Forbes

NO BIT SHERLOCK—THE ROLE OF FORENSICS IN TRACING THE DNC HACK

By Forbes Columnist/Skytop Strategies CEO and Founder Christopher P. Skroupa

Kristofer Swanson, CPA/CFF, CAMS, CFE is Vice President and Practice Leader for the Forensic Services practice at Charles River Associates (CRA), which helps companies and their counsel respond to allegations of fraud, abuse, misconduct, and noncompliance. These allegations present in a variety of contexts, including data/cyber breaches, accounting and financial reporting irregularities, money-laundering, FCPA/ABAC violations and trade secret theft. He is frequently called upon to present his findings to boards and executive management teams, and to government regulators such as the SEC, FDIC, Federal Reserve, and U.S. Department of Health and Human Services.

Christopher P. Skroupa: There is a lot of press about the DNC hack right now. How do investigators attribute a hack to a specific party or country and what role do forensics play?

Kristofer Swanson: When we respond to an intrusion, or hack, one of the things we assess is the mechanism used to gain access and what data was compromised. In our experience, hackers don't just get in—they attempt to get your data out. Hackers use commands sent from other potentially compromised computers to perpetrate the attack.

Tracing the destination of the data and the origin of the commands usually provides a place to start for attribution. Malware or software used in the hack can also provide clues, as there are leading forensic tools that can catalogue certain code snippets, behaviors, or pre-programed instructions. This type of behavior

analysis can provide attribution. Many government agencies have access to similar resources as well. That is likely how the DNC hack is being attributed—not necessarily by where the data went, but by the software and techniques used in the hack.

Skroupa: How do you believe the U.S. Government is attributing the DNC hack to Russia?

Swanson: State-sponsored cyber-warfare frequently uses specialized programs specifically written by the perpetrators. The code in the hackers' programs, and the method by which they work, usually betrays the attacker. We haven't looked at the evidence in this matter, but small tidbits of cultural references, phrases, names or folklore usually find their way into an attacker's method or custom-written programs. Those small clues, combined with the other evidence in the case, typically provide enough material for attribution. It is very much a digital "Sherlock Holmes" investigation.

Skroupa: Specifically, what role do digital forensics play in a case like this?

Swanson: Digital forensics practitioners are concerned with the evidence of human interactions with a computer or network. These investigations are very much detective stories peppered with small clues that are used to piece together the events of the attack. We use bits of data and various artifacts in a computer, network or program to piece together what happened and who could be responsible.

Skroupa: How long do these types of attacks take to enact?

Swanson: Hollywood would have you believe hackers gain root-level access within minutes. In reality, the attackers are frequently inside the breached computer or network for months–even years—before a problem is identified. Many companies only find out there has been a breach of their system once their data is located on the Dark Web or someone is exploiting it; in this case, data was disclosed to WikiLeaks. Media reports suggest the DNC attackers were in the DNC systems for at least 10 months prior to the WikiLeaks disclosure. Once the DNC knew they had an attack and brought in a forensics services firm, the method used was identified within weeks and the clandestine access was shut off within hours of identification.

Skroupa: How is it possible for companies not to know they have been breached?

Swanson: Hackers are continually improving their tradecraft—this is especially true for state-sponsored hacking. The artifacts and events used to uncover the hack look like normal user activity until some clue is discovered that provides context to the behavior.

For instance, an employee logging into their company's network during the workday isn't unusual, unless perhaps the employee was terminated 3 weeks prior. A fact such as the termination provides context to an otherwise a mundane fact. Once an anomaly such as a terminated employee has been identified, we then work through the other artifacts to string together that which is normal and that which is not. The threat landscape for digital security is constantly evolving—it is a balance between security and usability. As new solutions are developed, attackers find new vulnerabilities.

The views expressed herein are the views and opinions of the author and do not reflect or represent the views of Charles River Associates or any of the organizations with which the author is affiliated.