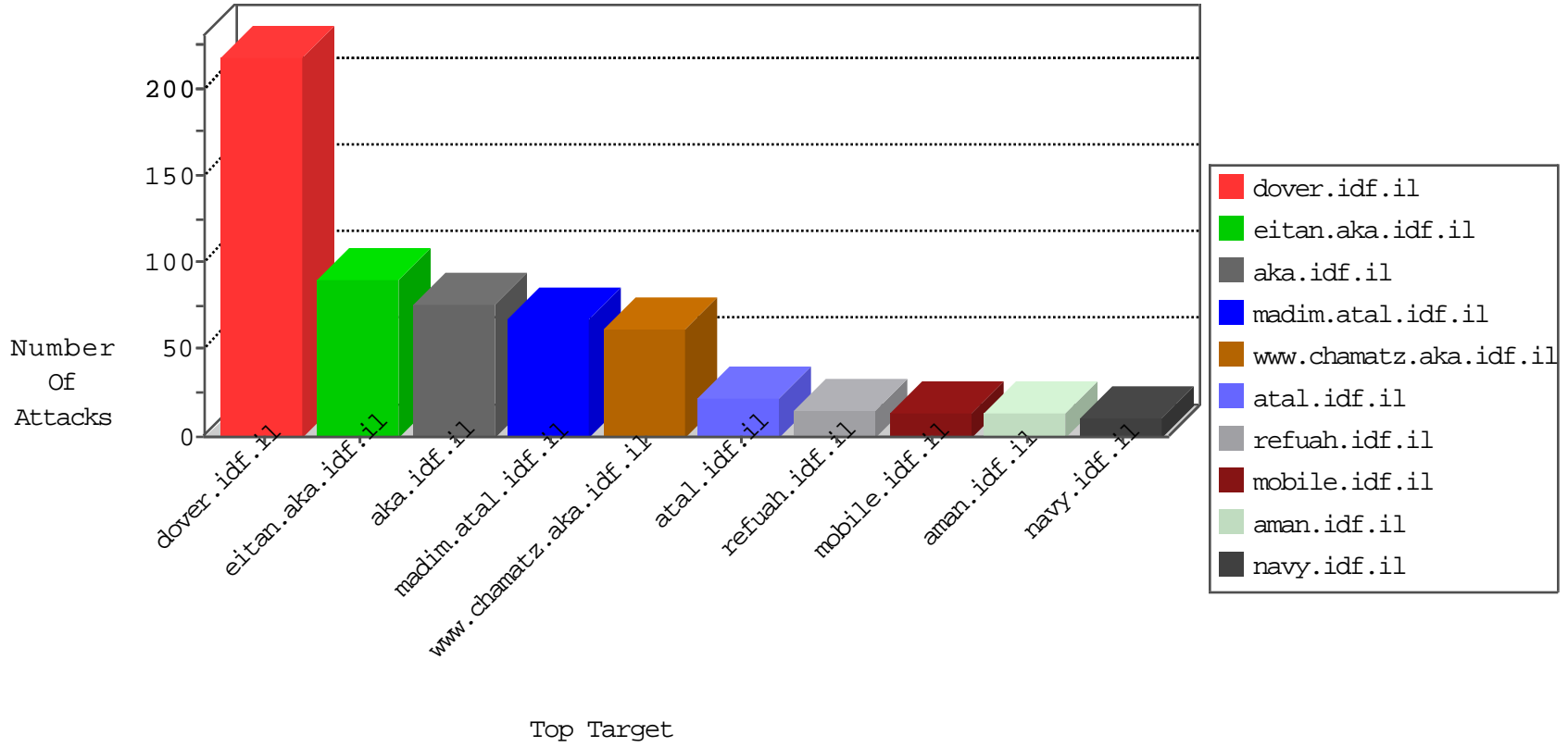


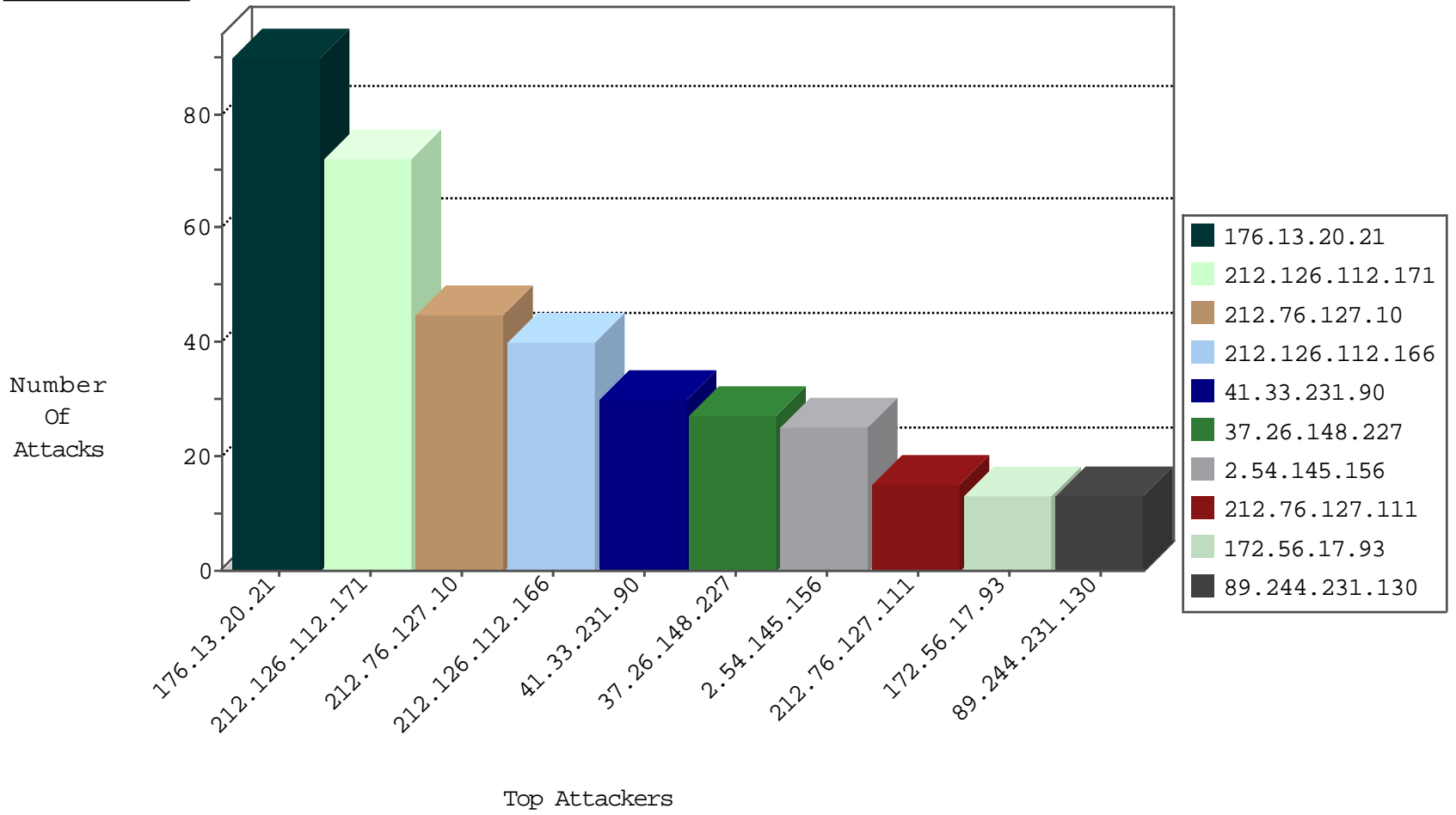
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.126.112.171	Iraq	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	18
212.126.112.171	Iraq	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	14
213.93.183.129	Netherlands	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
74.91.28.61	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-trafl	drop	1
142.54.160.211	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-trafl	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
83.246.206.218	Russian Federation	147.237.8.46	e.chinuch.idf.i	13891: TLS: OpenSSL Encrypted/Unencrypted Heartbeat Packet	Permit	1

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	4
89.244.231.130	147.237.77.74	Germany	law.idf.il	ET SCAN Potential SSH Scan	2
66.249.69.77	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	2
54.67.38.74	147.237.76.38	United States	e.e.meitav.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
172.56.17.93	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
89.244.231.130	147.237.76.148	Germany	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
89.244.231.130	147.237.76.31	Germany	nakchal.idf.il	ET SCAN Potential SSH Scan	1
89.244.231.130	147.237.72.156	Germany	aman.idf.il	ET SCAN Potential SSH Scan	1
89.244.231.130	147.237.0.200	Germany	m4u.idf.il	ET SCAN Potential SSH Scan	1
89.244.231.130	147.237.0.15	Germany	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
208.67.1.25	147.237.72.14	United States	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
89.244.231.130	147.237.77.178	Germany	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
89.244.231.130	147.237.76.176	Germany	test.noore.idf.il	ET SCAN Potential SSH Scan	1
89.244.231.130	147.237.76.39	Germany	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
89.244.231.130	147.237.72.167	Germany	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
89.244.231.130	147.237.8.24	Germany	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
89.244.231.130	147.237.0.16	Germany	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
85.93.5.65	147.237.77.19	Germany	law-forum.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.74	147.237.76.198	United States	e.yohanan.idf.il	ET DROP Dshield Block Listed Source	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
176.13.20.21	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
212.126.112.166	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
212.76.127.10	Israel	147.237.77.226	www.chamatz.aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	36
212.126.112.171	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
212.76.127.111	Israel	147.237.77.226	www.chamatz.aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	15
176.13.4.235	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.76.127.10	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
109.65.136.30	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.37	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
172.56.17.93	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.0.197.205	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.5	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.5	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
41.254.8.23	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
212.126.112.171	Iraq	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
80.215.167.183	France	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
202.171.186.156	Australia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.245	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.177.116.32	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.211.169	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.211	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.31.75	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.48.244	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
212.76.127.44	Israel	147.237.77.226	www.chamatz.aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
46.19.85.195	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.229.246.114	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.182.188.197	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.126.112.171	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.183.30.182	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.144.216	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
5.102.194.89	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.4.166	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.76.127.219	Israel	147.237.77.226	www.chamatz.aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
141.0.14.194	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
5.22.129.243	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.9	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.158	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
93.158.152.49	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.254.134	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
109.66.150.215	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
93.172.135.63	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
217.132.226.65	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.67	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
172.56.17.93	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
157.55.39.101	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.148.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
2.54.145.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
2.52.181.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
37.26.149.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.130.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.136.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
199.16.156.124	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/6/size220x0/16706.jpg	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	1
176.13.14.5	Israel	147.237.72.166	aka.idf.il	Unknown Parameter id in aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
66.249.78.58	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/3/105893.pdf	Block	1
199.16.156.126	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/sip_storage/files/3/size220x0/15933.jpg	Block	1
94.230.86.213	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1415	Block	1
2.54.142.44	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/960.css	Block	1
188.143.232.40	Russian Federation	147.237.77.176	matpash.idf.il	Parameter Type Violation fromDate in www.cogat.idf.il/901-en/cogat.aspx	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
37.26.149.211	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
199.59.148.210	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/sip_storage/files/6/size220x0/16706.jpg	Block	1
66.249.66.23	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/994-9067-he/atal.aspx	Block	1
192.157.245.129	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/pricing	Block	1
80.179.190.242	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 80.179.190.242	Block	1
66.249.64.48	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/3/108503.pdf	Block	1
207.46.13.157	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19748-he/idfgdover.aspx	Block	1
157.55.39.75	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/modiin/default.aspx	Block	1
66.249.66.26	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
23.247.151.161	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	1
198.20.69.74	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
80.179.190.242	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/8/	Block	1
66.249.64.53	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/4/107734.pdf	Block	1
172.56.17.93	United States	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.78.51	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 66.249.78.51	Block	1