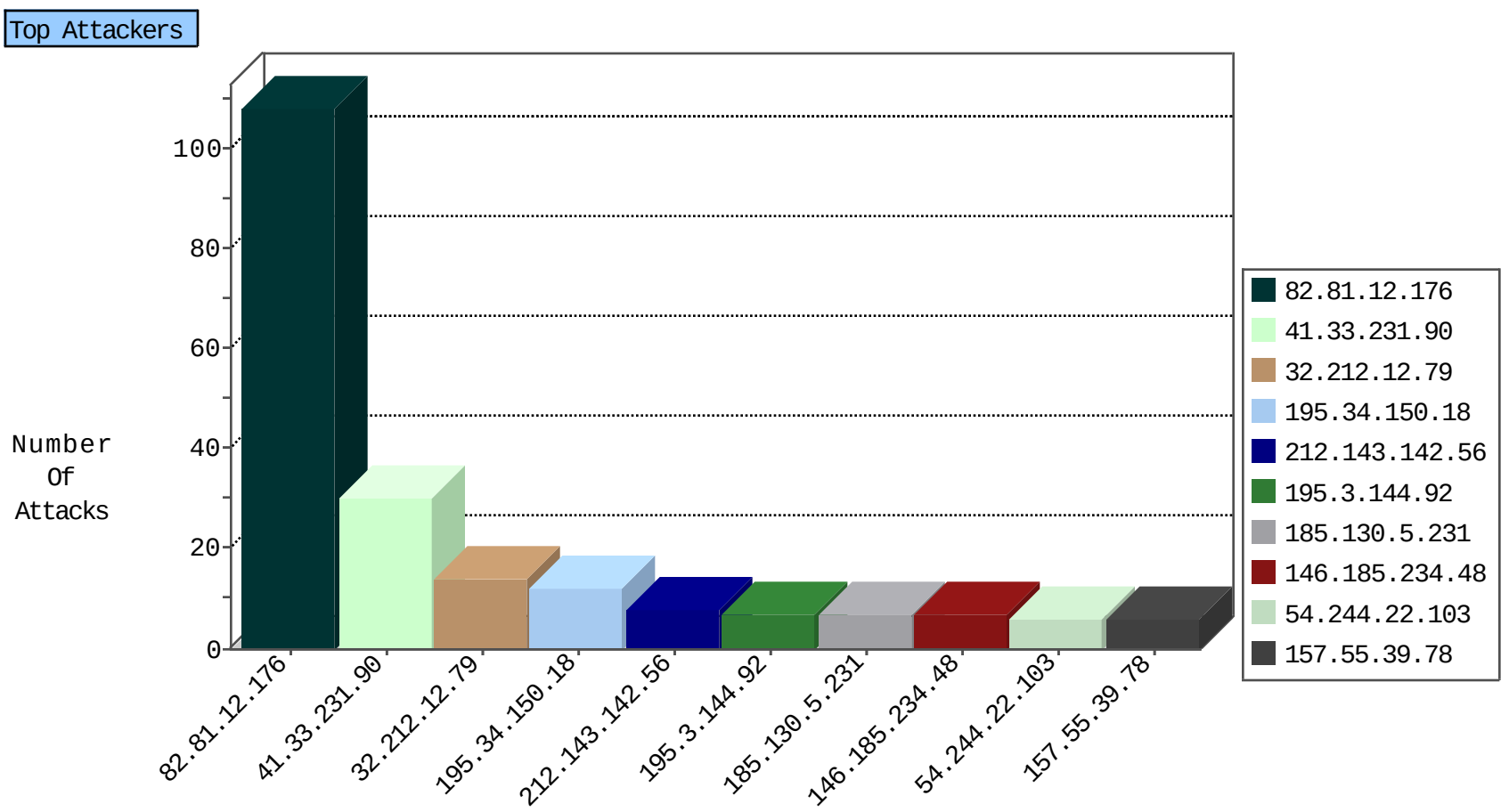
IDF Under Attack
Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

01-31-2016-04:04:07 to 01-31-2016-05:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	108
142.54.169.165	United States	147.237.77.233	atal.idf.il	block-sp-traf1	drop	1
74.91.28.58	United States	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	1
185.130.5.224		147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
80.82.78.39	Netherlands	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
195.13.231.183	Latvia	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1

01-31-2016-04:04:07 to 01-31-2016-05:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.176.172.168	United States	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
195.3.144.92	Latvia	147.237.76.200	eitan.aka.idf.i	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1

01-31-2016-04:04:07 to 01-31-2016-05:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
40.114.11.138	147.237.0.200	United States	m4u.idf.il	ET SCAN Potential SSH Scan	2
40.114.11.138	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
196.47.173.21	147.237.76.196	Cote D'Ivoire	e.sviva.idf.il	ET SCAN NMAP -sS window 4096	1
195.3.144.92	147.237.76.200	Latvia	eitan.aka.idf.il	SERVER-WEBAPP admin.php access	1
117.81.86.98	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
98.119.105.221	147.237.72.156	United States	aman.idf.il	ET SCAN NMAP -sS window 3072	1
221.228.143.241	147.237.0.33	China	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
98.119.105.221	147.237.72.156	United States	aman.idf.il	ET SCAN NMAP -f -sS	1
209.126.230.73	147.237.76.31	United States	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
82.117.208.243	147.237.77.234		halag.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.230.72	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
199.191.56.187	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 2048	1
40.114.11.138	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.74	147.237.76.39	United States	mobile.meitav.idf.il	ET DROP Dshield Block Listed Source	1
196.47.173.21	147.237.76.196	Cote D'Ivoire	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
173.242.113.145	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1
116.228.152.154	147.237.76.176	China	test.ncore.idf.il	ET DROP Dshield Block Listed Source	1
98.119.105.221	147.237.72.156	United States	aman.idf.il	ET SCAN NMAP -sS window 2048	1
209.126.230.74	147.237.76.176	United States	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.201.236.114	147.237.76.38	Ukraine	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.230.73	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
46.45.137.67	147.237.76.196	Turkey	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
199.191.56.187	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 3072	1
40.114.11.138	147.237.0.33	United States	idf.il	ET SCAN Potential SSH Scan	1
199.191.56.187	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -f -sS	1

01-31-2016-04:04:07 to 01-31-2016-05:04:07

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
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
157.55.39.78	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
32.212.12.79	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
32.212.12.79	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
77.126.144.202	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
146.185.234.48	Russian Federation	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
89.138.87.92	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
32.212.12.79	United States	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	2
157.55.39.172	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
91.200.12.106	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
62.210.209.237	France	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
91.200.12.141	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
157.55.39.70	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
66.249.78.161	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
191.232.136.33	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
185.130.5.231		147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.175	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.139.100	United States	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
68.104.238.96	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
32.212.12.79	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.247.219	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
157.55.39.167	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
185.130.5.231		147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.100	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
146.185.234.48	Russian Federation	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
68.132.15.93	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
185.130.5.231		147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.130.5.231		147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
32.212.12.79	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
184.105.139.111	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
146.185.234.48	Russian Federation	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
68.132.15.93	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
216.218.206.104	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.130.5.231		147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
178.33.126.108	France	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
185.130.5.231		147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.116	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
218.22.211.69	China	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.85.48	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.130.5.231		147.237.76.34	yohalan.idf.il	drop		drop	1
180.76.15.7	China	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
146.185.234.48	Russian Federation	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
184.105.247.211	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
85.25.43.94	Germany	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

01-31-2016-04:04:07 to 01-31-2016-05:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.229.224.159	United States	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	4
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	3
68.142.232.22	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 68.142.232.22	Block	2
32.212.12.79	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
195.3.144.92	Latvia	147.237.76.200	eitan.aka.idf.il	PHP Attempt	Block	2
89.161.202.147	Poland	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 89.161.202.147	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
68.142.232.21	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 68.142.232.21	Block	2
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
184.105.247.195	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
103.38.161.226	Hong Kong	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/xmlrpc.php	Block	1
77.40.129.123	Norway	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
195.3.144.92	Latvia	147.237.76.200	eitan.aka.idf.il	Admin Blocking	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
146.185.234.48	Russian Federation	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
2.54.26.64	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
84.25.166.74	Netherlands	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
184.168.192.130	United States	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
77.40.129.123	Norway	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
195.3.144.92	Latvia	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 195.3.144.92	Block	1
66.249.78.204	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/faq/faq.aspx	Block	1
149.88.213.130	Israel	147.237.76.39	mobile.meitav.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtPassword in mobile.meitav.idf.il/templates/login.aspx	Block	1
85.64.60.66	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1381-he/dover.aspx	Block	1
66.229.224.159	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	1
184.168.192.130	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/xmlrpc.php	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
79.183.97.201	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
157.55.39.47	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
188.143.232.35	Russian Federation	147.237.77.176	matpash.idf.il	Parameter Type Violation fromDate in www.cogat.idf.il/901-en/cogat.aspx	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/faq.aspx	Block	1
109.163.234.2	Romania	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
82.80.135.16	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
195.3.144.92	Latvia	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/wp-login.php	Block	1
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
176.103.48.30	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
103.38.161.226	Hong Kong	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
74.91.28.58	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to g00d.e0534.com/	Block	1
191.232.136.7	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18762-he/dover.aspx	Block	1
146.185.234.48	Russian Federation	147.237.77.176	matpash.idf.il	Distributed Parameter Type Violation on www.cogat.idf.il/901-en/cogat.aspx parameter fromDate	Block	1
84.25.166.74	Netherlands	147.237.77.74	law.idf.il	PHP Attempt	Block	1
204.13.201.137	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
68.142.232.21	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/test/wp-admin/	Block	1

01-31-2016-04:04:07 to 01-31-2016-05:04:07