Moqhao masters new tricks

telekom.com/en/blog/group/article/moqhao-masters-new-tricks-1031484

Blog.Telekom

03-31-2023
TR4xx@DTSecurity

0 Comments

- Share Share
  Two clicks for more data privacy: click here to activate the button and send your recommendation. Data will be transfered as soon as the activation occurs.

- Print
- Read out

Ever received a text message alerting you to problems with the delivery of a package - even though you weren't waiting for one? Then you've already met Moqhao in person, also known as Shaoye or XLoader. Moqhao is something like the bestseller from the Roaming Mantis malware family, ready to build a backdoor into your smartphone's Android operating system.

This group of Android malware is a proprietary brand of the Yanbian Gang. A Chinese threat actor also known for its DNS hijacking campaigns, where they "redirect" visitors from websites. Deutsche Telekom Security has been tracking the Yanbian Gang and consequently Moqhao infections since 2021. As result from our tracking, we discovered a new major feature introduced to Moqhao in order bypass CAPTCHA security access mechanisms in wireless routers. Right, the one with the combination of letters and numbers used as images.

This technique has not been attributed to the Yanbian Gang before. Instead, the security community has only speculated on how vulnerable routers were previously compromised by the actor. Now, we have found new evidence on how they are able to hijack wireless routers via Moqhao. In this blog post, we describe how these attacks are executed by Moqhao and what measures can be taken to prevent them.

Moqhao a key malware player of the Yanbian Gang

The Yanbian Gang is a threat actor that has been active since 2013 with operation from the Yanbian Prefecture in Jilin, China. Over the years, the Yanbian Gang expanded their criminal operation to target countries all over the world with a collection of Android malware known as the Roaming Mantis. This collection includes fake apps that impersonate banking services, engage in cryptomining, multilingual phishing, and other fraudulent activities.

As part of the Roaming Mantis, Moqhao was first discovered in 2015. Deutsche Telekom Security started monitoring this malware in February 2021 after multiple customers reported fake SMS messages. These messages indicated that a parcel has been sent and urged users for verification. An example of Moqhao's SMS Smishing (SMiShing) messages is shown in figure 1.

Figure 1: An example of Moqhao's fake SMS messages indicating that a parcel has been sent and urging users for verification.

Messages sent as part of Moqhao's campaign appear harmless and authentic at first, but they contain links from where the Moqhao malware is downloaded onto the victim's device. The downloaded file containing Moqhao, poses as an update of a legitimate App such as Facebook or Chrome. Once installed, it can be used to steal sensitive information, install additional apps, hijack the infected device to send SMiShing messages and recently for DNS hijacking in wireless routers. Once Moqhao obtains full control over the infected device, the device is used to engage in SMiShing campaigns to infect further victims.

Moqhao infects wireless routers to perform DNS hijacking attacks

Since the beginning of our tracking, efforts have been focused on monitoring Moqhao's activity in order to prevent infections and/or notify our customers in the event of an infection. During July 2022, we published an alert about new SMiShing waves spreading an updated version of Moqhao in Germany. The campaign exhibited geofencing and operating system checks which proves that the Yanbian Gang tailors their attacks to their victims (e.g., for German speaking users) and avoid detection while trying to keep a low profile.

As part of our monitoring, we periodically conduct analysis of Moqhao samples obtained during these SmiShing campaigns. As result of such analyses, we discovered a previously unknown feature in Moqhao to bypass text-based CAPTCHAs. This feature is used in combination with brute-force attacks on wireless router's web interfaces to compromise routers and perform DNS hijacking attacks.

DNS hijacking is a technique used to redirect network traffic to for instance malicious websites by altering the DNS resolution. In other words, Moqhao's intention is to seize the translation process of human-readable domain names (such as www.telekom.com) into IP addresses. This allows Moqhao to redirect the victims web traffic to malicious websites that mimic legitimate sites to steal sensitive information or deliver copies of Moqhao.

Wireless routers are critical in DNS hijacking because they contain information needed to perform this resolution process. This means that even if victims type in a legitimate website, their traffic is redirected to a fake one owned by an attacker.

What are CAPTCHAs and why are they important to Moqhao?

In terms of home network security, one of the most important devices we should try to protect is our router. They allow devices within a local network to reach resources on the Internet by relaying traffic between local network devices and remote servers. If routers are infected, threat actors may be able to capture or manipulate network traffic that the router relays. Threat actors like the Yanbian Gang have identified the criticality of routers and began targeting them for malicious purposes.

Router's settings and network configurations can often be accessed using a web-based login page that devices from the local network can access. By gaining access to the router's web page, all kinds of sensitive information such as login credentials, network configurations, and other personal data can be accessed and/or manipulated.

To prevent unauthorized access through brute-force attacks on the router's login panel, many manufacturers use CAPTCHAs to prevent automated authentication attempts. CAPTCHAs are verification challenges used to confirm that a user is a human opposed to a computer program. They consist of one or more morphed pictures that contain random objects, numbers and/or characters. To pass the verification step, the system asks the user to enter the content of the image into an input box or to perform an action based on such content. By requiring a human to complete the challenge, the system can verify that the user is legitimate and prevent automated attacks. Therefore, users need to confirm that they are human when logging in.

This procedure relies on the fact that automated attacks should not be able to complete the task of solving the challenges on the image. Unfortunately, not all CAPTCHAs are secure against machine learning mechanisms. Poorly designed CAPTCHAs that rely on fixed patterns of letters are vulnerable to Optical Character Recognition (OCR) engines. This is especially true for the CAPTCHA mechanism targeted by Moqhao's latest version.

In short, Optical Character Recognition is a mechanism designed to recognize and extract text from images. OCR engines work by analyzing a CAPTCHA image using pattern recognition algorithms to identify the characters on the image. Analogously, Moqhao can therefore profit from OCR to trick a system and bypass CAPTCHA challenges that rely on text-based verification.

Figure 2: Example of a CAPTCHA challenge from ipTIME routers.

Moqhao's new ability to PWNtcha your wireless router

Over the years, the Yanbian Gang has invested a lot of resources to maintain and improve Moqhao's features. A recent example of the Yanbian Gang's dedication to Moqhao's development is the adoption of OCR techniques. This represents a key addition in order to take over routers to perform DNS Hijacking.

When trying to "PWNtcha" (defeat via CAPTCHA challenge) a vulnerable router, Moqhao first determines the IP address of the router to request its web-based administration pages. By accessing this default pages, Moqhao can determine the router's model. Next, Moqhao compares the router model against a hardcoded list of vulnerable routers to decide whether it proceeds with the attack.

When Moqhao identifies a vulnerable model, it crawls the router's web-admin pages searching for specific patterns. These patterns are based on hardcoded strings embedded in Moqhao's configuration to extract login forms and images from the CAPTCHA challenges. If such predefined patterns are matched, Moqhao uses a list of default usernames and passwords such as "admin:admin". Although, the amount of hardcoded credentials in Moqhao is limited, default login combinations can be easily extended by the actor. For example, dictionary-based passwords or stolen credentials could be added to Moqhao's configuration to target further router models or tailor attacks to other devices in the future.

As described before, the malware needs to circumvent the router's CAPTCHA challenges to gain access to the router's settings. To achieve this, Moqhao forwards CAPTCHA images to an API-based OCR translation service that converts CAPTCHA images to text. If the OCR service successfully returns the correct text, the malware can brute force the login credentials to successfully take over the router.

Moqhao's OCR Translation Service

As part of its configuration, Moqhao depends on a list of profile account IDs hosted on different social media platforms. These profiles are created using false information such as name, location, age and gender to deceive others into believing that the profile belongs to a real person. The main purpose of these fake profiles is to publish information regarding the malware's infrastructure while avoiding detection. This information includes for example, the location of the C&C server, a rogue DNS service used for DNS Hijacking and its new OCR translation service. During Moqhao's execution, these profile accounts are accessed to dynamically retrieve network configuration updates made periodically by the threat actor.

Deutsche Telekom Security conducted analysis of the malware in order to extract the malicious profile IDs directly from malware. By extracting these IDs, it is possible to track where Moqhao's endpoints are published and obtain the malware configuration as soon as it gets updated.

Our collected data regarding profile accounts overlaps with Kaspersky's latest report on Moqhao's latest campaign. However, in addition to the DNS changer accounts reported by Kaspersky., we were able to obtain the OCR accounts and verify the use of this translation service. For example, samples that we analyzed connected to a social media profile hosted on vk.com which ID is id729071494. vk.com is a Russian social network analogous to Facebook. From this profile, Moqhao was able to retrieve the URL of a file called gif.txt hosted at **107.148.162[.]237:28810/gif.txt**.

Figure 3: OCR service information posted on hxxps://m[.]vk[.]com/id729071494?act=info.

When Moqhao requests the content of the gif.txt file shown in figure 2, i.e., **107.148.162.237:28810/gif.txt**, it obtains another IP, port and path which belongs to the OCR service, i.e., **27.124.38[.]58:10052/ocr.html.** Although, it is unknown what type of OCR backend system the threat actor uses or whether they rely on a proprietary solution, there are numerous services that can solve CAPTCHAs automatically.

Moqhao's OCR service is currently exposed to anyone on the Internet and is not protected by any form of authentication. As of February 2023, this service could be further employed by other criminals as a free CAPTCHA-bypass mechanism. At the time of our analysis, access to one of the vulnerable router models was not available. To overcome this limitation, we tested Moqhao's OCR service by emulating Moqhao's network communication.

To verify if Moqhao's OCR service is able to defeat the CAPTCHA challenges, we used the public CAPTCHA generator from one of the vulnerable router brands, i.e., ipTIME, which available here. These challenges are examples of the CAPTCHAs presented to the users during login and targeted by Moqhao.

We sent multiple requests to Moqhao's OCR service with these CAPTCHAs, i.e, the gif image files. For all of our test images using ipTIME's generator, we were able to successfully retrieve the correct codes as text. However, when using CAPTCHAS of other router brands and models, its success rate dropped. Therefore, we conclude that the threat actor's OCR translation service was designed to target Moqhao's list of router models specifically.

"ipTIME N3-i\nipTIME N604plus-i\nEFM Networks ipTIME N604plus-i"
"EFM Networks - ipTIME Q104\nEFM Networks ipTIME Q104"
"EFM Networks - ipTIME Q204\nEFM Networks ipTIME Q204\nEFM Networks ipTIME V108"
"EFM Networks ipTIME Q604\nEFM Networks ipTIME Q604 PINKMOD\nEFM Networks ipTIME N104R\nEFM Networks ipTIME N604R\nEFM Networks ipTIME Q504\nEFM Networks ipTIME N5\nEFM Networks ipTIME N604V"
"EFM Networks ipTIME N104T"
"EFM Networks - ipTIME G301"
"title.n704bcm\ntitle.a8004t\ntitle.a2004sr\ntitle.n804r"
"title.n104e\ntitle.n104pk\ntitle.a1004ns\ntitle.a604m\ntitle.n104pi\ntitle.a2008\ntitle.ax2004b\ntitle.n104q\ntitle.n604e\ntitle.n704e\ntitle.n704v3\ntit
"title.v504\ntitle.n1p\ntitle.n704bcm\ntitle.ew302\ntitle.n104qi\ntitle.n104r\ntitle.n2p\ntitle.n608\ntitle.q604\ntitle.n104rsk\ntitle.n2e\ntitle.n604s\ntitle.
"title.a604v\ntitle.n6004r\ntitle.n604p\ntitle.t3004\ntitle.n5\ntitle.n904\ntitle.a5004ns\ntitle.n8004r\ntitle.n604vlg"
Strings of wireless router models hardcoded in Moqhao's configuration.

Once Moqhao has gained access to the router's web admin, it continues to hijack the router's DNS settings as described here. Moqhao's final goal is to deliver copies of the malware on devices connecting to the compromised network via DNS hijacking.

Victims

Based on our telemetry, infections with Moqhao continue to happen via SMiShing campaigns in Germany. However, we have no indicators of victims of Moqhao's PWNtcha attacks at the time of writing.

By extracting the list of router models from the malware, we conclude that the current campaign targets users of wireless routers located in Asia, mainly in South Korea as reported by Kaspersky.

Deutsche Telekom Security is constantly monitoring Roaming Mantis related infrastructure and implementing protection mechanisms. As part of Moqhao's infrastructure, we have identified well-known Roaming Mantis IPs and monitor the registration of domain names on these IPs that are potentially used as landing pages. These landing pages serve as the destination to where the victims are lured during the Yanbian Gang's phishing scams. In other cases, these are used as well to host Moqhao payloads.

Our focus remain primarily on preventing customers from contacting the aforementioned Moqhao's malicious end-points. Our efforts also include detecting new Moqhao infections in order to notify customers and provide assistance during the cleanup process.

Conclusion

As more and more people rely on wireless routers to connect to the Internet, the risk of similar attacks to the one implemented by Moqhao is likely to increase. CAPTCHA attacks on routers can be challenging to detect and can compromise the security of an entire network. Once a router is compromised, attackers can use it as a launching pad for further attacks.

Neglected routers with poor CAPTCHA implementations and the use of weak passwords can additionally contribute and make such attacks effortless in order to gain unauthorized access or even take control of an entire network. In this regard, Moqhao and its OCR translation service are a successful duet for a chain of exploits that it starts with gaining unauthorized access to the router's web-admin and ends with hijacking the DNS settings of the compromised routers. During this scenario the potential for havoc from Moqhao is not only limited to spreading itself. Instead, it is rather limited only by the threat actor's interest.

Despite the Yanbian Gang actively using this attack only in South Korea as of March 2023, Deutsche Telekom Security believes in the possibility of this group extending the scope of these attacks to target victims in other countries. Although, router models targeted by Moqhao are currently not used in Germany, Moqhao's PWNtcha serves as a successful proof of concept to mimic and further extend. For instance, attackers can easily modify the list of default passwords and router models to include more popular brands such as FRITZ!Box, TP-Link, D-Link, etc. As a result, it is important for users to take steps to protect from these attacks.

Recommendations

In order to protect from Moqhao's router PWNtcha attacks, it is recommending the following practices:

- Change the default user+password combination for the web admin interface of your router and use a strong password when applying this change.
- There are several CAPTCHA systems available, each with varying levels of security. Choose a router model with strong CAPTCHA system.
- If your router model allows it, implement two-factor authentication to provide an extra layer of security. This can help prevent unauthorized access even if the CAPTCHA is bypassed.
- Make sure your router's firmware is up to date and that security patches have been applied. This can help prevent vulnerabilities from being exploited.
- Never install firmware from third-party/unknown sources.

Overall, a combination of these measures can help protect against CAPTCHA attacks and maintain the security of your wireless router.

IoCs

Hashes

83ba2b1c0352ea9988edeb608abf2c037b1f30482bbc05c3ae79265bab7a44c9
6e28c76b07d64fd1d0479d328207082b8d29f4560433d7f075328aa236a4f1ab
6b9fa3df72fc684f307cd6bac06788c2cd83ceb44ab9e5e04671b8ed1c107aad
89e593dc246cb0b4ef8decf59c3260697677e703d609a24807cb6ea58c0deda4
6257da70cb01826a6ce575e23cd2e42a0dbdc742f9b529f06fa9a13224701823
780992147fd4b8fd5c780f4fe1a5237a1729c61ec99dda010fe9313bb5ef5bac

C&C server accounts

https://imgur.com/user/shaoye99/about
https://imgur.com/user/shaoye88/about
https://imgur.com/user/shaoye77/about
https://m.vk.com/id674309800?act=info
https://m.vk.com/id674310752?act=info
https://m.vk.com/id674311261?act=info

https://m.vk.com/id730148259?act=info
https://m.vk.com/id730149630?act=info
https://m.vk.com/id761343811?act=info
https://m.vk.com/id761345428?act=info
https://m.vk.com/id761346006?act=info

OCR Translation Service
hxxps://m[.]vk[.]com/id729071494?act=info
107.148.162[.]237:28810/gif.txt

Configuration included in gif.txt:
27.124.38[.]58:10052/ocr.html

Rogue DNS
hxxps://m[.]vk[.]com/id728588947?act=info
107.148.162[.]237:26333/sever.ini

Configuration included in sever.ini:
[Severkt]----sever=193.239.154.16----sever1=193.239.154.17----
[Seversk]----sever=193.239.154.16----sever1=193.239.154.17----
[Severother]----sever=193.239.154.16----sever1=193.239.154.