Safeguarding the Self

Reflections Inspired by the Analysis of nls_933w.dll: On Safeguarding Energy in Research

“To understand the immeasurable, the mind must be extraordinarily quiet, still.”
— Jiddu Krishnamurti

By Seeker (李标明) China
Independent Malware Analyst & Researcher
From 2025.8.21 to 2025.8.24

Introduction

Hello everyone,
This article is both a record of my experiences and a reflection on my journey researching nation-state APTs. I will take you through the process as I saw and felt it. Analysts rarely talk about how they balance the intensity of technical work with lighter moments, let alone write an article about it—yet that balance shapes our craft. For that reason, I believe it is worth sharing my perspective.

Related Work

Before the start

In the report “Analysis of Equation Group’s nls_933w.dll: Revealing Core Tactics and Technical Mindset,” I had mentioned that I took weeks to learn about “Persistence Storage” and build the basic mindset. It also took patience and time, but I think preparation is very necessary. In contrast, I believe systematic learning remains important, since it is stable and comprehensive. I didn't have the opportunity to learn such knowledge when I was a student in school, and I had never even heard of it.

In the process of seeking, I am not sure how many times I have had the strong feeling that the true learning is to face the unknown world, and it really needs courage. Which I mentioned before in the e-book called The Path of Clarity.

After that, I tried to look for malware related to the firmware sample to do analysis.

In the process of research

At the beginning, I focused heavily on static analysis to understand what I was dealing with. I discovered that it contained a binary, drive-level malware that could be manually dumped from nls_933w.dll, but I didn’t yet know the name **WIN32M**. At the same time, I had no idea how to make it run normally, so I had to approach debugging almost blindly. Gradually, I started to identify valuable strings, like "**WDC WD**", and delved deeply into the custom XOR algorithm.

Whenever I discovered valuable information, I made sure to record it. Worried that I might forget something, I also created new snapshots to preserve the state for later observation—especially when I anticipated needing to dive deeper into details during subsequent analysis. Over time, I accumulated many snapshots and separate records of different findings. Combining everything into a single record felt overwhelming; it was messy, inconvenient to review, and required significant effort and attention to reorganize.

But I still had no idea how it interacted with the firmware through the key API DeviceIoControl. I manually installed the driver, which used a custom name by myself, and it repeatedly failed to send the I/O control codes (IOCTLs) to the kernel-mode drivers. Progress was painfully slow. I had a strong sense of being lost in the jungle—frustrated, disoriented, and unsure of where to go next.

Without a clear process, I sometimes just looked around and paid more attention to the debug strings, such as \\Device\\Harddisk%d\\Partition0. They seemed to hint at a connection with the firmware. Four days later, I realized I had been going down the wrong path. It was frustrating, but I didn't give up—instead, I tried a different approach and kept learning more.

For nearly two months I made no key progress, and during that time I even quit many social groups. I found it hard to concentrate and was overwhelmed by a sense of loneliness and helplessness. I wasn't sure how long it would take me to finish. Yet, fortunately, I never thought of giving up—instead, I tried every possible way to push through and overcome it.

Sometimes, when I made a bit of progress, I rewarded myself with something small—a nice meal or even a refreshing hair wash. Those were the moments when I felt most relaxed, without having to think about anything. Often, I passed the time by walking along the river, listening to the flowing water, watching the plants sway, and the birds flying above.

After more than two months, I finally confirmed that it had to be loaded manually, and during another round of static analysis, I also noted the name of its hidden functionality. At that point, I had learned how to load it. From there, everything changed—I felt excited, and suddenly one key of the whole picture became clear.

Then I quickly experimented with programming code using AI and created a simple wrapper DLL that exported a named stub.

I kept moving forward and finally succeeded in sending IOCTLs to the kernel-mode drivers. This was especially important when multiple sends were required to observe custom IOCTLs like 0x870021D0 and to successfully execute DeviceIoControl, as I described in the report.

Overall, the entire analysis process was filled with moments of blindness, exploration, confusion, frustration, clarity, and excitement. Both my physical and mental states experienced ups and downs, and I had to learn how to adjust and maintain balance. Progress was far from smooth sailing.

Technical Analysis Report

Once I had a solid understanding of the core tactics and technical mindset of the malware, I began thinking about how to organize the analysis process into a report. I didn’t finish it quickly; instead, I wrote and refined it slowly, focusing on structural organization, verification, image selection and layout, and polishing. Several versions were produced before I felt satisfied. The process took more than a week, and I realized that working on the report was also a way to relieve the pressure of the analysis.

After publishing the report

It took me more than two months to produce a limited report on nls_933w.dll. Even so, I felt physically and mentally exhausted. I had to stop and decided not to proceed to the next sample, even though it would have involved a lighter analysis.

To be honest, I even considered planning a trip, but in the end I gave it up—it would have cost too much. Instead, I chose cheaper ways to relax, like climbing mountains or strolling through the streets. Sometimes I would buy a cup of lemon tea and sit in a quiet spot, other times I listened to slow, ‘Sophie Zelmani-style’ music. I love this style because it is soft, slow-tempo, female-voiced, and folk-inspired, offering a warm, calm, and slightly melancholic experience—even sometimes while I was reversing malware.

When I tried to study file system concepts, I had to progress little by little. My body and mind kept telling me, ‘I’m so tired I can’t go on,’ so I had to pause.

It should have the basic cognition that engaging with nation-state APT groups is, in essence, not merely a technical confrontation but a war of attrition against one's mind, patience, and spirit. The adversaries are well-funded, patient, and highly intelligent opponents who design anti-analysis mechanisms with the sole purpose of inflicting pain and frustration and ultimately forcing you to surrender.

Both physical and mental exhaustion reminded me it did not quickly win anybody; it is long-term adaptation. It’s not a 100-meter sprint—it’s a marathon.

I had to understand the true meaning of slowness, which includes respecting challenges, maintaining the rhythm of scientific research, keeping regular work and rest habits, and balancing exercise and life.

Honestly, one week after publishing the report, I even dreamt about the dynamic analysis of the sample. It showed that the buffer of both physical and mental exhaustion hadn’t fully released. All of this left a deep impression on me.

Figure 1: one day in the mountains.

So I decided to prepare some snacks and water and go hiking in the mountains a little farther away—to breathe fresh air, see different scenery, get close to nature, clear my mind, reconnect with reality, and stay away from the virtual world.

Closing Thoughts

Finally, I want to mention that my recent reverse engineering research, which took me more than two months, involved an in-depth analysis of a sample from the Equation Group dating back over a decade. Although I published a report, it was very limited, and I was physically and mentally exhausted. This experience inspired me to write an article on how to safeguard physical and mental energy during such challenging work.

About me

Malware Analysis Space

All content is provided strictly for educational and defensive purposes.

seeker-lee

PDF format malware analysis report for my malware analysis space and my ebook.

clibm079 GitHub Pages.

Specifically designed to showcase research topics for my Malware Analysis Space.

MalwareBazaar

Follow me

■ Copyright Notice