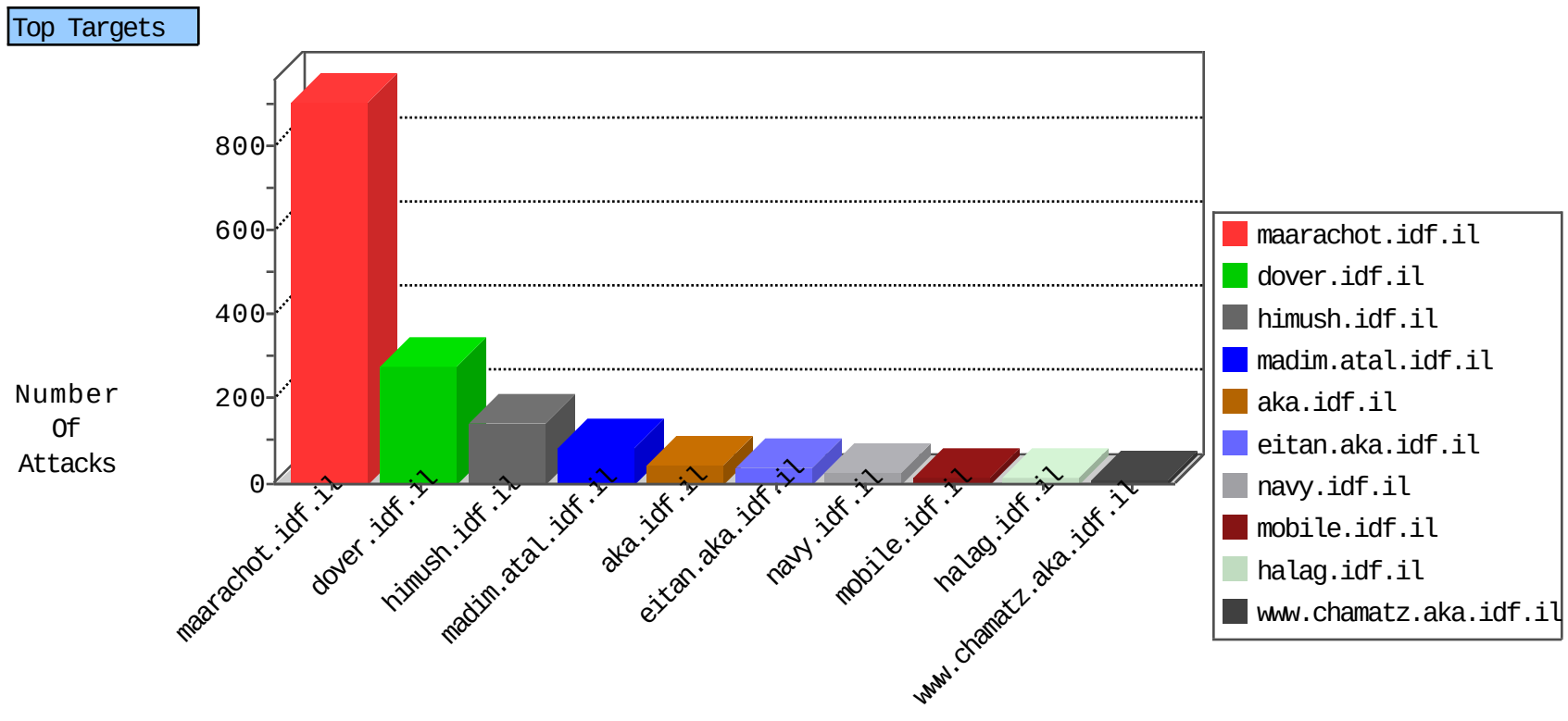
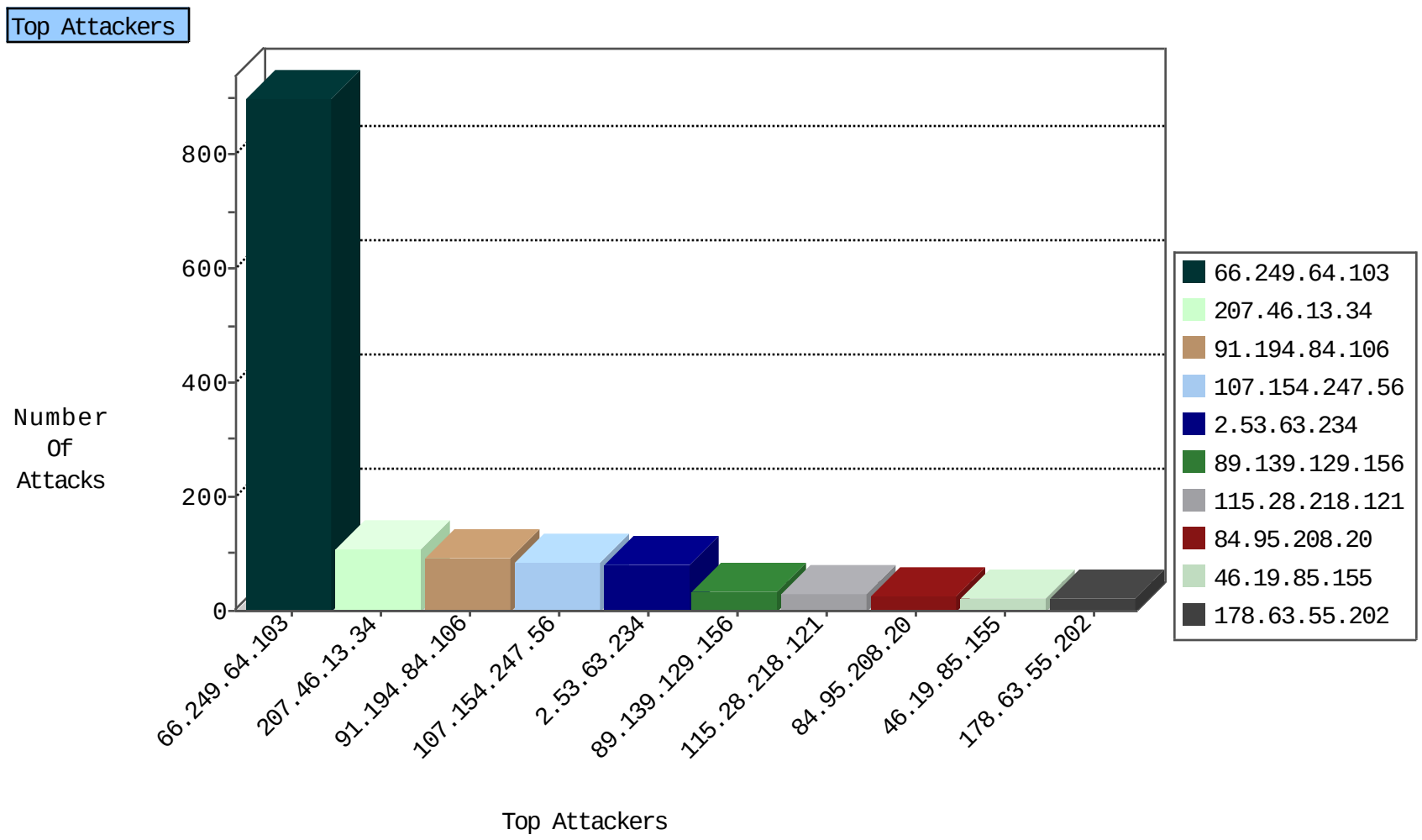
10-03-2016-10:04:08 to 10-03-2016-11:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-03-2016-10:04:08 to 10-03-2016-11:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.174.93.218	Netherlands	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	forward	2
185.94.111.1	Russian Federation	147.237.76.176	test.ncore.idf.il	Black List	drop	1

10-03-2016-10:04:08 to 10-03-2016-11:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
91.194.84.106	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	90
162.210.196.97	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
50.87.144.52	United States	147.237.77.74	law.idf.il	3630: HTTP: SQL Injection (Boolean Identity)	Block	1

10-03-2016-10:04:08 to 10-03-2016-11:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.64.103	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	901
62.210.124.129	147.237.77.216	France	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
14.152.59.11	147.237.76.197	China	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
139.162.168.200	147.237.76.202	United States	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
113.23.54.240	147.237.76.196	Vietnam	e.sviva.idf.il	ET SCAN NMAP -sS window 4096	1
106.187.45.144	147.237.76.198	Japan	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
85.143.216.168	147.237.76.201	Russian Federation	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.200.137	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
211.149.222.5	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
38.108.35.137	147.237.76.86	United States	navy.idf.il	ET SCAN Potential SSH Scan	1
198.52.97.92	147.237.77.216	United States	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
139.162.13.205	147.237.76.42	Singapore	refuah.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
113.23.54.240	147.237.76.196	Vietnam	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
91.232.105.190	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
59.127.0.203	147.237.77.234	Taiwan	halag.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.200.137	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
211.149.222.5	147.237.72.217	China	e.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.65	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
209.95.50.84	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1

10-03-2016-10:04:08 to 10-03-2016-11:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
207.46.13.34	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	108
89.139.129.156	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	34
107.154.247.56	United States	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	22
178.63.55.202	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
107.154.247.56	United States	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
107.154.247.56	United States	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	19
107.154.247.56	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
46.19.85.155	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
115.28.218.121	China	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	7
46.19.85.155	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
115.28.218.121	China	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
107.154.247.56	United States	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
84.95.208.198	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
115.28.218.121	China	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	6
107.154.247.56	United States	147.237.76.30	himush.idf.il	Bad TCP sequence		monitor	6
115.28.218.121	China	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
112.124.124.227	China	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	5
112.124.124.227	China	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	5
79.177.112.156	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
79.183.26.234	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
112.124.124.227	China	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
87.68.27.136	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
107.154.247.56	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
176.13.20.25	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
46.210.199.40	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.155	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
176.13.239.148	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
112.124.124.227	China	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
87.68.27.136	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
115.28.218.121	China	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
192.168.173.102		147.237.77.216	dover.idf.il	drop		drop	3
112.124.124.227	China	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
176.13.20.25	Israel	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.19.85.155	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
37.46.41.151	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.169.101.147	United States	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	2
79.177.112.156	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	2
59.90.255.4	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
84.229.70.148	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
80.246.136.51	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
5.22.134.95	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
176.13.232.14	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
84.95.208.198	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
66.169.101.147	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
80.246.136.51	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
187.61.127.159	Brazil	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
46.210.199.40	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
212.34.20.97	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
79.180.130.121	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.63.234	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	82
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	10
79.177.185.242	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	9
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	6
93.174.93.218	Netherlands	147.237.0.15	kosher-kravi.idf.il	Multiple NULL Character in Method from 93.174.93.218	Block	3
77.138.144.217	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	Block	3
77.139.135.45	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/miyun/miyunpersonalquestionnaire.aspx	Block	2
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
50.87.144.52	United States	147.237.77.74	law.idf.il	Parameter Type Violation FileName in www.mag.idf.il/templates/getfile/getfile.aspx	Block	2
50.87.144.52	United States	147.237.77.74	law.idf.il	Parameter Type Violation InfoCenterItem in www.mag.idf.il/templates/getfile/getfile.aspx	Block	2
198.20.87.98	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/robots.txt	Block	1
46.19.86.75	Israel	147.237.76.86	navy.idf.il	Malformed URL	Block	1
87.69.205.186	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
66.249.65.58	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8803-he/refuah.aspx	Block	1
2.53.40.154	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 2.53.40.154 (Open Mode)	None	1
109.67.190.117	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
212.143.164.58	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 212.143.164.58 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
46.19.86.75	Israel	147.237.76.86	navy.idf.il	Unknown HTTP Request Method te in URL	Block	1
89.139.129.156	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter SearchText in www.eitan.aka.idf.il/938-he/eitan.aspx	None	1
66.249.75.167	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/0/300.pdf..	Block	1
2.53.40.154	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
136.243.67.234	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
77.139.223.105	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	Block	1
212.143.164.58	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
46.120.98.93	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
93.174.93.218	Netherlands	147.237.0.15	kosher-kravi.idf.il	Multiple Illegal Byte Code Character in Method from 93.174.93.218	Block	1
84.95.208.20	Israel	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
66.249.79.21	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
192.185.2.191	United States	147.237.77.74	law.idf.il	Distributed Parameter Type Violation on www.mag.idf.il/templates/getfile/getfile.aspx parameter FileName	Block	1
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
79.177.112.156	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
212.235.34.231	Israel	147.237.76.86	navy.idf.il	Cookie Tampering on cookie __atrfs: Expected ab/	None	1
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
192.185.2.191	United States	147.237.77.74	law.idf.il	Distributed Parameter Type Violation on www.mag.idf.il/templates/getfile/getfile.aspx parameter InfoCenterItem	Block	1
40.77.167.54	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	1
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	1
93.174.93.218	Netherlands	147.237.0.15	kosher-kravi.idf.il	NULL Character in Method	Block	1
77.139.90.81	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	Block	1

10-03-2016-10:04:08 to 10-03-2016-11:04:08