

<http://biz.yahoo.com/prnews/070110/clw091.html?.v=13>

RSA Discovers New Universal Man-in-the-Middle Phishing Kit

Wednesday January 10, 11:09 am ET

New kit helps fraudsters easily launch increasingly-sophisticated and automated online fraud attacks

BEDFORD, Mass., Jan. 10 /PRNewswire/ -- RSA, The Security Division of EMC, (NYSE: [EMC - News](#)) announced today that its 24x7 Anti-Fraud Command Center (AFCC) has uncovered a new phishing kit being sold and used online by fraudsters.

This new kit, a Universal Man-in-the-Middle Phishing Kit, is designed to facilitate new and sophisticated attacks against global organizations in which the victims communicate with a legitimate web site via a fraudulent URL set by the fraudster. This allows the fraudster to capture victims' personal information in real-time.

RSA's analysts researched and analyzed a demo of the kit that was being offered as a free trial on one of the online fraudster forums that the AFCC monitors regularly.

How it works

Using the Universal Man-in-the-Middle Phishing Kit, the fraudster creates a fraudulent URL via a simple and user-friendly online interface. This URL communicates with the legitimate website of the targeted organization in real-time - whether it is the online banking site of a financial institution, the order tunnel of an ecommerce company, or any other such business transacting with its users online. The victim receives a "standard" phishing email, and when clicking on the link s/he is directed to the fraudulent URL. The victim then interacts with genuine content from the legitimate website - which has been "imported" by the attack into the phishing URL - thus allowing the fraudster seamless, invisible and immediate access to the victim's personal information.

Fraudster benefits

RSA's analysts have identified two primary benefits that fraudsters using this kit are set to reap:

1. It is a "universal" phishing kit, meaning it can easily be configured per target. Fraudsters who want to initiate a phishing attack do not have to purchase or prepare a custom phishing kit for each target. Once they acquire and operate this kit, the attack can be configured to "import" pages from any target website.
2. Unlike standard phishing attacks, which only collect specific requested data (typically login and card-related credentials), this attack is designed to intercept any type of credentials submitted to the site after the victim has logged into his account as well.

Detection and mitigation efforts

The RSA 24x7 Anti-Fraud Command Center handles this attack in a similar fashion to the way it deals with "standard" phishing attacks - relying on a broad monitoring and detection network, its broad blocking network, as well as industry-leading experience in site shutdown - as it does for more than 150 customers of its FraudAction(SM) anti-phishing, anti-pharming service. And, uniquely, RSA can further identify, analyze and mitigate this specific type of attack via the RSA eFraudNetwork(SM) community - the company's cross-institution anti-fraud network - by leveraging sophisticated analytics in the RSA® Risk Engine to further protect customers that also use RSA® Adaptive Authentication or RSA® Transaction Monitoring.

"As institutions put additional online security measures in place, inevitably the fraudsters are looking at new ways of duping innocent victims and stealing their information and assets. While these types of attacks are still considered 'next generation,' we expect them to become more widespread over the course of the next 12-18 months," commented Marc Gaffan, director of marketing, Consumer Solutions at RSA. "We are working with many organizations to ensure they are positioned to withstand whatever threats fraudsters may create. Some of these organizations have already deployed various layers of protection and others are in the process of strengthening their security."

About RSA

RSA, The Security Division of EMC, is the expert in information-centric security, enabling the protection of information throughout its lifecycle. RSA enables customers to cost-effectively secure critical information assets and online identities wherever they live and at every step of the way, and manage security information and events to ease the burden of compliance.

RSA offers industry-leading solutions in identity assurance & access control, encryption & key management, compliance & security information management and fraud protection. These solutions bring trust to millions of user identities, the transactions that they perform, and the data that is generated. For more information, please visit www.RSA.com and www.EMC.com

RSA, FraudAction and eFraudNetwork are either registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. EMC is a registered trademark of EMC Corporation. All other products or services mentioned are trademarks of their respective companies.

20 JANUARY 2007

\$5 PayPal security key gives false hope to stop phishers



Like many financial institutions, eBay and PayPal are late adopters of security devices for one time passwords. A security device (costing \$5 in the US) gives a different security code each time you log into your account. PayPal say it "[generates a unique six-digit security code about every 30 seconds. You enter that code when you log in to your PayPal or eBay account with your regular user name and password. Then the code expires - no-one else can use it.](#)" Or can they??

These devices have been around for almost twenty years with [Security Dynamics \(RSA Security\)](#) and [Vasco](#) being the earliest to market solutions. The eBay PayPal key has been developed in conjunction with [VeriSign](#).

The biggest concern is are the tokens effective in preventing phishing attacks? Well firstly it's not what they were designed for. They were designed originally for remote access solutions where an employee would dial into a company workplace over a telephone line. Rather than a password that could be written down the token ensured hackers couldn't dial in to the network with a compromised password. There was little chance of anyone intercepting the dial up phone call. The tokens were then deployed for use internally for all users on a network. Later they migrated outside the network as the Internet became more common for remote users connecting to

corporate networks, for online banking, and now for eBay and PayPal.

It's important to realise they weren't designed for use on the Internet in the first place, and that hackers have had decades to develop ways to combat the tokens. The actual keys generated are still secure, there is still no effective way to compromise the security codes generated. This doesn't deter the phishers though - they have other tools in their arsenal.

MAN IN THE MIDDLE ATTACK

We've all seen phishing emails where a hacker tries to get you to click to a fake eBay or PayPal website and enter your user name and password which they later use to access your account. Smarter phishing sites are becoming more common where the hacker captures your user name and password and instantly uses it to log on to the real site. They pass the information you request to the site and back to you - you may never realise you're not logged directly into the site, but in the mean time the hacker is able to perform any transaction they please while you make the transaction you logged on to do.

TROJAN ATTACKS

Far too few Internet users keep their security up to date allowing virus and trojan attacks. If a phisher manages to install a trojan on your computer next time you log on to eBay or PayPal they can piggy back on your logon to perform their own transactions.

These two methods for bypassing one time passwords are not new - they were reported by [Bruce Schneier back in March 2005](#). What does this mean to the new PayPal and eBay security devices? Well it'll make the phishers lives harder but so far they're only available in the US, Australia and Germany, leaving plenty of targets for phishers in the other eBay and PayPal territories. Secondly they're not compulsory, free for PayPal Business accounts but the \$5 cost

will put off many users who arguably are the most vulnerable. Finally the efficacy of the tokens themselves has to be questioned. It's technology that's been around before most of today's hackers first logged on to the Internet and was designed for dial up connections to corporate networks. Hackers have grown up looking for ways to render them useless.

It remains to be seen if the promise of security will result in users lowering their guard still further. After all no one can access your account without your token can they? Well possibly they can - users need to be as vigilant as ever. As [Blogging stocks ask](#) "Are the days at an end to eBay and PayPal phishing scams?". Sadly the chances are they're only just beginning!

An easier identity solution

January 19, 2007 5:28 AM PST

■ [del.icio.us](#)  [Digg this](#)

PayPal announced last week that it will [soon support a key fob](#) to provide its customers with two-factor authentication.

Costing \$5 for personal accounts--and free for business accounts--people can get a One-Time Password (OTP) device that displays a new six-digit code every 30 seconds. The intent is to provide customers with another line of defense against identity theft and the continuous onslaught of PayPal-based phishing attacks.

On the plus side, it's nice to see PayPal being aggressive with security. If people feel they can't trust PayPal, the financing company suffers. A big PayPal breach could also be the only thing that has the potential to crash the eBay party. If PayPal can't be trusted, the natural question consumers will ask is: What about eBay? A security breach at a brick-and-mortar business is bad. A security breach at an e-business can be lethal.

Now kudos to PayPal aside, I see a potential problem in the not-too-distant future. Pretty soon, we consumers will be required to have multiple security tokens, smart cards and passwords to do anything online. Imagine a string of security fobs you carry around next to the keys to your minivan and SUV. This could get out of hand rather quickly.

I believe that e-businesses and the security industry have this whole thing backward. Instead of putting the onus of strong authentication on the vendors, it ought to reside on the consumer. I should be able to go into my local Radio Shack and buy a security token of my choice. Once I own this, I ought to be able to register it with my bank, credit card company, and any other online service provider of my choice. This would create a one-to-many solution rather than today's many-to-one mess.

This idea would take some work and cooperation, but it is certainly possible. Back-end vendors would have to agree on a set of authentication standards they would support. There are several efforts already in place, including VeriSign's Open Authentication standard (OATH), RSA's OTP standard and various others being driven by the Liberty Alliance, the IEEE and the federal government.

Global two-factor authentication would also require services specialists to act as middlemen and handle technology, legal and support tasks. But I'm sure that VeriSign, Ping Identity, RSA and loads of others would be willing to fill this void. Finally, what happens if you lose your token? We need some seamless way to anticipate this with rock-solid processes for protecting consumers, reissuing tokens, and taking care of back-end updates. The identity service providers could certainly fill this void.

We need to figure this out soon, lest we end up a string of security tokens--or with online services that have gone away. Starting next year, for example, consumers will have to go

to the Registry of Motor Vehicles in person for many transactions we now do over the Web. Why? To enforce the federal [Real ID Act](#) starting in 2008.

Wouldn't it be easier if I had a single security token that let Uncle Sam and everyone else know that it is really me?

Posted by [Jon Oltsik](#)

Beware: First phishing, now vishing

Friday, January 19, 2007

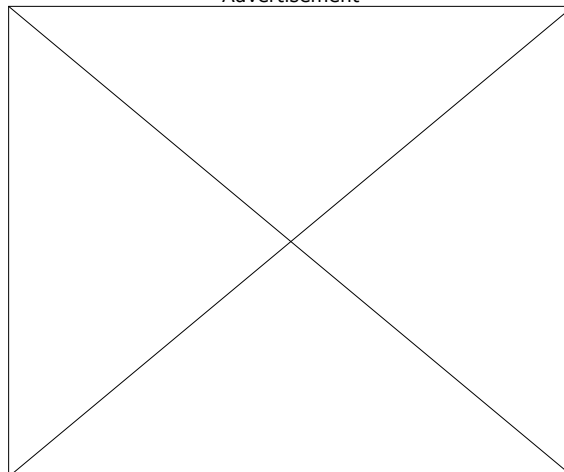
Financial Headlines

- [GE sees earnings double](#)
- [Citigroup beats estimates, but profits fall 26%](#)
- [Earnings plunge, CEO mulls change in tactics](#)
- [BRIEFS](#)

Yesterday's Headlines

- [Consumer Reports retracts negative report on infant car seats](#)
- [Oil prices edge up after sinking](#)
- [IBM beats the Street with fourth-quarter numbers; Shares drop 5 percent](#)
- [Others expected to fill Neteller void in U.S. online gambling](#)
- [House approves fees, taxes on oil companies; plans to use money for renewable fuels](#)
- [Analysts estimate huge percent margins for Apple iPhone](#)
- [Retail money funds rose in latest week](#)
- [Valero chairman donates \\$25 million to University of Texas Health Science Center](#)
- [Credit card companies watchful after TJX data breach exposes customers' cards](#)
- [Tribune reviews options after bids fall short](#)
- [Mistrial declared in California Vioxx lawsuits after deadlock](#)
- [McDonald's opens first drive-thru in Beijing in venture with Sinopec](#)
- [Delta to discuss US Airways' increased bid with board of directors](#)
- **Beware: First phishing, now vishing**
- [Natural gas prices dropping](#)
- [Farmers return to corn in ethanol crazw](#)
- [PSC Metals expands its scrap capacity](#)
- [Business briefs](#)
- [Inflation slows to three-year low; wages rise](#)
- [Bernanke issues strong warning about deficits](#)
- [Stocks fall on uncertainty over interest rates after strong economic data](#)
- [Dividends](#)
- [GE buying Abbott diagnostics](#)
- [Recalls](#)

Advertisement



Most sophisticated computer users know about “phishing” — the act of sending an e-mail to a user claiming to be a legitimate enterprise in an attempt to scam the user into giving information that will be used for identity theft and fraud.

But the Better Business Bureau says scam artists are the first to take advantage of new technology, and now there’s “vishing,” which is short for voice fishing.

It’s come about because of the proliferation of Voice over Internet Protocol (VoIP) phones.

One version works online, where the con artist sends an e-mail, disguised to appear as though it’s from a well-known business. The e-mail typically reports a “security” problem with the recipient’s account and urges the victim to call a telephone number to “straighten things out.”

When the victim calls, he or she reaches an automated attendant prompting them to enter an account number, password or other private information for “security verification” purposes. Entering the number on the phone is as good as typing it into the computer.

Some vishers use automated dialing programs to “cold call” victims. The caller ID device may even list a legitimate-looking local phone number, to inspire trust. A prerecorded message (or sometimes a live “employee”) claims the victim’s account has been compromised or needs updating or verification.

TIPS TO AVOID VISHING SCAMS

n Typical vishing e-mails imply urgency, ask you to verify account information, and may contain misspellings.

n If you receive a vishing phone call, hang up. Call your bank, using the phone number on the back of your debit or credit card, and report the matter.

n Banks do not use prerecorded messages to handle security issues. If they telephone you to report suspicious use of your card, they do not need to request identifying information because they already have that on record.

n Do not automatically trust a phone number based on its area code. Con artists can hack into Caller ID systems, and VoIP users can assign any area code to a phone number.

If you think you have been a victim of vishing visit the Federal Trade Commission’s Identity Theft Web site at www.consumer.gov/idtheft/con_about.htm.

SOURCE: Better Business Bureau

Washington post

Great Strides in Phishing

Earlier this month, Security Fix called attention to [a phishing scam](#) where bad guys were making use of the real **Amazon.com** Web site to trick people into entering personal information at a fake Amazon site they created.

Now, according to fraud investigators at **RSA Security Inc.**, comes the release of a simple, point-and-click tool for sale in the hacker underground that is designed to help criminals automate the construction of more scam sites employing this same, sophisticated approach.

The image shows a web-based configuration interface for a phishing tool. At the top left, there are navigation links: [Domains] [Pages] [Visitors]. The main area contains several input fields and sections:

- Domain rewriting:** A section with two input fields, each preceded by an arrow pointing right (=>).
- SSL:** A section with one input field preceded by an arrow pointing right (=>).
- Emails:** A section with two input fields, each preceded by an arrow pointing right (=>).
- Send posts to:** An input field preceded by an arrow pointing right (=>).
- Send emails «from»:** An input field preceded by an arrow pointing right (=>).
- HTML rewriting:** A section with two large text input areas. The left area is labeled 'From' and the right area is labeled 'To'. Both areas are preceded by an arrow pointing right (=>). The right area also has a 'Del' label next to it.
- Submit:** A button located below the HTML rewriting section.

At the bottom left, there are navigation links: [Domains] [Pages] [Visitors].

What made the Amazon phishing site that I wrote about so unusual was that it relied on a so-called man-in-the-middle attack, in which the fraudsters' fake site passes victim-supplied login credentials to the targeted institution's site on the user's behalf. The data passed to the legitimate site is stored or e-mailed to some free Webmail account set up by the fraudsters, and the victim is then typically handed off to the targeted institution's site.

This is a tactic used to make the fraudulent site appear more authentic: I've heard far too many people say they can tell whether a site is legit or not simply by entering completely made up or gibberish user names and passwords at a suspected phishing site. The reasoning here: "If this site is fake, it will accept my bogus login information, but if it tells me that the account information doesn't exist or is incorrect, then it must be the real thing." Obviously, the man-in-the-middle phishing method shows the folly of that line of thinking.

The phishing automation tool discovered by RSA is installable software that automates the creation of man-in-the-middle attacks so that any novice can set them up, and do so quickly. Using this tool, a criminal no longer has to buy or create custom phishing kits for a targeted organization. Also, the scam artist can intercept any data that is sent back and forth between the customer and the institution for as long as the victim is logged into his or her account.

I checked with a couple of reliable sources, and they said this simple software tool is indeed being sold on various shadowy online forums, apparently under the unassuming title "scams and fakes creation tool." It is being sold for about \$1,000, a hefty price -- roughly five to ten times the amount that most phishing kits fetch on the Internet black market. However, the inflated price makes sense if you consider that the kit offers the ability to create more effective and convincing phishing sites targeting multiple institutions in a very short period of time, said **Marc Gaffan**, director of marketing at RSA's consumer division.

"This thing absolutely increases the scalability [of phishing attacks] and the vulnerability of smaller companies, particularly non-financial institutions [and] retail institutions that are more gearing toward credit card fraud," Gaffan said.

As of last Tuesday, Gaffan said RSA had spotted fewer than a dozen sites generated by the new tool. Still, scammers are always looking for greater automation tools. Given some of the sophistication that is being built into online fraud tools these days, it's probably safe to assume that we will see this type of phishing attack become the norm very soon.

By Brian Krebs | January 17, 2007; 1:15 PM ET | Category: [Latest Warnings](#)

Previous: [Do Away With HTML Based E-mail](#) |

http://techdigest.tv/2007/01/rsa_discover_ne.html

RSA discover new phishing method



The more [advice for being careful online](#) we get, the further fraudsters push things to try to outwit us poor, innocent Net users and get hold of our credit card and bank account numbers.

Security firm RSA have discovered a new 'man-in-the-middle' phishing kit that lets a third-party sit between the user and a legitimate business and capture personal information in real time.

Premise: Why break into increasingly secure systems when you can just get between the legitimate user and that system and nick their details?

Unlike the existing crop of phishing web sites that take a few graphics from the authentic site, but not much else, these attacks actually direct the user to a rogue web site but interacts with genuine content from the legitimate site. This puts the attacker 'in the middle' - hence the name - and easily able to get hold of the data.

Fortunately for those with a bit of web sense, it sounds as if these attacks still rely on the user clicking on a fraudulent link.

Related stories: [McAfee offers advice for avoiding phishers and identity thieves](#)

Came straight to this page? Visit www.TechDigest.tv for all the latest news.