

Hacker's Pursuit: Stealth

By: Henrik Davidsson

Disclaimer

This is a work of fiction. Names, characters, businesses, events, and incidents are either the product of the author's imagination or used in a fictitious manner. Any resemblance to actual persons, living

or dead, or to actual events is purely coincidental — though if you think you recognize yourself, consider it either a remarkable coincidence or a flattering tribute. Either way, please take it up with your imagination, not the author.

Prologue

February 2022

On the morning of February 22, 2022, the Russian army invaded Ukraine under the pretense of a “special military operation,” with the stated intention to demilitarize and denazify the country. Missiles and airstrikes rained down across Ukraine, followed by a large-scale ground invasion along multiple fronts.

This was not just a military maneuver — it was part of a broader vision: a revival of Russian dominance, echoing the legacy of Peter the Great and the resurrection of the Soviet Union under the ideological shadows of Lenin and Stalin. In a single morning, the illusion of lasting peace in Europe shattered. The post–World War II promise of stability evaporated.

The continent was no longer on the brink. It had crossed over.

NATO held emergency consultations. Civil defense alerts were tested across Poland, the Baltics, and Finland. International markets spiraled. Cybersecurity threat maps lit up in real time, a staccato of red zones pulsing across Europe’s energy, telecom, and transportation grids.

In quiet corridors of power, the conversations were no longer about “if,” but about “how bad.” And who would move first.

In tech hubs across Europe, internal war rooms spun up. Global information security teams mobilized quietly—no headlines, no press releases. Only containment. Not panic. Not yet.

Signals began to pulse across closed networks. Some pointed outward. Others—more troubling—pointed inward.

And in Stockholm, buried deep inside Svenska Kraftnät’s digital architecture, a worm stirred.

Its original creator had thought she buried it.

But something—or someone—had brought it back to life.

Meanwhile in Stockholm, Sweden

Meanwhile, in a quiet corner of Stockholm's Old Town, far from tanks and air raid sirens, a different kind of war was unfolding. The café was a warm cocoon against the cold February drizzle. Dimly lit with amber-toned lamps and soft wood interiors, it offered a kind of urban sanctuary to locals and passersby. The air was fragrant with fresh cardamom buns and chai, and mellow chill music with Röyksopp playing through the speakers, adding a dreamlike backdrop to the subdued hum of conversation and clinking porcelain.

Alex sat at a window table, half-wrapped in her oversized coat, fingers curled around a ceramic cup. She looked like an ordinary Swedish young woman — dark blond hair tied loosely, clear blue eyes gazing out through rain-flecked glass. Yet beneath her stillness, a storm brewed.

She was a skilled hacker, fluent in the language of networks and encryption, shaped by years in the shadows of the dark web. She had exploited vulnerabilities, extracted secrets, and orchestrated attacks — sometimes for money, sometimes for the thrill. She wasn't yet infamous, not a legend in the hacking world. But her time was coming.

The last few weeks had been intense. Alex had found backdoors into Svenska Kraftnät, Sweden's transmission network — the national energy backbone — and into key control systems at the nuclear plants of Forsmark, Oskarshamn, and Ringhals. Together, those six reactors produced roughly a third of the country's electricity. Hydroelectric power accounted for another 35 to 45 percent, with wind, solar and cogeneration plants covering the rest. It was all intricately connected through the transmission grid — and now, it was all within her reach.

The code she had built was her most sophisticated yet — modular, stealthy, and devastating. A worm to deliver the payload. A link file to replicate and trigger execution silently. And a rootkit to mask it all beneath layers of misdirection and invisibility.

It was masterwork.

She took another sip of chai, letting the sweetness mingle with the soft beat of Röyksopp's Eple.

The music made her feel light, maybe even a little proud.

Then her burner phone buzzed.

It was a message from the Mentor — the enigmatic guide who had trained her, empowered her, and made her believe in her potential. “Have you shared this with anyone else? This is very big, Alex. I’m proud of you. I think it’s time for us to meet in person.

Her stomach tightened. The Mentor. She had imagined this moment a thousand times — wondering what they looked like, what their voice sounded like. Man or woman? Young or old? Every conversation had been over encrypted chats, every trace deleted. A ghost teaching a ghost. And now, suddenly, a real meeting.

A strange excitement passed through her — followed by something darker. She should’ve already received a crypto payout. There was none, and she didn’t like that.

She stared out the window, the chill music still playing. People passed by under umbrellas. Steam curled up from her cup. A beautiful, fragile moment.

Then the music stopped.

A news alert took over the café speakers. Confused murmurs rose around her. Screens lit up. Patrons leaned toward their phones. Russia had invaded Ukraine. The energy in the room shifted instantly — warmth replaced by a cold current of fear and disbelief.

Alex felt it pierce her like a wire through the spine. This wasn’t a drill. It wasn’t cyber-theater. This was real war. She sat frozen, thoughts racing. On the other side of the Baltic Sea, missiles were falling — and here she was, sipping tea, with code on her laptop capable of plunging a nation into darkness.

Her worm wasn’t just dangerous now. It was strategic. Weaponizable.

She had planned for money. Control. Respect.

Now her creation might become something much worse.

Her phone buzzed again.

“Meet me. There’s someone you need to know. Skeppsholmen. 6 PM. Come alone.”

She didn’t respond right away. The café’s warmth now felt stifling. The rain outside no longer romantic, but menacing.

She looked back at the screen. Should she go? Could she trust them? The worm, the plan, the ethics of it all — everything had changed in a heartbeat. And yet something in her gut whispered: Go. Find the truth.

First, she had to meet the Master.

Chapter 1: Unseen shadows

Somewhere in Sweden, April 2018

The air in the dimly lit room feels charged with anticipation as Alex sits before her computer, her fingers dancing across the keyboard with a practiced finesse. The soft glow of the monitor illuminates her face as she dives deeper into the intricate web of the organization's network that she has infiltrated.

With a successful phishing email as her entry point, she now finds herself landing on a random endpoint within the organization. The recipient's click on a malicious link provided just enough information for Alex to gain a foothold. The thrill of the hunt courses through her veins as she contemplates her next move.

Her first objective is clear: she must navigate the organization's network undetected and gather as much information as possible. Like a phantom in the digital realm, she carefully scrapes the endpoint for cached data. Credentials temporarily stored in memory, saved in browsers and connected file shares become valuable treasures in her hands. She traces the path of browsing history, searching for any entry points or vulnerabilities that can grant her access to higher privileges.

Stealth is paramount to her success. Alex knows that leaving behind any trace or triggering the antivirus software would jeopardize her mission. She maneuvers through the network, leaving no footprints and ensuring her actions remain hidden from prying eyes.

Her next objective is to establish multiple backdoors within the organization's network, allowing her to move laterally and explore deeper into its infrastructure. She understands that attacking network and hybrid cloud infrastructures can be highly effective in maintaining persistence and evading detection. Organizations rarely keep up the same security levels across their entire infrastructure and forget where they have their crown jewels.

As the pieces of the puzzle fall into place, Alex's true objectives come into focus. Privileged access to the organization's infrastructure, both on-premises and in the cloud, becomes her gateway to greater opportunities.

The stakes escalate as Alex aims to expand her control across the organization. Spreading malware, gaining elevated access, and seizing control of compromised accounts are the stepping stones to executing her ultimate objective. She relishes the thought of stealing valuable data, intellectual property, or even disrupting the organization's business continuity with extortion or ransomware attacks.

As she orchestrates her cyber symphony, Alex acknowledges the dangers that lie in the final step. She understands that erasing her presence is essential. Backups, logs, and any trace of her malicious activities must vanish. Ransomware often has been her weapon of choice, diverting attention and encrypting evidence to further obscure her tracks. And if the opportunity presents itself, she might even mine some Bitcoin, leaving a digital trail of her own.

But as Alex reads through the headlines, a subtle smile playing on her lips, she knows that the aftermath of such attacks often leaves more questions than answers. The victims are left grappling with the realization of their vulnerability, wondering how the breach occurred and what the motivations behind the attack were.

In the depths of her digital realm, Alex embodies the paradox of a hacker's drive. It's not merely the pursuit of power or financial gain that propels her forward; it's the allure of ruling her own kingdom, bending the rules of the digital world to her will. With each successful infiltration, she reigns as the unseen queen, driven by a thirst for control and an insatiable curiosity for what lies beyond the next breach.

The cursor blinks on her screen, a silent metronome to her thoughts. She doesn't rush — haste leads to mistakes. Instead, she lets the rhythm of the hunt guide her fingers. Commands are typed, scripts executed, logs dumped, erased and rewritten.

She uncovers a forgotten admin console. Unpatched, lightly guarded. Her pulse quickens.

Credentials harvested earlier unlock doors deeper inside the network. She slips through firewall rules like a ghost walking through walls. The organization's security posture, though bolstered by a recent audit, is riddled with blind spots. Shadow IT, legacy systems, poorly segmented networks — all liabilities now ripe for exploitation.

Another scan, this time horizontal. She maps the topology: user subnets, finance VLAN, cloud integration points. Then she finds it — the API bridge to the power load forecast dashboard. Not just metadata. Live access.

She leans back for a moment, eyes flickering with a mix of amusement and ambition. They have no idea she's here. No failed logins. No alerts triggered. No blinking lights in a SOC anywhere.

To them, everything still looks normal.

She returns her attention to the code she's injected — not a payload yet, but the infrastructure to carry it. Her worm isn't just a blunt weapon. It's elegant. Adaptive. A digital scalpel, not a hammer.

She packages the link file to auto-propagate on shared drives. Camouflaged behind innocent PDFs and Office files. Employees will do the spreading for her. The rootkit binds it all together, hiding her traces like wind covering footsteps in snow.

Everything is in place.

She could walk away now. Cash in. Wipe the slate.

But that's not what drives her.

Not anymore.

She wants more than access. More than ransom.

She wants the keys to the kingdom.

Not to break it — not yet — but to hold it quietly, without anyone realizing.

From this vantage point, she sees the future. A whisper in the dark that can silence power grids, sway decisions, maybe even reshape nations.

And no one — not even her Mentor — knows just how far she's already gone.

Now she has found a gold mine.

