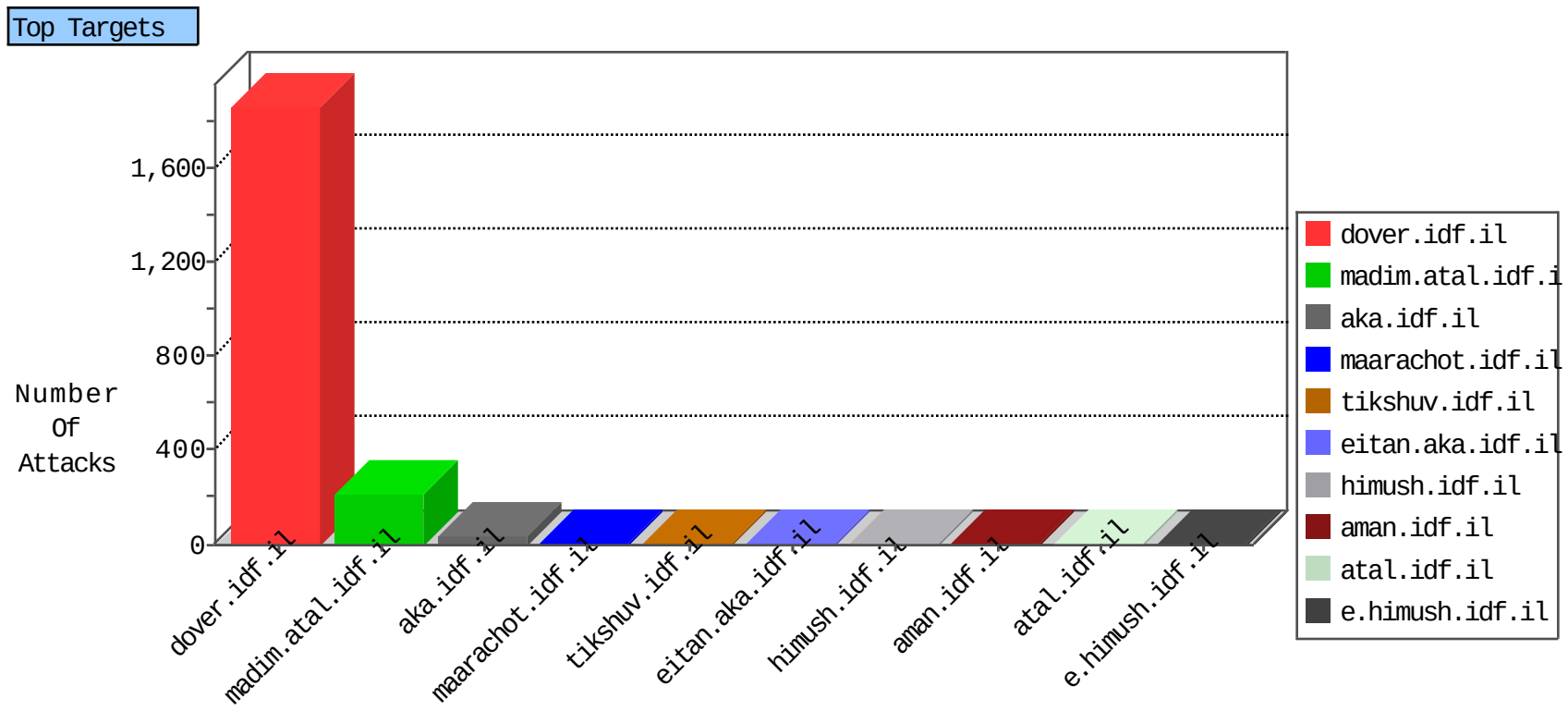
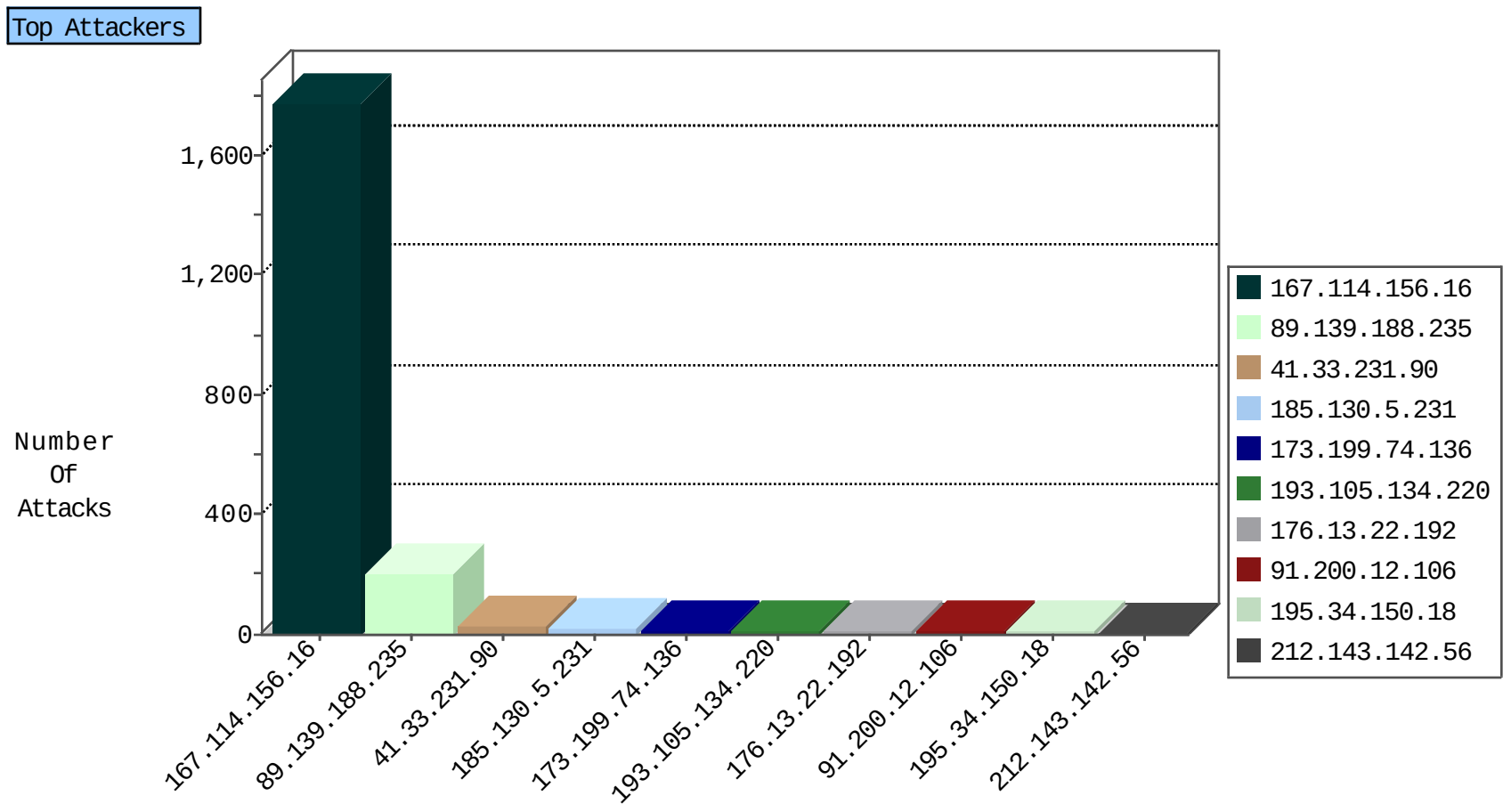
01-07-2016-02:04:04 to 01-07-2016-03:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-07-2016-02:04:04 to 01-07-2016-03:04:04

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	DOS-Tool-SwitchbladG	dest-reset	3047
195.158.100.38	Malta	147.237.76.197	e.himush.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
66.102.9.21	United States	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
89.248.174.4	Netherlands	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
208.67.1.60	United States	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
110.182.154.88	China	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1

01-07-2016-02:04:04 to 01-07-2016-03:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
184.173.50.36	United States	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1

01-07-2016-02:04:04 to 01-07-2016-03:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
80.248.146.42	147.237.72.156	Russian Federation	aman.idf.il	ET SCAN NMAP -sS window 1024	1
173.199.74.136	147.237.77.170	United Kingdom	maarachot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
58.101.85.198	147.237.76.30	China	himush.idf.il	ET SCAN NMAP -sS window 1024	1
173.199.74.136	147.237.76.200	United Kingdom	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
31.184.195.114	147.237.77.121	Russian Federation	e.navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
173.199.74.136	147.237.76.196	United Kingdom	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
27.40.159.54	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
173.199.74.136	147.237.76.39	United Kingdom	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
173.199.74.136	147.237.76.30	United Kingdom	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
209.126.116.147	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
173.199.74.136	147.237.8.45	United Kingdom	e.eitan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
114.26.24.225	147.237.0.17	Taiwan	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
173.199.74.136	147.237.77.233	United Kingdom	atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
80.248.146.42	147.237.72.217	Russian Federation	e.idf.il	ET SCAN NMAP -sS window 1024	1
173.199.74.136	147.237.77.176	United Kingdom	matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
58.101.85.198	147.237.76.31	China	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
173.199.74.136	147.237.76.202	United Kingdom	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.165.222.227	147.237.0.19	Germany	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
173.199.74.136	147.237.76.197	United Kingdom	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
31.184.195.114	147.237.8.28	Russian Federation	e.mobile-ks.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
173.199.74.136	147.237.76.42	United Kingdom	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
173.199.74.136	147.237.76.34	United Kingdom	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
173.199.74.136	147.237.72.156	United Kingdom	aman.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
204.151.12.240	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
122.242.83.93	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
193.105.134.220	147.237.77.233	Sweden	atal.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
173.199.74.136	147.237.77.205	United Kingdom	prisha.idf.il	ET SCAN NMAP -sS window 1024	1

01-07-2016-02:04:04 to 01-07-2016-03:04:04

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
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
176.13.22.192	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
176.13.22.192	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
91.200.12.106	Ukraine	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	4
91.200.12.106	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
46.19.86.117	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
65.95.65.219	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
66.249.78.160	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
199.30.25.121	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	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
106.185.22.218	Japan	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.130.5.231		147.237.76.202	e.halag.idf.il	drop	SAM rule	drop	1
185.130.5.231		147.237.76.148	gqcenter.aka.idf.i	drop	SAM rule	drop	1
45.35.71.181		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
185.130.5.231		147.237.72.156	aman.idf.il	drop	SAM rule	drop	1
146.185.239.102	Russian Federation	147.237.0.35	akaws.idf.il	drop		drop	1
193.105.134.220	Sweden	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.130.5.231		147.237.76.198	e.yohalan.idf.il	drop	SAM rule	drop	1
47.16.80.195	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.130.5.231		147.237.76.42	refuah.idf.il	drop	SAM rule	drop	1
2.54.190.202	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
193.105.134.220	Sweden	147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.169	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.130.5.231		147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
77.237.138.202	Czech Republic	147.237.77.19	law-forum.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
185.130.5.231		147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	1
45.35.71.181		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.130.5.231		147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	1
167.160.116.50	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
193.105.134.220	Sweden	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.130.5.231		147.237.76.199	e.nakchal.idf.il	drop	SAM rule	drop	1
52.53.251.67	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
185.130.5.231		147.237.76.44	e.refuah.idf.il	drop	SAM rule	drop	1
2.54.190.202	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.106.92.33		147.237.76.30	himush.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
193.105.134.220	Sweden	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.170	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
188.143.232.16	Russian Federation	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
81.44.224.176	Spain	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
185.130.5.231		147.237.76.177	ncore.idf.il	drop	SAM rule	drop	1
185.130.5.231		147.237.76.34	yohalan.idf.il	drop	SAM rule	drop	1
209.190.20.61	United States	147.237.72.166	aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
172.89.80.253		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
193.105.134.220	Sweden	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
106.75.199.201	China	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.130.5.231		147.237.76.200	eitan.aka.idf.il	drop	SAM rule	drop	1
185.130.5.231		147.237.76.86	navy.idf.il	drop	SAM rule	drop	1
5.22.131.79	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

01-07-2016-02:04:04 to 01-07-2016-03:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.139.188.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
89.139.188.235	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 89.139.188.235	Block	61
89.139.188.235	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 89.139.188.235	Block	34
37.26.146.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.18.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.57.134.251	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.220.159.115	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.220.159.119	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
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
66.249.79.9	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
183.79.223.13	Japan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/	Block	1
195.154.227.118	France	147.237.77.216	dover.idf.il	Illegal HTTP Version HTTP/	Block	1
150.70.97.86	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
68.64.194.86	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
40.77.167.17	United States	147.237.72.166	aka.idf.il	Unknown Parameter KEY in aka.idf.il/ishurim/cityofficers/	None	1
217.132.105.216	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.25.151.159	Poland	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to testp2.czar.bielawa.pl/testproxy.php	Block	1
2.54.50.14	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
150.70.97.86	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
77.237.138.202	Czech Republic	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to /	Block	1
45.35.71.181		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
185.25.151.159	Poland	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to testp4.pospr.waw.pl/testproxy.php	Block	1
91.196.50.33	Poland	147.237.77.176	matpash.idf.il	Unauthorized URL Access to testp2.czar.bielawa.pl/testproxy.php	Block	1
66.249.78.153	Israel	147.237.72.166	aka.idf.il	Unknown Parameter KEY in www.aka.idf.il/valtam/asp/default.asp	None	1
2.54.50.14	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
157.55.39.191	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/site/links.aspx	Block	1
46.19.85.240	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.25.151.159	Poland	147.237.77.233	atal.idf.il	Unauthorized URL Access to testp4.pospr.waw.pl/testproxy.php	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
66.249.79.6	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/2/1642.pdf	Block	1
2.54.163.61	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
209.190.20.61	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 209.190.20.61	Block	1
176.13.21.220	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
89.139.188.235	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	1
54.166.109.137	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	1
185.106.92.33		147.237.76.30	himush.idf.il	Unauthorized Method HEAD for 147.237.76.30/	Block	1

01-07-2016-02:04:04 to 01-07-2016-03:04:04