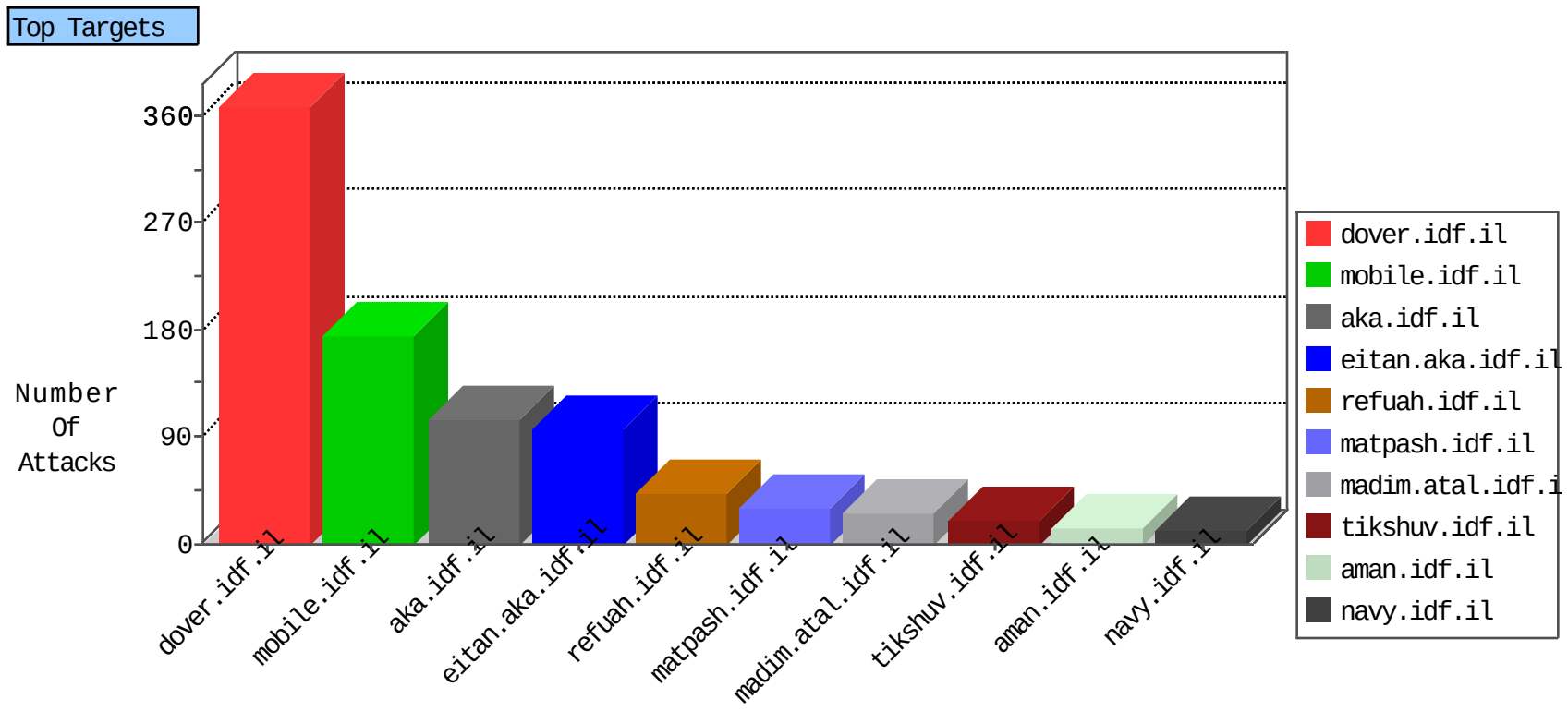
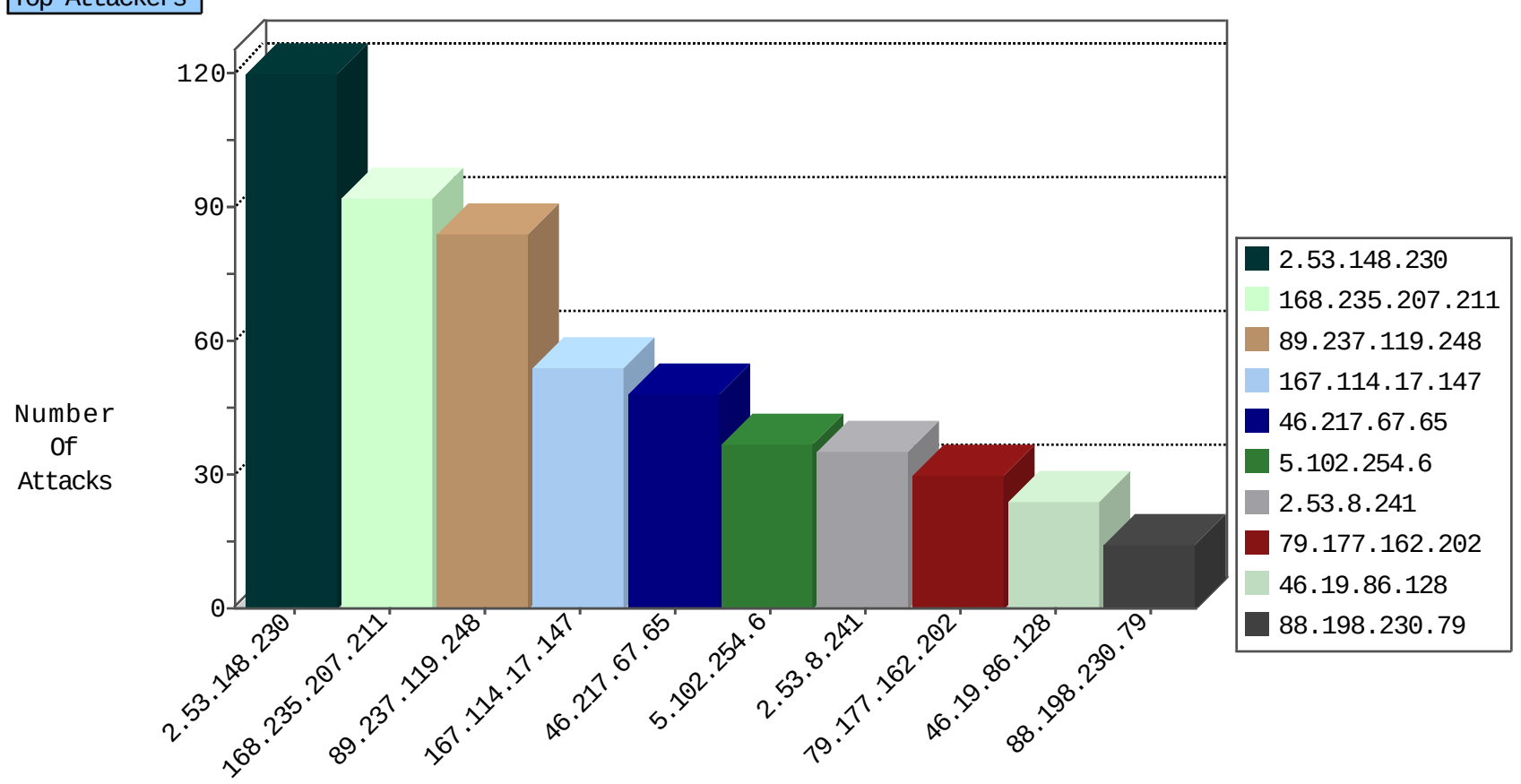
09-17-2016-18:04:01 to 09-17-2016-19:04:01

IDF Under Attack
Daily Report

Top Targets



Top Attackers



09-17-2016-18:04:01 to 09-17-2016-19:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
168.235.207.211	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	3
129.97.74.14	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.223.8.114	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
193.1.13.14	Ireland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
198.133.224.147	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
141.22.213.34	Germany	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.208.4.198	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
200.19.159.34	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.195.4.69	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.206.158.138	Spain	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.32.84.160	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
216.48.80.14	Canada	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
139.78.141.243	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-17-2016-18:04:01 to 09-17-2016-19:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
88.198.230.79	Germany	147.237.0.34	tikshuv.idf.i	C1000074: HTTP: majestic bot	Permit	4
88.198.230.79	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
88.198.230.79	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
88.198.230.79	Germany	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	2
88.198.230.79	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	2
212.252.57.54	Turkey	147.237.77.216	dover.idf.il	C1000016: HTTP: administrator in URI	Permit	1
212.252.57.54	Turkey	147.237.77.216	dover.idf.il	C1000018: HTTP: access to administrator/index.php -> Quarantine	Permit	1

09-17-2016-18:04:01 to 09-17-2016-19:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
167.114.17.147	147.237.77.216	Canada	dover.idf.il	Tehila - Perl LWP with fake user agent	48
5.255.90.133	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
185.129.148.230	147.237.72.14	Latvia	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
139.162.13.205	147.237.76.30	Singapore	himush.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
109.60.153.178	147.237.76.197	Russian Federation	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
95.154.250.21	147.237.77.235	United Kingdom	sviva.idf.il	ET SCAN Potential SSH Scan	1
66.249.64.103	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
62.215.38.173	147.237.77.233	Kuwait	atal.idf.il	ET SCAN NMAP -f -sS	1
54.205.154.137	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 3072	1
54.205.154.137	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -f -sS	1
201.38.68.132	147.237.8.27	Brazil	e.madim.atal.idf.i	ET SCAN NMAP -sS window 1024	1
112.67.77.0	147.237.77.61	China	e.cogat.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
103.207.36.31	147.237.8.45	Vietnam	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
79.180.103.222	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.215.38.173	147.237.77.233	Kuwait	atal.idf.il	ET SCAN NMAP -sS window 2048	1
58.218.200.137	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
54.205.154.137	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 2048	1

09-17-2016-18:04:01 to 09-17-2016-19:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.53.148.230	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	120
168.235.207.211	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	86
89.237.119.248	France	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	84
46.217.67.65	Macedonia, the Former Yugoslav Republic of	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
79.177.162.202	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
5.102.254.6	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	28
2.53.8.241	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
46.19.86.128	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
67.170.170.72	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
2.53.8.241	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.128	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	8
5.102.254.6	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
46.19.85.115	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.128	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.184	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.215	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.3	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
84.95.251.36	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.184	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.13.12.115	Israel	147.237.77.216	dover.idf.il	SYN Attack		monitor	5
46.19.86.246	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.191	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
37.142.199.210	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.191	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
87.69.79.43	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
176.13.231.99	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.85.115	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.185	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
45.217.92.51	Morocco	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
185.6.19.154	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.53.8.241	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
79.176.141.179	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
45.217.92.51	Morocco	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	alert	4
157.55.39.210	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
65.55.210.69	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.246	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.8.241	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
77.138.97.87	France	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
84.95.208.20	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.234.128	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
168.235.207.211	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.19.85.143	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.85.231	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.53.8.241	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
185.120.126.4	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.234.128	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
46.19.85.143	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

09-17-2016-18:04:01 to 09-17-2016-19:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.102.242.175	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	9
167.114.17.147	Canada	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 167.114.17.147	Block	6
176.13.18.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
79.182.133.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.8.204.12	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	3
87.69.117.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.153.98	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.139.108.87	France	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
66.102.9.24	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
109.66.132.77	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catID in www.aka.idf.il/yohalan/home/home.asp	None	1
79.180.169.128	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
185.6.19.154	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/'	Block	1
84.95.251.36	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
77.138.97.87	France	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/favicon.ico	Block	1
139.162.13.205	Singapore	147.237.76.30	himush.idf.il	Multiple Untraceable SSL Sessions from 139.162.13.205 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
2.55.47.161	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl13 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
139.162.13.205	Singapore	147.237.76.30	himush.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
80.246.137.118	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$txtSearch in www.aka.idf.il/main/giyus/	None	1
217.132.126.60	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
89.237.81.138	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/information.aspx	Block	1
77.139.173.168	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1
84.95.208.20	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1
5.102.254.6	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
109.65.47.69	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 109.65.47.69	Block	1
79.176.105.203	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
84.95.208.20	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/homepage/piwik.php	Block	1

09-17-2016-18:04:01 to 09-17-2016-19:04:01