

Security Trends Report

08/17/07

Hackers steal U.S. DOT, corporate data, security firm says

Among the firms affected are Booz Allen, Unisys and HP

July 17, 2007 ([Reuters](#)) -- Hackers stole information from the U.S. Department of Transportation (DOT) and several corporations by seducing employees with fake job listings on ads and e-mail, a computer security firm said yesterday.

The list of victims included several companies known for providing security services to government agencies such as consulting firm [Booz Allen](#), [Unisys Corp.](#), defense contractor L-3 communications, [Hewlett-Packard Co.](#) and satellite network provider Hughes Network Systems, a unit of Hughes Communications Inc., said Mel Morris, CEO of British Internet security provider Prevx Ltd.

HP declined comment, while officials with other companies couldn't be reached for comment. A DOT spokeswoman said the agency couldn't find any indication of a security breach.

Malicious programs were able to bypass sophisticated security systems undetected because the software was unaware that they were dangerous. Hackers also targeted a limited group of PCs, which kept traffic down and allowed them to stay under the radar of security police, who tend to identify threats when activity reaches a certain level.

"What is most worrying is that this particular sample of malware wasn't recognized by existing antivirus software. It was able to slip through enterprise defenses," said Yankee Group security analyst Andrew Jaquith, who learned of the breach from Morris.

It was not clear whether the hackers used information stolen from the computers, Morris said.

Internet security firms began to release patches to fight the malicious software last night. Trend Micro, for example, has sent customers software that prevents the malware from being installed on computers. It also blocks browsers from going to Web sites that the company identified as being infected with the dangerous programs, said company spokesman Mike Haro.

"This is a serious threat. It shows how sophisticated hackers have become," Haro said.

A piece of software, NTOS.exe, probes the PC for confidential data, then sends it to a Web site hosted on [Yahoo Inc.](#). That site's owner is likely unaware that it is being used by hackers, Morris said.

He said the site hosts data stolen from more than 1,000 PCs and encrypted before it was posted. Morris also said he believes the hackers have set up several "sister" Web sites that are collecting similar data from other squadrons of malware.

Officials with Yahoo weren't available for comment.

Morris said that he had downloaded the data from the Web site and decrypted it at the request of investigators from the [FBI's](#) Law Enforcement Online, or LEO, program, who are looking into the matter. An FBI spokesman declined comment, saying it is agency policy to neither confirm nor deny whether an investigation is ongoing.

Eric Auchard, John Crawley and Georgina Prodhon contributed to this report.

Gartner Update:

6.0 Security

Security continues to be a concern for corporations and is growing as a concern for users. An increase in financially motivated but undetected security violations provides a mandate for enterprises to focus more attention on detecting intrusions.

6.1 Prediction

By the end of 2007, 75% of enterprises will be infected with undetected, financially motivated, targeted malware that evaded their traditional perimeter and host defenses.

Analysis by Neil MacDonald

6.2 Key Findings

The threat environment is changing — financially motivated, targeted attacks are increasing, and automated malware-generation kits allow simple creation of thousands of variants quickly — but our security processes and technologies haven't kept up. Targeted attacks against a small number of organizations or attacks that morph quickly don't create the visibility for the creation of a signature, breaking the model of legacy antivirus and other signature-based prevention mechanisms.

Security products can't stop what they don't recognize as a threat, and this will affect all organizations, large and small. By the end of 2007, we believe that three out of four organizations will be infected with financially motivated, targeted malware that has evaded their traditional perimeter and host defenses and remains installed and undetected on their endpoints. Yet, these organizations will remain "blissfully ignorant," taking false comfort in antivirus and network scans that continue to show zero infections.

Although fewer than 10% of the attacks on the Internet are targeted against a single company, the financial impact to an individual business of a single successful targeted attack will be 50 to 100 times greater than the impact of a successful worm or virus event. We have projected that through 2009, the financial damage experienced by businesses because of targeted attacks will increase at least five times faster than damage caused by mass events (0.8 probability).

6.3 Market Implications

Advanced malicious-code detection and prevention capabilities are needed. Traditional signaturebased antivirus and firewalls are insufficient for comprehensive malicious-code detection and prevention. Legacy antivirus mechanisms must be supplemented with more-advanced styles of intrusion prevention in network- and host-based security. Addressing targeted threats should not require that organizations purchase dozens of new security point solutions. Rather, security platforms should evolve to deliver more types of security protection for little or no additional cost. The convergence onto security platforms is seen in the desktop, next-generation network firewalls and e-mail security servers, making their more-limited predecessors obsolete.

6.4 Recommendations

Protecting against targeted attacks requires strengthening all of an enterprise's information security processes and technologies:

- Investments in vulnerability management processes — Malicious code would have no impact if there were no underlying vulnerability to exploit. Consequently, ongoing improvements in patching capabilities are needed, but most successful attacks will occur at the application level. Organizations should proactively scan applications and

Publication Date: 1 December 2006/ID Number: G00144544 Page 15 of 28

© 2006 Gartner, Inc. and/or its Affiliates. All Rights Reserved.

application source code for security vulnerabilities, ideally in development and quality assurance before applications are placed into production.

- Investments in intrusion prevention systems (IPSs), network- and host-based — Because we can't patch as quickly as new exploits appear, organizations should proactively shield endpoints against attacks targeted on known vulnerabilities. On desktops and servers, behavioral IPSs are maturing that prevent unknown and targeted attacks by monitoring how applications interact with the operating system (OS). Leadingedge vendors offer malicious-code simulation in advance of execution in e-mail gateways and host-based intrusion prevention system (HIPS) products, with some providing virtual machine-based execution of code to observe behavior and contain damage. A simple way to strengthen protection capabilities is to activate hardwarebased protections mechanisms with an OS that supports them (for example, Windows XP Service Pack 2 with no execute/execute disable [NX/XD] activated).

- Investments in network access control — Keeping unmanaged and potentially infected devices off the network will reduce attacks. Even machines that appear healthy may be or become infected. Thus, once a machine is connected, network behavior analysis should be used for monitoring suspicious patterns of network behavior indicating a potentially compromised machine.
- Investments in identity and access management (activity monitoring, such as user activity monitoring, database activity monitoring and transaction monitoring for suspicious activity) — Use content monitoring and filtering, starting with network egress points and, longer term, ideally combined with device control, to prevent inappropriate disclosure of intellectual property. Perform separation-of-duties analysis for administrative control across all systems with check-in/check-out of administrative credentials with full logging of activities while the ID is in use.
- Investments in security information and event management (SIEM) — Use SIEM for the correlation of disparate sources of security information to determine illicit activity

DHS warns states not to reject Real ID

July 18, 2007 - - Despite several state and federal efforts to force noncompliance with the new federal identification law, or Real ID Act, the [U.S. Department of Homeland Security \(DHS\)](#) has continued work on the law's guidelines and warned states that they face consequences for failing to comply.

The [Real ID Act](#), passed by Congress in 2005, mandates national standards for all state driver's licenses and other official documents. The DHS hasn't released a final version of the law, but the agency has said that it will require the documents to include a digital photograph and a bar code that can be scanned by electronic readers.

The initial compliance deadline is next year, with full compliance required by 2013.

The Real ID Act led to an outcry from privacy advocates and to the [passage](#) of laws in some states, including New Hampshire, that prohibit compliance with the law.

Despite the criticism, the DHS continues to insist that the law be implemented on schedule. "I think residents of states that choose not to comply are going to be displeased with their leadership's decision when we get closer to full implementation," a DHS spokesman said. "They'll no longer be able do certain things that carriers of state-issued drivers licenses take for granted today."

He noted that residents of states whose identification cards don't comply with the law will be prohibited from entry to airports and federal buildings. It could also block access to "certain critical infrastructure sites" such as a power plants or dams, he said.

Critics won a small victory against the law last month when Montana's two Democratic senators, Max Baucus and Jon Tester, successfully [called on](#) colleagues to cut language from a now-stalled immigration bill that would have required all employers to check the eligibility of any potential employee by using Real ID documents.

"My boss and Sen. Tester don't support the Real ID program, as do a majority of Montana citizens," said a Baucus spokesman. "It amounts to a national ID system, and there are privacy concerns."

Tim Sparapani, legislative council at the Washington office of the [American Civil Liberties Union](#), said that the deleted language would have led to a "massive expansion" of Real ID-compliant documents. In effect, it would have made a driver's license an employment document, he said.

Sparapani predicted the final regulations will come from DHS around Labor Day, and individual states not now opposing Real ID will have to decide if they want to reject it or implement it.

The DHS spokesman declined to offer a specific date for when the final regulations would be issued.

--Legislators Say No to Financial Help for Real ID Implementation (August 2, 2007) The US Senate failed to approve legislation that would have provided US \$3 million annually to help states comply with the Real ID Act.

The law requires states to provide citizens with driver's licenses and state issued ID cards with machine-readable bar codes or RFID chips and to create a database of personal information that will be linked to databases from all other states. States are required to comply by 2008, though some have been granted extensions to 2010. The American Civil Liberties Union (ACLU) opposes the Real ID Act not because of the associated costs, but because it views the entire project as a "serious privacy threat." Seventeen US states have publicly opposed the federal law.

http://www.eweek.com/print_article2/0,1217,a=212765,00.asp

[Editor's Note (Liston): Turning Real ID into an unfunded mandate is just going to make states all the more reluctant to cooperate with the Feds. With the cost of ID conversion coming out of their own budget, State lawmakers will be far more willing to listen to those talking about Real ID's privacy implications.]

"Government Reports Cybercrime Poses National Risk" **InformationWeek (07/24/07) ; Gaudin, Sharon**

The public and private sectors are threatened by ever-increasing domestic and foreign cyberattacks on operational security and law enforcement, concludes a new Government Accountability Office report. The GAO reported that more stringent security must be employed by IT managers, while federal and commercial sectors are faced with ongoing difficulties in detecting Web-based crime. Rep. Jim Langevin (D-R.I.) of the subcommittee on Emerging Threats, Cybersecurity, and Science and Technology said that compromised federal Web sites, classified email susceptible to unclassified networks, and infiltration of Department of Homeland Security networks are among the government's security challenges. The DHS and its CIO Scott Charbo were faced with reports during a congressional hearing that the department had experienced 844 "cybersecurity incidents" within two years. Rep. Bennie G. Thompson (D-Miss.) wrote that the DHS is at the forefront of cybersecurity for the nation yet department investigations have demonstrated that "'information security' has become an oxymoron." Langevin said China has been "coordinating attacks against the Department of Defense for years," and that potential malware could infiltrate first-strike attacks on U.S. computer systems. "I encourage all businesses--small and large--to take a very close look at their cybersecurity practices," Langevin said. "Though 100 percent security may be unattainable, there are many policies and procedures that businesses can implement to better safeguard their data."

[\(Link to Source/Publication\)](#)

"OMB, DHS Outline Data Security Best Practices" **Federal Computer Week (07/17/07) ; Miller, Jason**

The "Common Risks Impeding the Adequate Protection of Government Information" released by the Office of Management and Budget and the Homeland Security Department cited 10 security mistakes that agencies make. The paper noted best practices that should be followed to prevent security breaches and the disclosure of sensitive information in areas such as training, contracting, and records management. The OMB and DHS said that Federal Acquisition Regulation language should be incorporated into all agreements and an operating procedure should be developed that guides employees about reporting suspicious incidents. "All of the best practices and important resources are interrelated, and they can help agencies address the risks associated with information security and privacy programs," said OMB information technology and e-government administrator Karen Evans. The paper was created in response to the President's Identity Theft Task Force recommendations.

[\(Link to Source/Publication\)](#)

"Security: A Business Enabler, Not Disabler" **Baseline (07/07)No. 74, P. 41 ; McCormick, John**

Purdue University professor Eugene Spafford, recipient of the ACM's President's Award for his "extensive and continuing record of service to the computing community, including major companies and government agencies," says one of the biggest weaknesses in corporate computer centers are business processes, operating systems, and applications that are developed and implemented with convenience or cost, rather than security, in mind. He says it is "just plain wrong" to assume that patches and add-ons will ensure the security of such products, when in fact security must be designed into the products from the outset. Spafford explains that part of this effort involves "having informed, empowered individuals who have the appropriate training and background to be making decisions about what goes in, and that those decisions are based on an adequate understanding of risk."

A lack of knowledge about specific risks and the value of components constitutes a major failing, and Spafford says CIOs must obtain a comprehensive perspective of resources in need of protection and their associated risks. Spafford recommends that managers ask questions concerning whether the proper applications/operations/business processes are running, who ultimately decides new acquisitions and the architecture as project momentum builds, and whether risk is properly integrated in those decisions. He also suggests that people should get in a mindset that views security as an enabler rather than a disabler.
([Link to Source/Publication](#))

"Managing Technology Patching Holes" **Government Executive (07/01/07) Vol. 39, No. 11, P. 53 ; Holmes, Allan**

Although known vulnerabilities such as viruses and malware remain a major threat to networks, two other threats are becoming a greater risk to networks as well. One of those threats is spear phishing, in which a hacker uses an email message to trick employees into providing personal information about themselves or their colleagues. The hacker then uses that information to create a false identity or to gain access to online accounts. The other threat is unvalidated inputs or input checking, in which a hacker inserts a command in a string of characters within a field that asks for personal information. The inserted command tricks the underlying database into providing its entire list of names and personal information. These two threats now account for two thirds of all cyber attacks, according to Alan Paller, director of research at the SANS Institute. The other third comes from the failure to patch systems on a routine basis. Most system administrators fail to create a patch management process because doing so takes a great deal of time. However, system administrators can take several steps to make the job easier, including conducting a risk assessment of their networks to find out where data is stored, and identifying conduits to that data.
([Link to Source/Publication](#))

"Net Criminals Shun Virus Attacks" **BBC News (07/20/07) ; Ward, Mark**

Security experts say hackers have detected new ways to execute cyberattacks that are much more difficult to detect and prevent. Some hackers are now exploiting file-sharing networks and popular Web sites, which they have found to be much easier platforms to infiltrate than direct PC attacks. Botnets have been favored among the more sophisticated of criminals, spamming or sending mass junk mail to online surfers as a tactic for obtaining credit card information or log-in data. Windows machines are the most susceptible to botnet attacks, occurring when a user opens an email with a virus or malware. Yet Prolexic's Paul Sop says hackers have discovered a method to release denial-of-service attacks without infiltrating PCs. Prolexic observed an attack that occurred when users were told to connect to another hub because its main server was down for maintenance. As such, the hackers could redirect traffic by bombarding a server with thousands of file-sharers. Sop noted that no malware or viruses were seen in the attacks, yet the hackers could target a site to bombard with traffic, noting it was one of the biggest large-scale attacks involving gigabits of traffic per second. "The topologies are varying as we see more P2P and http nets each day," says Shadowserver Foundation's Andre' M. Di Mino. "This is a very growing and troubling trend."
([Link to Source/Publication](#))

"What Can Be Done About Software Security?" **SD Times (07/01/07) No. 177, P. 37 ; Worthington, David**

Problems with project management and organizational commitment and training were traced by experts to be the most frequent root causes behind the increasing incidence of software code vulnerabilities, and tight schedules and a lack of management-defined standards were among the factors cited as contributing to software security deficiencies. SPI Dynamics co-founder Caleb Sima commented that security must be a process that encompasses the entire organization and that is embedded within the existing development life cycle, and he and other experts concurred that companies with a serious security investment must make a bigger commitment to quality assurance tooling, realize the effective use of such tools, and secure developers capable of using those tools to write vulnerability-free code.

Intelligent Decisions' director of security business units Roy Stephan advised the establishment of best practices emphasizing boundaries, where applications communicate via protocols or between libraries, and also supported peer code reviews. Consultant Rex Black explained that organizations currently lack an incentive to invest more in security because they can pass the cost of security failures on to users and consumers, and he suggested that government intervention might divert the cost back to companies, spurring a corporate interest in patching security flaws. Oracle program director John Heimann aimed criticism at entry-level developers' prowess, complaining about a dearth of secure coding classes offered by university computer science and training programs. "They do good things, but this is basic knowledge that software engineers should have," he said. Heimann attested that most academics have little secure code development skill, have no desire to teach such a subject, and do not wish to be criticized for their lack of knowledge; he indicated that accreditation standards should impel program revisions that would enable qualified faculty to teach secure programming.

[\(Link to Source/Publication\)](#)

IM Attacks Up Nearly 80 Percent, Akonix Says

Malicious code attacks over instant-messaging (IM) networks are up almost 80 percent over last year, according to a new study from vendor Akonix.

In July, the company, which develops IM hygiene and compliance appliances and services, said it uncovered 20 malicious code attacks over IM in July. The total number of threats for 2007 so far is 226, the company said. That number is a 78 percent increase over last year.

The company also said attacks on peer-to-peer networks, such as Kazaa and eDonkey, increased 357 percent in July 2007 over July 2006, with 32 attacks.

That report comes on the heels of a report by peer-to-peer network monitoring vendor Tiversa, which found contractors and U.S. government employees are sharing hundreds of secret documents on peer-to-peer networks.

In many cases, those users were overriding the default security settings on their peer-to-peer software to do so, according to Tiversa. Robert Boback, Tiversa's CEO, and retired U.S. Army Gen. Wesley Clark, a Tiversa board member, testified earlier this week before the U.S. House of Representatives Oversight and Government Reform Committee.

The IM attacks were tracked by the Akonix IM Security Center, which is a collaborative effort between Akonix, its customers, and other security and messaging vendors.

The code used in the attacks was either brand-new code or a variant of earlier code detected by the IM Security Center.

The new worms included Exploit-YIMCAM, Hupigon-SJ, InsideChatSpy, SpyPal, StealthChatMon, Svich and YahooSpyMon.

Akonix officials also said the attacks are moving beyond the nuisance stage and getting more malicious.

"Beginning at the end of last year we started seeing multi-stage attacks where IM will deliver a URL and when a person clicks on it they get code loaded that will pull down other code," says Don Montgomery, vice president of marketing at Akonix.

Montgomery says the IM Security Center also is seeing two-stage attacks, with the second stage being the downloading of a Trojan that waits for users to log into specific banking sites to activate a key-logging program.

- In addition, there are multi-vector attacks where a malicious URL may be delivered by IM but propagated using e-mail or come in via e-mail and go out over IM. And attacks, focused on

consumer services AOL, MSN and Yahoo, are beginning to span networks. *John Fontana, Network World (US)*

Data Security Risks Go Beyond Stolen Laptops"

Federal Times (07/23/07) Vol. 43, No. 22, P. 6 ; Hemingway, M.Z.; Peniston, Brad

In the aftermath of last year's theft of a Veterans Affairs Department laptop containing the personal data of more than 28 million veterans and service members, many government agencies opted to bolster their data security by encrypting data stored on laptops and other mobile devices. Despite these steps, many agencies were still vulnerable to data theft because their mobile devices were connected to wireless networks that were not secured or encrypted. Since these networks were not secured, a hacker in a building next to the agency or in a nearby coffee shop could easily log on to the network and access sensitive agency information, according to Bill Geimer, the program manager for the Agency for International Development's chief information security office. Some federal agencies are now beginning to take steps to address this problem. The Federal Aviation Administration, for example, is installing security devices at its air traffic control centers, training centers, and headquarters to protect proprietary payroll and personnel information and FAA financial figures. The security devices will monitor whether hackers are trying to gain access to the agency's network and will alert officials if the network's security has been compromised.

August 02, InformationWeek — Number of hackers attacking banks jumps 81 percent. The number of hackers attacking banks worldwide jumped 81 percent from last year, according to figures released at the BlackHat security conference Thursday, August 2. Researchers from SecureWorks also reported that hackers going after the company's credit union clients increased by 62 percent from last year. So why are there so many more hackers this year than last? Joe Stewart, a senior security researcher at SecureWorks, told InformationWeek that highly technical and savvy hackers are no longer the only ones in the game. Hackers no longer need to be technical wizards to set up an operation to steal people's banking information. Hacking toolkits and malware are for sale in the online underground. This new ease-of-use is evident in the numbers. SecureWorks reported that between June 2006 and December 2006, they blocked attacks from about 808 hackers per bank per month. From the beginning of this year through June, there's been an average of 1,462 hackers launching attacks at each of the company's bank clients. As for the credit unions, SecureWorks reported blocking attacks from 1,110 hackers per credit union per month. That number rose to 1,799 this year.

Source:

<http://www.informationweek.com/software/showArticle.jhtml;jsessionid=HJ33X3QS2DLEQQSNDLOSKHSCJUN2JVN?articleID=201202629&articleID=201202629>

"Security Researchers at Black Hat Show How Corporate Intranets are Ripe for Emerging Attacks"

InfoWorld (08/01/07) ; Hines, Matt

Many companies are leaving their IT operations vulnerable by failing to protect their internal Web sites, according to Jeremiah Grossman and Robert Hansen, two leading researchers who made presentations at the Black Hat 2007 security conference in Las Vegas. In his presentation, Grossman noted that hackers can find links to companies' internal Web sites by carrying out new attacks such as cross-site request forgery (CSRF) threats, which allow them to break into seemingly secure Internet sessions in order to steal password and browser history data. After breaking into these Internet sessions, attackers can then attempt to misappropriate victims' identities and privileges to carry out activities such as changing their applications passwords to log on to intranets or banking sites, or to log on to e-commerce sites to make fraudulent purchases in their name. Though such CSRF threats and cross-site scripting (XSS) techniques are typically being used together to steal money from online bank accounts, they can also be used to access prior Web browser sessions and remain logged into sites that have been accessed by an end-user to carry out illegal activities. In order to protect themselves, companies should defend their internal Web sites in the same way they protect their external sites. For example, public-facing Web sites should not be allowed to access intranets on any level, since this is a common way for hackers to break into the systems, Grossman and Hansen said.

[\(Link to Source/Publication\)](#)