



NEWSLETTER

Identity Theft 911<sup>®</sup>

VOLUME 4  
ISSUE 9  
SEPTEMBER  
2007

AMERICA'S LEADING IDENTITY THEFT RESOLUTION & EDUCATION SOURCE

THIS MONTH'S TOPIC...

## The Art of War and Data Security

Notes from our Chairman, Adam K. Levin

Hundreds of thousands of job seekers on Monster.com got way more than they bargained for when they received e-mails containing malware instead of job leads. On the surface, it seemed like a garden-variety phishing expedition, but upon closer investigation it's become clear that we're dealing with even bigger issues here: this is the work of organized crime, and we're not equipped to contend with it.

["Worst Ever: Monster of a Breach"](#) dissects the Monster.com assault to reveal the complexities and potential consequences of this case, and what it all means for the larger realm of Internet security. This month's editorial, ["The Monster in the Closet"](#) calls for a unified and steadfast response to the emerging threats. And of course, there are [ways to minimize your risks](#). However, while we as individuals must do our part by managing our own risky behavior, we must also demand that those in charge of the big picture get serious about reigning in our enemies once and for all.

For a complete newsletter archive, visit: [www.identitytheft911.org/newsletters](http://www.identitytheft911.org/newsletters)  
To learn about the latest scams on identity theft, visit: [www.identitytheft911.org](http://www.identitytheft911.org)  
Comments, questions? Contact us: [newsletter@identitytheft911.com](mailto:newsletter@identitytheft911.com)



Monster.com attack holds bigger implications than meets the eye

*Worst Ever:*  
**Monster**  
*of a Breach*

At first, the latest attack on Monster.com seemed like a simple little story. On Aug. 17, the company was notified that hackers accessed computers belonging to hundreds of thousands of its users, encrypted their files, and audaciously demanded \$300 to unlock them. The headline was obvious: "High-profile employment website used for file ransom!"

*Worse, most of the public agencies and corporations affected by the attack ignored warnings about the danger. "They pretty much blew us off,"*

For most media outlets, that was the beginning and end of the story. But strange details lingered. Prevx, the England-based Internet security company that discovered the attack, mentioned that huge corporations and American government agencies were somehow involved. Jacques Erasmus, director of research at Prevx, told anyone who would listen that this seemingly small computer breach was actually "the worst attack I have ever seen."

What Erasmus discovered, and what most news outlets failed to report, was a massive and sophisticated scheme that included stolen access to hundreds of thousands of private bank and credit accounts. It also may have compromised secure computer systems at the U.S. Department of State and major government contractors. This was smarter and more complex than many of the attacks that have come before—and was proof that the art of launching malicious online attacks had evolved.

Worse, most of the public agencies and corporations affected by the attack ignored warnings about the danger. "They pretty much blew us off," Erasmus says.

And here's the scary thing: The attack is continuing right now.

## Anatomy of a scam

The first step in any scam is to find victims. This is where the criminals in the Monster.com fraud truly excelled. They exploited a weakness in the computer system that recruiters use to log in to Monster.com and search for potential job candidates.

"There was a flaw in Monster's system where it was quite easy to access their information," says Erasmus.

Monster.com did not return several phone calls seeking comment for this story.

Armed with access to recruiters' online accounts, the scammers attacked in two different directions at once: individual job seekers; and the giant government and corporate entities for which they worked.

## Job seekers beware

Using stolen usernames and passwords, the scammers logged onto Monster.com's databases, posed as recruiters, and searched large numbers of resumes without setting off Monster's alarms. They stole 1.3 million pieces of information belonging to hundreds of thousands of users, Erasmus says, including names, email addresses, home addresses and Social Security numbers.

Included in the results were hits from USAJobs.gov, the database belonging to the Office of Personnel Management, which hires workers for many federal agencies. Monster.com runs the web site, said Peter Graves, spokesman for the office. According to Graves, of the two million people with resumes on USAJobs.gov, 146,000 had their personal information stolen in the attack. Social Security numbers were encrypted, which hopefully prevented them from being accessed, he added.

Next, the bad guys created an email message crafted to appear as though it came from Monster.com. Unlike many phishing messages, this one was well-written. It contained a convincing copy of Monster.com's logo and included hyperlinks to real websites maintained by Monster.

The only fake link was one described as a "job seeker tool." In fact, this was a Trojan horse. Clicking on it would download a small piece of software that scanned the victim's computer to see which operating system and antivirus programs the computer was running. Then, like an army scout whistling for the cavalry, the program invited larger Trojans designed to evade that computer's specific security settings.

"We call this a staged downloader," says Zulfikar Ramzan, senior researcher on the advanced threat research group at Symantec, the antivirus software company. "The leading edge of the attack is very narrow, and then you build from there."

One of the programs included ransomware. Once downloaded, it encrypted files on the computer, then sent an e-mail demanding the victim pay a ransom or the files would be deleted. The scammers signed off using a swashbuckling name: "The Glamorous Team."

It's unknown whether anyone actually paid the ransom, or how many people have been affected by locked files. Researchers at Prevx tried unlocking the files, which proved nearly impossible because the program used double-encryption. "Which is not very nice," Erasmus says.

*"If someone is really unhappy with their job or without a job, they may not even think about the risks [of downloading unknown software] because the potential opportunity may outweigh it."*

*“File ransom is difficult to do in bulk, so there’s a pretty low return on investment,”*

It’s easy to see why file ransom attracted so much attention. Having personal files held for ransom is a terrifying but easy-to-understand threat. And in this case it targeted users of a high-profile website. But since the first case was discovered in May 2005, file ransom never caught on as a popular tool among thieves. For one, very few victims actually pay the ransom. Also, thieves must establish a means to receive the money, leaving behind a trail of records that could expose them.

“File ransom is difficult to do in bulk, so there’s a pretty low return on investment,” says Don Hubbard, vice president of security and research at WebSense, a San Diego computer security company.

A quieter but far more powerful part of the Glamorous Team’s scheme was to secretly download programs that record victims’ keystrokes, Erasmus says. Whenever victims logged into their credit card or banking accounts online, the thieves watched over their shoulders, recording usernames and passwords. The thieves might have bundled these together with other identity information and sold it to other criminals on the black market, Ramzan says. Or they may have kept all the information to steal money from bank accounts, make purchases using victims’ credit cards, and open new bank accounts in victims’ names.

“They got enough information to do a lot of damage,” says Ramzan.

### **Also part of the package: recruitment**

The purpose of these schemes may be apparent in the Glamorous Team’s last consumer-oriented scam: Posting ads on Monster.com to recruit “money mules”—people willing to launder stolen money. The ads called these workers “Transfer Managers” and boasted, “What we offer you is something more than just a job—it’s the opportunity to earn really big money without having to work much. This job is not a full-time one—you can work from 9 to 5 at some other place and use our service as a source of extra cash—a lot of extra cash we should say.”

Applicants handed over their Social Security numbers and bank account information, Ramzan says. But the truly suspicious part was the requirement that applicants open a new account at Bank of America. Mules would receive money from online funds transfers, deposit it in their new bank account, withdraw most of it and send it to the thieves via Western Union, Hubbard says, keeping a portion for themselves.

Of course, when the bank discovers it's been had, it's the mules, not the thieves, who are left holding the bag.

"You'd have to be really naive to be doing that and not think you're doing something wrong," Hubbard says.

The fact that the Glamorous Team recruited money launderers suggests they probably plundered victims' accounts themselves, instead of selling account information to others, Ramzan says.

"When you see a mule scheme, it's an indication that there's been a lot of money stolen from other schemes that needs to be laundered out of the system," says Ramzan.

### **Glamorous? Maybe. Computer Geniuses? Not Quite.**

Given the sophistication of this attack, it would be easy to assume that the Glamorous Team includes some of the smartest computer programmers in the world. In reality, the software used in the attack was relatively basic.

"I can just send it to you and hope that you open it up," says Ramzan. "That's much simpler than trying to get around your firewalls."

The Glamorous Team also made a major mistake: They forgot to secure their own server. That allowed Prevx to follow the stolen documents to their final destination and observe the types of information the hackers had gained access to.

"That was just a dumb blunder," Erasmus says.

The Glamorous Team was sophisticated in other ways, however. First, bundling so many different scams together was relatively unique, although Internet security researchers say it's part of a growing trend.

"We call this a blended threat," says LaTanya Sweeney, computer science professor at Carnegie Mellon University. "It's becoming increasingly common."

Second, the attack involved a sophisticated play on human emotions. Recruiters using Monster.com receive hundreds of resumes each day by opening attachments, which makes them vulnerable to attacks involving downloads, Ramzan says.

*The Glamorous Team also made a major mistake: They forgot to secure their own server. That allowed Prevx to follow the stolen documents to their final destination and observe the types of information the hackers had gained access to.*

*If they clicked on the Glamorous Team's Trojan, they automatically downloaded software that captured their keystrokes, including passwords to secure intranets and databases.*

Job seekers also make vulnerable marks. "If someone is really unhappy with their job or without a job, they may not even think about the risks [of downloading unknown software] because the potential opportunity may outweigh it," says Dorothy E. Denning, professor of computer science at the Naval Postgraduate School.

Hitting vulnerable people with sophisticated e-mails, the Glamorous Team convinced 20 percent of their targets to download Trojan software, an almost unheard-of success rate (in most scams, a two-percent conversion rate is considered successful, says Erasmus). That meant that they could inflict about 14,000 computers with Trojans with approximately 70,000 emails, rather than the millions that would be required in a traditional scam. This low email volume allowed them to operate underground for weeks before being discovered.

### **The worst may be yet to come**


While the individuals affected by the Monster attack have gotten the most media attention, the Glamorous Team had even bigger targets: Some of the largest corporations and government agencies in the United States. What made these titans vulnerable? Their own dissatisfied workers.

Researchers at Prevx have files, obtained from the Glamorous Team's unprotected server, showing exactly which computers were accessed. They know that some of these machines had keystroke-stealing software secretly installed. But most of the companies, and all of the government agencies, never even bothered to ask which computers were compromised.

"Most of them just told us to get lost," Erasmus says.

All of the recruiters targeted in the attack, and most of the people applying for jobs, accessed Monster.com using their work computers, Erasmus says. If they clicked on the Glamorous Team's Trojan, they automatically downloaded software that captured their keystrokes, including passwords to secure intranets and databases. Those government and corporate computer systems may or may not have tools to identify and shut down such an attack. With the exception of USAJobs.com, none of the entities affected agreed to speak with Identity Theft 911.

Victims worked at huge government agencies, including the U.S. Department



*This represents a potentially huge breach of national security. But so far, the government and its contractors refuse to discuss it.*

of State and the federal Department of Transportation, as well as some of the nation's largest defense contractors, including General Dynamics and Hewlett-Packard. Which means that when those workers left Monster.com, the Glamorous Team could have recorded their usernames and passwords as they logged into some of our nation's most sensitive military and intelligence databases and intranets.

This represents a potentially huge breach of national security. But so far, the government and its contractors refuse to discuss it. Four computers were infected at Booz Allen Hamilton, a major government contractor specializing in military and intelligence projects, according to files retrieved from the Glamorous Team's server. It's unknown whether the hackers were able to record keystrokes as the company's employees logged into sensitive computer systems.

"We just don't talk about our information security events at all," company spokesman George Farrar in response to Identity Theft 911's request for information.

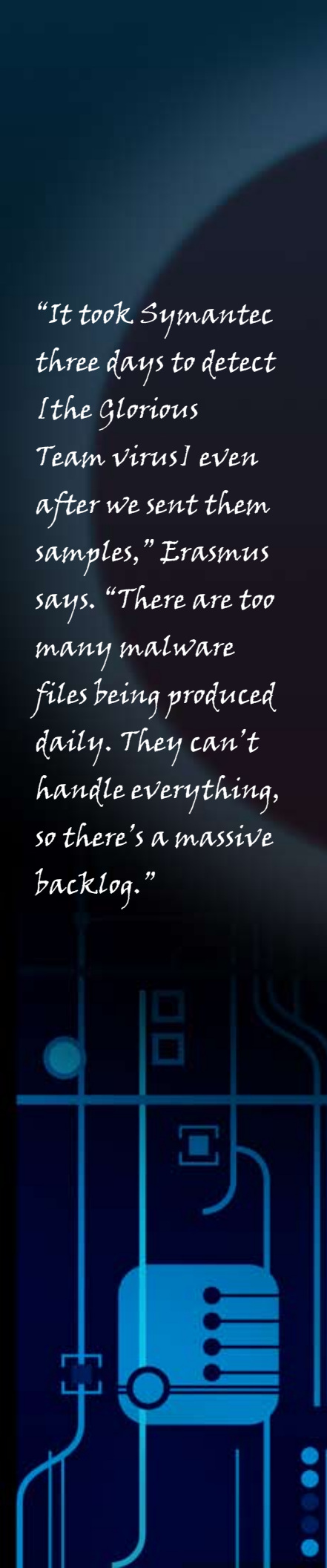
Not all of the hacked computers belonged to government agencies or contractors. A General Dynamics employee was witnessed filling out his passport application online, Erasmus says. The Glamorous Team successfully downloaded malware onto computers belonging to American Airlines, Unisys and Partners Health Care.

"I remember American Airlines said, 'If we can find time we'll call you, but don't hold your breath,'" Erasmus said.

Based on the information on the team's server, Erasmus couldn't tell which type of attack was launched against employees at American Airlines or any other company. But he did determine that the Glamorous Team gained access to an Office Max intranet, allowing them to pose as an Office Max store and order merchandise from the company's warehouses.

"The CIO at Office Max was quite shocked," Erasmus says. None of the companies involved returned calls seeking comment.

Nor were the federal agencies forthcoming about the attack. The State Department and the Department of Transportation "did not take our calls seriously," says Erasmus. "They said they didn't have any knowledge of any systems that were breached." Neither agency returned calls for this story.



*"It took Symantec three days to detect [the Glorious Team virus] even after we sent them samples," Erasmus says. "There are too many malware files being produced daily. They can't handle everything, so there's a massive backlog."*

## Gone, but not finished

The Glamorous Team is no longer targeting job seekers on Monster.com, Ramzan says. The stolen and encrypted data from their unsecured server has been reclaimed, and the server was shut down by Yahoo.

But the attack continues, says Erasmus. The Glamorous Team continues to send out bundles of Trojan software, mostly using porn sites. And we still don't know how the team plans to use its stolen access to sensitive government and corporate computer systems. Are they waiting for the right time to strike? Are they right now—today—designing sophisticated scams to steal sensitive government information?

No one knows. We do know that the Glamorous Team is sophisticated, audacious and fearless. And, by all appearances, the U.S. government and major corporations are not taking the threat seriously.

## More alarms ignored

The attack by the Glamorous Team also highlighted the inadequacies of our overburdened online security system, which is mostly handled by the large antivirus companies such as Symantec and McAfee. Each company employs hundreds of researchers like Ramzan, whose job is to analyze all the new programs distributed over the Internet every day and search them for malicious code. Most teams have about 200 people, Erasmus says, and they receive 12,000 files a day.

They simply can't keep up. "It took Symantec three days to detect [the Glorious Team virus] even after we sent them samples," Erasmus says. "There are too many malware files being produced daily. They can't handle everything, so there's a massive backlog."

Most people in the antivirus industry predict that the number of malicious applications being written and introduced every day will multiply in the next year to 18 months. No one knows how the industry will change to meet that rising challenge. In the meantime, more people will become victims of highly sophisticated scams, partially because their antivirus software cannot handle the load.

"I think the change will be accelerated by people saying, 'Why the hell am I spending \$90 a year for something that doesn't even work?'" says Erasmus. ■

# Monster in the Closet

CYBER-CRIME GETS ORGANIZED,  
GOES LEGIT

The attack on Monster.com is the most terrifying identity theft exploit yet. It isn't just the hundreds of thousands of people potentially affected, or the financial impact, or even the fact that it potentially gave an underworld gang access to "secure" systems of the United States government in time of war. What makes the Monster attack so scary is what it tells us about how good the bad guys really are, how far we are from beating them, and how little the Powers That Be seem to care.

It was 35 years ago that the film, *The Godfather*, invented the modern idea of the mob: bloody, to be sure, but run as strategically as any business and, in fact, more strategically than most. By comparison, some of today's criminal organizations are just as well ordered, and actually make Don Corleone's operation look quaint. The "new mob" employs hackers and network security experts, along with Wall Street investment managers and Ivy League-educated consiglieri. They're smarter, better organized and, in some cases, better financed than many mainstream companies, and all without having to pay taxes or to comply with Sarbanes-Oxley. Going legit? From their point of view, they're already there.

## Complacency is disaster's companion

Yet somehow, despite all evidence, we still think we're smarter than the criminals and we persist in underestimating them. When they get away with

something, we think: they were lucky. When they get caught: it was inevitable. By the end of the show, we believe the forces of good will prevail, order will be restored, life will return to normal.

Wrong.

For proof, consider what a criminal gang called "the Glamorous Team" did to Monster.com.

Now, to judge by most press accounts, the Monster.com scam came down to two little words: file ransom. On September 17, job site Monster.com was notified of a hacker-controlled server in Eastern Europe containing personal data for more than a million Monster customers. "The Glamorous Team" had obtained the job-seekers' data using legitimate login info stolen from corporate and government recruiters, then sent them official-seeming phishing emails that appeared to come from Monster.

Victims who clicked had their computers attacked in stages: A Trojan scanned the computer's defenses first, then downloaded a bundled series of malware programs specifically designed to overcome those defenses. Next, the program immediately double-encrypted the user's computer files, then sent an email (signed by "the Glamorous Team") demanding a ransom to unlock them.

It's not surprising that this garnered headlines. But the scheme involved other programs that were actually more effective, and more lucrative—notably one that captured victims' keystrokes and secretly recorded their passwords for online banking and other secure web sites.

On the "social engineering" side, too, the attacks were carefully calculated—so much so that 20 percent of recipients clicked their way into the trap, significantly more than the normal rate for a successful phishing scam.

If the "Glamorous Team" (also being human and thus prone to mistakes) hadn't left its own server unsecured, this complex scheme would have been very difficult to track and might never have been discovered. Was it the first of its kind? There's no way to know for sure, but it certainly won't be the last.

### Well played

Unlike your typical database hacker, this group was not content to probe for a single vulnerability, exploit it, and get out of Dodge. From the very start—and apparently based on considerable

experience—they came at this with a carefully conceived vision of a multifaceted fraud machine. Far more than a data breach, this intricate scheme generated a shadow economy in which the "Glamorous Team" played people, computers and companies like chess pieces on a grid of interlocking scams. The Wachowski brothers have nothing on this crew. Enter the Matrix? You're already there.

In fact, in a bizarre twist, Monster insisted that it hadn't been hacked, and it hadn't been—at least not in the customary sense. It's true that, for once, network security was not the weakest link in the chain. In this case, social engineering was infinitely more effective than any technical hack in exploiting Monster's weaknesses. The criminals were able to scurry away with at least 1.3 million pieces of sensitive data, not by smashing down the door, but by turning the key and walking in. Instead of merely breaking into a single server, they were able to co-opt the whole system on its own terms—either using phished or guessed passwords belonging to real recruiters or, possibly, posing as recruiters themselves. So while Monster wasn't hacked in the traditional sense, it is far from okay. In fact, the company may have a much larger problem to deal with than a traditional database breach.

The criminals were able to scurry away with at least 1.3 million pieces of sensitive data, not by smashing down the door, but by turning the key and walking in.

If we don't wake up and smell the coffee, we can look forward to a world where legitimate businesses cover their eyes and drag their feet while the crooks take the lead.

### Familiar strains

The more things change, the more they stay the same. This part of the criminals' M.O. is actually a painful echo of the ChoicePoint debacle—a story we can assume the decision-makers at Monster knew well. In 2005, Americans learned that a massive but little-known consumer data vendor called ChoicePoint had put more than 160,000 people at risk of identity theft by providing their credit information to supposedly legitimate client businesses. Those clients were running a business, all right—a fraud ring that duped ChoicePoint into selling tens of thousands of consumer credit files to made-up companies. No one hacked ChoicePoint, either, but that was cold comfort to the victims. Nor did it help ChoicePoint, which is still in business, but only after spending \$30 million in fines and other costs and being raked over the coals by Congress and the FTC.

Did consumers have a right to expect ChoicePoint—or Monster—to verify that their clients were actually legit before handing over people's personal information? Absolutely. Should the government require it? Of course, but don't hold your breath.

As bad as Choicepoint was, the recent incident at Monster was much worse. You see, Monster also operates the U.S. Office of Personnel Management's USAJobs.gov web site, where 2 million subscribers—146,000 of whom also had their data stolen—can post resumes and federal job openings. Most victims accessed Monster.com from work computers, and thousands of them worked for the Department of State, the Department of Transportation, or mammoth

defense contractors like Hewlett-Packard and General Dynamics. Which means that every time one of those workers logged on to a secure government database, file server, or intranet, the Glamorous Team could have wound up with the password.

What are the criminals doing with this information? No one knows—and the government agencies and companies don't seem to care. None will discuss it, and most blew off explicit warnings from computer security firms. The Department of State and the Department of Transportation "did not take our calls seriously," said one. American Airlines reportedly promised to call back to discuss it "if we can find time ... but don't hold your breath."

### Bottom line...

There's a very big problem here. If opportunities exist, they will be seized. That's capitalism, on both sides of the law. But what if the next "opportunity" is a joint venture between Crime Inc. and the Chinese military, or the ex-KGB leaders of the new Russian oligopoly? (Find stateless adversaries more threatening? Swap in the business-savvy jihadists of Al Qaeda.) There's no shortage of people keeping the United States in their strategic crosshairs. For them, access to government servers and secure data—or, for that matter, the ability to cozy up to and then blackmail a well-placed government employee—

could advance their agenda in horrifying ways. On this front, mixing political motives with criminal means could prove disastrous.

“If you know neither the enemy nor yourself, you will succumb in every battle,” said Sun Tzu in the third chapter of *The Art of War*. Two and a half millennia later, these words are still true. If we don’t wake up and smell the coffee, we can look forward to a world where legitimate businesses cover their eyes and drag their feet while the crooks take the lead.

“Misunderestimating” a smart, skilled and determined enemy—whether the goal is criminal profit, political terrorism, or both—is a sure path to disaster. If it wasn’t obvious before the *Monster.com* story broke, there can be no doubt now that in important ways, our adversaries have the edge. It doesn’t help when the people who are supposedly on our side—the businesses, institutions, and agencies we trust to protect our identities—turn out to be unwilling or unable to do their part. It may not be easy, but the rest of us need to look them in the eye and give them a simple message: You need us more than we need you. Get it right and be straight with us about it, or we’re gone. We don’t need another *Monster* in the closet.

# Protect yourself from online attacks

It’s simple to protect yourself from the next *Glorious Team* attack by following these rules:

- ✘ Be extremely cautious when you download files. Most corporations have stopped asking people to open unsolicited e-mails to download programs. If a company sends you an e-mail asking you to do this, call them first to make sure it’s legit. Unfortunately, the same rule applies to e-mails from friends, since hackers often hijack personal computers to send spam.
- ✘ Regularly back up all of your files. USB drives and blank CDs are cheap. Take half an hour to copy your files onto one.
- ✘ If you do become the victim of an online scam, odds are you’re not the only one. Go online to find advice on what to do. It’s possible that a company like *Prevx* or *WebSense* already has created a program to fix the problem.