1 The story behind NotPetya is not so cute, though. On June 27, 2017, Ukraine and Russian conflict would rise to new levels of belligerence as NotPetya was deployed. Within hours, NotPetya had taken out Ukraine’s electric grid, their subway system stopped working and even ATMs in Ukraine went out of service. Overnight, Ukraine was brought to its knees without firing a single bullet.

And the destruction wasn’t limited to Ukraine. The virus leaked from Ukraine into the whole world. The shipping giant Maersk ended up losing $300 million US dollars as their whole network went down. Later estimates would put the damage caused by NotPetya at $10 billion US dollars. It is still considered to be one of the most devasting cyber attacks in history.

2 Stuxnet to this day considered to be one of the [most dangerous pieces of malware](https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-stuxnet.html) to ever exist. Stuxnet was a sophisticated malware that attacked the Iranian uranium enrichment facility at Natanz. The malware would cause the centrifuges to burn out by accessing the industrial control system that controlled the entire system.

What is more devastating is that the facility at Natanz was air-gapped, meaning it was not connected to the internet. So, attackers used infected USBs to infiltrate the system. The scary part about Stuxnet is that it was designed to attack industrial control systems, such systems control our electric grids, dams, and oil pipelines. The most frightening part about Stuxnet is that it can potentially kill millions of people if used by the wrong people.

Even though officially the United States denies any involvement. Most cybersecurity experts attribute the virus to being created as a collaboration between the NSA, The US Department of Energy, and Israeli cyber division unit 8200.

3 The [Triton malware](https://www.technologyreview.com/2019/03/05/103328/cybersecurity-critical-infrastructure-triton-malware/) makes it number 3 because this was one of the first malware that could have potentially been fatal to the target. In the summer of 2017, a petrochemical plant in Saudi Arabia out of sheer luck discovered their systems were compromised.  
  
Immediately cybersecurity experts were flown in to take charge of the situation. What they discovered, would make the hair stand up on even the most seasoned cybersecurity experts. They found that the malware had gotten control over the plant’s safety instruments. With those compromised, the hackers with a flick of a single button could have caused massive explosions at the plant-killing hundreds of people in the process.

4 The [Shammon Virus attack](https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html" \t "_blank) was a computer virus that shut a trillion-dollar business empire back in 2012. The target of the virus was Saudi Arabia’s Aramco, the largest oil and gas company in the world:

On August 15, 2012, seemingly out of nowhere 30,000 windows based computers system were overwritten in a matter of hours. As Aramco would find out later, the attack wasn’t totally without warning. A few hours before the attack began, the group that claimed responsibility for the attack called ‘Cutting Sword of Justice’ posted a message on an Anonymous board.

The attack was so devasting that journalists reported miles and miles of truck lines outside Aramco refilling stations because no system was operational. It was a logistical nightmare. Overnight cybersecurity experts were flown in from all over the world to get everything online.

Later experts would attribute Iran state-backed hackers as the group responsible for the devastating attack

5 The [Bangladesh Bank cyber heist](https://www.dhakatribune.com/uncategorized/2016/03/12/the-great-bangladesh-cyber-heist-shows-truth-is-stranger-than-fiction) was a coordinated digital attack that took place in February 2016. The hacker planned to steal $1 billion US dollars from the Bangladeshi national bank by using fake SWIFT transactions. This money was sitting in the Federal Reserve Bank of New York, and the hackers exploited very poor cybersecurity at the Bangladesh bank to gain access to this fortune.

Five out of the thirty-five fraudulent transactions successfully went through before anyone noticed. The attackers managed to get away with $101 million US dollars before the Federal Reserve Bank of New York caught on. The remaining thirty transaction requests were blocked. $81 million US dollars were traced to the banking system in the Philippines and about $20 million US dollars were traced to a bank in Sri Lanka.  
  
The FBI would later attribute this devasting cyberattack to a North Korean hacker group called the Lazarus Group. This was a shock to the cybersecurity world, as for the first time a nation-state had performed a cyberattack not for information or sabotage, but purely for financial gains.