I am director of the Center for Cybersecurity, Information Privacy, and Trust in the College of Information Sciences and Technology at Penn State. Our center is certified by NSA and DHS as a National Center of Academic Excellence in Information Assurance Education.

The cybersecurity problem is caused by two basic characteristics of cyber systems: vulnerabilities in software & hardware, and psychological weaknesses in human users.

Cyber criminals know how to automatically exploit these vulnerabilities and steal personal data. By “automatically”, I mean malware. Through evolution, today’s malware is sophisticated and powerful.

For example, a study shows that the Target 2013 data breach could be resulted from a widely-used malware called Citadel. It is a sophisticated botnet malware. Below I describe how cyber criminals use Citadel in a step by step manner.

Step 1: the cyber criminal needs a server that is hosted by a company. Such companies are called Bulletproof hosting. Some foreign countries allow such companies to exist.

Step 2: the cyber criminal buys the Citadel kit for around $3,000 USD.

Step 3: the cyber criminal installs and runs Citadel. Next, Citadel will automatically create a small piece of bot malware. The bot malware is built to avoid Anti-Virus detection.

Step 4: Citadel distributes the bot malware to a large number of infected websites, as many as 2,500,000. These websites were previously infected either by Citadel or other malware, due to the first basic characteristic of cyber systems.

Step 5: A study shows that employees of a Target contractor, which is a heating and air conditioning firm in PA, had visited one of these websites. Due to drive-by download vulnerabilities, the bot malware was automatically installed on an employee’s computer without consent.

Step 6: the bot malware steals credentials used by employees of the Target contractor.

Step 7: A study shows that the malware could have used the stolen credentials to login onto a particular back-end server which interconnects an external billing system of Target called Ariba and the rest of the corporate network of Target. We know the network occupied by POS devices is part of the corporate network of Target.

Step 8: If the back-end server is infected, the malware could obtain the credential of a Target employee. Using the credential, the malware could access the POS devices. As we know, millions of credit and debit cards were stolen.

Step 9: A global black market exists, where the price tag for one set of credit card credentials ranges from $35 to $135.