Cologne, August 31, 2023

Bundesamt für Verfassungsschutz

BfV Cyber-Brief No. 02/2023

Groups APT 15 and APT 31 use home network devices for state-sponsored cyberattack campaigns

Groups APT 15 and APT 31 use home network devices for state-controlled cyberattack campaigns

Current indications point to the threat to German small and medium-sized companies shear companies (SMEs) and private households against by cyber attacks home network or Small Office/Home Office (SOHO) terminals. this end devices intended for use in small businesses or by private individuals are designed to be used by cyber attackers in increasing numbers taken over and subsequently used in cyber attack campaigns by the APT group 1 APT 15 and APT 31 **pledges against government and political bodies.**

To protect these SMEs and private households and those via their end devices Ultimately attacked state and political bodies are included in this cyber Briefly, a detailed explanation of the procedure of APT 15 follows and APT 31 as well as specific recommendations for action.

background information

APT 15 is a cyberespionage group that has been very active for years security primarily through attacks on diplomatic targets and on business enterprises became public knowledge (cf. cyber letter no. 01/2020). [2]

APT 31 is also a very active cyber espionage group whose cyber attacks are increasing increasingly aimed at targets in western countries in recent years. below fall, for example, ministries, authorities, political organizations and foundations (cf. cyber letter no. 01/2021). [3]

1 Advanced Persistent Threat (APT): APT refers to complex, targeted threats that directed at one or more victims. The concrete attacks within the framework of these threats ("threats") are elaborately prepared by attackers, become highly developed (“advanced”) and last for a long time (“persistent”).

2 The BfV Cyber-Brief 01/2020 from June 2020 also offered technical information on detection and is on the BfV Website available at www.verfassungsschutz.de.

3 The BfV Cyber-Brief 01/2021 from January 2021 also offered technical information on detection and is open available on the BfV website at www.verfassungsschutz.de.

facts

The Federal Office for the Protection of the Constitution (BfV) has findings about the exploitation protection of compromised home network or SOHO devices by the Cy mountain groupings APT 15 and APT 31. The end devices, which are often used by SMEs as well used by private households are used by the attackers for cyber attack campaigns against government and political bodies.

Cyber attackers' approach

Step 1: Compromise of home network or SOHO endpoints

The cyber attackers compromise home network or SOHO end devices on a large scale Number of pieces. Devices with be were aware of vulnerabilities, especially when support was discontinued by the manufacturer (so-called "end-of-life" devices).

So far, the following terminal device classes have been identified as attacked:

- Home or SOHO router,
- Network storage/hard drives (so-called NAS systems),
- SOHO firewall systems,
- Smart home or home automation systems.

All of the aforementioned end device classes are in the course of development, regardless of the manufacturer affected by the use of vulnerabilities. It is all the more important to ensure safety import dates promptly and end-of-life exchange devices. The range of suitable targets for cyber attackers targeting to align such end device classes is large. Compromiseable systems can be can also be determined with little specialist knowledge and special tools.

Step 2: Incorporation into attacker-specific obfuscation networks

Obfuscation or anonymization networks, also known as Vir in a broader sense tual Private Networks (VPN), basically serve to secure a Communication connection over the public Internet. Such networks exist than products from commercial VPN providers or can be used as freely available Pro products can be used, such as the TOR network. Considered a big advantage generally hiding the original IP address.

The cyber espionage groups APT 15 and APT 31 use this advantage in the context of Cyber attacks to disguise their authorship. Obfuscation networks that allegedly specifically for the cyber espionage groups using the in Step 1 compromised endpoints were created are used.

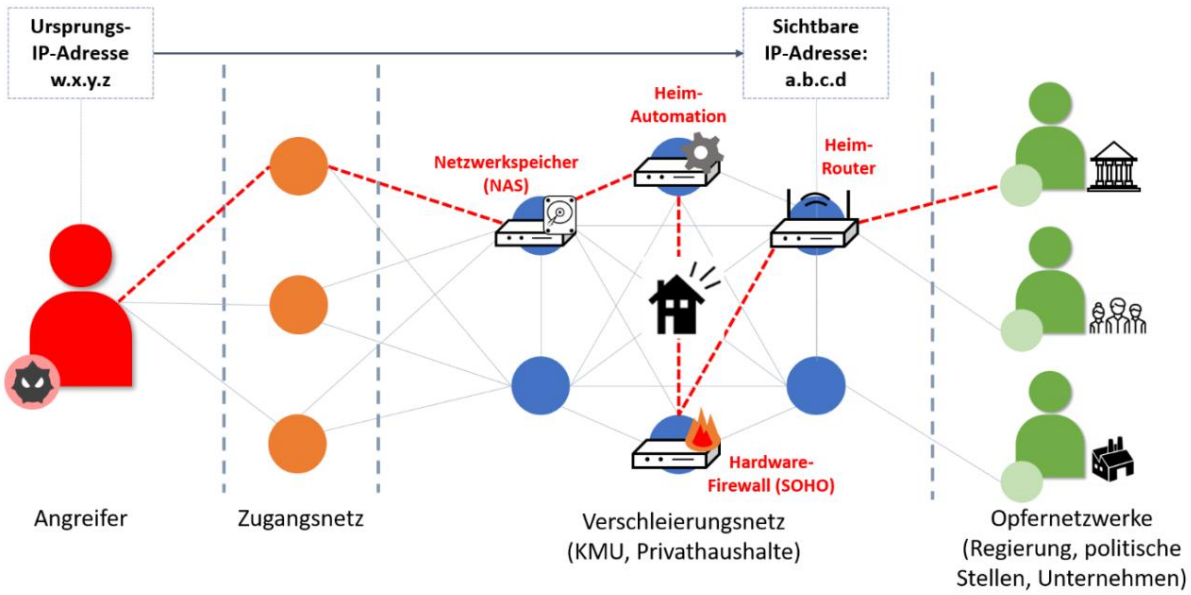

Figure: Schematic representation of an anonymization network

As shown in the figure, the actor (red) first accesses a node in an access network (orange). The access network is then used to access the actual concealment net (blue). Above all, the above-mentioned home network or SOHO terminals can also be found here. Over the network of obfuscation the actor finally calls out the actual victims (green).

The communication link (dashed red) is established by the attacker via a agreed path between the network devices of the obfuscation network builds. The victim usually only recognizes the last instance of the connection – the Home router with its IP address as the attacker. The originating IP address of the to gripper remains hidden. To appear as part of the editing of state controlled cyber attacks, in particular by the groups APT 15 and APT 31, increasing IP addresses of SMEs and private households.

Step 3: Cyberattack against the real targets using obfuscation network

With the help of these compromised endpoints and the resulting attacker network, the groups mainly carry out cyber attacks for espionage purposes against government institutions and political organizations. Also activities ge This makes it possible for companies to conduct economic espionage.

The detection of such attack attempts is important for the attacked organizations difficult, since the incoming connections from private Internet connections in Germany appear little conspicuous. All three steps go through unnoticed the operator. As a rule, there are no breaks in the connection or anything else abnormalities.

There are currently no known cases in which the operators of the home network or SOHO endpoints were themselves victims of a cyber attack. The acquisition of Ge Advice in step 1 has so far only been done to integrate into the concealment networks as described in step 2.

recommendations for action

SMEs and private households should take action to protect externals and therefore Cyberspi
to make it more difficult for groups to end work in companies and private households
devices and use them for cyber attacks against government institutions
and to use political organizations.

From the point of view of the BfV, three steps have priority:

Step 1: Reduce risks

- **Know devices**

  Get an overview of who you are in your network
  driven devices such as routers, network printers and network storage. The
  Also think of Internet of Things or Smart Home devices, as with
  for example controls for roller shutters, lights, heating or solar systems.

  Enter the credentials for management interfaces of all correspond
  the devices together. Make sure that the access data is a secure Ver
  currency.

- **Determine condition**

  Determine the status of the operated devices in your network. Is the
  Router still up to date? Current versions should be used here
  of the devices are recorded and checked for updates.

  Many manufacturers offer an automated update procedure via the user
  surface of your devices. The user's hand often provides information about this
  book. If you have the automated updates feature enabled, check
  Check whether the respective devices are still supplied with updates by the manufacturer
  become.

  Reputable manufacturers usually offer transparent handling of devices for
  for which no updated program versions are available ("End
  of Life" devices). For this purpose, they provide corresponding information on their website

Lists with device types or other query options. Inform
Check older devices to see if they may not have an updated Pro
gram versions more received.

Replace obsolete equipment if necessary.

Step 2: Harden systems

- **Make updates**

If you have outdated software on your devices, play what's available
(Security) updates promptly. Make updates should work for you
regular maintenance tasks for your equipment. Make
So make a plan and set reminders.

- **Maintain and maintain devices in the network**

Don't just update once, keep your devices persistent
up-to-date: Pay attention to the corresponding manufacturer information about already available
upcoming new program versions/updates or software to fix
Program errors, so-called patches. Also note current information
ions and notes on vulnerabilities and cyber attack campaigns. To use
You should also look at the public information available, for example from the
Federal Office for Information Security (BSI).4

- **Secure networks**

Devices integrated into your IT networks such as those you allow access
Rights for outsiders open the door to attackers. Check for remote access
from outside/on the go to your home network or smart home devices
is really required. Remove any previously set releases in the
Firewall settings on your router as soon as they are no longer needed
the. Also consider whether, for example, a web server from the office or

4 Cf. https://bsi.bund.de; Key word: “consumers”.

home network must be operated or a qualified provider (a so-called ter hoster) can take on this task.

- **Shut out cyber attackers**

  Design the operating systems you use and soft ware and cloud applications in such a way that you close unnecessary accesses and switch off or, if necessary, uninstall functions that are not required. With a Such hardening protects you better against cyber attacks of all kinds.

  Also check whether the default settings specified by the manufacturer, esp special security settings, can be changed sensibly for your use can.

Step 3: Exclude (new) attack surfaces

- **Consider IT security in your purchasing decisions**

  When making your purchasing decisions, check whether and for how long devices you want to advertise, get support from the manufacturer.

  Check products with cloud components such as security cameras Cloud storage, where and for how long data is stored and who is on it can access. Consider whether you want to entrust your data to the cloud provider want to trust.

- **Secure passwords**

  Change within the possibilities given by the manufacturer Default passwords for your devices.

  Use complex passwords, especially for access from outside. Use the BSI's instructions for creating secure passwords.5

5 Cf. https://bsi.bund.de; "BSI Basic Protection: Secure Passwords".

If possible, enable multi-factor authentication

More security for your connected devices and online accounts.

Further information

For more information on government-sponsored cyberattacks, visit the

Website of the BfV.6 Here you will find, in addition to the Federal Office for the Protection of the Constitution,

further cyber letters, the security instructions for business, politics and administration

tion, the economic protection information sheets and the leaflet “Cyberattacks: Ge

Recognizing driving – minimizing risks”. These BfV materials offer additional

Recommendations for action to protect against cyber attacks.

6 Vgl. www .verfassungsschutz.de.

imprint

Publisher
Federal Office for the Protection of the
Constitution
Department 4
Merianstraße
100 50765 Cologne
poststelle@bfv.bund.de
www.verfassungsschutz.de
Tel.: +49 (0) 228/99 792-0 Fax: +49 (0) 228/99 792-2600

Picture credits
© maxsim | fotolia.com

Stand
August 2023