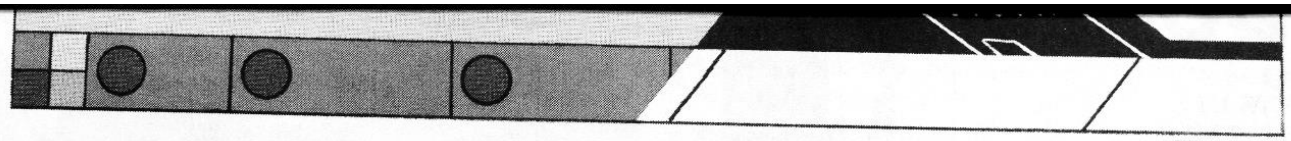

ELENI KALORKOTI

# Why the World Is Getting Hacked

**Zeynep Tufekci**

THE path to a global outbreak on Friday of a ransom-demanding computer software ("ransomware") started, as it often does, with a defect in software, a bug. This is perhaps the beginning of a global crisis that has been brewing for decades. Fixing this is possible, but it will be expensive and require a complete overhaul of how technology companies, governments and institutions operate and handle software.

Just this March, Microsoft released a patch to fix vulnerabilities in its operating systems, which run on about 80 percent of desktop computers globally. Shortly after that, a group called Shadow Brokers released hacking tools that took advantage of vulnerabilities that had already been fixed in these patches.

It seemed that Shadow Brokers had acquired tools the National Security Agency had used to break into computers. Realizing these tools were stolen, the N.S.A. had warned affected companies like Microsoft and Cisco so that they could fix the vulnerabilities. Users were protected if they had applied the patches that were released, but with a catch: If an institution still used an older Microsoft operating system, it did not receive this patch unless it paid for an expensive "custom" support agreement.

On May 12, an enormous ransomware attack targeting one of those vulnerabilities hit hospitals in Britain, telecommunication companies in Spain, FedEx in the United States, the Russian Interior Ministry and many other institutions around the world. They had either not applied these patches to systems where it was available free or had not paid the money for older ones.

Computer after computer froze, their files inaccessible, with an ominous on-screen message asking for about $300 worth of bitcoin — a cryptocurrency that allows for hard-to-trace transfers of money. The consequences are still being felt worldwide; the attack continued to affect more computer systems yesterday, as schools, companies and hospitals began their workweeks.

That the damage of this attack was contained is a stroke of luck: The ransomware had a "kill switch" that a British employee in a cybersecurity company managed to activate. Shortly after, Microsoft finally released the patch, at no charge, that it had been withholding from users who had not signed up for expensive custom support agreements.

But the crisis is far from over. This particular vulnerability still lives in unpatched systems, and the next one may not have a convenient kill switch.

While it is inevitable that software will have bugs, there are ways to make operating systems more secure — but that costs real money. While this particular bug affected both new and old versions of Microsoft's operating systems, the older ones like XP have more critical vulnerabilities. After the crisis, the president of Microsoft issued a statement criticizing the N.S.A. for the "stockpiling of vulnerabilities." However, Microsoft's operating systems, especially Windows XP, are insecure enough that their frailties would probably have been discovered and weaponized by someone if not the N.S.A.

This isn't all Microsoft's fault, though. Its newer operating systems, like Windows 10, are much more secure. During this latest crisis, it became clear there were many institutions that could have patched or upgraded their systems but did not. This isn't necessarily because their information technology departments are incompetent (though there are surely cases of that, too). Upgrades come with many downsides, including new expenses and unwanted features, that make people reluctant to install them. But users are often unaware that these unwanted features come bundled with a crucial security update.

**Our software systems are like unstable cities built on swamps.**

The problem is even worse for institutions like hospitals that run a lot of software provided by a variety of vendors, often embedded in expensive medical equipment, for which updates can render the equipment inoperable. For them, upgrading the operating system may also mean purchasing millions of dollars' worth of new software. Much of this software also comes with problems. How do you test new software when the upgrade might freeze your M.R.I.?

The situation is bleak: Our software evolves by layering new systems on old, and that means we have constructed entire cities upon crumbling swamps.

All the key actors have to work together, and fast. First, companies like Microsoft should discard the idea that they can abandon people who use older software. At a minimum, Microsoft clearly should have provided the critical update in March to all its users, not just those paying extra. Indeed, "pay extra money to us or we will withhold critical security updates" can be seen as its own form of ransomware.

Microsoft should help institutions and users upgrade to newer software, especially those who run essential services on it. This has to be through a system that does not force choosing between privacy and security. Security updates should update only security, and everything else should be optional and unbundled.

The United States government also has resources and institutions to help fix this. It should focus more on protecting its citizens and companies from malware, hacking and ransomware, and less on spying. This means disclosing vulnerabilities in software but also helping develop standards for higher security — something the N.S.A., an agency devoted to finding weaknesses, is very well suited to do — as well as identifying systemic cybersecurity risks and then helping fix them.

Part of the problem is that the technology industry moves fast and considers something just 10 years old to be ancient. But the infrastructure that controls software doesn't have such a short life span. The software that controls it needs to be reliable and secure for the life span of the systems it supports. You can't use an "upgrade your smartphone" model when it comes to trains or M.R.I. machines.

We need to consider whether the current regulatory setup, which allows all software vendors to externalize the costs of all defects and problems to their customers with zero liability, needs re-examination. In addition, the software industry, the institutions that depend on its products and the government agencies entrusted with keeping its citizens secure and its infrastructure functioning need to step up and act decisively. □

**ZEYNEP TUFEKCI**, *an associate professor at the School of Information and Library Science at the University of North Carolina, is the author of "Twitter and Tear Gas: The Power and Fragility of Networked Protest" and a contributing opinion writer.*