Time Bombs: Malware with Delayed Execution

By ANY.RUN

Published: 2020-09-17 · Archived: 2026-04-05 23:51:14 UTC

Did you know that there's malware that behaves just like cliched ticker-bombs from Hollywood blockbusters? It enters the system and waits there, sometimes for ages, with the timer slowly but inevitably counting towards the destructive explosion. Or in our case — execution. Once the time comes, a cyber-bomb like this can be devastating.

Time bombs are notoriously difficult to detect. They may not leave any signs of malicious activity for a while. There is even a chance that your network is infected with a time bomb right now.

That's why it's worth learning about the dangers this type of malware brings and how to deal with them.

What are Time Bombs?

Time bombs are a subcategory of logic bombs — programs with delayed execution that are designed to run when they detect that certain conditions are being met. For example, it could be reaching a specific date or detecting certain user behavior on the target machine. Although software like this doesn't have to be malicious, sometimes it's used by threat actors to create devious malware.

Logic bombs can enter a network and sit there undetected for prolonged periods of time, until a set date of execution. Sometimes it could months, or even years.

When the time comes, they act just like any other malware, potentially inflicting great damages to your network or your machine.

Where Time Bombs can be Used?

There are a lot of scenarios where attackers can use time-bombs instead of typical instantly executing malware.

- Any malware can be designed to work as a time bomb. It could be a Trojan, Ransomware, Spyware, a worm, or anything really.
- Time-bomb malware can be implanted by employees. If the malware executes long after the attacker left the company it would be much harder to connect the responsible person to the crime.
- Very often time-bombs are designed to execute on a notable holiday, like Christmas or New-Years-Eve. The idea is that at busy times like these are mind is not focused on work or security and the chance of a successful attack becomes much higher.

Famous Time Bomb Examples

Time bombs are not particularly uncommon, but there are a few that made an especially big splash. Let's look at them in detail.

Jerusalem malware

The first malware pandemic (an outbreak of computer viruses that affected multiple countries) was triggered by nothing other than a time bomb. This MS-DOS malware is the reason many cybersecurity professionals still fear Friday the thirteenth.

As you probably already guessed, Jerusalem, also known as "Friday the 13th" was designed to execute on the spooky date of any year except for 1987. Since Friday 13s aren't very common, most of the time the malware could spread completely stealthily.

The malware was notoriously known for deleting any file that the victim interacted with if the calendar showed Friday the 13th. Apart from that, on any regular date, Jerusalem slowed down affected PC-XT machines by up to five times.

Win95.CIH or Chernobyl malware

Released in 1998, Chernobyl was arguably the most destructive malware of its time. It was one of the first computer viruses that not only damaged software but also affected the hardware of infected machines.

This malware was set to execute on the 26th of April — the date of the infamous 26 Chernobyl disaster. Win95.CIH was able to wipe out all information on system hard drives as well as damage BIOS on certain motherboards. Chernobyl was the malware that revealed the BIOS overwriting vulnerability, showing that malware could be destructive to hardware just as well as to software.

How to Prevent Time Bomb Attacks?

A malware that does not immediately produce any indicators of malicious activity can be tricky to detect. However, you can follow some basic best practices to greatly increase the chances of noticing the danger in time.

1. Having a robust antivirus on all machines in the network is a must. This one goes without saying, but make sure it is regularly updated.
2. Don't skip on OS updates. Many of them contain vulnerability fixes and generally improve system security. However, before updating make sure to test that the new version doesn't bring its own security shortcomings and bugs, that can potentially open a door to malware.
3. We never get tired of saying this one — check all suspicious emails and make sure to be extra careful with attachments and links. You can safely analyze emails by uploading them into ANY.RUN. It barely takes a few minutes and ensures your safety.
4. Educate your colleagues about the dangers of malware and the most common attack vectors. The more people know about mechanisms that get users infected and the dangers of modern malware, the safer we will all be. It's just like with physical virus pandemics — the positive outcome is dependant on the majority following recommendations of healthcare professionals.

Source: https://any.run/cybersecurity-blog/time-bombs-malware-with-delayed-execution/