

## Network Security Case Study

A security breach has just occurred on your corporate network. It could be a virus or worm that is spreading quickly; it could be an unauthorized wireless access point that was just plugged into the network; it could be an insider logging into the corporate mainframe and stealing intellectual property.

The reality is that every Internet-connected network will come under attack eventually and, unless your enterprise is extremely unusual, one of those attacks will eventually succeed. Okay, now what? How will your network staff (or security staff if you're lucky enough to have one) deal with these and other threats?

This case study examines how one company used eTelemetry's Locate product to deal with three different security incidents that occurred during a single week.

### Sarbanes-Oxley Compliance

Since this company is publicly traded, it is required to maintain ongoing compliance with the Sarbanes-Oxley Act of 2002. In order to meet its compliance obligations, the company implemented eTelemetry's Locate product as part of its security infrastructure and controls.

*Locate also provides a way to assess the effectiveness of the company's security controls.*

Locate provides the company with additional layers of security controls or "defense-in-depth" by identifying unauthorized users on the network, unauthorized access points, and users flagged by internal IDS systems.

Locate also provides a way to assess the effectiveness of the company's security controls as required by the Act through the historical records of user-to-IP address mapping. This historical mapping is critical for effective auditing, assessment, and forensics analysis of the company's security systems.

### Company Background

The company in this case study, like many companies, has a network that has grown over time to meet the ever-changing needs of the users. The company headquarters is located in the suburbs of Washington, DC. It is a campus environment with three buildings and 800 users. There are regional offices in Philadelphia with approximately 200 users, Pittsburgh with 175 users, Atlanta with 350 users, and Boston with 475 users for a total of 2,000 employees.

All the remote offices are connected to headquarters via WAN. All of the offices have at least one wireless access point and several of the offices have three or more. Each office has its own local Internet connection.

The headquarters campus supports an older IBM mainframe that runs several legacy applications, including the accounting



system. The mainframe is accessed by a variety of staff at headquarters and in each of the regional offices.

The vast majority of the workstations are of the Windows variety (2000 and XP). There are a small percentage of Linux workstations but the exact number is unknown. The graphics department uses Macs and most are located in one office. However, a few secretaries in some of the regional offices also use Macs.

Static IP addresses are typically assigned to common resources and DHCP is used for workstations. When the network was originally designed, IP subnets were assigned to different offices and departments. However, over time and as the network grew, this subnet organization has broken down. Over the last several years IP subnets have been assigned and reassigned without any regard to department or location.

The networking staff has employed all of the standard security practices one would expect to find at most organizations of this size. All connections to the Internet are protected by firewalls and network intrusion detection systems. All of the workstations have virus-scanning software and a central console is used to push out signature updates. Workstations and servers are generally kept up-to-date with patches and service packs.

## **Security Incident #1: Virus Infection**

### **Scenario**

The first security incident of this week began on Tuesday evening when the network administrator received an alert from the central virus console reporting that approximately five percent or about 100 machines had been infected with the latest virus. The virus console listed the IP addresses of the infected machines.

### **The Challenge**

The network administrator was faced with the challenge of quickly identifying, locating, and disabling the switch ports of the 100 infected users so that appropriate measures could be taken before the virus spread throughout the enterprise.

### **The Solution Before Locate**

The network administrator may have tried several different techniques to locate the infected users including logging into and querying routers and switches. Once he located the appropriate switch or switches, he would then physically go to the switch and identify the port and trace the wire to the workstation. This process would have been even more difficult if the workstation happened to be located in a regional office.

This process is unproductive, costly, and time consuming. Additionally, it assumes some empirical knowledge of the network architecture. A new network administrator who did not possess knowledge of the network topology would have a much more difficult time locating the infected workstations.

It can take up to 45 minutes per workstation for a potential total of 75 hours to locate and identify the infected users using this approach.

### **The Locate Solution**

The network administrator simply logged into the Locate web console and looked up the IP addresses of the infected workstations. He was presented with the name, location, and phone number of the infected users. He was then able to immediately call each of the users, notify them of the situation, and disable their switch port. Appropriate steps were taken within minutes to fix the problem before other workstations were infected. The process to identify and locate all 100 users took less than 10 minutes.

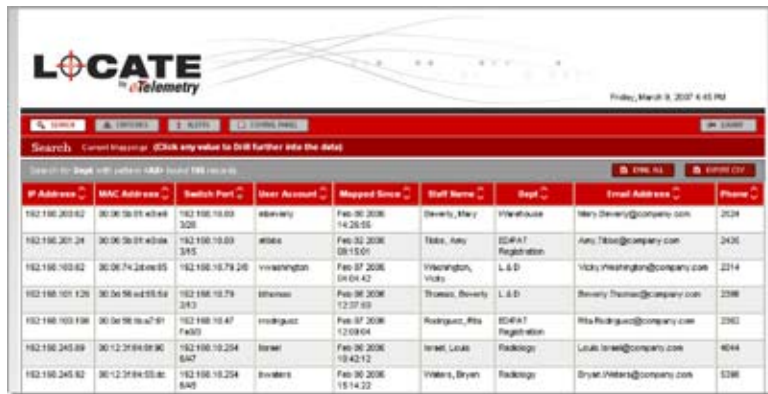
*Appropriate steps were taken within minutes to fix the problem before other workstations were infected. The process to identify and locate all 100 users took less than 20 minutes.*



## Cost to Identify IP addresses and Switch Port

Although it is nearly impossible to assess all of the costs associated with virus attacks, the immediate cost of locating and removing viruses can be easily quantified. Assuming the network engineer's yearly salary is \$75,000 and he spent 75 hours searching for the infected workstations, the loaded labor cost of responding to this incident would have been approximately \$3,750.

Using Locate the network engineer was able to identify the workstations in approximately 10 minutes for a total cost of approximately \$6.00. Because the network engineer was able to locate the workstations quickly, further infection was avoided resulting in additional



The screenshot shows the LOCATE Telemetry interface with a search bar and a table of network data. The table has columns for IP Address, MAC Address, Switch Port, User Account, Mapped Since, Staff Name, Dept, Email Address, and Phone. The data is as follows:

IP Address	MAC Address	Switch Port	User Account	Mapped Since	Staff Name	Dept	Email Address	Phone
192.168.203.62	30:36:50:01:40:68	192.168.10.03 320	abewery	Feb 30 2008 14:28:55	Bewery, Mary	Warehouse	Mary.Bewery@company.com	2124
192.168.201.24	30:36:50:01:40:68	192.168.10.03 345	elias	Feb 02 2008 08:15:01	Elas, Amy	IT/HR	Amy.Elas@company.com	2435
192.168.103.62	30:36:74:28:66:65	192.168.10.79 210	vinnington	Feb 07 2008 04:04:42	Vinnington, Vito	L.S.D.	Vito.Vinnington@company.com	2214
192.168.101.126	30:36:50:01:40:68	192.168.10.79 243	thomas	Feb 06 2008 12:37:59	Thomas, Beverly	L.S.D.	Beverly.Thomas@company.com	2288
192.168.103.198	30:36:50:01:40:68	192.168.10.47 F603	rodriguez	Feb 07 2008 12:03:04	Rodriguez, Rita	IT/HR	Rita.Rodriguez@company.com	2262
192.168.245.89	30:12:3F:84:55:4E	192.168.10.204 647	louis	Feb 30 2008 18:42:12	Louis, Louis	Rocklog	Louis.Louis@company.com	4594
192.168.245.92	30:12:3F:84:55:4E	192.168.10.204 649	louis	Feb 30 2008 18:14:22	Waters, Bryan	Rocklog	Bryan.Waters@company.com	5398

time savings and a significant reduction in risk to the rest of the company's workstations.

*Locate automatically maps people to IP address, MAC address, and switch ports in real-time and historically.*

The approximate cost savings to the company to resolve this one virus infection of 100 workstations was \$3,750.

According to network-protection firm Internet Security Systems (ISS), the number of security events detected by companies in the first quarter of 2003

jumped nearly 84 percent over the preceding three months. Based on this trend and the seemingly continuous supply of new virus and worm threats, most companies can expect multiple attacks each year. If we assume that this company is attacked five to six times within a year, the immediate savings directly resulting from Locate may be as high as \$22,500 annually. Of course the savings will potentially be higher since this number does not include the more difficult to quantify costs such as lost worker productivity and potential data recovery costs.

## Security Incident #2: Rogue Wireless Access Point

### Scenario

A salesperson that frequently holds meetings in a conference room near his office was frustrated by the lack of available network connections for meeting participants. He decided to pick up an inexpensive wireless access point at his local electronics store. On Wednesday morning he unboxed and plugged the wireless access point into an available network connection in the conference room. To his amazement, he was able to connect to the network with his wireless card. The salesman didn't consider that the conference room was next to the parking lot, making the access point available to the public.

### The Challenge

What the salesperson had unwittingly done was opened up an unsecured channel directly into the company's network, bypassing all of the perimeter security including firewalls and intrusion detection systems. Anybody with a wireless network card in proximity to the conference room could have gained access to the network. Furthermore, the network could have been accessed from the parking lot without the need to gain physical access to the building.

### The Solution Before Locate

Prior to the installation of Locate there was no easy way for the networking staff to locate unauthorized wireless access points. Therefore, the network staff would walk the halls

at the headquarters campus once a week with a wireless equipped laptop searching for unauthorized access points. This process took one network engineer approximately three hours per week.

Additionally, network engineers would physically scan the regional offices once a month. Each of these scans would take approximately two hours.

### **The Locate Solution**

With Locate running on the network, the network administrator was instantly alerted to the rogue wireless access point. Upon notification, the network administrator was able to take immediate action to disconnect the unauthorized access point. The wireless access point was located and removed from the network less than one hour after it was initially connected.

### **Return on Investment**

As in scenario #1, we assume the network engineer's yearly salary is \$75,000 and he spent three hours per week for 52 weeks per year scanning for unauthorized access points at the headquarters campus. Additionally, he spent two hours per month physically scanning each of the four regional offices. This works out to 252 hours per year spent on this activity for a total loaded labor cost of \$12,600 annually.

*The wireless access point was located and removed less than one hour after it was initially connected.*

Using Locate the network staff is now able to avoid the manual scans since Locate constantly watches for new nodes and access points. By avoiding manual scans, the company can expect an approximate annual cost savings of \$12,600.

## **Security Incident #3: Insider Theft of Intellectual Property**

### **Scenario**

The last security incident of this week occurred on Friday morning. The security administrator received an alert from the intrusion detection system (IDS) in the Boston office that indicated suspicious activity originating from that office directed at the company mainframe system. The workstation IP address was available in the IDS logs. The security administrator reviewed the access logs from the mainframe and confirmed that the suspicious activity reported by the IDS needed to be reported to the Vice President of Information Security.

### **The Challenge**

The security administrator needed to identify which user was associated with the IP address at the time of the suspicious activity. The only information the security administrator had was the IP address reported by the IDS.

### **The Solution Before Locate**

The security administrator logged into the Locate web console and input the IP address and dates from the IDS log. Locate looked up the historical information for the time period in question. He was immediately presented with the name, location, and phone number of the user who was using the workstation to log into the mainframe. Within seconds the security administrator had the information he needed to make his report.

### **The Locate Solution**

The security administrator logged into the Locate web console and input the IP address and dates from the IDS log. Locate looked up the historical information for the time period in question. He was immediately presented with the name, location, and phone number of the user who was using the workstation to log into the mainframe. Within seconds the security administrator had the information he needed to make his report.



## Return on Investment

It is clear that the theft of intellectual property is costly and all companies should take steps to avoid it. Locate speeds time to identify user of offending machine. When two theft losses are investigated each month at 10 hours per investigation the total loaded labor cost would be \$12,000. Locate can provide historical IP address usage in a matter of minutes.

## Summary

The total loaded labor cost for managing security incidents depicted in this document for a 2000 employee company could potentially reach \$47,000. The true value of Locate is realized by reducing these loaded labor costs to near zero. Locate replaces the labor and time intensive tasks of identifying, locating and disabling IP addresses and switch ports with an intuitive, easy to use network appliance.

## About Locate

Locate is a network appliance that automatically links network addresses and switch ports to an individual and their name, location, phone number, and email address. Based on a proprietary algorithm that analyzes network traffic, eTelemetry's patented mapping engine does not require the installation of an agent or client software on the networked device. The information is accessible through Locate's web client or it integrates with IT service, asset, and network management applications via an external API. The network appliance can be implemented in less than an hour. Locate provides knowledge of who is on the network at all times, where they are connected, and where they are physically located.

## About eTelemetry

eTelemetry is the leader in extracting real-time business information from network activity. eTelemetry's innovative products tell you everything about the people on your network, answering the who, what, where, when, and how much. By applying its proprietary technology, eTelemetry's award-winning products provide information leading to increased productivity, risk identification, reduced costs, greater E911 compliance, improved network efficiencies, and insights into how people collaborate. Since 2004, eTelemetry has been Turning Network Traffic into Business Intelligence™.

Contact eTelemetry

**eTelemetry**

Turning Network Traffic into Business Intelligence

41 Old Solomons Island Road • Suite 202 • Annapolis, MD 21401  
Phone: 888-266-6513 • Fax: 410-266-0796 • [www.eTelemetry.com](http://www.eTelemetry.com)

