Overview

The proliferation of smartphones and tablets and the subsequent demand by banking customers to conduct financial transactions at any time and from any location or device has prompted financial institutions to make it easier for customers to manage their money on the move. However, supporting and protecting this anytime, anywhere access has become increasingly difficult using traditional security measures. Not only are the access requirements growing, but the threat landscape is evolving, with attacks increasing in frequency and sophistication.

HID Global’s ActivID® Threat Detection Service (TDS) is a frictionless solution which allows financial institutions to mitigate the risks of even the most sophisticated malware whilst providing a seamless and easy to use experience. This paper outlines how ActivID TDS operates and details the technical requirements financial institutions should look for when seeking an integrated layered authentication platform to ensure a consistent security experience for multi-channel banking.

The Problem: Maintaining Security in the Face of Increased Threats – While Balancing Access Requirements and Costs

Any financial institution or business that offers Internet and mobile banking, online financial services, alternative payment solutions or an e-commerce website is a top target for hackers, due to the sensitive and potentially lucrative nature of the financial data transacted through those channels. They are likely to face targeted Man-in-the-Browser (MitB) trojans, viruses, phishing, social engineering, malware, malvertising, Remote Access Trojan (RAT) attacks and zero-day attacks as attackers try to execute fraudulent transactions that can often result in losses amounting to millions of dollars. In 2015 over one million new variants of malware were created specifically aimed at the banking industry representing a 40% rise compared with 2014. Typical losses were $500k per bank and total losses were $500m globally. Throughout 2015 someone had their identity stolen on average every 2 seconds resulting in over $14bn of losses due to financial fraud.

If customers connecting to banking applications are doing so via infected desktops, laptops or smartphones, the malware resident on these machines can spy on all their activity and collect sensitive information, including usernames and passwords. As a result, when customers conduct banking or other financial transactions, the attacker can perform and account takeover and capture critical information, such as physical address information, phone numbers, identity verification information (secret questions/answers) and account balances. In addition, they may also be able to gain complete control over any Internet sessions initiated from that end-user’s device, including Internet banking, online brokerage or other financial account service transactions (loan applications, credit card applications, etc.).

In most cases the victim remains unaware that their account has been compromised until money has been stolen from their account. If the fraudster wants to avoid detection they may choose to transfer a series of small amounts from the victim’s account which may go unnoticed in an age where most accounts are paperless and the only the most vigilant customers regularly check their on-line bank statements.

1 "Mobile malware evolution 2015, Kaspersky Lab"
While financial institutions know they need to add security, they can’t afford to add time or complexity; they need a way to support all the access requirements of their customers, while appropriately balancing the customer needs, costs and security requirements of their business.

**The Solution: How ActivID Threat Detection Service (TDS) Works**

HID Global’s ActivID TDS delivers malware detection transparently, identifying malicious software on an online banking customer’s device and preventing it from stealing information or committing fraudulent transaction activities. ActivID TDS detects common MitB threats (e.g., Zeus or SpyEye), and also targeted attacks.

Instead of relying on blacklists or the explicit knowledge (patterns/signatures) of a few particular trojans, it employs a “whitelist” approach, triggering alerts that an infected computer is attempting to connect to the bank’s systems. TDS also delivers critical data that details how that computer is infected.

Operating in the background, it detects and protects against web session manipulation, cookie hijacking, as well as web-based attacks. Because it is based on common web standards, it works on all browsers and device types, including PC, Mac®, iPad®, iPhone®, Android™ and Kindle™ devices. To take advantage of ActivID TDS, financial institutions, with the ActivID Appliance, only need to include one HTML tag for the webpage they want to protect.

By creating a unique fingerprint of the web page structure on an end-user’s device, the ActivID Appliance can verify the integrity of the device in real-time. It doesn’t matter whether the MitB trojan injects visible content elements, such as personal information:

ActivID TDS uses JavaScript to employ various techniques to detect the presence of malware on any computer or other endpoint, including:

- Patented page fingerprinting techniques to detect any page modification in real-time.
- Tagless device identification to create a unique fingerprint for a device for fraud detection purposes.
- Malware forensics to identify malware present on a device.

Using ActivID TDS, financial institutions can:

- Instantly determine whether they are being targeted by a MitB trojan, including Zeus, SpyEye, Carberp, Silon, Gozi, Torpig and many other known viruses.
- Manage online security threats from many types of web-enabled devices.
- Protect customer data from identity theft and insecure transactions.
- Reduce costs of fraudulent transactions and data breaches.
- Make existing fraud prevention efforts more efficient and effective.
Or, “invisible” content elements, such as malicious JavaScript elements:

ActivID TDS will identify and protect the financial institution and its customers from it.

ActivID TDS uses real-time Trust Analytics to provide advanced fraud prevention, frictionless authentication, and brand and customer protection, by combining device, identity, and behavioural analytics with collaborative feedback from millions of users across tens of thousands of sites. ActivID TDS is proven to achieve:

**Advanced Fraud Prevention**

- Immediately reduce fraud losses by 90% and cut manual reviews by 70%.
- Prevent account takeover attacks, payments fraud, and new account identity fraud with one integrated platform.
• Directly detect bots, proxies, malware, and stolen identities—based on facts, not heuristics.

**Frictionless Authentication**

• Reduces step-up authentication by 50%.

• Provides 100% coverage with passive two-factor authentication, leveraging device, location, identity, and behaviour over time.

• Immediately detects compromised devices and session hijacking attempts.

**Brand and Customer Protection**

• Stops customer records from being accessed, and provides an invisible layer of defense against third-party breaches.

**Conclusion**

The risk levels of financial institutions and their customers are growing exponentially, due to highly motivated attackers who are applying increasingly sophisticated and targeted attack techniques to commit financial fraud. These attacks are compromising legitimate users’ desktops, laptops and mobile devices in a way that circumvents the traditional customer identification mechanisms deployed by financial institutions today, in order to steal information and conduct fraudulent transactions.

Staying ahead of these sophisticated attacks, mitigate institutional risk, and enabling trusted online transactions from any device or browser requires a coordinated, layered approach.

To learn more about how our banking solutions can help provide you with continuous risk-based authentication and increase your protection from costly data breaches, register for our webinar, or visit us online at https://www.hidglobal.com/banking-financial.