BehavioSec

Cybercrime: It's Not About How, But Why?

by: Shane D. Shook, PhD, ForgePoint Capital

When most people think about cybercrime, especially when they are victims of a data breach or business interruption by hackers, they tend to focus on *the how.* While tempting, this rarely leads to the culprit or a better defense.

Most hacking today is contracted by perpetrators with an objective crime such as insider trading or intellectual property theft, to syndicated groups who offer previously compromised computers – or are willing to intrude on commission or at a set price.

The tools hackers use are utilitarian and more often take advantage of the weaknesses of people or systems around a target, than taking direct action that would reveal the actual objective. Focusing on the how also doesn't accurately point to the risks that organizations face. For example:

- **Corporate Botnets:** It is estimated that 70% of computers that belong to "botnets" (computers under the control of "botmasters") are behind corporate firewalls. The average duration of a botnet-controlled computer is only three to six months; however, the recidivism rate for the same computers to return to botnet control is more than 50%.
- **Outdated Software Vulnerabilities:** From audits of large and small organizations, both public and private, more than 80% of computers, network devices, and related services applications have outdated software – with known or identifiable weaknesses either because of improper configuration or inventory lethargy.
- **IT Staff Turnover:** Additionally, the average tenure of an information technology or services staff member in a distinct functional role is less than one year; while related pay and benefits change only approximately every three to five years.

The combination of these factors leads to opportunities for social or technical engineering to exploit weaknesses and gain access that is extremely valuable as a commodity. These are cybersecurity risks.

LOOKING AT COMMODITY VALUES DETERMINES THE OBJECTIVES

The commodity values determine the objectives which is why identity theft is the most valuable criminal enterprise in our interconnected cyberspace. We are vastly more connected as our cyber-selves than in our physical relationships. Cyber-connectivity enables identity thieves and impersonators to manipulate financial accounts, economic outlooks, information delivery, and even public perceptions.

Opportunity is the next most valuable commodity. Opportunities come in many forms such as controlling payments to suppliers, influencing value decisions in M&A, or acting as a puppeteer with public sentiments related

to patriotism, ecology or other core human values. The opportunity to take control of a commodity at a time and place of vulnerability is highly prized by competitive industry or political interests.

Although software vulnerabilities such as "Zero-days" get a lot of excitement in the press, they have comparatively low value. In fact, they aren't actually used in most cybercrimes. It is much easier for intruders to utilize known exploits for weaknesses to gain entry and control over systems.

The preferred tactics of intruders today are still phishing, social engineering (such as phone calls or payments to willing employees or contractors), or simple USB drops. These are tools in the arsenal of intruders that make it possible for botnet creation so that access can be provided to those with significant interests.

UNDERSTANDING THE WHY CAN HELP DETERMINE HOW IT MIGHT HAPPEN

A cybercriminal needs three things to be successful. They need a tool that will enable their actions, an identity (or credential) to access an organization's resources, and they need time to achieve their objective.

Because most cybercrimes involve two or more parties affiliated only by financial or otherwise intersecting interests, the means and motives are distinctly separate. This means it's really the opportunity that is the fundamental risk.

Managing cyber risk is dependent upon monitoring the opportunities that might exist for someone to exploit people, processes, or related technologies to gain an advantage. Yet, risk is typically measured by how an event will impact an organization, but seldom based on why.

Consider the difference in the following scenarios:

1. Malware is reported in antivirus alerts to IT on some computers.
2. Ransomware interrupts the financial quarter closing activities.
3. Customers complain of ransomware stemming from emails from your organization.
4. Your CFO discovers that funds have been wired from your corporate account.
5. Customers complain about emails and phone calls demanding renewal payments for your products.
6. Hackers contact your organization with an extortion demand.
7. The press learns of these events and reports.
8. Your organization is contacted by plaintiffs' attorneys…

The impact of the events in these scenarios are independently much less than if measured over time. Once its revealed as a coordinate cyber crime, the reasons (at least in the first 6 parts) is clearly financial gain *in retrospect*. But by reacting to each incident as they emerge, often without organizational coordination – the risk cannot be managed.

KNOWING THAT IT WILL HAPPEN, HELPS US TO DEFINE OUR DEFENSES

Competitors always look for weaknesses – and victim companies all have one thing in common, they have resources that have value to the criminals who take advantage of their weaknesses. But with targeted cyberattacks, professional services companies are often the preferred access points to reach their customers who are the intended victims. For example, an email from your investor, lawyer, accountant, or auditor – or network traffic between your company and theirs' are expected, "trusted" and easy to overlook.

This "trust" is an opportunity that cybercriminals have exploited through impersonation. Clients provide data rooms, financial accounts, and even remote access to company networks and systems to service providers, which has led to increased compromises at industry scale.

Defense depends upon first accepting the simple truth that cybercrimes will happen, because your property, your time, and your identity are all valuable to hackers. Next, it's about knowing your dependencies and trusted relationships:

- **Identity Services –** Who manages your domain?
- **Messaging Services –** Who controls your email?
- **Network Services –** Who facilitates your Internet access?
- **Computing Services –** Who administers your data processing and storage?
- **Personal Services –** What devices do you use?

Many organizations are struggling to understand that "cyber" security is not the same thing as information security. Information security is about information, but cybersecurity is about our dependency upon technology to facilitate our relationships and interactions. It is as much about ensuring resiliency as it is about ensuring privacy, because without those services we are blind, deaf and dumb.

So while many focus on the tools, tactics and procedures behind a hack, the best defense can only be put into place by first understanding the means, motives and opportunity – which are the why behind cybercrime.

ABOUT THE AUTHOR

Dr. Shook is a Venture Consultant with Forgepoint Capital, and a Security Advisor and Expert Witness. He has helped organizations around the world investigate and redress cyber fraud, theft and business interruptions.