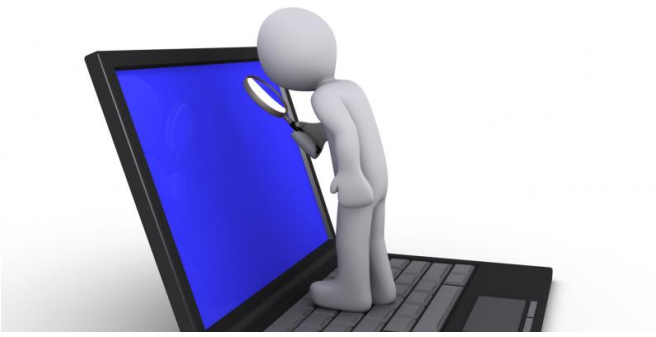
An ethical hacker explains how to track down the bad guys

2 February 2017, by Timothy Summers



Looking deep into computer activities. Credit: shutterstock.com

When a cyberattack occurs, ethical hackers are called in to be digital detectives. In a certain sense, they are like regular police detectives on TV. They have to search computer systems to find ways an intruder might have come in – a digital door or window left unlocked, perhaps. They look for evidence an attacker left of entry, like an electronic footprint in the dirt. And they try to determine what might have been copied or taken.

Understanding this process has become more important to the public in light of recent events in the news. In October 2016, the U.S. officially said Russia was trying to embarrass respected political figures and interfere with the U.S. presidential election process. Specifically, the Obama administration formally blamed Russia for hacking into the Democratic National Committee's computer systems. The statement hinged on the investigative capabilities of American ethical hackers working for both private companies and government agencies.

But how do people track down hackers, figuring out what they have done and who they are? What's involved, and who does this sort of work? The answer is that ethical hackers like me dig deep into digital systems, examining files logging users' activity and deconstructing malicious software. We often team up with intelligence, legal and business experts, who bring outside expertise to add context for what we can find in the electronic record.

Detecting an intrusion

Typically, an investigation begins when someone, or something, detects an unauthorized intrusion. Most network administrators set up intrusion detection systems to help them keep an eye on things. Much like an alarm system on a house, the intrusion detection software watches specific areas of a network, such as where it connects to other networks or where sensitive data are stored.

When it spots unusual activity, like an unauthorized user or a surprisingly high amount of data traffic to a particular off-site server, the intrusion detection system alerts network administrators. They act as cybersecurity first responders – like digital firefighters, police officers and paramedics. They react to the alert and try to figure out what happened to trigger it.

This can include a wide range of attacks, from random, unstructured incursions by individuals and small groups to well-organized and precision-targeted strikes from hackers backed by government agencies. Any of them can set off an intrusion alarm in a variety of ways.

The immediate response

Many times, the initial investigation centers on collecting, organizing and analyzing large amounts of network data. Computer networking equipment and servers keep records of who connects, where the connection comes from and what the user does on the system.

Depending on what that analysis shows, the administrator may be able to fix the problem right

away, such as by preventing a particular user from logging in, or blocking all network traffic coming from a particular place. But a more complex issue could require calling a sophisticated incident response team.

Ideally, each company or organization should have its own internal team or rapid access to a team from outside. Most countries, including the U.S., have their own national response teams, often government employees supplemented by private contractors with particular expertise. These teams are groups of ethical hackers who are trained to investigate deeper or more challenging intrusions. In addition to any self-taught skills, these people often have additional experience from the military and higher education. Their most vital expertise is in what is called "just-in-time learning," or figuring out how to apply their skills to new situations on the fly.

They conduct larger-scale digital forensic inquiries and analyze malicious software that may have been introduced during the attack. Typically, these teams work to stop the attack and prevent future attacks of that type. The teams can, at times, hunt down the attackers.

Attributing an attack

Determining the identity or location of a cyberattacker is incredibly difficult because there's no physical evidence to collect or observe. Sophisticated hackers can cover their digital tracks. Although there are many different attribution techniques, the best approach takes advantage of more than one. These techniques often include looking very closely at any files or data left behind by the attackers, or stolen and released as part of the incursion.

Response teams can analyze the grammar used in comments that are commonly embedded in software code, as programmers leave notes to each other or for future developers. They can inspect files' metadata to see whether text has been translated from one language to another.

For example, in the DNC hack, American cyber experts could look at the specific files published on Wikileaks. Those files' metadata indicated that some of them contained text converted from the Cyrillic characters of the Russian alphabet to the Latin characters of English.

Investigators can even identify specific sociocultural references that can provide clues to who conducted the attack. The person or group who claimed responsibility for the DNC hack – using the name Guccifer 2.0 – claimed to be Romanian. But he had a hard time speaking Romanian fluently, suggesting he wasn't actually a native. In addition, Guccifer 2.0 used a different smiley-face symbol than Americans. Instead of typing ":)" Guccifer 2.0 just typed ")" – leaving out the colon, implying that he was Eastern European.

Experienced cyber-investigators build an edge by tracking many significant threats over time. Just like with "cold cases" in regular police work, comparing the latest attack to previous ones can sometimes reveal links, adding pieces to the puzzle.

This is particularly true when dealing with what are called "advanced persistent threats." These are attacks that progress gradually, with very sophisticated tactics unfolding over long periods of time. Often attackers custom-design these intrusions to exploit specific weaknesses in their targets' computer systems. That customization can reveal clues, such as programming style – or even choice of programming language – that combine with other information to suggest who might be responsible.

The cyber-defense community has another advantage: While attackers typically work alone or in small groups and in secret, ethical hackers work together across the world. When a clue emerges in one investigation, it's common for hackers to share that information – either publicly on a blog or in a scholarly paper, or just directly with other known and trusted investigators. In this way, we build a body of evidence and layers of experience in drawing conclusions.

Very often, a report from an attack investigation will yield clues or suggestions, perhaps that an attacker was Russian or was using a keyboard with Korean characters. Only when the conclusions are clear

and irrefutable will investigators directly accuse specific attackers. When they do, though, they often share all the information they have. That bolsters the credibility of their conclusions, helps others identify weaknesses or failures of logic – and it shares all that knowledge with the rest of the community, making the next investigation that much easier.

The most skilled hackers can write self-erasing code, fake their web addresses, route their attacks through the devices of innocent victims and make it appear that they are in multiple countries at once. This makes arresting them very hard. In some attacks, we are able to identify the perpetrator, as happened to celebrity-email hacker Guccifer 1.0, who was arrested and imprisoned.

But when the attack is more advanced, coordinated across multiple media platforms and leveraging skillful social engineering over years, it's likely a government-sponsored effort, making arrests unlikely. That's what happened when Russia hacked the U.S. presidential election. Of course, diplomatic sanctions are an option. But pointing fingers between world superpowers is always a dangerous game.

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

Provided by The Conversation