THE PROXY THAT MADE NO SENSE

AUTHOR: Mikko Hypponen (@mikko)

I started working malware and viruses in 1991. Everybody remembers the big ones. Melissa. Loveletter. Stuxnet. Wannacry. NotPetya. Nobody remembers Fizzer malware from 2003. That is fine. Fizzer was never about the fireworks. Fizzer was the one that quietly changed what all of this was for, and almost nobody noticed at the time, including me.

This is the story of how I noticed. And how it took me longer than I would like to admit.

1. HOW IT FELT BEFORE

To understand why Fizzer mattered, you have to remember what cybersecurity work felt like in early 2000s, and what the people on the other side were like.

Back then we knew our adversaries. Not personally (well, sometimes personally) but we knew what they were like. They were kids, mostly teenage boys. They were bored show-offs. They wrote viruses for the same reason people climbed mountains and built demos and cracked games: because it was hard, and because they wanted to see just how far their creation might travel. And quite often they travelled around the world.

The point of viruses back then was the craft and the fame. Money never entered into it. The idea that you would write a virus to get paid was, honestly, a little vulgar.

And I should tell you what the work itself felt like then, because that is the part that does not survive in the archives. The early 2000s were the virus wars. Loveletter, Blaster, Slammer, Sasser, Sobig: the big email and network worms came in waves, day after day, and we fought them in a permanent state of emergency. We had an actual alarm in the F-Secure virus lab in Helsinki: a bell and a flashing light. We had outbreak levels, and the worst was Radar Alert Level 1. When we hit Level 1, every meeting was cancelled and the lab staff was barred from leaving the building, not even for lunch. The shift manager just ordered in pizza off a list where you had marked your favourite pizza in advance, so that even at the worst moment of the worst day you got your salami without having to think about it. The phone would ring in the middle of the night, the alarm would go, and we would scramble to grab the new sample, tear it apart, build detection and ship it as quickly as possible. We would work in Finland in the middle of the night to fight an outbreak underway in the United States. Four wake-up calls in a week was not unusual, and it went on for months, until everyone working in the lab was just living in a fog. Looking back, it was heroic and stupid. It was also the most alive I have ever felt at a keyboard.

I had been pulling apart malicious code since the early nineties, since the days you analysed a boot sector virus off a 5.25-inch floppy because somebody sent it you in the mail, to be analysed. We did it because it was the most interesting puzzle in the world that happened to also pay a salary. Cops and robbers, sure, but we respected the robbers, the way a locksmith respects a good lockpicker. It was a small world and a strangely innocent one.

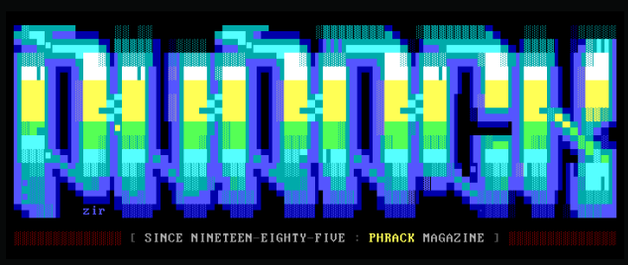
2. ENTER FIZZER

Fizzer turned up in May 2003. At first glance it was nothing special: another mass mailer, spreading through email and P2P networks. Standard stuff: we had seen the pattern before. We captured a sample via a honeypot, named it and added detection.

But when we're taking it apart in the lab in Helsinki, Fizzer was a bit strange. It contained a keylogger. It had an IRC backdoor so somebody could command it remotely. It tried to phone home to a Geocities page to pull down updates of itself, which meant somebody intended to keep maintaining it. And it dropped an HTTP and SMTP proxy onto every single machine it infected.

That proxy is the thing I kept staring at.

A proxy. On a home user's Windows XP box in some living room in Germany or Brazil or Japan. Why? It did not do anything by itself. It just sat there, quietly, turning a random infected PC into a relay that anyone who knew it was there could route traffic through.



I remember sitting in the lab, next to the humming servers, staring at the code, and it did not click. Every other capability in Fizzer I could explain. The proxy made no sense to me. What is the point of an army of open proxies running on grandma's computer? The best theory I had was that somebody wanted to have large number of machines they could SSH through in order to hide their tracks.

3. SO, WE LET IT LOOSE

We did what we often did with a specimen we did not understand. We took a clean Windows XP test machine and infected it with Fizzer on purpose, then connected it to a throttled internet connection, and we waited to see what it would do when it thought nobody was looking.

Nothing happened.

A day went by. Nothing. A week. Nothing. The machine sat there, infected, patient, idle. I started to wonder if the proxy was just dead weight, half-finished code from an author who never wired it up.

And then, after three weeks, the machine burst into life. It had received it's orders and now it was generating traffic. A lot of it, megabytes of it, far more than I had expected. All of it outbound, over TCP port 25. So, SMTP. Mail. I looked at Wireshark view of the traffic to see what our infected PC was suddenly so busy sending out.

It was spam.

Specifically, it was Viagra spam. Thousands of messages relayed via an infected computer, so the real senders - the spamlords - would stay invisible.

That was the moment it dawned on me. The virus writers were not working alone anymore. The proxy was not for them. It was a product. Somebody had written this worm to build a network of relays, and then rented it out, or sold the access, to spammers who wanted to send their junk email without getting their own servers blocked. The proxy could relay anything, but they only wanted to relay email.

And the blacklisting was the reason any of this was worth doing. Spam was already a big headache in 2003 but fighting it had been fairly easy: the spammers ran their campaigns from dedicated servers, so you identified the server, blacklisted it, and the flood stopped. Their countermove was simple: stop using your own servers. Send the spam from ordinary people's home machines instead, thousands of them, each pushing a trickle. You cannot blacklist everybody's home computer, because that is where the real mail comes from too (remember, Gmail was not invented yet). An infected Windows XP box was the perfect laundering point for a spam run, and Fizzer was a factory for producing them by the tens of thousands.

The virus writers were now cooperating with the spammers. And they were doing it for one reason, the oldest reason there is.

Money.

4. MONEY CHANGES EVERYTHING

The instant there was money to be made by malware, the profile of our adversary changed. Up to that afternoon, the worst case was a clever kid who created malware outbreaks because they wanted to be famous. A kid will brag. A kid will sign his work. A kid will eventually get caught because the urge to be recognised is the entire motive, and you cannot be anonymous and famous at the same time. They were caught because they could not shut up.

If you write malware for the fun of it, you want the loudest, fastest thing on earth, and the hobbyists openly competed to see whose worm would circle the globe first and grab the biggest headlines. But the moment you are writing malware for a living, that logic inverts completely. If your malware makes the headlines, you have already failed.

A criminal who wants money never wants to be seen. He has no interest in your respect or your attention. He wants to operate for years in total silence and get paid. There are no hidden shout-outs or greetings.

Fizzer was the hinge. It was not the biggest, it was not the most sophisticated, and if you search for it today you will find a dry technical writeup and not much else. But it was the first piece of malware I analysed where the actual designed purpose was to generate revenue. There had been one freak exception years before, the AIDS Information Trojan of 1989, which mailed to victims on floppy disks and demanded payment to a post office box in Panama, but that was a dead-end curiosity from another age. In 2003, Fizzer was the one that opened the

gates. After Fizzer came the flood: the banking trojans, the credit card keyloggers, the bot herders renting out their networks by the hour, and eventually, years down the road, ransomware.

All organised online crime traces back through that lineage to the simple, ugly idea that you could make malware pay. I happened to be sitting in front of a packet capture in Helsinki when that idea was first executed.

5. WHAT WE LOST

I am not nostalgic for viruses. People lost data, lost work, lost sleep, and the hobbyist era did real harm even when nobody meant it to. I do not want it back.

But I will admit there was something we lost that afternoon that I did not have a word for until much later. We lost a kind of innocence. The game I had grown up inside, the locksmith and the lockpicker who secretly admired each other, was over. The other side stopped being people I could understand and relate to. The work got more serious and more grim at the same time.

The small flip in the stomach when I saw port 25. The slow, sinking understanding that the world had just changed and it was not going to change back.

Money had arrived. And once money arrives, it never leaves.

- Mikko