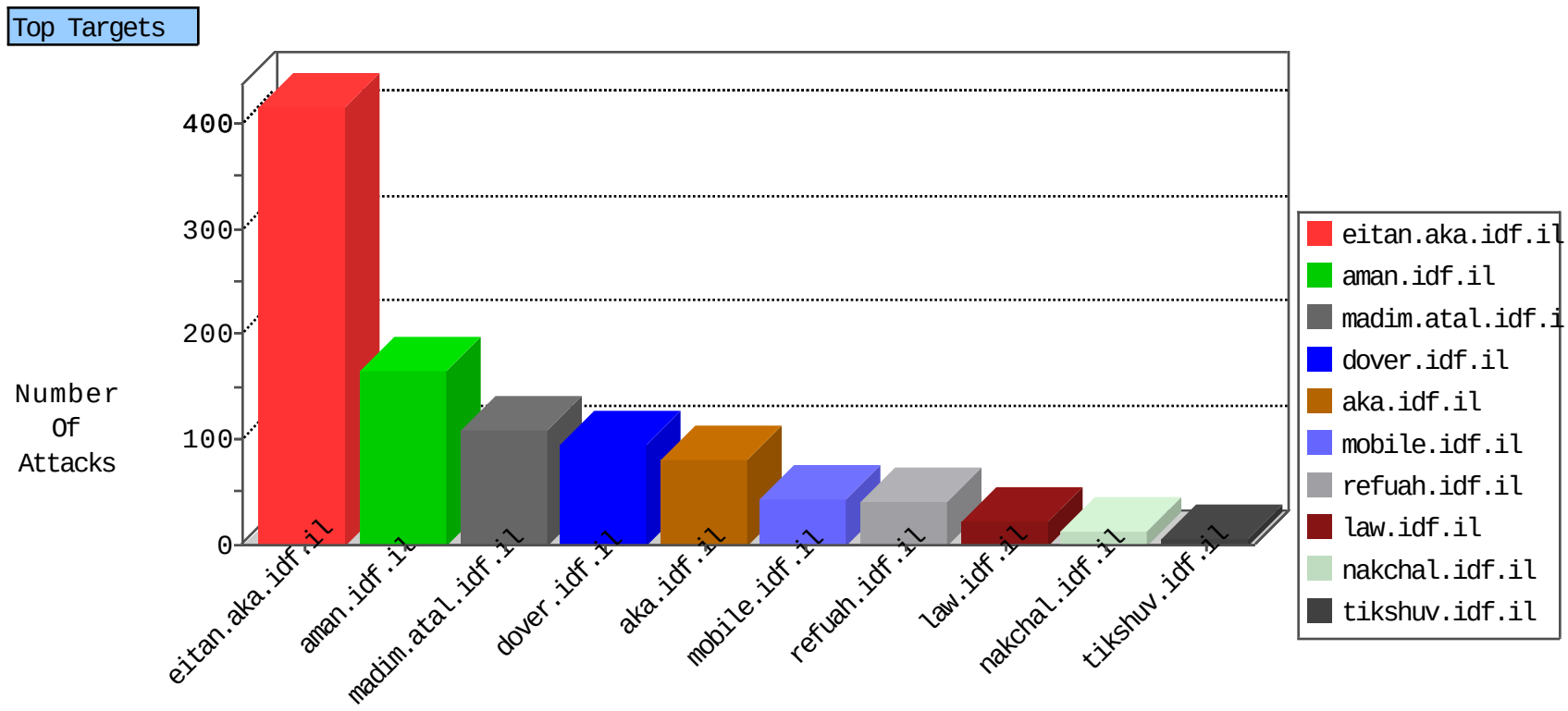
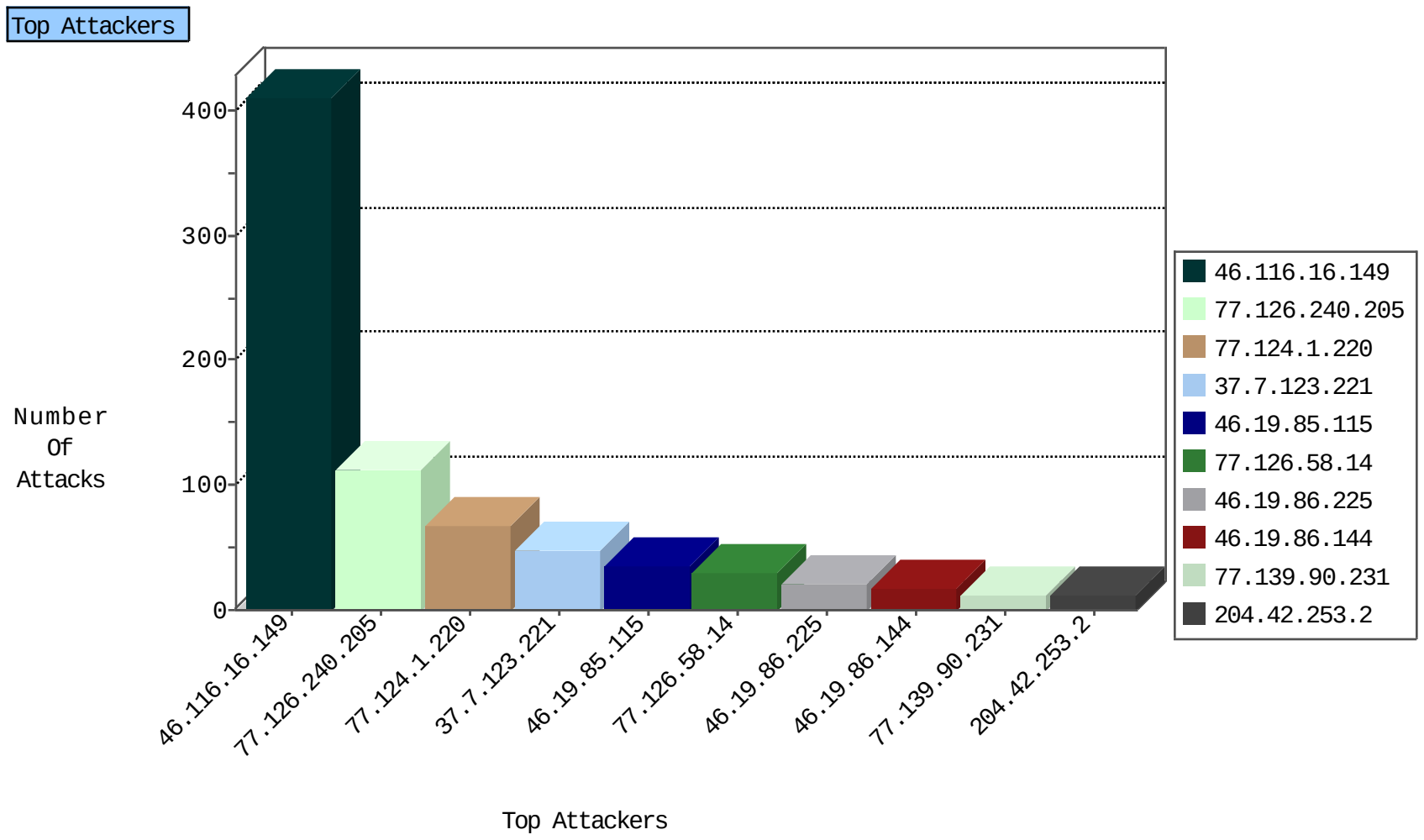
09-23-2016-13:04:07 to 09-23-2016-14:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-23-2016-13:04:07 to 09-23-2016-14:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.109.92.217	Israel	147.237.77.216	dover.idf.il	Black List	drop	2
204.42.253.2	United States	147.237.76.200	eitan.aka.idf.il	Black List	drop	2
204.42.253.2	United States	147.237.76.197	e.himush.idf.il	Black List	drop	2
204.42.253.2	United States	147.237.76.201	e.atal.idf.il	Black List	drop	2
204.42.253.2	United States	147.237.76.198	e.yohalan.idf.il	Black List	drop	2
204.42.253.2	United States	147.237.76.202	e.halag.idf.il	Black List	drop	2
204.42.253.2	United States	147.237.76.199	e.nakchal.idf.il	Black List	drop	2

09-23-2016-13:04:07 to 09-23-2016-14:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
51.254.131.244	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

09-23-2016-13:04:07 to 09-23-2016-14:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
163.172.129.15	147.237.76.34	United Kingdom	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
128.232.110.28	147.237.76.38	United Kingdom	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
109.60.153.178	147.237.72.217	Russian Federation	e.idf.il	ET SCAN NMAP -sS window 1024	1
77.126.240.205	147.237.72.166	Israel	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
46.116.14.127	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
211.149.240.243	147.237.76.44	China	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
36.72.228.72	147.237.76.147	Indonesia	chinuch.aka.idf.il	ET SCAN NMAP -sS window 2048	1
210.212.207.80	147.237.76.44	India	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
210.212.207.80	147.237.0.35	India	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.129.15	147.237.76.176	United Kingdom	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
139.162.187.89	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
121.46.102.78	147.237.72.156	India	aman.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
93.174.93.210	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.64.124	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
216.218.206.99	147.237.77.176	United States	matpash.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potentia Scan or Infection	1
36.72.228.72	147.237.76.147	Indonesia	chinuch.aka.idf.il	ET SCAN NMAP -sS window 4096	1
211.149.240.243	147.237.76.42	China	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
36.72.228.72	147.237.76.147	Indonesia	chinuch.aka.idf.il	ET SCAN NMAP -f -sS	1
210.212.207.80	147.237.76.44	India	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.169.150	147.237.76.42	United Kingdom	refuah.idf.il	ET SCAN NMAP -sS window 1024	1

09-23-2016-13:04:07 to 09-23-2016-14:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
46.116.16.149	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	412
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	91
77.126.58.14	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
46.19.85.115	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.19.86.225	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.19.85.115	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
37.7.123.221	Poland	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
176.13.227.155	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.115	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
46.19.86.144	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
109.253.217.92	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
37.7.123.221	Poland	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.7.123.221	Poland	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
37.7.123.221	Poland	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
46.19.85.115	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.115	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.7.123.221	Poland	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
37.7.123.221	Poland	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.156	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
31.168.133.168	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.144	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.225	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
37.142.217.2	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.86.144	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.249	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
84.108.184.95	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
37.7.123.221	Poland	147.237.72.156	aman.idf.il	SYN Attack		monitor	4
193.191.219.80	Belgium	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.7.123.221	Poland	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	4
59.99.21.125	India	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
109.253.193.33	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.85.71	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.225	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.161	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.253.218.131	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
59.99.21.125	India	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
46.19.85.83	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.29	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
37.26.148.144	Israel	147.237.0.19	madim.atal.idf.i	Bad TCP sequence		alert	2
37.26.149.232	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
109.253.143.144	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
31.154.7.4	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
82.81.39.225	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
213.57.236.167	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
37.26.148.144	Israel	147.237.0.19	madim.atal.idf.i	Bad TCP sequence		monitor	2
46.19.86.19	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
84.109.112.207	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

09-23-2016-13:04:07 to 09-23-2016-14:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.124.1.220	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	67
77.139.90.231	France	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
37.26.148.144	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
109.253.158.19	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
77.138.140.185	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	3
80.246.138.99	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.148.168	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
37.26.148.192	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
37.26.148.216	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
37.26.147.205	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
37.26.148.240	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
31.44.132.40	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/https:/www.aman.idf.il/	Block	1
77.126.240.205	Israel	147.237.72.166	aka.idf.il	Malformed URL	Block	1
77.126.240.205	Israel	147.237.72.156	aman.idf.il	NULL Character in Header Name at üžƒ}„[[#20]]+13õ]wQYÿ]à¤È𹕠(ÝMâZ7V	Block	1
66.249.76.70	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/robots.txt	Block	1
77.126.240.205	Israel	147.237.72.166	aka.idf.il	Abnormally Long Request method	Block	1
207.46.13.86	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/wut	Block	1
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Illegal Byte Code Character in Header Value	Block	1
66.249.64.166	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/.well-known/assetlinks.json	Block	1
31.154.7.4	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
77.126.240.205	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 77.126.240.205 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
77.126.240.205	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
118.201.50.146	Singapore	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
77.126.240.205	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name	Block	1
207.46.13.123	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush	Block	1
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Illegal Byte Code Character in Method zJ53Ÿ6ÄÌ°DÓfWÜ¿¯2ˆ”gâ[[#24]]h%úñÖL%-¨Í`ƒ,W	Block	1
84.108.184.95	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.66.182	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/2827.jpg	Block	1
37.26.146.165	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
77.126.240.205	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Too Many Headers per Request - 30 Headers	Block	1
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Abnormally Long Header Line request header name	Block	1
157.55.39.28	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/templates/oprolescategory/oprolescategory.in.aspx	Block	1
77.139.208.69	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/miyun/miyunderugtafkidim.aspx	Block	1
77.126.240.205	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Method CÎþJð•[[#24]]˜óØT²“}[[#24]]CYÞ[[#14]]"V¥¡Œ¹Ki†Ÿø	Block	1
216.244.66.236	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation docId in tikshuv.idf.il/site/story.aspx	Block	1
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Malformed HTTP Header Line 10	Block	1
85.64.117.153	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl25 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.73.172	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-he	Block	1
77.126.240.205	Israel	147.237.72.166	aka.idf.il	Unknown HTTP Request Method CÎþJð•[[#24]]˜óØT²“}[[#24]]CYÞ[[#14]]"V¥¡Œ¹Ki†Ÿø in URL	Block	1
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Unknown HTTP Request Method zJ53Ÿ6ÄÌ°DÓfWÜ¿¯2ˆ”gâ[[#24]]h%úñÖL%-¨Í`ƒ,W in URL	Block	1
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Abnormally Long Request method	Block	1
157.55.39.159	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/edim/fund/„'ƒ„'„,¬„¯„ƒ‚€Š„,¬¿„ƒ„'½„,„Š€‚ƒ„'§'½„,„Š€‚ƒ„'„,¬„¯„ƒ‚€Š„,¬¿„ƒ„'½„,„Š€‚ƒ„'„,¬„¯„ƒ‚€Š„,¬¿„ƒ‚€Š„,¬½	Block	1
77.249.173.146	Netherlands	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/miyun/miyunsummary.aspx	Block	1
77.126.240.205	Israel	147.237.72.166	aka.idf.il	Malformed HTTP Header Line 1	Block	1
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Malformed URL	Block	1
66.249.76.30	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.76.30	Block	1
89.248.167.131	Netherlands	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to 147.237.0.19/robots.txt	Block	1
77.138.26.183	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/	Block	1
77.126.240.205	Israel	147.237.72.166	aka.idf.il	Abnormally Long Header Line request header name	Block	1

09-23-2016-13:04:07 to 09-23-2016-14:04:07