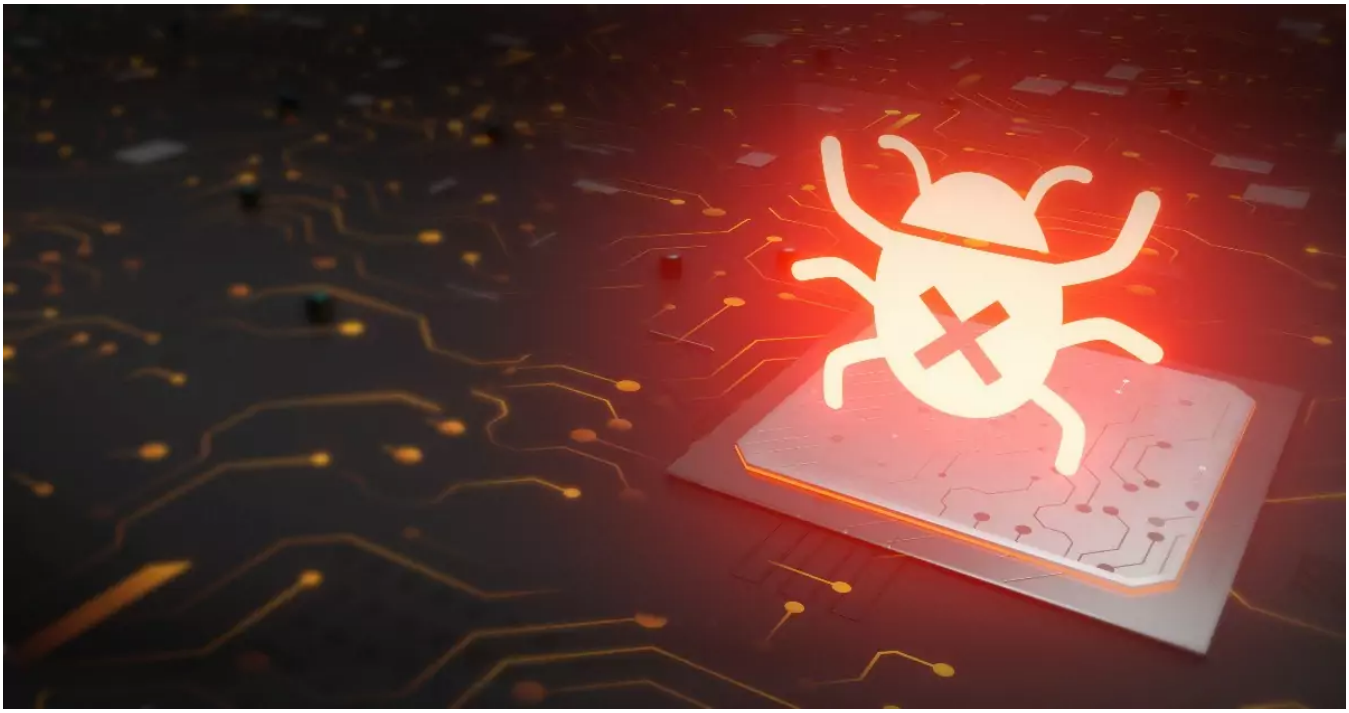
Stealthy WailingCrab Malware misuses MQTT Messaging Protocol



Light Dark

November 21, 2023

By Charlotte Hammond, Ole Villadsen, Kat Metrick

14 min read

Threat Intelligence X-Force

Cookie Preferences

Hammond and contributions from Ole Villadsen and Kat Metrick.

IBM X-Force researchers have been tracking developments to the WailingCrab malware family, in particular, those relating to its C2 communication mechanisms, which include misusing the Internet-of-Things (IoT) messaging protocol MQTT.

WailingCrab, also known as WikiLoader, is a sophisticated, multi-component malware delivered almost exclusively by an initial access broker that X-Force tracks as Hive0133, which overlaps with TA544. WailingCrab was first observed in December 2022, and since then it has been used extensively in email campaigns to deliver the Gozi backdoor often against Italian targets. In recent months, Hive0133 has targeted organizations beyond Italy with email campaigns delivering WailingCrab, frequently using themes such as overdue delivery or shipping invoices.

The malware authors have focused on stealth and anti-analysis techniques in the continued development of the WailingCrab malware. The malware itself is split into multiple components, including a loader, injector, downloader and backdoor, and successful requests to C2-controlled servers are often necessary to retrieve the next stage. Legitimate, hacked websites are used for initial C2 communications to lower the chance of network detection, and payloads are often hosted on well-known platforms such as Discord. C2 servers are often taken down quickly or stop responding soon after a campaign which may prevent threat researchers from accessing them and retrieving the next stages of the malware. Additionally, WailingCrab makes use of code obfuscation, anti-analysis, and anti-sandbox techniques throughout its code.

WailingCrab's core component is its backdoor, which is installed on the system only if the malware's initial stages are completed successfully. Since mid-2023, WailingCrab's backdoor component has communicated with the C2 using the MQTT protocol which is a lightweight IoT messaging protocol. MQTT uses a publish/subscribe architecture, whereby messages are published to 'topics' and received by subscribers, with message distribution handled by a centralized broker. In this instance, WailingCrab uses the

WailingCrab's use of the MQTT is notable, as this protocol is not commonly used by malware. There have only been a handful of instances reported, with the most recent being the MQsTTang backdoor attributed to the threat actor Mustang Panda. As a result of this, the protocol's use may not be monitored as closely by security teams, allowing the backdoor's C2 communications to fly under the radar.

This blog provides an overview of WailingCrab and its C2 communications, with a focus on its use of the MQTT protocol.

Delivery

Since its inception, WailingCrab has been distributed via email spam campaigns using Microsoft Excel attachments, Microsoft OneNote attachments or PDF attachments. In recent months, Hive0133 has favored the use of PDF attachments containing malicious URLs in their email campaigns delivering WailingCrab. When clicked, the links will download and execute JScript files, which in turn will download and execute the WailingCrab loader, which is usually hosted as an attachment file on Discord. Below is an example of a Hive0133 email campaign delivering WailingCrab on 19 October.

Figure 1: Hive0133 Email from 10/19/2023 delivering WailingCrab Loader.

Figure 2: Hive0133 Email PDF Attachment with Malicious Link Leading to WailingCrab Loader.

WailingCrab components

Many of the technical details of WailingCrab's operation and early variants have already been discussed in other research, therefore in this blog, we will focus on new developments and those aspects which have not already been reported on.

The primary samples used for this research are **24c5f4868dc5af255edbb993d98de51a** and **f6ea7ec5d94bc65bf82a6b42b57a6c82**, which were from campaigns in September, and **f6d0b9617405f35bb846d671edda75d3** which was observed in July and is the reference for the earlier version of the MQTT protocol use. These samples are all first-stage WailingCrab Loaders, which

blog were all unpacked or downloaded by these loaders.

WailingCrab loader

The first component of WailingCrab is its loader, which commonly uses a legitimate DLL file as a template, with the malicious code patched over one of the DLL's exported functions. Its purpose is to load the second stage which is stored within the DLL as an encrypted shellcode.

This initial loader component of WailingCrab has received a few updates in more recent samples. In the previous version, the loader would overwrite its own data section in memory with the code for its second-stage component. In the new version, the malware first loads a legitimate Windows DLL, such as **BingMaps.dll**, and then overwrites the code for one of the DLL's exported functions with WailingCrab's second-stage shellcode. It also patches the code at the DLL's original entry point such that it returns immediately rather than running its original code, allowing execution to proceed unimpeded to the maliciously patched export function.

The WailingCrab loader then creates a new thread to run its second-stage shellcode within the context of the legitimate loaded DLL.

WailingCrab injector

The second stage is the WailingCrab injector, the functionality of which has not changed much from the previous version.

The Injector component starts by looping through the currently running processes on the host system and creates a hash of each process filename until it finds one that matches its target hash, which in the analyzed sample corresponds to **explorer.exe**. At this point, the malware will also compare the hash of each running process name to a list of hashes associated with sandbox or debugging applications, and will not continue if any of these are found.

component using XOR and writes the decrypted payload contents to the allocated memory region, along with a string containing the file path of the initial loader.

Next, WailingCrab searches the DLLs loaded within the target process (i.e. explorer.exe) and looks for ntdll.dll. Within the ntdll.dll instance, it finds the address of a target API function, in this case, **RtlWow64GetCurrentMachine**. It then overwrites the contents of this function with 12 bytes of trampoline hook code, the purpose of which is to jump to the start of the copied payload.

The malware then creates a new thread within the target process. The start address of the thread is set to that of the hooked API function, e.g. **RtlWow64GetCurrentMachine**. Upon creation, the new thread executes the target API function, which now contains the hook code, and this then transfers execution to the payload, which is the next WailingCrab component.

WailingCrab downloader

The third WailingCrab component is a Downloader/Loader, which is responsible for loading the Backdoor component. The code for this stage is run within the context of the injected process; in this case, **explorer.exe**.

Much of the functionality of the downloader is the same as in previous versions, however, there have been some updates. In prior versions, this component would download the backdoor, which would be hosted as an attachment on the Discord CDN. However, the latest version of WailingCrab already contains the backdoor component encrypted with AES, and it instead reaches out to its C2 to download a decryption key to decrypt the backdoor.

The WailingCrab downloader starts in the same manner as prior versions, by sleeping for a set period, and then deleting the original loader file on disk. It also creates a mutex, where the mutex name is a hardcoded numeric string, for example, “**823264″**.

https://www.wikipedia.org/ and also a non-existent domain and confirming that the results of both are what it expects. However, these checks have been removed from the new version, and the malware proceeds straight to C2 communication.

WailingCrab proceeds to register with the C2. It randomly generates bot ID values and also gathers basic system information including domain, hostname, username, language and system time. These values are then formatted into a pipe-delimited string, along with an eight-digit campaign ID which is hardcoded into the malware.

In the previous version, the randomly generated bot ID was a single eight-digit string, however in the new variant three 16-digit strings are generated instead, and these will be used later on by the backdoor component as MQTT topic names during its communication with the C2.

Previous Version:

Click and scroll to view full table

New Version:

Click and scroll to view full table

This string is then base64 encoded and added to the Cookie field in the HTTP registration request sent to the C2. The C2 URL is chosen at random from a list, and the following URLs were present in the analyzed sample:

view full table

The C2 registration domains are usually legitimate WordPress-based websites that have been compromised by the threat actor to include a malicious PHP file that processes the requests from the WailingCrab malware. When a request is made to one of these URLs with the correct cookie set, the malicious PHP code inserts a comment into the source code of the returned webpage which contains the response data for the downloader.

The below image shows a request being made to one of the C2 URLs, where the cookie field contains the base64 encoded registration string.

If the registration request is successful, the source code of the returned web page will contain a comment containing the word ‘gmail’ followed by a base64 string, similar to that seen in the below image.

In prior versions of WailingCrab, the base64 response would be decoded to reveal a Discord CDN URL path which the next stage of the malware could be downloaded from.

In the new version, the decoded base64 instead contains an encrypted AES [illegible]e first 8 bytes of the decoded data are XOR’d together,

The AES key is then used by WailingCrab to decrypt the backdoor component using AES-256 in CBC mode with a null-byte IV. The backdoor code is then executed.

WailingCrab backdoor

The WailingCrab backdoor is a sophisticated piece of malware responsible for installing persistence and beaconing to the C2. The backdoor installs itself in a randomly named subdirectory of either the user's %AppData% folder or the %ProgramData% folder. WailingCrab copies several files to this directory and modifies some by overwriting them with chunks of its code:

Click and scroll to view full table

WailingCrab installs persistence by creating a randomly named subkey under the registry Run key and adding the file path of the copied and randomly renamed **printfilterpipelinesvc.exe** file. When this file is executed it loads the modified version.dll file via DLL hijacking, and execution then jumps between the various WailingCrab code chunks loaded from the other files, eventually ending up within an injected **explorer.exe** instance. The full technical details of this process are beyond the scope of this blog but are available in our full malware report on X-Force Exchange.

MQTT communication

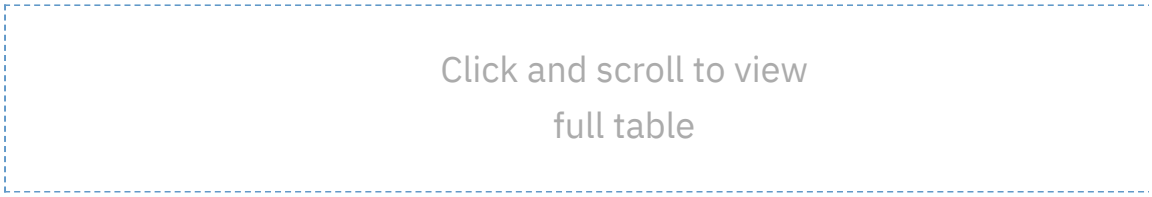
Communication between the WailingCrab backdoor component and the C2 is performed using the MQTT protocol which is a lightweight IoT messaging protocol. MQTT uses a publish/subscribe architecture, with message distribution handled by a centralized broker. WailingCrab uses a third-party

The basics of the MQTT protocol are quite straightforward. The client starts by sending a connect request to the broker, specifying its client ID, which the broker then acknowledges. After that the client can either publish messages to specific 'topics', or it can request to subscribe to a topic. Any clients who are subscribed to a topic will then receive future messages published on that topic.

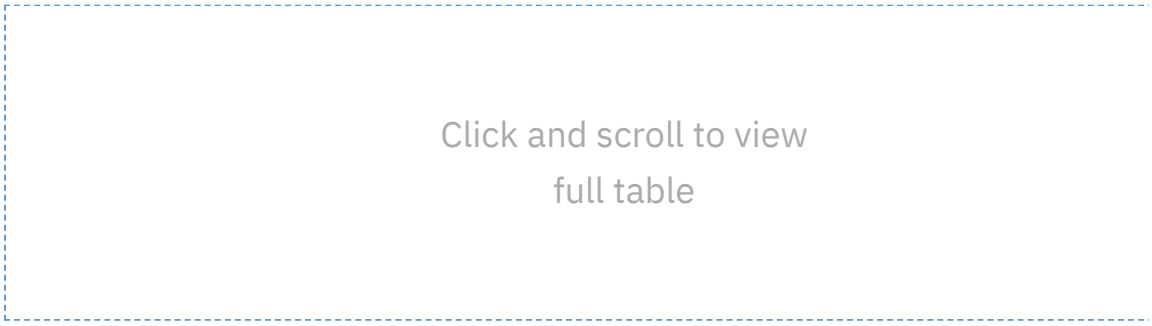
Previous version

We initially observed WailingCrab using the MQTT protocol in mid-2023, and this version of the backdoor communicated with the C2 using the following procedure.

1. The backdoor starts by sending a connect request to broker.emqx[.]io using a randomly generated client ID.



2. It then registers with the C2 by publishing a message to a topic named using the same campaign ID string found in the WailingCrab downloader. The registration message is 25 characters long and consists of the number '1', which is likely the message type, followed by a randomly generated 16-digit string, followed by the eight-digit bot ID generated by the downloader. For example:



3. The purpose of the randomly generated 16-digit string L782546) is for it to be a client-specific topic name for the

backdoor sends a subscribe request to the MQTT broker with the topic name set to this 16-digit string, which means that the broker will forward any future messages published to this topic to the backdoor. Once the subscription request is sent, the broker will then respond with a 'subscribe ack' packet to acknowledge the subscription request.

Click and scroll to view full table

4. The backdoor then publishes a general 'check-in' type message to the campaign topic, which consists of the character '2' followed by the eight-digit bot ID.

Click and scroll to view full table

5. At this point, the backdoor checks for any received messages. The C2 will publish any messages for the target to the client-specific topic, which the broker will then forward to the backdoor since it has subscribed to that topic. The messages from the C2 take the form of the character '0' if the C2 does not have any further instructions for the client, or the character '2' followed by a download path:

Click and scroll to view full table

6. If the backdoor receives a download path from the C2 it will append the received path string to the URL

backdoor will then download a payload from the constructed URL, decode it using base64 and then decrypt it using the same XOR-based algorithm used throughout the malware. The malware will generate a random filename with the .log extension, write the payload to the user's Temp directory, and then execute the file by creating a new process with the following command:

Click and scroll to view full table

7. The backdoor will then report the status back to the C2 by publishing a message to the campaign channel. If the payload download and execution operation was a success then it will send a message consisting of the character '3' followed by the bot ID. Otherwise, if there was an error, it will send the character '4' followed by the bot ID.

Click and scroll to view full table

8. The malware will then disconnect the MQTT connection and then sleep for a fixed period of time before checking in with the C2 again.

New version

Newer versions of WailingCrab, observed from September 2023 onwards, use an updated protocol when communicating with the C2.

As described above, in the previous version, all clients infected by a specific campaign would register with and send regular check-in messages to a single centralized MQTT topic named after the campaign ID. The initial registration message sent by each client would then contain a randomly generated 16-character numeric string which would then serve as the name of a client-specific topic where the C2 could send commands/payloads to the respective client.

topics, the names of which are taken from the three randomly generated 16-digit strings created by the downloader component and shared with the C2 as part of its initial request to the WordPress C2 URL.

For example, if the initial registration request sent by the downloader component contained the following:

Click and scroll to view full table

Then the three client-specific topic names would be:

Click and scroll to view full table

The use of Discord for hosting payloads has also been removed from this stage of the malware, and the backdoor now receives a shellcode-based payload directly from the C2 via MQTT rather than a Discord-based download path.

A full breakdown of the new C2 communication protocol is as follows:

1. As with the previous version, the backdoor starts by sending an MQTT connect packet to broker.emqx[.]io via TCP port 1883 using a randomly generated eight-character client ID.

   Click and scroll to view full table

2. It then retrieves the local time of the infected system and constructs a datetime structure which it encodes using base64. The backdoor then publishes a message containing the base64 string, with the topic set to the second of the randomly generated topic names.

Click and scroll to view
full table

3. The backdoor then sends a subscribe request to the third topic.

Click and scroll to view
full table

4. The backdoor checks to see if it has received any messages via the subscribed topic, and then sends a disconnect packet. If no message is received, the malware proceeds to sleep and then restart the communications loop. If a message has been received, the backdoor checks that the length is greater than 128 bytes, and if so proceeds to decode it from base64. The first 8 bytes of the decoded payload contain a payload ID value, and the second set of 8 bytes is used to calculate the XOR key to decrypt the rest of the payload data. The backdoor expects the decrypted payload to be another shellcode component which it then executes in a new thread.

Click and scroll to view
full table

5. If a payload is received then, the backdoor reconnects to the MQTT client using a new randomly generated client ID. It then publishes a message with the character '0' to the third client-specific topic acknowledging receipt of the payload, and publishes a second message to the first client-specific topic with the results of loading the payload. This message consists of the eight-byte payload ID followed by either the character '3' if the payload was executed successfully, or the character '4' if an error was encountered. The backdoor then sends a disconnect packet and proceeds to sleep before restarting the communications loop.

Click and scroll to view full table

Conclusion

The move to using the MQTT protocol by WailingCrab represents a focused effort on stealth and detection evasion. The MQTT protocol is currently not commonly used by malware. It therefore is unlikely to come under much scrutiny by existing security solutions, especially in environments that use MQTT for legitimate IoT traffic. However, as MQTT is primarily used for IoT traffic, this may also make malicious use of it easier to detect in environments or systems that should not have IoT-related activity.

The newer variants of WailingCrab also remove the callouts to Discord for retrieving payloads, further increasing its stealthiness. Discord has become an increasingly common choice for threat actors looking to host malware, and as such it is likely that file downloads from the domain will start coming under higher levels of scrutiny. Therefore, it is not surprising that the developers of WailingCrab decided on an alternative approach.

The upgrades to the C2 communication protocol have also been an unfortunate blow to security researchers. In the initial version, the use of the communal campaign topic made it relatively straightforward to observe the malware's activity. The fact that WailingCrab uses a public broker means that anyone could subscribe to the campaign topic and monitor the messages being sent to it. In the new version the developers have switched to communicating via client-specific topics only, and unfortunately removing of the malware's activity.

- Ensure anti-virus software and associated files are up to date
- Search for existing signs of the indicated IOCs in your environment
- Consider blocking and or setting up detection for all URL and IP-based IOCs
- Consider blocking or monitoring the use of the MQTT protocol, especially in environments or systems that should not have IoT-related activity
- Keep applications and operating systems running at the current released patch level
- Exercise caution with attachments and links in emails.

IOCs

Click and scroll to view full table

Data Protection | Data Security | IBM X-Force Research | Security Intelligence | security intelligence & analytics | X-Force

INTELLIGENCE & ANALYTICS | December 19, 2023

Web injections are back on the rise: 40+ banks affected by new malware campaign

8 min read - Web injections, a favored technique employed by various banking trojans, have been a persistent threat in the realm of cyberattacks. These malicious injections enable cyber criminals to manipulate data exchanges between users and web browsers, potentially compromising sensitive information. In...

DATA PROTECTION | December 20, 2023

5 common data security pitfalls — and how to avoid them

4 min read - Data protection has come a long way. In previous years, it was considered a “nice to have” and a line item on the budget further down the page. Today, it’s top of mind for almost every CIO or CISO across...

CLOUD SECURITY | December 13, 2023

Best practices for cloud configuration security

5 min read - Cloud computing has become an integral part of IT infrastructure for businesses of all sizes, providing on-demand access to a wide range of services and resources. The evolution of cloud computing has been driven by the need for more efficient,...

MORE FROM THREAT INTELLIGENCE

December 8, 2023

ITG05 operations leverage Israel-Hamas conflict lures to deliver Headlace malware

12 min read - As of December 2023, IBM X-Force has uncovered multiple lure documents that predominately feature the ongoing Israel-Hamas war to facilitate the delivery of the ITG05 exclusive Headlace backdoor. The newly discovered campaign is directed against targets based in at least 13 nations worldwide and leverages authentic documents created by academic, finance and diplomatic...

November 30, 2023

IBM identifies zero-day vulnerability in Zyxel NAS devices

12 min read - While investigating CVE-2023-27992, a vulnerability affecting Zyxel network-attached storage (NAS) devices, the IBM X-Force uncovered two new flaws, which when used together, allow for pre-authenticated remote code execution. Zyxel NAS devices are typically used by consumers as cloud storage devices for homes or small to medium-sized businesses. When used together, the fla...

November 6, 2023

GootBot – Gootloader's new approach to post-exploitation

8 min read - IBM X-Force discovered a new variant of Gootloader — the "GootBot" implant — which facilitates stealthy lateral movement and makes detection and blocking of Gootloader campaigns more difficult within enterprise environments. X-Force observed these campaigns leveraging SEO poisoning, wagering on unsuspecting victims' search activity, which we analyze further in the blog....

October 30, 2023

Hive0051's large scale malicious operations enabled by synchronized multi-channel DNS fluxing

12 min read - For the last year and a half, IBM X-Force has actively monitored the evolution of Hive0051's malware capabilities. This Russian threat actor has accelerated its development efforts to support expanding operations since the onset of the Ukraine conflict. Recent analysis identified three key changes to capabilities: an improved multi-channel approach to DNS fluxing, obfuscated multi-...

Cybersecurity News

By Industry

X-Force

Events

About Us

By Topic

Exclusive Series

Podcast

Contact

Follow us on social