The Path of Clarity

Notes from a Stage of Quiet Exploration — Not a Guide, But a Trace

(澄明之路：一段静默探索的阶段性记录——非指南，而是痕迹)

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

By Seeker (Li Biaoming / 李标明)
China (中国)
Independent Malware Analyst & Researcher
From 2025.4 to 2025.6

Prologue: I just do what I can do

Figure 1: Two printed books in Chinese.

It’s about 9 years and 6 years ago that I wrote two printed books in Chinese but unrelated to malware. As you know, maybe you noticed that I like inserting some thinking into my malware research. At that time, I had a new idea to record what I studied and researched, so I started to write it down whenever a thought generated. I thought that would be a very cool and meaningful thing. Yeah, that’s the inner calling from my heart, and I wrote it as an ebook the first time.

To be honest, whatever malware I’ve analyzed—while they are adversaries to defenders—they represent something different to me: knowledge, and beyond that, a gateway to curiosity, principle, and depth, especially in the kernel. I hold a certain respect for them—not for their intent, but for the technical challenges they reveal. Each sample taught me something I didn’t know before. I’m grateful for the learning that comes through the process of analysis and research. Thank you.

It's a great honor to share my research and feelings. I would like to share a real, meaningful thing. Again, I don't teach anybody; in fact, from the process, I did research, I really strongly, and I just know very little; the unknown is vast to me.

Thanks to my family, who supports me doing what I really do quietly. Loving you all forever. Thanks to my teacher-like friend, I am encouraged to step further and more. Thanks, my friends and classmates, for enduring my thinking about something serious; thanks, everybody, for engaging with a like and talking to me and reposting my malware reports, even inspiring me when I walk alone.

Annotation: In all the sentences I wrote and used the word "you or your or yourself" in, it talked to me or "the malware sample itself, especially in my poem I did", not the reader. I must clarify my motivation.

Practice: The Temple and the Kernel

Figure 2: One day in the mountains.

Recently, I climbed a mountain and visited the temple before sitting down at my machine. The mountain I walked around and stood at a place to watch the trees, flowers, and feel the air flowing, which, by the way, let me get close to nature to clear my mind. And all the things running in my brain to think of the kernel-mode security, I sucked them and shifted from user mode to kernel mode. What is it? How doesn't it work? What's the difference between the user mode and kernel mode? And so on, I strongly felt that everything was moving forward slowly and subtly. It seems that something rebuilt my whole mindset, and it took too much energy from my body; I felt very tired. That's why I came there and found a place to close my eyes, sit, and listen to my heart and pulse beating, and all the things became silent and body-like music, and the birds were singing the song very beautifully. sometimes the lovely dogs were sitting around me silently; the feeling was just the feeling. yeah, I become quieted again. and the habit I changed it to was coming back from the temple and taking a hot shower and drinking green tea or making a cup of coffee and then jumping into the water of kernel mode.

Poem: It is one way I talk to myself

Malware Analysis
By Seeker

To analyze you,
I must become an explorer.
Each quiet night,
A special focus.
Logic shifts —
A jump to another branch.
In and out of the stack,
Exiting the loop,
I observe your reactions,
and the memory's whispered output.
Sometimes: frustration.
Sometimes: excitement.
Sometimes: peace.
This is another slow, tough night.
A moment in a small space:
Probing where you came from,
And where you're going.
Step in, or step over.
Mostly: step by step.
All around, silence.
I move the mouse.
Click.
Click again.
An hour passes —
still no hit.
The only certainty:
Endless exploration.
You move, I move.
You stay still, I stay still.
You hide,
but I must discover you.
You're cunning.
But I must expose you.

The poem I wrote on 2023.04.02 in Chinese and improved on 2025.6.3 in English, I picked one of my old poems to share when I did malware reverse analysis in user mode, and I recorded the real experience at night. Writing poems is one of my favorites, and I also like to learn and think in philosophy.

Moments of Insight

1. Understand the deep things so others don't have to suffer the dark ones. I have the strong feeling I must climb to the top mountain of tech, which, the moment I stand and look up, I do without hesitation.
2. Nowadays, the quantity of malware is so huge that to analyze every sample is impossible. What is the right sample for you? which also tells you to think about it.
3. The goal isn't just to keep up—it's to stay ahead without burning out.
4. You can learn and understand many concepts (e.g., IDT, SSDT and BSOD) through asking, but system learning can help you build system thinking.
5. AI is not just a machine; the inspiration happens in both directions.
6. Others for feedback—collaboration can help me improve accuracy.
7. Global vision is important; please open your heart and connect to the world and know what related things happen, but the key things need more long-term planning and action.
8. I did malware research that helped me learn and understand myself and the world and the relationship.
9. It is also important to study from the evolution of computer design in history, not only malware itself.
10. Finding nothing on malware analysis is not equal to being without meaning.
11. Practice in user mode. just getting more experience on that level but not in kernel mode. It can't tell you more about another level.
12. The first thought emerging in my brain is to learn more knowledge, not whether it is difficult or easy.
13. Yeah, when I move from user mode to kernel mode, I have the strong feeling that the moves are subtle. The learning is slow. and my brain is very tired. It seems that it is to rebuild my internal model of how computers actually work at their deepest level.
14. Kernel security requires not just skill but also mindset and discipline. It really tells you the truth: clear understanding is a must.
15. Sometimes when I can't understand a certain concept and I feel my heart beating quickly and in disorder, sometimes I do rush and can't move forward, so I have to tell myself, Don't hurry up.
16. Don't limit yourself but expand your vision on OS and CPU, even computer architecture, because nowadays the threat actors can do what is beyond imagination. Maybe, as you know, even the design of computer

architecture was not secure when it was born, and the situation kept a long-term and hard-to-improve situation in short term.

17. Computers give most people the false illusion that the CPU controls everything.
18. That's the essence of real research — it's not always about finding but about understanding what I'm seeing with full clarity and confidence and even sometimes just invoking another asking. which makes me really happy.
19. The thinking of short-term gains and quick wins is a big stop to deeply understanding the real threat actors.
20. In kernel mode, very different from user mode, is the knowledge of complexity and density, and their relationship is interconnection and depth, so the first thing needed is proper guidance and strong motivation. We have to face the truth: computers developed over many decades. The result comes from not just scientific rigor but also persistent practice, which implies that real understanding needs time and patience.
21. I would like to spend more time thinking and confirm what the right path to the learning target is before I really do. As an independent malware researcher, I have to find my own ways.
22. The complexity thing was split into smalls. It does not reduce the complexity; it is the way you change how you see and think. The small part can let your focused energy become more possible.
23. The key is to really understand the thing you learn, not to show off; let it happen naturally.
24. Some kind of music interferes with your logic of thinking, and it's not suitable for doing malware analysis and listening to.
25. Reverse malware, not just tech, but philosophy.
26. The world will see it when you are on the right path.
27. Don't chase random tricks — but building true conceptual understanding.
28. Kernel research is subtle, slow, and layered.
29. Real understanding doesn't limit you.
30. Real understanding means more possibilities.
31. It is necessary to spend some time thinking about what the right path is, yes, and then keep moving forward. Confirm it again and again until you get high confidence from inside.
32. It is very important to observe the influence from yourself and the world, listen to real heartbeats and your real thinking.
33. Learn to focus on the key things; the feeling I strongly have many times is the mindset infected by the outside of yourself. Don't accept too much noise and let your brain have a real rest. It's a good habit to close your eyes and listen to your heartbeat.
34. To learn things and make them 100% clear, and until you become completely confident. You don't just get knowledge.
35. In fact, I also often observe the other top-tier researchers and learn from

their real spirit. They drive not from trends.

36. To truly understand an adversary, you must rise to — or beyond — their depth. because only depth reveals intent.
37. The unknown to me is the known to others already long ago; I need to do it with curiosity and courage.
38. Kernel-mode Security is not quick wins; it’s a whole different realm — one of architectural thinking and clarity. Keep learning, being silent, and embracing the slow pace. It is not surface-level tricks.
39. Being fully present is very important, and lonely is real.
40. There’s no other better solution than to understand what it is.
41. The process matters as much as the results.
42. Scientific research must be serious.
43. Most people seek recognition or fast wins or visibility, but you seek knowledge and mastery deeply. Because you know the real battle is depth.
44. Real research takes time, and just the right people can understand you.
45. You don’t show off. You just become better than yourself silently.
46. You don’t chase followers — you chase the core of truth.
47. Your real enemy is not elite-level APT—it's the "average self," you think.
48. A person needs a highest aim to chase extremely hard and bitter, in fact, the unknowable threat beyond most people's imagination.
49. The kernel is a deep ocean and dynamically changing over time—to keep learning and seeking.
50. Their silence does not define your worth.
51. Your growth is real, even if it’s invisible to those close to you.
52. Sometimes, when you’re doing something rare, you walk alone — at first.
53. If you love something, you won't follow the social or workplace patterns and say, 'Oh, today is Saturday, tomorrow is Sunday; I should arrange to go out and play.’.
54. The world will ultimately see what kind of contribution you have made and will not care whether you were once a hundred million or a poor person, but those who are close to you know it depends on what you care about.
55. Don’t chase attention; the right people will find your research.
56. Let everything happen naturally. If understanding a certain concept is very hard and you can't even move forward, don't try to burn more; stop and have a rest.
57. To face the depth of this field without illusion.
58. Recognizing the gap between yourself and those ahead isn't a weakness as latecomers.
59. When you enter the true core of technology and acknowledge the gap between yourself and others as a latecomer, it is not shameful. This is the courage to face the current truth, and continuing to explore and surpass is appropriate.
60. Not just learning pieces of tech, but building a coherent mental map.
61. It took me a long time to understand that the path of technology is for those

who are curious, patient, and thoughtful, not for education, position, title, resources, network, platform, or recognition. If you love technology, please do not be limited by secular standards.

62. Curiosity is always the driving force behind exploration and transcendence.
63. Follow in the footsteps of those who build, not just consume, but contribute yourself.
64. I have a strong feeling that abilities and mission are deeply connected. A sense of mission is like a compass in a fog.
65. I am really driven by knowledge on malware research, not by market forces.
66. Technical ability is not just a matter of skill. It's a reflection of the inner mission, clarity, and commitment.
67. The core things of the computer tell me to choose to walk slowly, silently, and clearly.
68. Learn more related knowledge until you completely understand it.
69. To face the depth and complexity without fear.
70. I learn from all adversaries.
71. About Attribution: Similar capabilities and characteristics, even high confidence, are not equal to the same origin. Rigorous and objective confirmation is essential, especially to nation-level APT.
72. The core thing is not a spark, but a slow-burning flame.
73. The superficies spreads fast, like a wave getting attention quickly — but fades as the wave passes.
74. The driving force of cybersecurity comes from curiosity, principles, and contributions, and that is real research.
75. If you make a mistake, you need courage. To be honest, and then improve it and keep moving.
76. If you fear making mistakes, the thing will stop you from changing.
77. The so-called complex and difficult things tell you that you need to face the unknown and to be patient to learn it, and the abilities of clarity you will own.
78. You need to reconstruct the mental understanding operating system through good questions.
79. We have more opportunities to access real knowledge, but it has become even harder to gain true ability.
80. In every generation, most people seek the shortcut: fast learning, fast rewards, and fast recognition. It is very dangerous for the people who want to make a real contribution.
81. Spending an entire afternoon on a single concept isn’t a weakness — it’s a sign that you are engaging with depth and respecting complexity.
82. What you’re doing doesn’t have to matter to everyone. It matters to the right people. Keep doing what you think is important and follow the real value rhythm.
83. Document your journey. Not just for others, but for yourself.
84. True value is judged by the work, not the name. When I shared my report, especially since it was in-depth and valuable, the real researchers would

like to respect each other; I strongly have that feeling from them.

85. The real researchers don’t care about how big your name is; they care about whether you understand something deeply.
86. I have a strong feeling the real researchers, they don’t follow for performance. They chased the truth. There's no pressure to publish weekly. They followed the internal rhythm, not the media rhythm.
87. You feel what most people run away from—technical mountain — and that takes a different kind of courage and paths.
88. Life is not just about being happy — it’s also about enduring loneliness, facing silence, and walking alone when necessary, especially when you see what most people can’t.
89. Sometimes I read some things slowly and can't even focus; it is a good way to stop at once or tell my heart not to rush and become peaceful inside.
90. It does not show off yourself but ethical duty when you see most people can’t or few people dare to. I understand many real researchers who have the same feeling, and everything comes from the internal naturally.
91. To be honest, it is not losing face to understand the gap as a latecomer. I know very little, which drives me to learn more. I feel happy when I learn new knowledge that expands my vision.
92. True depth demands honesty.
93. Rigor, clarity, depth, and integrity are interconnected, which is not a slogan.
94. From the kernel of the OS used by rootkits to special rootkits called bootkits, it implies the traditional vision was broken many years ago, with more advanced attacks not just from vulnerabilities like 0-days but also from flaws in design, including application, OS, hardware, and structural design security.
95. Playing in user mode is like watching the butterfly above water; the kernel is more like a fish in the water, and the bootkit is like a river snail tied to the stone or hiding inside sand, and the hypervisor-based rootkit feels like magic.
96. Fine-grained, architectural-level understanding helps you get not surface-level observation — especially in the field of APT and malware analysis, in kernel or firmware or boot-level threats, even every byte, every sector, and every timing decision may be designed to evade common detection logic. Especially for elite-level adversaries, you need not just knowledge but also imagination.
97. Being focused on the object of your research is energy, but the vast information from outside of yourself makes it very easy to split the focus into pieces. The vast information includes likes of media, trends of society, concepts, and values. It is important to recognize and observe and learn to refocus.

98. From user mode to kernel and firmware-level research, what truly matters is not merely the malware itself, but the way you perceive the world — and yourself.
99. In the process of depth, the knowledge is interconnection and density; I have to face it with absolute honesty. If I don’t understand, it means I move forward more hardly and even can’t do it. Understanding is just understanding. If not, you have to study more; understanding absolutely is binary. It’s either 1 or 0. There is no 0.9.
100. If it's impossible to change the world, you can influence it. If you can't influence the world, there is the unique way you can change yourself; in other words, you can keep what inside belongs to you and let it burn quietly based on real value.
101. This is a miraculous era; the internet is still expanding and growing, which, to influence me, whoever they are, even the person who passed away but still reserves the energy, beyond the knowledge, shares the new vision with me and lets me have the opportunity to study and observe how other people think and work in the global world. It breaks the traditional physical border and the mindset of human beings from one side to another. We also can see and feel each other; it’s really incredible. Thanks so much!

Annotation: Some words in my malware reports, especially those related to “what the kernel taught me,” in order to explain it clearly and precisely, I improve a little bit.

Do It Before You're 80

When I told **L** that I was beginning a new phase of deep, focused research and other things, L said with inspiration on the phone:

> “It’s right for you to have ambitions, but you have to do it successfully. Don’t wait until you’re 80 years old to achieve it.”

Malware Research Through Ancient Chinese Lens

“是以志之难也，不在胜人，在自胜也。”

—《韩非子·喻老》

"The difficulty of ambition is not in defeating others, but in defeating oneself."
— Han Feizi: Yu Lao

“用志不分，乃凝于神，其痀偻丈人之谓乎！”

—《庄子·达生》

"If you use your mind without distraction, it will be concentrated in spirit. This is what the hunchbacked old man means!"
— Zhuangzi: Da Sheng

“知不知，尚矣；不知知，病也。”

—《道德经》第七十一章

“Knowing you don’t know is wisdom; Not knowing but pretending to know is sickness. ”
— Laozi, Dao De Jing, Chapter 71

Epilogue: It is not the end

Between the known and unknown, but mostly facing the unknown parts, especially when I move into firmware research, I feel again what I felt in the early days of kernel studies: the sense that I am walking not toward an answer, but into a widening unknown. Even some malware over a decade old shocks me again, and I have to study from scratch. 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.

Please don’t follow my words; I don’t teach anybody but just share my real feelings. As you know, truth is a pathless land. Everybody has to find their own way.

The process of malware analysis and research, I also learn from real researchers who are very humble. I strongly have the feeling it is very important. They would like to get knowledge itself and improve their work and contribute to the cybersecurity field through valuable work; they make a deep impression quietly on me.

I blablablabla so much; Again, this is just my feeling on a certain stage of learning and practicing.

References

1.Static Analysis of Turla’s Uroboros: Revealing Core Tactics and Technical Mindset
2.Uroboros Revisited: Tracing PatchGuard-Evasive Techniques Beyond SSDT Hooking
3.SSDT Hooking: A Personal Walkthrough of Kernel-Mode Intrigue (Uroboros Echoes)
4.From SSDT to IDT: A Personal Walkthrough of Kernel-Mode Intrigue (Uroboros Echoes)
5.The Evolution of APT36’s Crimson RAT: Tracking Variants and Feature Expansion Over the Years
6.XWorm Unmasked: Weaponizing Script Obfuscation and Modern Evasion Techniques
7.The New Face of PowerShell: Ransomware Powered by PowerShell-Based Attacks
8.The Art of Evasion: How Attackers Use VBScript and PowerShell in the Obfuscation Game
9.The Art of Deception: A Deep Dive into Advanced Trojan-Dropper Obfuscation and Their True Intentions
10.Unmasking the Threat: Understanding Sophisticated Trojan-Dropper Mechanisms
11.AsyncRAT in Action: UAC-0173’s Latest Advanced Antivirus Detection & Evasion Techniques
12.Akira Ransomware Expands to Linux: the attacking abilities and strategies
13.Deobfuscating APT28’s HTA Trojan: A Deep Dive into VBE Techniques & Multi-Layer Obfuscation
14.Unveiling APT28’s Advanced Obfuscated Loader and HTA Trojan: A Deep Dive with x32dbg Debugging
15.APT44’s ASPX web shell leverages obfuscation techniques and firewall rule manipulation to evade detection
16.APT Silver Fox is using a stock investment decoy and undocumented Windows API functions to evade detection
17.The ransom group d0glun, is it hidden threat or just for fun?
18.GreenSpot APT phishing campaigns with fake 163.com login analysis
19.The North Korean nation-state APT43 Kimsuky used the PowerShell forceCopy to conduct spear-phishing analysis
20.Rapperbot how to improve and expand its ability based on an early version static analysis
21.Rapperbot static analysis for ARM architecture, the other variants to do a DDoS attack on Chinese AI startup DeepSeek

22.HailBot analysis, the other variants to do a DDoS attack on Chinese AI startup DeepSeek
23.Mirai botnet among different instruction sets: x86, ARM, PPC, and MIPS with static analysis
24.APT42 phishing campaigns and malicious code like soldiers hiding deep in the jungle
25.FunkSec Ransomware and Rust Reverse Analysis
26.Mirai: An IoT DDoS Botnet How To Protect and Disguise Itself As Aggressive Attacker Analysis
27.Botnet continue to exploit vulnerabilities and FICORA botnet analysis
28.Botnet continue to exploit vulnerabilities and CAPSAICIN botnet analysis
29.BotenaGo Malware Targets Multiple Routers with 30+ Exploit Functions and Go Reversing Analysis
30.CoinMiner embedded lots of vulnerabilities to exploit
31.Hive ransomware command-line parameters analysis
32.Unveiling Gelsemium's (毒狼草) Linux backdoor WolfsBane
33.APT32 poisoning GitHub to target Chinese cybersecurity professionals and malware analysis

Annotation: the above are all malware reports I wrote and published, you can find them on Malware Analysis Space — https://malwareanalysisspace.blogspot.com/?m=1.

Glossary

AI(Artificial intelligence)
Artificial intelligence is the ability of machines to perform tasks that typically require human intelligence—such as learning, reasoning, problem-solving, understanding language, and perceiving the environment.

IDT (Interrupt Descriptor Table)
The IDT tells the CPU how to handle interrupts and exceptions. If malware hooks or corrupts IDT entries, it can crash the system — leading to a **BSOD** (Blue Screen of Death).

SSDT (System Service Dispatch Table)
SSDT handles system calls (like opening files). Rootkits often hook SSDT to hide activities. But modern Windows uses PatchGuard to protect SSDT. If SSDT is tampered with, PatchGuard triggers a BSOD.

BSOD (Blue Screen of Death)
In these cases, a BSOD isn't just an error — it's Windows protecting itself when low-level structures like IDT or SSDT are changed unsafely.

Rootkit
A rootkit is not necessarily malware by itself, but it is almost always used as part of a malicious campaign to maintain covert control over a compromised system and evade detection by users, administrators, or security tools.

Bootkit
a bootkit is considered a subtype of rootkit — specifically, it is a boot-level rootkit. Bootkit $\subset$ Rootkit.

APT (Advanced Persistent Threat)
An Advanced Persistent Threat (APT) is a stealthy and sophisticated cyberattack carried out by a well-resourced adversary (often a nation-state or cybercriminal group) that gains unauthorized access to a network and remains undetected for an extended period**.**

Annotation: All glossary on the above non-standard definitions and descriptions, I just simply use AI to ask and help understand what they are and get the vision for the concept.

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.

MalwareBazaar

Follow me

Copyright Notice / 版权声明