White Paper

Dissecting Operation High Roller

Dave Marcus, Director of Advanced Research and Threat Intelligence, McAfee
Ryan Sherstobitoff, Threat Researcher, Guardian Analytics

How the high-tech mantra of "automation and innovation" helps a multi-tiered global fraud ring target high net worth businesses and individuals. Building on established Zeus and SpyEye tactics, this ring adds many breakthroughs: bypasses for physical multi-factor authentication, automated mule account databases, server-based fraudulent transactions, and attempted transfers to mule business accounts as high as €100,000 ($130,000 USD). Where Europe has been the primary target for this and other financial fraud rings in the past, our research found the thefts spreading outside Europe, including the United States and Colombia.

Table of Contents

Executive Summary

McAfee and Guardian Analytics have uncovered a highly sophisticated, global financial services fraud campaign that has reached the American banking system. As this research study goes to press, we are working actively with international law enforcement organizations to shut down these attacks.

Unlike standard SpyEye and Zeus attacks that typically feature live (manual) interventions, we have discovered at least a dozen groups now using server-side components and heavy automation. The fraudsters' objective in these attacks is to siphon large amounts from high balance accounts, hence the name chosen for this research: Operation High Roller.

With no human participation required, each attack moves quickly and scales neatly. This operation combines an insider level of understanding of banking transaction systems with both custom and off the shelf malicious code and appears to be worthy of the term "organized crime."

This study found 60 servers processing thousands of attempted thefts from high-value commercial accounts and some high net worth individuals. As the attack shifted emphasis from consumers to businesses, mule business accounts allowed attempted transfers averaging in the thousands of Euros, with some transfers as high as €100,000 (US$130,000)[1]. Three distinct attack strategies have emerged as the targets have expanded from the European Union, to Latin America, to the United States.

Debunking the popular wisdom that only big banks are affected, the research documents attacks at every class of financial institution: credit union, large global bank, and regional bank. So far, we estimate the criminals have attempted at least €60 million (US$78 million) in fraudulent transfers from accounts at 60 or more financial institutions (FIs). If all of the attempted fraud campaigns were as successful as the Netherlands example we describe in this report, the total attempted fraud could be as high as €2 billion.[2]

Glossary

GIRO
A standard form of payment in Europe where funds are pushed from the payer to the payee. The United States uses a similar transaction model for direct deposits called the Automated Clearing House.

IBAN
A standard for identifying bank accounts across national borders.

Fraudulent Transaction Server
A server that interacts with the FI's banking portal to process the actual transaction (including account login).

Web Inject
An attack where extra HTML code and JavaScript are inserted within a browser window. This code can display text or images or add fields to a form, enabling collection of required authentication information.

Zeus/SpyEye
Toolkits that can install malware payloads to control a computer and its applications. The toolkits often deliver web injects to alter browser-based forms and collect password, login, and other account information for transmission to an attacker.

A Timeline in Case Studies

Our research included discovery and analysis of multiple attacks. Below is a sequence of specific examples we investigated in detail, followed by a discussion of the innovation and automation inside the attack. We continue with step-by-step descriptions of the three types of attack strategies we uncovered.

An Automated Attack In Italy

The first series of attacks our researchers found affected a popular bank in Italy and its consumer and business accounts. The attack used SpyEye and Zeus malware to transfer funds to a personal mule account or pre-paid debit card where the thief could retrieve the funds quickly and anonymously.

While at first consistent with other client-based attacks we have seen, this attack showed more automation. Instead of collecting the data and performing the transaction manually on another computer, this attack injected a hidden iFRAME tag and took over the victim's account—initiating the transaction locally without an attacker's active participation.

In this Italian instance, the code used by the malware looked for the victim's highest value account, looked at the balance, and transferred either a fixed percentage (defined on a per campaign basis, such as 3 percent) or a relatively small, fixed €500 amount to a prepaid debit card or bank account.

Some of the consumers targeted were what we call "high rollers," with an average of €250,000 to €500,000 in their accounts. Some transfers were domestic, and some crossed international boundaries via an IBAN transfer.

This fraud showed one other important innovation. Where transactions required physical authentication (see sidebar on page 8) in the form of a smartcard reader (common in Europe), the system was able to capture and process the necessary extra information, representing the first known case of fraud being able to bypass this form of two-factor authentication.

Within 60 seconds, a script navigated to the GIRO transfer page, retrieved mule account information from a remote database, and initiated a transfer. No human interventions, no delays, no data entry errors.

The Expanding Footprint

Once we knew the attack patterns to look for, we found evidence of other attacks at other European and Latin American banks. These attacks built on the code found in Italy, adapted for each specific bank. For the first time, we knew this fraud was global in nature, and we suspected that other regions might be affected. Our suspicions were confirmed when we subsequently found evidence of active campaigns in Colombia and the United States.

The following European examples provide a useful bracket of smaller and larger total attempted fraud campaigns. With 60 servers found, we estimate the potential overall range of attempted theft based on these brackets to be between €60 million and €2 billion.

Campaign Appears in Germany

In late January 2012, we discovered a replication of the Italy attack in Germany. The victim log data on the server showed that the fraudsters compromised 176 accounts and attempted to transfer nearly one million Euros to mule accounts in Portugal, Greece, and the United Kingdom. The average account balance was close to €50,000, showing a focus on high net worth targets. Although the average transaction had risen to about €5500, international transactions had even larger amounts, ranging from €27,563 to well over €50,000 in a single IBAN transfer.

Total sum of all compromised account balances	€8,339,981
Total sum of all transactions initiated to mules	€962,335
Average balance of victimized accounts	€47,924
Average transaction amount initiated to mule	€5,499

Fraudsters Hit Netherlands Banking Hard

In March 2012, the fraudsters turned their attention to the Netherlands banking system and enhanced their approach to include a payload containing a server-side automated attack. By performing the fraudulent transfer on the server side, the criminals found they could circumvent endpoint security tools and stymie monitoring tools used by fraud detection teams at the financial institution. The server performing these transactions was based in San Jose, California.

This campaign compromised more than 5,000 primarily business accounts in two banks in the Netherlands. From the victim logs retrieved and analyzed from the transaction server, the total attempted fraud was estimated at €35,580,000. The shift from consumer to business targets allows the fraudsters to transfer larger sums without bumping up against thresholds or money laundering limits (in the United States, for example, they would be limited to $10,000 for consumer accounts) or raising red flags. Higher value wire transfers, including large commercial transfers, are common for businesses, and the volume of activity and nature of these transactions allow the fraudulent transactions to go unnoticed. Often, the transfers are sent to international destinations to reduce the chance of detection or legal action. International transfers offer two advantages. First, they make detection and recovery on the receiving end less likely. Second, they make pursuit more difficult since regulations, tracking, and law enforcement efforts vary greatly by country.

Total sum of all compromised account balances	€141,303,005
Total sum of all transactions initiated to mules	€35,580,000
Average balance of victimized accounts	€28,171
Average transaction amount initiated to mule	€2,500

Expansion to Latin America

As campaigns were rolling out across Europe, the fraudsters also expanded to Latin America. On March 3, 2012, we discovered an attack that targeted more than a dozen businesses in Colombia (see Figure 1). All of them banked with the same bank, and each had an account balance between US$500,000 and close to US$2,000,000.

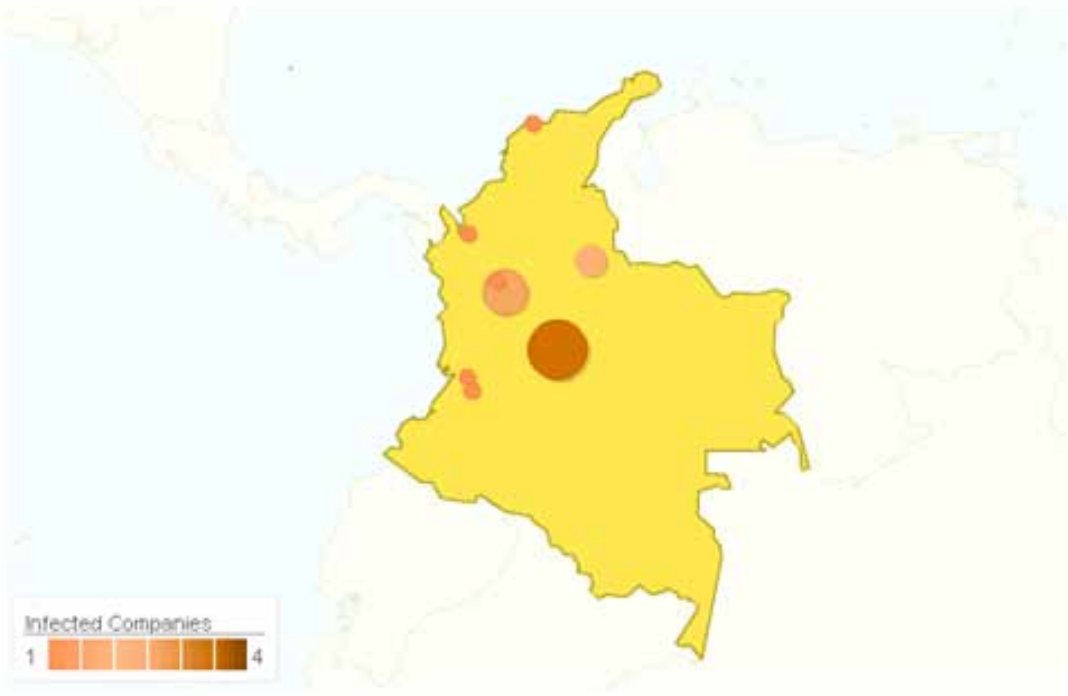

Figure 1. The attacks were concentrated in Bogota, Colombia.

The fraudulent transaction server controlling this campaign was hosted in Brea, California. Although most of the attacks were automated by this server, we found evidence of the fraudster logging in from Moscow, Russia, to manipulate some of the transactions in an attempt to transfer arbitrary amounts as high as 50–80 percent of the victim's balance (see "Strategy 3" in the examples below).

Fraudsters in the Netherlands Also Active in the United States

Also in March 2012, we discovered that the San Jose-based fraudulent transaction server used in the Netherlands attacks was being used to target banks in the United States. This server used client- and server-side components to launch automated attacks against US financial institutions by initiating wire transactions from special purpose commercial and investment accounts, ones that typically hold assets valued at tens of millions of dollars. This first evidence of attacks on North American financial institutions affected 109 companies. Evidence in the United States indicates there are eight to ten malware variations exclusively targeting American businesses, using commercial transactions to fund mule accounts.

One innovation seen in a US attack involved the automated transfer of funds from the victim's corporate savings to the victim's corporate checking account, after which it would be normal (within standard business practices) for the funds then to be transferred to an external account. In this case, the transfer went to a business account controlled by a mule in another country.

US Attack Unfolds in 60 Days

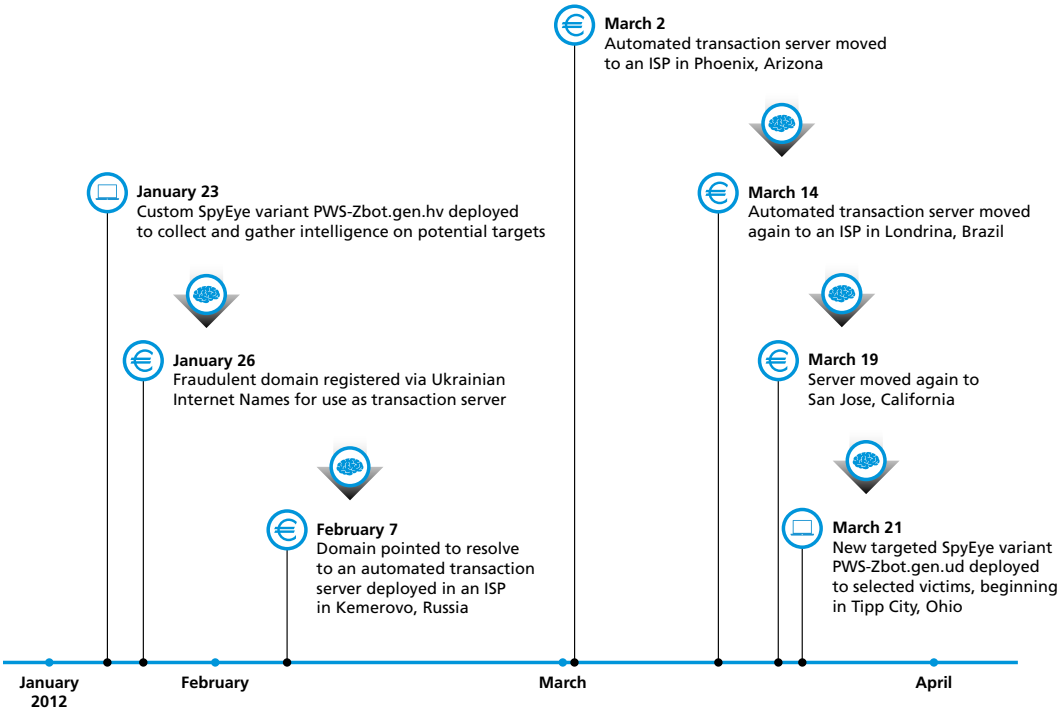

Figure 2. Our research uncovered the globe-hopping activities of one US attack. Once the server reached San Jose, California, it became part of campaigns in the Netherlands and the United States.

What's Two-factor Authentication?

As fraudsters innovate, financial institutions enhance authentication to online banking applications. Use of any two of the below categories qualifies as two-factor authentication.

Something You Know

- Password
- 4-digit Personal Identification Number (PIN)
- Transaction Authentication Number (TAN) (provided by a FI, either in a list or generated on the fly and sent via SMS or a separate session on the client computer)

Something You Have

- One-time password generated from a physical token or a software token installed on the account holder's device
- Digital token generated by a pair of physical devices, such as a smartcard and a smartcard reader—a solution commonly used in Europe but deemed too cumbersome by US financial institutions

Something You Are

- Biometric thumb reader
- Iris scanner

What's New? The Automated Bypass of Physical Chip, Reader, and PIN

The malware discovered within Operation High Roller is the first to work around the "smartcard/physical reader + PIN" combination. Normally, the victim inserts a smartcard into its reader device and enters a PIN into the device. The bank's system generates a digital token based on the data contained on the physical smartcard, authorizing a transaction.

The malware defeats this authentication by generating an authentic simulation of this process during login to capture the token. To allay suspicion, the script collects the token as the user logs in, rather than during the transfer authorization process. It then uses the digital token to validate the transaction later in the online banking session while the user is stalled with a "Please Wait" message.

New Heights In Heists: What's New Compared To SpyEye and Zeus?

Because the attacks build on SpyEye and Zeus, Operation High Roller has a familiar core of web injects code (altering what an account user sees in the browser session) and information theft (extraction of money from an account), as well as transaction hiding add-ons.[3] However, the fraudsters have gone far beyond these basics.

Extensive Automation

Most Zeus/SpyEye attacks rely on manual components and active participation by the fraudster. They use social engineering and a remote manipulation to compromise each host system and online bank account. They plant malware and execute a Man-in-the-Browser attack to skim credentials and form data, then go on to process a fraudulent transfer from the victim's machine.

In contrast, although there can be live intervention in the most high-value transactions, most of the High Roller process is completely automated, allowing repeated thefts once the system has been launched at a given bank or for a given Internet banking platform. For example, before it does the transfer, the code looks up account information from an "active mule account" database so that the "drop" information is always current. The automation extends to include several of the other features mentioned below, in particular the bypass of two-factor physical authentication.

Server-side Automation

The attack also has adopted sophisticated server-side automation to conceal the actual methodology as to how the system interacts with the victim's online banking platform to create the fraudulent transaction. Unlike the initial malware discovered in Europe, the updated attacks found in the Netherlands and the United States move fraudulent transaction processing from the client to the server. Fraudulent activities—including the actual account login—are performed from a fraudster's server that is located at a "bullet proof" ISP (one with crime-friendly usage policies), locked down against changes, and moved frequently to avoid discovery. After each move, the web injects are updated to link to the new location.

Rich targets

The United States victims were all companies with commercial accounts with a minimum balance of several million dollars. Typically, victims are found through online reconnaissance and spear phishing (see Figure 3), although some attacks target existing infected hosts.

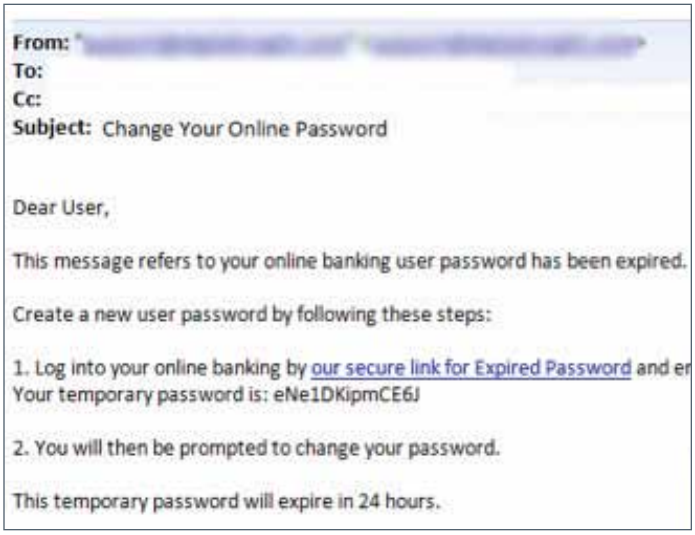

Figure 3. An example of a spear phishing email. The disguised link takes the user to a malicious site where the infection sequence begins.

In cases where hosts are already infected with malware, the fraudsters profile the host using SpyEye or Zeus to gather intelligence—such as the Internet banking platform used and other account specific data—that can be used to craft a custom attack. Fraudsters load malware that contains a customized payload into these infected hosts, perpetrating the attack and allowing the botnet managers to monetize further their existing botnets.

Automated Bypass of Two-Factor Physical Authentication

All of the instances that involved High Roller malware could bypass complex multi-stage authentication. Unlike recent attacks that collect simple form authentication data—a security challenge question, a one-time token, or PIN—this attack can get past the extensive physical ("something you have") authentication required by swiping a card in a reader and typing the input into a field (see Two-factor Authentication sidebar).

The attack asks the victim to supply the information required to get around the physical controls of smartcard reader plus pin pad entry to generate a one-time password (or digital token).

One difference from other publicly discussed attacks is the complex process that the fraudsters use to defeat the physical two-factor system. In the typical GIRO transfer, there are two steps: an account login and later, the authorization of the outbound payment. In the High Roller scheme, an extensive JavaScript uses web injects to alter the login experience to collect all the information the fraudsters need for both steps within the login step. Since the physical authentication information is gleaned during the login, outside the context of a transaction, the victim is less likely to be suspicious—they just think the login experience has been upgraded.

Having collected all the information it requires for the entire transfer, the malware stalls the user and executes its transaction in the background using the legitimate digital token. Fraudsters can replicate this automated process across accounts and reuse it in multiple accounts on the same banking platform, so it scales.

The defeat of two-factor authentication that uses physical devices is a significant breakthrough for the fraudsters. Financial institutions must take this innovation seriously, especially considering that the technique used can be expanded for other forms of physical security devices.

Techniques Against Standard Security Software

Extensive customizations secure the code and the attack infrastructure. Rootkits help the client-side malware burrow deep into the system to avoid detection by antivirus scans. In addition, the actual binaries (the payloads tailored for each bank and injected into the browser) have very limited distribution to a small number of victims. Once our researchers began tracking the binaries using the McAfee® Global Threat Intelligence™ database, the relatively small population of infected systems (such as the 5016 accounts compromised in the Netherlands) confirmed that fraudsters wanted the attack to stay under the radar of detection systems.

The links and code are obfuscated—encoded, packed, and encrypted—within the web injection to prevent detection and hinder inspection. And some of the web servers move dynamically so that blacklisting and reputation-centric technologies are not effective. For example, the server side components (both the command and control servers and the fraudulent transaction servers) are hidden to avoid classification by reputation-based systems. This allows servers to remain online for longer periods.

Inside the Analysis

This scheme is not a typical use of Zeus and SpyEye, which made it particularly difficult to detect. Our investigations succeeded because the fraudsters made one huge mistake: they failed to properly secure the directory structure that contained victim logs, transfer data, and mule information. This data provided a virtual map to their operation.

After reviewing the log information, we found critical forensic intelligence, such as the code version, code date, and affected victims.

During our research, we identified 426 unknown SpyEye and Zeus variants.

- 4 unique SpyEye binaries contained passive transaction poisoning
- 16 unique binaries contained the JavaScript code
- 44 unique binaries contained evidence of EU style JavaScript code

Techniques to Avoid Fraud Detection

The fraudsters clearly know the banking industry. They carefully navigate around the thresholds and regulatory triggers of bank fraud detection processes. For example, automated transactions are set to check the balance and not to exceed a fixed percentage of the account value nor (in most cases) perform more than one transfer per account. The attack algorithm will also simulate page navigation and vary the timing in each transaction to appear as a natural human interaction. Further, the web injections attempt to mimic the typical use cases of a banking customer. The content inserted will look different according to what the customer is doing: considering a login, viewing an account summary, or initiating a transaction.

Techniques to Hide Evidence

Multiple after-the-theft behaviors hide evidence of the transaction from the user. For example, the client-side malware kills the links to printable statements. It also searches for and erases confirmation emails and email copies of the statement. Finally, it also changes the transactions, transaction values, and account balance in the statement displayed on the victim's screen so the amounts are what the account holder expects to see. While these tactics are not new, their use together with the other tactics shows a high level of expertise.

Three Attack Strategies

The underlying technologies of the attack have evolved as the target has shifted from the individual high net worth consumers initially defrauded in Europe to the high net worth businesses victimized in Latin America and the United States.

Strategy 1: Automated Consumer Attacks

Initially, the infection pattern seen in Europe was similar to other SpyEye and Zeus fraud activities, but performed hands-free, automated transactions.

This is the standard flow:

- A Phishing email is sent to individuals or businesses that bank with a specific financial institution
- The email contains a disguised link. When the victim clicks the link, they visit a web page that starts a malicious sequence:
  - The page contains a blackhole exploit kit or other similar framework. The kit will look for an appropriate vulnerability in the victim's browser, and upon finding one, will load exploit scripts that compromise the victim's computer.
  - The exploit script installs a Downloader Trojan.
  - The Downloader Trojan then will install SpyEye or Zeus on the victim's device.
  - The next time the victim logs into online banking, the malware will check certain parameters, such as the type of accounts and account balances. If the client parameters are what the malware is seeking, the SpyEye/Zeus Trojan contacts the command and control server and pulls down the appropriate web inject for the victim's financial institution. The web inject carries a JavaScript payload.
- The fraud process starts when the account holder subsequently attempts to log into his account from the infected computer
- The victim sees his standard, genuine bank portal, but it displays the fraudsters' custom JavaScript web injection to capture the information needed for the victim's bank
- The injected script takes control of the session and contacts the fraudsters' server for specific instructions. It may insert content within the session, such as a transaction field or error message. For example, as the victim logs in, he may be asked to answer a security question and get an error. The error message creates the delay that allows the fraudster's software to perform the transaction.
- At this point the victim has not actually authenticated and typically is stalled with a "please wait" message for about 60 seconds (see Figure 4).

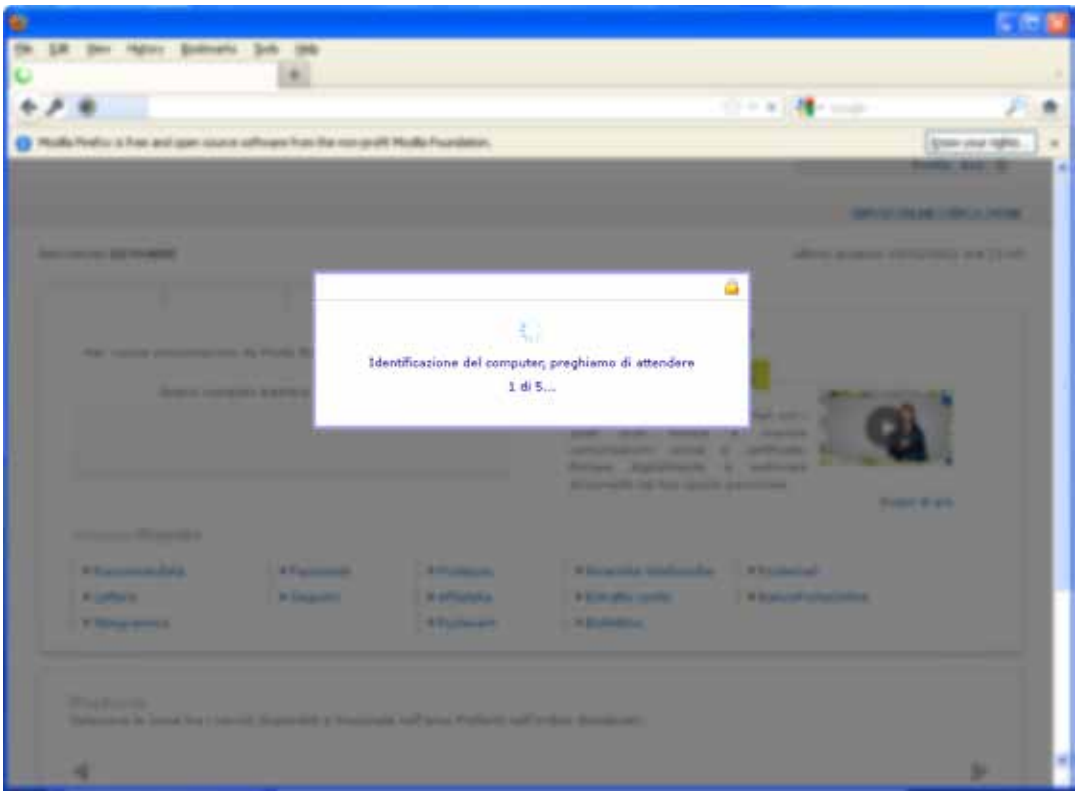

Figure 4. When a consumer logs into their account, they might see a fake "please wait" screen.

- If during the automated attack, the financial institution requests a transaction authorization number (TAN), the fraudsters' client-side web injection displays a fake TAN page to the victim and the malware proceeds as follows:
  - The malware collects the TAN from the victim's screen and presents the authentic TAN to the financial institution to enable the fraudulent transaction, while delaying the victim from accessing their account.
  - The malware uses the intercepted credentials to initiate a silent, separate transaction to a mule account (either individual or business) or in one case, a prepaid debit card.
  - The malware looks up a valid mule account from a separate database, automating a traditionally manual step in the process. The transaction is performed in a hidden iFrame, a parallel instance of the online banking session on the client that operates in the background. The code navigates to the transaction page and initiates an automated form submission that adds the mule information.
- The user is allowed to proceed with the session
- The mule withdraws the money and converts it to a Western Union or Liberty Reserve payment that he remits to the fraudster. The mule retains a small percentage of the take, and the money is untraceable within a few days.
- To conceal the theft, the malware will stay resident in memory on the victim's computer. It will alter the victim's bank statement to show a false balance, remove line items associated with the transaction, and block printing of statements that would show the true account balance and transaction sequences.

Strategy 2: Automated Server-based Attacks

The second type of attack moves the fraud logic to the server side to reduce the visibility of the fraudster's logic. Some of the US attacks work through specific Internet banking platforms, so they can launch automated attacks against any size financial institution. The fraudsters invest time identifying which financial institutions use a particular Internet banking platform and finding clients of that FI. The malware automates subsequent fraudulent transfers leveraging server-side web injections.

This is the standard flow:

- The infection and compromise of the client occurs as in Strategy 1. Custom web injects are downloaded with the malware.
- Where Strategy 1 allows the victim to move ahead in 60 seconds and perform the intended transaction, in this version the business user is typically given a "system under maintenance" or "please wait" message (see Figure 5) and is locked out for a longer period. For example, the victim might be told to try back in 12 hours or as much as two days, permitting the fraudster to complete the transfer without the victim noticing anything unusual.
- In this attack, the fraudulent transaction is performed from a server, not from the victim's computer. The server logs onto the FI's online banking portal and performs the transaction—the victim doesn't actually authenticate.
- Once the transaction has been completed, the "system under maintenance" message will no longer appear. The victim is allowed to authenticate and will have to reenter his login data.
- As before, the funds are moved to a mule account where they will be extracted within a few hours of the funds becoming available. The complete process may take 1–3 days.

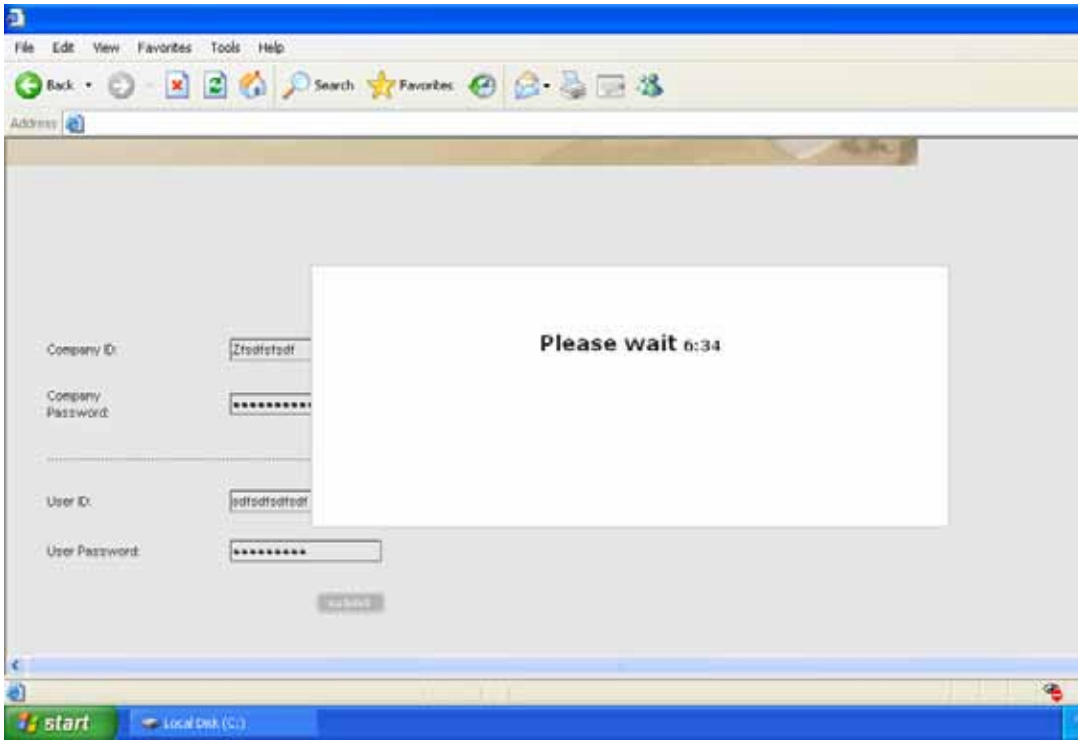

Figure 5. In business scams, users are asked to wait much longer, in this case more than 6 hours, to allow the transfer to be completed without the user noticing an unexpected change in the balance.

In addition, we observed a scheme known as "transaction poisoning" that targeted a well-known online escrow company. Rather than initiating new wire transactions on behalf of infected victims, the scheme would silently modify transactions initiated by the legitimate account holder. The original transactions were intended to go from a North American account to a recipient in the United Kingdom to fund an escrow account for auctioned vehicles. Instead, the funds were diverted to a mule account (see Figures 6 & 7).

This attack used a remote script that injected the necessary information behind the legitimate data, so the fraudulent transfer was invisible to the account holder. The script altered the following fields:

1. Bank Name
2. Sort Code
3. Swift Code
4. IBAN code
5. Account Number
6. Beneficiary Address

This method allows the fraudsters to bypass bank controls that use "call backs" to verify transactions. If the call back confirmed only the amount but not the recipient, then the hijacked transaction would go through.

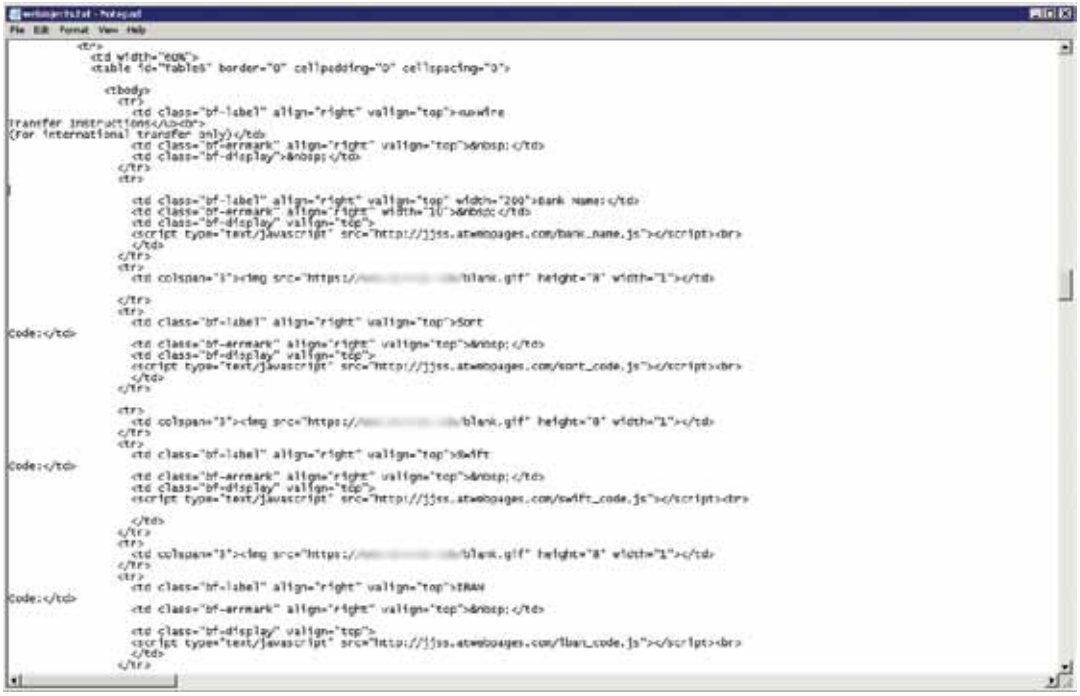

Figure 6. SpyEye web injects to insert mule address information for a mule drop point in the UK.

Figure 7. The mule's address information being injected.

Strategy 3: Hybrid Automated/Manual Attacks Against Marquee Business Accounts

For elite victims, specifically high-value business accounts and boutique banks that service high net worth individuals, our research found that the fraudsters sometimes participate more actively in a semi-manual parallel session. The fraudsters use this parallel session to work around extra security controls, such as bank-specific technology, systems, or policies. This strategy also allows an override of the fraudster's self-imposed restrictions so the attackers can steal custom amounts from each account.

This is the standard flow:

- The victim's computer is compromised as in previous examples
- The fraudsters monitor events across potential victims
- When the user attempts to log in, the malware alerts the fraudster to take over the session (the client sends a Jabber, instant message, or SMS notification to the fraudster)
- The client-side malware prevents the user from authenticating while the fraudsters field the security questions and process transactions in the background
- As the fraudsters need additional information, they can inject requests into the victim's session
- Fraudsters can manually adjust the transaction amount at this point if they want to attempt to steal more than the fixed amount or fixed percentage of the account balance that's programmed into the malware
- The server will process the fraudulent transfer, then present the "system under maintenance" message as described in Strategy 2, stalling the victim while the money is processed and extracted from the mule account
- In some cases, the fraudsters may want to perpetrate more than one theft on a given business. They could make a change to the client web inject script to point to a different server and thus avoid detection by blacklisting software. They also could redirect victims to a new server or upgrade the script with new functionality. Through these interventions, the attacks can continue.

Recovery and Remediation Efforts

In March 2012, as the scope of the fraud became clear, the team began working actively with law enforcement to report the location of criminally-controlled servers found in the United States and to educate others on the attack.

We are working to assess and improve the defenses at McAfee and Guardian Analytics financial services customers. This attack should not be successful where companies have layered controls and detection software correctly. We are working to map out appropriate security configurations, such as activation of real-time threat intelligence on client hosts and use of hardware-assisted security to defeat evasive malware.

The success of Operation High Roller behooves financial institutions, consumers, and corporations to reexamine their security controls and assumptions.

- Many regional banks and credit unions lack anomaly detection software, so they are completely exposed to this attack
- Enterprises must boost both security controls and privileged user education against the social engineering and phishing attacks
- Consumers, while not the primary targets, should strengthen and maintain endpoint controls and remain alert to unexpected changes when performing online banking transactions

Fundamentally, security software—whether designed to audit access, detect anomalies, or disconnect attackers—must be layered around assets in reinforcing systems. Since attacks like Operation High Roller use multiple tactics and extensive automation, multiple diverse protections must be deployed to detect and disrupt the different aspects of each attack. No single tool is a panacea. More than one layer is required for effective risk mitigation, and automated defenses offer the primary way to keep pace with automated attacks.

For example, many banks consider server takedowns and blacklisting systems to be effective buffers against these types of risks. But our analysis shows that some of these server-side systems will move dynamically and outwit the inevitable lag of blacklisting technologies. Also, the advances we witnessed in security features—including bypassing physical authentication and encoding and obfuscating links—show that the fraudsters remain on the cutting edge of malware development.

Lessons Learned

While larger financial institutions have well-resourced fraud detection departments, resources are no guarantee of safety. Our research found attacks succeeding in the most respected financial institutions, as well as the small, specialized credit unions and regional banks that may have felt they presented too paltry a target. Through the leverage and efficiencies of Internet banking platforms, these attackers can defraud banks of any size.

Financial institutions should anticipate more automation, obfuscation, and increasingly creative forms of fraud. Botmasters will likely upgrade and exploit the population of existing Zeus/SpyEye infected machines to use more automation. Further, different payment models will be targeted: Automated Clearing House (ACH) payments, remittance payments, and more. As this report shows with the evolution from client-side to server-side attacks, fraudsters will evolve their model to move a majority of the fraud logic to the server. This practice makes it much more difficult for security leaders to develop prevention strategies.

However, there are fraud prevention solutions that have been proven to work, even against the highly sophisticated and automated attacks documented here. Due to the uniqueness of each and every account holder, fraudsters will still do something different, something unexpected when compared to legitimate behavior. Anomaly detection solutions have been proven to detect the widest array of fraud attacks, including manual and automated schemes, and including both well-known and newly emerging techniques. Anomaly detection solutions monitor all online and mobile banking activity of each account holder from login to logout, and compares it to established legitimate patterns. The Federal Financial Institutions Examination Council (FFIEC) reinforced the effectiveness of anomaly detection in preventing banking fraud when it included it in their 2011 Guidance Supplement as a minimum expectation for a layered security solution.

Our researchers concluded that the fraudsters bank on a slow and disjointed "white hat" detection system. However, the model used to dissect and track Operation High Roller shows the impact of industry cooperation against fraud. Guardian Analytics and McAfee contributed different technical and data resources to the investigation, drawing on complementary perspectives, customer bases, and skillsets.

Through partnerships like this, the research community can do a better job of following the money to the root of an attack. The industry should be able to quickly answer questions such as:

- Where is the transaction going?
- Where is the transaction server?
- How should we engage with law enforcement?
- How can we get breaking threat intelligence to targeted brands (including industry software vendors)?
- How can we more quickly profile an attack's complex behavior and map out its ecosystem?

Today, some security researchers still simply watch for malicious binaries like SpyEye. Some devote their lives to behavioral analysis and detections of polymorphic malware. However, malware is only part of the problem. We need to work to strike down the system in each phase of its activity. McAfee already invests in the areas below, but our researchers and the rest of the security community must push farther, faster:

- Phishing—Filter out suspicious emails and malicious senders
- Web servers—Find and kill the web servers (where the automatic transfers are processed) in minutes, not months
- Network—Categorize behavioral information from a network flow aspect as well as protocols and patterns in the communications to the servers (not just binaries)
- Endpoint—Assess behavior of code earlier in the boot process to identify rootkits and memory manipulation, detect and close browser and software vulnerabilities that provide the entry points for attackers , and enforce application whitelists to reduce the attack surface

We can do this. The machinery exists. For example, with McAfee Global Threat Intelligence, sensors gather billions of data points in the cloud. Our systems assign reputations to malicious sites already. This machinery can also work to identify compromised transaction servers and block access. This is a new application of reputation-based blocking.

The intelligence gathered from Operation High Roller has helped to shed light on the strategies and scope of financial crime innovation. We encourage other security vendors and the global banking industry to take action against this ballooning fraud ring and similar future attacks by improving detection and information sharing. Hopefully, this report also will spur more sensitivity and vigilance by the high-value businesses and consumers whose accounts are being plundered.

Appendix

The following heat maps show where the fraudster activities have occurred around the globe. We have seen high concentrations of malicious servers in Eastern Europe, as well as strategic placement in other countries. The victim map of the United States attack shows a much larger attack footprint than we might have expected based on the lack of similar attacks discussed prior to this report.

Figure 8. Hosting locations of the servers performing the fraudulent transactions.

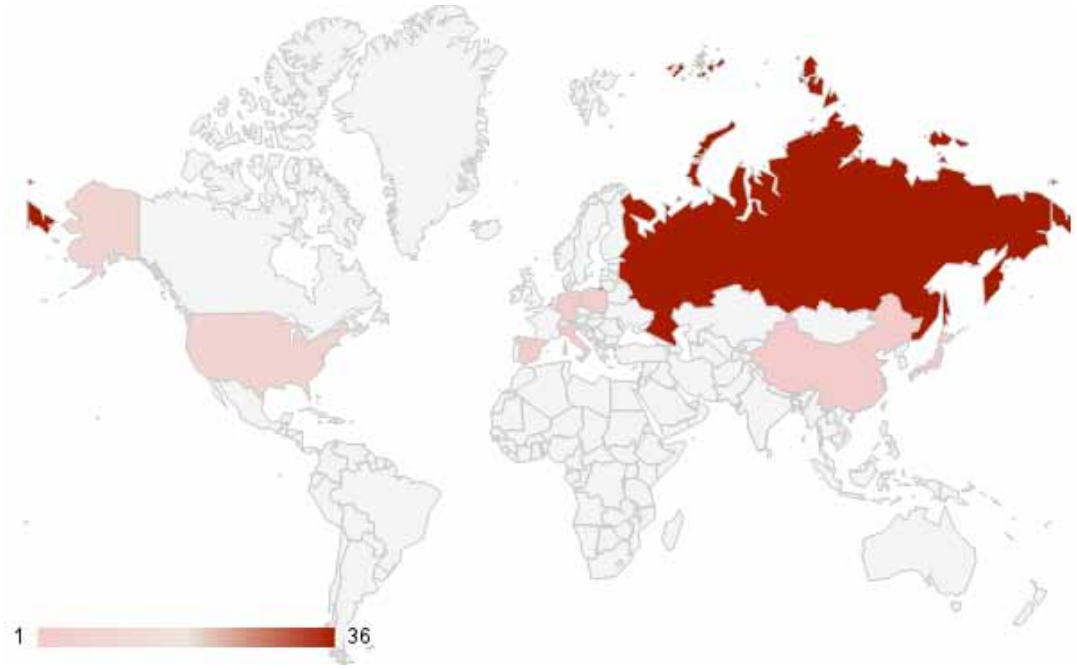

Figure 9. The distribution of command and control servers used in server-side automated attacks against the US banking system (analysis across 16 variants).

Figure 10. The distribution of command and control servers used in server-side automated attacks against the European banking system (analysis across 44 variants).

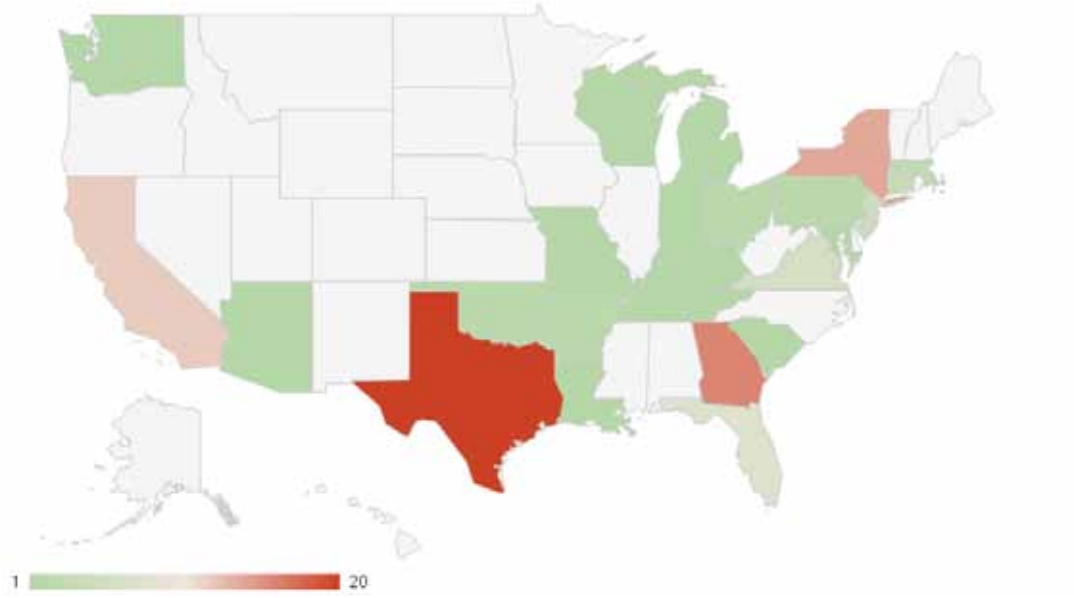

Figure 11. Locations of victim companies in the US tracked during an active campaign.

About the Authors

Dave Marcus is Director of Advanced Research and Threat Intelligence for McAfee Labs™. His focus includes open source and social media intelligence, SCADA and ICS systems, and research into using silicon-assisted technologies for threat detection. His media and thought leadership responsibilities include social media technology engagement and research. In his spare time, he collects guitars, is an avid power lifter, and is a founding keyholder of Unallocated Space, a Maryland Hackerspace. He also enjoys practicing the art of lockpicking and is a hacker of things.

Ryan Sherstobitoff is a Guardian Analytics Threat Researcher. Formerly, he was Chief Security Strategist at Panda Security, where he managed the US strategic response for new and emerging threats. Ryan is widely recognized as a security and cloud computing expert.

About McAfee

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ:INTC), is the world's largest dedicated security technology company. McAfee delivers proactive and proven solutions and services that help secure systems, networks, and mobile devices around the world, allowing users to safely connect to the Internet, browse, and shop the web more securely. Backed by its unrivaled global threat intelligence, McAfee creates innovative products that empower home users, businesses, the public sector, and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. McAfee is relentlessly focused on constantly finding new ways to keep our customers safe. www.mcafee.com

About Guardian Analytics

Guardian Analytics was founded and is completely focused on fraud protection for financial services institutions. We're proud to serve banks and credit unions that are taking a proactive step to lead the way in fraud prevention. Our customers take the promise of security very seriously—as an essential element of their brand, reputation and their commitment to protect their institution and their account holders from fraud attacks. Our behavior-based anomaly detection solution, FraudMAP, was developed by leveraging our employees' direct experience and deep expertise in electronic banking fraud prevention—including solving actual fraud cases—built up over many years with extensive investment in intellectual property. www.guardiananalytics.com

[1] Our report uses a €1.0=$1.30 exchange rate.

[2] We have investigated 60 server logs, representing at least 60 different banks. Research included in this study provides the low end and high end of the numbers we use for the total estimate of the attempted fraud. The logs show the amounts pushed to the mule accounts. We do not have visibility into the final total of attempts that succeeded.

[3] See http://threatpost.com/en_us/blogs/ramnit-worm-evolves-financial-malware-082311 and http://www.trusteer.com/blog/gift-wrapped-attacks-concealed-online-banking-fraud-during-2011-holiday-season

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

46903wp_high-roller_0612