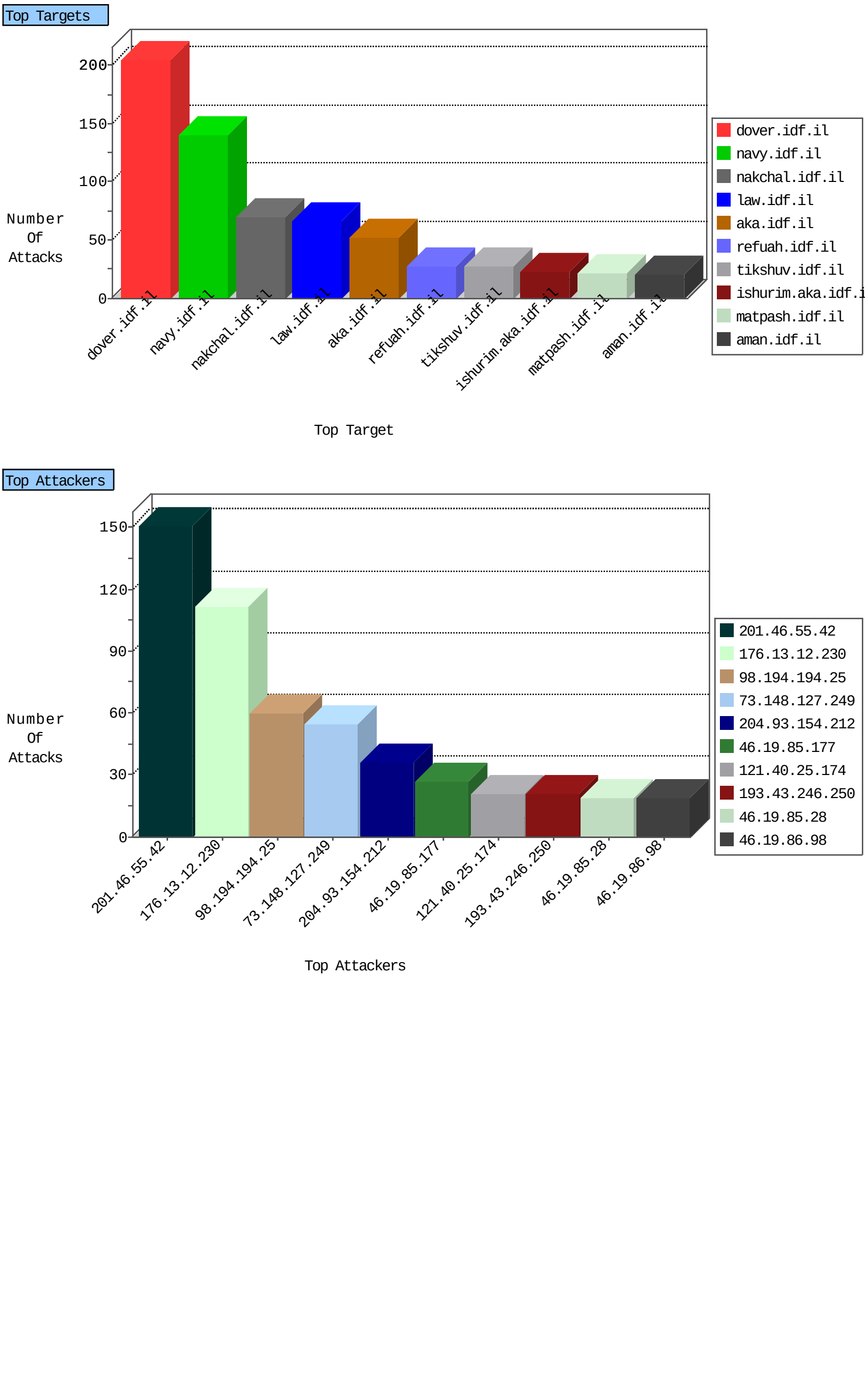
09-05-2016-07:04:06 to 09-05-2016-08:04:06

IDF Under Attack
Daily Report



09-05-2016-07:04:06 to 09-05-2016-08:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
204.93.154.212	United States	147.237.77.74	law.idf.il	TCP Scan (vertical)	drop	155
58.186.25.153	Vietnam	147.237.77.170	maarachot.idf.il	Frk_Under_Attack_Con_Tcp	drop	1
185.94.111.1	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1

09-05-2016-07:04:06 to 09-05-2016-08:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
121.40.25.174	China	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	9
204.93.196.218	United States	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	7
121.40.25.174	China	147.237.77.216	dover.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
213.203.204.143	Germany	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	5
204.93.196.218	United States	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
50.77.136.81	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	3
210.242.135.203	Taiwan	147.237.76.42	refuah.idf.il	34161: ICMP: Communication with Destination Host is Administratively Prohibited (Code 10)	Block	1
210.242.135.203	Taiwan	147.237.76.147	chinuch.aka.idf.i	34161: ICMP: Communication with Destination Host is Administratively Prohibited (Code 10)	Block	1

09-05-2016-07:04:06 to 09-05-2016-08:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
121.40.25.174	147.237.77.216	China	dover.idf.il	SQL Injection - Select From	6
91.121.78.42	147.237.77.74	France	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
46.19.86.228	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
208.100.26.228	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
50.116.123.135	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
5.255.90.133	147.237.77.227	Netherlands	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
208.100.26.228	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
204.93.196.218	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	1
94.102.48.195	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
79.182.100.8	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	1
46.227.67.172	147.237.76.176	Sweden	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
5.255.90.133	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1

09-05-2016-07:04:06 to 09-05-2016-08:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
176.13.12.230	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	26
176.13.12.230	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
74.208.218.66	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	18
98.194.194.25	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
85.232.60.142	United Kingdom	147.237.76.86	navy.idf.il	drop	SAM rule	drop	15
73.148.127.249	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
98.194.194.25	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	15
46.19.85.177	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
80.213.68.236	Norway	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
192.118.36.53	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	14
98.194.194.25	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	14
73.148.127.249	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	14
98.194.194.25	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	14
73.148.127.249	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	13
73.148.127.249	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	13
40.77.167.88	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
201.46.55.42	Brazil	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
201.46.55.42	Brazil	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
176.13.12.230	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	8
201.46.55.42	Brazil	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
176.13.12.230	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
176.13.12.230	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
201.46.55.42	Brazil	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
176.13.12.230	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
176.13.12.230	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	7
176.13.12.230	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
201.46.55.42	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
201.46.55.42	Brazil	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.86.98	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
201.46.55.42	Brazil	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
201.46.55.42	Brazil	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
201.46.55.42	Brazil	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
201.46.55.42	Brazil	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
201.46.55.42	Brazil	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
201.46.55.42	Brazil	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.85.177	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.28	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
201.46.55.42	Brazil	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
201.46.55.42	Brazil	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
201.46.55.42	Brazil	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
176.13.12.230	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
176.13.12.230	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
176.13.12.230	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
201.46.55.42	Brazil	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
176.13.12.230	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
201.46.55.42	Brazil	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
201.46.55.42	Brazil	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
176.13.12.230	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.28	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.98	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	5

09-05-2016-07:04:06 to 09-05-2016-08:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	9
109.67.33.76	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.159.108	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	3
2.55.10.216	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
91.143.234.207	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ https:/twitter.com/	Block	2
77.138.12.84	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/klali.aspx	Block	2
212.129.62.79	France	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1008-he/mousemove.mousewheel	Block	1
66.249.76.115	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18939-he/dover.aspx	Block	1
66.102.9.30	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
148.251.2.180	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 148.251.2.180	Block	1
79.180.211.240	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
66.249.76.39	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/6/ שקופית3	Block	1
213.151.53.59	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
89.237.111.92	France	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$cb15128160 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
68.180.230.54	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation PageNum in www.tikshuv.idf.il/901-he/tikshuv.aspx	Block	1
66.249.66.197	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-17753-he/dover.aspx	Block	1
148.251.2.180	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
80.179.118.150	Israel	147.237.76.31	nakchal.idf.il	Parameter Type Violation search in www.nakhal.idf.il/1085-he/nakhal.aspx	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/tizmoret/gallery/showpicture.asp	Block	1
216.72.40.185	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
77.138.7.248	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
66.249.69.83	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/forums/asp/showforum.asp	Block	1
157.55.39.11	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/templates/general/general.aspx	Block	1
80.246.138.21	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp	Block	1
46.19.85.141	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.69.97	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/938-he/patzar.aspx	Block	1
157.55.39.148	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.76.83	Block	1
65.55.210.51	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.180.32.23	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.69.119	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1

09-05-2016-07:04:06 to 09-05-2016-08:04:06