

## The Irretrievable Losses of Malware-Enabled ACH and Wire Fraud

Rodney Joffe  
SVP and Sr. Technologist  
Neustar, Inc.  
46000 Center Oak Plaza  
Sterling, VA 20166  
480-804-8250

November 1, 2009

The information contained in this document represents the current view of Neustar, Inc. on the issues discussed as of the date of publication. Because the technologies discussed are subject to rapid change, Neustar cannot guarantee the accuracy, comprehensiveness, or sufficiency of any information presented.

This White Paper is for informational purposes only. NEUSTAR MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT AND CANNOT BE HELD LIABLE FOR ANY RELIANCE ON SUCH INFORMATION

## **You are ALREADY a Target, and you may already be a Victim.**

Small and medium-sized commercial, educational, and state and local government organizations (“SMEs”) in the United States are losing on average \$100,000-\$200,000 per day to criminals who steal their money using various forms of Malware [Malicious software] designed to leverage weaknesses in both the wire transfer and ACH [Automated Clearing House] process – the rather mundane mechanism that lets banks and other financial institutions process checks and other forms of payments on a daily basis. As such, this is regular crime, carried out in the real world, resulting in real financial losses. But it is based on a technique that relies on the Internet. This briefing document will describe the general class and behavior of the malicious software that is used, the criminal gangs who use it, and the effects on the individuals, enterprises, and economies that fall victim to it. In addition it will identify recommended steps to mitigate some of the effects of the Malware.

The problem of Malware-enabled Wire/ACH Fraud is a real issue with growing economic implications. It is rooted in the nature of the United States’ diverse economy; the most common victims are the small and mid-size financial institutions and SMEs that dot our landscape and rely on third-party ACH services to compete with global banks and corporate entities. The criminals are international financial terrorists, and by taking advantage of the third-party ACH processors to whom the smaller banks entrust their own financial transactions in an effort to remain competitive in the market, they are stealing directly from America’s SMEs.

Like the global epidemics of the H1N1 flu virus, and the AIDS virus, the issue of cybercrime is now everyone’s problem; it affects the lives of all of us. The problem is not isolated to those who are direct victims; we all suffer by bearing the increased costs and reduced convenience as a result of cybercrime. We are in a race against the criminals who stand to gain financially from exploiting the problem. Sitting back and blaming the manufacturers of operating systems, Anti-Virus companies, or the federal governments of the countries involved, is counter-productive, and misses the point.

While we lay blame and wring our hands searching for issue-specific solutions, cybercriminals are launching widespread Malware attacks, compromising personal and financial information, and account credentials, and ultimately stealing OUR money. In the 2008 Internet Crime Report<sup>1</sup>, the FBI identified over \$264 million in confirmed losses from reported online fraud. But this is just the tip of iceberg; the crimes reported through the FBI represent a small portion of overall online crime, even in the United States. Many victims fail to report their losses, and many that do report, do so to state and local law enforcement organizations rather than to the FBI.

---

<sup>1</sup> [http://www.ic3.gov/media/annualreport/2008\\_IC3Report.pdf](http://www.ic3.gov/media/annualreport/2008_IC3Report.pdf)

Trying to stop widespread eCrime using the “whack-a-mole” approach isn’t working either; tactical intervention may thwart or reduce the effects of individual Malware strains, but it will not help with the fundamental cybercrime challenge we all face. Governments and private industry across the world must improve collaboration, and in a more efficient way, to contend with the very real and growing cybersecurity issues that threaten the ability of SMEs and consumers to execute transactions and bank online with confidence. And while we should be deeply concerned by the direct economic damage caused by this malicious activity, we must also be cognizant of the fact that in a growing number of cases, those funds support the ongoing operations of not only criminal gangs, but also the activities of terrorist organizations.<sup>2</sup>.

People who understand the IT, telecom and research world must cooperate and create a comprehensive plan to re-examine the way we interact and how the systems interact, in order to attack the problem.

## **Overview and Document Objective:**

- 1) Define the problem and key issues as an alert to stakeholder executives in SMEs
- 2) Explain the nature, frequency and known details of the problem
- 3) Suggest options for SMEs to avoid the problem
- 4) Suggest options for consumers to avoid the problem

---

<sup>2</sup> <http://www.washingtonpost.com/wp-dyn/content/article/2007/07/05/AR2007070501153.html>

## **The Problem of Malware-Enabled Wire and ACH Fraud**

In Malware-Enabled Wire/ACH Fraud, criminals infect victim's computers with Malware, and then use the Malware to:

- Steal account credentials, including Personally Identifiable Information (PII);
- Modify the victim's version of the Financial Institution's website, falsely displaying additional input boxes that ask the victim for additional key information to authenticate the transactions;
- Initiate new transactions in real time while the victim banks online;
- In some cases store the stolen credentials and later empty accounts after the victims have disconnected; and
- Proxy through the victim's computer to perform theft.

SMEs are especially vulnerable, because they often bank with regional financial institutions that either can't or won't return money lost to Wire/ACH fraud, and who generally have limited experience or expertise in dealing with leading edge cybercrime techniques. In some cases the criminals rely on the fact that the smaller banks outsource their Wire and ACH functions to specialist third party clearing houses. With these third party clearing houses, the responsibility for authentication of customer validation rests with the banks that are generally ill prepared to identify sophisticated fraud. In addition, by concentrating on victims at smaller banks, the criminals allow themselves an additional time cushion that is often the key to a successful crime.

Worse yet, the protections available to personal/consumer accounts are not available to business accounts; unlike the typical 60 day window that consumers have to dispute discrepancies with their accounts, online banking transactions are subject to the Uniform Commercial Code<sup>3</sup> which typically provides a window of less than 48 hours, after which the recovery of misappropriated funds becomes extremely difficult.

In other words, the stakes are far higher for SMEs both in terms of vulnerability to Wire and ACH Fraud and diminished chances of recovering any of the stolen funds.

## **The Nature, Frequency and Known Details of Malware-Enabled ACH Fraud**

There are several ACH operators who provide clearinghouse services. By examining a small sample of recent well-documented attacks, it is easier to understand how the Malware-Enabled

---

<sup>3</sup> <http://www.law.cornell.edu/ucc/ucc.table.html>

ACH Fraud issue is a threat that will likely accelerate at an alarming rate. If unchecked, this problem could erode confidence in online financial transactions such that SMEs and consumers would need to seek alternative methods of transactions, at a far higher cost to their own operations and the financial institutions that serve them.

Three recent incidents of Malware-Enabled ACH Fraud that were widely reported in The Washington Post and The New York Times illustrate the scope and nature of the attacks. It is important to note that these attacks are merely representative; data shows that **several such successful attacks occur daily across the United States alone, resulting in the irretrievable loss on average of between \$100,000 and \$200,000 per victim.**

The first incident we cite was reported on July 2, 2009 by Brian Krebs of The Washington Post<sup>4</sup> and details how criminals from the Ukraine stole \$415,000 from the government payroll account of Bullitt County, Kentucky. The criminals used a version of the “Zeus” keystroke logging Trojan to steal the online credentials, log-in to the Bullitt County bank account and steal payroll funds.

To paraphrase key events from the story, the thieves:

- 1) hacked into the treasurer’s Internet connection to steal the judge’s name and password used to access the bank account,
- 2) changed the judge’s password and associated email address to a password and email under miscreant control,
- 3) created 25 false employees who were miscreant co-conspirators hired by the attackers to accept the stolen funds, and
- 4) logged in to the bank account with the falsified credentials they created, and approved the batch of wire transfers to the 25 false employees.

The 25 “employees” who accepted the transferred funds are commonly referred to as “mules”, doing the work of accepting money into their accounts, taking a percentage as their fee, and funneling the balance of the funds upstream to the criminals through services such as Western Union® and MoneyGram®). These online criminal gangs function much like regular real-world criminal gangs (and increasingly operate in both venues), with money flowing up from lower level operators to the gang leaders at the top of the chain.

---

<sup>4</sup> [http://voices.washingtonpost.com/securityfix/2009/07/an\\_odyssey\\_of\\_fraud\\_part\\_ii.html](http://voices.washingtonpost.com/securityfix/2009/07/an_odyssey_of_fraud_part_ii.html)

To further illustrate, Brian Krebs wrote a second article published in The Washington Post on July 20, 2009 entitled “The Pitfalls of Business Banking”<sup>5</sup>. In this article he detailed the small enterprise thefts from the Western Beaver School District in Pennsylvania of \$700,000, and of Slack Auto Parts in Gainesville, GA of \$75,000. In both cases, criminals used Malware to hack into accounts and transfer funds into the account of hired “mules” who then funneled the stolen funds back to the criminals for a small percentage of the take. Shockingly, very polished and professional-looking money mule recruitment sites were used to recruit the mules. Recruitment, money laundering and reshipping via these sites is a common practice that has been occurring for many years; one site that tracks such activity is <http://www.bobbear.co.uk/>. By reviewing some of the “Active Frauds” listed one can see how professional and organized they have become.

Of course, as the number of cases and victims grows, and as smaller banks begin to balk at bearing the losses, lawsuits are being filed. These filings provide real insight into how difficult it is for an SME to take timely action after the fact. Krebs discusses a prime example again in an article dated September 23, 2009, where Patco Construction is suing its bank for over \$350,000 that has not been recovered<sup>6</sup>. The article provides a link to the actual filing.

In another article by Saul Hansell from the New York Times published August 20, 2009<sup>7</sup>, additional insights into these types of Malware-Enabled Wire and ACH Fraud schemes were revealed. In one type of attack, criminals use a Trojan to compromise a user’s temporary credentials, even for accounts using a two-factor authentication token or device such as those made by RSA, which change every 60 seconds. The Trojan transmits the user’s temporary credential back to the criminals in real-time so that they can access and empty the user’s account during the active banking session. In another type of real-time attack, criminals use Malware called “Clampi”<sup>8</sup> to capture the account information and empty the account. One of the features of “Clampi” is that it quickly infiltrates nearly all machines on an SME network. “Clampi” was identified as the Malware used in the Slack Auto Parts heist of \$75,000.

However, these reports represent just the tip of the iceberg; during September of 2009, utilizing data from a series of sinkholes and reporting systems that Neustar collaborates on, our

---

<sup>5</sup> [http://voices.washingtonpost.com/securityfix/2009/07/the\\_pitfalls\\_of\\_business\\_banki.html](http://voices.washingtonpost.com/securityfix/2009/07/the_pitfalls_of_business_banki.html)

<sup>6</sup> [http://voices.washingtonpost.com/securityfix/2009/09/construction\\_firm\\_sues\\_bank\\_af.html](http://voices.washingtonpost.com/securityfix/2009/09/construction_firm_sues_bank_af.html)

<sup>7</sup> <http://bits.blogs.nytimes.com/2009/08/20/how-hackers-snatch-real-time-security-id-numbers/?pagemode=print>

<sup>8</sup> <http://www.secureworks.com/research/threats/clampi-trojan/>

Security Analysis Group was able to categorize and validate, by IP address, in excess of 24 million successfully compromised computers. These computers are identified every day based on their active probing of strategically placed “honey pots” which provides evidence of their being infected, and the nature of the malware with which they are infected. These include systems infected with Zeus, Clampi, and Torpig which were then able to transmit information outside of their local networks, and on to the open Internet.

### **SME options: Avoiding Malware-Enabled Wire and ACH Fraud:**

This is an ever-changing landscape and we all must remain vigilant of what is occurring on the battlefield. There may never be a silver-bullet solution, but SMEs can take several steps to reduce the risk of exposure to Malware-Enabled Wire/ACH Fraud attacks. And while the use of up-to-date Anti-Virus Software is important, the state-of-the-art versions of most Malware are able to avoid detection at least 50% of the time. However the overriding assumption that should be employed by all concerned (until such time as the challenge of insecure computing is met) is that user machines have been compromised. As such, systems should be designed and implemented that do not depend on the user’s system to be safe.

Notwithstanding this assumption, the options listed below represent some recommended guidelines to protect the computers performing online transactions:

- Computers are relatively inexpensive; use a separate dedicated machine for all of your online financial transactions. This model also requires implementing the following requirements:
  - This machine **MUST NOT** be part of a Windows domain. Only utilize a Local Administrator account that can operate on the account access information. This avoids the “Clampi effect” of one compromised machine leading to a fully infiltrated network where miscreants can more easily steal sensitive account information.
  - As trivial as this sounds, shut the machine down when it is not in use; this can limit your exposure – many of the modern worms/trojans exploit vulnerabilities in the Windows Operating System, and contrary to popular belief do not require the user to have taken any actions such as opening emails or visiting malicious websites.
  - Implement Firewall/Proxy instrumentation on both your ingress and egress points, monitoring and logging all traffic to/from your machine to ensure unauthorized access is denied no matter from what point it is initiated. The

machine should be used for financial transactions ONLY; all non-business essential network traffic should be denied to/from this machine.

- Separate your network into different operational VLAN segments with Firewall/Proxy instrumentation to permit access to/from certain locations.
  - Only utilize VPN connections for remote access into your network, which includes remote access to dedicated machines (which should have their own policy/restrictions).
- 
- Implement a Change Management process<sup>9</sup> for any work that is to be done on machines performing financial transactions (this should include any changes to proxy or firewall settings that could impact these machines). Changes must require multiple party approvals. Convenience is not an acceptable reason to open access.
  - If multiple people need transaction access, each person must have an additional, separate computer – or leverage Terminal Services to create a system of clients and Dumb Terminals.
  - Virtualized environments are another option employees can leverage; the solution can work for multiple employees, or employees who travel and who need to perform financial functions on the road. Again, computers are cheap, use a netbook or comparable alternative dedicated exclusively to financial transactions.
  - Leverage dedicated? bootable media (CD/DVD/USB...) when performing financial transactions. One could even go a step further and remove the ability to write to the hard drive so that nothing can actually be stored on the machine, other than the core operating system and key applications.
  - The Health Care Industry has done a lot of work in documenting the protection of patient information; review existing documentation (such as HIPAA regulations) for some guidance/best practices.

---

<sup>9</sup> [http://en.wikipedia.org/wiki/Change\\_Management](http://en.wikipedia.org/wiki/Change_Management)

Most importantly, ensure that the proper policies and procedures are in place to enforce all of the guidelines set and obtain Senior Management support for the use and enforcement of these guidelines.

By employing these interim recommendations, SME executives can greatly reduce the threat and risk of Malware-Enabled Wire and ACH Fraud. Additionally, by examining the available bank provided account authentication choices, executives can make the best possible banking security decisions to protect their enterprise.

### **Bank Safely**

Financial institutions often offer tiered services, with differing levels of authentication choices that may include a combination of the items listed below. Your organization will need to weigh the acceptable risks/costs structure, noting that there is no silver-bullet solution; each mitigation strategy raises the bar for the criminals, affecting both the cost and technical capability associated with performing such nefarious activity. As consumers, we drive the market place. If your current financial institution does not meet your needs, tell them what you want, and if they're unable to comply, move your business to a bank that does meet your requirements. This is NOT the area for compromise.

There are long-standing debates on what account authentication mechanisms should be used. Unfortunately current Malware already has the ability to circumvent many of the protocols that banks offer today. Understanding some of the attack scenarios will assist in educating users on how to mitigate the effects of such threats. Some of the more common authentication options are:

- Username/password (u/p) only– this is not a viable option and should never be the only item used to protect your financial transactions
- u/p and token – raises the bar, but as we've seen there is Malware in use today that can exploit this method
- u/p and token to log in, with a separate token for the transaction. This is a reasonable option, as long as only one transaction can occur per token cycle and errors during this process are easily noticed, clearly written and not easily blocked by malicious actors.

- o Users need to understand what it means to use a token and the potential risks that remain despite token usage. (Man In The Middle <sup>10</sup>or Man In The Browser <sup>11</sup>attacks). Factors in token vulnerability include:
  - § Token regeneration time: people do not wish to be waiting around for lengthy periods of time to attempt a login into their account.
  - § Token expiration time variability: can range from 30 seconds to 10 minutes and in some cases, can be set to infinite. The shorter the better, or implement usage to restrict only one successful login per token ID.
  - § Tokens need to reflect how much time consumers have left to initiate a process.
  - § Institutions need to be clear on how their systems are set up and users need to be able to easily locate this information as well have reference material or training on how their tokens work.
- Multiple parties being required to initiate, perform and authorize a transaction.
- Machine authorization restriction by limiting authorization to designated machines – can be done a number of ways such as cookies, or the installation of certain custom software on the computer.
- Additional authentication steps and time delay requirements if transactions occur from machines not currently authorized.
- Implement access controls for accounts when multiple users accounts can be used or are needed to complete a transaction:
  - o Considerations need to be taken on how the individual SMEs authenticate the addition and or modification of accounts.
  - o Considerations need to be taken on how the financial institutions authenticate the addition or modification of accounts for their SME customers.

---

<sup>10</sup> [http://en.wikipedia.org/wiki/Man-in-the-middle\\_attack](http://en.wikipedia.org/wiki/Man-in-the-middle_attack)

<sup>11</sup> [http://en.wikipedia.org/wiki/Man\\_in\\_the\\_Browser](http://en.wikipedia.org/wiki/Man_in_the_Browser) - Note, this attack can be performed after all the authentication/security transactions between your computer and the bank have taken place (including but not limited to: SSL, PKI, password and token authentication).

- o Users must not have the ability to change other account's credentials – at least not easily and without notification to multiple parties requiring approval prior to the actual change being accepted (including some sort of built in time delay, which can be circumvented with a physical appearance at the financial institution).
- Examine out-of-band notifications as a requirement for certain classes of requests/changes. Many of these options can't easily be faked/modified by the miscreants, especially if some of the options above are implemented.
- Work with your bank so that certain changes/transactions require a visit to one of their brick and mortar facilities or notarized documentation is required, followed up with a call by the bank to ensure the documentation has been received and that the change has been approved (caution should be taken on the usage of any contact information that can easily be modified, including information that is listed in emails and on web sites).
- Utilize baseline alerts: while some institutions have very diverse transactions occurring on a daily basis, others do not. This "baseline" could potentially be leveraged to notify account holders prior to the transaction being processed (notification should be something other than an email, especially when a recent account change has been made).

Above all, be aware of what transactions are occurring within your account at all times, and verify every transaction as soon as you see it appear on your online account.

**Customer Options: Avoiding Malware-Enabled Wire and ACH and other Fraud:**

To avoid mass and widespread panic and loss of confidence on the part of individual customers, financial institutions need to increase consumer education and awareness about phishing attacks and consumer transaction fraud. Such educational efforts could include teaching consumers the following:

- A) What an attack looks like.
- B) Resources/education available to the user
- C) Signs of a keylogging attack, which can include
  - 1)When a user knows they've typed in the correct credentials, yet they are prompted to re-enter information.
  - 2)New fields that appear or are added to new/existing pages without explanation.

D) Posting an easily locatable page on the financial institution site indicating the security posture and clearly stating how the bank operates, what information it requires and when and how to easily notify the bank of questionable activity.

E) Banks can also:

- 1) Provide a live presentation/demo prior to account completion.
- 2) Require consumers to acknowledge in writing that they viewed the demo and understand the risks involved.

These precautions don't have to be offered for every account, but can be made available for a certain class of account or as an account upgrade.

Customers also need to consider the following:

A) How to handle notification emails (multiple) or other out-of-band communication on transfers being made to and from the ACH and for wires.

B) What are the transaction review mechanisms your bank is going to/willing to/able to provide?

C) What are the actual options/permissions on your account and how are those set for specific transaction events such as:

- 1) Receiving money
- 2) Sending money
- 3) Permit/Deny options: if possible, everything should be a default "deny" and users should need to turn things "on".

D) If an incident occurs, whom should it be reported to and why you should report it?

E) Documents such as this should be reviewed by both senior management and IT staff. Discussions between all parties of interest need to happen so that one can properly evaluate, determine risk and implement a solution that works for the organization.

In conclusion, organizations are being stolen from every day. Many will never see a return of their stolen funds. Some will be forced to go "out-of-business", and some will recover, but the Malware-Enabled Wire and ACH Fraud will continue. The question is not whether it will happen to you, but rather, what steps you should take to insulate your SME, and to minimize the threat.

As consumers, we need to ensure that we are educated about the problems we face, and the options we have to mitigate these threats. We need to take action and be accountable for our actions. We need to stay abreast of what is going on in the cyber world and how infrastructure is being exploited.

Your organization likely takes precautions to ensure your facilities are physically secure by the use of guards, motion sensors, locks, alarms, and cameras. You are aware if one of these fails or if better technology becomes available, so why would you not do the same to lock down your computer infrastructure? This isn't a "set it and forget it" job; users need to remain vigilant and active to ensure they know and understand the impending threats. Implementing these suggestions will reduce vulnerability, but the solution to ending the threat lies in the aggregated efforts of SME, government and law enforcement collaborating to solve the problem.