



The Case of the *Uninvited Guest*

This series, a part of MITRE’s Cyber Awareness Program, recounts security-related incidents that have taken place at MITRE and that help educate employees on their responsibilities and best practices. The stories show the risks and threats we face to keep both MITRE and our customers secure.

It was a beautiful New England August morning, recalls a MITRE Information Security (InfoSec) engineer. So he elected to go outside to walk over to the MITRE cafeteria from his office in <name of> Building. As he approached the cafeteria, he noticed a man on the outside patio, apparently talking on a cell phone.

As he passed the man, the employee remembers, “I noticed a badge, but it was turned around so I could not see the front. I assumed he was a MITRE employee, based on where he was and the way he was dressed, ‘business casual.’ “

As the MITRE employee approached the automated access door to the cafeteria, he realized the man had gotten in line right behind him. After swiping his badge and entering his PIN, the employee stepped into the intermediate booth between the two sets of doors. It was only when the sliding door closed behind him and the man spoke up, saying, “I hope it’s okay that I’m coming in with you,” that the MITRE staffer realized the man had entered the booth with him.

“I was surprised and alarmed,” the employee relates. “So I replied, ‘No, it is not okay. You’re not supposed to do that.’ I was quite perturbed but still thinking he was a goofy MITRE guy.”

Our co-worker stepped into the cafeteria, but kept an eye on the man. “He was act-

ing distracted, looking at his phone, kind of wandering,” the MITRE staffer recalls. “I said to myself, ‘Should I let him go or not?’ I decided to do something.”

The man left the cafeteria and entered the <name of> Building hallway. The employee walked up to him and told the man he would feel better if the man ‘badged in.’ The man said, “Okay, sure.”

Tailgaters wait for someone with access to enter a controlled area, and then follow the authorized person through the door.

“I walked him over to the Guard Desk, went up to the guards and said to them that this guy had ‘tailgated me’ and needed to badge in,” the MITRE worker recounts.

The guards asked the man if they could help him, and he replied that he had a meeting with an employee (the name he provided later turned out to be fictitious). The guards

challenged him for an ID, and the man said he had it in his car. The man then returned to his car and quickly drove off the campus.

Tailgating or “piggy backing” is one of the most common methods malicious outsiders use to physically access buildings without authorization. Tailgaters wait for someone with access to enter a controlled area, and then follow the authorized person through the door.

“Tailgaters are a threat to our security and business,” states MITRE’s Corporate Security Manager. “We all need to be aware of the possibility that someone might attempt to tailgate us when we enter MITRE through a card access door.”

The employee “did the right thing, didn’t just ignore the situation,” the Corporate Security Manager adds. “Employees should be aware that this could happen to them and that if it does, they should escort that person to the

reception desk and that if he or she takes off, they should call the Security Control Center. We rely on the employees to guard against this.”

In fact, even allowing another employee to tailgate or piggy back when you enter or exit a building via a card access door or booth is not permitted, the security manager notes.

Based on his experience, the MITRE staffer says, “I’ll be more vigilant about checking into things that don’t seem to be right. You don’t want to come across as a jerk, but after this, I won’t be shy about approaching people if I sense something is wrong.

“I made a couple of assumptions that maybe I shouldn’t have made,” our co-worker continues. “Should we talk to folks if their badge is turned around or inside their breast pocket? Maybe we should. We all have a shared responsibility to keep MITRE secure.” □

Contact: For more information on this and other MITRE cyber awareness publications, see www.mitre.org/work/cybersecurity.html



MITRE InfoSec



MITRE True Story Series

The Case of the *Averted Cyber Attack*

This series, a part of MITRE's Cyber Awareness Program, recounts security-related incidents that have taken place at MITRE and that help educate employees on their responsibilities and best practices. The stories show the risks and threats we face to keep both MITRE and our customers secure.

“To paraphrase the title of the Spike Lee movie (Do the Right Thing)”, says a member of MITRE Information Security (InfoSec), “the employee did the right thing.”

An email laden with malware had been sent to 15 employees, including an Associate Department Head (ADH) at MITRE. The ADH had previously attended a MITRE InfoSec threat briefing. As a result of her heightened awareness of threat indicators, she reacted promptly to this latest attack by contacting the MITRE Corporate Help Desk. She also got word out to her colleagues about the email because she thought they, too, might be targets of the same email attack.

The incident occurred in mid-March, when the <site office>-based ADH received an email ostensibly from a cleared defense contractor supporting the <name of sponsor>. “I didn’t recognize the name of the sender, but she was supposedly at <name of sponsor>, which we work with, and the subject of the email was familiar, and the name of the attachment made sense,” recalls the

ADH. So what made her dubious about its authenticity?

“As I read the email itself I noticed there were slight syntactical errors and odd phrasing, as if the email had been written by a non-native English speaker. In addition, the

email text was very short and reminded me of the phrases I’ve seen in spam, trying to get me to go to a pharmaceutical or investment site. So my radar was up.”

The suspicious MITRE employee hit the email reply-to button and noticed that instead of replying to xxxxx.mil the email was replying to an army.mil address. “That was three in a row,” she says.

Even though the virus scan she had run on the attachment had failed to detect anything amiss, she immediately forwarded the email, without opening its Word attachment, to the Help Desk.

MITRE InfoSec was contacted. Along with the newly created Security Operations Center (CSOC), they determined that the spoofed email came from a compromised system and that the Word document was laden with a

... she immediately forwarded the email, without opening its Word attachment, to the Help Desk.

(continued...)

MITRE InfoSec Threat Awareness Briefings

MITRE InfoSec briefs groups on cyber threats such as the one described in this month's feature story. If you feel your program or project is a potential target, we can give you an in-depth briefing on the threat picture that is relevant to you. To arrange a briefing email us.

Trojan Horse program that was so new it had not been detected by the anti-virus filters on our email gateway, servers, or desktop client. This was a zero-day attack, for which no patch was yet available.

A targeted 'spear-phishing' attack

MITRE InfoSec determined the malware-laden email had been sent to 15 current employees who support related programs. They informed the ADH that the email was indeed malicious, and started contacting the other employees. She did the same, utilizing a shared email distribution list to make her colleagues at other locations aware of the targeted attack. "I knew others in my group might have received the email and didn't want them to be fooled by the genuine-looking nature of the email," she explains. "None of us want cybercriminals or cyberspies to steal the contents of our computers or to embed their malware so deeply that we end up having the hard drives of our computers 'wiped.'"

Further investigation revealed that a previous mailing from the same compromised email address had been intercepted by MITRE's email gateway filters a few days earlier. This email included a link to a zip file that contained four "Trojanized" .exe (executable) files disguised as valid-looking <name of sponsor> briefings. The hidden .exe files were designed to bury themselves in the recipient's hard drive and to "beacon out" the user's keystrokes to a command-and-control server out on the Internet. "A common practice in these targeted spear-phishing attacks," notes the MITRE InfoSec member, "is to send multiple email messages with multiple attachments, each with customized malware to increase the odds of one of them making it through our defenses."

Just as insidious, he states, is the fact that the documents were all from a <name of sponsor> technical exchange held last year and were not publicly available. "In other words, these were 'real' <name of sponsor> documents that included the names and emails of attendees, by which an Advanced Threat Actor was able to launch a well-crafted email designed to get targeted MITRE people to click and open it." Fortunately, none of the email recipients' systems had been compromised.

Sharing lessons learned and the "big picture" with employees, sponsors

"The important lesson is, this wasn't a 'one-off,'" comments the MITRE InfoSec member. "If you get one of these targeted emails, you're bound to get another like it in the future, even 18 months down the road. They've got you on their target list; they'll be back. But we put you on our 'at-risk' list. Our targeted threat awareness briefings will enable you to spot these threats and know what to do should they make it through our defenses."

What to do in the event of a targeted phishing attack?

If you suspect that you are the target of a spear-phishing attack:

1. Do not open the email attachment or click on any link contained in the message body.
2. Do not reply to the email message.
3. If possible, call the sender to verify the email is legitimate.
4. If it is not legitimate, or you cannot verify its authenticity, contact the MITRE Corporate Help Desk and indicate you have received a seemingly targeted, suspicious email message.

MITRE InfoSec, in turn, learns a lot from the audiences of these threat briefings, he adds. “Employees have provided great suggestions about preventative methods and best practices. The briefings are an opportunity for us to create relationships, learn how employees work with sponsors, and even how we can forge relationships with others in the sponsor community. They help us share our findings with <name of sponsor> and other investigative groups, which in turn helps them to understand the big picture of what is going on.”

By the very nature of MITRE’s work and support for our many sponsor programs, we are seeing more of these targeted attacks, the MITRE InfoSec member says. “This is a growing concern,” he states. “But the key point is how useful these threat awareness briefings can be. I wish we could automate the MITRE ADH and her kind of threat awareness intelligence. We depend on our employees for our security, on the individual who detects the odd system behavior or suspicious email and contacts the Corporate Help Desk. In my opinion, she was the employee of the month.” □

Contact: For more information on this and other MITRE cyber awareness publications, see www.mitre.org/work/cybersecurity.html



MITRE InfoSec



MITRE True Story Series

The Case of the *Midnight Eavesdroppers*

This series, a part of MITRE's Cyber Awareness Program, recounts security-related incidents that have taken place at MITRE and that help educate employees on their responsibilities and best practices. The stories show the risks and threats we face to keep both MITRE and our customers secure.

It was a cold early winter evening just after midnight. While making their rounds, Corporate Security staff observed an unmarked, white van parked at the top of <name of> Drive, near the front of the MITRE <name of> building. On closer inspection they saw two occupants in the van, one of whom appeared to be working on a laptop computer.

Security walked up to the van and asked to see the occupants' identification and why they were parked there. The men in the van readily replied that they were testing cellular service for a local carrier. The Security reps walked back to <name of building> and called the local carrier company for confirmation of the story; it was untrue. While they were inside the men in the van drove away.

Was it a case of "wardriving," a deliberate attempt to scan MITRE's wireless access points? MITRE Security wasn't taking any chances, and contacted MITRE Information Security (InfoSec) and Information Systems, Infrastructure & Services (ISIS), who then started a security review and audit.

ISIS staffers measured the signal strengths in the <name of building> and <name of building> parking lot areas using a wireless detection tool to determine which MITRE wireless network access points (APs) were reachable from the van's location. Both the wireless

Every employee 'an extension' of our security program

"In looking back, we can't be sure, but suspect this was a case of attempted wardriving by the men in the van," says MITRE's Director of Corporate Security. "It serves as a reminder that employees can — and often do — play a vital role in serving as eyes and ears for Corporate Security. We have just a handful of Security folks, most of whom are restricted to certain work areas," he points out, "but there are many employees who are out there in our parking lots and walking around our buildings. They can supplement us, and often are our best source of security information. Every employee is really an extension of our security program.

"Employees quite often report someone sitting in an idling car in a MITRE parking lot looking at a laptop, or a visitor trying to get in a side door, claiming to be lost," he continues. "Usually, the person in the car is an employee looking up driving directions, and the visitor is indeed lost. But that is not always the case.

(continued...)

Going Wireless at home?

MITRE InfoSec and the MITRE Institute offer clinics on securing your home wireless network.

What to do should you see a suspicious vehicle or person

“If you see a suspicious vehicle or person, don’t approach them yourself,” the director cautions. “Instead, contact our 24-hour Security Control Centers. We have procedures and protocols in place for approaching them. We also notify law enforcement for possible backup when we have an unknown vehicle on our campus, and provide them the license plate of the vehicle as well. So if you see a car or person loitering in the parking lot or near a MITRE building, please notify us!”

In an emergency, call...

In an emergency, call the following numbers

(Consider adding this to your phone’s speed dial.)

<Location>- ext. xxxx.

<Location>-- ext. xxxx

<Location>- -xxxx

Sites - your Site Security Rep.

You will automatically be connected to Security and Health Services representatives.

Connecting to MITRE remotely?

When working away from MITRE with your MITRE laptop, we urge you to use <name of product> to securely connect to the MITRE network. This is especially true when you are connecting to MITRE from a public venue, such as an airport, hotel or coffee shop. Your traffic is visible unless you use <name of product>. And make sure after connecting to any free wireless networks (like at airports), that you disable ad hoc peer-to-peer network sharing when you get back to MITRE. Call the MITRE Corporate Help Desk if you need assistance.

device and system security logs were also reviewed for weekend wireless connections, especially to determine whether an attempt had been made to penetrate MITRE’s wireless networks: no such effort had been made.

“MITRE’s wireless networks are isolated from the corporate network. So even if an outsider had been able to connect to one of our wireless networks, they still wouldn’t be able to access the corporate network without having <hyperlinked name of product> and <hyperlinked name of product>,” points out one of the ISIS staffers.

Nonetheless, the incident reinforced ongoing efforts by ISIS and MITRE InfoSec to protect MITRE’s wireless networks. Recent and planned upgrades include:

ISIS now has a real-time, automated alert system to detect attempts to penetrate MITRE’s wireless networks. MITRE is moving from <name of encryption> to <name of encryption> this year to ratchet up encryption protection for our wireless networks. Long-term plans are to migrate to <name of encryption method>.

As a reminder to employees, if an AP is found to be operating within MITRE without MITRE InfoSec authorization, the device will be disabled. Please note that willful violation of MITRE Security Procedures is cause for disciplinary action.

“We’re now much better positioned to identify potential security threats,” states the ISIS staffer, “and are alerted when unauthorized APs show up in our wireless frequency spectrum.” □

Contact: For more information on this and other MITRE cyber awareness publications, see www.mitre.org/work/cybersecurity.html



The Case of the Unexpected eTicket Charge

This series, a part of MITRE's Cyber Awareness Program, recounts security-related incidents that have taken place at MITRE and that help educate employees on their responsibilities and best practices. The stories show the risks and threats we face to keep both MITRE and our customers secure.

The content of the email appeared legitimate,” recalls the MITRE executive. “What was interesting about this email was that it triggered a natural human reaction. It was telling me it was billing my account for \$467.50, which is consistent with an airline ticket cost, and it was from a carrier I’ve flown on in the past. But I was being billed for a reservation I had not made. Human nature makes you want to click, to try to get this thing resolved.”

But rather than click the email’s attachment as directed, he thought twice, and instead reported the email, thus helping to alert his fellow employees to a malicious Trojan Horse spam email that was responsible for stealing 1.6 million records from Monster.com last year alone.

The so-called “eTicket” attack occurred in late July. Some 1,700 of these emails hit the MITRE email servers, with 36 making it through our anti-spam filters to employee Inboxes. In some cases the alleged sender was JetBlue airlines, in other cases Delta or Northwest. The bogus emails posed as ticket invoices.

So what was it about this email that caused the MITRE executive to be suspicious?

“There were two clues,” he says. “The first was the return address. The email said it was from JetBlue, but the return address was so-and-so@overboardart.com rather than so-and-so@jetblue.com. The second clue was the relatively small size of the attachment, which just didn’t feel right. It was very small, measured in bits. This provoked me to report it, as I had never heard of this kind of attack before.”

... rather than click the email's attachment as directed, he thought twice, and instead reported the email.

As a result of his report, the corporate email filters were updated and an alert went out from the Corporate Help Desk to tell employees to delete the email if they received it. End of story? Not really.

“If the email hadn’t been so sloppy about the return address it would have been even more tempting to have opened it,” states the executive. “And you don’t know what opening that email attachment would have done to me personally and potentially to the company.

“As good as our firewalls and intrusion-detection and virus alert systems are,” he continues, “the key thing is for us to protect ourselves and the company from a malicious attack. Every employee has to be on guard, on the defensive.”

Zero incident culture

“Our values of public service and excellence help guide us in the achievement of our goals to strengthen national security and to enable the enterprise (to name just two of our six goals). So shouldn’t we be striving to create a zero-incident culture, for our sponsors and ourselves?”

- MITRE Information Security Program Manager

Two percent of 14 million equals how many spam emails per week, per employee?

About 98 percent of the spam that tries to enter MITRE is stopped by our spam filters. “In some ways, our filtering of all this doesn’t raise that much attention, since people are getting far more legitimate than illegitimate emails,” the MITRE executive notes. (In fact, MITRE’s spam filters intercept nearly 14 million messages a week.) “If, say, 35 spam emails per week are reaching each of us, that means there are about 2,000 total spam emails coming my way. And if something like one in five of those is malicious, that means of the 35 that make it through, seven are likely to be malicious, attempting to attack me and MITRE in some fashion.

“We do a very good job blocking spam as a corporation,” he continues. “But our corporate defenses can never be perfect, which is why we all have to be suspicious, and to err on the conservative side if there is any question of origin or content. Delete has become my favorite button.”

Why not falling for spam is an important task for every employee

“I think we should consider ourselves privileged to hold our customers’ information in our systems,” states the MITRE executive. “As much as we need to protect our own information, we need to take extra measures to protect the information that has been put under our stewardship. If that’s compromised, we lose trust. And if we lose trust, we’re out of business. That’s why we need to be continually vigilant.

“The point is,” he adds, “we’re going to see more of these kinds of attacks, and they’re going to get more sophisticated. So we need to heighten our attention and awareness of these things, and really pause more often.”

Alluding to our<name of document>, he says this heightened awareness also ties into our <name of> goal. “Key to enabling the enterprise is to make sure you don’t disable the enterprise by allowing an intruder to enter our network or our systems. Our best defense is the 6,000-plus employees we have here, and for each of us to recognize we have an individual responsibility.

“Even if you don’t think you have anything valuable on your computer, the moment someone enters your computer they have assumed the level of trust you have within our organization,” he asserts. “So they can now bounce around freely within the organization. So everybody’s computer is of vital concern to the company. And it’s not just computers, it’s <name of> devices, it’s anything that gets connected to the information infrastructure of this company. It’s amazing how many bad guys are out there. And they know we’re here.” □

Contact: For more information on this and other MITRE cyber awareness publications, see www.mitre.org/work/cybersecurity.html