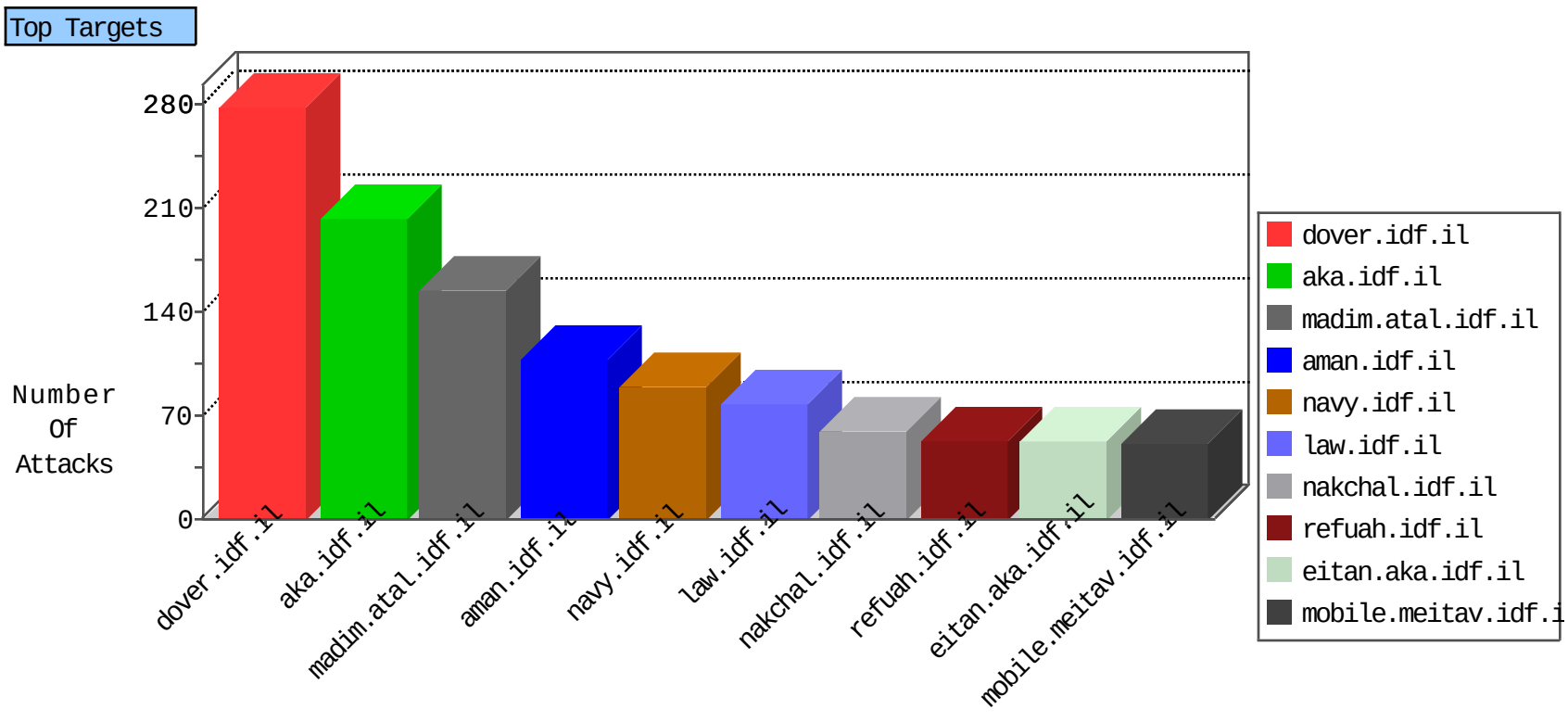
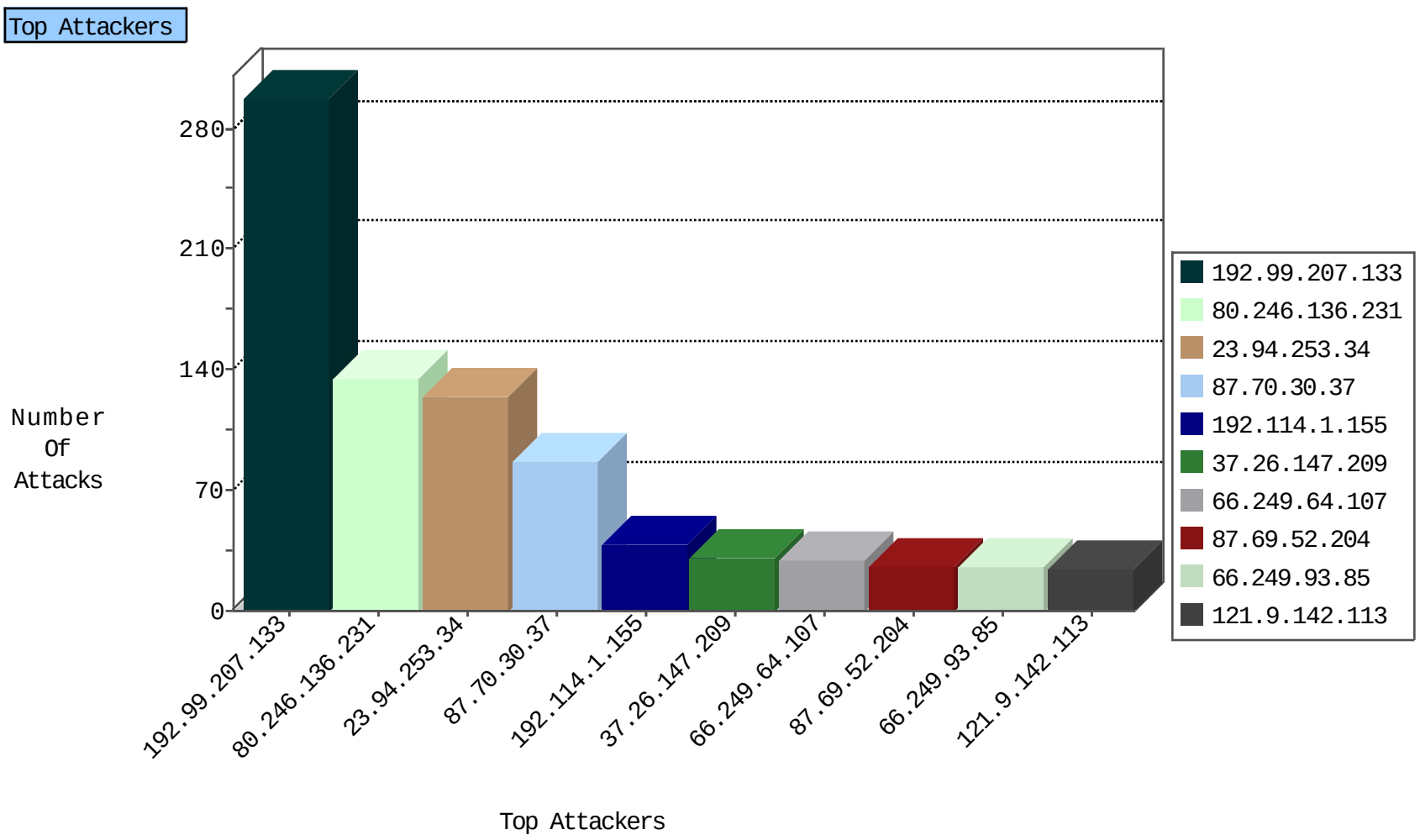
09-08-2016-19:04:07 to 09-08-2016-20:04:07

IDF Under Attack
Daily Report





09-08-2016-19:04:07 to 09-08-2016-20:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
94.177.164.99	Romania	147.237.76.202	e.halag.idf.il	Black List	drop	1
138.59.16.54	Costa Rica	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
85.64.202.181	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
138.59.16.55	Costa Rica	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
94.177.164.99	Romania	147.237.76.44	e.refuah.idf.il	Black List	drop	1

09-08-2016-19:04:07 to 09-08-2016-20:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.105	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	11
162.210.196.130	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
61.135.189.125	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

09-08-2016-19:04:07 to 09-08-2016-20:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.64.107	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	29
192.114.1.155	147.237.77.74	Israel	law.idf.il	WEB-FRONTPAGE /_vti_bin/ access	2
180.97.106.37	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
163.172.67.13	147.237.77.19	United Kingdom	law-forum.idf.il	ET SCAN Potential SSH Scan	1
132.252.173.4	147.237.77.216	Germany	dover.idf.il	GPL SCAN nmap TCP	1
80.246.130.24	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
65.39.201.30	147.237.0.19	United States	madim.atal.idf.i	ET SCAN Potential SSH Scan	1
2.53.171.207	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.88.208.193	147.237.77.205	Russian Federation	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
180.97.106.37	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
163.172.129.15	147.237.77.19	United Kingdom	law-forum.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
163.172.67.13	147.237.76.200	United Kingdom	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
80.246.136.18	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
50.116.123.135	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
208.80.155.222	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	1

09-08-2016-19:04:07 to 09-08-2016-20:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
87.70.30.37	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	42
87.70.30.37	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	41
192.99.207.133	Canada	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	38
192.99.207.133	Canada	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	37
192.99.207.133	Canada	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	37
192.99.207.133	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	37
192.99.207.133	Canada	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	37
192.99.207.133	Canada	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	37
192.99.207.133	Canada	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	37
192.99.207.133	Canada	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	37
89.139.99.79	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
23.94.253.34	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
23.94.253.34	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
23.94.253.34	United States	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
23.94.253.34	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
23.94.253.34	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
23.94.253.34	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
23.94.253.34	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
23.94.253.34	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
87.69.52.204	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
87.69.52.204	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
37.26.147.209	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	12
217.132.174.73	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	10
195.60.235.58	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
62.205.40.58	Greece	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
132.66.236.114	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
176.13.9.129	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
66.249.93.83	Europe	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	7
66.249.93.85	Europe	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
66.249.93.85	Europe	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.192	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.147.209	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.65.55.126	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
41.13.212.81	South Africa	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
66.249.93.87	Europe	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	6
94.230.86.21	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.26.147.209	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
176.13.9.129	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.9	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.125	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
66.249.93.85	Europe	147.237.77.216	dover.idf.il	drop		drop	5
46.19.85.123	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.9	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.125	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.123	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
87.69.148.128	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
109.67.219.223	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
185.87.183.52	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	4
212.199.11.136	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
54.201.145.11	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4

09-08-2016-19:04:07 to 09-08-2016-20:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.136.231	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	134
192.114.1.155	Israel	147.237.77.74	law.idf.il	Distributed Unauthorized HTTP Method	Block	22
121.9.142.113	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 121.9.142.113	Block	17
192.114.1.155	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 192.114.1.155	Block	13
109.66.15.22	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	6
176.13.233.8	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
121.9.142.113	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	6
109.253.221.121	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.230.77	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
80.178.204.97	Israel	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	2
84.108.105.46	Israel	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	2
2.53.45.49	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
81.218.203.154	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
80.246.136.81	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
213.57.142.174	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	2
77.139.58.63	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
54.164.206.82	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;docId in www.aka.idf.il/brothers/skira/default.asp	None	1
82.80.170.97	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
192.114.1.155	Israel	147.237.77.74	law.idf.il	Multiple signatures from 192.114.1.155	Block	1
66.249.64.228	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/724-4483-he/patzar.aspx	Block	1
91.120.14.98	Hungary	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
31.168.208.38	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/	None	1
80.246.136.181	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 80.246.136.181	Block	1
79.176.146.28	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.253.214.12	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/tfasim.aspx	Block	1
66.249.64.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
80.178.204.97	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/7/	Block	1
192.115.116.26	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/images/shared/gray_tri_down.gif	Block	1
66.249.93.85	Israel	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../../images/infocenteritem/browser.png	Block	1
94.230.86.155	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
46.19.85.153	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	1
80.246.136.231	Israel	147.237.0.19	madim.atal.idf.i	Cookie Tampering on cookie Login: Expected ********** ********** ********** ****, Observed ********** ********** **********	None	1
185.120.126.33	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.180.119.89	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/https:/www.aman.idf.il/	Block	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
84.109.113.192	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
80.178.208.189	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
212.199.11.136	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
68.180.228.94	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/general/youtu.be/dsh2chqxxt0	Block	1
121.9.142.113	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.asp	Block	1
109.64.29.108	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
46.19.85.153	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method mluz45 in URL	Block	1
79.183.28.8	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.220	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/321-en/patzar.aspx	Block	1
113.68.161.150	China	147.237.77.74	law.idf.il	PHP Attempt	Block	1
5.102.242.175	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
89.139.156.38	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
80.188.7.84	Czech Republic	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
213.8.204.32	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
132.66.236.114	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1

09-08-2016-19:04:07 to 09-08-2016-20:04:07