GEORGIA TECH INFORMATION SECURITY CENTER

Emerging Cyber Threats Report for 2008

Leading technology experts share thoughts on top emerging Internet threats for 2008

The Georgia Tech Information Security Center (GTISC) will convene a panel of cyber security experts on October 2, 2007 to discuss emerging security threats and countermeasures that are expected to affect the digital world in the coming year. As one of the leading academic research centers focusing on information security, GTISC endeavors to create a collaborative environment for individuals, industrial, academic and government organizations to engage in real-world problem solving for effective information security and policy.

Based on GTISC research and advance interviews with the panelists, this report covers five emerging threats expected to increase and evolve in 2008:

Web 2.0 and client-side attacks

Targeted messaging attacks

Botnets

Threats targeting mobile convergence

Threats to Radio Frequency Identification (RFID) systems

While some of the emerging threats GTISC and the panel experts identified fit neatly within an established category or take advantage of a specific application, others share common characteristics and are often used in tandem by malicious elements. Financial gain is the primary motivator behind all five emerging threat categories.

In an effort to educate the online community about current and future risks, the GTISC report will describe each emerging threat, its impact, existing or potential countermeasures and any additional expectations for the coming year.

Web 2.0 and Client-side Attacks

As Web 2.0 makes Web applications more interactive and improves the user experience, it also pushes more code execution onto the client browser. Web 2.0 describes advanced Internet technology and applications including blogs, wikis, RSS and social book-marking. The Ajax programming language enables many of the technological advances found in Web 2.0, which primarily allow greater collaboration and interaction among Internet users, content providers, and enterprises. In the original Web medium, users simply viewed or downloaded Web site content. Web 2.0 lets users have more input into the nature and scope of Web content, with much of the Web site code execution occurring on the user's browser.

When browsing a Web 2.0 site, the user's browser silently makes requests and communicates with the Web application in the background. This scenario gives hackers the opportunity to embed malicious code on an otherwise legitimate Web site, which the user's browser will automatically execute. Ironically, the same time-tested exploit techniques—HTML code injection, SQL injection, cross-site scripting (XSS) and session hijacking—still work very well against Web 2.0 and unsuspecting users. Put another way, Web 1.0 exploits still work effectively against Web 2.0 applications. Since the malicious code is actually running on the client, many threats in this category are also referred to as client-side attacks. GTISC expects the available attack surface for Web 2.0 and client-side threats to become even larger in 2008 based on the following trends:

Attacks residing in the social networking environment—As social networking sites gain popularity, they will increasingly become a hacker target. Malicious attackers will install malware on social networking pages to infect unsuspecting visitors. Malcode on these sites will also drive traffic to other malicious Web pages in order to execute phishing scams or to monetize users in other ways

Mashup technology—Mashup technology is used by Web applications to combine data/media from multiple sources, locations and coding styles. For example, a retail store locator Web page will add location information from Google maps. The use of mashup technology makes it more difficult to validate the security and integrity of Web code.

Polymorphic exploitation—In response to standard regular-expression and heuristic-based signature protection that identifies and thwarts Web exploits at the network or host, attackers are dynamically altering their exploits each time a potential victim visits the malicious page—effectively creating a unique exploit with each request and making it impossible for signature-based protection engines to uniquely detect each attack instance.

Financial gain is the primary driver behind Web 2.0 attacks. Stealing private data, hijacking Web transactions, executing phishing scams and perpetrating corporate espionage are all motivators. Traditional security techniques focus on stopping file execution and viruses at the client's operating system (OS) layer. Unfortunately, it is far more difficult to protect users at the browser level. While some signature-based protection is able to detect one layer of Web exploit obfuscation, polymorphic exploitation poses a new problem. Proposed countermeasures for Web 2.0 and client side attacks include:

- Educating Web developers on the need for secure coding throughout the development lifecycle, with emphasis on input validation.
- Transitioning from finger-print or pattern matching protection to heuristics or behavior-based protection.
- Enabling protection engines to understand JavaScript just as the browser does.
- Utilizing feedback networks to analyze malicious Web sites, encourage remediation and improve content filtering at the browser level.

Web 2.0 and client side technology has been developing far more rapidly than the security technology required to protect applications. In 2008, GTISC hopes that security vendors and application developers can begin to close the gap.

"As the natural evolution of the Web progresses from 1.0 to 2.0 and beyond, more content and code from multiple and varied sources will be housed together on the client side, creating a highly complex environment for security governance and protection. In 2008, expect to see underground organizations shift tactics and focus more on Web 2.0, particularly mash-up technologies, leading to more abuses at the user end wherever possible."

Gunter Ollmann - Director of Security Strategy, IBM Internet Security Systems

"With Web 2.0, applications and data are moving off the PC and into the cloud, and threats and attacks will follow. Attacks now live in social networks and other client-side applications, and the everyday user is the target."

Rowan Trollope - Senior Vice President of Consumer Product, Symantec.

Targeted Messaging Attacks

Targeted messaging attacks will continue to advance in the coming year. Instead of focusing on corporate infrastructure, targeted messaging attacks are pinpointing individual users to steal authentication, permissions and private data. The amount of attack activity moving through e-mail, instant messaging (IM), peer-to-peer (P2P) networks and social networking communities will only increase.

The driving force behind the evolution of targeted messaging attacks is the hacker's desire to reach the target. As anti-spam technology and user education have advanced, attackers have had to invent new spam techniques to bypass filters, firewalls, gateways and more suspicious, knowledgeable recipients. GTISC predicts the following trends related to targeted messaging attacks in 2008:

Spam disguised as business content—While anti-spam software purges most blatant spam e-mails, incidents of spam designed to look like business content will increase. This includes PDF spam, Excel spam and experimentation with other file formats to make spam messages appear legitimate.

Attacks embedded in instant messaging—Attackers will embed links to malicious sites within otherwise legitimate instant messages. At the end of an IM conversation (and unbeknownst to the sender), a hacker will include a message urging the recipient to visit a malicious link. From there, various phishing scams will be carried out.

Financial gain and the rate of technological change drive new threats—The popularity of video sharing Web sites will make them a more common threat vector in the coming year. Hackers will install malcode within video content, which will then affect users accessing the video clips.

Attackers will also move beyond transient attacks like traditional phishing scams to more permanent threats like installing malware directly on a client machine (client-side attacks). Today most phishing sites only last for a few hours before they are detected and shut down. GTISC expects a subsequent upsurge in resident malware on computers, which represents a more long-lived attack that can silently collect user data undetected.

Evolving targeted messaging attacks will have far-reaching impacts on the Internet. Identity theft will increase, burdening financial institutions that agree to bear the cost of restitution. More importantly, the lack of trust on the Internet will challenge the productivity gains users expect from the online environment.

Filter security technologies such as anti-virus, anti-spam, anti-phishing and anti-malware will continue to make progress in blocking unwanted and/or malicious traffic. And many of the countermeasures needed for Web 2.0 security will also help prevent targeted messaging attacks. But the battlefield will become increasingly anonymous and decentralized, making traditional security approaches less effective. Ongoing user education must also occur to discourage users from "trusting by default" with regard to online interaction.

> "Attackers will continue to post malicious links as part of the user's everyday online activity—at the end of an IM string, hidden in a YouTube video or embedded in an Excel spreadsheet."
>
> **Paul Judge** - Senior Vice President and Chief Technology Officer, Secure Computing

Botnets

Botnets consist of a number of computers unknowingly controlled by a malicious server or master. GTISC currently estimates that 10 percent of computers on the Internet—representing tens of millions of computers—are infected by botnets. While the existence of botnets is not new, GTISC expects their uses and appearance in 2008 to include:

Perpetrating fraud—While botnets have traditionally been used to launch spam and denial of service attacks, they will increasingly be utilized for information theft in the future, whether as a form of financial fraud or corporate espionage.

Abusing the DNS infrastructure—Botnets will continue to play a significant role in:

Domain Name Server (DNS) abuse—In July 2007, GTISC researchers noted a large increase in the number of open recursive servers, and found many of them related to botnet infections. In two surveys, GTISC found nearly 17 million open recursive servers in a population of approximately 24 million open resolvers. Of these, nearly 600,000 were botnet-related. Further, approximately 2.4 percent of the open recursive servers would provide misleading or incorrect answers to questions about "phishable" domains, such as banks and anti-virus update sites.

Spreading via P2P networks. More botnets will be formed via P2P networks in 2008 to avoid detection by traditional intrusion detection and prevention systems (IDS/IPS). Once botnet activity is detected and traced back to a con-

trolling server, IDS and IPS devices can block connections to the server. However, the decentralized P2P environment enables hackers to administer botnets from multiple machines, helping evade existing security solutions.

Countermeasures against mobile convergence threats include security on the handset and more strategic security at the carrier network level. Anti-virus and anti-malware solutions for mobile devices will be promoted by carriers in the coming year. In addition, carriers themselves must explore improved security strategy and placement of firewalls and IPS within the IP multimedia subsystem architecture to better protect the network from threats introduced by the mobile customer base. GTISC also encourages more primary vulnerability research in the area of session initiated protocol (SIP) enabled devices related to VoIP and mobile convergence.

"We'll see a continued increase in the amount of fraud carried out by botnets in 2008, pushing the levels of users infected by a bot to 1 in 10 or greater. The entire IT community—service providers, security vendors, websites and users—all must play an active role in protecting from this evolving and expanding threat."

Wenke Lee - Associate Professor of GTISC and the College of Computing at Georgia Tech

Threats to Mobile Convergence

Just as threats to PCs have evolved, GTISC expects more threats to affect mobile devices in 2008. With the growing popularity of Voice over Internet Protocol (VoIP), instances of voice spam and voice phishing will likely increase. There are already hundreds of viruses targeting mobile devices and the first self-propagating malcode for mobile devices has already appeared. Future threats to mobile convergence include:

Voice spam, vishing and smishing—As more users merge their fixed existence with their mobile existence, hackers will utilize existing techniques to steal information or perpetrate fraud via smart phones and new mobile applications. This will include more voice spam and voice phishing scams, such as attackers registering their own long distance service and installing malcode on mobile phones that reprograms the phones to route all calls through the hacker's long-distance service. An example of "smishing" or short message service (SMS) phishing would be a hacker sending a text message to a user with a "click here" link to unsubscribe to an unwanted service. When the user clicks on the link, the premium SMS charges the user $10.

Denial of service (DoS) affecting voice infrastructure—Just as the recent Storm worm infected a large population of broadband users, a massive worm designed to take control of VoIP applications could adversely affect carrier infrastructure. Ironically, the more functionality and mobile applications carriers deliver, the more customers become a threat vector capable of introducing exploits into the carrier infrastructure. In one example of a DoS attack, a hacker could program 50 million mobile and/or VoIP phones to call 911 simultaneously in order to disable the Enhanced 911 system.

Countermeasures against mobile convergence threats include security on the handset and more strategic security at the carrier network level. Anti-virus and anti-malware solutions for mobile devices will be promoted by carriers in the coming year. In addition, carriers themselves must explore improved security strategy and placement of firewalls and IPS within the IP multimedia subsystem architecture to better protect the network from threats introduced by the mobile customer base. GTISC also encourages more primary vulnerability research in the area of session initiated protocol (SIP) device related to VoIP and mobile convergence.

"When massive numbers of users are infected, it poses a serious risk to the infrastructure. When the Storm Worm virus broke out last January, it infected 40 to 50 million of some 300 million users connected by broadband. To combat this, network and point-based security solutions need to be invented for the mobile environment."

Chris Rouland - Chief Technology Officer, IBM Internet Security Systems and IBM Distinguished Engineer

RFID Attacks

RFID applies to a bundle of technologies that remotely read or interrogate sensors over preset radio frequencies, linking the sensors to a particular ID. Analysts expect investments in extended Internet technologies such as RFID and sensor networks to fuel an $11.6 billion global market by 2012[1]. Emerging threats to RFID technology center on its deployment and the ability to trust the input and output of RFID sensors. GTISC expects the following attack trends to affect RFID in 2008:

Automated exploit tools targeting RFID—Technology has consolidated multiple RFID protocols, frequencies and formats into single RFID tokens and card readers—making it cheaper to deploy RFID in the consumer space—and easier for hackers to exploit RFID technology. Attacks against RFID will follow the same course as WiFi hacking. In the early stages, only the hacking elite could exploit WiFi devices, but as the technology gained popularity and became standardized, the first generation of automated WiFi hacking tools and instructions became available. In the near future, GTISC expects mainstream exploit tools to enable less technical hackers to attack RFID technologies. Many and varied attack vectors affecting RFID—The diverse deployment of RFID engenders a wide variety of threats and attack vectors. Unfortunately, RFID security protocols are extremely limited and all but the most recent versions/implementations can be easily bypassed. In one example, building entry systems using RFID cards require the user to pass a card over a sensor that interrogates the RFID chip and retrieves a unique ID number. The RFID system looks up the number in a database to verify the user's identity and allow or deny building access. Possible attacks against this RFID deployment include:

- The ability to track the user via RFID card even when not attempting building access.
- The ability to clone the RFID card, or to copy RFID cards from within or outside of the building.
- Causing the building entry system to crash by sending too many ID numbers at once (a form of DoS attack).
- Blocking the RFID reader's frequency to disable any cards from being read.
- Sending the RFID system a larger ID number than it expects in an attempt to exploit the system.
- Submitting inputs completely different from the ID number, such as SQL commands, in an attempt to exploit the system.

Existing countermeasures for RFID threats remain extremely limited. So far, the security industry has focused on strengthening the encryption of RFID communication and blocking unwanted/unknown RF signals. In the near future, RFID usage will expand into the consumer arena—replacing barcodes on grocery items, tracking patients in hospitals, and marking high-denomination monetary notes. As more people encounter RFID technology, GTISC expects greater emphasis to be placed on its security.

1 Global Extended Internet Forecast 2006-2012, Forrester Research, Inc., September 2006

"The inherent danger in attacking RFID systems is that, if a virus is placed on an RFID chip, the RFID reader picks it up and quickly spreads throughout the system. As RFID systems continue to gain popularity in 2008, particularly with credit cards and other personal and financial systems, this vulnerability will be a major threat for years to come."

Chris Rouland - Chief Technology Officer, IBM Internet Security Systems and IBM Distinguished Engineer

Financial gain and the rate of technological change drive new threats

Continuing an existing trend, new cyber threats to emerge in 2008 will continue to seek financial gain over personal glory. The ability to monetize Internet victims has lured powerful organized crime syndicates to the online environment and will continue to drive commerce in exploit techniques and vulnerabilities. Emerging threats to Web 2.0, client browsers and mobile devices will be increasingly intertwined. And the rapid rate of application development for these mediums has outpaced information security technology so far. While the emphasis on functionality over security may not change in 2008, GTISC expects collaboration between the security industry, carriers, ISPs, application developers and Internet users to begin closing the security gap.

GTISC Emerging Cyber Threats Panelists and Report Contributors:

Merrick Furst
Associate Dean and Professor, College of Computing at Georgia Tech

Richard (Dickie) M. George
Information Assurance Technical Director, National Security Agency (NSA)

George Heron
Vice President and Chief Scientist, McAfee

Mike Hunter
GTISC Research Scientist

Dr. Paul Judge
Senior Vice President and Chief Technology Officer, Secure Computing

Wenke Lee
Assistant Professor, GTISC and the College of Computing at Georgia Tech

Gunter Ollmann
Director of Security Strategy, IBM Internet Security Systems

Chris Rouland
Chief Technology Officer of IBM Internet Security Systems and IBM Distinguished Engineer

Caleb Sima
Co-Founder and Chief Technology Officer, SPI Dynamics, Inc.

Rowan Trollope
Senior Vice President of Consumer Products, Symantec

GEORGIA TECH INFORMATION SECURITY CENTER