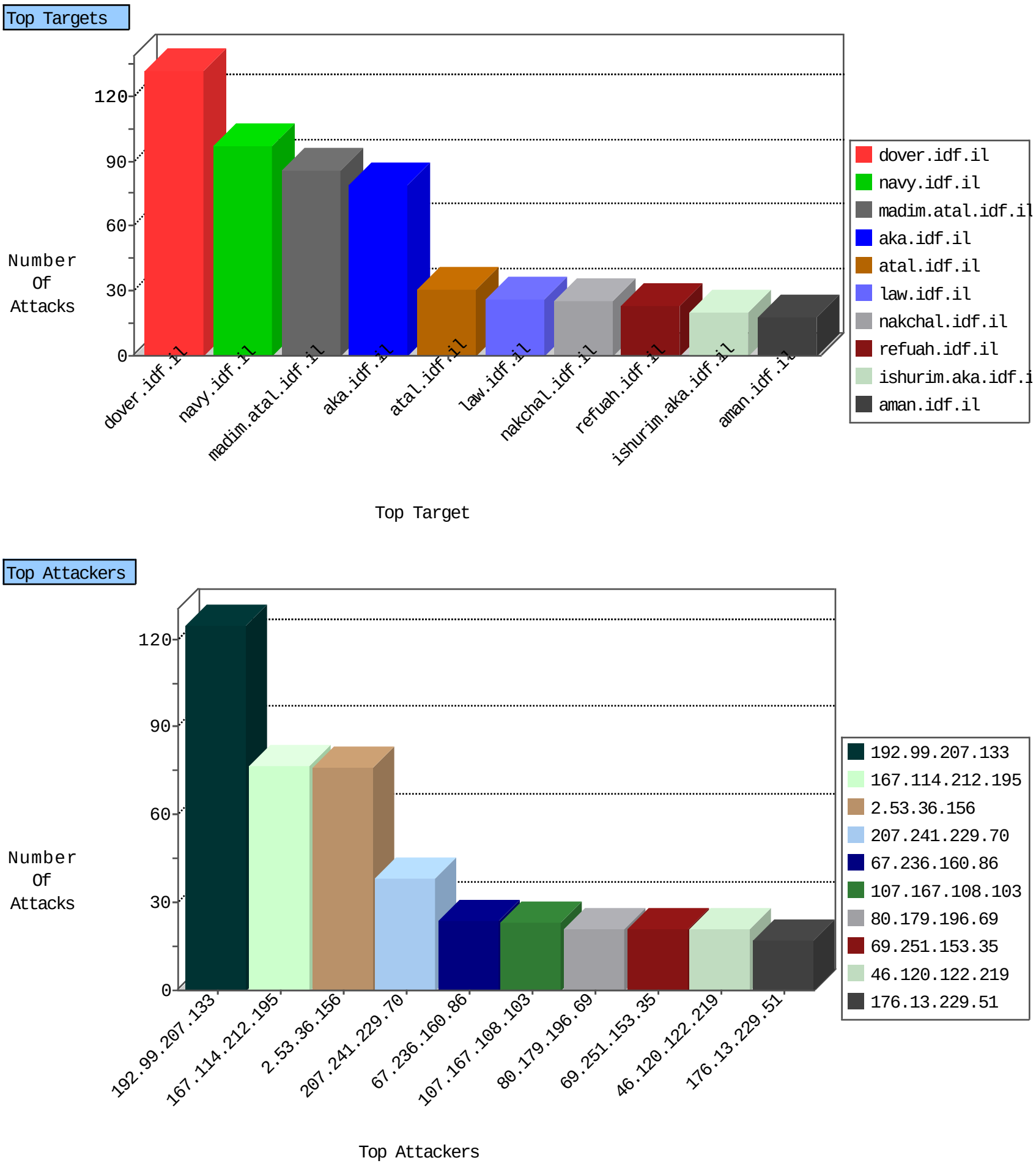
09-06-2016-00:04:02 to 09-06-2016-01:04:02

IDF Under Attack
Daily Report



09-06-2016-00:04:02 to 09-06-2016-01:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
95.86.69.203	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
89.248.168.21	Netherlands	147.237.76.42	refuah.idf.il	Black List	drop	1

09-06-2016-00:04:02 to 09-06-2016-01:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
216.68.91.180	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
162.210.196.130	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	4

09-06-2016-00:04:02 to 09-06-2016-01:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	14
216.68.91.180	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
41.128.185.15	147.237.72.156	Egypt	aman.idf.il	ET SCAN Potential SSH Scan	1
193.201.225.138	147.237.77.243	Ukraine	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
41.128.185.15	147.237.0.19	Egypt	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
178.20.188.164	147.237.72.167	Jordan	ishurim.aka.idf.il	ET SCAN NMAP -sS window 2048	1
109.65.117.123	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.195	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
64.137.171.55	147.237.76.38	Canada	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
41.128.185.15	147.237.76.39	Egypt	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
208.100.26.228	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
41.128.185.15	147.237.76.34	Egypt	yohalan.idf.il	ET SCAN Potential SSH Scan	1
208.73.143.36	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
41.128.185.15	147.237.0.34	Egypt	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
178.20.188.164	147.237.72.167	Jordan	ishurim.aka.idf.il	ET SCAN NMAP -sS window 4096	1
178.20.188.164	147.237.72.167	Jordan	ishurim.aka.idf.il	ET SCAN NMAP -f -sS	1
103.207.37.82	147.237.76.38	Vietnam	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
93.158.203.197	147.237.77.234	Netherlands	halag.idf.il	ET SCAN NMAP -sS window 1024	1
64.137.171.55	147.237.8.45	Canada	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
41.128.185.15	147.237.76.199	Egypt	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
41.128.185.15	147.237.76.38	Egypt	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
208.100.26.228	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1

09-06-2016-00:04:02 to 09-06-2016-01:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
207.241.229.70	United States	147.237.77.216	dover.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	38
67.236.160.86	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	24
107.167.108.103	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	23
69.251.153.35	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	21
80.179.196.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	12
80.179.196.69	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid sequence number	monitor	9
176.13.229.51	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
176.13.229.51	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
24.238.70.81	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
192.99.207.133	Canada	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
192.99.207.133	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
109.253.245.121	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
192.99.207.133	Canada	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
192.99.207.133	Canada	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
192.99.207.133	Canada	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
2.53.36.156	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.11.69	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
192.99.207.133	Canada	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
79.179.11.69	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
192.99.207.133	Canada	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
192.99.207.133	Canada	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
192.99.207.133	Canada	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
192.99.207.133	Canada	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
167.114.212.195	Canada	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
192.99.207.133	Canada	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
192.99.207.133	Canada	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
167.114.212.195	Canada	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.86.49	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	5
84.110.185.23	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.99.207.133	Canada	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
167.114.212.195	Canada	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
77.139.154.121	France	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
84.110.185.23	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
167.114.212.195	Canada	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
192.99.207.133	Canada	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
192.99.207.133	Canada	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
192.99.207.133	Canada	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
138.246.253.19	Germany	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
84.95.255.154	Israel	147.237.77.170	maarachot.idf.il	HTTP Format Sizes	'Referer' header length exceeded maximum allowed length	monitor	4
192.99.207.133	Canada	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
167.114.212.195	Canada	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
195.239.16.40	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
84.110.185.23	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
167.114.212.195	Canada	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
192.99.207.133	Canada	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
195.239.16.53	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
141.0.14.150	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
167.114.212.195	Canada	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
167.114.212.195	Canada	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
192.99.207.133	Canada	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4

09-06-2016-00:04:02 to 09-06-2016-01:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.36.156	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	69
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.120.122.219	Block	7
109.253.157.72	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.197.149	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.76.83	Block	2
79.176.129.181	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
66.249.76.115	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1153-22717-he/dover.aspx	Block	1
46.19.86.136	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
176.13.232.130	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
79.183.13.52	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dover/site/mainpage.asp	Block	1
66.249.69.122	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/modules/shared/usercontrols/navmenu/undefined	Block	1
66.249.76.116	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
185.77.91.109	Turkey	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/index.php	Block	1
87.71.69.246	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/fund/funddesc.asp	Block	1
2.53.36.156	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.62	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/994-8847-he/navy.aspx	Block	1
66.249.79.139	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/3259.jpg	Block	1
65.55.210.88	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
207.46.13.70	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/994-8992-he/navy.aspx	Block	1
89.237.69.232	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
5.29.204.177	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1448-he/atal.aspx	Block	1
157.55.39.72	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/994-9020-he/navy.aspx	Block	1
66.249.83.221	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.69.14	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/.well-known/apple-app-site-association	Block	1
207.46.13.173	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/994-9004-he/navy.aspx	Block	1
109.65.94.182	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
31.13.110.99	Ireland	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/sip_storage/files/9/size220x0/2019.jpg	Block	1
157.55.39.99	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/994-9014-he/navy.aspx	Block	1
66.249.69.119	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1

09-06-2016-00:04:02 to 09-06-2016-01:04:02