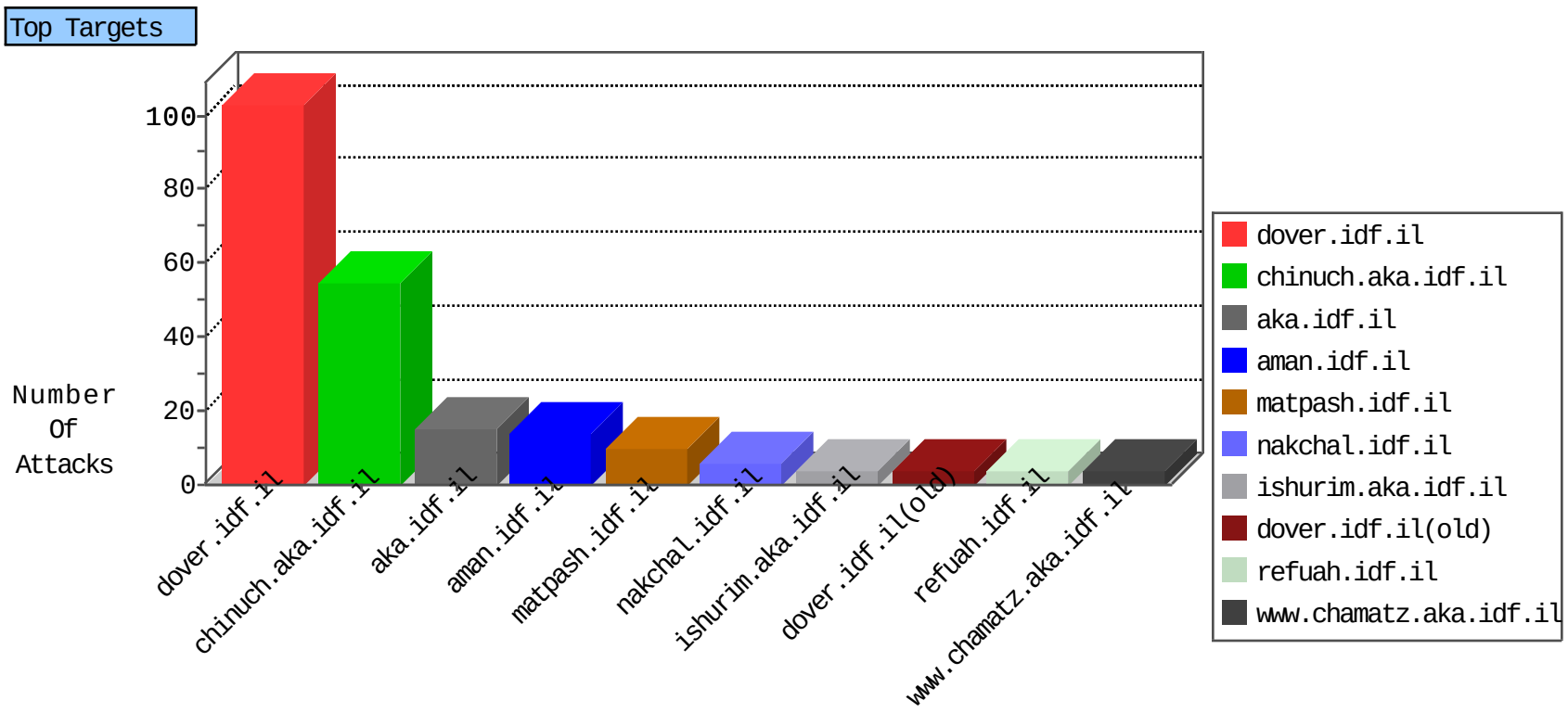
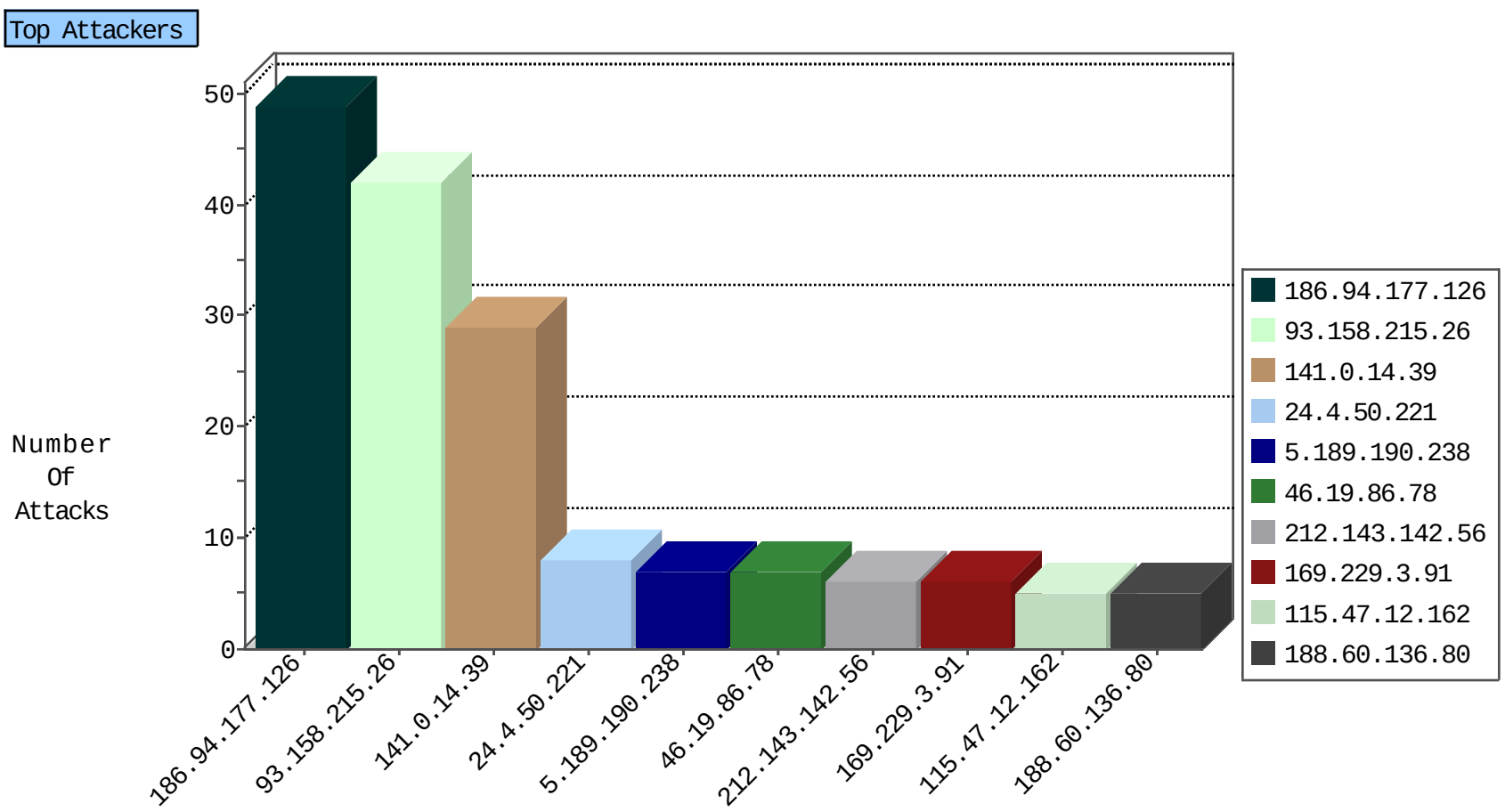
09-27-2016-02:04:05 to 09-27-2016-03:04:05

IDF Under Attack
Daily Report



Top Target



Top Attackers

09-27-2016-02:04:05 to 09-27-2016-03:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
45.32.205.113	Netherlands	147.237.76.177	ncore.idf.il	Black List	drop	1
45.32.199.242	Netherlands	147.237.76.44	e.refuah.idf.il	Black List	drop	1
104.238.147.65	United States	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1
45.32.200.117	Netherlands	147.237.76.176	test.ncore.idf.il	Black List	drop	1
45.32.204.130	Netherlands	147.237.76.34	yohalan.idf.il	Black List	drop	1

09-27-2016-02:04:05 to 09-27-2016-03:04:05

Top Attackers In IPS

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

09-27-2016-02:04:05 to 09-27-2016-03:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
109.75.43.41	147.237.72.14	Armenia	dover.idf.il(old)	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	3
198.252.110.108	147.237.77.212	United States	e.dover.idf.il	GPL SCAN superscan echo	1
125.65.82.44	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
196.47.173.21	147.237.76.34	Cote D'Ivoire	yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
115.47.12.162	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
196.47.173.21	147.237.76.34	Cote D'Ivoire	yohalan.idf.il	ET SCAN NMAP -f -sS	1
115.47.12.162	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
188.83.12.28	147.237.72.156	Portugal	aman.idf.il	ET SCAN Potential SSH Scan	1
179.43.144.18	147.237.77.176	Switzerland	matpash.idf.il	ET SCAN Potential SSH Scan	1
103.207.37.81	147.237.77.226	Vietnam	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
179.43.141.198	147.237.0.200	Switzerland	m4u.idf.il	ET SCAN Potential SSH Scan	1
78.129.171.173	147.237.76.197	United Kingdom	e.himush.idf.il	ET SCAN Potential SSH Scan	1
161.106.88.6	147.237.76.196	France	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
221.229.172.116	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
36.72.228.72	147.237.77.19	Indonesia	law-forum.idf.il	ET SCAN NMAP -sS window 2048	1
161.106.88.6	147.237.0.16	France	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
198.252.110.108	147.237.77.227	United States	e.hamaz.idf.il	GPL SCAN superscan echo	1
139.162.187.89	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
198.252.110.108	147.237.77.178	United States	e.matpash.idf.il	GPL SCAN superscan echo	1
115.47.12.162	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
196.47.173.21	147.237.76.34	Cote D'Ivoire	yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
115.47.12.162	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
188.83.12.28	147.237.72.166	Portugal	aka.idf.il	ET SCAN Potential SSH Scan	1
115.47.12.162	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
188.83.12.28	147.237.72.14	Portugal	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
108.250.76.145	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
179.43.144.18	147.237.76.38	Switzerland	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
93.174.164.92	147.237.76.30	Romania	himush.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
176.13.247.207	147.237.76.86	Israel	navy.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
221.229.172.116	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
36.72.228.72	147.237.77.19	Indonesia	law-forum.idf.il	ET SCAN NMAP -sS window 3072	1
161.106.88.6	147.237.76.177	France	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
220.121.222.101	147.237.76.196	Korea, Republic of	e.sviva.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
36.72.228.72	147.237.77.19	Indonesia	law-forum.idf.il	ET SCAN NMAP -f -sS	1
161.106.88.6	147.237.0.15	France	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1

09-27-2016-02:04:05 to 09-27-2016-03:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
93.158.215.26	Netherlands	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	42
141.0.14.39	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	29
186.94.177.126	Venezuela	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
186.94.177.126	Venezuela	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
186.94.177.126	Venezuela	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
186.94.177.126	Venezuela	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
186.94.177.126	Venezuela	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.86.78	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
186.94.177.126	Venezuela	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
109.253.193.222	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	3
24.4.50.221	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
79.176.73.99	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.53	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
24.4.50.221	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	2
79.176.73.99	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
2.55.47.224	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
24.4.50.221	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	2
157.55.39.21	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
79.181.208.112	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.85.195	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
169.229.3.91	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
24.4.50.221	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
141.212.122.165	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
5.189.190.238	Germany	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
207.46.13.106	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
66.108.189.205	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
46.19.85.53	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
169.229.3.91	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
5.189.190.238	Germany	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.162	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
2.53.151.38	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
89.248.172.16	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
188.60.136.80	Switzerland	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
46.19.86.78	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
169.229.3.91	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.165	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
5.189.190.238	Germany	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
109.253.211.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
5.189.190.238	Germany	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
141.212.122.163	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
2.53.175.175	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
188.60.136.80	Switzerland	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
176.13.4.116	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.172	United States	147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
5.189.190.238	Germany	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
138.246.253.19	Germany	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.85.126	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1

09-27-2016-02:04:05 to 09-27-2016-03:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.108.189.205	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en	Block	3
183.232.175.2	China	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/	Block	2
66.249.79.114	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/sip_storage/files/3/68633...	Block	1
24.251.42.207	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
89.248.172.16	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/robots.txt	Block	1
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	1
204.79.180.146	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/templates/home.asp	Block	1
66.249.79.122	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/mobile/	Block	1
46.120.25.138	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 46.120.25.138 (Open Mode)	None	1
138.201.140.208	Germany	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
66.249.75.4	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9180-he/refuah.aspx	Block	1
220.181.108.170	China	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/3/size338x0/1613.jpg	Block	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-he/dover.aspx	Block	1
157.55.39.21	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/main/haredim/general.aspx	None	1
66.249.75.8	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9023-he/refuah.aspx	Block	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/	Block	1
66.249.66.235	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.66.235	Block	1
180.76.15.144	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/960.css	Block	1
66.249.75.12	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 66.249.75.12	Block	1
89.138.98.163	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/size100x0/sip_storage	Block	1
66.249.66.243	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/31ms02082010.aspx	Block	1

09-27-2016-02:04:05 to 09-27-2016-03:04:05