



# GTISC

GEORGIA TECH INFORMATION SECURITY CENTER

Security Summit **2010**

EMERGING  
[ CYBER THREATS ]  
REPORT **2011**



# EMERGING [ CYBER THREATS ] REPORT **2011**

## [ Table of Contents ]

- 2**    Introductory
- 3**    Proliferation & Sophistication of Botnets
- 6**    Pervasive Devices & Social Networking
- 8**    Cyber Threats Targeting Physical Systems
- 10**   Privacy & Responsibility

## **Growing sophistication of botnets, pervasive devices and social networking, and threats to physical systems will demand increased vigilance in 2011**

Cyber threats cannot be adequately thwarted unless they are fully understood. The Georgia Tech Information Security Center (GTISC) therefore remains dedicated to thoroughly researching, analyzing and understanding the motives and methods of cyber attackers, and sharing that information with the community at large.

On October 7, 2010, GTISC hosted its annual Security Summit, bringing together leading experts from academia and industry to discuss the ever evolving nature of cyber security threats and the various measures that can be taken to defend against cyber attacks.

Further leveraging its own in-house research as well as in-depth collaboration with security industry leaders, GTISC developed the following Emerging Cyber Threats

Report for 2011. The report draws upon a wide range of security research to uncover and explain the top three trends that will strongly impact the security landscape in 2011. These include the further proliferation and sophistication of botnets, attacks on pervasive devices and social networking, and the impact of cyber security issues on physical systems. Common features of these threats are their increased sophistication and the monetary gain motives that drive them.

“Traditional cyber security has been largely reactive in nature,” said Mustaque Ahamad, director of GTISC. “Our goal is to remain at the forefront of security research and collaborate with our partners so that we may begin to develop solutions to impending cyber concerns at an early stage before they become widespread sources of harm. The GTISC Security Summit and Emerging Cyber Threats Report are two key facets of our efforts to keep security discussions alive and cutting edge, as well as to engage the broader community in our programs.”

# [ Proliferation & Sophistication of Botnets ]

As malware numbers continue to climb, traditional forms of security such as signature-based antivirus become ineffective. According to Wenke Lee, a professor at the Georgia Tech College of Computing, cyber criminals now have automated tools capable of releasing very large volumes of malware with extreme variety and sophisticated features.

With security researchers now uncovering close to 100,000 new malware samples a day, the time and resources needed to conduct deep, human analysis on every piece of malware has become overwhelming. According to McAfee, the first six months of 2010 was the most active half-year ever for total malware production.<sup>1</sup> Today, automated analysis technologies are being used to keep up with this volume, but according to Lee, they lack the precision needed to decipher purposely compressed, encrypted and obfuscated malware.

Botnets are collections of software agents that run automatically to compromise large numbers of machines for malicious activity including spreading spam, stealing log-in credentials and personal information or distributing malware to others. Symantec reported in August that the percentage of spam sent from botnets had increased to 95 percent of all spam.<sup>2</sup> Meanwhile, M.A.D. Partners, LLC estimates that more than 100 million computers are currently part of criminal networks.<sup>3</sup>

When it comes to botnets, targeted attacks are on the rise, including attacks launched on the U.S. Federal government. Symantec also reported in August that the government/public sector had become the most targeted industry for malware with 1 in 74.6 emails being blocked as malicious.<sup>4</sup>

One current trend in the world of botnets is the release of large-scale botnet attacks to hide more targeted malware. For example, cyber criminals or even nation-states will either send out a widespread attack or take advantage of an existing widespread attack to launch similar malware targeted towards a specific organization such as the Federal government. That way, their targeted attacks are much more difficult to trace or attribute.

Earlier this year, organizations including Google, Adobe and a few dozen others in the commercial sector acknowledged that they had been the victims of a highly targeted attack known as Aurora. According to Gunter Ollmann, vice president of research at Damballa, "the Aurora botnet was targeted against large international businesses with the goals of network infiltration, theft of business secrets and modification of critical system data."

"Today's botnets are sophisticated, money-making machines that not only hijack the data present upon the victim machines or compromise the business networks they are on, but have also become the backbone for an entire criminal ecosystem. Given the breadth of criminal enterprise and methods of monetizing botnets, everyone is at risk," said Ollmann.

"Modern malware is almost exclusively authored by professional criminals that act in the domain of organized crime," agrees Paul Royal, a research scientist with GTISC. "Given the enormous popularity of inexpensive malicious software generation kits, even the technically illiterate can easily build stealthy malware with sophisticated anti-detection mechanisms. These days, most malware is sheathed inside a series of executable protections, which include obfuscations that make the malicious executable look like legitimate software."

*"The bad guys are getting more and more knowledgeable at figuring out how to get the most bang for their buck."*

— **Paul Royal**, Research Scientist, GTISC

According to Royal, some malware frequently self-updates so that it is no longer detected by traditional security technologies. He pointed to last year's Waledac outbreak as a prime example of a self-updating botnet. In an experiment conducted by GTISC, two Waledac samples showed very different detection rates by security tools, one being detected by 38 out of 39 tools and the other only being detected by 11 out of 39 tools, demonstrating the efficacy of self-updating malware.

One way to combat the explosion of malware samples, says Royal, is through the use of a scalable, transparent (meaning the attackers cannot detect it) and automated analysis system to obtain actionable malware intelligence and leverage the intelligence in meaningful ways. GTISC has developed such a system, called MTrace. Information from MTrace was used to help take down the large, data-stealing botnet named Mariposa, which was

Continued on Next Page

<sup>1</sup> Source: McAfee Threats Report: Second Quarter 2010, McAfee Labs, [http://www.mcafee.com/us/local\\_content/reports/q22010\\_threats\\_report\\_en.pdf](http://www.mcafee.com/us/local_content/reports/q22010_threats_report_en.pdf)

<sup>2</sup> Source: August 2010 MessageLabs Intelligence Report, Symantec Corp., [http://www.marketwatch.com/story/symantec-announces-august-2010-messagelabs-intelligence-report-2010-08-24?reflink=MW\\_news\\_stmp](http://www.marketwatch.com/story/symantec-announces-august-2010-messagelabs-intelligence-report-2010-08-24?reflink=MW_news_stmp)

<sup>3</sup> Source: <http://www.mobileactivedefense.com/faq/>

<sup>4</sup> Source: August 2010 MessageLabs Intelligence Report, Symantec Corp., [http://www.marketwatch.com/story/symantec-announces-august-2010-messagelabs-intelligence-report-2010-08-24?reflink=MW\\_news\\_stmp](http://www.marketwatch.com/story/symantec-announces-august-2010-messagelabs-intelligence-report-2010-08-24?reflink=MW_news_stmp)

discovered in the spring of 2009. At its peak, the Mariposa botnet included more than one million members, including compromises in half of the Fortune 1000. GTISC began collaborating with others in the community, and together formed an international working group to fight Mariposa, which consisted of members from security providers and key law enforcement agencies including the FBI. By January 2010, all of the command-and-control domains for the botnet were shut down and its operators were arrested. At the time of arrest, 800,000 financial credentials were found on one of the operator's home computers, all stolen using Mariposa.

Another alarming trend in the botnet space is the resurgence of previous attacks, which occurred recently with the large, spamming botnet, Kraken. The Kraken botnet, which at one point comprised about 650,000 members including 10 percent of the Fortune 500, reemerged about a year after its takedown, bootstrapped by another botnet that acted as a malicious installation

## [ Botnet Research at GTISC ]

At GTISC, researchers are working to come up with an accurate and scalable method of analyzing vast quantities of malware. One such technique is analyzing anomalous behavior of malware at specific "choke points." For example, malware typically needs to communicate from a host computer to the outside world to conduct activities such as sending out spam or transmitting sensitive data. Thus, by allowing outgoing data only if it is authorized by a user, we can stop malware traffic, which by definition is not generated and authorized by a user. A prototype system developed at GTISC can copy the email message authored by the user from the message window on the screen, verify that the outgoing email traffic matches the contents, and allow only such email traffic to leave the host computer.

GTISC is also conducting research into which web sites are origin points for malware. Typically, the 100,000 samples of malware being found each day are only coming from a few thousand sites. According to Wenke Lee, sites being used to spread malware and botnets display distinct characteristics that differ from legitimate sites. These characteristics can include similar domain names and network providers. Based on these characteristics, GTISC researchers can develop suspicious scores for web sites, which can be used in warning users not to click on certain sites to reduce their chances of being infected by malware.

GTISC has also developed and deployed a malware analysis sandbox, which processes over 15,000 new malware samples a day. Called MTrace, the system is a scalable, automated malware analysis framework that uncovers certain characteristics of each malware sample and aggregates the information into a malware intelligence database that is used by corporate security groups, hosting providers, domain registrars and law enforcement.

*"The innovation within the botnet ecosystem is amazing. If there are ways of monetizing access to a botnet victim's computer, their data, or even the way they use their computers, then the bad guys will be experimenting with it."*

— **Gunter Ollmann**, Vice President of Research, Damballa

service. This example illustrated that cyber criminals are indeed making efficient reuse of malicious software, and are also becoming increasingly sophisticated as various groups within the criminal underground work together to share malware and attack methods, making additional money by selling malware code, compromised systems and specialized attack services to each other. GTISC was able to discover and take down this second occurrence of Kraken through intelligence gathered from MTrace. According to Royal, this shutdown took exceptional persistence, as the Kraken operators employed many resistance techniques including continuously changing their domain names and hosting providers.

"New threats such as identity laundering and reputation hijacking have appeared in recent times in order to maximize the profits derived from building and maintaining large international botnets," said Ollmann. "We have found that between 20-25 percent of residential computer systems are not only compromised with malware agents, but are under active control by their criminal masters. The spreading of botnets is a highly profitable business that is constantly attracting new criminals to the fold and driving new innovation."

Interestingly, alongside increasing sophistication, Jon Ramsey, CTO of SecureWorks says we're also seeing a "back-to-basics" trend out there with the reuse of simplified attack methods, such as socially-engineered emails containing malicious links. This was the initial infection vector for the recent "Here You Have" mass-mailer worm which struck U.S. corporations and government agencies, taking down many mail servers.

Paul Judge, chief research officer at Barracuda Networks, says, "The 'Here You Have' email worm, while simple in nature, was just different enough to persuade many users to download and run the payload. The emails offered up a type of file that people trust and then delivered a file type that most people are unfamiliar with – a .scr file. This simple outbreak easily could have been used for something more malicious to keep the worm alive for a long time."

Ramsey continued, "This points to the importance of continual investment in the security community so that we can maintain our innovative edge. The criminals are going back to the basics because the basics still work. We need to increase the effort and risk required by cyber criminals to launch attacks, while reducing their rewards."

Yet another trend on the rise is the compromise of legitimate sites or the use of information stolen from them. In the middle of last year, a banner ad on the *USA Today* web site was hacked, leading visitors to a malicious site regardless of whether they clicked on it, said Royal. Additionally, information extracted from a hack of PayChoice, one of the nation's largest payroll organizations, was used to spread an especially tricky bot called Zeus, which inserts extra fields into a victim's browser when they visit a bank's web site in order to maximize the information stolen. "Given the popularity of the web as a medium for e-commerce and social media, the threat landscape will evolve even further as the demand for new features spawns the use of new, often only lightly tested software," says Royal.

Ramsey pointed to virtualization as another key area that will result in further security issues in the future. "So far we have seen proof-of-concept exploits specifically targeting virtualization technologies," said Ramsey. "However, I think that within the next six to eighteen months we will see a rise in attacks in this area." Ramsey also cited data security as a key issue. He said that in the future, instead of securing just systems, he sees the industry also securing the data itself by embedding it with technologies like digital rights management so that the data can in essence protect itself, no matter what system it ends up on.

Chris Rouland, CEO and co-founder of Endgame Systems, believes that the cloud will be the enabler for delivering more scalable, comprehensive and affordable security moving forward. Rouland sees the cloud playing a major role in both delivering antivirus protection, as well as in sharing threat intelligence. Through the cloud, computers can pass threat information back and forth, so that if one organization uncovers a specific attack, that data can be quickly and easily shared among a wide network of security professionals.

"Nowadays, organizations need to be focused not only on their traditional perimeter defenses, but also look into external services for threat intelligence and continuous, real-time monitoring," said Rouland. "Whereas at one time managed security services were nice to have, they are now mandatory, the same way that your burglar alarm is generally better managed by someone else."

In addition to cloud-based security, Rouland sees IP reputation services as playing a greater role in fighting botnets in the future. As IP reputation begins to become integrated into every transaction on the Internet, these services will make it easier to detect whether or not to interact with certain systems based on their previous online behavior.

# [ Pervasive Devices & Social Networking ]

According to Patrick Traynor, assistant professor at Georgia Tech's School of Computer Science, the sheer volume of cell phone users around the world indicates a current need for proactive mobile security measures. While more than 1.5 billion people use the Internet daily, over 4.5 billion use a cell phone every day, creating an attractive target for cyber criminals. Over the next five to ten years, this number will double or even triple, as phones become less expensive and more powerful, enabling people even in rural areas of the world without sophisticated infrastructure to easily get on the Internet. According to M.A.D. Partners, "Smartphones are the new computers. An estimated 2 billion of them will be deployed globally by 2013."<sup>5</sup>

Coupled with this immense volume is the fact that despite the ever-rising amount of applications users are downloading to their phones (including banking software), they are still viewing them simply as phones versus mini computers. This is dangerous, says Traynor, because people tend to think of their phones as innocuous, protected devices, which these days they are not.

Additionally, phones have traditionally been so diverse that it was difficult for cyber criminals to effectively take advantage of them. But now we are seeing a move towards homogeny where the majority of phones are being built on a few core operating systems including Windows, Android and Mac, making the smartphone world look more like the desktop world, which according to Traynor could cause further security concerns. "The traditional security measures we have been using on computers have not been working that well," he said. "Worse still, phones have further constraints such as battery life that make traditional security measures – which require the continuous running of software in the background – unrealistic."

Combine these factors with the fact that GTISC and other security researchers have uncovered rootkits, botnets and other malware being created specifically for phones, and it becomes clear that new security measures for smartphones are needed immediately. The first worm for the Apple iPhone was uncovered in late 2009 in Australia. While it only seemed to affect "jail-broken" phones, meaning the users had removed Apple's protection mechanisms to allow their phones to run any software, it was still indicative that we had a serious problem on our hands, according to Traynor.

"This is a big sign of what is to come," he said. "Knowing that people are carrying around sensitive information including their exact location and financial data on their phones, attackers are seeing huge value and are actively trying to subvert these devices."

*"You don't just reach out and touch someone anymore, they reach out and grab you."*

— **Patrick Traynor**, Assistant Professor, Georgia Tech School of Computer Science

Traynor also added that while jail-breaking is not currently widespread, there are tools out there that are making it extremely easy to do, so it is logical to assume that more individuals will be jail-breaking in the future to obtain greater control over their phones.

Another security issue pertaining to phones, much like computers, is that they offer so many different gateways of attack. Attackers can take advantage of smartphone users through email, Internet applications, text messaging and even through call fraud, i.e., calling users pretending to be their bank or another reputable organization and spoofing the caller ID to make the call look legit. Users need to be as skeptical on their phones as they are on their computers – not giving away sensitive information to callers, being selective about which emails and text messages they open, and about which applications they install on their phones.

According to Robert Smith, CTO and co-founder of M.A.D. Partners, "The single biggest thing threatening any enterprise today on a security basis is mobile. Furthermore, mobile phone application stores are the greatest malware delivery system ever invented by man."

When mobile phone vendors receive applications to sell, they run tests to ensure that the applications do what they say they will, but they do not receive the source code to determine what else the application might do. In some cases, said Smith, there isn't much of an approval process at all, and it is feasible that someone could write a virus and have it for sale in an app store an hour later.

According to Smith, everyone within corporations from the C-level down is clamoring for iPhones and other cutting-edge devices, essentially dictating the consumerization of the corporate network. This can lead to serious issues since these devices were not intended for use in a corporate environment. Smith added that less than one percent of all smartphones have any form of security. In addition to security issues, the proliferation of consumer mobile devices within corporations can also lead to compliance problems. Organizations across industries have sets of compliance laws that they are obligated to follow, and as much as a single unprotected mobile device on the network can cause them to break the law.

Corporations therefore need to be just as vigilant about mobile security as individual users, whether it is through developing and enforcing usage policies or employing service providers that

<sup>5</sup> Source: <http://www.mobileactivedefense.com/blog/>

*“Businesses should make use of available forms of protection. Further, users should not simply rely on workplace safeguards, but should also take these security technologies with them when they are not in the office.”*

— **Paul Judge**, Chief Research Officer,  
Barracuda Networks

can protect their networks from mobile attacks via cloud-based security services. According to Smith, the “mobile 9-1-1” is a reality, and the real question is when, not if, it will happen. “As more and more people use the devices,” said Smith, “the criminals will come in waves.”

Along with the rise in smartphones has come an immense increase in social networking, both on phones and traditional computers. While privacy issues with social media are fairly well-recognized, additional security risks pertaining to Facebook, Twitter and other platforms are not as widely discussed. According to Judge of Barracuda Networks, the tremendous success of social networking sites is causing concern for security professionals. With more than 100 million accounts on Twitter and more than 500 million on Facebook, attackers are taking advantage of the social networking craze as a new medium for launching insidious attacks.

While many of the accounts on Twitter and Facebook are legit, Judge pointed out that there is a significant number of accounts that are not legitimate or not in use. In fact, only about 30 percent of Twitter accounts have been created by true Twitter users, those users who actively use the service on a regular basis (follow 10 or more accounts, are followed by 10 or more accounts or have tweeted 10 or more times). Cyber criminals are getting more and more sophisticated in their efforts to appear as trustworthy users on these sites, tricking people into “friending” or following them and clicking on their status updates, which often lead to malicious web sites. One key example of a social networking attack is the Koobface (Facebook inverted) worm that spread through social networking sites last year, attempting to steal users’ personal information, redirect them to malicious sites and recruit their systems for use in botnets, among other insidious actions.

Security professionals at Barracuda Networks are studying user behavior on social networking sites in an effort to decipher between legit and fake accounts, and are also studying the crime rate on Twitter to determine what percent of the accounts created have been suspended for inappropriate behavior. In October 2009, the crime rate on Twitter rose to 12 percent, says Judge, accounting for one in eight accounts being suspended.

.....  
<sup>6</sup> Source: Lemire, Christy. “Twitter hack attack hits home for AP writer.” The Associated Press, September 9, 2010. [http://www.herald-review.com/business/technology/article\\_032654a0-bb7c-11df-9e1d-001cc4c002e0.html](http://www.herald-review.com/business/technology/article_032654a0-bb7c-11df-9e1d-001cc4c002e0.html)

In another study over the past four months, an average of 130 instances of malware were found every day simply by searching for content on popular, “trending” topics via Twitter, Google, Yahoo! and Bing. “While the issue of malware on social networking sites and popular search engines is quiet, it is consistent and happens around the clock, all day every day,” said Judge.

Just last month, a reporter for The Associated Press announced that someone had hacked into her Twitter account, sending out about one hundred nonsensical and inappropriate tweets that led her followers to dangerous links.<sup>6</sup> In addition to not trusting unknown users or suspicious links on social networking sites, Judge advises the public at large to make use of available forms of protection such as URL filtering, malicious JavaScript detection and URL reputation services. He also warns that users should not just rely on workplace safeguards, but should also take these security technologies with them when they are not in the office.

Beyond traditional forms of security, social networking is demanding new research and technology specifically focused on identifying malicious accounts. Both GTISC and security companies are conducting significant research on these types of protection. Judge adds that eventually social networking users will expect providers like Facebook and Twitter to do their part in cleaning up fake accounts, much like they expect search engine providers to clear malicious links from their search results today. While services like these are now being offered by software-as-a-service providers that offer security in the cloud, it will eventually be up to the social networking sites and/or ISPs to deliver a safer Internet experience to users, says Judge.

## [ **GTISC Research in Mobile Security** ]

### **Call Provenance**

In order to help combat mobile phone threats, Georgia Tech is working on a project through which users can figure out where calls are really coming from, as well as the path the call took to get to them. For example, if you get a call from your local bank in the U.S., but discover that the call actually came from Eastern Europe, you can easily decipher that the call is not legit.

### **Remote Repair**

To help solve the malware problem on mobile phones, Georgia Tech is developing a service called Remote Repair. Through Remote Repair, instead of having to take infected phones back to the store for assistance, users could obtain remote assistance from either their phone providers or a third party. The provider would maintain records of issues on the overall phone network and be able to match the issues to problems on specific phones, providing a fast, efficient fix for common malware attacks. As mobile phone attacks increase, this type of solution will become even more necessary, as phone providers will not be able to keep up with the huge demand for phone fixes in the store.

# [ Cyber Threats Targeting Physical Systems ]

Once botnets and other types of malware wreak havoc on computers, there is a rising concern that the damage done could also cause the destruction and malfunction of physical systems in areas including critical infrastructure and even information technologies deployed in the healthcare sector. While there are differing opinions in terms of how real this threat to physical systems is, according to Ahamad of GTISC, "It is known that there are vulnerabilities that would allow cyber criminals to reach into physical systems, and we are aware of the sophistication of today's attackers, so to think that physical systems are not at risk is really having your head in the sand."

David Batz, manager of Cyber & Infrastructure Security at the Edison Electric Institute agrees. "I first want to stress that the sky is not falling," he said. "However, there is a threat out there to physical systems that we have to work together to manage."

Ramsey of SecureWorks used the analogy of "preparing the battlefield" to describe the cyber to physical threat. He said that nation-states not friendly to the U.S. are plotting and testing the waters for the takedown of our critical infrastructure including the power grid, communications systems, emergency services and financial systems as a means of preparing the battlefield for invasion. In other words, the compromise of these systems would cause the confusion, chaos and hysteria needed to make it easier for these nation-states to physically invade our country.

Ramsey stated, "We already saw this scenario played out during the Russia/Georgia conflict in 2008. At the same time Russia commenced physical attacks on Georgia, cyber attacks were launched against the country's government communications systems, media outlets and banking institutions, knocking many of them offline for long periods. This made it extremely difficult for Georgian citizens to receive emergency warnings, get updates on the armed conflict and conduct business."

Most recently, SecureWorks discovered ample evidence to suggest that the "Here You Have" worm, which took down U.S. corporate and government email servers in September, originated with a cyber-jihad organization. "This cyber attack did minor damage compared to what could have occurred if the authors had acted with more malicious intent," said Ramsey. "Between the existing vulnerabilities on physical systems and evidence of increasing attacks on our critical infrastructure, it is clear that the physical threat is real."

Batz went on to add that the persistence of attackers alone is reason enough for concern. "In recent years, we have seen an emerging environment of persistence on the part of attackers," he said. "Whether it is a representative from a competing business, someone with strong philosophical or religious motives or a representative of a nation-state, there are individuals out there with the determination and resources needed to make a concerted investment in launching whatever attacks they can to realize their objectives."

*"As physical systems become more information-driven, the kind of attacks we have seen in other areas will show up here as well. This is a true concern that requires the collaboration of a wide range of experts, not just technologists, to fully understand and prevent."*

— **Mustaque Ahamad**, Director, GTISC

The move towards smart grid, or more automated power grids, is in full swing. The smart grid brings with it a plethora of benefits including greater efficiency and reliability, and the simpler incorporation of renewable energy sources to lessen environmental impact. However, as more data is filtered into and out of the grid, and as it becomes more connected to the Internet and reliant on digital communications, it is being opened up to greater risk. According to an article in *IEEE Security & Privacy*, "As the grid matures, it will be important to devise a defense supervisory system that can efficiently process myriads of data to evaluate system status, identify failures, predict threats, and suggest remediations."<sup>7</sup>

Experts from Landis+Gyr, providers of smart meters and other grid technologies, agree. According to Heath Thompson, CTO, "Security for the smart grid is clearly one of the top concerns in the entire energy sector right now, and is a strong focus for utilities, vendors and regulatory agencies."

While security measures and technologies for utilities are still in the early adopter phase, organizations are working hard to ensure that their utility is not the first to appear in news headlines for having their infrastructure compromised by malware. According to Thompson, forward-thinking utilities are beginning to do a lot of work around authentication, encryption and ensuring the integrity of their computing infrastructure, but there is still a long way to go in terms of developing comprehensive, formal security plans and procedures.

Stephen Chasko, principal security architect at Landis+Gyr, said that one main threat to the electric grid is cyber terrorism, including the disconnection of power for a large population and the disabling of devices, requiring a physical visit to every device to reconnect power. Thompson added that there is also an economic

<sup>7</sup> Source: Khurana, Himanshu, Mark Hadley, Ning Lu and Deborah A. Frincke. "Smart-Grid Security Issues." *IEEE Security & Privacy*, January/February 2010: 81-85.

## GTISC Research in Countering Cyber Physical Threats

Researcher David Dagon is conducting key investigations that will enable GTISC to work with the medical community to understand how regulatory issues may impact timely patching of infected computers and medical devices in hospitals. He is also conducting research that will help rectify issues being caused by the widespread and unmonitored use of USBs within hospitals and other medical facilities.

The MedVault project at Georgia Tech is exploring several security technologies to enable better patient control over how health information is used. Through the project, Georgia Tech is also developing new techniques for the storage, maintenance and control of electronic medical record (EMR) data that permit open sharing among a wide variety of legitimate users while protecting the data against unauthorized use and disclosure.

threat in the form of power theft when it comes to utilities' increasing connection to the Internet. As with botnets, power theft criminals will deliberately fly under the radar, making comprehensive security extremely important for combating this threat.

Per Chasko, while well-known incidents such as the massive power failure in Brazil in November 2009 fall into a gray area of conjecture in terms of whether they were actually caused by cyber attack, there is an active community out there that Landis+Gyr and others have seen trying to attack power systems. While the electric grid has been a main focus for both attackers and the utilities industry, there is also a concern that other areas of critical infrastructure including gas and water systems can be compromised as they too leverage advancements such as smart meters and advanced metering infrastructure (AMI). According to Thompson, there are also other emerging areas that smart grid and AMI are moving into, including electric vehicles. "The more proliferation there is of intelligent metering and energy usage, the more opportunities there are for attackers," he said.

In addition to compromise from externally-launched malware, a major concern for the utilities industry is the insider threat, whereby employees utilize cyber tactics to defraud utilities or perhaps, disgruntled, cause power outages. Another interesting concern is the new intersection between utilities networks and home area networks as a result of smart metering, as criminals could leverage the utilities network to break into home networks or vice versa.

To combat these various attack vectors, utilities must focus on end-to-end security from plant generation to the point of consumption, says Thompson. Basic internal security governance around the use of these systems is also critical. The ability to assess the maturity of existing assets will be a key focus area for the future. According to Thompson and Chasko, having mechanisms to assess the security maturity of already-deployed technologies is the next area of uncharted waters for utilities and vendors.

<sup>8</sup> Source: <http://www.secureworks.com/research/newsletter/2010/01/>

Batz added that as control systems are used in more and more areas of industry as a means of automating various processes, including in manufacturing and in national defense and electric systems, they introduce greater complexity and security risk, making the outcome of attacks very difficult to predict. He cautioned that in the future, as technologists are designing various systems from cars to computers, it will be important to carefully weigh the benefits of powerful, complex capabilities – such as Bluetooth in vehicles – against the new risks that they introduce. He added that in instances where prevention is not possible, the technology industry also has to consider the resiliency of systems and make sure that if systems are compromised, they can be easily restored.

GTISC researcher David Dagon says similar attacks that target physical systems are also possible in the healthcare industry. "Hospitals and other medical facilities operate under a very different regulatory framework than in other industries," said Dagon. "If an infected device is used in patient care, it may not be possible to patch it the same way as other systems because the FDA may have specific guidelines for making changes to devices that interact with patients."

Because of the regulatory risks and potential litigation involved in modifying computer systems that interact with medical devices, some facilities may choose not to patch known infected systems, which those of us in the security field know can cause a whole new set of issues, says Dagon.

Ramsey of SecureWorks said he has also seen the compromise of medical systems as a result of cyber attacks. He pointed to a hospital in which one of the radiology systems used to share images between doctors was compromised due to a cyber issue, having a direct impact on the standard of patient care. According to SecureWorks, attempted hacker attacks launched against their healthcare clients nearly doubled during the last quarter of 2009. Attempted attacks rose from an average of 6,587 per healthcare client, per day during the first nine months of 2009 to an average of 13,379 attacks per client, per day in the last three months of 2009.<sup>8</sup>

Another interesting security issue that GTISC has uncovered in the healthcare industry is the widespread use of USB devices. "We have seen systems in hospitals that were patched, but then quickly re-infected through the insertion of USBs containing malware," said Dagon. Other organizations like the U.S. military have banned the use of USBs for this reason, so this is an area where GTISC plans to conduct further research. Dagon compared the situation to the cleaning of an operating room within a hospital. "Why would you clean the entire operating room, but not disinfect the scalpels?" he questioned. "It is similar to cleansing computers but letting viruses live on USBs."

In addition to affecting medical devices, cyber issues within hospitals can compromise confidential patient information. Dagon believes it is not long before cyber criminals begin to monetize this information as they have other types of personal data like financial and log-in credentials, making the threat to physical systems as a result of cyber issues a true concern.

# [ Privacy & Responsibility ]

Another topic brought up almost unanimously throughout these security discussions was privacy. As the use of mobile phones and social networking, as well as resulting attacks proliferate, users' personal information is subjected to more and more risk. Adding to that risk is the increasing connection between the cyber and physical worlds.

According to Lee of Georgia Tech, as the college-age users of Facebook and Twitter grow older, they will still want the social networking capabilities they are used to, but will also be more concerned about privacy. Lee says there are companies out there developing and testing both secure social networking sites and privacy technologies to run on top of existing sites. For now, according to Traynor of Georgia Tech, users should pay close attention to the kinds of information the applications they use are sharing about them with others.

When speaking of physical systems, it is easy to recognize privacy concerns within the healthcare industry as malware captures patient information and sends it out across the Internet, or as busy doctors carry vital data around on USB drives. However, according to Chasko of Landis+Gyr, it is important to note that privacy concerns also come into play with the compromise of utilities networks. He pointed to a recent set of smart grid cyber security guidelines published by the National Institute of Standards and Technology (NIST), saying that it includes an evaluation of privacy issues at residences based on new smart grid technologies.

According to *IEEE Security & Privacy*, "Electricity use patterns could lead to disclosure of not only how much energy customers use but also when they're at home, at work, or traveling. When at home, it might even be possible to deduce information about specific activities (for example, sleeping versus watching television)."<sup>9</sup>

So who is responsible for all of this? Who is responsible for protecting users' privacy and for halting the compromise of computers, mobile phones and other devices? Who is responsible for stopping the spread of malware and preventing the damage it could cause to our nation's critical infrastructure?

Throughout this report, it has become clear that the cyber security problem cannot be solved by a single group of people. Users,

*"Our adversaries are very skilled in sharing information with each other. In order to keep up, those of us working to defend against the threats must learn how to structurally improve our communications to efficiently share information and make further progress in security."*

— **David Batz**, Manager, Cyber & Infrastructure Security,  
Edison Electric Institute

government, technology vendors and security researchers all have a role to play in this fight, but each group alone can only go so far. According to Smith of M.A.D. Partners, "We can't make the users responsible. Within an enterprise, the CSO has to be aware of what the real threats are and be dictating policies for the employees."

However, Ollmann of Damballa adds, "Users have to be extra vigilant. Because so much of the initial infection today is driven by carefully crafted social engineering, botnet operators are successful even against computers that have practically every protection technology known to man. That said, those layers of defense should not be neglected – at the very least they limit the scope of attack."

From the perspective of Ahamad at GTISC, the solution is not just technology-based or policy-based, but requires a more holistic approach to obtaining a deep understanding of the threats through the collaboration of users, government, academia and industry.

Ramsey of SecureWorks agrees. "The name of the game today is knowing what you don't know," he said. "Staying plugged into external environments and the overall 'threatscape' is key for being prepared for when attacks really do emerge. Today, security has gotten so complex that there is no way a single person can even know everything about one aspect of cyber defense. It is therefore critical for leaders in the security industry to share information with one another."

Batz of the Edison Electric Institute also stressed that government and industry collaboration is key when it comes to protecting physical systems from cyber attack. "When you consider how much of our critical infrastructure is owned and operated by the private sector, it becomes clear that there is a need for greater public/private partnership when it comes to mitigating risk," he said. "Moving forward, government organizations that possess classified information about potential threats will need to regularly share this actionable intelligence with the private sector in a more timely and structured manner to effectively defend our nation against attacks."

To summarize, Rouland of Endgame Systems added, "The threat is now so big that the old style of developing a separate remedy for every threat simply does not scale, so a community-based defense approach is key."

The threats discussed in this report can affect any corporation, organization or individual. It is therefore up to all of us to educate ourselves on the various cyber security risks and do our part to stop enabling and spreading malicious cyber activity.

<sup>9</sup> Source: Khurana, Himanshu, Mark Hadley, Ning Lu and Deborah A. Frincke. "Smart-Grid Security Issues." *IEEE Security & Privacy*, January/February 2010: 81-85.

## [ GTISC Emerging Cyber Threats Report Contributors ]

**Dr. Mustaque Ahamad**

Director of the Georgia Tech Information Security Center (GTISC)

**David Batz**

Manager, Cyber & Infrastructure Security, Edison Electric Institute

**Stephen Chasko**

Principal Security Architect, Landis+Gyr

**David Dagon**

GTISC Researcher

**Dr. Paul Judge**

Chief Research Officer, Barracuda Networks

**Dr. Wenke Lee**

Co-Director, Georgia Tech Information Security Center (GTISC)

**Gunter Ollmann**

Vice President of Research, Damballa

**Jon Ramsey**

Chief Technology Officer, SecureWorks

**Chris Rouland**

CEO & Co-Founder, Endgame Systems

**Paul Royal**

Research Scientist, GTISC

**Robert Smith**

CTO & Co-Founder, M.A.D. Partners, LLC

**Heath Thompson**

Chief Technology Officer, Landis+Gyr

**Dr. Patrick Traynor**

Assistant Professor, Georgia Tech School of Computer Science





[www.gtiscsecuritysummit.com](http://www.gtiscsecuritysummit.com)



266 Ferst Drive, Atlanta, GA 30332-0765

**P** 404.385.4272 **F** 404.894.1155 **E** [gtisc-info@cc.gatech.edu](mailto:gtisc-info@cc.gatech.edu)

[www.gtisc.gatech.edu](http://www.gtisc.gatech.edu)