ASUS warns of Cyclops Blink malware attacks targeting routers

bleepingcomputer.com/news/security/asus-warns-of-cyclops-blink-malware-attacks-targeting-routers/

Bill Toulas

By
Bill Toulas

- March 17, 2022
- 01:12 PM
- 0

Multiple ASUS router models are vulnerable to the Russia-linked Cyclops Blink malware threat, causing the vendor to publish an advisory with mitigations for the security risk.

Cyclops Blink is a malware linked to the Russian-backed Sandworm hacking group that has historically targeted WatchGuard Firebox and other SOHO network devices.

The role of Cyclops Blink is to establish persistence for threat actors on the device, allowing them a point of remote access to compromised networks.

Because Cyclops Blink is modular, it can be easily updated to target new devices, constantly refreshing its scope and tapping into new pools of exploitable hardware.

Cyclops Blink now targets ASUS routers

In a coordinated disclosure, Trend Micro warned that the malware features a specialized module that targets several ASUS routers, allowing the malware to read the flash memory to gather information about critical files, executables, data, and libraries.

The malware then receives a command to nest in the flash memory and establish permanent persistence, as this storage space doesn't get wiped even by factory resets.

For more details on the ASUS module of Cyclops Blink, Trend Micro has published a technical writeup today explaining how it works.

```
size = 0;
buf_to_write = NULL;
mtd = NULL;
if ( buff )
{
  if ( count )
  {
    mtd = j_getnvram();
    if ( mtd )
    {
      if ( mtd->size >= count )
      {
        for ( size = mtd->erasesize; size < count; size += mtd->erasesize )
          ;
        buf_to_write = j_malloc(size);
        j_memset(buf_to_write, 0, size);
        if ( j_lseek(mtd->fd, -size, SEEK_END) != -1 && j_read(mtd->fd, buf_to_write, size) > 0 )
        {
          j_memcpy(&buf_to_write[size - count], buff, count);
          if ( j_lseek(mtd->fd, -size, SEEK_END) != -1 )
          {
            erasesize = mtd->erasesize;
            for ( i = mtd->size - size; i < mtd->size; i += erasesize )
            {
              j_ioctl(mtd->fd, MEMUNLOCK, &i);
              if ( j_ioctl(mtd->fd, MEMERASE, &i) == -1 )
                goto _exit;
            }
            if ( j_lseek(mtd->fd, -size, SEEK_END) != -1 )
              j_write(mtd->fd, buf_to_write, size);
          }
        }
      }
    }
  }
}
```

Module's code for writing to flash memory *(Trend Micro)*

At this point, the spread of Cyclops Blink appears indiscriminate and widespread, so it doesn't matter if you consider yourself a legitimate target or not.

As the malware is tied to the elite Sandworm hacking group (also tracked as Voodoo Bear, BlackEnergy, and TeleBots), we will likely see the threat actors targeting other router manufacturers in the future.

Sandworm has been linked to other well-known cyberattacks, including the BlackEnergy malware behind the Ukrainian blackouts of 2015 and 2016 [1, 2, 3] and the NotPetya ransomware, which led to billions worth of damage to companies worldwide starting in June 2017.

Vulnerable ASUS devices

In an advisory released today, ASUS warns that the following router models and firmware versions are vulnerable to Cyclops Blink attacks:

- GT-AC5300 firmware under 3.0.0.4.386.xxxx
- GT-AC2900 firmware under 3.0.0.4.386.xxxx
- RT-AC5300 firmware under 3.0.0.4.386.xxxx
- RT-AC88U firmware under 3.0.0.4.386.xxxx
- RT-AC3100 firmware under 3.0.0.4.386.xxxx
- RT-AC86U firmware under 3.0.0.4.386.xxxx
- RT-AC68U, AC68R, AC68W, AC68P firmware under 3.0.0.4.386.xxxx
- RT-AC66U_B1 firmware under 3.0.0.4.386.xxxx
- RT-AC3200 firmware under 3.0.0.4.386.xxxx
- RT-AC2900 firmware under 3.0.0.4.386.xxxx
- RT-AC1900P, RT-AC1900P firmware under 3.0.0.4.386.xxxx
- RT-AC87U (EOL)
- RT-AC66U (EOL)
- RT-AC56U (EOL)

At this time, ASUS has not released new firmware updates to protect against Cyclops Blink but have released the following mitigations that can be used to secure devices:

- Reset the device to factory default: Login into the web GUI, go to Administration → Restore/Save/Upload Setting, click the "Initialize all the setting and clear all the data log," and then click Restore button."
- Update to the latest available firmware.
- Ensure the default admin password has been changed to a more secure one.
- Disable Remote Management (disabled by default, can only be enabled via Advanced Settings).

If you are using any of the three models designated as EOL (end of life), note that these are no longer supported and thus won't receive a firmware security update. In this case, you are recommended to replace your device with a new one.

If you own WatchGuard network devices and are looking for that advisory instead, you can find the vendor's threat mitigation advice on this webpage.

Related Articles:

US, UK link new Cyclops Blink malware to Russian state hackers

US offers $10 million reward for tips on Russian Sandworm hackers

Sandworm hackers fail to take down Ukrainian energy provider

US disrupts Russian Cyclops Blink botnet before being used in attacks

Google shut down caching servers at two Russian ISPs

Bill Toulas

Bill Toulas is a technology writer and infosec news reporter with over a decade of experience working on various online publications. An open source advocate and Linux enthusiast, is currently finding pleasure in following hacks, malware campaigns, and data breach incidents, as well as by exploring the intricate ways through which tech is swiftly transforming our lives.