

# Information Technology



# Quarterly

Vol. 9 No. II

Second Quarter 2007

Edwin Poisson, Director, Information Technology

## New Service Center System Makes Requesting Support Easier

by Norma Miller, Internal Services

As part of an ongoing effort to improve services to its customers, on April 30, 2007, Information Technology (IT) launched a new web-based Service Center System. When completely implemented, the new system will act as a repository for all customer support requests. The new system uses the Information Technology Infrastructure Library (ITIL) as its foundation.

ITIL is an internationally accepted best-practices framework for providing Information Technology services. First introduced during the late 1980's in the United Kingdom, ITIL offers IT organizations guidance on how to standardize and optimize services for its customers. The heart of ITIL focuses on restoring or providing service to customers as quickly as possible. So, what are some of the best-practices associated with the new Service Center System?

**Enhanced Customer Access.** ITIL asserts that the quicker service requests are recognized by IT, the faster the service can be provided or restored. Therefore, providing additional methods for capturing service requests can quicken restoration of service. With the new system, customers can still call the IT Service Center, send an email, or now log their request directly into the Service Center System.

As a web-based system, the new Service Center System provides customers with the ability to login and add service requests or check on the status of existing requests. An online procedures manual is available from within the system to guide customers. Service requests include change orders, defined as requests to add new services (formerly known as work orders or CSAs) or incidents, defined as requests to repair non-functioning services (formerly help desk tickets or calls).

Oakland County employees, Court and Law Enforcement Management Information System (CLEMIS) system administrators, and Access Oakland business customers have Service Center System access through the Self-Service module. The system synchronizes regularly with source systems (e.g., County employees with PeopleSoft HR, Access Oakland Business Account Customers with Access Oakland) so that contact information for these customers is always current. In order to gain Service Center System access, City, Village, and Township (CVT) employees register online for an account.

As of the drafting of this article, 248 customers have logged incidents using the Self-Service module. Thanks to the following customers for being the first to use Self-Service: Diane Bannick from the

Prosecutor's Office for submitting the first incident; Caryn Thompson from the Health Division for submitting the first change order; and Robert Scripture from Equalization for submitting the first change order electronic sign-off.

**Enhanced Communication.** ITIL asserts that when it comes to service support "no news IS NOT

### Inside

<i>New Service Center System Makes Requesting Support Easier</i> .....	1
<i>Odds &amp; Ends</i> .....	2
<i>Venturing Into "The Wild"</i> .....	3

Continued on next page

## ***New Service Center System... Continued from page 1***

good news.” Two-way communication between IT and its customers is essential to faster service restoration and expectation realization.

The new system automatically notifies customers when a request is logged as well as when IT closes the request. Through the use of Self-Service, customers have the ability to monitor progress of their requests online. In addition, the new system sends satisfaction surveys to customers asking about the quality of the service received.

**Knowledge Base.** ITIL asserts that the earlier relevant information reaches those who can resolve the situation; the faster the situation can be resolved. ITIL has established a benchmark to challenge IT organizations to reach an 80% first call resolution rate – resolving 80% of incidents with the first contact at IT. Now that’s a benchmark all can look forward to attaining!

To facilitate first call resolution, the new system has a state-of-the-art Knowledge Base. The Knowledge Base is a database of how-to, technical, frequently asked questions, and general information documents. Not only is the Knowledge Base available to IT staff, it is available through Self-Service to customers as well.

These are just a few of the service enhancements made available through the deployment of the new Service Center System. If you have any questions, please don’t hesitate to contact the Service Center at 248-858-8812 or better yet, log in to the new system and try it! County employees login through OakSource by clicking on the Help tab. Other customers login through the [sc.oakgov.com](http://sc.oakgov.com) URL.

---

### **Odds & Ends**



A nursery school teacher launched into her lesson about the upcoming Fourth of July celebration. She stood in front of the class to give them an overview of patriotism and said: “Class, America is truly a great country.” She paused to let her words sink in, and then continued. “And one of the best things about this country is that we are all free.”

One boy stood up in the classroom and declared, “I’m not free, I’m four.”

*-As retold from 101July4th.com*

### **Halfway Point of 2007. July 2.**

At noon, 182 days of the year have elapsed, and 182 remain before Jan. 1, 2008.

### **Declaration of Independence Approval and Signing Anniversary. July 4.**

The Declaration of Independence was approved by the Continental Congress. “Signed by Order and in Behalf of the Congress, John Hancock, President, Attest, Charles Thomson, Secretary.” The official signing occurred Aug. 2, 1776. The manuscript journals of the Congress for that date state: “The Declaration of Independence being engrossed and compared at the table was signed by the members.”

### **On signing the Declaration of Independence**

There, I guess King George will be able to read that!

*—John Hancock (on his boldly written name on the document)*

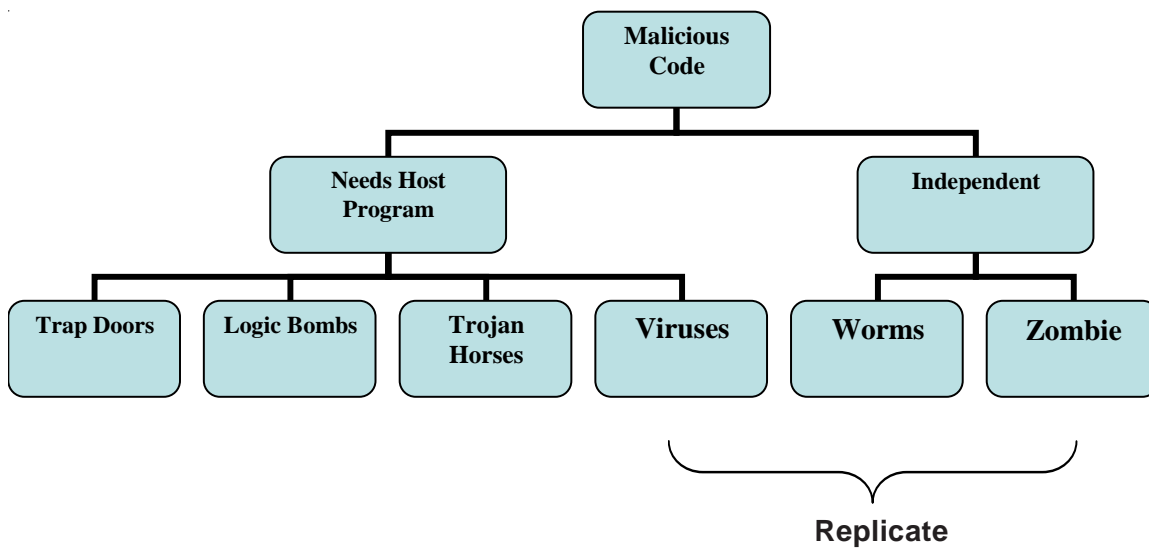
## Venturing Into “The Wild”

by Ken Jaworski, *Technical Systems and Networking*

In data security lingo, the public world outside of a company’s internal data communications network, which includes the Internet, is often referred to as “The Wild.” *The Wild* is typically the source and the method of propagation and transportation of software written by individuals that hope to negatively affect the confidentiality, availability, and/or integrity of electronic data and information.

Although the biological term of virus is often used, it is important to know that this term is an often misused generic term to represent the hostile “flora and fauna” of malicious software found in *The Wild*. In fact, there are many instances of malicious software that defies the definition of an electronic virus. So when speaking in a generic-broad sense, rather than using the term virus, it is more correct to use the term “malicious code.” Malicious code refers to any unwanted code/software which modifies or destroys data, steals data, allows unauthorized access, exploits or damages a system, or does something that the user did not intend to do. A computer virus is just one of many types of malicious code, and just like a biological virus, the method of detection and cure differs from other forms of malicious code.

In 2004, information security writer Mohammad Heidari in his paper, “Malicious Code in Depth,” introduced a classification and naming system for the various malicious codes found in *The Wild*.



Malicious code branches out into two areas. One branch of code needs a host program to operate. The other branch is independent of programs in the environment that it has contaminated.

A **Trap Door**, just like the name implies, is a secret entry point into a program that allows someone that is aware of the trap door to gain access without going through the usual security access procedure. At times a trap door will be installed by the application developer or maintenance programmer. However, a trap door can also be installed by someone gaining entry through either unauthorized external or internal access.

A **Logic Bomb**, is not a real bomb, but rather a metaphor of a program that is triggered and causes damage in an electronic sense. It is code embedded in some legitimate program that executes when a certain predefined event occurs. The event can be date triggered, or triggered by other means such as the processing of someone’s identification number. These codes are secretly inserted into an application or operating system and cause it to perform some destructive or security compromising activity.

A **Trojan Horse** acts just as the term implies. The name was borrowed from the legend of the Greeks presenting the citizens of Troy with a large wooden horse in which they had secretly hidden their warriors. During the night, the warriors emerged from the wooden horse and overran the city.

*Continued on next page*

## ***Venturing Into “The Wild”... Continued from page 3***

An electronic trojan horse masks its identity as a seemingly useful, or apparently useful program or command procedure, containing hidden code that when invoked performs some unwanted or harmful function. The key here is that the integrity of the system or applications is put at risk due to the unwanted code.

A **Zombie** refers to a machine that has been “entered” or is under the spell or influence of a third party. It is a program that secretly takes over another internet-attached computer and then uses that computer to launch attacks that are difficult to trace to the zombie’s creator. Most owners of a zombie computer are unaware that their system is being used in a malicious way. According to, “Spam Slayer: Slaying Spam-Spewing Zombie PCs,” a past article in PC World, in 2005 an estimated 59-80% of spam was being sent by zombie computers.

A **Virus**, in its true sense of the term is a classic example of a program that mimics biological life. A virus is a program that can ‘infect’ other programs or hosts by modifying them. The modification can include a copy of the virus program, which can then go on to infect other programs. A virus can do anything that other programs do. The only difference is that it attaches itself to another program and executes secretly when the host program is run. Once a virus is executing, it can perform many functions such as erasing files and programs. These were the first forms of malicious code. Although any sort of malicious code on a workstation is often referred to as a virus, in many instances the malicious code is not, in fact, a virus.

**Worms**, although less known, cause more damage in terms of network outages or denial of service attacks than any other form of malicious code. A worm is a self-replicating stand-alone program that exploits security holes to compromise other computers and spread copies of itself through the network.

Unlike viruses, worms do not need a host. Because of the recursive structure of this propagation, the spread rate of worms is very fast and poses a big threat on the Internet infrastructure as a whole. The worm consumes all of the network’s resources, preventing any other forms of communication from passing through causing what is referred to as a “denial of service” attack.

In *The Wild*, there are all sorts of approaches being taken in an attempt to compromise the data and information on County workstations, servers, and the network. Rest assured Oakland County’s Department of Information Technology is in a constant battle to ensure malicious code in *The Wild* stays there and does not enter the internal network. If it does, it is immediately detected and removed. The approach of that detection and removal depends on what sort of code it is, which is why it is so important to be knowledgeable of the malicious code taxonomy.

The Department of Information Technology has implemented a sophisticated layered approach, or as we call it “defense in-depth,” to securing the County’s Information Technology infrastructure. Although this defense in-depth is in place, the last and most important line of defense is its users. If while operating your County workstation, you notice it exhibiting strange behavior, by all means don’t hesitate to contact the IT Service Center at 248-858-8812. It’s always better to “call the doctor” and be safe rather than sorry.

### ***Information Technology Quarterly***

***Editor:***

*Vickie Worrell*

***Assistant Editor:***

*Danielle Randall*

***Contributing Writers:***

*Norma Miller*

*Ken Jaworski*

***Published by:***

***Oakland County***

***Department of Information Technology***

*1200 North Telegraph Road*

*Pontiac, Michigan 48341-0421*

*Phone: (248) 858-0810*

*© 2007*

*Visit Oakland County’s Home Page at*

*www.oakgov.com*

*This newsletter is designed to share useful technology news and information with Oakland County Employees!*

*For comments, views, and suggested topics*

*please contact Vickie Worrell at*

*worrellv@oakgov.com*