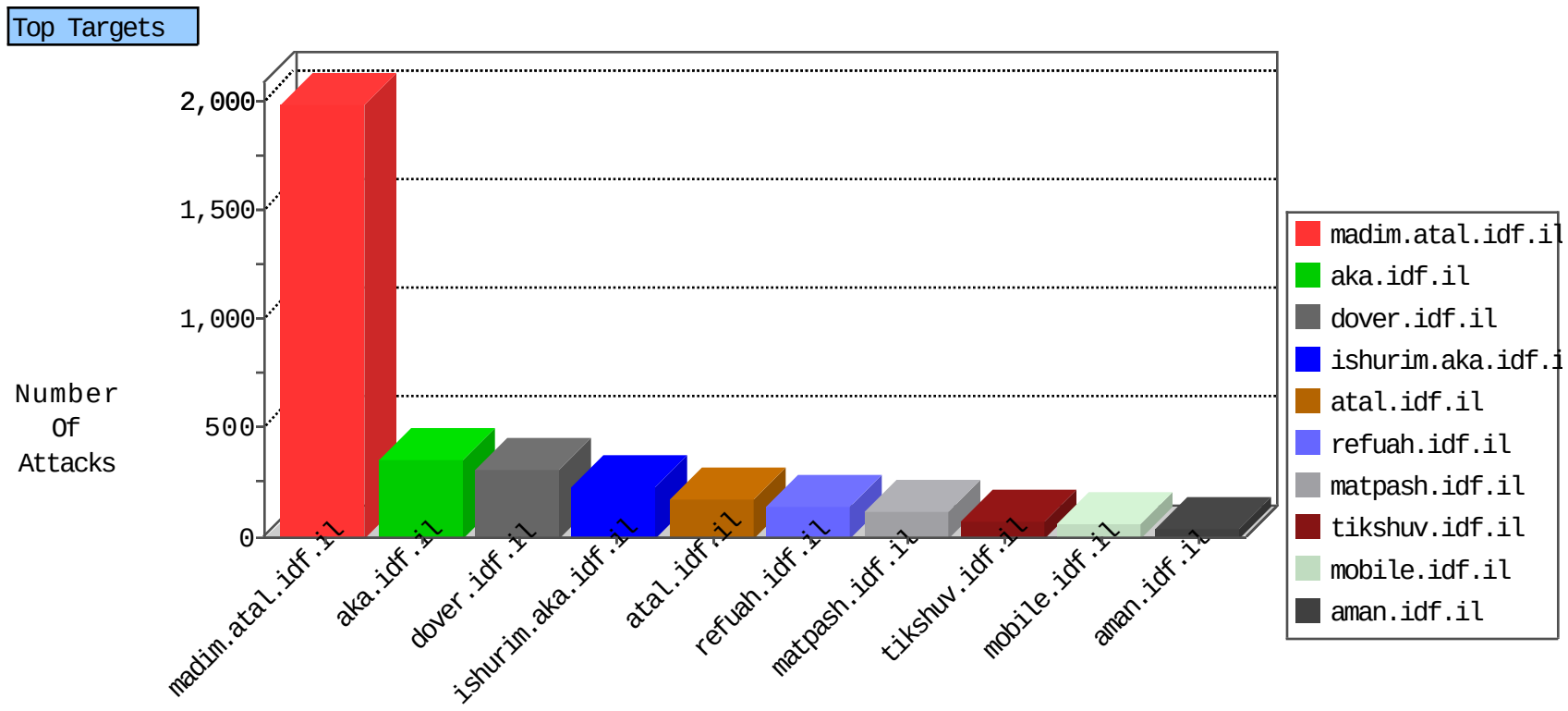
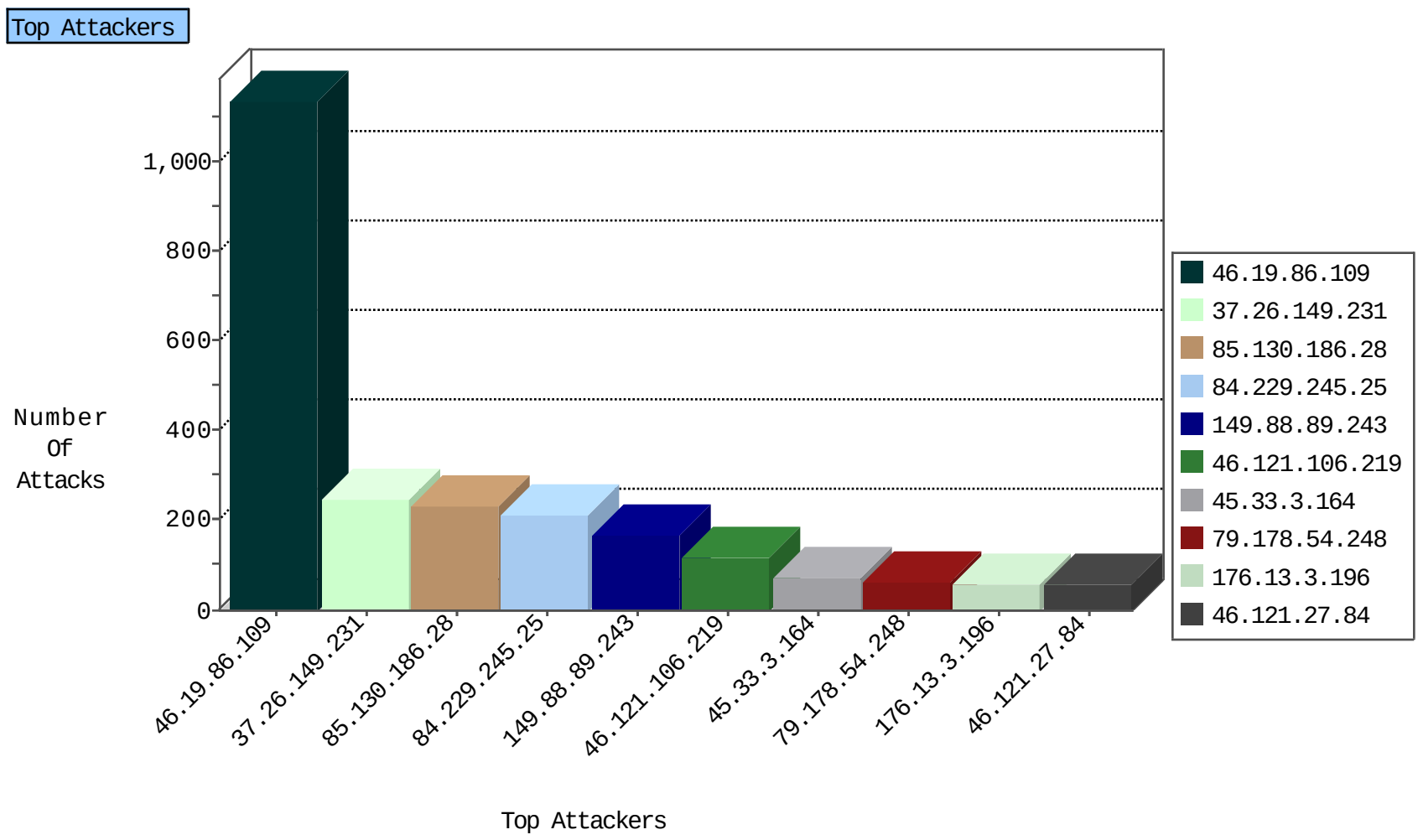
02-03-2016-20:04:00 to 02-03-2016-21:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-03-2016-20:04:00 to 02-03-2016-21:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	4
115.230.124.164	China	147.237.76.38	e.e.meitav.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
142.54.160.214	United States	147.237.77.233	atal.idf.il	block-sp-traf1	drop	1
142.54.169.162	United States	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	1

02-03-2016-20:04:00 to 02-03-2016-21:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-03-2016-20:04:00 to 02-03-2016-21:04:00

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	5
66.249.81.227	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	2
208.80.155.224	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	1
46.166.129.183	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN NMAP -sS window 4096	1
190.10.9.246	147.237.77.19	Costa Rica	law-forum.idf.il	ET SCAN NMAP -sS window 4096	1
46.166.129.183	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN NMAP -f -sS	1
189.219.192.237	147.237.77.235	Mexico	sviva.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.117.109.142	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
177.245.75.13	147.237.77.235	Mexico	sviva.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
5.102.226.4	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
112.196.49.101	147.237.76.42	India	refuah.idf.il	ET SCAN NMAP -sS window 2048	1
112.196.49.101	147.237.76.42	India	refuah.idf.il	ET SCAN NMAP -f -sS	1
84.109.116.104	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.183.150.193	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.78.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
46.166.129.183	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN NMAP -sS window 2048	1
190.10.9.246	147.237.77.19	Costa Rica	law-forum.idf.il	ET SCAN NMAP -sS window 3072	1
46.121.248.248	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
189.219.192.237	147.237.77.216	Mexico	dover.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
5.189.176.80	147.237.72.156	Germany	aman.idf.il	ET WEB_SERVER PHP Crawler	1
149.78.32.224	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.29.140.27	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
112.196.49.101	147.237.76.42	India	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
104.128.144.131	147.237.76.44	Canada	e.refuah.idf.il	ET SCAN NMAP -sS window 3072	1
84.94.90.222	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
216.177.129.96	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1

02-03-2016-20:04:00 to 02-03-2016-21:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
149.88.89.243	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	164
85.130.186.28	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
46.121.27.84	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	55
82.166.247.138	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	38
85.130.186.28	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	32
85.130.186.28	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	31
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
207.243.51.246	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	26
45.33.3.164		147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	26
79.180.206.212	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
45.33.3.164		147.237.77.176	matpash.idf.il	drop		drop	19
46.19.86.239	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
45.33.3.164		147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
93.173.235.199	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.59.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
45.33.3.164		147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
85.64.55.174	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.131.77	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.148.235	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
37.26.146.160	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
149.78.32.224	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
46.19.85.97	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
85.130.175.28	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
85.130.175.28	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
85.130.175.28	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.85.1	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	7
188.120.148.124	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.31	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.19.55	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.120	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.46.39.95	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.127.161.100	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
85.130.218.128	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.56	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
85.130.218.128	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.56	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.1	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.253.223.64	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
79.178.100.166	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.56	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.31	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.182.38.61	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.120	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.56	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
85.130.218.128	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	6
79.183.13.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.130.253	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
129.171.6.44	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.109	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	702
46.19.86.109	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	283
37.26.149.231	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	173
46.19.86.109	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 46.19.86.109	Block	151
84.229.245.25	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	148
46.121.106.219	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	69
37.26.149.231	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	69
84.229.245.25	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	65
79.178.54.248	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	62
176.13.3.196	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	55
149.78.136.43	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	45
46.121.106.219	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	38
82.80.17.163	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	30
80.246.139.139	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 80.246.139.139	Block	27
37.142.68.133	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	20
87.68.52.18	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	19
5.29.212.105	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
37.26.148.186	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
46.121.106.219	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.121.106.219	Block	10
5.34.161.100	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 5.34.161.100	Block	7
46.19.86.81	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
85.64.55.174	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
5.29.110.197	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
46.19.86.239	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
80.246.133.50	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/size100x0/sip_storage	Block	4
109.253.131.77	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
5.34.161.100	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	4
37.26.149.159	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
84.108.211.143	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	3
37.26.149.159	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	3
79.176.35.241	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.185.172	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.85.157	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.85.66	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
213.57.136.46	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.19.86.248	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$35 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
79.176.6.253	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$7 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
149.88.234.231	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.65.3.52	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$83 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
2.54.129.42	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$11 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
2.54.3.246	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl02$ctl03$txtField in aka.idf.il/main/giyus/questionnaire.aspx	None	2
31.210.187.250	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$67 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
82.166.247.138	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
46.120.91.42	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.66.57.146	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
5.29.101.135	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
79.183.37.137	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl02$ctl03$txtField in aka.idf.il/main/giyus/questionnaire.aspx	None	1
213.8.204.7	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$67 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
46.19.86.72	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$103 in aka.idf.il/main/giyus/questionnaire.aspx	None	1