BLUE COAT

Security Empowers Business

BLUE COAT LABS REPORT: ADVANCED PERSISTENT THREATS

WHITEPAPER

Advanced Persistent Threats (APTs) are well-researched and highly coordinated attacks designed to circumvent technical, procedural and user training defense mechanisms. Unlike mass-market malware attacks, APTs are not crimes of opportunity. They are targeted, specialized attacks against specific organizations or groups, and typically blend a broad range of common malware, phishing, hacking, spying and other tools together in a well-orchestrated operation.

Executive Summary

While these threats may involve an insider or other physical security vulnerability that goes beyond the jurisdiction of IT, this document focuses primarily on issues within IT.

APTs are not a new kind of threat. They date as far back as the 1990's, but increased activity over the last few years should put them at the top of the corporate security agenda. While APTs have historically targeted government agencies,1 contractors2 and suppliers,3 they have rapidly entered the private sector as demonstrated by attacks at ExxonMobil, British Petroleum,4 RSA,5 Heartland Payment Systems, TJX,6 Sony,7 Google and others.8 And, because an APT is not a single incident, organizations may need a more comprehensive way to coordinate alerts and intelligence to thwart attacks in progress. All too often, by the time an organization suspects an APT attack, the damage is done.

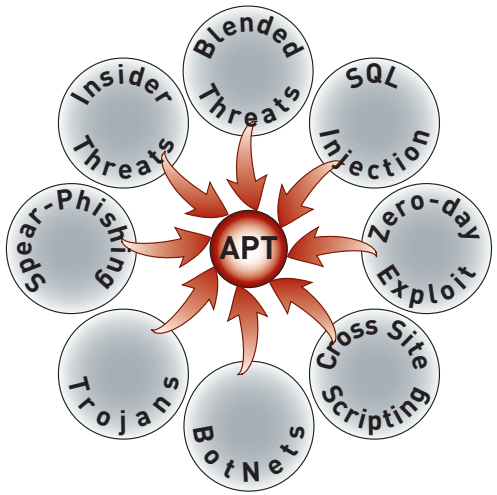
A successful APT security strategy requires executive sponsorship and support. However, a 2011 report by the Ponemon Institute indicated that only 16% of surveyed IT organizations believed that senior management had a sufficient grasp of this threat.9 The good news is, most organizations already have the tools necessary to defend against APTs. What's needed is a strategy to identify security gaps and more effectively use the solutions already in place.

This document will provide a working definition of APTs and their attack lifecycle. Some high-level strategies and best practices will address a broad range of technical and non-technical aspects of an APT attack. Finally, a review of common layered defense strategies will outline the capabilities of various security solutions to defend against a comprehensive APT.

Understanding the Enemy

APTs are commonly misunderstood to be a new kind of malware, vulnerability or other technology. But APTs go far beyond a programming style, exploit technique or threat hiding mechanism. Instead of a single threat or incident, it's better to think of an Advanced Persistent Threat as "Advanced Persistent Attackers."

An APT is actually an extended campaign targeted at a specific organization (or group of organizations) to achieve a clear objective. APTs can use a range of tools, from common malware to complex, zero-day threat tactics to achieve their goals. But the reason we call an Advanced Persistent Threat advanced is because it is very well planned, executed and coordinated with every available tool. It is persistent because the perpetrators are patient and focused on avoiding detection. If a targeted organization uncovers an APT, the entire APT malware network can suffer a serious setback by losing months of research and planning. By contrast, mass-market attacks go for volume, so detection by a single individual rarely weakens the effectiveness of the attack.



BLUE COAT

Security Empowers Business

Mass-market Malware vs. APTs

There are a few key differences between an APT and mass-market malware:

An APT does not necessarily need unique malware, zero-day or exploit code to be successful. However, APT architects are more likely to be early adopters of new zero-day exploits, or use less popular tools in their attack as long as it exploits a key weakness in the target organization.

Mass-market attacks often involve blended threats that use multiple tools, such as an email with a link, which leads to a web site that performs a drive-by malware infection. But an APT treats even a blended threat as just one aspect of a more complex, multi-stage attack.

The following table illustrates some of the other similarities and differences between an APT and the typical mass-market malware attack we are more familiar with.

THREAT CHARACTERISTIC	MASS-MARKET ATTACK	APT ATTACK
Financial Backing	Well-funded	Well-funded; may have political resources
Targeted	Largest possible audience	Specific organization(s)
Use Zero-Day Exploits	Uncommon	Common
Objective	Almost exclusively financial	Financial, interrupt operations, acquire sensitive data to gain some advantage
Opportunistic	Typically	No. Clearly defined objective
Patient Execution	Rarely	Definitely
Social Engineering	Yes	Yes, but highly specific and targeted
Tweak/Customize Common Malware	Yes	Yes
Attack Tool Coordination	Minimal beyond traditional blended threats	Extensive; tools applied may vary based on findings at each step of operation
Data collection Method	Typically smash-n-grab	Methodical & unobtrusive
Research	Minimal; about payload and delivery mechanism	Extensive; Includes applications, policies best practices, employee interests, etc.
Spread Infections to Other Systems	Often attacks any susceptible system	Yes, but more strategic, possibly following a planned path, leveraging different tools on different systems

A Sharper Spear

Spear phishing also illustrates how mass-market malware attacks go for volume, unlike APTs, which are more personalized and targeted attacks. Famous mass-market spear phishing attempts include fake Bank of America or PayPal emails that trick users into following a link to a fake web site where they are guided to enter their login credentials or reveal personal information. In the mass-market attack, even people who do not bank with Bank of America, or do not have a PayPal account, may receive such emails. But an APT attack is much more precise. For instance, if an APT targets your organization's technical support personnel, only those in your technical support department will receive the message.

A Clear Objective

As part of an APT, a set of tools is identified, collected, customized and executed in a coordinated manner with a very specific objective in mind. The goal could be to collect specific pieces of sensitive research, large volumes of personally identifiable information, financial records, trade secrets, or other sensitive information. This is the case with the majority of APT attacks to date.

But APTs can also be used to sabotage or otherwise disrupt critical systems or infrastructures. For instance, some experts believe the 2010 Stuxnet incident was intended to disrupt Iran's nascent nuclear program.10 An APT disruption would differ from a more typical denial-of-service (DoS) attack because of the systems involved. For example, the Programmable Logic Controllers (PLC) involved in the Stuxnet attack could not be accessed directly from the outside. An attacker had to find entry to the network and penetrate deeper until they could locate a susceptible PLC. And, to achieve the intended results, the penetration activity might continue for some time until a sufficient number of PLCs had been compromised.

Zero-day Vulnerabilities and Exploits

Despite all the media and corporate attention to security lapses and the need for frequent patching, vulnerabilities tend to remain long after a security fix becomes available. So both mass-market malware criminals as well as APT attackers often leverage available exploit code. However, a high level of customization is required to use such exploits without raising any red flags in the early stages of the attack. So those behind

BLUE COAT

Security Empowers Business

APTs, given their very specific target and clear objectives, are more likely to invest in extensive zero-day exploit customization if their research shows how it might get them closer to their objective.

It's important to note that APT attackers do not care about the latest vulnerability or how to exploit popular applications. They focus exclusively on the target and the objective. If a target organization is using a semi-obscure system with known vulnerabilities, and the attackers feel the investment in creating an exploit will render sufficient results, they will use it. They are funded, and motivated, purely by results.

The Insider Threat

APTs are much more likely than a mass-market malware attack to involve a physical intrusion component, such as willing insiders or insiders who are tricked into revealing sensitive data. Attackers may also use traditional phishing and other social engineering techniques, or impersonate a company employee on the phone to fool real employees into divulging important information. They may also pretend to deliver flowers or other gifts to gain access to someone's work area (especially an employee they know is out of the office from their phone call research). Or they might drop USB drives in the company parking lot hoping that a curious employee might plug the malware-infected device into their work computer.

The APT Lifecycle

While every APT is tailored for the target and objective of the attack, there are some common stages to the preparation and execution of an APT attack. After extensive research and successful entry and penetration of key systems, much of the life of a typical APT will be in harvesting the desired information. However, as indicated in the following diagram, the rigorous monitoring of the attack, even during the harvesting stage, may indicate the need to infect additional systems or follow new penetration paths to compromise new resources. Like a good spy, they begin with a plan but are ready to improvise based on security responses and opportunities uncovered. The objective drives all activity throughout the entire lifecycle and it is never left entirely on automatic.

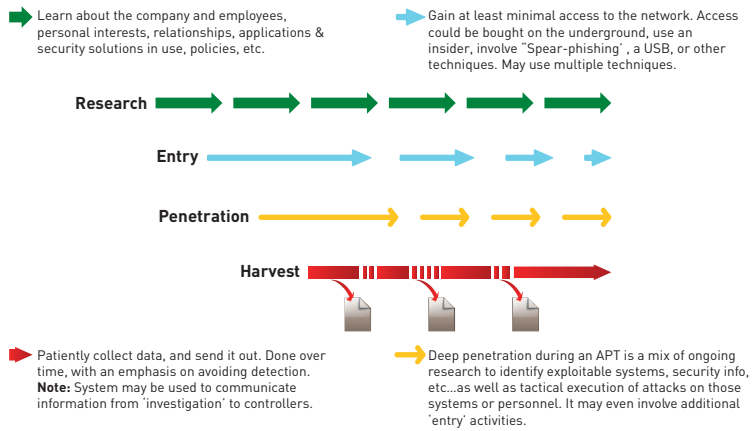


Figure 3: The APT Attack Lifecycle: Once it starts, it doesn't end until it is detected and eradicated.

RESEARCH PHASE

One of the greatest differences between an APT and a traditional mass-market malware attack is the depth and breadth of research both before and during the attack. The well-funded organizations behind an APT will spend a great deal of time researching their very specific targets. They may leverage company events, send their own emails about registering for new benefits (on fake web sites), physically enter through a back door used by the organization's smokers and so forth. They will try to understand the network architecture, legacy systems, potential for rogue systems, applications and version numbers, and anything else they might be able to use. They may also research specific details about the corporate culture or target individual(s) in an effort to gain access through fake messages about company events, or by impersonating the target with highly detailed emails or phone calls to trick users into revealing key information.

Today, much of the information might be uncovered through some creative Google searches on Facebook pages, tweets, etc. Easily available penetration testing tools can help them discover much about an organization's network and systems. Phone calls pretending to be from remote company employees asking one or two innocuous questions, spread out over time and across several departments, may provide critical details without revealing the attack underway.

With this preliminary research, the APT attackers typically begin some advanced planning for each of the other stages of the attack. Working back from the objective, they identify systems and people who are closest to their objective, and build a map to identify multiple paths that might lead them to success. They might explore social engineering options and research available tools to help them gain entry and methodically penetrate the network towards the objective. The research phase also involves the customization and development of the actual tools to be used in the attack.

An APT attack can employ common malware code, penetration testing modules and other tools as is or with minor modifications. Some tools are used to uncover exploitable weaknesses and others for specific aspects of the multi-staged attack. For example, the 2010 Stuxnet attacks noted earlier have been repurposed by others to attack companies in the utility and energy industries.11

The planning team will identify what they can do with their own resources and identify services they may need to buy or sub-contract out to those who sell their expertise in the underground cyber-economy.

ENTRY PHASE

In the entry phase of an APT, gaining a foothold on the network is perhaps the first demonstration of the attackers' persistence. They will try one thing after another until they have access. They may even try several methods simultaneously so that, if any of them are detected, they simply refocus on those attempts still in operation.

Experts believe that spear phishing is among the most common tools used during the entry stage of an attack. Typically, spear phishing involves an email with a malicious attachment such as a PDF containing an exploit. But neither the email nor the attachment is required. To bypass email antivirus defenses, the message may be transmitted via webmail, a social networking account, instant messaging, and so on. And rather than an attachment, a simple link to a malware file stored on a public file share service may accomplish the same task.

It should be no surprise that social networking has also become a very popular vehicle for introducing malware in mass-market attacks as well as APTs. The environment of trust within the social networking environment often reduces the victim's awareness of the danger of certain activities.

These and other methods are employed in an attempt to get a foothold within the network, with at least a minimum level of remote access and control. Remote Access Tools (RATs) are an established, relatively common tool that the APT attackers will leverage for their own purposes. Once a RAT is in place, attackers can leverage the infected platform in further phases of the attack.

Regardless of the technical aspects of the attack, social engineering plays a key role. Information gained during the research phase is essential to tricking users into revealing key network access credentials (such as in a mass-market malware attack), but the tactic must also be finely crafted to avoid raising suspicions later. Even in the early stages, an APT attempts to avoid leaving traces that might uncover their higher-level objective. In hindsight, those who have discovered APTs in progress at their organizations were able to see how easily they wrote off early indicators as simply another malware attack or spam incident.

Perhaps the easiest way to gain network entry is to buy it online from someone who has already gained access as part of a mass-market attack. This is where the opportunistic mass-malware market connects with the APT attackers. In fact, hackers have been known to offer root access to U.S. government servers and other networks for US$49912 or even less.

PENETRATION PHASE

Success rarely happens in the early penetration phase, but the attackers can gain important information from the initially compromised systems.

First, they may discover the need for more research as the initially infected systems collect information about the network, traffic patterns, potential weaknesses, connected servers and more. Remote control of each compromised system can yield valuable information, such as the identity of the owners and their level of access.

Once the attackers have enough information from the initially compromised systems, they will patiently move through the network to find their target system or systems.

HARVEST PHASE

Attackers move closer to their objective during the harvest phase. "Harvest" is an apt description of this phase, because APTs do not simply grab information and leave. They gather what they can and wait

patiently for new and changing data to become available. This is how an APT differs dramatically from mass-market malware, which attempts to extract as much information as possible as fast as possible, often setting off security alerts in the process. An APT tends to stay for an extended period of time and is designed to remain undetected.

The APT Attack Strategy Requires an APT Defensive Strategy

Defending against these sophisticated attacks requires a well-planned defensive strategy. First you need to know how your organization functions, communicates, uses current security solutions, and how to fully utilize their capabilities. You also have to identify how attackers can use data that is stored or transferred on your network to meet their objectives.

Using Log Files to Connect the Dots

Since a typical APT attack applies common tools in a coordinated fashion over time, it's almost impossible to identify a single incident, such as a blocked spear phishing attempt, as a symptom of a larger APT attack. But by correlating information from various systems, typically using log files, you can connect the dots and see the relationship between seemingly unrelated incidents.

Traces of APT activity may be found at the web gateway in log files from a proxy, gateway antivirus, firewall, web filter, DNS, IPS/IDS and other solutions. Once you establish a baseline of typical activity, your team should develop sensitivity to anomalies so you know when to check the logs of other systems for similar APT warning signs. Reporting tools that correlate multiple systems make it easier to establish a baseline and design reports that highlight anomalous activity.

For example, the Conficker botnet, which was an enormous problem in 2009 and 2010, was discovered when someone noticed anomalous activity in their DNS logs because Conficker asked DNS for IP addresses for thousands of non-existent URLs every day.

While many other items discussed in this document may provide some level of defense against various aspects of an APT attack, nothing may be more effective in helping you identify an APT than learning to leverage your log files.

AV, Web Filters and Patching...Oh my!

Since most APTs leverage common attack methods and tools, your defense begins with the proper application of standard defenses. Of course, it helps if you are using them correctly, and if they are frequently updated. Better yet, include a cloud service so you don't need downloads, patches or updates.

Gateway antivirus for HTTP, HTTPS and FTP traffic has been part of a multi-vendor strategy since 2000, and is employed by most high-profile, target organizations. However, many companies today still depend solely on the endpoint for antivirus other than email. Given the proliferation of webmail, social networking and other vulnerable web applications, this is a grave oversight. Having two or more vendors with different approaches to behavioral analysis and heuristics will increase your chance of proactively detecting malware variants, such as those used in APTs.

The web filtering industry shifted from a primarily porn-blocking approach to a frontline gateway malware defense about 7-8 years ago. Plus, some quality web filters today include a separate category to identify outbound transmissions that could indicate compromised systems as early as the entry phase – before an APT can effectively penetrate the network.

Exploits that take advantage of vulnerabilities have become very common in the last few years, and have shifted from operating systems to popular applications. APTs are especially adept at exploiting vulnerabilities, so closing these gaps must be a top priority for IT. Granted, it may be impossible to keep all systems patched all the time. But the fewer holes you have, the more time you have to uncover and stop an APT in progress.

Insider Threat

By far, the most dangerous insider is the employee who innocently provides attackers with the means to attack the organization. While Post-it® notes with passwords are rarely left on monitors today, users continue to make egregious security mistakes out of ignorance. Far too many users are unaware of the security risks their careless login and social networking habits can pose to corporate data, and both APTs and mass-market malware attacks routinely exploit this oversight. That's why even minimal but regular end-user security training can significantly reduce social network security breaches.

BLUE COAT

Security Empowers Business

Security training can also be coordinated between groups who may have a shared interest. For example, legal and HR departments are typically responsible for privacy polices, such as defining what kind of information can be given out on the phone. So you can often apply the same training program to both of these groups.

Beyond educating users, IT should also consider repealing certain privileges. For example, IT can prevent a RAT from using webmail to transmit data files by blocking attachments. Similar controls can be put in place for Facebook and other collaboration services, other than those approved by the organization. Combined with even a basic, core DLP implementation, you can dramatically reduce the available avenues for an APT to enter and harvest information.

On the network side, IT should identify the information and resources an APT might target. It's also important to identify which users have access to those resources, and whether or not they need that access. In many data loss cases, an innocent user made a mistake with information they should never have possessed in the first place. As a result, tighter implementation of access and authentication controls, at least on suspected primary APT targets, could provide a strong proactive defensive measure.

A Layered Defense

Blue Coat advocates a layered defense strategy to address threats at every stage of their lifecycle for a fault-tolerant security posture. With a working definition of APTs, it is possible to evaluate existing solutions for their ability to defend against the various tools attackers might use during each stage. While many security vendors may position their offering as a solution against APTs, the intelligent buyer will ask more pointed questions to understand exactly how the solution addresses the different kinds of APT tools described in this white paper.

Here we will review some of Blue Coat's solutions in general, and highlight the role they play in a layered APT defense:

ProxySG

Blue Coat ProxySG provides a scalable proxy platform to secure web communications. In addition to other capabilities, it can monitor web traffic for anomalous activity such as non-SSL traffic using port 443, non-HTTP traffic on port 80, file transfers at unusual times or from suspicious users or systems, and much more. ProxySG can also enforce security policies defined by using an extensive amount of traffic information, all of which is logged to assist investigations into possible APT attacks in progress.

WebFilter

Combined with ProxySG, Blue Coat WebFilter blocks real-time malware downloads and other web threat activity, filters URLs and IP addresses, protects user productivity and enables compliance. WebFilter has proven to be an excellent zero-day and exploit defense because its cloud component, WebPulse, provides real-time analysis of new or previously unrated URLs. And, because WebFilter supports IPv6, it can prevent attacks that exploit weaknesses in non-IPv6-compatible security solutions.

From the Entry stage (when APTs may try to lure users to malware or phishing sites) to the Penetration stage (when botnets, RATs and other tools communicate with their creators for instructions), WebFilter can dynamically rate web destinations for potential threats, block those incidents and log activity details for use in APT investigations. WebFilter can also identify and block attempts to transmit stolen information during the Harvest stage by correlating information from both ProxySG and WebFilter.

To protect mobile users, WebFilter also includes ProxyClient to secure and log web activity on remote or mobile systems.

WebPulse

WebPulse is a cloud service component included with WebFilter, PacketShaper and the Blue Coat Cloud Service – Web Security Module. WebPulse applies behavior analysis, active script analyzers, heuristics and much more to dynamically rate URLs. Customers using solutions incorporating WebPulse are instantly protected as new identification and analysis processes are put in place. And, with over 75 million users in the WebPulse community, every user is instantly protected when another user encounters malicious content.

ProxyAV

To help protect against threats from webmail, social networking or other non-SMTP entry vectors, ProxyAV offers a best-practice, multi-vendor compliment to endpoint antivirus solutions. Customers choose from

five leading antivirus solutions to increase their ability to detect viruses, including malware variants, often used in APTs during the Entry and Penetration stages. ProxyAV logs are also stored with ProxySG and WebFilter data for improved correlation value.

Reporter

Reporter leverages available logs from ProxySG, ProxyAV, WebFilter and ProxyClient to provide complete visibility into web activity. The intuitive interface makes it easy to drill down into data, build ad-hoc reports and identify abusive behavior by employees. And, by viewing antivirus activity, unusual port or encryption activity, webmail use, and suspicious URLs or IP addresses accessed by a specific user or system, you can identify and respond to a potential APT attack in the early stages.

Cloud Service - Web Security Module

The Blue Coat Cloud Service – Web Security Module provides complete web protection without the need to maintain or update appliances, servers or desktops. It delivers much of the same protection and logging features as ProxySG, ProxyAV, and WebFilter, but on a platform better suited for mobile workers and branch offices. The administration and reporting capabilities are comparatively powerful as well, providing another opportunity to correlate activity to uncover an APT in action.

The Web Security Module, while available separately, may be deployed in parallel with other Blue Coat appliances to offer large offices security and performance benefits without the need to commit to a single appliance platform.

Blue Coat DLP

Blue Coat DLP enables organizations to detect and block potential data leaks quickly and accurately. In addition to email monitoring, Blue Coat DLP can also interrogate web traffic for sensitive data attempting to leave the network. It can also defend against APTs by monitoring network traffic to identify personnel or systems that may be accessing information in a suspicious way or at an unusual time. Central management capabilities can correlate information on network activity and at all exit points to help identify APT patterns and attempts to extract information from your company.

PacketShaper

PacketShaper can identify traffic related to over 700 common application types, provide port details and protocol information, and categorize outbound traffic based on its destination. As part of an APT defense strategy, PacketShaper provides invaluable visibility, as well as the ability to implement policy controls by automatically correlating a wide variety of information. For instance, the ability to correlate application traffic with other traffic, time and web information could help thwart an APT during the Penetration and Harvest stages of the attack.

PacketShaper can also monitor and respond to those parts of an APT that may use applications to spread malware, access information or perform other malicious activities on the LAN or WAN. PacketShaper's application monitoring features can detect unusual system activity, such as applications that work around the network, or consume excessive bandwidth or operate in a suspicious way (such as 100 infected computers attempting to access a company database that is typically used by only 4-5 people simultaneously).

Conclusion: Take the next step against APT attacks

With APTs on the rise, government and industry organizations everywhere need the right strategy and solutions to defend themselves. A thorough understanding of how APTs operate and how they can exploit social, physical and network vulnerabilities in your organization are the crucial first steps to addressing APT attacks.

All too often, organizations fail to recognize an APT in progress because they lack the ability to correlate seemingly isolated events. For instance, what appears to be typical email spam or a random phone call might actually be the initial stages of an APT. Learning how make the most of log files and reporting tools can improve your APT awareness. But strengthening your active APT defenses can be more complex. It may involve updated physical security policies and end-user awareness training in addition to the proper application of technology.

Because the web now dominates global communications, large IT organizations need a more comprehensive security approach. That's why, for the network, Blue Coat advocates a layered defense strategy that can defend against individual APT tools and coordinate multiple defensive layers to identify higher-level APT attacks. Layered

BLUE COAT

Security Empowers Business

security works by delivering comprehensive gateway and network-based defense, control and monitoring solutions, as well as real-time intelligence that doesn't require patches and updates. As a result, a successful APT security strategy mitigates malicious activity at each stage of the APT lifecycle, identifies and correlates the trail of suspicious footprints and enables IT to continuously improve security policies.

To learn how Blue Coat solutions can help protect your organization from APTs and other security and bandwidth threats, please visit www.bluecoat.com.

References

1. Wikipedia, http://en.wikipedia.org/wiki/GhostNet
2. ComputerWorld, Jun 5, 2011, "LulzSec claims it hacked FBI linked organization" http://www.computerworld.com/s/article/9217320/LulzSec_claims_it_hacked_FBI_linked_organization
3. IBTimes, May 28, 2011, "Lockheed Hunting Cyber Attackers" http://www.ibtimes.com/articles/154086/20110529/lockheed-rsa-attacks-emc-apt.htm
4. CNET, February 10, 2011, "Data theft attacks besiege oil industry, McAfee says" http://news.cnet.com/8301-30685_3-20031291-264.html?tag=mantle_skin;content
5. PCWorld, March 18, 2011' "RSA SecurID Hack Shows Danger of APTs" http://www.pcworld.com/businesscenter/article/222555/rsa_securid_hack_shows_danger_of_apts.html
6. Wired, August 17, 2009, "TJX Hacker Charged With Heartland, Hannaford Breaches" http://www.wired.com/threatlevel/2009/08/tjx-hacker-charged-with-heartland/
7. TechWorld, May 18, 2011, "Hacker sheds light on Sony PSN attack" http://features.techworld.com/security/3280561/hacker-sheds-light-on-sony-psn-attack/
8. Wikipedia, http://en.wikipedia.org/wiki/Operation_Aurora
9. Ponemon Institute Blog, April 3, 2011, "Are we taking adequate steps to protect the critical infrastructure?" http://www.ponemon.org/blog/post/are-we-taking-adequate-steps-to-protect-the-critical-infrastructure
10. Wired, September 28, 2010, "Blockbuster Worm Aimed for Infrastructure, But No Proof Iran Nukes Were Target" http://www.wired.com/threatlevel/2010/09/stuxnet/
11. V3.co.uk, April 7, 2011, "Two-thirds of energy firms at risk from Stuxnet-like Scada attack" http://www.v3.co.uk/v3-uk/news/2041556/-thirds-energy-firms-risk-stuxnet-scada-attack
12. Cyberinsecure.com, January 22, 2011, "Access To Hacked Government, Educational, Military Websites Sold On Underground Market" http://cyberinsecure.com/access-to-hacked-government-educational-military-websites-sold-on-underground-market/

BLUE COAT

Security Empowers Business

v.WP-BC-LAB-REPORT-APT-EN-v2ba-0513

Blue Coat Systems Inc.
www.bluecoat.com

Corporate Headquarters
Sunnyvale, CA
+1.408.220.2200

EMEA Headquarters
Hampshire, UK
+44.1252.554600

APAC Headquarters
Singapore
+65.6826.7000