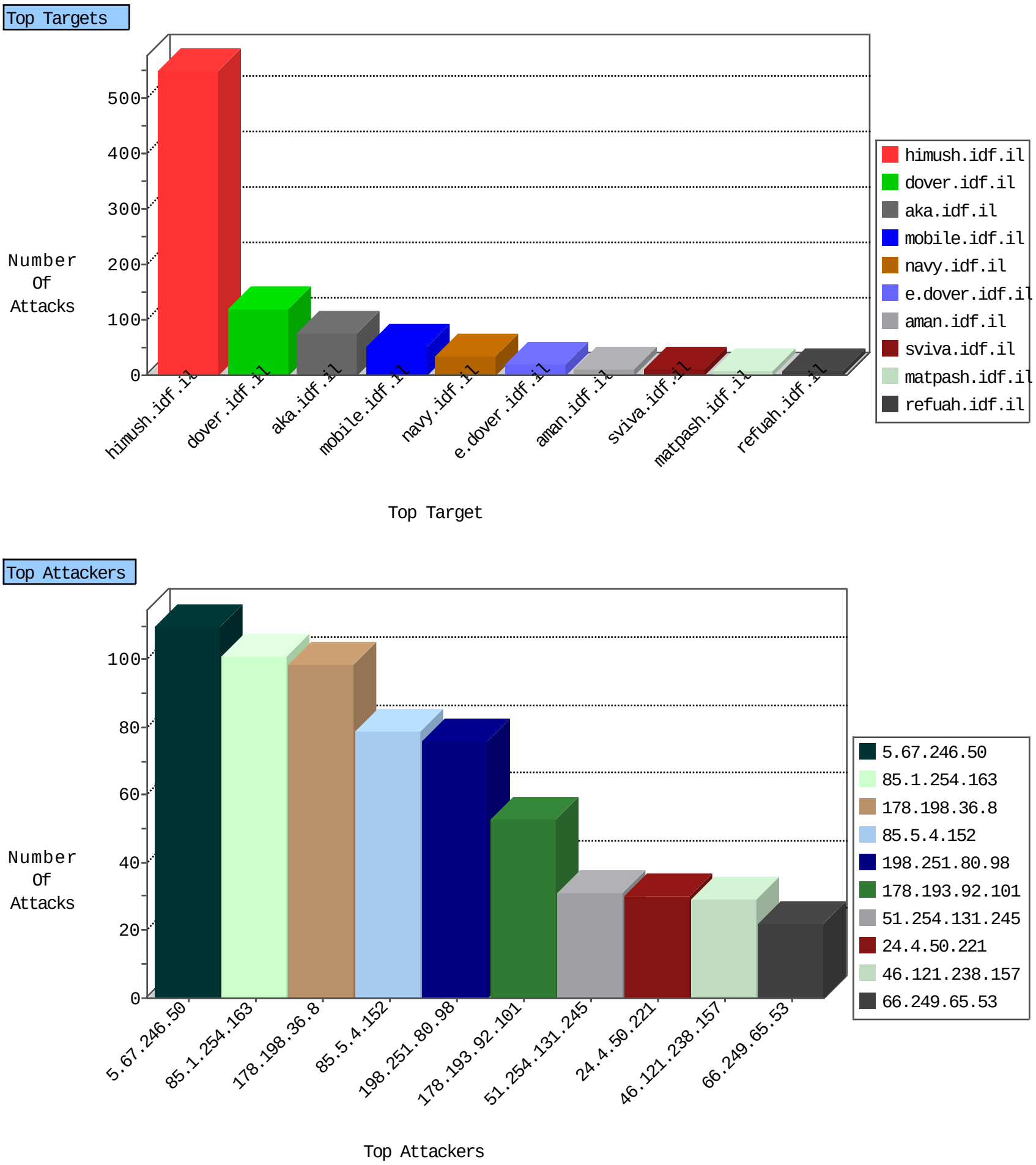
10-03-2016-23:04:09 to 10-04-2016-00:04:09

IDF Under Attack Daily Report



10-03-2016-23:04:09 to 10-04-2016-00:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.37.105	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
93.174.93.218	Netherlands	147.237.77.235	sviva.idf.il	block-sp-traf1	forward	2
195.62.53.168	Russian Federation	147.237.72.156	aman.idf.il	block-sp-traf1	forward	2
36.75.122.219	Indonesia	147.237.76.42	refuah.idf.il	Black List	drop	1
212.83.168.81	France	147.237.76.38	e.e.meitav.idf.i	Black List	drop	1
212.83.168.81	France	147.237.76.202	e.halag.idf.il	Black List	drop	1
93.174.94.235	Netherlands	147.237.76.42	refuah.idf.il	Black List	drop	1

10-03-2016-23:04:09 to 10-04-2016-00:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
51.254.131.245	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	22
51.254.131.245	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	3
51.254.131.245	France	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	2
51.254.131.245	France	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	2
199.58.86.211	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
51.254.131.245	France	147.237.72.156	aman.idf.il	C1000074: HTTP: majestic bot	Permit	1

10-03-2016-23:04:09 to 10-04-2016-00:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
91.121.143.113	147.237.72.166	France	aka.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	6
85.108.174.9	147.237.77.216	Turkey	dover.idf.il	Tehila - Perl LWP with fake user agent	5
163.172.238.45	147.237.0.33	United Kingdom	idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
128.199.124.88	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
61.240.144.65	147.237.0.35	China	akaws.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
91.201.236.158	147.237.76.39	Ukraine	mobile.meitav.idf.i	ET SCAN NMAP -sS window 4096	1
91.201.236.158	147.237.76.39	Ukraine	mobile.meitav.idf.i	ET SCAN NMAP -f -sS	1
91.201.236.155	147.237.8.28	Ukraine	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 3072	1
91.201.236.155	147.237.8.28	Ukraine	e.mobile-ks.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.65	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
180.118.51.172	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
61.240.144.65	147.237.77.74	China	law.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
162.248.76.109	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 3072	1
61.240.144.65	147.237.72.217	China	e.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
93.190.90.226	147.237.0.33	Germany	idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
91.201.236.158	147.237.76.39	Ukraine	mobile.meitav.idf.i	ET SCAN NMAP -sS window 2048	1
91.201.236.158	147.237.76.39	Ukraine	mobile.meitav.idf.i	ET DROP Spamhaus DROP Listed Traffic Inbound	1
91.201.236.155	147.237.8.28	Ukraine	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 2048	1
62.210.243.100	147.237.76.44	France	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
183.129.160.229	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	147.237.77.176	China	matpash.idf.il	ET SCAN Potential VNC Scan 5800-5820	1

10-03-2016-23:04:09 to 10-04-2016-00:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.67.246.50	United Kingdom	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	25
5.67.246.50	United Kingdom	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	24
5.67.246.50	United Kingdom	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	23
198.251.80.98	United States	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	23
85.1.254.163	Switzerland	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	22
178.198.36.8	Switzerland	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	22
85.1.254.163	Switzerland	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	22
178.198.36.8	Switzerland	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	22
178.198.36.8	Switzerland	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	21
198.251.80.98	United States	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	21
66.249.65.53	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	21
178.198.36.8	Switzerland	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	20
85.1.254.163	Switzerland	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	20
5.67.246.50	United Kingdom	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	20
85.1.254.163	Switzerland	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	20
198.251.80.98	United States	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	19
5.67.246.50	United Kingdom	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	18
85.5.4.152	Switzerland	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	18
186.233.175.22	Brazil	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	18
85.5.4.152	Switzerland	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	18
85.5.4.152	Switzerland	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	17
85.5.4.152	Switzerland	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	17
85.1.254.163	Switzerland	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
178.198.36.8	Switzerland	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
213.8.204.80	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
178.193.92.101	Switzerland	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	11
178.193.92.101	Switzerland	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	11
178.193.92.101	Switzerland	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	11
178.193.92.101	Switzerland	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
198.251.80.98	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
85.5.4.152	Switzerland	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
178.193.92.101	Switzerland	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
192.117.13.30	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
24.4.50.221	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
24.4.50.221	United States	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	6
24.4.50.221	United States	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	6
24.4.50.221	United States	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.176.94.114	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	6
24.4.50.221	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
46.120.198.171	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.121.238.157	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	6
46.121.238.157	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence		monitor	5
79.176.94.114	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.55.146.214	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.120.198.171	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.94	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.94	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
65.55.210.13	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
79.176.94.114	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4

10-03-2016-23:04:09 to 10-04-2016-00:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.71.54.34	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 87.71.54.34	Block	12
46.19.86.113	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
91.77.231.156	Russian Federation	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	3
93.174.93.218	Netherlands	147.237.77.235	sviva.idf.il	Multiple NULL Character in Method from 93.174.93.218	Block	3
87.71.54.34	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
62.48.253.20	Portugal	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/sachar	Block	2
192.117.13.30	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp	Block	1
93.174.93.218	Netherlands	147.237.77.235	sviva.idf.il	NULL Character in Method	Block	1
79.178.62.136	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
66.249.65.8	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
213.8.204.80	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/0/71520.pdf	Block	1
51.254.131.245	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
190.216.73.60	Argentina	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22256-es/dover.aspx	Block	1
81.57.243.140	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	Block	1
66.249.65.60	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/1901.doc	Block	1
68.180.230.216	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1073-he/nakhal.aspx	Block	1
84.111.137.99	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
66.249.69.93	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1
46.19.85.94	Israel	147.237.76.86	navy.idf.il	Malformed URL	Block	1
93.174.93.218	Netherlands	147.237.77.235	sviva.idf.il	Multiple Illegal Byte Code Character in Method from 93.174.93.218	Block	1
68.180.231.60	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1927-he/cogat.aspx	Block	1
66.249.64.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
195.62.53.168	Russian Federation	147.237.72.156	aman.idf.il	Unauthorized URL Access to gmail.com/engine/log.txt	Block	1
84.111.137.99	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/wp-login.php	Block	1
66.249.73.133	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19667-he/idfgdover.aspx	Block	1
46.19.85.94	Israel	147.237.76.86	navy.idf.il	Unknown HTTP Request Method k.katana in URL	Block	1
77.138.214.36	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
66.249.64.12	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/iturim/asp/wars.asp	Block	1
204.79.180.206	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/miluim/templates/inner.asp	Block	1

10-03-2016-23:04:09 to 10-04-2016-00:04:09