Reasons to Update Your System

A recent study conducted by the Danish security firm CSIS caught the attention of the IT Security Office. The article, "This is how Windows get infected with malware" by Peter Kruse, describes a study of Windows systems compromises. As stated in the article, "Up to 85% of all virus infections happen as the result of drive-by attacks." The study also concludes that as much as 99.8% of all virus/malware infections caused by commercial exploit kits are a direct result of the lack of updating five specific software packages."

As a reminder, make sure your systems are kept up to date with operating system and application patches. Also make sure if you do not grant users the ability to patch, that your central patching process can update applications such as Java.

A New Tool to Combat Malware

Malware detection and removal has become a major challenge for Virginia Tech IT staff. Today’s advanced malware threat is more sophisticated than ever and has the ability to evade AV software, log keystrokes, take screenshots, and help intruders gain access to computers and data. To help counter this, the IT Security Office has gained a new tool to help detect malware operating on Virginia Tech’s network.

A FireEye malware detection appliance was recently purchased that aids the IT Security Office in detecting malicious communication with Command and Control (CnC) servers associated with malware. FireEye also has the capability to capture a copy of suspicious files and test them in a virtual environment to detect zero day vulnerabilities. Use of the FireEye appliance has had an immediate impact and has helped the IT Security Office remove over 200 malware infected machines from Virginia Tech’s network.

It is important to note that nothing replaces sound computing practices when it comes to protecting Virginia Tech’s data and systems. Please visit www.security.vt.edu for more information on safe computing practices.
**Morto Worm Attack Using Weak Passwords**

The Morto worm is a new worm attacking ALL Windows platforms through the Remote Desktop Protocol (RDP). It attempts a brute force guessing attack against weak system passwords in an effort to not only infect your machine, but also to propagate itself via your RDP connections on your network. It uses a pre-determined set of common usernames and weak passwords in an attempt to access other Windows machines on your subnet. We have detected this attack in the wild on our networks. As more machines become infected, it is important to make certain you take the appropriate precautions to protect your machine.

To help prevent Morto from compromising your computer, keep your operating system and application software up to date and ensure your system passwords follow the PID password strength guidelines found at [http://www.awareness.security.vt.edu/passwords/strong_passwords.html](http://www.awareness.security.vt.edu/passwords/strong_passwords.html).

**Identity Finder Support Update**

There has been some confusion over the support model we are using for Identity Finder. Our contract with Identity Finder stipulates that all support communication be funneled through the IT Security Office before it is sent on to Identity Finder. Please direct all questions about the Identity Finder console and client to Nicolas Pachis (npachis@vt.edu) in the IT Security Office.

Identity Finder does provide a knowledge base with a large number of frequently asked questions and help topics. One of the topics system administrators may find useful is the "Settings Viewer" which can be found at [http://www.identityfinder.com/kb/Enterprise-Documentation/181999](http://www.identityfinder.com/kb/Enterprise-Documentation/181999). This tool helps to explain the different settings that each policy can have within the enterprise console.

**Updates Made to Important IT Standards**

The [Standard for Protecting Sensitive University Information Used in Digital Form and the Standard](http://www.it.vt.edu) for Storing and Transmitting Personally Identifying Information have been updated. The changes reinforce the need to protect university information and the encryption for covered data elements.

A notable change in the Standard for Storing and Transmitting Personally Identifying Information is that first name, last name, in combination with DOB are no longer considered a covered data element that requires encryption. More information about the IT policies and standards can be found at [www.it.vt.edu](http://www.it.vt.edu).
Top 10 Malware Detected

The list below represents the top 10 malware infections found on Virginia Tech’s network for the month of October.

1. InfoStealer.PWS.LdPinch *
2. Spyware.AddMovie
4. Trojan.Anamika
5. Trojan.LdPinch
6. Bot.Gbot *
7. Trojan.VBInject *
10. Trojan.TDSServ *

* Capable of stealing information.

BE SECURE, BE UNIQUE.

CHANGE YOUR Pa55w*r*rd

All PID, Hokies, and production Oracle/Banner passwords are required to be changed annually.

Virginia Tech
Invent the Future®