

Security Trends Report

09/09

Study: Malware persists on compromised machines

[Chuck Miller](#)

September 16, 2009

Eighty percent of computers that have been compromised are still infected after 30 days, and nearly 50 percent remain compromised after 10 months, according to an analysis released Wednesday by Trend Micro.

"When machines are compromised, they're compromised for a long time," Dave Rand, CTO of Trend Micro, told SCMagazineUS.com Wednesday.

The machines remain undiscovered because they tend to stay under the radar – they don't do anything blatant, such as consuming system resources, that would tip off the victim, he said.

Also, because these infected PCs typically are part of botnets, they get new software revisions frequently, making them even more difficult to detect.

"One of the joys of having a botnet machine is that they are updated regularly," Rand said. "After the machine is infected, the auto-updates take over, and they are actually more efficient than many AV applications."

In 2009, virtually all malware tracked by Trend Micro was used by cybercriminals to steal information, Rand [wrote](#) on the TrendLabs blog. The three most dangerous botnets in terms of information, financial and identity theft are [Koobface](#), Zeus/[Zbot](#) and Ilomo/[Clampi](#).

"The most important thing to recognize is that the machines will not fix themselves," Rand said. "Someone has to look at the activity of these machines, and that should happen at the network level. We need to get better network tools into the hands of the enterprise."

Likely a few hundred criminals have more than 100 million computers under their control, he said. This means that cybercriminals have more computing power at their disposal than the entire world's supercomputers combined.

"The internet is a dangerous place still," Rand said. "We need to be aware that there is an incredible amount of information leaking out of the enterprise."

DHS report: IT sector is resilient against serious cyberattacks

Many measures already in place to mitigate risks, although more can be done, report says

By Jaikumar Vijayan

August 26, 2009 01:52 PM ET

[Computerworld](#) - A report from the U.S. Department of Homeland Security presents several scenarios in which well chosen attacks against key IT infrastructure elements could cause disruptions on a national scale. But the document also offers a surprisingly sunny assessment of the resilience and redundancies within the IT sector to mitigate the risk of such disruptions.

The [114-page report](#), released Tuesday, titled the "IT Sector Baseline Risk Assessment," was a joint effort between the DHS and the Information Technology Sector Coordinating Council (IT SCC). It is designed to give planners in the IT sector and in government a way to identify high-consequence risks and strategies for addressing them.

The report examines risks to six critical areas in the IT sector - IT supply chain, domain-name resolution services, identity management and trust support services, Internet-based content and communications services, Internet service and routing providers and providers of incident response services.

Experts in their fields evaluated high-consequence risks in their areas. They also looked at related vulnerabilities and the potential consequences of incidents that are either enabled or deliberately caused by someone with malicious intent.

On the supply chain side, for instance, the report describes a scenario where an organized crime group manages to install a bank-password keystroke logger in the software distribution image of a notebook manufacturer. Such an event could cause considerable business disruptions and loss of consumer confidence, the report noted. Attacks against the supply chain can also manifest themselves physically, such as when the flow of materials required for manufacturing hardware becomes limited, the report noted.

Similarly, on the DNS (Domain Name Systems) infrastructure front, an attacker could try to establish an alternate Internet root to which DNS inquiries could be diverted, the report warned. An alternate Internet root server that denied service for financial transactions could undermine U.S. economic stability and security, the report cautioned. In similar fashion, large scale denial-of-service attacks, Web re-directs and spoofing attacks on payment processing and e-commerce companies could have cascading effects on consumers, businesses and government entities that rely on such services, the report said.

For the most part though, measures are already in place or are being planned that mitigate the likelihood of such high-consequence disruptions, according to experts at the DHS and IT-SCC who performed the risk assessment. On the supply chain side for instance, while the consequences of an untrustworthy component entering the distribution chain are high, the likelihood of this scenario playing out is low. That's because of the use of sophisticated sourcing strategies, supply chain monitoring processes and product recall capabilities.

On the DNS services front, large-scale DNS attacks and attacks that disrupt a "single interoperable Internet" could have serious consequences, the risk assessors said. At the same time, however, the likelihood of such events playing out in reality were medium to low at best, they claimed. Here again, they said, there are many measures already in place that mitigate risk, including real-time monitoring of production equipment by network operations centers, protections against unexpected configuration changes and process checks to prevent the running of malicious code.

The geographic distribution of the servers that maintain the DNS (Domain Name systems) root and top-level domains also means that an attack on one part of the Internet will not necessarily paralyze the system. Going forward, attempts to build more diversity into the DNS infrastructure and the migration to DNSSEC, a more secure version of DNS, will further reduce the risk of high consequence threats, the report noted.

Ironically, such assessments come at a time when a growing number of government and commercial entities are coming under cyberattack from domestic and foreign adversaries. So far, most of the attacks have been either for financial gain or to leech away government and military secrets. Many experts believe cyberattackers have already penetrated many core government and financial systems and are poised to cause large scale disruptions if needed. Such concerns have [prompted calls for a comprehensive strategy for defending U.S. interests in cyberspace](#). They have also prompted calls for the [development of a cyber-offensive capability](#) aimed not only at defending against attacks but at actively deterring them.

IT Sector Regulation Appears Inevitable

Federally Imposed Rules Seen by 2015

August 28, 2009 - Eric Chabrow, Managing Editor

In 2001, it was big news when a rogue employee stole 35,000 credit card numbers. Eight years later, the Heartland Payment Systems security breach exposed 130 million credit card accounts. Such breaches along

with other woes with information technology products and services will likely lead to the government regulating the IT industry by the middle of the next decade, says Richard Hunter, a fellow and vice president at the IT advisory firm Gartner.

"Markets don't seem to have done it (self regulate) on their own so far," Hunter says in an interview with GovInfoSecurity.com. "The progression in consequences for the public of failures in IT has been climbing pretty steadily and rather steeply in the last few years. ... Indeed, as information technology becomes more and more deeply imbedded in the fabric of society, there is no reason to believe that the consequences of IT failures will lessen over time."

Like the airlines, automotive, financial services, pharmaceutical and telecommunications industries, the government will regulate the IT sector, Hunter predicts.

"There's a trajectory that industries tend to follow; when an industry is extremely successful - that is to say that when an industry succeeds in moving its products and services right into the heart of daily life, regulation tends to follow. in the 20th century," Richard Hunter, a Gartner fellow and vice president, says in an interview with GovInfoSecurity.com.

"We saw the Food and Drug Administration, we saw regulation of telecom, we saw regulation of the airlines industry, we saw regulation of the automobile industry," he says. "I think the information technology industry has been extraordinarily successful in the last 40 to 50 years in increasing the importance of its products and services to almost every aspect of modern life. And, what usually happens in any industry when you reach that level of importance in society is that regulation takes place."

Security test prompts federal fraud alert

By Robert McMillan

August 28, 2009 01:22 AM ET

IDG News Service - A sanctioned security test of a bank's computer systems had some unexpected consequences this week, leading the federal agency that oversees U.S. credit unions to issue a fraud alert.

On Tuesday, the National Credit Union Administration (NCUA) warned all federally insured credit unions of a bogus letter that an unnamed credit union had received along with two CDs. The bogus letter claimed that the CDs contained NCUA anti-fraud training materials, but in its [fraud alert](#), NCUA warned that running the CDs "could result in a possible security breach to your computer system, or have other adverse consequences."

Only it turned out that the CDs were not sent by fraudsters. They were sent by employees of MicroSolved, a Columbus, Ohio, security testing company. "It was a part of some social engineering we were doing in a fully sanctioned penetration test," said MicroSolved CEO Brent Huston in an e-mail message.

Companies like MicroSolved are routinely hired to independently test the security of corporations and government agencies.

Penetration testers often use so-called social engineering techniques as part of their security assessment work. With social engineering, the attacker typically pretends to be a legitimate partner or co-worker in order to trick employees into compromising their computer systems or divulging sensitive information. "Social engineering exercises are a part of most of our assessments," Huston said.

NCUA spokesman John McKechnie did not have much to say about his organization's alert. In a brief e-mail Thursday, he wrote "at this point, it appears that this is an isolated event."

Even if the threat that prompted the NCUA warning was not based on a real attack, the warning contains good information, according to Johannes Ullrich, chief research officer at the SANS Institute, a security training group.

"It's a good lesson," he said. According to him, all of the parties in the exercise acted pretty much as they should have. The bank "reported it to their controlling agency, who then put out this alert based on it."

California Credit Union League Director of Research and Information, Rita Fillingane, said the alert was still useful, even if it wasn't based on an actual criminal act." In the future something like this could come down the pike," she said.

Still, Ullrich said he is not aware of any cases where bogus CDs were actually used to compromise a computer network.

He said he was initially extremely interested when he saw the initial NCUA warning. "I thought, 'Finally this is in the wild, because I've only seen it in pen tests before.'"

Privacy Office approves laptop searches without suspicion at U.S. borders

Such searches no different than inspecting briefcases or backpacks, DHS office says

By Jaikumar Vijayan

August 31, 2009 07:05 PM ET

Computerworld - The Department of Homeland Security's Privacy Office has approved the controversial searches, copying and retention of laptops, PDAs, and other digital devices without cause at U.S. borders.

Travelers could soon start seeing notices from the Privacy Office, which last week released a report supporting the right of customs agents [to conduct such searches](#).

The 51-page [Privacy Impact Assessment](#) also supported the right of U.S. Immigration and Customs Enforcement agents to copy, download, retain or seize any content from these devices, or the devices themselves, without assigning any specific reason for doing so.

Also, while in many cases searches would be done with the knowledge of the traveler in some situations, the report says, "it is not practicable for law enforcement reasons to inform the traveler that his electronic device has been searched."

In arriving at the assessment, the Privacy Office argued that such searches of electronic devices were really no different from searches of briefcases and backpacks. They are needed to interdict and investigate violations of federal law at U.S. borders and have been supported by courts in the past, the assessment said.

That conclusion is sure to rile privacy and civil rights advocates, who have been vehemently protesting such border searches for about two years. They have argued that searches of electronic devices without any reasonable cause are very different from similar searches of backpacks and other items by customs agents, because unlike with briefcases and packs, electronic devices are capable of storing far more data, including personal and business data some that could be highly personal or protected.

The Association of Corporate Travel Executives and other groups [have warned of potential security breaches](#) when corporate data contained in a laptop or PDA is downloaded by a customs agent as part of a border search. Similar concerns have been raised about data involving client and lawyer privileges, intellectual property, and other sensitive information.

Last week, the [American Civil Liberties Union filed a lawsuit against the DHS](#) after an attempt to get information on such searches from the DHS had failed to elicit a response from the agency. In it, the ACLU asked DHS to disclose details on the criteria it uses for selecting passengers for such searches, and the number of such searches it has carried out so far.

The ACLU suit also sought information on the number of devices and documents that have been retained by the DHS following such searches and the reasons for their retention. A similar suit was filed last year by the Electronic Frontier Foundation and the Asian Law Caucus.

In its analysis, the Privacy Office noted some of the privacy concerns that have been expressed over its border searches. The report conceded that a person who would not mind a briefcase being inspected by a customs agent might feel that a laptop search "increases the possibility of privacy risks due to the vast amount of information potentially available on electronic devices."

Nevertheless, making such devices exempt from customs inspection would create a dangerous loophole" for those seeking to break the law, the report said. A traveler's claim of privilege or statement that something is personal or business related, "does not preclude the search," the report said. It pointed to a process that needs to be followed when customs and immigration agents conducted such searches and the notice that needs to be provided to travelers whose devices may be retained or seized.

The report also highlighted the measures currently in place for sharing data with other federal agencies, and ensuring that any data that is copied and retained is properly protected -- including via encryption where needed and "storing in locked containers." It mentions a process for destroying any data that is not needed within a maximum of 21 days from when it was collected.

Lillie Coney, associated director with the Electronic Privacy Information Center (EPIC), said that the Privacy Office's support for "very general, non-specific" searches of electronic devices was troubling. "They are every vague on intent, or any rational cause why people might be pulled [for such searches,]" she said. "They don't talk about data retention or about restricting access to the purpose for which they information is collected." She also said such searches within U.S. borders would be considered unconstitutional and in violation of privacy rights. What the DHS is saying is, "because you happen to go through a border your citizenship rights magical disappear to fo into a state where it doesn't exist," Coney said. "That's a big problem."

Privacy, consumer groups want news laws to protect Web users

By Grant Gross

September 1, 2009 03:21 PM ET

IDG News Service - A coalition of 10 U.S. privacy and consumer groups has called for new federal privacy protections for Web users, including a requirement that Web sites and advertising networks get opt-in permission from individuals within 24 hours of collecting personal data and tracking online habits.

The groups, including the Center for Digital Democracy, the Electronic Frontier Foundation (EFF) and the U.S. Public Interest Research Group (US PIRG), want the U.S. Congress to pass legislation that would bar Web sites and online advertising networks from collecting sensitive data such as information about health, finances, race and sexual orientation.

In a broad set of new recommendations for privacy regulations released Tuesday, the groups also called on the U.S. Congress to prohibit Web sites and ad networks from collecting behavioral information about children under age 18, whenever it's possible to distinguish the age of the Web user, and to require that online businesses inform consumers about the purpose of the information collection.

"The basic idea is ... we want consumers to be able to take advantage of all the new technologies without having the technologies take advantage of the consumers," said Pam Dixon, executive director of the World Privacy Forum. "Right now, that balance is not there."

Many Web users are unaware of all the information that's being collected about them, especially by ad networks engaged in targeted or behavioral advertising, the groups said. The groups released recommendations to Congress just before lawmakers return to Washington, after August recess. Several lawmakers, particularly Representative Rick Boucher, a Virginia Democrat and chairman of the House Subcommittee on Communications, Technology and the Internet, have talked about pushing for online privacy legislation late this year.

The groups recommended that consumers should be able to obtain the information collected by behavioral advertising vendors, and should be able to challenge the data held about them, the groups said.

The groups also called on the U.S. Federal Trade Commission to establish an online behavioral tracking registry, similar to the national do-not-call list, through which consumers could sign up to opt out of all behavioral tracking.

Congress should also allow consumers to file lawsuits against online companies that do not follow privacy rules, and Web sites should not be able to use pretexting practices, such as running a contest that seeks the collection of consumer information in exchange for the chance to win a prize, the groups said.

The new rules are needed because consumer protections are outdated and online advertising industry efforts to self-police have fallen short, the groups said. "The technology has outpaced consumer protections," said Gail Hillebrand, a senior attorney at Consumers Union.

Representatives of the Network Advertising Initiative (NAI), a cooperative of online advertising and analytics companies, and the Interactive Advertising Bureau (IAB), a trade group representing online advertisers, disputed the privacy groups' assertions that industry self-policing hasn't worked.

The NAI allows Web users to opt out of behavioral tracking by 35 ad networks, including the 10 largest, said Charles Curran, NAI's executive director. Behavioral advertising allows Web sites to deliver relevant advertising to visitors, which in turn helps Web sites make money through ad clicks, he said.

Forcing Web sites to get opt-in permission before tracking user behavior would lead to much less behavioral advertising, less profits for Web sites and fewer free services on the Web, critics of an opt-in approach have said.

NAI's approach, which requires an opt-in only for sensitive information, achieves a balance between privacy and economics, Curran said. "We think we're trying the right approach," he added.

Targeted online advertising is nothing new, and many consumers want to see more relevant ads, added Mike Zaneis, vice president for public policy at IAB.

"It is naïve for consumer groups to claim that the delivery of more relevant online advertisements is a new phenomenon that has suddenly developed, thereby creating a new threat to consumers," he said. "The creation of a broad opt-in requirement for online advertising would be detrimental to both consumers and businesses. Consumers love the free services and content that online advertising pays for, and the industry principles strike the right balance of providing strong consumer privacy protections, while allowing industry to innovate and provide new and better products free of charge."

Instant messaging speeds up data theft danger

By Jeremy Kirk

September 1, 2009 09:23 AM ET

IDG News Service - One of the more sophisticated pieces of malware in circulation has been given an upgrade that lets cybercriminals act even faster after they've stolen data from a PC.

According to security company RSA, the Zeus Trojan -- blamed for enabling countless online bank account heists -- now uses an instant messaging component that alerts hackers immediately when they've captured someone's authentication credentials. That can enable fast use of time-sensitive information, such as one-time passwords now often employed in online banking.

Zeus isn't the first piece of malware to employ instant messaging, notes RSA in its [Online Fraud Report](#) for August. Another password-stealing program called [Sinowal](#) was found to be using it in 2008.

Once on a PC, Zeus sends log-ins and passwords to a remote server, which the hacker must then access and sort through. RSA found that several variants of Zeus have a Jabber instant messaging module. The Jabber

project -- as well as other services such as Google's Gmail chat feature -- employ [XMPP](#) (Extensible Messaging and Presence Protocol), an open standard for instant messaging.

The hackers set up two Jabber accounts, one to send information and one to receive. When Zeus obtains log-ins, it sends them to a remote server. The Jabber module then looks for credentials for specific financial institutions and then transmits the information to the hacker by instant message, RSA said.

The number of computers in the U.S. alone infected with Zeus was estimated last month by the security company Damballa at around 3.6 million computers, making it one of the most prevalent malicious software programs and a large botnet.

Users can be infected if they haven't installed the latest security patches on their computer and visit a Web site that is designed to automatically hunt for software vulnerabilities and then deliver the malware. Zeus may also be inadvertently installed on a computer if a person is tricked into opening an e-mail attachment containing Zeus.

Zeus, which is believed to be the product of a Russian hacker who goes by the name A-Z, is sold in underground forums to budding cybercriminals, according to another security company, [Secureworks](#). It can be customized according to the needs of the buyers. For example, Zeus can be coded to only record the log-in details for a certain specific list of Web sites.

"The ease-of-use of the Zeus crimeware toolkit for individuals to create their own tailored Trojan botnets has meant that it has become a favored toolkit for entry-level criminals to get involved in the underground economy," according to Peter Coogan of Symantec, writing on one of the company's [blogs](#). "The greater availability of this toolkit on underground forums as of late has also led to an increase in its usage."

Zeus has been on the radar of security professionals for a while, and one group runs a Web site that tracks Zeus infections and the command-and-control servers, which can issue instructions to infected PCs.

The [Zeus Tracker](#) now counts 802 malicious hosts with Zeus. The organization also publishes a [block list](#) that administrators can use to ensure people on their network don't access dangerous Zeus-related domains.

Internet Security Trends 2009: An Interim Update

By **Zulfikar Ramzan**

September 2, 2009 02:38 PM ET

CSO - The effects of cybercrime are far reaching. It would be a difficult task to find someone who has never been affected by malicious Internet activity, or who does not at the very least know someone who has been negatively impacted by cybercriminals. Advances in Internet technology and services continue to open up innumerable opportunities for learning, networking and increasing productivity. However, malware authors, spammers and phishers are also rapidly adopting new and varied attack vectors. If the Internet is to become a safer place, it is imperative to understand the trends and developments taking place in the Internet threat landscape and maintain online security best practices.

In December 2008, Symantec researchers predicted a number of security trends to watch out for in 2009. Now that we are into the second half of the year, it's time to check in on those predictions to see not only how they have panned out, but also what other developments have occurred. What follows is an update on the predictions Symantec made late last year, as well as a few new trends that our analysts have seen develop in the first half of 2009.

A Trends Predictions Check Up

Attackers take advantage of the economic crisis

The global economic recession has been one of the most noticeably exploited bases for attack in 2009. Its impact has been far-reaching and the computer industry is far from immune to its affects. Schemes and scams

targeting victims of the recession and touting solutions to its problems are prevalent. Some of the threats are new and some have been around for awhile. These scams include:

- * Home foreclosure scams
- * Scams targeting people seeking mortgages or refinancing
- * Scams exploiting the U.S. economic stimulus packages
- * Scams targeting the unemployed with offers almost too good to resist
- * Attacks seeking to exploit users of classifieds and online job placement boards
- * "Work at home" schemes

Social networking becomes an even more popular attack vector

There's no question that online social networking continues to rise in popularity due to the numerous conveniences and opportunities it provides. There's also no question that social networking provides phishers with a lot more bait than they used to have. Threats can come from all sorts of avenues within a social networking site. Games, links and notifications are the low-hanging fruit for phishers to use as they lead people into dangerous territory. As society picks up one end of the social networking stick, it finds that it inevitably picks up the security problems on the other end.

We may not want it, but it still keeps coming. In July 2009, an average of 89 percent of all e-mail messages were spam. The overall amount does fluctuate, and a fight is underway to ward off or close down as many spammers as possible, but on average, the levels of spam have primarily risen rather than fallen. Big headlines almost always lead to more spam, and major headlines from 2009, such as the death of Michael Jackson, the H1N1 flu outbreak and the Italian earthquake are obvious examples of this.

Web threats grow in complexity and sophistication

Distribution and channel options are not the only things that have increased for cybercriminals, their skills and creativity have followed the same pattern. In addition to the threats being new, they are becoming increasingly sneaky and complex. New scams, such as drive-by downloads, or exploits that come from seemingly legitimate sites, can be almost impossible for the average user to detect. Before the user knows it, malicious content has been downloaded onto their computer, and they face an often expensive and time consuming recovery process. As predicted, the level of sophistication in such threats continues to rise.

New malware variants explode onto the scene at an unprecedented rate

One of the most noticeable increases we have observed in the security landscape is the sheer number of attacks and various methods for their distribution. Each month, Symantec security researchers block an average of more than 245 million attempted malicious code attacks across the globe. Most of the attempted threats have never been seen before. A combination of new distribution strategies, new media and Internet channels and increasingly advanced hacker techniques all add up to more malware. While attackers previously used to distribute a few threats to a large number of people, they are now micro distributing millions of distinct threats to smaller, unique groups of people. All of these factors combined together equal an unlimited number of unique malware attacks occurring.

New and Developing Trends

Cross-industry cooperation increases in an effort to tackle cybercrime

The Conficker worm, which grew to alarming proportions early this year, prompted collaboration across several groups to solve one of the most complex and widely spread threats to hit the Web in a number of years. The [Conficker Working Group](#) was comprised of industry leaders and people from academia and as they worked together, the combined efforts of the group proved successful. Security researchers, Internet Corporation for Assigned Names and Numbers (ICANN) and operators in the domain name system were able to work with several industry vendors to coordinate a response that disabled domains targeted by Conficker. This example

represents the type of collaboration that will likely increase in the industry in order to successfully address today's ever-more complex security threats.

Some old threats make comebacks

While much has changed on the threat landscape, some basic components remain, and, more interestingly, some older trends have made a comeback. As stated earlier, many cybercriminals have begun sending multiple distinct threats to smaller numbers of people, but there have also been notable examples of the older technique of sending a few threats to a massive number of people. The motivation for either method is frequently financial, as much of today's malicious Internet activity is, and the goal is often to steal personal data, distribute rogue antivirus software or propagate spam. There are of course those attacks that have no real purpose except to wreak havoc, but whatever the motivation, the various methods are prompting the need for a multi-layered defense that combines traditional detection with complementary detection such as reputation-based security models.

Deceptive methods that imitate traditional business practices continue to be utilized

One tactic cybercriminals are growing fonder of is imitating traditional business practices in an attempt to ensnare unsuspecting users. In today's world, business on the Internet is part of life. Cybercriminals recognize this and are clever enough to imitate business interactions. Even apart from business interactions, cybercriminals have figured out how to deceive people by presenting counterfeit messages. Examples of this include malicious advertisements or "malvertisements," which redirect people to malicious sites, or "scareware," which appear as antivirus scanners and scare people into thinking that their computer is infected when that's not really the case. The user is then lured into buying a fake product. Such deception is a prevalent security risk and is growing in use.

Internet threats continue to increase in volume and severity. It is important that computer users are on guard in order to make themselves less vulnerable to risks and threats. Staying abreast of the trends and developments taking place in online security is critical for both industry researchers and all computer users alike. ##

Spam's Hidden Victims: Mobile Users

By Cameron Brown

September 1, 2009 05:03 PM ET

Network World - Spam costs organizations \$712 per employee/per year, according to [Nucleus Research](#).

However, these staggering numbers don't even take into consideration one of spam's latest victims: enterprise mobile users. Spam targeted at smart phones is on the rise and becoming a growing security and productivity concern.

Protecting the inboxes of Blackberries, iPhones and other mobile devices requires new thinking. Spam, viruses and phish getting through to a desktop inbox is troublesome enough, but on a mobile device these threats present a unique set of security concerns and consequences, some of which are only just beginning to surface. Here are the problems and measures IT managers can take to combat them.

Distraction & Diminished Productivity: Spam in a mobile environment presents users with a significant productivity problem. Mobile users' time on-the-go is precious. While you can argue it's acceptable for desktop users to spend time weeding out the spam the corporate e-mail security solution allows through (typically 5%-20% of all email), or tracking down false positives, the argument can't fly for mobile users. Viewing, sorting and deleting messages takes significantly more time and effort on a small mobile device than on a traditional desktop. Screen space, storage and user time is too valuable in a mobile environment to dedicate any amount to spam.

Compounding matters, the traditional tools used to deal with false positives (e.g., access to quarantine) will often not be available or will not be easy enough to use on mobile devices, leading to calls to IT which waste the time

of several people. So, while some number of false positives may have been deemed acceptable for desktop users, the same number can cripple the average mobile user and present a significant distraction to the organization.

Difficulty Identifying Threats: Many regard the mobile device as inherently more secure than the traditional desktop PC, but because of its interface and limited functionality, it can hinder a user's ability to identify and avoid security threats. A primary concern for IT managers here will be phishing attacks. Smartphone users that do not have an effective security solution in place and are receiving spam or phish, do not have all the tools desktop users can employ to effectively judge which messages can be trusted.

Fonts, headers, images, text and links that may provide users with clues as to the true source or intent of a message may be skewed in a mobile environment. Users that are accustomed to mobile formatting issues may fall prey to phishing messages that they would not have been susceptible to in a desktop environment.

Viruses & Malware: The world of smartphone-based viruses and malware is largely yet-to-be-discovered. But if the past is any indication of the future, it is not a matter of whether these threats will take shape, but when. Because the particulars of how malware will exploit mobile device vulnerabilities are largely unknown, sufficient countermeasures do not yet exist on the devices themselves. This makes it imperative that, whenever possible, threats be stopped before they reach the mobile inbox, especially when you consider the challenge mobile users have in distinguishing threats from valid email.

A New Approach to Mobile Security

The approach to solving these problems is two-fold and must include both a technology and education component. From a technology perspective, you have to use tools that will protect both the desktop and the mobile inbox. While some security solutions may be well-suited for the desktop environment, they often will not adequately support the mobile environment. Keeping this in mind, you will want to consider technologies that are better able to address the unique security needs surrounding a mobile environment.

A best-in-class mobile/ desktop security solution does not necessarily mean the costliest one, but instead the one that has the right approach to the problem. It should yield a spam, virus and phish catch rate as close to 100% as possible. It must also provide the same easy-to-use self-management tools to users of mobile devices that are provided to desktop users to enhance security and reduce calls to IT.

Increasingly, leading e-mail security solutions are incorporating sender reputation components such as sender authentication and domain and IP reputation, and do not rely solely on the content of messages to identify spam. Solutions that rely solely on content analysis typically have higher false positive and spam rates, a frustration to users in a mobile environment. Sender reputation systems will be able to yield a higher spam catch rate, a lower number of false positives and supply both a more secure and productive mobile environment.

But technology alone won't cure the problem. Users must become involved in the security process for a mobile security strategy to be successful. By educating users about potential threats and providing tools to avoid them, IT managers will be able to better mitigate spam attacks and the associated consequences.

Topics to discuss with users include the potential security risks associated with spam, how to identify phishing attempts in the mobile environment, and ways to moderate security risk. Users that proactively manage their personal network of contacts (i.e. manage who they distribute contact information to, what they open, and what they respond to) will inherently be able to operate in a more secure environment.

Industry trends are aligning with this thinking. In a recent report from the [Messaging Anti-Abuse Working Group](#) (MAAWG), [A Look at Consumers' Awareness of Email Security and Practices](#), the group offered a number of recommendations to combat spam, and first and foremost is involving users in the security process. The report offers a number of suggestions, including educating users on reporting spam, identifying and handling false positives, and taking advantage of spam reporting capabilities.

By implementing a user-education component within your mobile security strategy, users can serve as the resource closest to the problem, rather than as a potential liability within an effective strategy. When taken

together, these steps will allow you to not only address the security threats mobile users are facing today, but begin preparing for those we will surely face in the future. These measures will also preserve the benefits that enterprise smartphone users have come to depend on.

Defying Experts, Rogue Computer Code Still Lurks

New York Times (08/26/09) ; Markoff, John

Conficker, a rogue software program that was discovered spreading across the Internet last November, continues to baffle top security experts working to eradicate the program and discover its origin and purpose. Conficker uses a flaw in Windows software to co-opt machines and connect them to a virtual computer that can be remotely controlled by the software's creators. More than 5 million computers, including government, business, and home computers in more than 200 countries, are now under the control of Conficker, giving the malicious program computing power far beyond the world's largest data centers. Computer security experts from industry, academia, and the government are working together in a highly unusual collaborative effort to stop the program. So far, their efforts have succeeded in decoding the program and developing antivirus software that removed the software from millions of computers. "It's using the best current practices and state of the art to communicate and to protect itself," says Conficker Working Group director Rodney Joffe. "We have not found the trick to take control back from the malware in any way." Researchers speculate that Conficker could be used for a variety of purposes, including sending massive amounts of spam, stealing information such as passwords and logins by capturing keystrokes, or delivering fake antivirus warnings to trick users into buying fake antivirus software. Perhaps the most concerning possibility is that the virus was not launched for criminal purposes, but rather by an intelligence agency or military in a foreign country looking to monitor or disable another country's computer network.

Infected USB Drive Wreaks Havoc on London Area Council IT Systems

(September 4, 2009) One infected USB drive cost the Ealing Council more than GBP 500,000 (US \$817,000) in lost revenue and repairs. The drive appears to have been infected with Conficker, which exploited a Windows Autorun vulnerability on the council's Windows 2000 machines and spread throughout the council's IT systems. The infection occurred in May and took days to clean up. During that time, the council lost an estimated GBP 90,000 (US \$147,000) from parking tickets it was unable to process and an estimated GBP 25,000 (US \$40,850) in library fines and fees.

[Editor's Note (Pescatore): For this to happen in May 2009, a lot of patches had to be ignored. This proves that even if you are running ooold Windows operating systems, if you don't patch you will pay.

(Northcutt): UK friends, I need help. In our Security Leadership Essentials class we talk about the importance of a smoking gun, proof that infosec is important and saves money.

Survey: Hackers on Vacation Before Q4 Saturation

Security Watch (08/26/09) ; Hines, Matthew

Malware and spam may not be diminishing, but a recent query of hackers at the DEFCON 17 conference in Las Vegas in August found that many network intruders work less during the third quarter in order to prepare for the fourth quarter holiday season. Security experts have observed for years that attacks seem to ebb during the summer months, but even the post-collegiate hacker demographic seems to lay low in the third quarter, according to Tufin Technologies, which conducted the study at DEFCON. Based on interviews with approximately 80 attendees of the security show, about 81 percent said that malicious attackers are much more aggressive during the fourth quarter, with 56 percent citing Christmas as the most popular holiday for corporate, not personal, attacks. New Year's is another popular holiday for hackers, with one in four survey respondents saying that hackers usually spend time on end-of-the-year threats.

Analysis: Still struggling to protect remote data

BY EARL HICKS JR. 08/28/2009

In 2006, one of my key responsibilities as a Justice Department senior security official was protecting sensitive legal data. When a [laptop was stolen](#) from an employee at the Veterans Affairs Department in May of that year, exposing data on 26.5 million veterans and military personnel, it left a serious and lasting impression on me.

So, when the Office of Management and Budget issued [Memorandum 06-16](#), the remote data encryption mandate, in June 2006 to better protect the flow of information in federal agencies, my reaction was to implement an immediate policy that required only encrypted removable media to be used when carrying sensitive but unclassified (SBU) data outside a Justice Department office. I anticipated a long-term effort to secure in-the-field government security operations effectively. I didn't expect that we'd still be grappling with it today, however.

The premise of the OMB mandate was to protect all information collected and stored on removable media. While a majority of government operations process information in offices, where security procedures are controlled by systemwide encryption programs, many federal employees conduct interviews and gather information in the field, where network and server-based encryption programs are not enabled. The mandate requires agencies to transport sensitive data only on mobile devices protected with a level of encryption described in the National Institute of Standards and Technology's guidance called Federal Information Processing Standards 140-2.

While laptops have received most of the attention when it comes to cybersecurity, a bigger vulnerability is the government's use of CDs, DVDs and flash drives, which can hold up to 10 times the amount of data on a laptop. We're not talking about the equivalent of file cabinets, but rather rooms of file cabinets. To achieve compliance, many agencies rely on NIST's list of approved flash drives. The challenge is FIPS 140-2 encrypted flash drives are expensive and many are not compatible with more than one computer or more than one user.

Another challenge in the remote data encryption mandate is the security of transcriptions of federal testimonies and interviews. Each year there are more than 300,000 federal cases that generate millions of pieces of testimony, evidence and witness accounts. Attorneys and law enforcement professionals collect most of this information in the field and they send them unencrypted to commercial firms to transcribe.

One of my challenges at Justice was ensuring the security of these transcriptions, because none of the transcription companies previously complied with the OMB memo, and transcripts were being processed on unsecured home computers and transmitted over the Internet. There have been two quick fixes: Transcriptionists now work on site in government offices or chief information officers are required to sign a waiver, if there is no approved transcription provider, to allow a nonapproved provider to do the work on unsecured networks and equipment.

Both of these solutions still have risky implications. The former decreases the productivity of others in the office because they have to give up workspace and equipment, and the latter compromises the integrity of the data.

Ultimately, the information security best practices that the remote data encryption mandate set out to achieve are imperative to the protection of witnesses, undercover agents and sensitive government contractor data that -- in the wrong hands -- could affect our nation's security. CIOs, procurement officers and inspectors general should be reevaluating their suppliers' use of government data to ensure it is not exposed to risk. While there is no worst-case scenario to drive all government agencies to act yet, it is only a matter of time before one arises.

7 Reasons Websites Are No Longer Safe

By Bill Brenner

September 9, 2009 01:59 PM ET

CSO - Conventional wisdom is that Web wanderers are safe as long as they avoid [sites that serve up pornography, stock tips, games](#) and the like. But according to recently gathered [research from Boston-based IT security and control firm Sophos](#), sites we take for granted are not as secure as they appear.

Among the findings in Sophos' threat report for the first six months of this year, 23,500 new infected Web pages -- one every 3.6 seconds -- were detected each day during that period. That's four times worse than the same period last year, said Richard Wang, who manages the Boston lab. Many such infections were found on legitimate websites.

In a recent interview with [CSOonline](#), Wang outlined seven primary reasons legitimate sites are becoming more dangerous.

1. Polluted ads

Many legitimate sites rely on paid advertisements to pay the bills. But Wang said recent infection statistics gathered by his lab show that they are often hiding malware, without the knowledge of the website owner or the user.

"A lot of sites supported by advertisers, rather than contracting directly with the advertiser, work through ad agencies and network affiliates," Wang said. "Some of these affiliates are less than diligent in reviewing content for flaws and infections."

Ads that incorporate Flash animation and other rich media are often rife with security holes attackers can exploit. When the user clicks on the ad, the browser can be (and often is) redirected to sites that download malware in the background while the user is reading the legitimate site. Someone in the ad-providing supply chain can be the culprit, though tracing a compromise back to them can be exceedingly difficult, Wang said.

Whatever the case may be, a downloaded Trojan is then free to gather up usernames, passwords and other sensitive banking data.

2. SQL injection attacks

SQL injection attacks are among the most popular of tactics and have been used in several high-profile incidents in the last couple of years.

SQL injection is a technique that exploits a flaw in the coding of a Web application or page that uses input forms. A hacker might, for example, input SQL code into a field that is intended to collect email addresses. If the application doesn't include a security requirement to validate that the input is of the correct form, the server may execute the SQL command, allowing the hacker to gain control of the server.

"The hacker essentially takes advantage of flaws related to shoddy site development," Wang said.

3. User-provided content

It doesn't take a genius to write a comment to a blog posting or something they see on a social networking site like Facebook or Twitter. The bad guys know this and are therefore taking the opportunity to pollute discussion threads and other sources of user-supplied content with spam-laden links

"You can get comment spam, completely irrelevant comments including links to sites trying to sell you stuff," Wang said. "They can also try posting full links to malicious sites or work in a little scripting, depending on the filter they are trying to work around."

4. Stolen site credentials

Using the types of malware and social networking tactics described above, as well as other means, attackers can steal the content provider's log-in credentials. From there it's no sweat logging into the site and making changes. It typically is a change so subtle and small that it escapes notice. The tiny bits of code added in can then steal the site visitor's credit card or other data.

5. Compromised hosting service

This one is similar to number 4, where the credentials of the content provider are stolen and hackers log in to make sinister changes. Through this vector, Wang said the bad guys could potentially poison thousands of sites the provider is hosting in one strike.

6. Local malware

The website you visit may be perfectly safe, but if there's malware hidden on your own machine you can unwittingly become part of the attack, Wang said. For example, the user can visit their online banking site, and when typing in a user name and password the Trojan is there to record that information and pass it back to the attacker, allowing him to go in later and empty out your account or that of others.

7. Hacker-engineered fakes

Finally, there's the problem of hackers trying to sell you fake merchandise that includes phony security software. If a box appears warning that your machine may have been infected and that you must immediately download a particular security tool to remove it--a common occurrence if you have visited a site that surreptitiously downloads malware onto your computer--it's a sure sign of trouble.

"You spend your \$39.95 and you get a worthless piece of software, and at the same time you have given them your credit card data," Wang said.

What is one to do if their website relies on ads and open access? Wang suggested IT security administrators use security scanners against anything coming in by way of third-party hosts and, for in-house apps and other online property, that developers redouble efforts to write more ironclad code.

For those who heavily rely on third-party forums, a wise practice is to take a daily scan of vulnerability reports that may affect those providers and to keep up to date on security patches that will harden your own environment against these threats, he added.

Raiders of the Lost Archive: SaaS, Disaster Recovery

By David Taber

September 9, 2009 11:48 AM ET

CIO - The starting point for SaaS applications: everything related to the apps is in the cloud, so data maintenance, redundancy, and recovery is the responsibility of the SaaS vendor. But the reality is more complex, so interesting subtleties have developed in the largest SaaS deployments. While this article is focused on Salesforce.com's applications, the lessons learned can be applied to nearly any SaaS vendor.

The Database Basics Let's start with the basics: the database underlying the application. For service continuity, nearly any SaaS vendor must have clustering or replication strategies for the customer data. Salesforce.com has a continuous replication of user data and a significant amount of redundancy in their data centers. As they have a clustered multi-tenant architecture, the backup and redundancy services are pretty sophisticated-and they have a lot of work to do. A main production cluster may have to handle 10,000 customers and the transactions of 100,000 users, and SFDC has an excellent record of uptime.

While data backup is included for free in SaaS applications, data recovery is free only if it's needed to recover from a *vendor's* error. If a customer needs to recover data to some historical point in time because of a user error, getting this data out is a chargeable extra. Given the number of simultaneous backup threads in flight at all times, you can imagine the complexity of unraveling the historical state of just your records from three weeks ago.

So the first lesson learned is, do a regular backup of your own data. If your SaaS vendor has an automatic export or archive function that pushes the data to local file storage, use it. If not, use a high-speed data loader. For a CRM system, a complete weekly snapshot taken early Saturday morning (US timezone) works best, and we typically recommend keeping 6 months worth of backup files. Don't forget to develop a strategy to back up attached files (as well as the pointers to them in the object model).

The Plot Complication But it's not quite that simple, because there is inevitably data that you'll need which is omitted from the standard export tool. You'll really want every scintilla of data from every table, including administrative logs. For example, a client of ours is dealing with the discovery phase of a lawsuit from a disgruntled employee, and they need to show that the employee was not logging into the system as often as they were supposed to do. Two years ago. The cost of recovering that data from the SaaS vendor involves fees that would make even lawyers blush.

Further, the SaaS backup systems will not do a snapshot of the system's object model, metadata, customizations, report definitions, or your code. These don't need to be backed up every week, but it doesn't hurt for configuration control purposes. Backing up these data may involve some outboard utilities to extract data through the application's APIs, but these utilities are usually open source and without charge.

Go Into the Archives The next thing to consider is archival: removing inactive or obsolete records from the online system. This may be required because of your company's information retention policy, performance issues (particularly with big reports), or a desire to reduce storage charges. I have yet to find a situation where data that's been untouched for 7 years needs to stay in a CRM system, and in certain businesses data that's more than 2 years old may never need to be seen again.

But CRM data is never a simple database, and removing records from the system can have complex repercussions. Depending on the vendor, CRM databases comprise between 10 and 200 tables, and user-level objects may create some really amusing pointer chains across tables. For this reason, some CRM objects can never be removed from a system. We further recommend that the Account and Opportunity objects never be removed, as they are at the center of a large number of pointers.

The easiest things to archive and remove from the system are objects at the leaf nodes of the pointer tree. For example, archiving old attached documents, emails, notes, and leads is fairly straightforward. However, the whole point of making an archive is to be able to get to the data if needed so make sure that each archive includes a "readme" file that includes the checklist of how the archive was made. Six months down the road, no one will remember how to unpack or interpret the data in the archive.

For objects that are more central to the CRM system, creating an archive can be quite complex. Properly archiving "Contacts" in Salesforce.com, for example, involves 10 extracts and a sequence of deletion passes that must be done in order.

The alternative? In many cases, it's easier to hide unwanted data than to actually remove it from the system. Hiding the data typically involves setting special record type values to indicate inactive data. The key to this strategy is making sure that all views, reports, workflows, trigger thresholds, and external interfaces are modified to exclude the marked records. This may sound complicated, but with proper configuration management this approach can be more straightforward than archiving the most deeply embedded of CRM data.

SANS: Security Ignores the Two Biggest Cyber Risks

Client-side application vulnerabilities and insecure web apps deserve more attention than operating systems bugs, says new research from SANS Institute

By [Joan Goodchild](#), Senior Editor

September 15, 2009 — [CSO](#) —

Two major cyber risks dwarf all others, but organizations are failing to invest in the proper tools to mitigate them, choosing instead to focus security attention on lower risk areas, according to [a report released Tuesday by SANS Institute](#).

The research, which draws upon data collected from March to August 2009 from thousands of organizations, claims companies give insufficient attention to today's risks and put their systems in peril by continuing to maintain the status quo with an emphasis on operating system patches and other outdated protection methods. Attack data for this research was drawn from TippingPoint appliances deployed at customer sites, while vulnerability data was collected via Qualys' scanning services.

The most surprising conclusion may be that client-side application software vulnerabilities pose the largest threat to network security as opposed operating system vulnerabilities, which tend to get more attention when it comes to patching. SANS claims many [spear-phishing attacks](#) exploit vulnerabilities in commonly-used programs such as Adobe PDF Reader, QuickTime, Adobe Flash and Microsoft Office.

"This is currently the primary initial infection vector used to compromise computers that have Internet access," the report states.

The report notes that most large organizations take at least twice as long to patch client-side vulnerabilities as they take to patch operating system vulnerabilities, choosing to place a higher priority on the lesser risk.

In addition to unpatched client applications, SANS said the other priority for IT security now should be attention to [web application vulnerabilities](#). Web applications constitute more than 60 percent of the total attack attempts observed on the Internet, according to the report.

"These vulnerabilities are being exploited widely to convert trusted web sites into malicious web sites serving content that contains client-side exploits," the report states. "Web application vulnerabilities such as [SQL injection](#) and [Cross-Site Scripting](#) flaws in open-source as well as custom-built applications account for more than 80 percent of the vulnerabilities being discovered."

Despite the enormous number of attacks, and despite widespread publicity about these vulnerabilities, most web site owners fail to scan effectively for the common flaws and become unwitting tools used by criminals to infect the visitors that trusted those sites to provide a safe web experience, said SANS researchers.

The two risks, and their tendency to be low priority for security, create a perfect storm for infection. With so many Internet-facing web sites vulnerable, and so many applications that contain bugs, it makes it easy for attackers to take advantage of unsuspecting web browsers. When users visit a trusted site, they feel safe downloading documents, or simply opening documents, music or video which exploit client-side vulnerabilities.

"Some exploits do not even require the user to open documents," the report states. "Simply accessing an infected web site is all that is needed to compromise the client software. The victims' infected computers are then used to propagate the infection and compromise other internal computers and sensitive servers incorrectly thought to be protected from unauthorized access by external entities. In many cases, the ultimate goal of the attacker is to steal data from the target organizations and also to install back doors through which the attackers can return for further exploitation."

The report's other conclusions include data that finds operating systems continue to have fewer remotely-exploitable vulnerabilities that lead to massive Internet worms. Other than Conficker/Downadup, no new major worms for OSs were seen in the wild during the reporting period, the report said. However, the number of attacks against buffer overflow vulnerabilities in Windows tripled from May-June to July-August and constituted over 90 percent of attacks seen against the Windows operating system.

The research also finds rising numbers of zero-day vulnerabilities.

"World-wide there has been a significant increase over the past three years in the number of people discovering zero-day vulnerabilities, as measured by multiple independent teams discovering the same vulnerabilities at different times. Some vulnerabilities have remained unpatched for as long as two years."

Security considerations critical in the cloud

[Angela Moscaritolo](#)

September 17, 2009

With the dragging economy as a driver, IT departments are increasingly realizing the benefits of [cloud security](#), but business leaders must ask themselves a few questions before handing over control to a third-party.

That was the message from analysts at a conference, "Gaining business and technical advantages from cloud, SaaS and hybrid security services," held Thursday in New York, and sponsored by consultancy IDC.

Cloud security is sometimes being driven – along with the cost saving benefits it provides – by what analysts referred to as "appliance fatigue," or the frustration of having to manage numerous on-premise security products.

But while some smaller organizations might ultimately replace all in-house solutions with cloud security services, the majority – especially larger organizations – see the technology as a complement to their existing solutions, analysts said.

Before turning to the cloud, though, corporate decision-makers must consider a number of factors, including what cost savings, scalability, reliability and functionality the third party will provide, said Brian Burke, program director of security products at IDC.

When evaluating moving to the cloud, security professionals should consider the cost of maintaining their current investments, potential changes to compliance regulations in the future, and whether the cost of a potential breach justifies the investment, analysts said.

Performance is one of the most important considerations for cloud security, and organizations must ensure that the vendor with which they contract has adequate internal protections to minimize latency and avoid disruptions in services. Burke warned that if latency is introduced, help desk calls could rise dramatically.

To combat this possibility, the cloud vendor should provide a service-level agreement to ensure reliability, analysts said.

In terms of functionality, businesses must realize that in today's environment, web and email threats are not mutually exclusive, so look for a cloud vendor which has expertise in both, Burke recommended. When looking to secure a [virtualized](#) environment in the cloud, choose a solution that provides a single console to manage all devices.

And, one of the key risk mitigation defenses is a multitenant architecture [different services with a shared code-base that appear different to end-users], though it requires high-speed routing, switching and load balancing, added Chris Christiansen, vice president of security products and services at IDC.

Cloud security through control vs.ownership

By Andreas M. Antonopoulos

September 15, 2009 05:57 PM ET

Network World - [Cloud computing](#) makes [auditors](#) cringe. It's something we hear consistently from enterprise customers: it was hard enough to make virtualization "palatable" to auditors; cloud is going to be even harder. By breaking the links between hardware and software, virtualization liberates workloads from the physical constraints of a single machine. Cloud takes that a [step further](#) making the physical location irrelevant and even obscure.

Traditionally, control of information flows directly from ownership of the underlying platform. In the traditional security model location implies ownership, which in turn implies control. You build the layers of trust with the root

of trust anchored to the specific piece of hardware. Virtualization breaks the link between location and application. Cloud (at least "public cloud") further breaks the link between ownership and control.

As we've examined in many previous columns we are rapidly moving from a location-centric security model to a more identity- and data-centric model. The unstoppable forces of ubiquitous connectivity and mobility have broken the location-centric security model and perimeter strategy, and left us searching for a better model for security. In the process, certain fundamental assumptions have also changed. When security is location-centric, then location, ownership and control are aligned. The logical security model coincides with the physical security model and a perimeter separates trusted (owned, local) from untrusted (other, remote). As we move beyond this model we have to examine the links between location, ownership and control.

Control of information is not in fact dependent on total ownership or a fixed location. An easy example is public key encryption. I maintain ownership of a private key and I control access to it. Usually the private key is stored in a secure location. But from the ownership of the key I can exert control over the information without having to own the rest of the infrastructure. I can build a trusted VPN over an untrusted infrastructure.

The key here is that public cloud computing requires us to exert control without ownership of the infrastructure. We can exert control and secure the information through a combination of encryption, contracts with service-level agreements and by (contractually) imposing minimum security standards on the providers. If those are in place, then there is no inherent reason why a cloud computing environment cannot be made secure and compliant. We do not need to own the assets in order to exert security, anymore than we need to own the Internet in order to trust a VPN.

Auditors and regulators are continuously adapting to new technologies and business models. As long as we can clearly demonstrate control through technology and contracts we should be able to make a cloud computing environment as compliant and as secure as a privately owned facility.

Talk to your auditors about their understanding of risk as it relates to location, ownership and control. Once you clearly separate the concepts you might find it easier to have that discussion.

The US Government is going Cloud with Google

[Apps.gov](#) is a new website that will help government agencies move their IT applications to the Cloud. Federal Chief Information Officer Vivek Kundra unveiled the initiative today at a press event at NASA's Ames Research Center.

The site uses technologies from Google and other big Cloud vendors, but the Government isn't going to just upload all of their data to Google. Kundra said the government would follow a two-prong approach. Classified data and processes will be managed through a government owned and operated platform developed by NASA called Nebula.

Less sensitive information could be offloaded to the Cloud, however, with the help of companies like Google.

Google specifically will be offering up a version of its Google Apps enterprise platform that is already at home in millions of businesses and universities.

Because government agencies have unique regulatory and compliance requirements for IT systems, Google is [currently getting its platform certified for use](#) in accordance with the [Federal Information Security Management Act](#):

FISMA certification for Google Apps. In July, we announced our intent to secure certification for Google Apps to demonstrate compliance with the Federal Information Security Management Act (FISMA), the law defining security requirements that must be met by all US Federal government information systems. Our FISMA process is nearing completion. We will submit a Certification and Accreditation (C&A) package to the U.S. Government

before the end of this year. Upon review and approval of the Google Apps C&A package, agencies will be able to deploy Google Apps knowing that it is authorized to operate under FISMA.

Google is creating a special "Government Cloud" that will be located on Google's present facilities, yet have more security features such as those required by FISMA. Google expects this separate cloud space to be open in 2010.

This could be a huge win for Google, who would be replacing legacy Microsoft and IBM products throughout the government. It will also be a big win for contractors like [Onix Networking](#) who [look to be doing](#) the migrations to Google Apps.

The government accreditation will also lend more respectability to Google's Apps platform. Google Apps IT admins will now be able to say that they use the same backoffice technology as NASA.

Will security concerns darken Google's government cloud?

Biggest challenge will be to overcome fears about cloud security in government setting

By Jaikumar Vijayan

September 17, 2009 07:10 AM ET

Computerworld - When Google Inc. launches its cloud computing services for federal government agencies next year, one of its biggest challenges will be to overcome concerns related to data privacy and security in cloud environments.

Earlier this week, Google said that it was [planning on offering cloud services such as Google Apps](#) to federal agencies starting in 2010. Google said it is speaking with several federal agencies about its offerings, which the company has assured will be fully compliant with the requirements of the Federal Information Security Management Act (FISMA). A FISMA certification is required for a service provider, such as Google, to sell to federal agencies.

At a cloud computing event in California, Google announced its plans to deliver a government cloud. At the event, a company executive noted that the government services would be hosted on Google's data centers, but on systems that are compliant with government regulations. The government cloud service would also be operated by individuals with the appropriate security clearances, and all data that is part of a government cloud service would remain in the U.S, the executive said.

How far such assurances will go in assuaging concerns related to cloud computing service, especially in a government setting, remains unclear.

Karen Evans, former de facto federal CIO under the Bush administration, said that using cloud services such as Google's could help federal agencies significantly reduce IT costs. But for many "the biggest concern is going to be the security and information assurance associated with a cloud service."

A lot will depend on the kind of FISMA certification and accreditation that Google's cloud services receive, she said. Under FISMA, federal systems are classified into three risk categories: low, medium and high. Each level has its own requirements, Evans said, adding that she hoped that Google will be certified and accredited at the highest risk levels. Then it's just a matter of agencies working out a service level agreement that spells out their security requirements. She added that agencies interested in using cloud services will probably be best served moving their external, Web facing applications first before considering more sensitive applications.

Meanwhile, Unisys Corp., a major provider of IT services to the government, Wednesday released the results of an online survey that looked at the issues affecting adoption of cloud computing.

Of the 312 respondents, about 51% cited security and data privacy concerns as the biggest impediment to adopting cloud services. The next highest barrier was integration of cloud-based applications with existing systems. Concerns about the ability to bring applications back in-house ranked third.

The results are consistent with previous Unisys surveys on the same topic and with what the company has been hearing from clients, said Sam Gross, vice president, global IT outsourcing at the company. "For us [the results] are not surprising," Gross said. "We have been surveying our customer base and doing quick polls for a long time. The numbers are always different, but never the ranking," he explained. "Security continues to be the number one concern for cloud computing."

Many of the concerns are related to issues such as inadvertent access to enterprise resources in a shared cloud infrastructure and accidental release of protected data. According to Gross, another big concern has to do with the level of access that a cloud provider might have to an enterprise's systems and data.

"They want to know how a cloud provider can assure that an administrator within a shared cloud infrastructure cannot gain access to or view their data," Gross said.

In a [report](#) issued earlier this year the World Privacy Forum raised other privacy issues that can arise when a government agency outsources to a cloud provider. For example, a federal agency that uses a cloud service to host personal data [could violate certain provisions of Privacy Act of 1974](#), especially if it doesn't have provisions for protecting the data in its contract with the cloud provider. In addition, federal records management and disposal laws may limit the ability of agencies to store official records in the cloud. The location of a cloud provider's operations may also have a significant bearing on the privacy laws that apply to the data it hosts, the report noted.

Such security concerns bubbled to the surface recently, when several groups [protested a \\$7.25 million plan by the city of Los Angeles](#) to replace its Novell GroupWise e-mail and Microsoft Office applications with Google Apps. Though city IT officials reiterated their plans to go ahead with the project, and Google itself has vigorously defended its security controls, the incident highlighted the continuing concerns with cloud computing.

The Internet is now like the Wild West: IBM consultant

500 per cent rise in malicious Web links: IBM report.

September 10, 2009 ([NETWORKWORLD](#))

"The Internet has finally taken on the characteristics of the Wild West where no one is to be trusted," said Sukhdev Singh, senior security consultant and regional X-Force expert, IBM Internet security systems, IBM ASEAN.

He was referring to the results of the tech giant's X-Force 2009 Mid-Year Trend and Risk Report. The report found that there has been a 508 per cent increase in the number of new malicious Web links discovered in the first half of this year. This problem is no longer limited to malicious domains or untrusted websites. The report notes an increase in malicious content on trusted sites, including popular search engines, blogs, bulletin boards, personal websites, online magazines and mainstream news sites.

"Safe browsing does not exist in today's cyberspace; neither is it only the red light district sites, such as gambling and pornographic sites, that are responsible for malware," Sukhdev added. "Search engines and social media websites like blogs and bulletins are also top categories of websites compromised now. We've reached a point where every website should be viewed as suspicious and every user is at risk. The threat convergence of the Web ecosystem is creating a perfect storm of criminal activity."

Web security is no longer just a browser or client-side issue; criminals are leveraging insecure Web applications to target the users of legitimate websites. The X-Force report found a significant rise in Web application attacks with the intent to steal and manipulate data and take command and control of infected computers.

On taking responsibility, Sukhdev points to application developers, not the operating system or Web server

vendors, for allowing their codes to be easily compromised. "Web application developers are not doing the necessary pre-release code checks," he said.

Phishing decreased dramatically in the first half of 2009 due to the shift away from financial targets, the report also found. Analysts believe that banking Trojans are taking the place of financial targets that were typically phished in the past, said IBM. Last year, phishing volume was, on average, 0.5 per cent of the overall spam volume. In the first half of 2009, this figure decreased dramatically to only 0.1 per cent.

Top 10 phishing urls--country of origin

1. US: 17.1 per cent
2. Romania: 14.3 per cent
3. China: 13.8 per cent
4. South Korea: 13.2 per cent
5. UK: 5.1 per cent
6. Canada: 5 per cent
7. Russia: 4 per cent
8. Japan: 3.4 per cent
9. Singapore: 2.6 per cent
10. Poland: 2.1 per cent

The report also found that:

- Vulnerabilities have reached a plateau.
- PDF vulnerabilities have increased.
- Trojans account for more than half of all new malware.
- Phishing has decreased dramatically.
- URL spam is still number one, but image-based spam is making a comeback.
- Nearly half of all vulnerabilities remain unpatched

World's nastiest trojan fools AV software... Pounces on banking passwords

September 18, 2009 ([TheRegister](#))

One of the world's nastiest password-stealing trojans evades detection by the majority PCs running anti-virus programs, according to a study that examined 10,000 machines.

Zeus, a stealthy piece of malware that sits on a PC and waits for users to log in to bank websites, is detected just 23 per cent of time by AV programs, according to the study (PDF) released by security firm Trusteer. Even AV programs with up-to-date malware signatures were unable to identify the infection a majority of the time, the

authors said.

Zeus, which also goes by the name Zbot and PRG, escapes detection using sophisticated techniques such as root-kit technology, the Trusteer report said. The company is able to detect it by examining the fingerprint Zeus leaves when it penetrates an infected PC's browser process.

A recent report estimated that Zeus is the No. 1 trojan, with 3.6 million infections in the US alone, or about 1 per cent of the installed base of PCs. Trusteer's study, which found Zeus accounted for 44 per cent of the banking malware infections, was consistent with that finding. After sneaking onto a PC, it sits quietly in the background until a user logs on to a financial website. It then sends the login credentials to a remote server in real time, sometimes by use of instant messaging programs.

Of Zeus-infected machines, about 31 per cent don't run AV at all and 14 percent run AV that's out of date. The remaining 55 per cent had AV programs that were up to date.

Gov-Owned USBs to be Used on DoD Nets

Navy CIO Robert Carey Updates Progress on Lifting Ban

September 21, 2009 - Eric Chabrow, Managing Editor

The Defense Department is taking steps to lift a 10-month-old ban on the use of most removable storage devices on Pentagon and military networks, but with a catch: only government-owned and procured USB flash media will be allowed.

"The bottom line is, the days of using personally owned flash media or using flash media collected at conferences or trade shows are long gone," writes Navy CIO Robert Carey in his [blog](#). "Unfortunately, it was our bad IT hygiene that resulted in the ban of this all too flexible use of storage media."

The commander of the U.S. Strategic Command last November suspended the use of USB flash media and removable storage devices on all DoD networks, including USB thumb drives, memory sticks/cards and camera flash cards, because some Navy personnel failed to follow procedures aimed at protecting the networks from viruses and safeguarding data stored on Defense systems.

In an update on the progress the Pentagon is taking to allow use of flash drives, Carey says the DoD Removable Storage Media Tiger Team, led by the Defense-wide Information Assurance Program, has been coordinating policy for incorporation into future Strategic Command operational guidance. The Navy and Marine Corps are drafting organizationally specific concepts of operations and communications tasking orders in preparation for secure USB flash media pilots once the DoD-wide ban is lifted.

"In the future," Carey writes, "we expect that a government-owned and procured USB flash media, that is uniquely and electronically identifiable for use in support of mission-essential functions on DoD networks will be permitted for use by authorized individuals. We are working on upgraded anti-virus and malware detection, alert and eradication capabilities as well as implementation of controls to deny network access to unauthorized USB flash media and revised operating procedures for scanning and cleaning flash media. Those who are authorized to use portable media devices will receive updated user training and awareness and be informed again of his/her accountability through compliance audits and inspections."

Until authorized USB drives are allowed, Carey says, the Navy will establish collaborative workspaces, file shares and portals within its networks to reduce reliance on USB flash media.

"While the future restricted use of flash media may seem somewhat draconian, the expanded use of portals and

collaborative work spaces keeps our information in the protected net-centric environment," Carey writes. "It is accessible with the proper identity credentials. Seems to me, we are actively working to make sure that access to information is balanced with the appropriate security controls."