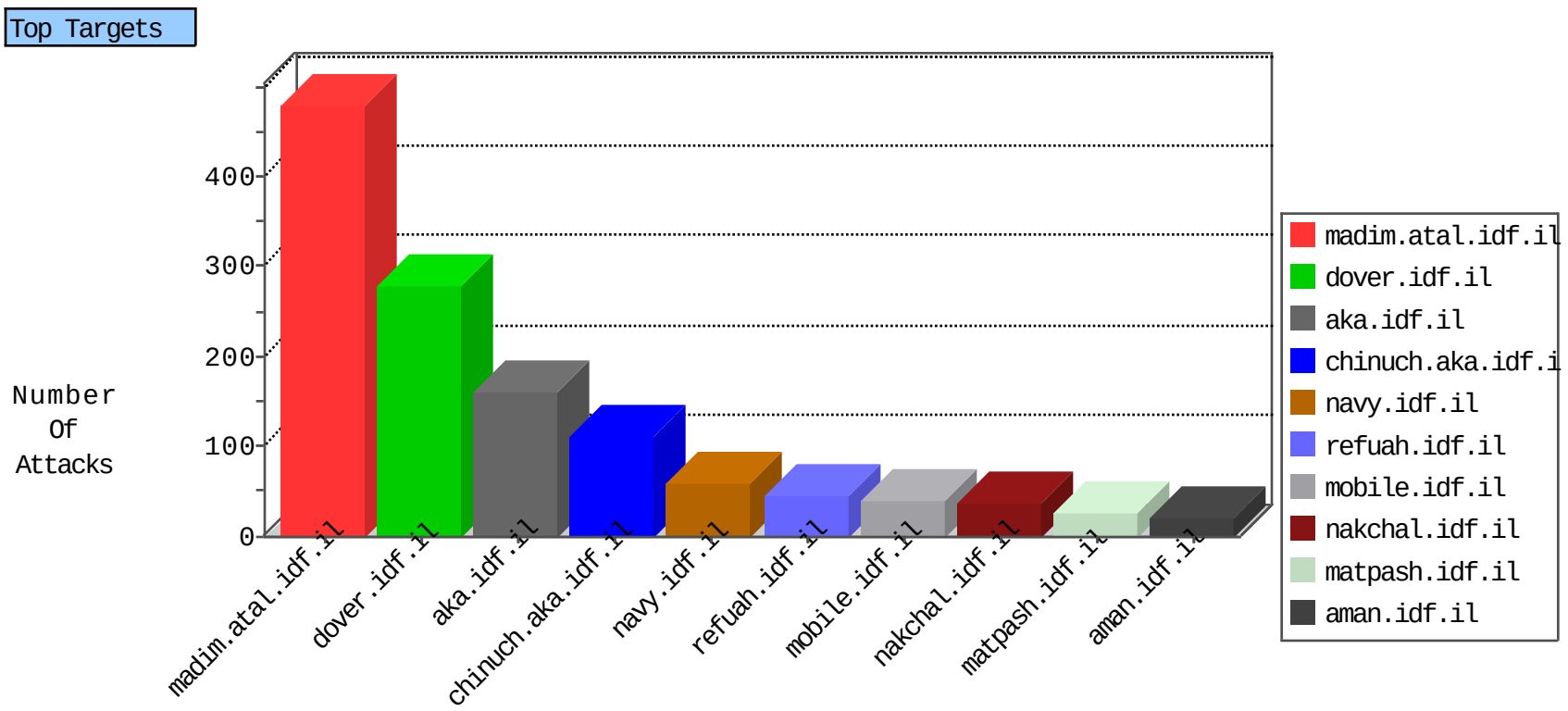
09-27-2016-10:04:05 to 09-27-2016-11:04:05

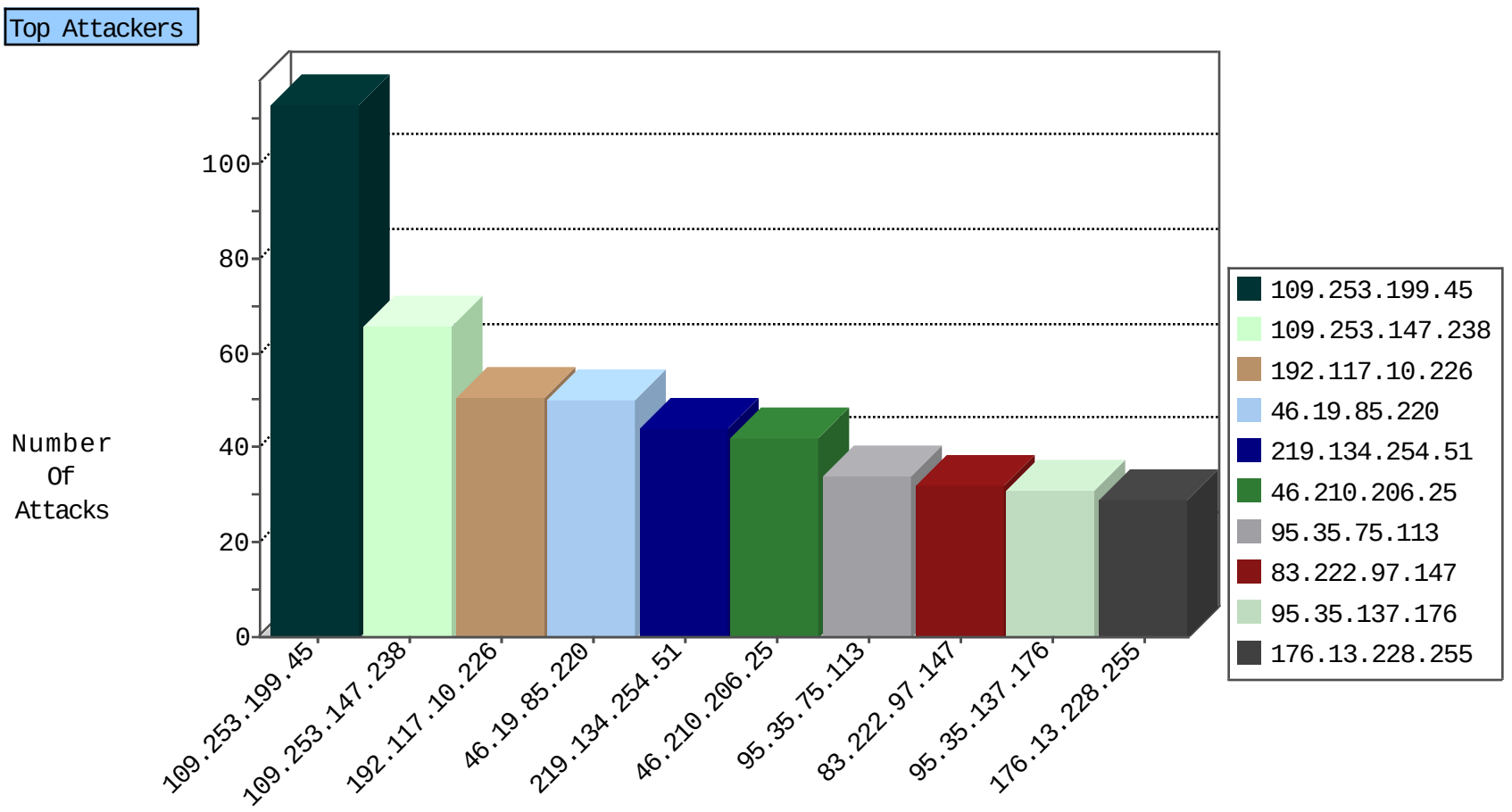
IDF Under Attack
Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

09-27-2016-10:04:05 to 09-27-2016-11:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.117.10.226	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	36
50.87.144.145	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
176.13.8.66	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
104.238.147.149	United States	147.237.76.202	e.halag.idf.il	Black List	drop	1
45.32.197.166	Netherlands	147.237.76.196	e.sviva.idf.il	Black List	drop	1

09-27-2016-10:04:05 to 09-27-2016-11:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-27-2016-10:04:05 to 09-27-2016-11:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
37.220.31.10	147.237.77.226	United Kingdom	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	2
46.19.86.43	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.201	147.237.8.14	Ukraine	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.235	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.201	147.237.0.19	Ukraine	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
40.121.139.43	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
176.13.3.63	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
124.8.223.198	147.237.76.177	Taiwan	ncore.idf.il	ET SCAN Potential SSH Scan	1
2.53.186.99	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.170.68.2	147.237.76.199	Russian Federation	e.nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
124.8.223.198	147.237.76.39	Taiwan	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.26.15	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
112.217.150.112	147.237.77.216	Korea, Republic of	dover.idf.il	ET SCAN Potential SSH Scan	1
188.120.154.165	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.95.133.30	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.201	147.237.77.74	Ukraine	law.idf.il	ET SCAN Potential SSH Scan	1
62.0.1.82	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.201	147.237.76.31	Ukraine	nakchal.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.25	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.201	147.237.0.34	Ukraine	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.104	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.228.184.8	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
40.121.139.43	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
124.8.223.198	147.237.76.196	Taiwan	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
37.26.148.211	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
124.8.223.198	147.237.76.44	Taiwan	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
2.53.26.207	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.170.68.2	147.237.76.199	Russian Federation	e.nakchal.idf.il	ET SCAN NMAP -f -sS	1
124.8.223.198	147.237.0.16	Taiwan	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
194.114.146.227	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.219.31	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.129.148.230	147.237.77.233	Latvia	atal.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.64.141	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
185.110.132.201	147.237.76.38	Ukraine	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1

09-27-2016-10:04:05 to 09-27-2016-11:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.53.177.12	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
141.0.13.203	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	18
95.35.145.13	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
2.53.141.237	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	15
46.19.85.170	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
192.115.83.5	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
192.117.10.226	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.86.93	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
31.154.14.46	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
84.109.180.20	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
80.246.137.223	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
83.222.97.147	Russian Federation	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
46.105.213.15	France	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	8
46.105.213.15	France	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
83.222.97.147	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	8
62.0.200.213	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.190	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.105.213.15	France	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	6
66.249.88.25	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.0.207.1	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.190	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.211	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.64.153.253	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.211	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
83.222.97.147	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	6
46.19.86.161	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.220	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
77.139.253.136	France	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
192.117.10.226	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
83.222.97.147	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
66.249.76.67	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.220	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.177	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.86	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
90.189.192.217	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	5
46.19.85.170	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.250	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.177	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.86	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.250	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.121	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.115.83.5	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
77.139.253.136	France	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
90.189.192.217	Russian Federation	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
83.222.97.147	Russian Federation	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
46.19.85.229	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.86.24	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
90.189.192.217	Russian Federation	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4

09-27-2016-10:04:05 to 09-27-2016-11:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.199.45	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	113
109.253.147.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	66
46.210.206.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	42
46.19.85.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	38
95.35.75.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	34
95.35.137.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31
176.13.228.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
37.26.148.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
176.13.238.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
46.19.86.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	17
219.134.254.51	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 219.134.254.51	Block	16
219.134.254.51	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 219.134.254.51	Block	16
37.26.146.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
109.253.159.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
212.235.23.119	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	8
219.134.254.51	China	147.237.77.176	matpash.idf.il	PHP Attempt	Block	6
176.13.14.0	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
212.235.23.119	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 212.235.23.119	Block	5
219.134.254.51	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	5
212.179.46.50	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.179.46.50	Block	4
109.253.220.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
46.19.86.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
31.168.23.59	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.168.23.59	Block	3
46.19.86.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.154.19.5	Block	3
46.19.86.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
31.168.65.160	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	3
2.53.135.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.148.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
31.168.65.160	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/sip_storage/files/2/	Block	2
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.224	Block	2
84.95.208.20	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
37.26.146.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
165.72.200.11	Europe	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar	Block	2
77.138.247.44	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar	Block	2
109.253.134.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	2
31.154.19.5	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 31.154.19.5	Block	2
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.i	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
194.27.242.254	Turkey	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/	Block	2
66.102.9.5	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
212.25.102.63	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl51 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
84.95.208.20	Israel	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
46.19.85.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
176.13.236.49	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
79.181.222.192	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/home/def	Block	1
2.55.162.74	Israel	147.237.72.166	aka.idf.il	Unknown Parameter utm_medium in www.aka.idf.il/giyus	None	1
194.90.15.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl50.x in www.aka.idf.il/main/sachar/payslips.aspx	None	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1

09-27-2016-10:04:05 to 09-27-2016-11:04:05