ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 1, January 2014

Advanced Persistent Threats & Recent High Profile Cyber Threat Encounters

Vaishali S Raj[1], Dr. R. Manicka Chezhian[2], M.Mrithulashri[3]

Research Scholar, Dr. Mahalingam Centre for Research & Development, NGM College, Coimbatore, India[1]

Associate Professor, Dr. Mahalingam Centre for Research & Development, NGM College, Coimbatore, India[2]

Assistant Professor, Dept of Computer Science, KGISL Institute of Information Management, Coimbatore, India[3]

ABSTRACT: Advanced Persistent Threat's (APT) are sophisticated and high – outlined covert attacks which are bent on surreptitiously stealing/exfiltration of data and classified information from targeted/victimized systems inflicting unrecoverable and serious impairments. These unremitting and persistent threat intrusions typically target users or systems within the organizations to gain access and infiltrate and to haul out Trade Secrets, Collapse Stock Values and other sensitive information, Technology/IP, steal Intellectual Property, State/Nations & Military Secrets, computer Source Codes and other Valuable Information and extending up to crippling a Nation's Critical Infrastructure. APT's continue to emerge as a prominent concern and the expansion in APT's exposure is trending heavily towards High – Profile Stealthier and Cyber Espionage activities. The threats involve stealthy and shadier right of entry into end – point systems and ongoing theft of confidential and top – secret information. This paper illustrates the anatomy of the Advanced Persistent Threat and their terminologies with the Recent and Concentrated threat scenarios on cyberspace in obliging times.

Keywords: Advanced Persistent Threats, Ransomware, Banking Trojans, Sophisticated Malwares.

I. INTRODUCTION

The Advanced Persistent Threats are evolving into a surgically précised attacks breaking every technical barriers making the traditional defences and high end security void. The APT's rendered in the year 2013 were well deliberated and Nation – State sponsored cyber attacks carried out by highly motivated, technically advanced skilled adversaries. The APT's are characterized by Stealthy, Targeted, Evasive, Persistent, and Adaptable Characteristics and designed to break into the target systems without leaving any hint of their existence making them complex to trace back their origin or the Command and Control centre and stays even for years within the system. A rapid lateral movement of Data collection (aiding with Command Shells, NetBIOS commands, Windows Terminal Services other than malwares) ensues once the APT's slithered or break through the security defences. Multiple breaches of Sony's Playstation and making it offline for 24 days made an estimated loss of $171 million as a result of an APT, while high – profile companies like Google, Yahoo, Symantec, Adobe systems and other major industries were victimized for these advanced threats. The 'Icefog' is one such APT, discovered in recent times and was active since 2011 and despite their lack of technical complexity; they were successful in compromising targets in Governmental institutions, Military and Defence contractors, Ship Building and Maritime Corps., Telecom, Aviation and other high tech companies. The name 'Icefog' comes from a string used in the Command & Control server name in one of the samples, the Command & control software is named "Dagger Three", in Chinese language. The 'Icefog' backdoor set (also known as "Fucobha") is an interactive espionage tool that is directly controlled by the attackers (unlike other APT's that involves Botnet and other malicious malwares). There are versions for Microsoft Windows and Mac OS X. In its latest incarnation, Icefog doesn't automatically exfiltrated data; instead, it is operated by the attackers to perform actions directly on the victim's live systems [1].

II. ADVANCED PERSISTENT THREAT – AN OVERVIEW

The Advanced Persistent Threat's are primarily designed to leave no hint of their Entry or Exit making it a complex task of classifying and tracing their Source and the Command & Control centre for their existence and remain Persistent even for years. To trail an Advanced Persistent Threat, the foremost entities deployed are:

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 1, January 2014

- Wide range of Highly Advanced and Mutating Malwares to infringe either the whole of the target system or a part (Ex: Stuxnet – Targeted mainly for Centrifuges that spin nuclear materials)
- Ultra Sophisticated Cyber Hacks (Ex: Operation Aurora – Targeted Google & high profile corps.)
- Technically Advanced Espionage and Data Exfiltration tools
- Persistent Target Surveillance
- Creating Watering Holes
- Creating Un-Patchable Zero Days, Discovering the Zero-Day vulnerabilities
- Social Engineering (i.e., Spear Phishing Emails, Spams, Malvertising, Web based Attacks)
- Technically Elevated Network Sniffing Tools.

A. Stages Involved In an APT

The main stages involved during an APT attacks choosing the Target and performing the Infiltrations upon the target, Reconnaissance involving establishing the Backdoors and mapping out the Network and Vulnerabilities, Lateral Data movements involves Key logging, Surveillance and initiating the target system connection with the Command & Control centre ending up with cleaning their trail leaving no hint of existence.

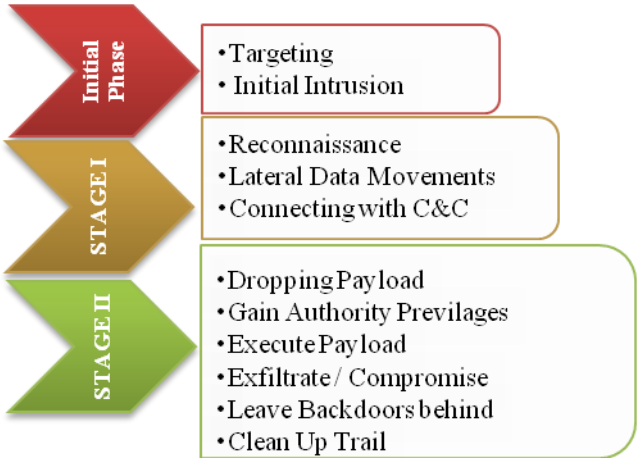

Fig 1: Stages involved during the APT attacks into the Target

Gaining a strong foothold in the target environment is the primary goal of the initial intrusion. Once a system is exploited, the attacker usually places malware on the compromised system and uses it as a jump point or proxy for further actions. Malwares placed during the initial intrusion phase is commonly a simple downloader, basic Remote Access Trojan or a simple Shell. Overcoming a target's perimeter defences and establishing a foothold inside the network can require substantial effort. The APT attackers knows that most organizations run Antivirus solutions in their environment and they take steps to ensure that their tools are undetected which means producing or customizing malware and rewriting or repackaging commonly used tools. These custom tools are tested against the Up-to-Date Antivirus and other security tools to evaluate whether they are detected. Modifications continue until the tools evade all scans [2].

III. ADVANCED PERSISTENT THREAT - TERMINOLOGIES

The major terminologies in the Advanced Threat scenarios are:

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 1, January 2014

TABLE 1
CENTRAL APT TERMINOLOGIES

Backdoor	Allow unauthorised access into Target system. A Backdoor can be a result of a Vulnerability, Programming Error or Malware
Spear – Phishing/ Social Engineering	Email spoofing attempts that target specific organizations seeking unauthorised access into confidential data.
Exploit Kit	A piece of software, sequence of commands that take advantage of a Bug, Glitch or Vulnerability in order to cause unintended & unanticipated behaviour on the target systems.
Payload	Once the Exploit Kit/Code accesses a target system, the payload is executed (usually to install a Backdoor).
Root Kit	Set of codes that enable Admin level access to the target systems & their networks. It facilitates masking the intrusion and is installed gaining the user level access
Sand Box	Mechanism of executing untrusted and unauthorised code within tightly controlled set of resources.
Sink Hole	Multi faceted security tool – portion of the network that is designed to accept & analyse attack traffic & used mainly by the attackers to divert network traffic of the target systems, worm propagation and other network activity.
Vulnerability	Typically a Flaw in the OS or Application software.
Zero – Day	An exploit that takes advantage of security vulnerabilities for which there are no patches available which are extremely dangerous. The Zero – Days are sold in black market.
Botnet	Network of computers infected with malicious software and controlled as groups to cause DDoS attacks, sending spams etc.,
Rouge Certificate	Digital certificates whose Private key and certificate files are illegitimately accessed & copied
Drive – by – Download	Compromising the targets by tricking them into unintentionally download malicious codes through Web, clicking a Pop up or viewing Emails.
Watering Holes	Infusing malwares into the website the target frequently visits or likely to visit.

IV. RECENT HIGH PROFILE THREAT SCENARIOS/APT ATTACKS

A. Complex and Polymorphic Android Malware Platform

Unlike Sophisticated Malwares, the Android Malware platform has equally and highly evolved into resisting their Detection through digital defences, obfuscation of class names, URL encryptions , Command & Control server thus moving towards Polymorphic attacks like APT's. The first Ransomware attack against Android devices called 'Android Defender' was discovered in June 2013, this hybrid fake antivirus app demanded a $99.99 payment to restore access to the android device. 'Andr/spy-ABN', sometimes called as 'QUADARS' discovered in September 2013 is a new form of Banking Trojan for Androids that combined "Man - in – the – Browser" attack against Social Engineering designed to compromise the Android Smartphones. When launched, Quadars recursively looks for folders inside the %APPDATA% directory. Quadars is a banking malware performing a usual Man – in – the – Browser attack to steal online credentials and lure the user to install a fraudulent SMS-Stealing Mobile application [3]. The Android platform scenario is broadened into another vulnerability of Data Leak. One of the recent Huge Data leak in the android platform is the Snapchat app with Usernames and Phone numbers of 4.5 million users published on a site called SnapchatDB.info after attackers took advantage of an exploit disclosed. According to Trend Micro's analysis, around 20% of all apps are consistently leaking the data and the most common data leaks are Contacts, Location, access to Photos & Videos, Phone Number and details about the device and SIM [4] which are on the other side are made mandatory to provide to proceed with almost every app activity in the Android platform creating a huge security gap.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 1, January 2014

B. Banking & Financial Sector Trojan Attacks:

The dominance of Banking Trojans in the year 2013 was significant and extremely flexible supporting wide series of functionalities intended to assist fraudulent transactions across variety of services. The main entities in recent times are 'zbot (+Gameover)' which compromised more than 2,000,000 banking systems & cridex which compromised 1, 25,000 financial systems and Shylock, spyeye, Mebroot to name a few advanced banking Trojans. Today's banking Trojans typically utilize an updatable and encrypted configuration file, which is stored in the file system, the registry (or) is actually embedded in the Trojan itself. The configuration file contains a list of target URL's along with the rules to be applied to the WebPages. Modern day Banking Trojan kits typically contain of the following components: Builder Application – used to configure and generate Trojan Payload; Backend Scripts – include a Control panel on a Command & Control server to direct compromised computers; Configuration Files – target URL's [5]. Emerging adaptation of Banking Trojans includes Captcha and SQL Injections within their config files. Another advanced Banking APT is 'Man – in – the – Browser' (MitB) which takes place at the Presentation Layer of the Internet & engages in infiltrating the Banking Websites while capable of handling Web Injection Scripts that dynamically Loads & Transfers Banking data from the target. The intelligence of MitB is, it presents no indications of malicious activity, legitimate appearance of the Banking Domain, Perfect Digital Signatures presenting every aspects of a Credible & Secure Banking Transactions ending up fooling the user.

C. Sophisticated Malwares & Exploit Kits

Malware Intrusion & Embedding endows as an indispensable entity of initiation for any APT actors towards the target systems, thereby are evolving into highly complex, mutating and hard to trace back and bye-passes every kind of technical security defences. The Malwares are gaining tremendous technicality such that Re-Engineering of the Malwares are becoming an exceptionally complex undertaking.

1) *Metamorphic & Polymorphic Malwares for APT attacks*: Metamorphic Malwares are designed to automatically Re-Code or Re-Engineer itself each time it propagates or is distributed within the target system, Rewritten every iteration, the metamorphic malwares are entirely different from the succeeding and preceding ones. In spite of Permanent changes to code, each iteration of metamorphic malware functions the same way. The longer the malware stays in a target system, the most iteration it produces and the more-sophisticated the iterations are; making it increasingly hard for Antivirus applications to detect quarantine and disinfect [6]. In a Metamorphic malware, 10 – 20% consists of malicious code and the remaining percentage consists of Morphing Engine Code. The Polymorphic Malware poses increasing challenges to effective signature-based antivirus protection. They can morph themselves and self-obfuscate themselves when infiltrated within the target systems in response to a Signature updates by the Antivirus software's.

2) *Web-Based Malware attacks:* In March 2013, 'Darkleech' and related attacks were the most prevalent web threat detected on customer end-points & web appliances accounting for almost 30% of all detected web threats [7].The Darkleech compromised systems running mainly over Apache web servers, and once it takes a hold, it injects invisible code into WebPages which in turn surreptitiously opens a connection that exposes visitors to malicious third-party websites [8]. Malvertising was on high during 2013 arriving through prominent sources like YouTube. Troj/SWFRed-D (Macromedia Shockwave Flash (SWF) file) is a widely encountered Malvertising Trojan encountered in YouTube ads during 2013 which redirected large number of users to exploit kits.

   Yahoo's advertising servers were anonymously attacked and the clients visiting the Yahoo site received ads as originating from legitimate 'ads.yahoo.com' server; upon clicking the ad, an exploit-kit is sent that exploits Java vulnerabilities and installs malwares. Initially believed to have affected only European users on January 3, 2014, the malware ad attacks were then said to have occurred during December 31, 2013 – January 3, 2014. But Yahoo revealed the attack actually took place December 27, 2013 – January 3, 2014, infecting almost 2 million machines during the four day attack [9].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 1, January 2014

Trojan.APT.Seinup – recently encountered Trojan on Google Docs. This Trojan was found to have used a number of advanced techniques and leverages Google Docs to perform redirection to evade call-back detection. By connecting the malicious server via Google Docs; the malicious communication is protected by the legitimate SSL (Secure Socket Layer) provided by the Google Docs [10].

3) *Increase in Exploit Kits:* Blackhole Exploit Kit is another popular web threat around the year 2012, and are growing and evolving at rapid rate and according to AVG's Threat Labs; over 30% of all instances of malware in the world are caused by the Blackhole exploit kits [11]. The Blackhole kit was updated frequently and the code is highly obfuscated. It is often used to deploy Ransomware and Fake Security Software [12]. In the year 2013, newer and advanced versions of exploit kits like Neutrino, RedKit became more prevalent than the Blackhole. By July 2013, RedKit has become the most prevalent exploit kit reported, accounting for 42 % of exploit kit detections [13]. RedKit that targets legitimate websites was involved in National Broadcasting Company (NBC, USA) Website Hack in February 2013. The NBC's hacked pages were altered to add some malicious Java Script that injected an additional HTML component known as 'iframe' (inline frame) into the web page [14]. In case of any web based attacks, the targets are redirected to exploit-kit or any malicious contents, but RedKit does things differently. The initial redirect (typically an iframe) will be to another legitimate, but a compromised server. The compromised web servers used by RedKit are loaded with PHP Shells, which connects to remote RedKit Command & Control server and delivering malicious landing page and JAR (Java Archive) content to the victim via HTTP's from the C&C [15].

4) *Increase in Spams and Spam Servers:* India has seen an 280% increase in the Bot Infections, and the country accounts for nearly 15% of global Bot-Net Span, responsible for disseminating an estimated 280 million Spam Messages per day worldwide, and ranked First in Spam Zombies with 17% Spam Zombies located in India [16]. Pump – and – Dump Stock spams, imaged- based Spam (fake Rolex watch), health/weight loss spams, and Snowshoe spams were some of the chief spam campaigns encountered in the year 2013. In June 2013, two loaders, Fareit and Andromeda, were the leading forms of malware embedded in the Spam attachments [17].

5) *Increase in Botnet Infections:* The botnet's have become more widespread, resilient and stealthier in the recent times and are flexible in setting constraints for their controlling bots for participating in activities like widespread of DDoS (Distributed Denial of Service) attacks, sending Malwares & Trojans. Botnet operators are responding well for counter measures when the users are becoming defiant towards fake alerts, spams by deploying Ransomware instead. 'Carberp'- a banking-oriented credential- pilfering Botnet kit and 'Cryptolocker' - highly advanced Ransomware deployed by the APT actors were two most significant Botnet encounters in 2013 which resulted in loss of millions of dollars. The Cryptolocker implemented highly complex and strong encryption to encrypt important and confidential files of the target systems thereby storing the decryption keys in their Command & Control Servers making them authority in demanding a huge Ransom through Bit coins or other payment modes to gain access and take back the system. The Cryptolocker can camouflage itself as a list of essential Start-up programs of windows. While laterally uploads malicious tracking codes to determine the encryption and decryption keys.

V. CONCLUSION

The recent encounters of the Cyber attacks and APT's show an increasing, advancing & evolving trend of Cyber activities and attack intelligence in a mounting graph for the coming years. The rising volume of sophisticated and persistent threats, targeted data exfiltration, Ransomware, Financial and Banking attacks, Security Breaches at all levels of Defence, Un-Patched System Vulnerabilities and other rampant Web and Network attack areas creates a huge Security & Confidentiality Gap. Nation – State Sponsored Cyber Attacks, Cyber Extortion, Cyber Espionage and other Targeted attacks are getting bigger. Malwares with stolen Digital Signatures & Certificates are equally counter – Intelligent in response to the High Security Barriers and Telemetry Analysis making them complex to impede. The APT actors are highly skilled in making the Re-Engineering of their Malicious code very complex and are capable of infringing Sandbox Detection and by-passing all technical securities that imposes before them making them hard to identify or track down. Potential threat assessment, an integrated platform of Web And Network Analysis across

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 1, January 2014

different environments for any kinds of Intrusions, measures to store Identified Malware for analysing their Behaviour to mitigated future attacks, putting any kinds of suspicious files even from a legitimate source into the threat circle and scrutinize Incoming Mail Priorities can be some of the Counter measures that be used against APT attacks.

REFERENCES

[1] Global Research and Analysis Team (GREAT), "The 'Icefog': A Tale of Cloak and Three Daggers", Version 1.00, Kaspersky Labs, 2013.

[2] Dell Secure Works Counter Threat Unit (CTU) Research, "Lifecycle of an Advanced Persistent Threat", Dell SecureWorks, 2012.

[3] Daniel Lunghi, "QADARS: A New Banking Malware With A Fraudulent Mobile Application Component", www.lexsi-leblog.com/cert-en/qadars-new-banking-malware-with-fraudulent-mobile-application-component.html., October 2013.

[4] Snapchat user data exposed in huge data theft, http://countermeasures.trendmicro.eu/snapchat-user-data-exposed-in-huge-data-theft/, January 2014.

[5] Stephen Doherty, Piotr Krysiuk, "The State of Financial Trojans 2013", Version 1.02, Symantec Security Response, December 2013.

[6] Metamorphic and Polymorphic Malwares, http://searchsecurity.techtarget.com/definition/metamorphic-and-polymorphic-malware

[7][13][17] Security Threat Report 2014, Sophos Lab, 2014.

[8] Dan Goodin, "Ongoing Malware attack targeting Apache hijacks 20,000 sites", http://arstechnica.com/security/2013/04/exclusive-ongoing-malware-attack-targeting-apache-hijacks-20000-sites/ , April 2013.

[9] Chris Smith, "Yahoo ad malware attack far greater than anticipated", http://bgr.com/2014/01/13/yahoo-malware-attack/ , January 2014.

[10] Alastair Stevenson, "Google Docs Hijacked by Trojan.APT.Seinup malware", www.v3.co.uk/v3-uk/news/2276007/google-docs-hijacked-by-trojanaptseinup-malware, June 2013.

[11] AVG Blogs, "Threat Encyclopaedia: Blackhole Exploit Kit", http://blogs.avg.com/news-threats/threat-encyclopedia-blackhole-exploit-kit/ , May 2012

[12][16] Symantec Corporation, "Internet Security Threat Report 2013", Volume 18, April 2013.

[14] Paul Ducklin, "NBC Website hacked and distributes malware", http://nakedsecurity.sophos.com/2013/02/22/nbc-website-hacked-and-distributes-malware/ , February 2013.

[15] Fraser Howard, "Lifting the lid on the RedKit exploit kit", http://nakedsecurity.sophos.com/2013/05/03/lifting-the-lid-on-the-redkit-exploit-kit-part-1/ , May 2013.