

BATTLING THE BOTNETS AND ROOTKITS:
A LAYERED IDENTITY STRATEGY

A WHITE PAPER

Author:

Guy Huntington

President

Huntington Ventures Ltd.

“The Business of Authentication”

www.authenticationworld.com

Date: October, 2006

**BATTLING THE BOTNETS AND ROOTKITS:
A LAYERED IDENTITY STRATEGY**

The emergence of organized crime using sophisticated malware attacks (keyboard logging, phishing, botnets, rootkit attacks, Trojan Horse, etc.) is quickly highlighting the weaknesses of individuals and enterprise security systems. For example, in [March 2006](#), Russian organized crime used rootkit software. This places malicious code at the heart of the Microsoft operating system. The code was installed when a user visited certain sex websites. It then watched for when a user entered uid and password information for banks, dating, social websites and email. As the data was entered, in seconds, the rootkit software then began passing the information back to a Russian web server. Over four day's time **90,000 pieces of user information from 6,500 companies was sent before the server was shut down.**

Organized crime now sells millions of uids, passwords, social security and credit card numbers in eBay type auctions. For example a web mob named Shadowcrew: [“In the past two years, the Shadowcrew's 4,000 members, according to the U.S. Secret Service, ran a worldwide marketplace in which 1.5 million credit card numbers, 18 million e-mail accounts, and scores of identification documents—everything from passports to driver's licenses to student IDs—were offered to the highest bidder.”](#)

As well, the code for writing these types of attacks has become modularized. This allows the criminal to effectively order a piece of code that performs specialized functions. Further, the code can be checked before purchase by the criminal to ensure it will bypass the enterprise's existing intrusion detection systems. [Code is being offered at \\$25 per 10,000 hijacked computers it infects.](#)

The increase in phishing attacks (where the user is directed to a fictitious site resembling the enterprise web site and then entering in personal identity information) as well as keyboard logging attacks by both hardware and software devices is also part of the organized crime toolkits. [McAfee in April 2006](#) stated that the increase in Windows based stealth components was 2,300% from 2001 to 2005.

The bottom line? You need to have an enterprise security strategy that keeps one step ahead of the game. You don't want to face lawsuits from your employees or customers for not protecting their personal identity data. Nor do you want to have impostors successfully logging on to your systems and perpetrating crimes against your enterprise. Finally, you definitely don't want to be in the media explaining why your security was breached.

The existing intrusion detection systems, even the best ones, are insufficient on their own to preventing all types of attacks. The result is that enterprises need to adopt a multi-layered identity security strategy that adapts to these types of attacks and mitigates enterprise and user risk. This paper examines the strategic framework for such a strategy.

FIRST LEVEL OF DEFENCE: IDENTITY REGISTRATION

When an employee comes to work for you, what kind of identity check did you do on them? Was there any criminal record check? Did you check out their education credentials? Do you do any kind of criminal or education background check on contractors and consultants working for you? What kind of identity check do you apply to customers who will be using your systems?

As the enterprise risk rises for applications and information systems your customers will be using, so to must the initial identity registration check increase. This level of first line defence is usually poorly thought out in most enterprises, especially beyond employees.

SECOND LEVEL OF DEFENCE: USER TRAINING

Does your enterprise do any kind of annual training for all users of your systems about email, phishing and rootkit attacks? Are you strongly warning them about the danger of clicking on any links in an email document? This kind of basic training, while it might be ignored, put's some of the enterprise defence on the shoulders of its users. A 2-3 minute online flash presentation can be put together cheaply. It may result in your enterprise being able to avoid an enterprise breach.

THIRD LEVEL OF DEFENCE: DEVICE SECURITY CHECK

When a user tries to log on to your enterprise systems, is there a device check done? Is the software and hardware platform checked out and ensured that all available patches are in place? If not, before the device can even reach your network, is it placed in a quarantine area where patches can be recommended to be installed? If you're not doing this, using a device like from [Caymas](#), then you're enterprise is open to unexpected forms of attack.

FOURTH LEVEL OF DEFENCE: INITIAL IDENTITY AUTHENTICATION

Your users, if you're going to require password authentication (which is the weakest form of authentication) should enter in their id and password using a keyboardless entry. Companies like [RSA](#) and [Bharosa](#) provide excellent tools allowing you to minimize the risk of keyboard hardware and software attacks. **DO NOT USE KEYBOARDS FOR PASSWORD ENTRY...IT IS TOO RISKY TO BE CAPTURED.**

In [2005 in the UK](#), janitors installed hardware keyboard loggers on user's keyboards in a bank. This led to an attempted theft of \$200 million pounds. Even if the computers are turned off when the janitors are in late at night cleaning, it means that they are now easily attackable by using janitors to install the device.

There have been several high school students in the US who have been charged with using these same devices, obtainable legally for \$40, to obtain their teachers and

BATTLING THE BOTNETS AND ROOTKITS: A LAYERED IDENTITY STRATEGY

administrator's passwords. In one case, the student changed numerous marks for students to allow them to enter university.

Therefore, the use of keyboard entered passwords is not advised. The initial authentication must only allow the identity basic, low risk access to specific pieces of the network, applications and information. Do not trust the authentication for medium and high risk enterprise applications.

Further, if the user is coming in via a wireless device are they given more restricted access privileges than if they are logging on from inside the enterprise? If not, then you should be rethinking your enterprise security strategy. Wireless devices authentication methods are relatively easily breached. Therefore, limit your enterprise risk by either restricting access to low risk applications or, requiring stronger authentication from the user in order to access higher risk networks, applications and information.

FIFTH LEVEL OF DEFENCE: QUICK PROVISIONING AND DE-PROVISIONING

When a user no longer requires access to your enterprise, an application, building, room, network, etc., how long does it take until they are de-provisioned? Many enterprises have very weak to poor provisioning and de-provisioning processes. In today's age, this puts the enterprise at greater risk, since a user who is gone may still have access to the enterprise. Put in place the infrastructure to quickly add, adjust or remove someone from having physical or electronic access to your enterprise

SIXTH LEVEL OF DEFENCE: STRONGER AUTHENTICATION

As the enterprise risk rises for networks, applications and information access, so too must the level of authentication strength. The financial system, payroll and payables are all higher risk. So too are users who hold super-user privileges like senior network administrators.

For all of the medium and higher risk applications, your enterprise should be using a graded series of stronger authentication. For instance, low to medium risk might be addressed by the user providing their id, password and a digital certificate.

Medium risk should be addressed by the user providing things like a secureID token along with their id and a password.

Medium to high risk should be addressed by the user providing something like a smart card, a secure id token, a biometric and a second unique password.

Can your existing security and identity sign on systems support this? Do you have budgets for this? All of this requires senior management support to successfully implement.

SEVENTH LEVEL OF DEFENCE: RE-IMAGING NETWORK OPERATING SYSTEMS

Are you prepared for a successful rootkit attack against your enterprise? Currently, Microsoft is recommending that the best way to recover is to re-image all desktops and servers affected! This could bring your IT department to a halt. Are you prepared for this?

Don't rely upon the firewall and the vendors. While they will assure you of their defensive abilities, the chance of an attack getting underneath the firewall is currently a lot higher than they would let you believe. If you are the unlucky enterprise who gets hit by a rootkit attack before the firewall vendors figure it out, then you had better be prepared to deal with it and fully recover, quickly and at low a cost as is possible.

EIGHTH LEVEL OF DEFENCE: TRANSACTION AUTHENTICATION

The emergence of numerous attack vectors on an enterprise means that enterprise must assume that criminals will successfully penetrate their outer layers of defence i.e. the firewall and the authentication systems. The answer to this is to deploy transaction authentication.

In transaction authentication, software watches the following:

- IP address being used by the user
- Geo-location of the user
- Time of day the event is occurring
- Historical user pattern
- Computer hardware the user is using

If any of these criteria are different than expected, even with a successful authentication, the transaction authentication software will start alarm bells ringing in the enterprise.

This may result in:

- The user being asked all sorts of personal questions to verify it is really them
- Security or business managers being paged in real time
- The event, process or transaction refused

All enterprises should be using this type of software to protect high risk applications like payables and other sensitive applications. [RSA](#) and [Bharosa](#) are recommended vendors.

NINTH LEVEL OF DEFENCE: ENTERPRISE REAL TIME AUDITS

The final layer of defence is the ability to quickly go back in minutes, hours, days, weeks or months to find out every network, application, information resource, type of device used, building and room the identity used at a specific point in time. All too often, the audit data is very hard to interpret from a application audit trail and worse, hard to integrate with other audit data from other applications.

BATTLING THE BOTNETS AND ROOTKITS: A LAYERED IDENTITY STRATEGY

Get a team organized on trying to provide an end to end user audit that is quickly available, easy to access and use. This will help you find out where problems and breaches occurred and then prepare remedial action.

CONCLUSION:

Today's digital world is becoming an arms race as attackers increase their sophistication in attack vectors. Further, the likely targets are no longer the defence and financial sectors. Mid-sized enterprises, educational institutions and local government are now also high quality targets for local or international organized crime.

Modern identity tools provide the overall framework for managing this throughout the enterprise. You need to integrate with this framework tools from vendors supplying network authentication and device security systems along with products for doing keyboard less authentication and transaction authentication.

This layered identity structure mitigates risks from modern day attacks. It provides enterprises with cost effective ways of applying more expensive risk management solutions to only those users who are high risk. Without it, your enterprise lays itself open to increasing level of security breaches, criminal attacks and possible lawsuits from your users when their identity data is stolen.

ABOUT THE AUTHOR:

Guy Huntington, President of Huntington Ventures Ltd, has many years of experience leading large, complex, Fortune 500 identity projects. His work has included leading Boeing's single sign on, Capital One's single sign on, Capital One's Sarbanes-Oxley provisioning project and Kaiser Permanente's web single sign on review.

He maintains a website on authentication at www.authenticationworld.com . He also maintains an authentication blog available off his website. He can be reached at guy.huntington@authenticationworld.com or by phone at 604-921-6797.