

Bank Fraud & IT Security

REPORT

Prepared by
Southeast Consulting, Inc.



Curtailing Data Theft via Outbound Traffic Monitoring

By Ryan Spanier, Gladiator Technology

A financial institution's greatest asset is its information. This critical information often includes data on customers, finances, personnel, credit cards, online accounts, and other proprietary records. This information exists in various forms, stored within your bank's information technology infrastructure. This same infrastructure has connections to the Internet, through which most financial institutions connect to core service providers, managed service providers, and online Web services. However, the Internet also potentially connects your bank to bot herders, spam operators, fraudsters, malware authors, and identity thieves.

To protect their proprietary information, bank IT security managers *wall up* their financial institutions with multiple security layers consisting of firewalls, intrusion protection appliances, event log monitors, antivirus software, and strict network policies. Bank management believes that these precautions will protect their banking information from hackers trying to break in. And, for the most part, they are correct. All of those port scans, brute force attacks, and SQL injection attacks typically do not get through to their bank's network infrastructure. However, many banks overlook the network traffic and the accompanying data that is leaving the bank. What's more, the destination of much of this outgoing data is often

unknown.

Cyber thieves and bank fraudsters have found a new way to successfully attack your bank's network. Unfortunately, this approach is easy to implement and tends to be very reliable. All the cyber thieves have to do is advertise their programs on the Internet. And why not? This approach works for other Web services, so why not bank fraud.

Hidden in Plain Sight. Who can tell the difference between a legitimate anti-malware program named *Malware Bytes* and a malicious, fraudulent application called *Mallware Bites*? Since most banking employees have access to the Internet as well as administrative rights for their personal computers, Web-based malware applications are often downloaded and installed on banking equipment at an alarming rate. Even if an employee knows not to download programs from the Internet, there is still the issue of malware exploiting trusted client applications, such as Adobe Acrobat or Internet Explorer, by compromising these applications' automatic download and update functionality. Unfortunately, traditional protection methods are not keeping up with the growing pace of this dangerous threat.

Camouflaged Malware. Malware authors have become much better at disguising their applications, and not just by making it look professional and by using proper grammar. Since traditional antivirus and intrusion protection services technology is based on tell-tale

Bank Fraud and IT Security Report

signatures, malware authors have started changing their code more often. Cyber thieves frequently alter their malicious code signature each time their application is downloaded. It is difficult to have a signature for something that is constantly changing.

Malware has also become multi-purpose. That is, instead of using one piece of malware to send spam, another to steal data, and another for a backdoor application, cyber thieves can now change and update their programs to meet the changing defense landscape within the banking community. What's more, once one piece of a malware application is installed, there is a strong probability that other features will be downloaded to expand the fraudster's hold on the system. And if an antivirus signature is developed to detect it, these malicious programs can simply download an update that will change the code signature once again so it will not be detected. New malware has recently been discovered that can even disable your bank's desktop antivirus applications altogether.

Where to Turn for Help. So if applying the concept of *defense-in-depth* along with using a good antivirus suite is not the answer, then what is? Although there is no perfect solution, a good start is to conduct outbound traffic analyses. If malware is stealing your data, it is likely sending it somewhere, because if it just sits on your system, it is of no benefit to the malware authors. Moreover, if the malware is going to send spam or join a botnet, the application must still check in with a command and control server.

So why not monitor all outbound connections to the Internet? Realistically, this task would be a tall order for most financial institutions to undertake alone. Accordingly, the answer to this data security dilemma may be to engage a

managed security service provider (MSSP). Several high-performance MSSPs have recently developed new services to analyze raw traffic data to fill this existing protection gap.

For example, Gladiator Technology has developed a product called *Raw Traffic Analyzer* (RTA) to identify and track suspicious traffic transmitted from a banking client's network. This traffic often includes malware downloads, malware check-in traffic, botnet traffic, and suspicious connections to known malicious subnets.

If a connection is flagged by RTA, it is then examined to determine content and intent. If deemed malicious, Gladiator Technology specialists alert the bank. This important new service provides relevant data along with the alerts, including internal IP address, what connections were discovered and possible malware variants that may have initiated the suspect transmission.

In addition, RTA can assist in determining if malware was fully removed by ensuring that no additional malicious transmissions are occurring from the internal IP. RTA can even detect malware connections from a laptop that was infected outside the bank's network architecture and then attached to the internal secured banking network.

Furthermore, the subnets and malicious addresses monitored by RTA are constantly updated with new information from the security community at large as well as from Gladiator's own Security Research Department. When new threats are identified, RTA technology can also examine archived data to determine if other financial institutions were infected previously, even if the malware was unknown at the time.

Defense in Depth. Even though cyber

thieves have *upped the ante*, a defense-in-depth approach coupled with an antivirus suite is still your bank's recommended first line of defense. However, bank IT security managers should not rely solely on antivirus software to determine if a network is infected with malware. There is a growing coverage gap, and until antivirus programs catch up, this gap may leave your financial institution vulnerable to data theft. RTA offers a viable option to fill this dangerous gap. However, no matter what course your bank management may choose, it is vitally important to closely monitor your bank's outgoing network traffic. Identifying suspicious connections can go a long way in determining if your bank has a data thief lurking within your network perimeter.

Ryan Spanier is a senior information security engineer with Atlanta-based Gladiator Technology, a division of ProfitStars, which provides enterprise network and information security solutions exclusively to financial institutions nationwide. In his key role focusing on professional services and security research, Spanier's duties include performing security assessments and malware research, as well as directing Gladiator's Security Research Department. He has a BS degree in computer engineering from the Georgia Institute of Technology and holds certifications from GIAC and ISC2.

GLADIATOR
TECHNOLOGY  A PROFITSTARS® SOLUTION

About Gladiator Technology - A ProfitStars® Jack Henry company
based in Atlanta, Georgia,
Gladiator Technology (www.gladiatortechnology.com) is a managed security services provider focused specifically on information security protection for the financial institutions industry. The company assists more than 650 financial institutions nationwide in securing networks and protecting financial data in adherence with Federal Financial Institutions Examinations Council (FFIEC) regulations.