CYBER THREATS AND SECURITY

PROTECTING THE INFORMATION FORTRESS

by Blair Watson

In April 2009, the *Wall Street Journal (WSJ)* reported that computer hackers – thought to be Chinese or Russian – had breached a key computer network of U.K. defence giant BAE Systems in 2007 and 2008 and stolen "several terabytes of data" related to the United States' F-35 Lightning II Joint Strike Fighter (JSF). BAE has been a major industrial partner on the $382-billion aerospace program during the past eight years. Not surprisingly, U.S. officials downplayed the story.

On March 11, 2012, *The Sunday Times*, a British newspaper, reported: "Details of the [cyber] attack on BAE have been a closely guarded secret within Britain's intelligence community since it was first uncovered nearly three years ago. But they were disclosed by a senior BAE executive during a private dinner in London for cyber security experts late last year." According to the report, the executive confirmed that the Chinese had electronically penetrated BAE's network and stolen plans for the F-35's stealthy design, electronics, and other systems.

In late 2010, China unveiled its Chengdu J-20 stealth fighter-attack jet. Photographs reveal JSF-like housings for electro-optical sensors and all-moving tail-fins. With the *WSJ* report and photographic evidence, military aviation experts think the J-20 is probably equipped with Chinese versions of the American fighter jet's electro-optical distributed aperture system, digital fly-by-wire interface, sophisticated AESA radar, colour liquid crystal cockpit monitors and holographic head-up display, and other 21st-century war-fighting innovations.

CYBER ATTACKS AGAINST DIVERSE ORGANIZATIONS

Hardly a week goes by without a news report of a prominent organization being cyber-assaulted. "Hackers attack Vatican website 2nd time in days" was the *FOX News* headline in mid-March. Authorities believe the notorious Internet hacker group *Anonymous* was behind the onslaught. Four weeks earlier, *Information Week (IW)* reported that Anonymous had taken down a U.S. Central Intelligence Agency website via a distributed denial of service (DDoS) blitz. "Anonymous and other hacktivists also left their marks on the U.S. Census Bureau, Interpol, and Mexico, as well as law enforcement websites in Alabama and Texas," wrote *IW* in February.

The following month, the U.S. Office of the Inspector General released a report confirming that Chinese hackers had gained control over NASA's Jet Propulsion Laboratory in November, which gave them the ability to delete sensitive files, add user accounts to mission-critical systems, upload hacking tools, and more.

Paul Martin, NASA's inspector general, told U.S. lawmakers: "The attackers had full functional control over these [computer] networks." His report said that in 2010 and 2011, "NASA reported 5,408 computer security incidents that resulted in the installation of malicious software on or unauthorized access to its systems. These incidents spanned a wide continuum from individuals testing their skill to break into NASA systems, to well-organized criminal enterprises hacking for profit." Some of the incidents "may have been sponsored by foreign intelligence services seeking to further their countries' objectives."

The Chengdu J-20 on a test flight

As a result of the computer breach reported in the *Wall Street Journal*, and photographic evidence, military aviation experts think the J-20 is probably equipped with Chinese versions of the American fighter jets' electro-optical distributed aperture system, sophisticated AESA radar, digital fly-by-wire interface, colour liquid crystal cockpit monitors and holographic head-up displays, and other 5th Generation war-fighting innovations.

F-35 Lightning II.

PHOTO: BAE SYSTEMS

Using the code name OpPiggyBank, a hacking collective called *CabinCr3w* attacked the Los Angeles Police Department website in February and obtained email addresses, passwords, names, and physical addresses of more than 1,000 officers. They also copied 15,000 police warrants; hundreds of thousands of court summons; more than 40,000 Social Security numbers; and thousands of police reports.

THREAT SOURCES

According to the U.S. Department of Homeland Security (DHS), there are five main sources of threats to computer networks or other types of linked electronic control systems: governments, terrorists, industrial spies and organized crime groups, hacktivists, and hackers.

Governments: Various state players have developed cyber resources that pose a significant threat to systems and programs deemed important to national security and economic stability. For example, in 2010 a new computer "worm" dubbed Stuxnet infiltrated Iranian computer networks and accessed control systems of the country's nuclear program. Reportedly, about 1,000 centrifuges used to enrich uranium were secretly ordered to spin so fast that they destroyed themselves, setting the program back by months.

The Stuxnet malware (malicious software) also fed erroneous indications to technicians in the control facility, making it appear that the centrifuges were running normally. The U.S. and Israeli governments are widely believed to have been behind the operation. In a September 2010 statement, computer security firm Kaspersky Labs described the worm as a "fearsome prototype of a cyber-weapon that will lead to the creation of a new arms race in the world." The company is convinced that the malware could only have been created with "nation-state support."

Terrorists: In early March, FBI Director Robert Mueller warned a House appropriations subcommittee that violent extremists may try to carry out cyber attacks on the U.S., and advised government to be prepared. "To date, terrorists have not used the Internet to launch a full-scale cyber attack, but we cannot underestimate their intent," he warned. "They may seek to train their own recruits or hire outsiders, with an eye toward pursuing cyber attacks. As our nation's national security and criminal adversaries constantly adapt and evolve, so must the FBI be able to respond with new or revised strategies and operations to counter these threats."

Industrial Spies and Organized Crime Groups: These individuals and collectives pose a medium-level threat because of their ability to conduct industrial espionage as well as large-scale monetary theft. They typically have the resources to hire or develop hacking expertise. Their motivation is money and their methods include attacks on infrastructure for profit, stealing trade secrets, and acquiring potentially embarrassing information that can be used to blackmail key officials.

Hacktivists: Nuisance hackers, like those in Anonymous, target organizations in furtherance of a political agenda. Their isolated-yet-damaging assaults, pose a medium-level threat to organizations, says the DHS. Most hacktivist groups have focused on carrying out irritating attacks rather than damaging important infrastruc-

What types of organizations are targeted the most?

Robert Freeman, manager of IBM's X-Force Research

"Although government organizations have always worried about the threat of state sponsored computer intruders, it is apparent that both large and small private enterprises also face this type of threat. A number of prominent publicly reported breaches in 2010 and early 2011 appear to drive this point home. Attackers are interested in the intellectual property of businesses of all sizes, and are even interested in businesses that may not have interesting intellectual property but are key business partners with those that do. In the latter case, they are looking for ways to gain access to data by pivoting in. Attackers may also target small, seemingly irrelevant businesses that can act as storage and proxy for their attacks. Organizations of all sizes should be concerned. Usually the more elaborate enterprise attacks are part of what the industry commonly refers to as 'Advanced Persistent Threat' or APT. These attacks rarely use high tech exploits and malware these days. The complexity is in the operation and management of the attack towards stealing data and keeping a foothold in a given organization. Only once discovered does the complexity tend to increase. There are many steps to a successful attack that pivots and steals data. If an organization can detect and stop any of the events during the attack, it wins."

Do organizations have adequate resources to deal with cyber threats?

Kurt Baumgartner, senior security researcher at Kaspersky Labs

"Unfortunately, it's uncommon to see all of an organization's resources fully secured. Potentially less than 50% of them have adequate planning, implementations, and maintenance in regards to securing important resources. There are diverse infectors, some of which are omnipresent in cyberspace (e.g., Sality, Virut, Xpaj, Qbot). Usually there are established procedures to deal with them. Mass exploitation and cyber criminals spreading Zbot, FakeAV, TDSS, SpyEye and other spyware is a problem for every organization, whether the adversary is after financial data or other private resources. The APT (Advanced Persistent Threat) is a different story, however. Depending on the group, they don't go away for years, and innovate to get in. It's rare to see organizations adequately protected with technology, and human error will continue to be a critical weak point."

ture. Achieving notoriety for their cause is part of their motivation.

Hackers: The large majority of hackers do not have the requisite knowledge or experience to threaten difficult targets such as critical computer networks or systems directed by programmable logic controllers (nuclear enrichment centrifuges for example). However, the electronic penetration of BAE Systems, NASA, and other high-tech and sensitive organizations (including government departments, banks and law firms) proves that some hackers are very good at their craft.

EMERGING THREATS

According to cyber security experts, threats are constantly evolving. Georgia Tech's *Emerging Cyber Threats Report 2012* warns about the *Mobile Threat Vector* and *Botnets*. The latter is a collection of compromised computers, each known as a 'bot', which are set up to forward transmissions such as spam or viruses via the Internet. Often, when a computer is penetrated by a hacker, code within the introduced malware commands the device to become part of a botnet. The "botmaster" or "bot-herder" controls compromised computers via standards-based network protocols such as IRC and http. The following are highlights of Georgia Tech's report:

MOBILE THREAT VECTOR

- Mobile applications, such as those on smartphones, increasingly rely on a browser, presenting unique challenges to security in terms of usability and scale.
- Expect compound threats targeting mobile devices that use SMS, e-mail and the mobile Web browsers, then silently recording and stealing data.
- USB flash drives have long been recognized for their ability to spread malware, but mobile phones are becoming a new vector that could introduce attacks on otherwise-protected systems.

The good news is: encapsulation and encryption of sensitive portions on a mobile device can strengthen security.

BOTNETS

- Botnet controllers build massive information profiles on their compromised users and sell the data to the highest bidder.
- Adversaries query botnet operators in search of already compromised machines belonging to their attack targets.
- Criminals will borrow techniques from Black Hat SEO (search engine optimization) to deceive current botnet defences like dynamic reputation systems that compute "reputation" scores of domain names.

WHAT CAN BE DONE?

Robert Freeman of IBM recommends the following steps to better secure a network:

- Perform regular third party external and internal security audits.
- Control your endpoints.
- Segment sensitive systems and information.
- Protect your network.
- Audit your web applications.
- Train end users about phishing and spear phishing.
- Search for bad passwords.
- Integrate security into every project plan.
- Examine business partners' policies.
- Have a solid incident response plan.

Keep malicious activity out of an enterprise network by keeping up with vulnerability patches and detecting attacks at the perimeter can be a significant challenge," says Robert Freeman, a manager at IBM's X-Force Research, "and the threat landscape appears to be getting only more complicated." S

Blair Watson is a contributing editor at ***FrontLine*** *Magazine.*

Is cyber security in government organizations better than in the private sector?

Gerry Egan, Symantec's Director of Product Management

"They're very similar. The quality of personnel is the same as you'd find in the private sector, and cyber security as a priority is just as high. IT [information technology] organizations in the public sector are just as constrained by resources and trained security personnel as what you would find in the private sector. The shortage of trained cyber security personnel is a national issue that spans across all industries – public and private – and can only be solved with a renewed emphasis on science and mathematics at the middle and high school levels, followed by more courses, professors and research funding at the collegiate level."