Advanced Persistent Threats: A Decade in Review

Command Five Pty Ltd
June 2011

Abstract

This document defines the term Advanced Persistent Threat (APT) in the context of cyber threats and cyber attack. It presents a timeline and summary of prominent cyber attacks likely attributable to APTs over the past decade. Commonalities are identified and assessed in the context of the current cyber threat environment. Trends are used to predict future APT targeting. APT attack methodology is discussed, and, in conclusion, a set of security practices and policies are provided that could help many organisations increase their resilience to APT attack.

Definition

When the term Advanced Persistent Threat (APT) is used in the context of cyber threats (or cyber attack) each component of the term is relevant.

Advanced

The hacker has the ability to evade detection and the capability to gain and maintain access to well protected networks and sensitive information contained within them. The hacker is generally adaptive and well resourced.

Persistent

The persistent nature of the threat makes it difficult to prevent access to your computer network and, once the threat actor has successfully gained access to your network, very difficult to remove.

Threat

The hacker has not only the intent but also the capability to gain access to sensitive information stored electronically.

Advanced Persistent Threats

Advanced Persistent Threats (APTs) are a well-resourced, highly capable and relentless class of hacker increasingly referred to in the media, by IT security companies, victims, and law enforcement. Most hackers target indiscriminately and instead of persisting with a particular target draw their focus to more vulnerable targets. APTs on the other hand are not only well resourced and capable but persistent in their covert attempts to access sensitive information, such as intellectual property, negotiation strategies or political dynamite, from their chosen targets.

The sophistication of APT intrusion attempts varies and likely depends on the attacker's objectives, the tools and techniques available to them, and the anticipated ability of their target both to detect and defend against an attack. The activity conducted by APTs is not necessarily sophisticated but the attacker has the ability to upgrade their sophistication in order to gain or maintain access to computer systems of interest. The level of covertness employed may depend on factors such as the anticipated ability of the target to detect the

COPYRIGHT © COMMAND FIVE PTY LTD. ALL RIGHTS RESERVED.

activity, the anticipated response of the target should the targeting be detected, the level of risk the hacker is willing to accept, their timeframe to obtain the desired information and the effects on their longer term goals.

The term APT is commonly used in reference to the cyber threat posed by foreign intelligence services, or hackers working on behalf of such entities, but is not limited just to this and can equally be applied to other threat actors such as organised crime syndicates and those involved in traditional espionage. Even though some organised crime syndicates are very well resourced and capable, they are not usually classed as an APT since they are less likely to persist with attempted access to a particular target. The term is not usually used to refer to the threat posed by an individual hacker as they rarely have a sufficient level of resourcing.

APTs often target unpublicised vulnerabilities in computer programs or operating systems using 'zero day' exploits[1]. Typically only well-resourced hackers develop such exploits as they are expensive[2], time-consuming[3], and the vulnerabilities they target may be patched prior to deployment affecting the value of the investment. In addition, zero day exploits are exposed the first time they are used and, if detected, may be less effective in future attacks. As such, zero day exploits are usually only deployed when the hacker has determined that other exploits (that take advantage of publicly known vulnerabilities) will not work on the target, or are not expected to work within an acceptable timeframe. Increased use of a zero day exploit may also be observed if the hacker believes their exploit has been detected or the vulnerability it exposes has become known. This behaviour reflects a desire to maximise the return on their investment before the relevant vulnerability is patched. Zero day exploits are commonly used in combination with social engineering techniques, to exploit vulnerabilities in human nature and make the targeting more effective. Social engineering techniques are also often used to increase the effectiveness of exploits that target known, but unpatched, vulnerabilities.

Victim Reporting

Many of the organisations targeted by APTs are likely unaware they are among the victims. Those that are aware of attacks against them may not publicly disclose the fact due to concerns about their reputation or share price. Public reports of APT attacks date back to at least 1998, when the Pentagon, National Aeronautics and Space Administration (NASA), the United States (US) Energy Department, research laboratories and private universities were targeted. The past year (2010/2011) has seen an increase in the number of organisations coming forward, admitting they have been targeted. It has also seen an increase in US Securities and Exchange Commission filings warning shareholders about the risks of cyber attack.

The majority of companies that have come forward and admitted they are among the victims have not been forthcoming with the details. This is presumably because they do not want to provide the hackers with feedback, or cause further embarrassment to their organisation. It is unfortunate that such potential negative ramifications of detailed reporting are often seen to outweigh the community benefit of sharing lessons learned.

[1] A 'zero day' exploit is a computer attack capability that takes advantage of a software flaw before it is known to the public or patched by the vendor, that is, before the first day of public awareness of the flaw; on the zeroth day.

[2] On the black market zero day exploits can be worth hundreds of thousands or possibly even millions of dollars. (Moyanhan, 2011)

[3] Developing a zero day exploit can take up to several months even from the most expert hackers. (Borders, 2007)

COPYRIGHT © COMMAND FIVE PTY LTD. ALL RIGHTS RESERVED.

Timeline of Significant Attacks

Through examination of media reports and public announcements a timeline of significant cyber attacks likely attributable to APTs can be drawn as in Figure 1. In several cases a single operation is named to refer to a set of similar intrusions, or intrusion attempts, affecting numerous targets.

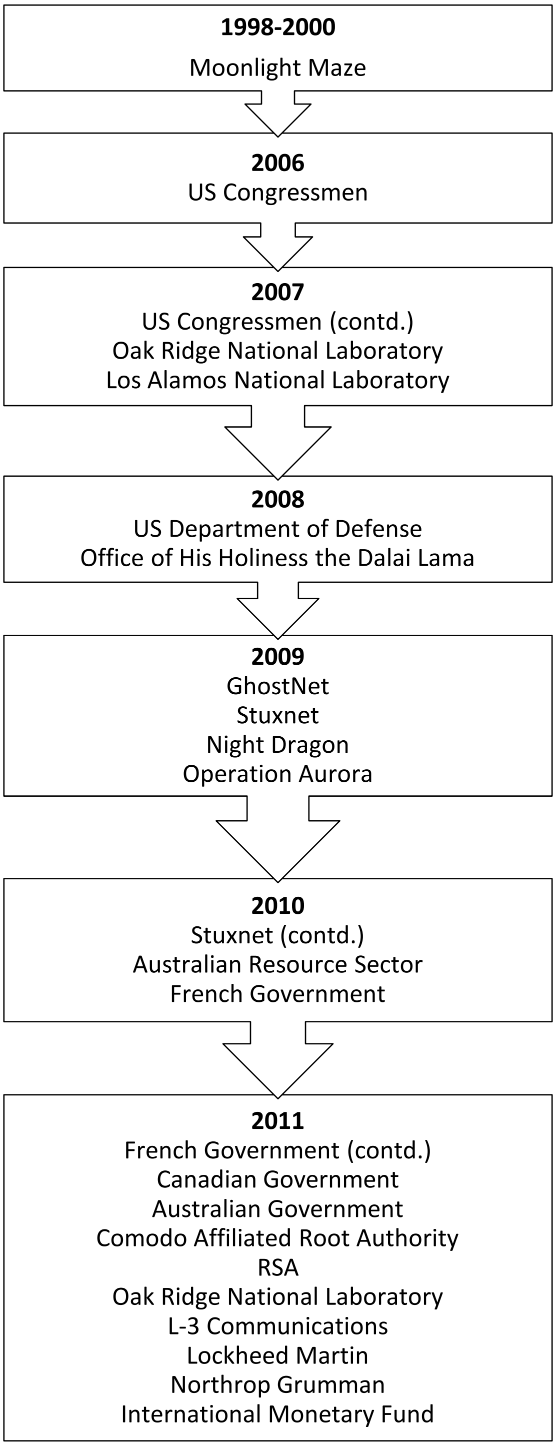

FIGURE 1 - TIMELINE OF APT ATTACKS

Summary of Significant Attacks

March 1998-2000 – Moonlight Maze

Cyber attacks dubbed 'Moonlight Maze' targeted computers at the Pentagon, NASA, the US Energy Department, research laboratories and private universities. The attackers successfully gained access to tens of thousands of files. (Arquila, 2003) (Central Intelligence Agency, 2007)

August 2006-2007 – US Congressmen

The office computer networks of two congressmen were reportedly compromised. Information is believed to have been stolen about dissidents critical of the Beijing regime. (The Washington Times, 2008)

29 October 2007 - Oak Ridge National Laboratory

Oak Ridge National Laboratory was successfully targeted using emails that were socially engineered to appear as though they were legitimate official communications. Computers were compromised, as was a database which contained information about visitors to the facility. The hackers are believed to have stolen data from the database. (Oak Ridge National Laboratory, 2007)

9 November 2007 – Los Alamos National Laboratory

Los Alamos National Laboratory advised all employees of a recent malicious hacking event that affected a small number of computers on the laboratory's unclassified 'Yellow' network. A significant amount of unclassified data was stolen. The attack is believed to have been part of a broader, coordinated attack against US laboratories and other institutions. (Anastasio, 2007) (Snodgrass, 2007) (Goodin, 2007)

Early 2008 – US Department of Defense

The US Department of Defense suffered a significant compromise of both unclassified and classified military computer networks after a foreign intelligence agency placed malicious software on a USB flash drive. The device infected a US military laptop upon insertion. The malicious code then propagated through US networks infecting numerous computers. (Lynn III, 2010)

COPYRIGHT © COMMAND FIVE PTY LTD. ALL RIGHTS RESERVED.

September 2008 – Office of His Holiness the Dalai Lama

A legitimate email was intercepted in transit to the Office of His Holiness the Dalai Lama (OHHDL) and the attachment replaced with a file containing malicious content. This attack appeared to be part of a concerted effort in which hackers used social engineering techniques to gain access to the OHHDL computer network. The hackers appear to have obtained user passwords through the intrusion and later used these to remotely access the OHHDL mail server. (Nagaraja & Anderson, 2009)

29 March 2009 – GhostNet

Researchers released a report detailing a cyber espionage operation dubbed 'GhostNet' which infiltrated at least 1295 computers in 103 countries, including those belonging to embassies, South Asian governments and the Dalai Lama. (Secdev, 2009)

June 2009 – Stuxnet

First known targeting of an unnamed organisation occurred using the Stuxnet[4] worm. The organisation was again targeted in March and April 2010. Numerous other organisations, primarily in Iran, were also targeted. The worm appears to have been part of a coordinated effort to reprogram a specific industrial control system, such as a gas pipeline or power plant, likely located in Iran. (Farlliere, O Muchu, & Chien, 2011) (U.S Office of Counterintelligence, 2011)

November 2009 – Night Dragon

Starting in November, coordinated covert and targeted cyber attacks were observed against global oil and petrochemical companies. These attacks, labelled as 'Night Dragon', used socially engineered emails along with Microsoft Windows operating system vulnerabilities to gain access to computers. Using the access obtained the hackers accessed information on operational oil and gas field production systems and financial documents relating to field exploration and bidding. (McAfee Foundation Professional Services and McAfee Labs, 2011)

Mid December 2009 – Operation Aurora

Google detected a highly sophisticated and targeted attack on Google corporate infrastructure that resulted in the theft of intellectual property. This event is believed to have been part of a coordinated attack, known as 'Operation Aurora', in which hackers sought source code from Google, Adobe Systems and dozens of other high profile companies. (Drummond, 2010) (Zetter, 2010)

2010 – Australian Resource Sector

Three major Australian resource sector companies (BHP Billiton, Fortescue Metals Group and Rio Tinto) were targeted by cyber attacks. Targeting of Rio Tinto's computer network occurred around the time of the arrest of Stern Hu in July 2010. (AAP, 2010)

December 2010-March 2011 – French Government

The French Government was successfully targeted by a socially engineered email campaign. Over 150 computers in the French Ministry of Economy and Finance's Central Services division were compromised. The hackers were able to remotely control the ministry's computers and retrieve documents for over three months. The hackers sought documents related to the French presidency of the G20 and international economic affairs. (Walid Berissoul et agencies, 2011) (AFP, 2011)

January 2011 – Canadian Government

Canadian Government departments were targeted using emails socially engineered to appear as though they were sent from senior staff members within the departments. The emails contained malicious attachments that compromised Canadian Government computers and resulted in the theft of classified information. (Postmedia News, 2011)

February-March 2011 – Australian Government

Australian parliamentary computers were accessed over a period of at least one month. During that time several thousand emails may have been accessed including those of the Australian Prime Minister, Foreign Minister and Defence Minister. (Benson, 2011)

[4] The Stuxnet worm is a malicious computer program capable of replicating itself to infect multiple linked computer systems.

COPYRIGHT © COMMAND FIVE PTY LTD. ALL RIGHTS RESERVED.

15 March 2011 – Comodo Affiliated Root Authority

A Comodo affiliated digital certificate Root Authority (RA) was compromised resulting in the issue of fraudulent SSL certificates for the popular domains: mail.google.com, www.google.com, login.yahoo.com, login.skype.com, addons.mozilla.org, login.live.com and global trustee. (Comodo, 2011)

17 March 2011 – RSA

RSA released a public statement advising that they were recently targeted via socially engineered emails containing malicious attachments that exploited a zero day Adobe Flash vulnerability. Hackers successfully gained access to the network and exfiltrated information including that related to RSA's SecurID two-factor authentication products. The stolen information was later used to enable targeting of defence contractors. (Coviello, Open Letter to RSA Customers, 2011)

Mid April 2011 – Oak Ridge National Laboratory

Oak Ridge National Laboratory was targeted with socially engineered emails tailored to appear as though they were from the laboratory's Human Resources department. The emails tricked recipients into downloading malicious software that exploited a zero day vulnerability in Internet Explorer. The laboratory shut down all internet access and email systems from April 15 to April 17 to ensure no data was exfiltrated before the infection could be cleaned up. No large scale exfiltration of data is known to have occurred. (Munger, 2011)

6 April 2011 – L-3 Communications

An L-3 Communications executive notified employees that the company had been actively targeted leveraging information stolen from RSA the month prior. (gHale, 2011) (Poulsen, 2011)

21 May 2011 – Lockheed Martin

Lockheed Martin detected a cyber attack on its computer network. The company's information security team took aggressive actions to protect the systems. No exfiltration of data is known to have occurred. RSA has publicly stated that information stolen from it in March was used as an element of the attack on Lockheed Martin. (Lockheed Martin Corporation, 2011) (Coviello, Open Letter to RSA SecurID Customers, 2011)

26 May 2011 – Northrop Grumman

Northrop Grumman reportedly shut down remote access to its network without warning and conducted an organisation wide password reset, raising speculation that it had also been targeted using information stolen from RSA. (Kaplan, 2011)

May-June 2011 – International Monetary Fund

At least one International Monetary Fund (IMF) computer was compromised in a large and sophisticated cyber attack that involved significant reconnaissance and utilised software written specifically to target the IMF. The compromised computer was used to access internal systems and files. The hackers' access could have given them visibility of sensitive economic and political information. (Reddy, Gorman, & Perez, 2011; Sanger & Markoff, 2011) (The Guardian, 2011)

COPYRIGHT © COMMAND FIVE PTY LTD. ALL RIGHTS RESERVED.

The Current Cyber Threat Environment

APTs have targeted governments around the world, global oil, energy, and petrochemical companies, the mining sector, financial institutions, military contractors, the science and technology sector, dissidents, critical infrastructure and likely many additional sectors. They have also targeted technology companies that could enable future targeting. The Operation Aurora attacks, the Comodo affiliated RA compromise and the RSA attack set a precedent for such targeting.

The Aurora attacks appear to have been carried out to provide the attacker with source code and other information that may allow them to develop zero day exploits and rootkits[5] for use on their targets. The certificates generated in the Root Authority attack would likely be of use for future state-driven attacks (despite a lone Iranian individual claiming full responsibility for the attack, and stating that there was no government involvement (Kobie, 2011)). The attack against RSA appears to have been conducted to gather sensitive information to facilitate attacks against organisations that use RSA security tokens for two factor authentication; including US defence contractors who work on classified projects.

Based on the trend toward the targeting of enabling companies and the increasing popularity of virtualisation, VMware Inc. and other virtualisation companies seem likely to be among companies targeted by APTs in the future. If unknown vulnerabilities in VMware software were discovered it could have far reaching ramifications, affecting the security of other companies. Especially given the increased popularity of cloud computing which often uses virtualisation to separate data belonging to different customers. It could also make it easier for malicious software to escape from virtualised analysis platforms and infect connected systems.

Even though details of APT attacks are scarce in the media, the released information is quite informative. Firstly, it tells us that humans are often the weakest link in the security chain and that users need to be better educated on the threat from social engineering. Socially engineered email campaigns are the most common social engineering technique used but not the only one. Secondly, it tells us technology companies need to be better prepared to protect sensitive information that can be used to negatively affect the security of their customers and business partners, and undermine the security safeguards put in place.

[5] Rootkits consist of software designed to hide an attacker's presence on a computer system. They can change the way malicious programs are seen by the operating system, making it blind to the presence of the malicious programs.

COPYRIGHT © COMMAND FIVE PTY LTD. ALL RIGHTS RESERVED.

Target	Targeting methods	Social Engineering?	Zero days?	Data stolen?	Confirmed by target?
Oak Ridge National Laboratory	Socially engineered emails	Yes	Yes (2011)	Yes	Yes
Los Alamos National Laboratories	Socially engineered emails	Yes		Yes	Yes
GhostNet (various targets)	Socially engineered emails (primarily)	Yes		Yes	Some targets
US Department of Defense	Infected USB drive			Yes	Yes
Stuxnet	Infected USB drive Network shares SQL databases		Yes (multiple)		Some targets
Night Dragon (various targets)	Socially engineered emails (primarily)	Yes		Yes	Some targets
Google	Socially engineered emails	Yes	Yes	Yes	Yes
Operation Aurora (various targets)	Socially engineered emails	Yes	Yes	Yes	Some targets
The French Finance Ministry	Socially engineered emails	Yes		Yes	Yes
Canadian Government	Socially engineered emails	Yes		Yes	Yes
Australian Government				Yes	No
Comodo affiliate Root Authority				Yes	Yes
RSA	Socially engineered emails	Yes	Yes	Yes	Yes
Lockheed Martin	VPN?		No	No	Yes
L-3 Communications	VPN?		No		No
Northrop Grumman	VPN?		No		No
International Monetary Fund				Yes	Yes

FIGURE 2 - COMMONALITIES BETWEEN REPORTED ATTACKS

ANATOMY OF AN ATTACK

Figure 2 shows us that the most common attack vector observed is socially engineered emails frequently, but not always, used in combination with zero day exploits. While most victims do not provide many details about the attacks against them, RSA[6] is one of the few that has provided quite detailed information. The attack methodology observed in the case of RSA appears to be quite typical. The distinct attack phases are shown in simplified form in Figure 3. (Rivner, 2011)

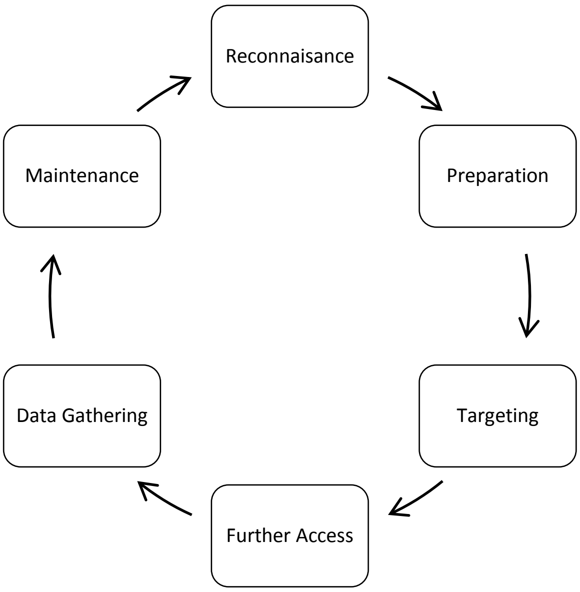

FIGURE 3 - BASIC APT ATTACK METHODOLOGY

Reconnaissance

The attacker passively gathers information about their target to identify the best targeting method. This may include research into the location of the target's offices, the location of their computers, technologies used by the company, how they communicate (between offices, with customers, suppliers and shareholders), their employees, their employees' contact details, interests and contacts.

Preparation

The attacker actively prepares for the attack, developing and testing appropriate tools and techniques to target their intended victim. This may include scanning to determine vulnerabilities, writing malicious code or acquiring code, drafting socially engineered emails, determining which email account to send socially engineered emails from, acquiring necessary hardware (such as USB flash drives), determining what infrastructure to use to launch the attack and for command and control communications, registering for and setting up necessary accounts (email addresses, callback domains etc.) and conducting testing.

Targeting

The attacker launches their attack and monitors for signs of compromise or failure. The sender may attempt to connect remotely to a server to exploit a vulnerability, strategically place a USB flash drive or give one to a target, send socially engineered emails and if possible, check for bounce back notifications, monitor command and control infrastructure for beaconing activity from the victim, try to connect inbound to the potentially compromised computer, or await feedback from an insider.

Further Access

Once an attacker has successfully gained access to a computer network they will usually try to identify where in the network they are and move laterally within the network to access data of interest and to install additional backdoors. This will usually require a return to step 2 (Preparation) and step 3 (Targeting), the upload of tools and malicious software, privilege escalation, network enumeration and identification of vulnerable hosts on which to install backdoors. It may also involve gaining access to the domain controller to obtain password hashes, covering tracks by altering logs, and accessing mail or file servers to enable data gathering.

Data Gathering

Once an attacker has identified information of interest they will try to gather this information and exfiltrate it. They may do this using a 'smash and grab' approach, trying to exfiltrate the desired data before it is detected, or they may opt for a 'low and slow' approach in which they exfiltrate the data in small quantities over a longer period.

[6] The attack on RSA is described in a blog post on the official RSA blog site; see http://blogs.rsa.com/rivner/anatomy-of-an-attack/

COPYRIGHT © COMMAND FIVE PTY LTD. ALL RIGHTS RESERVED.

Maintenance

Once an attacker has gained access to a network for information gathering purposes they will usually attempt to maintain their access. This may involve minimising the amount of malicious activity they generate on the network to avoid detection, periodically communicating with backdoors on the network to ensure they are working as intended, and making changes as appropriate. If automated data gathering tools are in use, it may also involve modifying search terms or the exfiltration path, volume or frequency. Maintenance also requires maintaining callback domains and any intermediary infrastructure used to communicate with the backdoors. If access is lost, the attacker may return to step 1 (Reconnaissance) or step 2 (Preparation) in an attempt to regain access.

IMPROVING ORGANISATIONAL RESILIENCE

To improve resilience to APTs organisations should employ good security practices and policies including those described below.

Information Centric Security

Adopt an information centric approach to security by applying multiple layers of security, affording the most sensitive information the most protection. If possible store sensitive information offline, or on a separate restricted access network.

Regular Patching

Regularly patch operating systems and applications including document viewers (e.g. Microsoft Office, Adobe Acrobat) and web browser plugins.

Computer Administration Restrictions

Minimise administrative access and restrict access so users do not possess both 'write' and 'execute' privileges for the same folder.

User Education

Educate users on the threat from socially engineered emails and other forms of social engineering. Encourage users to notify IT staff of suspicious events.

Network Access Restrictions

Restrict which computers can be placed on the corporate network via wired, wireless, and remote access methods.

Known Network Topology

Ensure system administrators are aware of the location of all computers, computer equipment and Internet gateways so they can secure the network (including wireless access points and 3G USB modems).

USB Drive Control

Restrict which USB drives can be used on corporate networks and develop policies on permitted usage and minimum encryption requirements.

Intrusion Analysis

Conduct intrusion analysis (both host-based and network based) to detect anomalous activity.

Access Control

Employ two-factor authentication where possible, particularly on Virtual Private Networks. Restrict user access using least privilege methodology, encourage good password control, regularly audit access logs, and review access levels.

Sender Policy Framework

Employ the Sender Policy Framework[7] to help protect against spoofed emails.

[7] The Sender Policy Framework is an open standard specifying a technical method to prevent sender address forgery. (Mehnle, 2010)

COPYRIGHT © COMMAND FIVE PTY LTD. ALL RIGHTS RESERVED.

References

AAP. (2010, April 19). *Mining firms hit by China cyber attack*. Retrieved June 13, 2011, from The Sydney Morning Herald: http://www.news.smh.com.au/breaking-news-national/mining-firms-hit-by-china-cyber-attacks-20100419-spc9.html

AFP. (2011, March 07). *French government comes under cyber attack.* Retrieved June 13, 2011, from The Age: http://news.theage.com.au/breaking-news-world/french-government-comes-under-cyber-attack-20110307-1bl8z.html

Anastasio, M. (2007, December 06). *Los Alamos also hacked.* Retrieved June 13, 2011, from Frank Munger's Atomic City Underground: http://blogs.knoxnews.com/munger/2007/12/los_alamos_also_hacked.html

Arquila, J. (2003, March 04). *Interviews - John Arquilla.* Retrieved June 13, 2011, from Cyber War! | Frontline | PBS: http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/arquilla.html

Benson, S. (2011, March 29). *Hackers log in to federal MPs' emails.* Retrieved June 13, 2011, from The Daily Telegraph: http://www.dailytelegraph.com.au/news/national/hackers-log-in-to-federal-mps-emails/story-e6freuzr-1226029677394

Borders, K. (2007, July 19). *Building a Threat Model: Hackenomics (Part 2 – The Cost of Hacking)*. Retrieved June 13, 2011, from StraightSecTalk: http://www.straightsectalk.com/?p=16

Central Intelligence Agency. (2007, May 02). *Annual Report 1999 Counterintelligence.* Retrieved June 13, 2011, from Central Intellgence Agency: https://www.cia.gov/library/reports/archived-reports-1/ann_rpt_1999/dci_annual_report_99_16.html

Comodo. (2011, March 31). *Comodo Report of Incident*. Retrieved June 13, 2011, from Comodo Group Inc.: http://www.comodo.com/Comodo-Fraud-Incident-2011-03-23.html

Coviello, A. (2011, March 17). *Open Letter to RSA Customers*. Retrieved June 13, 2011, from RSA: http://www.rsa.com/node.aspx?id=3872

Coviello, A. (2011, June). *Open Letter to RSA SecurID Customers*. Retrieved June 13, 2011, from RSA: http://www.rsa.com/node.aspx?id=3891

Drummond, D. (2010, January 01). *A new approach to China*. Retrieved June 13, 2011, from The Official Google Blog: http://googleblog.blogspot.com/2010/01/new-approach-to-china.html

Farlliere, N., O Muchu, L., & Chien, E. (2011, February). *W32.Stuxnet Dossier.* Retrieved June 13, 2011, from Symantec: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

gHale. (2011, June 03). *Second Defense Contractor Targeted*. Retrieved June 13, 2011, from Industrial Safety and Security Source: htp://www.isssource.com/second-defense-contractor-targeted/

Goodin, D. (2007, December 07). *Top-secret US labs penetrated by phishers.* Retrieved June 13, 2011, from The Register: http://www.channelregister.co.uk/2007/12/07/national_labs_breached/

Kaplan, J. (2011, June 01). *Exclusive: Northrop Grumman May Have Been Hit by Cyberattack, Source says.* Retrieved June 13, 2011, from Fox News Network: http://www.foxnews.com/scitech/2011/05/31/northrop-grumman-hit-cyber-attack-source-says/

COPYRIGHT © COMMAND FIVE PTY LTD. ALL RIGHTS RESERVED.

Kobie, N. (2011, March 29). *Lone Iranian claims credit for Comodo certificate hack.* Retrieved June 13, 2011, from PC & Tech Authority: http://www.pcauthority.com.au/News/252662,lone-iranian-claims-credit-for-comodo-certificate-hack.aspx

Lockheed Martin Corporation. (2011, May 28). *Lockheed Martin Customer, Program and Employee Data Secure*. Retrieved June 13, 2011, from Lockheed Martin: http://www.lockheedmartin.com/news/press_releases/2011/0528hq-secuirty.html [sic]

Lynn III, W. J. (2010, October 04). *Defending a New Domain: The Pentagon's Cyberstrategy.* Retrieved June 13, 2011, from U.S. Department of Defense: http://defense.gov/home/features/2010/0410_cybersec/lynn-article1.aspx

McAfee Foundation Professional Services and McAfee Labs. (2011, February 10). *Global Energy Cyberattacks: "Night Dragon"*. Retrieved June 13, 2011, from McAfee: http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf

Mehnle, J. (2010, April 17). *Sender Policy Framework: Introduction.* Retrieved June 13, 2011, from The Sender Policy Framework Project: http://www.openspf.org/Introduction

Moyanhan, M. (2011, February 14). *The Price of a Zero Day Exploit*. Retrieved June 15, 2011, from Veracode, Inc. The State of Software Security: http://www.veracode.com/ceo-blog/2011/02/the-price-of-a-zero-day-exploit/

Munger, F. (2011, April 19). *Lab halts Web access after cyber attack*. Retrieved June 13, 2011, from Knoxville News Sentinel Co.: http://www.knoxnews.com/news/2011/apr/19/lab-halts-web-access-after-cyber-attack

Nagaraja, S., & Anderson, R. (2009, March). *The snooping dragon:social-malware surveillance of the Tibetan movement.* Retrieved June 13, 2011, from University of Cambridge: http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-746.html Shishir Nagaraja, Ross Anderson March 2009

Oak Ridge National Laboratory. (2007). *Potential Identity Theft*. Retrieved June 13, 2011, from Oak Ridge National Laboratory: http://www.ornl.gov/identitytheft/

Postmedia News. (2011, June 03). *Classified infromation accessed during cyber attacks on federal departments: Report.* Retrieved June 13, 2011, from Postmedia Network Inc: http://www.canada.com/news/Classified+information+accessed+during+cyber+attacks+federal+departments+Report/4888892/story.html

Poulsen, K. (2011, May 31). *Second Defense Contractor L-3 'Actively Targeted' With RSA SecurID Hacks*. Retrieved June 13, 2011, from Wired: http://www.wired.com/threatlevel/2011/05/l-3/

Reddy, S., Gorman, S., & Perez, E. (2011, June 13). *IMF Mum on Details of Network Cyberattack.* Retrieved June 13, 2011, from The Wall Street Journal: http://online.wsj.com/article/SB10001424052702304665904576381973865291928.html

Rivner, U. (2011, April 01). *Anatomy of an Attack.* Retrieved June 13, 2011, from Speaking of Security: The Official RSA Blog and Podcast: http://blogs.rsa.com/rivner/anatomy-of-an-attack/

Sanger, D., & Markoff, J. (2011, June 11). *I.M.F Reports Cyberattack Led to 'Very Major Breach'.* Retrieved June 13, 2011, from The New York Times: http://www.nytimes.com/2011/06/12/world/12imf.html

Secdev. (2009, March 29). *Tracking GhostNet: Investigating a Cyber Espionage Network.* Retrieved June 13, 2011, from Information Warfare Monitor: http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network

COPYRIGHT © COMMAND FIVE PTY LTD. ALL RIGHTS RESERVED.

Snodgrass, R. (2007, December 14). *Cyber attack on LANL outs personal info.* Retrieved June 13, 2011, from LANL: The Rest of the Story: http://lanl-the-rest-of-the-story.blogspot.com/2007/12/cyber-attack-on-lanl-outs-personal-info.html

The Guardian. (2011, June 13). *IMF hit with serious state-sponsored cyber attack.* Retrieved June 13, 2011, from The Sydney Morning Herald: http://www.smh.com.au/technology/security/imf-hit-with-serious-statesponsored-cyber-attack-20110613-lfzm0.html

The Washington Times. (2008, June 12). *Hacking on Hill traced to China.* Retrieved June 13, 2011, from The Washington Times: http://www.washingtontimes.com/news/2008/jun/12/hacking-on-hill-traced-to-china/

U.S Office of Counterintelligence. (2011, June 14). *Stuxnet Worm*. Retrieved June 13, 2011, from Spy and Terrorist Briefing Center: http://www.hanford.gov/oci/ci_spy.cfm?dossier=138

Walid Berissoul et agencies. (2011, March 07). *Bercy: la cyber-attaque visait le G20*. Retrieved June 13, 2011, from Europe1: http://www.europe1.fr/France/Cyber-attaque-le-G20-vise-selon-Bercy-442555/

Zetter, K. (2010, January 14). *Google Hack Attack Was Ultra Sophisticated, New Details Show*. Retrieved June 13, 2011, from Wired: http://www.wired.com/threatlevel/2010/01/operation-aurora/

COPYRIGHT © COMMAND FIVE PTY LTD. ALL RIGHTS RESERVED.

COPYRIGHT NOTICE

Copyright © Command Five Pty Ltd. All rights reserved.

This document is provided by the copyright holders under the licence that follows. By obtaining, using, and/or distributing this document you agree that you have read, understood, and agree to the terms and conditions that follow.

The names and trademarks of Command Five Pty Ltd may not be used in advertising or publicity relating to this document or its contents without specific, prior, written permission.

No permission is given for this document to be used for commercial purposes or as part of any commercial activity or undertaking, including, but not limited to, use in or relating to advertising or publicity, and/or use in support of, or as part of, any pre-sales or sales activities.

No permission is given to create modified or derivative works. You may distribute this document in its original form for non-commercial purposes in accordance with the other terms and conditions stated herein. Copyright title will at all times remain with the copyright holders.

All referenced trademarks remain the property of their respective owners.

THIS DOCUMENT IS PROVIDED 'AS IS' FOR INFORMATIONAL PURPOSES ONLY WITH NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, INCLUDING BUT NOT LIMITED TO ANY WARRANTY, EXPRESS OR IMPLIED, OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE; WARRANTY OF NON-INFRINGEMENT, OR TITLE; NOR ANY WARRANTIES PERTAINING TO THE ACCURACY OR COMPLETENESS OF CONTENT.

ANY OPINIONS EXPRESSED IN THIS DOCUMENT MAY CHANGE WITHOUT NOTICE AND ARE NOT NECESSARILY THE CONSIDERED OPINIONS OF COMMAND FIVE PTY LTD, ITS PARTNERS, EMPLOYEES, OR AFFILIATE ORGANISATIONS. ANY ADVICE OFFERED IN THIS DOCUMENT IS OFFERED WITHOUT WARRANTY OF ANY KIND.

Command Five Pty Ltd
ABN: 49 149 576 670

http://www.commandfive.com
info@commandfive.com