Recorded Future

CYBER THREAT ANALYSIS

Mirai-Variant IoT Botnet Used to Target Financial Sector in January 2018

By Priscilla Moriuchi and Sanil Chohan
Recorded Future

Executive Summary

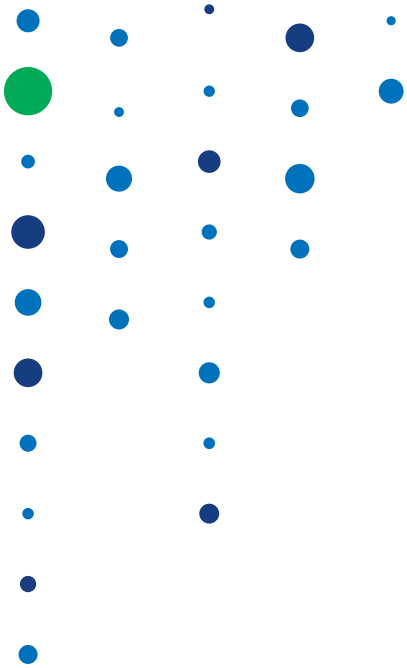
Insikt Group assesses that a Mirai botnet variant, possibly linked to the IoTroop or Reaper botnet, was utilized in attacks on at least one company, and probably more, in the financial sector in late January 2018. This assessment is based on third-party metadata and existing open source intelligence. IoTroop is a powerful internet of things (IoT) botnet primarily comprised of compromised home routers, TVs, DVRs, and IP cameras exploiting vulnerabilities in products from major vendors including MikroTik, Ubiquity, and GoAhead. This is the first time we have observed an IoT botnet being used in a DDoS since Mirai, and it may be the first time IoTroop has been used to target victims since it was initially identified last year.

Key Judgments

- The first attack occurred on January 28, 2018 at 1830 UTC. A second financial sector company experienced a DDoS attack the same day and time, likely utilizing the same botnet. A third financial sector company experienced a similar DDoS attack a few hours later at 2100 UTC the same day.
- The initial attack was a DNS amplification attack with traffic volumes peaking at 30Gb/s. We do not have enough information to determine the volume of the subsequent two attacks.
- If these attacks were conducted by IoTroop, then our observations indicate the botnet has evolved since October 2017 to exploit vulnerabilities in additional IoT devices and is likely to continue to do so to propagate the botnet and facilitate larger DDoS attacks.
- We identified at least seven IP addresses that we assess are controllers for the botnet that were likely engaged in attack coordination and scanning of new botnet infrastructure.

Background

In October 2017, researchers identified a new botnet named IoTroop, composed of IoT devices such as routers and wireless IP cameras, manufactured by companies including TP-Link, Avtech, MikroTik, Linksys, Synology, and GoAhead. IoTroop was unique in that the malware used to propagate the botnet, also called Reaper, "was built using a flexible Lua engine and scripts, which means that instead of being limited to the static, pre-programmed attacks of previous exploits, its code can be easily updated on the fly, allowing massive in-place botnets to run new and more malicious attacks as soon as they become available."



IoTroop malware can exploit at least a dozen vulnerabilities and can be updated by the attackers as new vulnerabilities are exposed. See the appendix for a complete known list of vendors, technologies, and vulnerabilities observed in the botnet used for these attacks and in the IoTroop botnet.

In February 2018, Netherlands police arrested an 18-year-old man on suspicion of launching DDoS attacks on several Dutch entities — the technology site Tweakers, and the internet service provider Tweak. There is speculation that this man was also responsible for DDoS attacks against financial institutions that we observed, however, that link has not been confirmed by police.

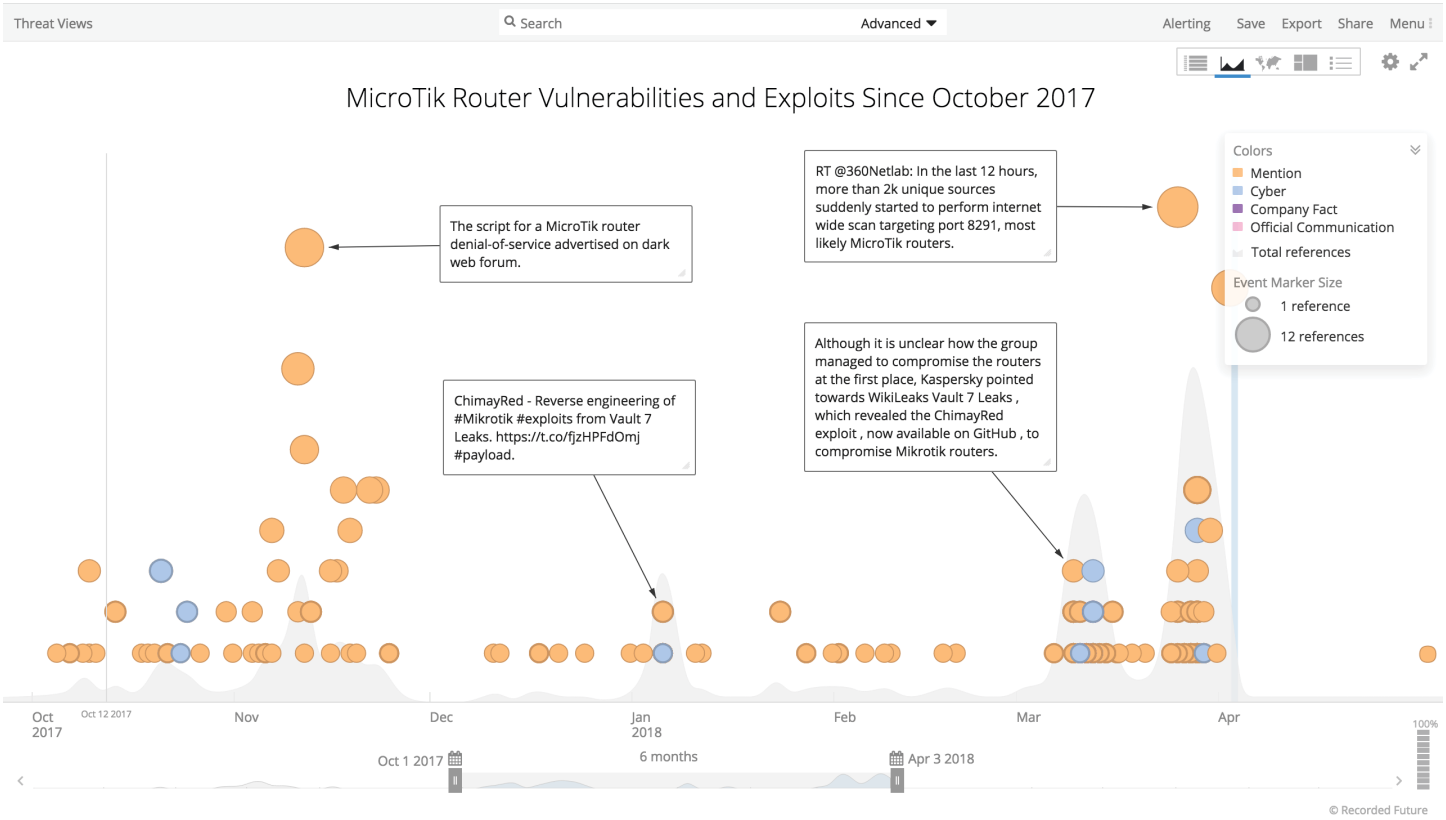
The arrested individual appears to have leased the botnet for use in the September attacks under the guise of purchasing a "stresser," or network stress test. If this man is also responsible for the January attacks we observed, he likely also leased this Mirai-variant IoT botnet for those attacks as well. As of publication, we do not know who is behind the compilation of this botnet or who executed the attacks we observed in January 2018.

Threat Analysis

First Financial Sector Company Targeted

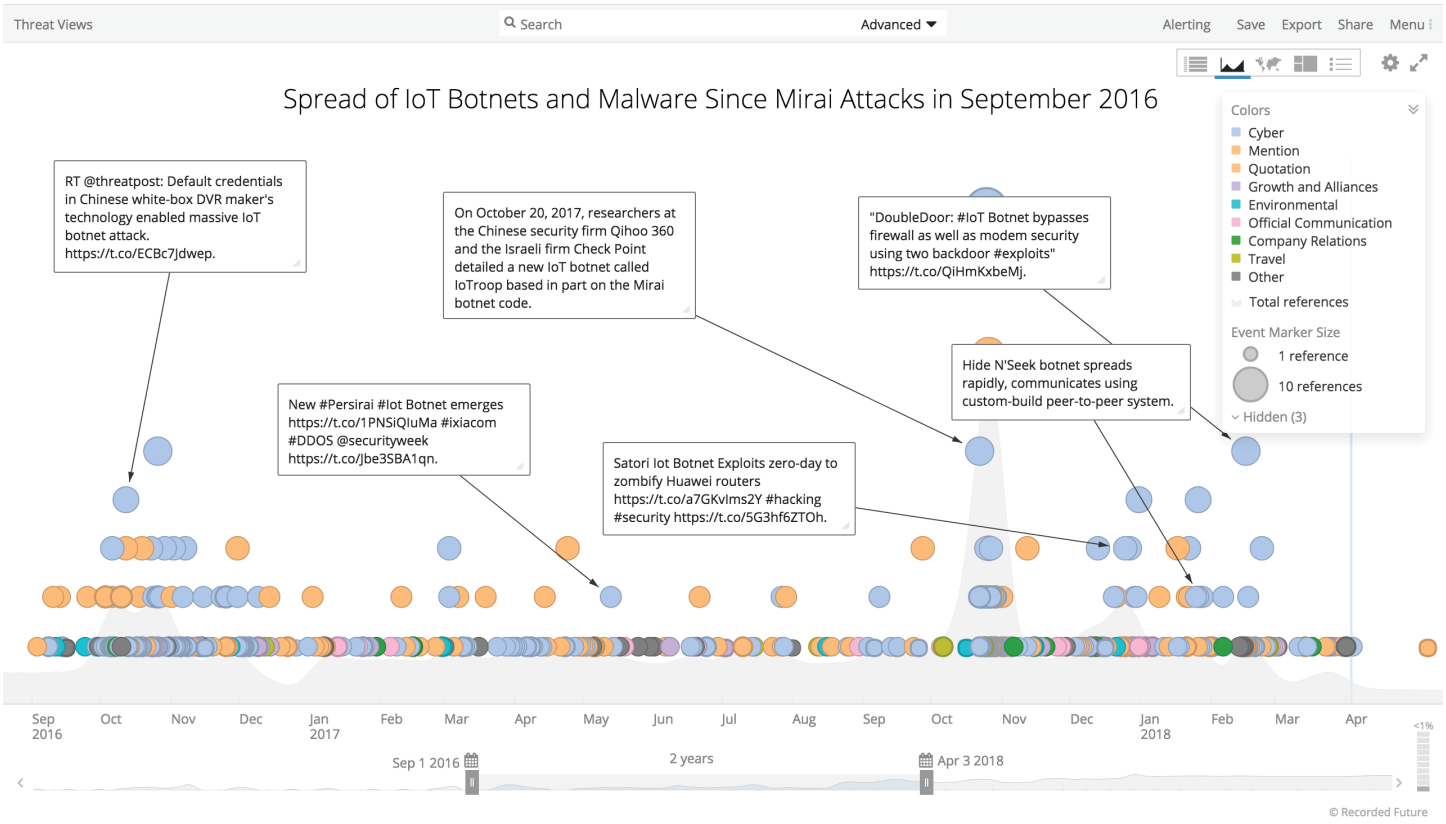
The botnet targeted the first financial sector company using at least 13,000 devices, each with a unique IP address, and generated traffic volumes up to 30Gb/s. Insikt Group used IP geolocation, service banners from Shodan, and additional metadata to analyze the composition of the botnet. Candidate controllers, or bot masters, were shortlisted based on the frequency and the number of distinct botnet clients with which they were in communication. Further anomalous activity was noted based on unusual port usage.

Our analysis shows that the botnet involved in the first company attack was 80 percent comprised of compromised MikroTik routers, with the remaining 20 percent composed of various IoT devices ranging from vulnerable Apache and IIS web servers, to routers from Ubiquity, Cisco, and ZyXEL. We also discovered webcams, TVs, and DVRs among the 20 percent of IoT devices, which included products from major vendors such as MikroTik, GoAhead, Ubiquity, Linksys, TP-Link, and Dahua.



Recorded Future timeline of MicroTik router vulnerabilities and exploits since the discovery of the IoTroop botnet.

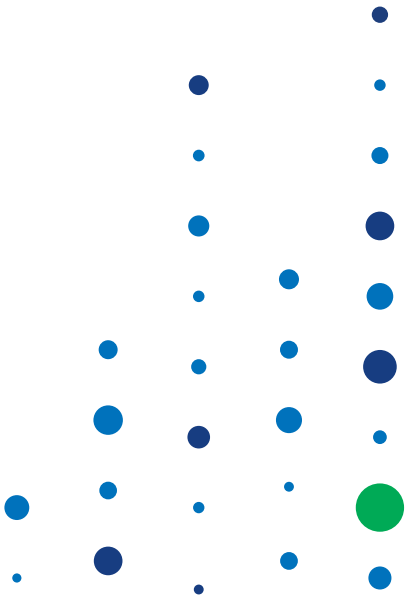
The spread of devices from different manufacturers suggests a widespread and rapidly evolving botnet that appears to be leveraging publicly disclosed vulnerabilities in many IoT devices. While many of the IoT vendors and devices appeared in the research published in October 2017, many of the devices such as Dahua CCTV DVRs, Samsung UE55D7000 TVs and Contiki-based devices were previously unknown to be vulnerable to Reaper/ IoTroop malware.

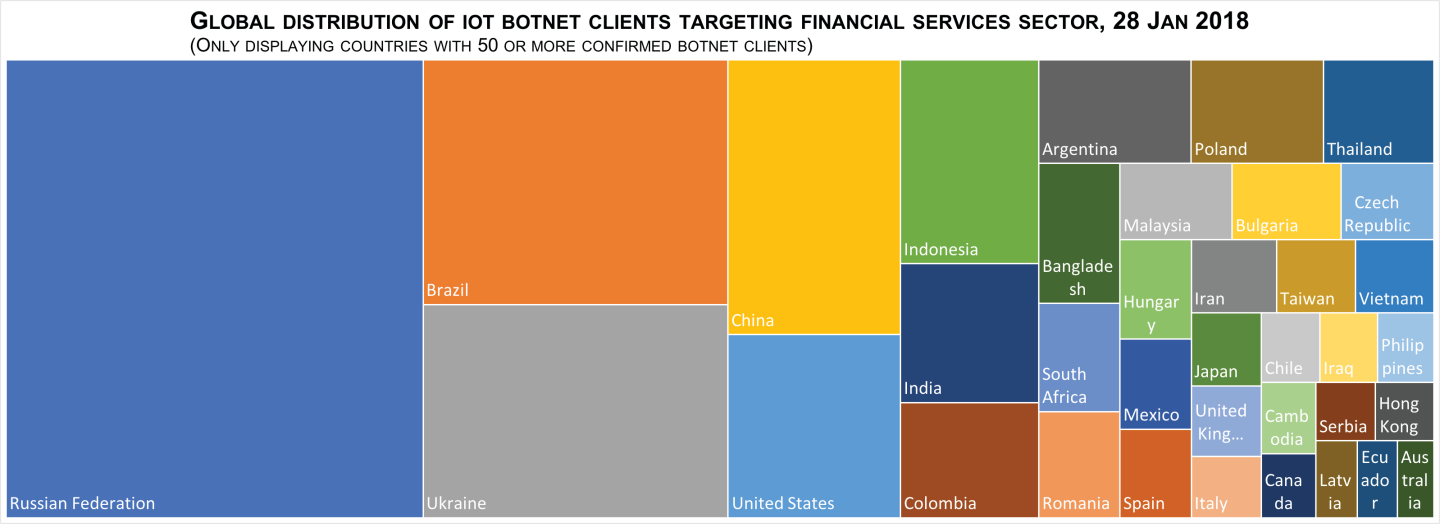


Recorded Future timeline of the spread of IoT botnets and malware since the September 2016 Mirai attacks.

All of the compromised MikroTik devices had TCP port 2000 open, which is usually reserved for MikroTik's bandwidth test server protocol. This port is usually enabled by default in new MikroTik devices. No MikroTik devices with TCP 2000 disabled (a recommended security measure in production environments) were discovered within the botnet.

Below is a graphic of the geographic breakdown for the botnet:





Global distribution of IoT botnet clients targeting financial services sector, January 2018 (via Microsoft Excel).

As the graphic shows, the geographic spread of the botnet clients was heavily skewed toward Russia, Brazil, and Ukraine. This is likely to just be a reflection of the popularity of MikroTik's devices in those countries, rather than anything specific relating to the botnet configuration. In total, there were 139 different countries represented in the data, demonstrating a widespread targeting of vulnerable IoT devices around the world. This distribution differed from the original Mirai botnet, where Brazil was the only country that appeared in the top five botnet client lists for both botnets.

We discovered a number of IPs that we believe are command and control servers (or "controllers") for the botnet and created a Recorded Future Threat List to enable customers to track these controllers. Please reach out to your intelligence services representative for access.

The following IP addresses are candidates for botnet controllers. While volume alone is an indicator for a controller, the below IPs are ones we have additional confidence in based on further data.

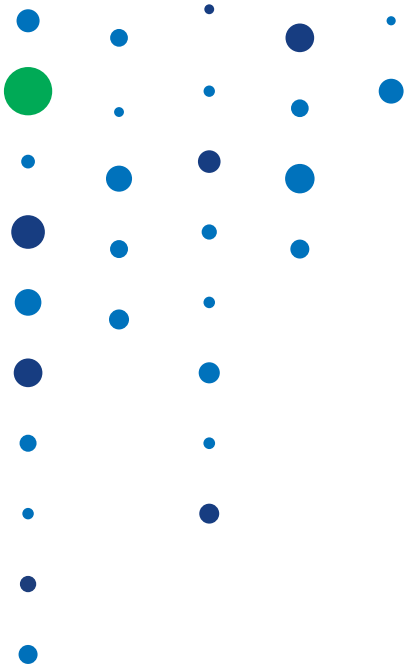
98.95.228.104: 34 percent of all activity we observed targeting the first financial sector company included UDP DNS requests to or from this IP.

71.68.32.251: Similarly, we observed a large amount of activity to or from the first company to this IP.

213.160.168.18: We observed no specific threat data on this IP, but it is part of a /24 range that has historically been linked to malware deployment and suspect proxies.

84.47.111.62: This is likely a top controller, based on volume and pattern analysis.

The next two IPs are both Slovakian. Both have slightly elevated Recorded Future risk scores because they triggered the predictive risk model.



87.197.166.13 and **87.197.108.40**: We observed large amounts of data exchanged between these two IPs and a couple of the controllers. We believe these could be primary controllers, or at a minimum, one hop closer to source.

62.204.238.82: This IP was one of the 13,000 IPs originally involved in the DDoS attack. It resolves to the Czech Republic, and accounts for almost three percent of the traffic generated from our metadata analysis. During the researched window, we observed this IP make repeated connections to three suspected Internet Relay Chat (IRC) servers in France (**149.202.42.174**, **51.255.34.80**, **5.196.26.96**). All three of these suspected IRC servers triggered Recorded Future's predictive risk model.

Second Financial Sector Company Targeted

Additionally, we determined that a second financial sector company was also targeted by a DDoS attack during the same weekend of January 27 to January 28, 2018. We believe this attack was conducted using the same Mirai-variant IoT botnet because of an overlap in the use of botnet infrastructure and the timing of the attacks.

During the course of our analysis, we uncovered evidence that the second company had likely been targeted by the same Mirai-variant IoT botnet on the same day. Further analysis identified that IP addresses from the second company communicated with 26 unique IP addresses, of which 19 had been involved in the attack against the first financial sector company.

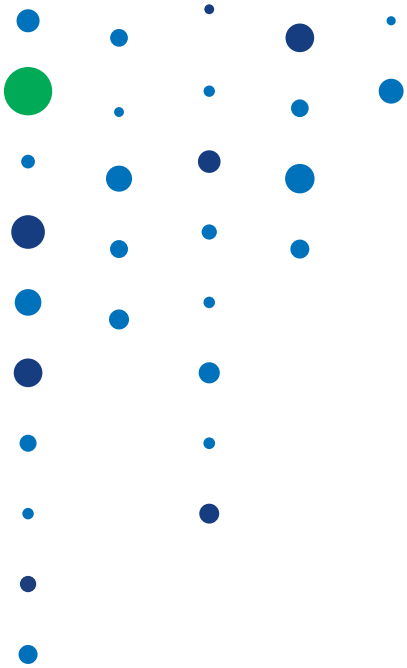
Third Financial Sector Company Targeted

We also discovered that on January 28, 2018, only a few hours later at approximately 2100 UTC, a third financial sector company's network experienced very high data volumes of TCP 443 events. While technical details of this activity are not currently available to compare with the original DDoS, the close temporal proximity of these events suggests a possible connection.

Outlook

These attacks highlight the ongoing threat of DDoS to the financial sector from continuously evolving botnets. The similarity in device composition with the IoTroop/Reaper botnet suggest IoTroop has evolved to exploit vulnerabilities in additional IoT devices and is likely to continue to do so in the future in order to build up the botnet to facilitate larger DDoS attacks against the financial sector.

As more data comes to light on the continued targeting of financial institutions from IoTroop, it will become increasingly important to monitor the potential controllers and identify new IoT devices being added to the botnet in preparation for further attacks.



Recorded Future customers are advised to subscribe to the published Threat List of botnet controllers to track malicious activity. These controllers are likely to be engaged in aggressive scanning for new vulnerable IoT infrastructure to commandeer as well as be responsible for any denial of service attack commands issued to the botnet clients.

We also recommend that users of IoT devices take the following simple measures to mitigate the risk of their devices being commandeered by an IoT botnet:

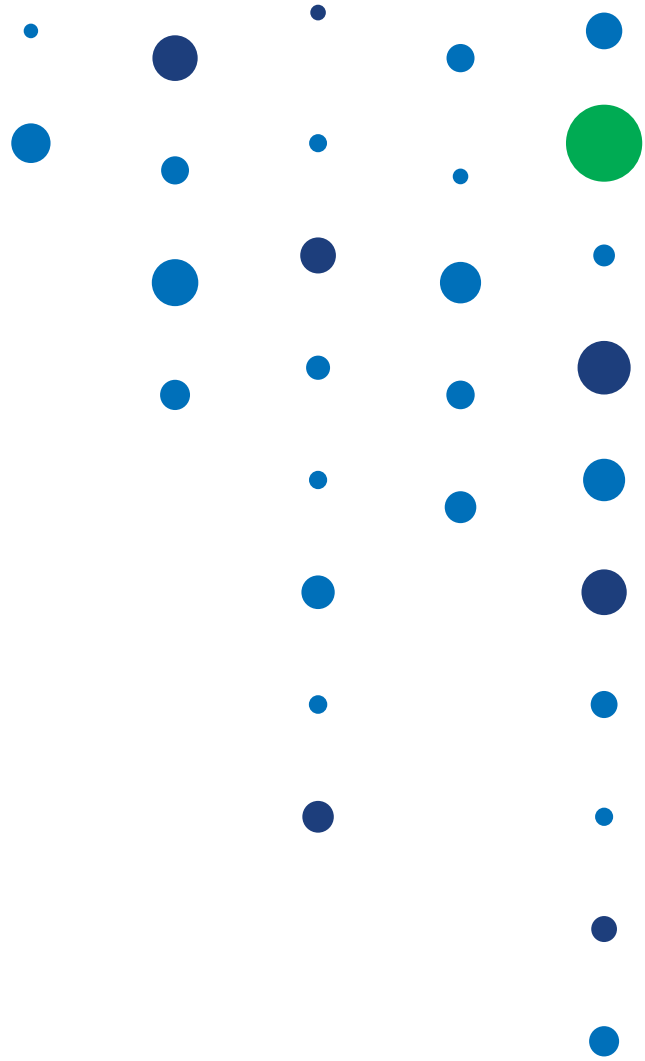
- Always replace default manufacturer passwords immediately upon use.
- Keep the firmware for devices current and up to date.
- For IP camera and similar systems that require remote access, invest in a VPN.
- Disable unnecessary services (e.g., Telnet) and close ports that are not required for the IoT device.

Appendix A: Vendor Devices Exploited by Mirai-Variant Botnet

Below is a list of vendor device vulnerabilities exploited by the Mirai-variant IoT botnet targeting the financial sector in January 2018. A column depicting Checkpoint's observations of the IoTroop botnet as well as a listing of whether the same vendor devices were seen in the original Mirai botnet have been included for reference.

Vendor	Details	CVE #	Date Published (cvedetails.com)	Vendor devices observed by Recorded Future in Mirai-variant IoT botnet attacks in January 2018	Vendor devices noted in Checkpoint research on IoTroop botnet activity in October 2017	Vendor devices noted as being vulnerable to original Mirai malware
AVTECH	AVTECH Devices Multiple vulnerabilities	CVE-2013-4981 CVE-2013-4980	3-Mar-14	Yes	Yes	No
Dahua Technology Co.	Use of password hash instead of password for authentication, cwe-836, Dahua DVR	CVE-2017-7927	5-May-17	Yes	No	Yes
	Password in configuration file, cwe-260, Dahua DVR	CVE-2017-7925	5-May-17	Yes	No	Yes
GoAhead	Wireless IP Camera (P2P) WIFICAM Cameras Information Disclosure	CVE-2017-8225	25-Apr-17	Yes	Yes	Yes
	Wireless IP Camera (P2P) WIFICAM Cameras Remote Code Execution	CVE-2017-8224	25-Apr-17	Yes	Yes	Yes
Linksys	Linksys WRH54G HTTP Management Interface DoS Code Execution – Ver2	CVE-2008-2636	9-Jun-08	Yes	No	No
	Belkin Linksys WRT110 Remote Command Execution – Ver2	CVE-2013-3568	23-Sep-13	Yes	No	No
	Cisco Linksys PlayerPT ActiveX Control Buffer Overflow	CVE-2012-0284	19-Jul-12	Yes	No	No

MikroTik	MikroTik RouterOS SNMP Security Bypass	CVE-2008-6976	19-Aug-09	Yes	No	No
	MikroTik RouterOS Admin Password Change	CVE-2015-2350	19-Mar-15	Yes	No	No
	Mikrotik Router Remote Denial Of Service	CVE-2012-6050	26-Nov-12	Yes	No	No
Samsung	Samsung UE55D7000 TV http config	Unknown	Unknown	Yes	No	No
Synology	Synology DiskStation Manager SLICEUPLOAD Code Execution	CVE-2013-6955	9-Jan-14	Yes	No	No
TP-Link	TP-Link Wireless Lite N Access Point Directory Traversal	CVE-2012-5687	1-Nov-12	Yes	No	No
	TP-LINK WR1043N Multiple Cross-Site Request Forgery	CVE-2013-2645	5-Oct-14	Yes	No	No
Ubiquity	Airgrid m5 hp series, 5ghz, 27dbi grid antenna with integrated radio by Ubiquiti networks	Unknown	Unknown	Yes	No	Yes
	Ubiquiti EdgeRouter Lite Router - Gigabit	Unknown	Unknown	Yes	No	Yes
	Ubiquiti EdgeRouter Router - 1 Gbps - Gigabit	Unknown	Unknown	Yes	No	Yes
	Ubiquiti EdgeRouter X SFP Router - 5-port - Gigabit	Unknown	Unknown	Yes	No	Yes



Recorded Future

www.recordedfuture.com

@RecordedFuture

About Recorded Future

Recorded Future arms security teams with the only complete threat intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.