SafenSoft

# Securing ATMs, POS Systems and Electronic Voting Machines in the 21st Century

*Transaction Processing Network Security*
*in Unattended Environments*

SafenSoft Corporation
Published: October 1, 2009

## Executive Summary

A rapid convergence of factors is contributing to an urgent call for transaction processing equipment manufacturers to address the overall security of their devices in unattended environments. Networks that used to operate on proprietary hardware platforms and operating systems over dedicated, private networks are rapidly migrating to Intel-based systems running Microsoft® Windows® operating systems communicating over a TCP/IP network, increasing exposure to both known and unknown threats.

Traditional anti-malware is not up to the task of protecting Automated Teller Machines (ATMs), Point-of-Sale (POS) systems, and electronic voting machines, due in large part to the sheer volume of new threats appearing, and the consequent requirement for frequent protection updating. Additionally, targeted attacks are in increasing in sophistication and number, fueled by the recent world economic downturn. Current and pending legislation requires that all possible steps be taken to protect personally-identifiable information and, should there be a data breach, most states require prompt public disclosure.

This paper explores the “perfect storm” created by these factors, and the need to incorporate a proactive data protection solution such as SafenSoft TPSecure into any Windows XP-based transaction processing system. At stake are the legitimacy of local, state, and national elections, the financial stability and brand equity of our corporations, and our confidence in both. Would you take the risk?

# Table of Contents

# What's Driving the Need for a Different Approach?

Quite simply, the need for a new approach to security for unattended transaction-processing systems is driven, regardless of industry, by the expectation on the part of the customer, whether voter, retail purchaser, or ATM user, that their personally-identifiable data will be secured against abuse.

## *The Business Threat is Real*

On Monday, August 17th, 2009, Albert "Segvec" Gonzalez was indicted by a federal grand jury in New Jersey for conspiring to break into the servers of five companies, including Heartland Payment Systems, Hannaford Bros. grocery chain, and 7-Eleven. This followed a previous indictment for breaching the servers at TJX Companies, along with those of six other retailers and two restaurant chains. Gonzalez allegedly worked with two hackers located "in or near Russia" and a third person in Miami. It is believed that this team is responsible for the theft of over 225 million debit and credit card accounts. On September 13th 2009, Gonzalez pled guilty to 20 counts, including identity theft, wire fraud, computer fraud, and conspiracy. At the time of writing, charges remain open for the August 17th indictment.

Cybercrime is real, it is big business, and there is money to be made. *CNNMoney.com* recently reported that, "the number of new Internet security threats rose nearly three-fold last year to 1.7 million." Hackers are using increasingly sophisticated methods to circumvent existing security systems with targeted malware designed to steal sensitive information for financial gain and to further the propagation of viruses to such a degree that no signature-based system could possibly keep up.

Further, according to Information Technology Association of Canada (ITAC) experts, the number of applications designed to steal personal information is likely to increase tenfold in the next several years as criminals take advantage of the global economic downturn, deploying numerous get-rich-quick and cheap refinancing scams to gullible and desperate individuals. Such people have proven easy marks for cybercriminals – unemployed individuals looking for an easy way to get out of the hole.

Utilizing legitimate job boards, hackers are able to assemble a team of "mules" that unwittingly receive and transfer stolen funds for a small fee. Yet others knowingly participate in "cash-out" schemes, withdrawing funds from ATMs using cloned cards with stolen data. At the same time, malware is becoming cheaper to obtain and easier to customize, allowing even non-technical criminals to hack into systems for financial gain and creating a perfect storm of opportunity.

Nor are insiders not immune to the change in economic climate. Disgruntled employees, angry about lay-offs or unable to pay their bills, can take advantage of vulnerabilities in their company's IT infrastructure, corrupting programs and data or stealing proprietary information. The Identity Theft Resource Center (ITRC) indicates that there were 47% more insider-originated security leaks in 2008 than 2007, and four times as many as in 2005.

Many of the reported cyber attacks, on ATMs have taken place in Europe and Russia, which may have created a sense of complacency among US businesses. However, this is shortsighted. In a recent address, President Obama indicated that he believes the potential for cyber attacks is a matter of National Security. He made it clear that the attacks in Europe have been noted, and that we would be naïve to think similar incidents cannot happen here given the interconnected nature of today's global financial systems. Industry analyst firm Gartner suggests that we will see regulation of consumer-oriented information technology (IT) products as early as 2011 in Europe and 2015 in the United States.

The migration from proprietary to open transaction processing systems, while advantageous in several respects (ease of use, cost to deploy, performance, etc.) has created significant potential for vulnerabilities, especially at unattended endpoints, increasing exposure to both known and unknown threats. The frequent updates and system reboots required by traditional malware solutions to deliver ongoing protection are simply not feasible in unattended systems such as ATMs, POS systems, and electronic voting machines. Host intrusion protection systems (HIPS) modify the operating system kernel, making effectiveness dependent on operating system updates, again a challenge for unattended systems; operating system patching is also not a timely solution in an era of burgeoning "zero-day attacks."

High profile incidents like those involving Albert Gonzalez (see previous page), and the exorbitant costs associated with attacks, are penetrating the consciousness of business executives around the world.

### *The Costs are High*

According to the Ponemon Institute's fourth annual *US Cost of a Data Breach Study*, breach incidents cost US businesses on average $6.6 million in 2008 (up from $4.7 million in 2006). This equates to $202 per compromised record, which includes such items as a forensic audit, fines for breach of compliance regulations (FTC, PCI, SOX, etc),claims for fraudulent charges, replacement card costs ($5 - $30 per card), free credit monitoring services for victims, security updates, and legal and public relations consulting costs. Not to mention the cost to the business of potential lawsuits and damage to consumer confidence, corporate reputation, and brand equity. Electronic voting system vendors, in particular, are susceptible to lawsuits at the mere possibility of a fraudulent election due to voting machine tampering, in addition to the loss of state contracts in a highly competitive market.

Forty-four states, as well as the District of Columbia, Puerto Rico and the US Virgin Islands, have enacted data breach disclosure laws. In most cases, businesses that own, lease, or store personally-identifiable information must notify all individuals whose personal data has been compromised. There are some exceptions to current law: for example, if the stolen data was encrypted or there is an ongoing criminal investigation, the business is not required to disclose a breach. One further loophole exists – when card numbers and Personal Identification Numbers (PINs) are stolen, but not the corresponding customer names, reporting of the breach is not mandated by law. But in general, if a business suffers an attack, and personally identifiable data is stolen or abused, that business must disclose the breach. Some state laws also include the possibility of civil damages for each compliance violation (California) or for each state resident not notified of a breach (Alaska). And while data breaches are currently regulated on a state-by-state basis, Congress is considering several bills intended to regulate data breach reporting at the federal level.

## The Challenges

### *ATM Networks*

With the exception of the Citibank ATM heist and the 7-Eleven breach, the majority of documented ATM attacks have thus far occurred in Europe and Russia. Unfortunately, these incidents have not achieved a high level of visibility in North America. But these attacks, alongside the migration of ATM systems to Windows operating systems and the appearance of Zbot/Zeus, indicate a high likelihood of ATM crime here.

The RBS WorldPay theft of an estimated $9 million from ATMs in 49 European cities in a 15-minute window demonstrates the sophistication of today's cybercriminals. Because of the large amount of money withdrawn over a short period of time, it is believed that the hackers gained access through the RBS WorldPay network and were able to modify the withdrawal limits on the accounts.

In March 2009, Diebold disclosed the presence of malware on ATMs in Russia. The Windows-based ATMs were attacked and infected with three trojans designed to capture and print card and password information. While this attack required physical access to the ATMs, rather than a network-level intrusion, the installation of the malware could only have been accomplished by a team of experienced cybercriminals, and, critically, would not have been detected by conventional anti-virus software.

Earlier this year, 20 ATMs in Russia and the Ukraine were infected with malware similar to that used in the Diebold attack. All of the ATMs affected were running under Windows XP. Given the access required to install the malware, it is believed that the attacks were an inside job. Trustwave, which uncovered the attack, collected multiple versions of this malware, in all likelihood proof that it is rapidly-evolving, polymorphic code. It is also likely to spread to a broader population of ATMs and, according to the ATM Malware Analysis Briefing, a proactive approach in prevention and identification will be necessary to prevent future attacks.

Western Europe appears to have received the message. In August 2009, the European Network and Information Security Agency (ENISA) published a report entitled ATM Crime: Overview of the European Situation and Golden Rules on How to Avoid It." The report calls attention to the rising rate of ATM incidents and recommended measures to protect against it. The European ATM Security Team's (EAST) found that "ATM crimes jumped 149% when compared to the previous year." The majority of crimes were based on card skimming techniques. "However, more disturbing are recent reports of attacks that are leveraging readily-available and advanced malware that has affected ATM networks and ATMs themselves."

The agency noted that the number of parties involved in the functioning of ATM networks creates communication issues, particularly where security is concerned. Often it is difficult to determine where ownership for a problem resides. ATM manufacturers must recognize this, and take responsibility for securing their products. ENISA also called attention to the industrial nature of ATM networks, and the resulting security vulnerabilities, specifically that, ATMs "once installed, are rarely updated and poorly managed. Furthermore, as industrial products, patches of the operating system (mainly Microsoft Windows) first have to be tested, licensed and distributed by the manufacturer, introducing an additional obstacle."

Malicious code is often introduced into the banks' information networks through undocumented network connections, wireless networks configured without encryption keys, un-patched operating systems, or laptops, USB drives, and other portable devices. Once launched in a network, the banking trojan Zbot, which steals online banking credentials, is particularly troublesome due to its morphing capability and advanced rootkit mechanisms. A study by Internet security firm Trusteer found that anti-virus products effectively protect against Zbot a mere 23 percent of the time. Clearly, anti-virus software alone is not enough. And Zbot is just one of hundreds of thousands of malicious programs currently in circulation.

> *"With a mass migration well underway in the industry to the more open environment of Windows XP away from proprietary systems, it was considered timely to reinforce defense against evolving software threats, from malware to denial-of-service attacks … We are beginning to see evidence that criminals are trying out ATM software as a possible new frontier of fraud. The goal of this guide is to fend off potential ATM software attackers."* - ATMIA, regarding their reasons for publishing the "ATM Software Security Best Practices Guide" in September2009

ATM fraud is costly. "The US Secret Service estimates that annual losses from ATM fraud totaled about $1 billion or $350,000 a day in 2008." (ENISA, *ATM Crime*) Beyond the associated costs noted above, what should be particularly troubling to financial institutions affected by ATM fraud is the likelihood of customer churn. The Ponemon Institute has estimated that in the case of a breach, a financial institution can expect a churn rate of 5.5 percent. State data breach disclosure laws ensure that, in most cases, the consumer is made aware of such an instance, increasing the likelihood of defection to another institution that has a perceived higher level of trust.

Financial institutions require an ATM security solution that proactively protects against targeted attacks and inappropriate activity, and ensures known good state operation at each point in the ATM network without requiring frequent updates, reboots, or other "hands-on" attention. Such a solution needs to be real-time, always-on, and hands-free, lowering risk, cutting costs for the institution, and increasing consumer confidence.

## Point-of-Sale Systems

As with ATM networks in the financial industry, there has been a significant shift from legacy to Windows-based systems for POS solutions deployed by retailers. In the 2004 VDC Survey of Retail IT Executives, Microsoft Windows operating systems were running 43 percent of all POS systems. By 2008, the IHL Group's *North American Retail POS Terminal Study*, released in March of this year, 76 percent of all new POS terminal shipments were running under Microsoft Windows operating systems, up from 71 percent in 2007. Given that there was an overall decrease of 4.2 percent in POS shipments in 2008, the increase in Windows market share is attributed to the replacement of legacy operating systems by retailers seeking an easy route to Payment Card Industry Data Security Standard (PCI-DSS) compliance.

Much has been written about the need for, and effectiveness of, PCI-DSS and its requirement for all businesses processing debit and credit card payments to protect their systems from "current and evolving malicious software threats." (PCI DSS Requirements and Security Assessment Procedures c1.2, October 2008). The requirements take both the financial and retail industries to task, as evidenced by the rapid migration of systems and software underway in order meet compliance standards, or face the risk of fines by credit card companies for non-compliance, or by federal or state authorities in the case of a data breach. *Requirement 7: Restrict access to cardholder data by business need-to-know* mandates the implementation of access control systems, protecting against accidental or malicious insider activity. And, *Requirement 10*: *Track and monitor all access to network resources and cardholder data* minimizes losses due to insider activities, and requires an audit trail for both users and system components.

> *"Application security is at the heart of the Payment Card Industry (PCI) security standards and requirements. In the last few years, data breaches have resulted in hundreds of millions of data records being compromised. In most of these cases, the firewalls worked, the encryption worked, the logging worked, but the application contained security holes which obviated much of the security. It's like barring the front doors to the bank and leaving a back window open."* - Online security and risk publication CSOonline.com.

However, many other requirements fall short when it comes to protecting consumer interests against the current threats to transaction processing systems. In order to "Maintain a Vulnerability Management Program" *Requirement 5* instructs the retailer to "Use and regularly update anti-virus software or programs …to protect systems from current and evolving malicious software threats." While anti-virus software is certainly a valuable component of any security implementation, the frequent signature updates that would be required to secure a POS system against known viruses, and the lack of protection against unknown and polymorphic malware, render it inadequate as the sole defense against these threats. In addition, *Requirement 6: Develop and maintain secure systems and applications*, falls short of requiring the operating system to be secured, as well as internal and "public-facing web applications." All critical application security patches are to be "installed within one month of release." In today's threat climate, that is one month too long. Proactive, real-time operating system and application protection is required.

Further, while the PCI-DSS Standard goes a long way towards securing personal data in transaction networks, compliance does not necessarily mean security. In the case of the Hannaford Bros. supermarket chain breach, their transaction processing system was compromised, resulting in the theft of 4.2 million credit and debit card numbers, despite the fact that they were PCI-DSS compliant at the time of the breach, which was disclosed in March 2008. The nature of the Hannaford attack was audacious: malware was loaded onto the servers of all 300 stores; the malware then grabbed the credit/debit card data as each card was swiped through the checkout machines; and the data was sent overseas. After an exhaustive investigation of the Hannaford breach, and those at Heartland and 7-Eleven, authorities now believe that the corporate networks of all three companies were infiltrated using SQL (Structured Query Language) injection, allowing for the installation of packet sniffer malware, which captured debit and credit card numbers real-time, and enabled the periodic transmission of the stolen data.

Layered security, which includes a corporate data loss prevention system monitoring and controlling network activities of all users, as well as proactive behavioral analysis of all application activity and maintaining all applications in their last known good state, is critical to the prevention of this type of attack.

### *Electronic Voting Machines*

When it comes to electronic voting machines, the promise is simple: the delivery of a trusted electron result. This means:

- ♦ Voters have access and can vote in a timely fashion;
- ♦ Ballots are kept secret;
- ♦ Personal information is not misused;
- ♦ Votes are not altered.

On July 20, 2007, the University of California, Berkeley, under contract to the California Secretary of State, published its findings as part of a “Top-to-Bottom” review of electronic voting machines certified for use in California. The review involved three prominent manufacturers of electronic voting systems. While all three vendors were certified at the time, none met the 2005 Voluntary Voting Systems Guidelines.

> *“Part of the promise of electronic voting is that technological and procedural safeguards can be combined to conduct elections more securely than ever before.”*
> - University of California, Berkeley

All three of the manufacturers studied (and most others) run their election management systems (EMS) and voting machines on the Windows operating system. Once the election is prepared in the Windows-based EMS at election headquarters, it is typically downloaded onto memory cards which are distributed to the polling stations (one card per voting machine). This memory card records all of the votes during the election. Once the polling station is closed, the votes are tallied, and the cards are removed and shipped to election headquarters where they are placed in the EMS for tabulation.

In the UC Berkeley assessment, the team was able to easily exploit known holes in the operating system on one manufacturer’s system, despite patches being readily available. The study also warned that, once a single memory card becomes infected and is used to boot a voting machine, the virus can then spread back to the EMS and throughout an entire county’s voting system.

The Voluntary Voting System Guidelines (VVSG) 2005 were prepared by the US Election Assistance Commission in order to present States with a set of specifications and requirements to use in their voting system certification processes. Recognizing that the VVSG 2005 did not recommend security measures sufficient to ensure a trustworthy election, the Commission prepared Draft Requirements for the VVSG 2007 which are currently available for public comment. Chapter 5 of the Draft VVSG 2007 mandates that electronic voting systems must:

- Prevent the installation of malicious software on voting machines and election management systems. If installed, malware has the potential to miscount or record votes incorrectly, thereby altering election results. It could also initiate a denial-of-service attack preventing citizens from casting their votes;
- Block viruses with the ability to move from voting machine to voting machine or voting machine to the election management system;
- Protect voter data (ballot secrecy and personal data);
- Limit network access of county workers to those applications necessary to perform their function to prevent insiders from installing malware on the EMS and/or voting machine, or tampering with election results;
- Log all system events for audit.

An effective security solution must employ proactive, hands-free protection to ensure that election management systems are not infected by malware introduced by removable media or direct injection into the network. Potential insider tampering should be prevented through a well-defined, policy-driven access class differentiation system, providing a large number of settings and data access policies to give individual users, or groups of users, specified access to information resources. There must also be a robust built-in reporting system to monitor and log the network activity of all users and provide the necessary audit trails.

## A New Approach

Anti-malware solutions have essentially remained unchanged for the past 20 years. With tens of thousands of new virus samples arriving at labs every day, these traditional solutions are no longer enough. Protection that is dependent on signature updates, operating system and application patching, host intrusion prevention systems, and even application whitelisting are not sufficient to protect transaction processing networks against the growing range and number of threats, both external and internal.

It's time for a new approach: the proactive, automatic defense of all points in the transaction system against external and internal threats, made possible only by the real-time control of system software to ensure that nothing and no one tampers with authorized applications. Safe application operation delivers a network that operates in a continuous known good state, a network that cannot be penetrated by known or unknown malware threats, a network that cannot fall prey to accidental or malicious data loss from inside the organization.

This solution would:

- Protect customer data;
- Ensure the availability of end-point systems;
- Limit financial risks;
- Maintain brand equity and consumer confidence;
- Meet compliance and regulatory requirements;
- Reduce security costs.

SafenSoft TPSecure is this solution.

## *Strong Transaction Processing Security*

Delivering on these benefits is no small task. The threats to transaction processing systems, including their unattended end points, such as ATMs, POS terminals, and voting machines, are numerous. In order deliver strong transaction processing security, a solution will need to protect the entire network against:

- Viruses, worm, trojan horses – malicious programs that corrupt or remove system data;
- Spyware – programs that send data from the network end point to third parties without the operator's knowledge;
- Rootkits – programs that obscure the presence of intruders and malicious code residing on an end point or server;
- Keyloggers – monitoring programs that record and store customers' personal data (e.g. PINs) and other privileged information;
- Any software attempting to secretly install on an endpoint;
- Hacker attacks – denial of service and transaction network data destruction;
- Unauthorized off-site control of the transaction network and/or its components;
- Exploits – system abuse enabled by vulnerabilities in the operating software;
- Accidental and malicious insider activities – installation of malware, and destruction or theft of confidential data.

What's more, it needs to be able to do this without the need for continuous updating, patching, and rebooting to ensure the protection remains current.

# TPSecure: Hands-Free, Real-time Network Security

## *Proactive Protection Technology*

SafenSoft TPSecure is built around **VIPO® -** Valid Inside Permitted Operations – technology. **VIPO** combines adaptive profiling, sandboxing, and a behavior-based rules engine to deliver dynamic, proactive application integrity. Real-time maintenance of safe application operation ensures that transaction processing networks operate in a continuous known good state, and cannot be penetrated by known and unknown malware threats, including "zero-day attacks," from external or internal sources. Because the protection is not dependent on signature updates for effectiveness, hands-on management is not required, creating an ideal solution for unattended systems, such as ATMs, POS terminals, and voting machines. Once installed, and a baseline known good state is established, hands-on administration is not required; the system can block an ongoing attack unattended, as it does not require a system reboot to enable the device to recover and continue operating.

**VIPO** is designed to prevent malware from installing itself in the operating system and to prevent the execution of software that has not been authorized to run on an individual machine or group of machines. Based on system function call interception at the operating system kernel (Ring 0) level, and loaded ahead of all other applications, **VIPO** identifies, analyzes, and, when necessary, blocks access to file system and registry objects, application execution, and other network activities that have the potential to impact application integrity. By operating from the core of the computer outwards, **VIPO** creates a wall around the heart of the machine to prevent the execution of harmful code. It represents a completely different approach to security – one that is extremely well-matched with the needs of today's transaction processing environment.

Preventing the execution of unidentified code attempting to infiltrate the operating system is accomplished by the creation of an isolated environment – or sandbox – in which to safely execute the code without impacting any other part of the computer. In practical terms, this means that malware cannot access the operating system, permitted applications, or the clipboard to install eavesdroppers, keyloggers, or other potentially harmful code. It also means that the code and data associated with other processes cannot be altered, nor can executable files be modified without authorization.

- System scanning and profiling of every application in an operating system;
- Compilation of a trustworthy application list;
- Functioning of the system in strict compliance with all the privilege specifications;
- Prevention of potentially harmful application execution;
- Execution of new applications only with the appropriate authorization.

**VIPO** technology employs stable hashing algorithms and allows authorized users to control file and registry activity, as well as to ensure system file and installed application integrity, and only permits the execution of applications that are known to be trustworthy a priori. No unidentified process can be spawned until the authorized user specifies the level of trust for the application attempting to spawn the process in question. **VIPO** also controls and blocks unidentified executable modules from being launched, which prevents the infection of the system via a security hole in a trusted application. Self-learning optimizes protection for normal working processes and functions.

## *Unique Benefits of TPSecure for Transaction Processing Systems*

- **Easily secures the end point** with remote or local installation (including silent mode option) using Microsoft Installer®. This functionality significantly improves the performance of endpoint (ATM, POS terminal, voting machine) operators.
- **Endpoint licensing and activation** through the Internet.
- **Has the ability to adjust the GUI interface** to fit any screen size, facilitating its use on a wide variety of endpoint terminals.

- **Detects and prevents the launch of malicious software** introduced via removable media.
- **Scheduled system resources access** creates dedicated service periods when endpoints can be serviced, improving security against unauthorized access.
- **File control using wildcards** significantly simplifies system settings (e.g. ability to disallow changing all files to *.doc).
- **User/group access control** is provided through data confidentiality-mode administration with the aid of a well-defined corporate policy-driven access class differentiation system. A large number of settings and data access policies can be implemented with ease, giving individual users, or groups of users, multilevel access to information.
- **Prohibition of access to system resources** for all applications, except those specifically authorized to do so, significantly simplifies system settings.
- **Centrally logs and reports all system events**.
- **Shadow mode monitoring** provides a constant presence of software on a user's workstation. It cannot be detected or removed.*
- **Administrator controls all user actions**, be it online activity, access to online resources, or the volume of transmitted data. All data copy activities are controlled in shadow mode, as are all files copied to removable media.*
- **A forensic camera** provides the capability to view and record users' screens at any time, disclosing accidental and malicious insider activity in both online mode and during retrospective analysis.*
- **A small footprint and low resource utilization** ensures minimal performance hit.

* *These features may be activated/deactivated via a licensing key to comply with local laws and corporate policy.*

## Conclusion

It is not sufficient to rely on one or two security tools to protect transaction processing networks against today's growing threats. A layered approach where firewalls, anti-virus software, host intrusion prevention systems, and operating system patches work in conjunction with real-time software monitoring and control is critical. Proactive behavioral analysis, sandboxing, and adaptive profiling which result in a transaction processing system application running in a known good state is the ideal solution.

Gartner concurs. In their September 2009 "Marketing Research Paper - Pattern Discovery With Security Monitoring and Fraud Detection Technologies" they contend that:

- ♦ Targeted attacks requires broad-scope user activity monitoring and the ability to discern activity patterns that signal exceptions to normal resource access and behavior.
- ♦ Inappropriate use of entitlements by employees requires exception monitoring of user activity patterns in combination with resource and role context.
- ♦ Prevention of fraudulent activities requires a mathematically predictive and/or rule-based alerting approach that monitors users, accounts, transactions and other defined entities for "abnormal" behavior and characteristics.
- ♦ Inappropriate access to and movement of sensitive data requires recognition of sensitive data patterns in combination with access policy context.

For ATM networks, POS systems, and electronic voting systems, SafenSoft TPSecure is this solution.

## About SafenSoft Corporation

SafenSoft is a leading developer of cutting edge information security software solutions, with offices in Moscow, Silicon Valley, and Southern California. Founded in 2006 when the Proactive Computer Security department of StarForce, a leader in the field of digital content copyright protection software, decided to branch out, SafenSoft is today a recognized major player in the market of computer security, with an extensive distribution network in 20 countries. Executive management is drawn from the top echelons of the information security world – Kaspersky Labs, Symantec, McAfee, Trend Micro, AVG, Computer Associates, and more. SafenSoft software solutions are already used by thousands of individual PC owners as well as a number of enterprises associated with the military industrial complex, aircraft and engineering industries, and a growing number of government institutions.

## More Information

For more information about SafenSoft Corporation and TPSecure, contact Jim Leonard at jim.leonard@safensoft.com or call 1-866-846-6779