Hacking risks are intensifying. For example, hackers recently wired $1 billion dollars from a bank in Bangladesh directly connected to the World Bank.\(^1\)

The Opportunity

Innovations such as public and private clouds, enterprise mobility, and BYOD are enabling digital business transformations and breakthroughs in collaboration, process, and service efficiency. But they have also opened government and corporate networks, and the organizations that run them, to greater risk from hackers.

Hackers and information thieves have the resources and expertise to find and exploit every network weakness. As the following examples illustrate, even the most hardened networks are at risk:

- The U.S. Government Office of Personnel was attacked in 2015, with personal information of 21.5 million people stolen in a massive data breach.
- Iranian hackers conducted a series of coordinated attacks on major U.S. banks, resulting in millions of dollars of lost business. These same hackers also tried to shut down a dam located in New York.\(^2\)
- Hackers breached Bangladesh Bank’s systems in 2016 and stole its credentials for initiating payment transfers. They nearly succeeded in a $1 billion US heist involving the New York Fed – and managed to walk away with $80 million even after the suspicious activity was detected.\(^3\)

\(^1\) http://www.cbc.ca/news/technology/bangladesh-bank-typo-hack-new-york-fed-1.3485125
\(^2\) http://www.reuters.com/article/us-usa-iran-cyber-idUSKCN0WQ1JF
One of the most notable commercial data breaches was Target Corporation, who was attacked in 2013 and had a large amount of customer credit card information stolen from various systems on its’ network. Years later, Target settled lawsuits from consumers for $39 million.

The Target data breach clearly shows how traditional defenses such as firewalls are no longer sufficient protection. In the case of Target, once the attackers got behind the firewall, they were able to roam the Target internal networks “looking” for sensitive and valuable information, which was found in POS systems. Equally important, many breaches occur behind the firewall due to the accidental and malicious behavior of employees and contractors.4

The good news is, even the most skilled perpetrators leave digital footprints across an organization’s network. And using the right analytical tools, these footprints can be used to identify suspicious behavior on networks and stop breaches before it’s too late. For example, forensic analytics can identify anomalies in the network as hackers work – and if a hack happens, it can determine which servers and data were accessed.

Datameer’s Approach

Datameer’s Modern BI platform helps both network detection and forensic analysis. It empowers analysts to integrate and analyze network data with sophisticated algorithms that have been made point-and-click to find meaningful patterns and hidden events that reveal hacker activity. Specifically, the solution:

• Helps you integrate and analyze all of your data – both structured and unstructured – from servers, network browsers, and other resources
• Uses path analytics, including advanced time series analytics and event correlations, to provide insight into the patterns and paths of security threats
• Uses SCP (Secure Copy Protocol) to load log data from thousands of servers in parallel, move it into Hadoop and render it ready for immediate analysis
• Employs a public-private key infrastructure for to encrypt and mask sensitive, personally identifiable information and credit card data

4 According to the Online Trust Alliance’s 2015 Data Protection Best Practices and Risk Assessment Guide, between January to June 2014, only 40 percent of data breaches involving the loss of personally identifiable information were due to external actors; 29 percent occurred due to the actions of employees. (http://www.zdnet.com/article/over-90-percent-of-data-breaches-in-first-half-2014-were-preventable/)
Use Cases

As illustrated in the following use cases, Datameer augments your existing firewalls and detection methods with forensic analytics and pattern detection to help identify suspicious activity on your network and the risk they pose. You'll be able to detect threats with known signatures faster, identify new but suspicious activity, track the paths of hackers, and calculate your true risk and exposure levels.

Identify Anomalies in Device Behavior

Using Datameer, you can detect when someone is using a device connected to your network to steal data or perform other malicious acts. For example, if your company has a BYOD program, and an employee's iPhone is accessing 200 systems in parallel, it's likely being used as a Trojan horse to access and steal data.

A global bank with a vast network of servers, cloud resources, mobile devices, and other assets recognized the growing security risks associated with having hundreds of thousands of employee devices connected to its network. Many of these devices bridge public and private networks. The bank deployed Datameer to analyze the behavior patterns of connected devices and their users around the clock.

Identify Anomalies in Employee and Contractor Behavior

You can also use Datameer to detect suspicious employee and contractor behavior on the network. Datameer can identify when users with broad or unlimited permissions access servers they don't normally access or download large amounts of data – just as Edward Snowden did when he made off with a huge trove of highly classified government documents. These are the kinds of behaviors that even the NSA couldn’t detect as late as 2014. According to investigators, Snowden’s “insider attack” was hardly sophisticated and should have been easily detected.5 It would have been detected if they had employed forensic analytics on their network.

---

As this example suggests, Datameer can be used to understand the activity and behavior of everyone on your network. It can integrate and analyze log files from the servers used to run database and applications with employee role, profile and permission data to identify changes in behavior. Based on these behavior patterns, suspicious events can then be detected and escalated, as needed.

Detect Anomalies in the Network

Hackers are intelligent and are constantly finding new ways to disguise their attacks and slip behind corporate networks to steal information. Datameer can provide the analytic horsepower to identify new threats without known signatures, so you can quickly protect your networks and systems.

Datameer’s forensic capabilities are so powerful that a leading antivirus software uses it to help protect its customers from Internet threats. Because of the massive volume of customer samples they need to analyze, they wanted to harness the power of Hadoop, but the complexities of programming on it prevented them from moving forward. They needed to correlate data from various silos to understand the complex nature of various attacks.

Datameer changed everything by eliminating the need to do complex programming on Hadoop. Datameer provided an easy to use, analyst-friendly interface that allowed the research and analysis team to bring together all their data, correlate it, and apply powerful analytic functions to identify the attack patterns and signatures.

Now the company can perform complex analysis at scale – up to 300,000 samples a day – as well as look at wide range of data attributes. If Datameer detects suspicious network activity, it flags the file, tracks it to monitor behavior, and escalates it for review by experts. The signatures of new, unknown viruses are captured, added to the database of its antivirus software, and used for future, automatic detection.
Assess Network Vulnerabilities and Risks

Other companies are using Datameer to perform network vulnerability analysis. For example, a national retailer purchased several companies and wanted to understand the network vulnerabilities these businesses posed. Using Datameer, they ingested data from every company’s database and analyzed it to understand, for example, which databases have customer-identifying information, and the degree to which they are vulnerable to hackers.

In one instance, Datameer identified a customer support system used to track issues as a high-risk system. Service representatives using the system were asked to verify the credit card customers used to make their initial purchase, but it was determined that such highly sensitive customer data shouldn’t be exposed in this kind of system or to these employees. The company took action to stop this practice and thus eliminated a serious potential source of risk.

To learn more about how Datameer can help your business, please visit www.datameer.com.