Persirai: New IoT Botnet Targets IP Cameras

blog.trendmicro.com/trendlabs-security-intelligence/persirai-new-internet-things-iot-botnet-targets-ip-cameras/

May 9, 2017

Cyber Threats

A new IoT botnet called Persirai has been discovered targeting over 1,000 IP Camera models based on various Original Equipment Manufacturer (OEM) products.

By: Tim Yeh, Dove Chiu, Kenney Lu May 09, 2017 Read time: (words)

Updated on May 10, 2017, 6:52 PM (UTC-7): We updated the source code and made changes to Figures 4 and 6.

A new Internet of Things (IoT) botnet called Persirai (Detected by Trend Micro as ELF_PERSIRAI.A) has been discovered targeting over 1,000 Internet Protocol (IP) Camera models based on various Original Equipment Manufacturer (OEM) products. This development comes on the heels of Mirai—an open-source backdoor malware that caused some of the most notable incidents of 2016 via Distributed Denial-of-Service (DDoS) attacks that compromised IoT devices such as Digital Video Recorders (DVRs) and CCTV cameras—as well as the Hajime botnet.

We detected approximately 120,000 IP cameras that are vulnerable to ELF_PERSIRAI.A via Shodan. Many of these vulnerable users are unaware that their IP Cameras are exposed to the internet.

Figure 1

Figure 1: The number of vulnerable IP Cameras as of April 26, 2017 (derived from Shodan data)

This makes it significantly easier for the perpetrators behind the malware to gain access to the IP Camera web interface via TCP Port 81.

Behavior and Analysis

Figure 1

Figure 2: Infection Flow of ELF_PERSIRAI.A

IP Cameras typically use Universal Plug and Play (UPnP), which are network protocols that allow devices to open a port on the router and act like a server, making them highly visible targets for IoT malware.

After logging into the vulnerable interface, the attacker can perform a command injection to force the IP Camera to connect to a download site via the following command:

Figure 1

The download site will then respond with the following commands:

Figure 1

These commands will download and execute malicious shell script from the domain *ntp.gtpnet.ir* T

he wificam.sh will download and execute the following samples, which will be deleted after execution:

Figure 1

After the samples are downloaded and executed, the malware deletes itself and will only run in memory. It will also block the zero-day exploit by pointing ftpupdate.sh and ftpupload.sh to /dev/null to prevent other attackers from targeting the victim's IP Camera. However, once the camera is rebooted, it will again be vulnerable to the exploit.

The affected IP Camera will report to the C&C servers:

- load[.]gtpnet[.]ir
- ntp[.]gtpnet[.]ir
- 185[.]62[.]189[.]232
- 95[.]85[.]38[.]103

After receiving commands from the server, the IP Camera will then start automatically attacking other IP Cameras by exploiting a zero-day vulnerability that was made public a few months ago. Attackers exploiting this vulnerability will be able to get the password file from the user, providing them the means to do command injections regardless of password strength.

A sample of the payload is shown below:

Figure 1

Figure 3: ELF_PERSIRAI.A sample payload

The IP Camera will then receive a command from the C&C server, instructing it to perform a DDoS attack on other computers via User Datagram Protocol (UDP) floods. Notably, Persirai can perform User Datagram Protocol (UDP) DDoS attack with SSDP packets without spoofing IP address.

The backdoor protocol can be seen below:

Figure 1

Figure 4: C&C server backdoor protocol

The red portions indicate communication from C&C server to the victim's IP camera. It contains the attack commands and DDoS target IP and port.

Figure 5

Figure 5: Special characters used by Persirai

C&C servers we discovered were found to be using the IR country code. We also found some special Persian characters which the malware author used.

The IP Camera manufacturer for the sample we used claimed that the latest firmware addressed the vulnerability, so we tried updating the firmware of the IP Camera. However, the firmware indicates that it is already using the latest version.

Figure 1

Figure 6: IP Camera firmware

Conclusion and Mitigation

Aside from being the first malware that brought IoT security into the limelight, we also noted how Mirai's open-source nature gave it the potential to act as the core template upon which future IoT-centric malware will be built upon.

As the Internet of Things gains traction with ordinary users, cybercriminals may choose to move away from Network Time Protocol (NTP) and Domain Name System (DNS) servers for DDoS attacks, instead concentrating on vulnerable devices—an issue compounded by users that practice lax security measures.

A large number of these attacks were caused by the use of the default password in the device interface. Thus, users should change their default password as soon as possible and use a strong password for their devices.

However, as seen in the presence of the password-stealing vulnerability mentioned above, a strong password alone does not guarantee device security. IP Camera owners should also implement other steps to ensure that their devices are protected from external attacks. In addition to using a strong password, users should also disable UPnP on their routers to prevent devices within the network from opening ports to the external Internet without any warning.

The burden of IoT security does not rest on the user alone—it's also dependent on the vendors themselves, as they should be the ones responsible for making sure that their devices are secure and always updated. In line with this, users should make sure that their devices are always updated with the latest firmware to minimize the chance of vulnerability exploits.

Trend Micro Solutions

In addition to the best practices mentioned above, users can look into solutions such as Trend Micro™ Security and Trend Micro Internet Security, which offer effective protection for threat's to IoT devices using security features that can detect malware at the endpoint level. Connected devices are protected by security solutions such as Trend Micro Home Network Security, which can check internet traffic between the router and all connected devices. In addition, enterprises can monitor all ports and network protocols to detect advanced threats and protect from targeted attacks via Trend Micro™ Deep Discovery™ Inspector .

Deep Discovery Inspector protects customers from this threat via these DDI Rules:

- DDI beta rule 3664: "IP Camera Remote Code Execution - HTTP (Request)"
- DDI beta rule 3665: "IP Camera Authentication Bypass - HTTP (Request)"

Users with Trend Micro Home Network Security are protected via the following signatures:

- 1133578 WEB GoAhead system.ini Information Disclosure Vulnerability -1 (CVE-2017-5674)
- 1133642 WEB GoAhead system.ini Information Disclosure Vulnerability -2 (CVE-2017-5674)
- 1133641 WEB Shell Spawning Attempt via telnetd -1.u

The Yara rule for detection is provided below:

> rule Persirai { meta: description = "Detects Persirai Botnet Malware" author = "Tim Yeh" reference = "Internal Research" date = "2017-04-21" hash1 = "f736948bb4575c10a3175f0078a2b5d36cce1aa4cd635307d03c826e305a7489" hash2 = "e0b5c9f874f260c840766eb23c1f69828545d7820f959c8601c41c024044f02c" hash3 = "35317971e346e5b2a8401b2e66b9e62e371ce9532f816cb313216c3647973c32" hash4 = "ff5db7bdb4de17a77bd4a552f50f0e5488281cedc934fc3707833f90484ef66c" hash5 = "ec2c39f1dfb75e7b33daceaeda4dbadb8efd9015a9b7e41d595bb28d2cd0180f" strings: $x1 = "ftpupload.sh" fullword ascii $x2 = "/dev/misc/watchdog" fullword ascii $x3 = "/dev/watchdog" ascii $x4 = ":52869/picsdesc.xml" fullword ascii $x5 = "npxXoudifFeEgGaACScs" fullword ascii $s1 = "ftptest.cgi" fullword ascii $s2 = "set_ftp.cgi" fullword ascii $s3 = "2580e538f3723927f1ea2fdb8d57b99e9cc37ced1" fullword ascii $s4 = "023ea8c671c0abf77241886465200cf81b1a2bf5e" fullword ascii condition: uint16(0) == 0x457f and filesize < 300KB and ((1 of ($x*) and 1 of ($s*)) or 2 of ($s*)) }

Related SHA256 Hashes detected as ELF_PERSIRAI.A:

- d00b79a0b47ae38b2d6fbbf994a2075bc70dc88142536f283e8447ed03917e45
- f974695ae560c6f035e089271ee33a84bebeb940be510ab5066ee958932e310a
- af4aa29d6e3fce9206b0d21b09b7bc40c3a2128bc5eb02ff239ed2f3549532bb
- aa443f81cbba72e1692246b5647a9278040400a86afc8e171f54577dc9324f61
- 4a5ff1def77deb11ddecd10f96e4a1de69291f2f879cd83186c6b3fc20bb009a
- 44620a09441305f592fb65d606958611f90e85b62b7ef7149e613d794df3a778
- a58769740a750a8b265df65a5b143a06972af2e7d82c5040d908e71474cbaf92
- 7d7aaa8c9a36324a2c5e9b0a3440344502f28b90776baa6b8dac7ac88a83aef0
- 4a5d00f91a5bb2b6b89ccdabc6c13eab97ede5848275513ded7dfd5803b1074b
- 264e5a7ce9ca7ce7a495ccb02e8f268290fcb1b3e1b05f87d3214b26b0ea9adc
- ff5db7bdb4de17a77bd4a552f50f0e5488281cedc934fc3707833f90484ef66c
- ec2c39f1dfb75e7b33daceaeda4dbadb8efd9015a9b7e41d595bb28d2cd0180f
- f736948bb4575c10a3175f0078a2b5d36cce1aa4cd635307d03c826e305a7489
- e0b5c9f874f260c840766eb23c1f69828545d7820f959c8601c41c024044f02c
- 35317971e346e5b2a8401b2e66b9e62e371ce9532f816cb313216c3647973c32