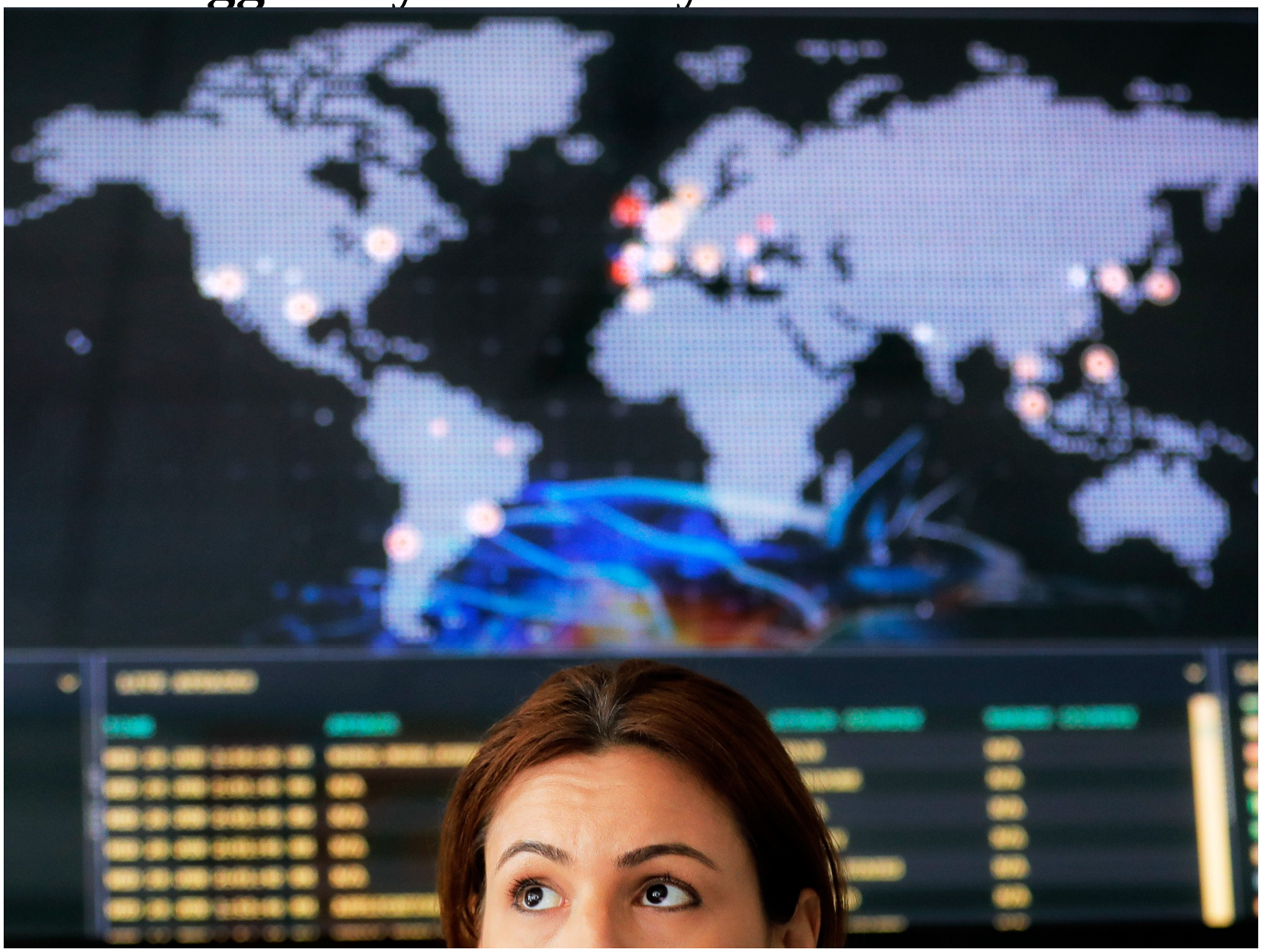
The Biggest Cybersecurity Disasters of 2017



A woman sits backdropped by a real time cyber attacks world map at the headquarters of Bitdefender in Bucharest, Romania.

Shadow Brokers

The mysterious hacking group known as the Shadow Brokers first surfaced in August 2016, claiming to have breached the spy tools of the elite NSA-linked operation known as the Equation Group. The Shadow Brokers offered a sample of alleged stolen NSA data and attempted to auction off a bigger trove, following up with leaks for Halloween and Black Friday in 2016.

This April, though, marked the group's most impactful release yet. It included a trove of particularly significant alleged NSA tools, including a Windows exploit known as EternalBlue, which hackers have since used to infect targets in two high-profile ransomware attacks (see below).

The identity of the Shadow Brokers is still unknown, but the group's leaks have revived debates about the danger of using bugs in commercial products for intelligence-gathering. Agencies keep these flaws to themselves, instead of notifying the company that makes the software so the vendor can patch the vulnerabilities and protect its customers. If these tools get out, they potentially endanger billions of software users.

WannaCry

On May 12 a strain of ransomware called WannaCry spread around the world, walloping hundreds of thousands of targets, including public utilities and large corporations. Notably, the ransomware temporarily crippled National Health Service hospitals and facilities in the United Kingdom, hobbling emergency rooms, delaying vital medical procedures, and creating chaos for many British patients.

Though powerful, the ransomware also had significant flaws, including a mechanism that security experts effectively used as a kill switch to render the malware inert and stem its spread. US officials later concluded with "moderate confidence" that the ransomware was a North Korean government project gone awry that had been intended to raise revenue while wreaking havoc. In total, WannaCry netted almost 52 bitcoins, or about $130,000—not much for such viral ransomware.

WannaCry's reach came in part thanks to one of the leaked Shadow Brokers Windows vulnerabilities, EternalBlue. Microsoft had released the MS17-010 patch for the bug in March, but many institutions hadn't applied it and were therefore vulnerable to WannaCry infection.

Petya/NotPetya/Nyetya/Goldeneye

A month or so after WannaCry, another wave of ransomware infections that partially leveraged Shadow Brokers Windows exploits hit targets worldwide. This malware, called Petya, NotPetya and a few other names, was more advanced than WannaCry in many ways, but still had some flaws, like an ineffective and inefficient payment system.

Though it infected networks in multiple countries—like the US pharmaceutical company Merck, Danish shipping company Maersk, and Russian oil giant Rosnoft—researchers suspect that the ransomware actually masked a targeted cyberattack against Ukraine. The ransomware hit Ukrainian infrastructure particularly hard, disrupting utilities like power companies, airports, public transit, and the central bank, just the latest in a series of cyber assaults against the country.

Wikileaks CIA Vault 7

On March 7, WikiLeaks published a data trove containing 8,761 documents allegedly stolen from the CIA that contained extensive documentation of alleged spying operations and hacking tools. Revelations included iOS and Android vulnerabilities, bugs in Windows, and the ability to turn some smart TVs into listening devices.

Wikileaks called the dump "Vault 7," and the organization has followed the initial release with frequent, smaller disclosures. These revelations have detailed individual tools for things like using Wi-Fi signals to track a device's location, and persistently surveilling Macs by controlling the fundamental layer of code that coordinates hardware and software.

WikiLeaks claims that Vault 7 reveals "the majority of [the CIA] hacking arsenal including malware, viruses, trojans, weaponized 'zero day' exploits, malware remote control systems and associated documentation." It is unclear, though, what proportion of the CIA toolbox the disclosures actually represent. Assuming the tools are legitimate, experts agree that the leaks could cause major problems for the CIA, both in terms of how the agency is viewed by the public and in its operational abilities. And as with the Shadow Brokers releases, Vault 7 has led to heated debate about the problems and risks inherent in government development of digital spy tools.

Cloudbleed

In February, the internet infrastructure company Cloudflare announced that a bug in its platform caused random leakage of potentially sensitive customer data. Cloudflare offers performance and security services to about six million customer websites (including heavy hitters like Fitbit and OKCupid), so though the leaks were infrequent and only involved small snippets of data, they drew from an enormous pool of information.

Google vulnerability researcher Tavis Ormandy discovered the problem on February 17, and Cloudflare patched the bug within hours, but the data leakage could have started as early as September 22, 2016. Leaked data was only deposited on a small subset of Cloudflare customer sites, and usually it wasn't visible on the pages themselves. Search engines like Google and Bing that crawl the web, though, automatically cached the errant data—everything from gibberish to users' Uber account passwords and even some of Cloudflare's own internal cryptography keys—making it all easily accessible through search.

Cloudflare worked with search engines ahead of and after the announcement to remove the leaked data from caches, and experts noted that it was unlikely that hackers used the data malevolently; the random leaks would have been difficult to weaponize or monetize efficiently. But any exposed sensitive data creates risks. The incident was also significant as a reminder of how much rides on large internet infrastructure and optimization services like Cloudflare. Using one of these services makes sites much more robust and secure than they probably would be on average if owners attempted to build defenses themselves. The tradeoff, though, is a single point of failure. A bug or a damaging attack affecting a company like Cloudflare can impact, and potentially endanger, a significant portion of the web.

198 Million Voter Records Exposed

Unfortunately, it's not uncommon to hear that a trove of voter data was breached or exposed somewhere in the world. But on June 19, researcher Chris Vickery announced a discovery that would give even the most jaded security expert pause. He had discovered a publicly accessible database that contained personal information for 198 million US voters—possibly every American voter going back more than 10 years.

The conservative data firm Deep Root Analytics hosted the database on an Amazon S3 server. The group had misconfigured it, though, such that some data on the server was protected, but more than a terabyte of voter information was publicly accessible to anyone on the web. Misconfiguration isn't a malicious hack in itself, but it is a critical and all-too-common cybersecurity risk for both institutions and individuals. In this case, Deep Root Analytics said that the voter data, though publicly exposed, was not accessed by anyone besides Vickery—but it's always possible that someone else discovered it, too. And though a lot of voter information is readily available anyway (names, addresses, etc.), Deep Root Analytics specializes in compiling revealing data, so being able to access so much pre-aggregated information would be a boon to a cyber criminal.

Macron Campaign Hack

Two days before France's presidential runoff in May, hackers dumped a 9GB trove of leaked emails from the party of left-leaning front-runner (now French president) Emmanuel Macron. The leak seemed orchestrated to give Macron minimal time and ability to respond, since French presidential candidates are barred from speaking publicly beginning two days before an election. But the Macron campaign did release statements confirming that the En Marche! party had been breached, while cautioning that not everything in the data dump was legitimate.

The attack was less strategic and explosive than the WikiLeaks releases of pilfered DNC emails that dogged Hillary Clinton's presidential campaign in the US, but Macron also had the advantage of observing what had happened in the US and preparing for potential assaults. Researchers did find evidence that the Russian-government-linked hacker group Fancy Bear attempted to target the Macron campaign in March.

After the email leak heading into the election, the Macron campaign said in a statement, "Intervening in the last hour of an official campaign, this operation clearly seeks to destabilize democracy, as already seen in the United States' last president campaign. We cannot tolerate that the vital interests of democracy are thus endangered."