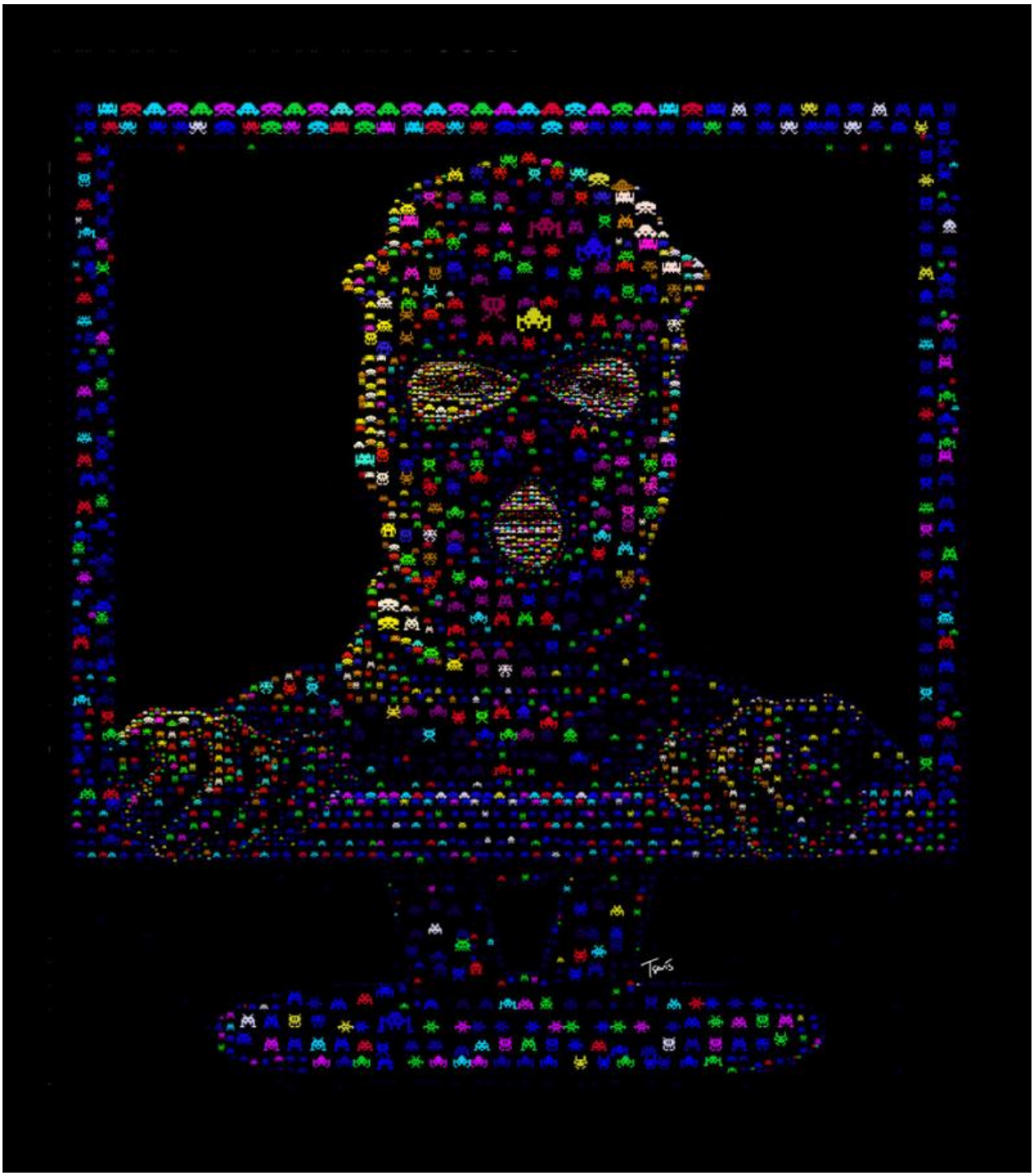
After the NSA hack: Cybersecurity in an even more vulnerable world

August 22 2016, by Nir Kshetri



Cybersecurity just got even more difficult. Credit: Charis Tsevis/flickr, CC BY-NC-ND

It is looking increasingly likely that computer hackers have in fact successfully attacked what had been the pinnacle of cybersecurity – the U.S. National Security Agency (NSA). A few days ago, reports began emerging of claims by a hacking group called the Shadow Brokers that it had breached the network of, and accessed critical digital content from, computers used by the Equation Group. This attracted more than the usual amount of attention because the Equation Group is widely believed to be a spying element of the NSA.

It is possible – perhaps even likely – that Shadow Brokers is a group of hackers linked to the Russian government.

Shadow Brokers posted online some examples of the data it said it had stolen, including scripts and instructions for breaking through firewall protection. Cybersecurity analysts poring over that information are confident that the material is in fact from Equation Group. This news raises a bigger question: What are the consequences if the Equation Group – and by extension the NSA – were actually hacked?

What has been breached?

The NSA holds a massive amount of data, including information on U.S. citizens' and foreign nationals' phone calls, social connections, emails, web-browsing sessions, online searches and other communications. How much data? NSA's Utah data center alone is reported to have a storage capacity of 5 zetabytes – 1 trillion gigabytes. However, judging from what has been made public of what has been stolen by Shadow Brokers, this massive data trove has not been breached.

But the NSA's other key digital asset is a collection of very sophisticated, often custom-designed, hacking, analysis and surveillance software. The agency uses these tools to break into computer networks at home and abroad to spy on specific targets and the public at large.

The Shadow Brokers have claimed to have copies of this software and information on security vulnerabilities the NSA uses in its attacks, including instructions for breaking into computer networks. If true, these would be of very high strategic value to someone seeking to defend against cyberattacks, or wanting to conduct their own.

What is the Equation Group?

The Equation Group has been closely watched since its existence was first revealed in an early 2015 report by security researchers at Kaspersky Lab, a Russian-based computer security company. Cyberattacks using the Equation Group's signature methods have been carried out since 2001, using extremely specific customized techniques.

In addition to engineering the attacks to ensure a very low risk of detection, they maintain a close watch on their targets to ensure their surveillance does in fact go undetected. And the number of targets they choose is very small – tens of thousands of computers as opposed to the hundreds of thousands or even tens of millions of machines hacked in other major attacks.

Equation Group's targets included government and diplomatic institutions, companies in diverse sectors as well as individuals in more than 30 countries.

Kaspersky Lab reports that China and Russia are among the countries most infected by the Equation Group's hacking tools. Among the alleged targets were the Russian natural gas company Gazprom and the airline Aeroflot. Likewise, China's major mobile companies and universities were allegedly victimized by the NSA.

Who hacks whom?

Cyberweapons and their capabilities are becoming an increasing part of international relations, forming part of foreign policy decisions and even sparking what has been called a "cyber arms race."

The Shadow Brokers attack may be a part of this global interplay. The U.S. government is considering economic sanctions against Russia, in response to the alleged cyberattack on the Democratic National Committee computers by two Russian intelligence agencies. Those same attackers are believed to have been behind the 2015 cyberattacks on the White House, the State Department and the Joint Chiefs of Staff.

If the material Shadow Brokers have stolen can link cyberattacks on Gazprom, Aeroflot and other Russian targets with the NSA, Russia can argue to the international community that the U.S. is not an innocent victim, as it claims to be. That could weaken support for its sanctions proposal.

Russia and China, among other adversaries, have used similar evidence in this way in the past. Edward Snowden's revelation of the U.S. PRISM surveillance program, monitoring vast amounts of internet traffic, became an important turning point in China-U.S. cyberrelations. Commenting on the NSA's alleged hacking of China's major mobile companies and universities, an editorial in China's state-run Xinhua News Agency noted: "These, along with previous allegations, are clearly troubling signs. They demonstrate that the United States, which has long been trying to play innocent as a victim of cyberattacks, has turned out to be the biggest villain in our age."

In general, allegations and counterallegations have been persistent themes in Chinese-American interactions about cybercrimes and cybersecurity. China's approach shifted toward more offensive strategies following Snowden's revelation of the PRISM surveillance program. It is likely that this hack of cyberweapons may provide China and other U.S.

adversaries with even more solid evidence to prove American involvement in cyberattacks against foreign targets.

Cyberattack tools now more widely available

There are other dangers too. Hackers now have access to extremely sophisticated tools and information to launch cyberattacks against military, political and economic targets worldwide. The NSA hack thus may lead to further insecurity of cyberspace.

The attack is also further proof of the cybersecurity industry's axiom about the highly asymmetric probabilities of successful attack and successful defense: Attackers need to succeed only once; defenders have to be perfect every time. As sophisticated as NSA's highly secure network is, the agency cannot ever fully protect itself from cyberattackers. Either these attackers have already gotten in, or some other group will be the first to do so in the future.

Actors with fewer financial and technical resources can compromise high-value targets. What will come of this attack remains to be seen, but the potential for profound and wide-ranging, even global, effects is clear.

This article was originally published on The Conversation. *Read the* original article.

Source: The Conversation