APT – Will the current incident response methodologies be effective?

Lokesh Pidawekar

Information System Forensics – IA 5210

April 20, 2014

Contents

Figures

Introduction

Advanced Persistent Threat (APT) is a special category of threat which has evolved over last few years. It has been seen that conventional security tools such anti-virus, intrusion detection and prevention systems etc. are not sufficient in preventing APTs on larger extent. Cisco has reported in 2014 annual security report that investigations of multinational companies revealed signs of internal compromise and suspicious traffic originating from internal network and connecting to the malware hosting websites, anonymous FTP and VPN sites. Report also concluded that network penetrations remain undetected over longer periods of time. There is no silver bullet to stop APT in general. Hence incident response is very crucial during such attacks. This has created need for an effective incident respond methodology to mitigate/overcome APT and build necessary defense strategies and intelligence. Effective incident response will help in assessing the state of attack and formulate robust prevention mechanism. (Cisco, 2014)

What is APT?

Advanced Persistent Threats (APT) can be defined as stealthy and targeted attacks accomplished by sophisticated and organized attackers. These involve use of advance techniques and novel malwares by exploiting vulnerabilities in various resources of an organization. These attacks target against highly sensitive military, economic or proprietary information and continue for long duration since it is hard to detect. Thus persistent nature of attack causes more damage as compared to regular worm or virus attack.

APT Threat Actors

Advanced Persistent Threat actors are most sophisticated and well trained adversaries which may be state sponsored organized criminals or terrorists. They use social engineering, root kits, exploit kits, zero-day exploits, drive by downloads, DNS and routing modifications, rogue Wi-Fi devices and other useful methods to gain access and information. The actors adjust their techniques according to effectiveness of intrusion methods, incident response and security controls of target organization. The driving force behind such attacks ranges from financial advantage, competitive advantage and critical intelligence information. Hence, financial organizations, defense and aerospace, healthcare, manufacturing etc. organization becomes target of APT. (Nigel Willson, 2014)

Why it is different?

APT is growing rapidly with more complexities in hyper-extended networks. According to APT1 attack findings attackers are not only stealing intellectual property but they are interested in taking executive emails, conversation of scientists and even minutes of meetings. Hence it is important for organizations to be ready for adversaries and strengthen the overall security postulate of organization. Conventional methods of prevention and detection will not be sufficient to build strong defense against such attacks. Strong defense can be designed by involving latest technologies, threat intelligence and effective incident response strategy. (Mandiant, 2013)

The Preventive techniques

The evolution of advanced persistent threats prevention strategies require an intelligence-based threat model. Organizations need to monitor network continuously and protect critical information. This intelligence can be applied to understand network patterns of intrusion, mapping all threat indicators and iteratively learning adversary's behavior. The intelligence in prevention and detection will help the defenders mitigate not only vulnerability, but the threat as well. The growth of advanced persistent threats has created need for intelligence-driven computer network defense. (Eric M. Hutchins, Michael J. Cloppert, Rohan M. Amin, Ph.D.)

How APT infiltrates system

APT is step by step attack. There are several phases of attack as defined in white paper from Lockheed Martin Corporation.

1. *Reconnaissance*

   Reconnaissance is gathering information about the target in terms of IP range, domain names, open ports and services etc. Generally this is done for profiling the target in terms of determining effectiveness of various attack vectors. It can be done using web based search engine, crawling the website, social engineering, reading job posting and mailing lists etc.

2. *Weaponization*

   Weaponization can be defined as coupling malware payload with well-known files such as documents, PDF, spreadsheets etc. It is important to craft the file in such a way that it

should not be detected by antivirus, IDS or IPS devices. Poison ivy and gh0st RAT are well known backdoors used in APT in past few years.

3. *Delivery*

Delivery can be defined as transmission of payload to target. Payload can be delivered in form of email attachment, website or through USB removable media. Spear phishing is used to deliver malicious email attachment.

4. *Exploitation and installation*

Once the payload is delivered to victim, it is important to obtain persistent presence on target system. This is achieved by tricking the victim to install the payload in covert manner and exploiting an application or operating system flaw. The exploitation is also used for privilege escalation.

5. *Command and Control*

Once payload is installed on victim machine, compromised host can be used to scan other local machines for possible intrusion. It needs a permanent host to install the command and control which will connect outbound to Internet controller server to establish C2 channel. This provides a reliable mechanism of controlling compromised system remotely. The internal compromised host will communicate to C2 over SSL to avoid detection of activity from firewall.

6. *Actions on objectives*

Once the above steps are completed successfully, the attacker will start working on original goal like stealing money or sensitive information. Attackers will try to compromise more systems on target infrastructure and ex-filtrate data.

What is incident response?

Incident can be defined as adverse event causing potential harm to computer system or data. Incident Response includes actions taken subsequently to understand incident and take remedial steps. It focuses on assessing the damage, responding to events and recovering back to normal operation. One of the key steps of incident response is computer forensics which is process of analyzing, finding and presenting digital evidence in court. (Eric Cole, 2012)

Bruce Schneier, well known security researcher says, "*If you go back to the definition of security being protection, detection and response, this feels like the last area that needs work, and the idea of incident response coordination and working on a response is really important and something that isn't there.*" It is often seen that incident response is neglected in awe of preventive measures. It is important to understand that an effective incident response plan will make preventive measures more efficient. Furthermore, detection will not be worthwhile if it is not comprehended with good response plan. Hence it is important to get an operational incident response plan along with prevention and detection procedures. (Nigel Willson, 2014)

Why incident response is important in APT?

Threats cannot be eliminated completely but mitigating the threat quickly is need for the hour. Preventive measures of APT include Next generation firewalls, Data loss prevention technologies, unified threat management solutions such as IDS, IPS AV etc. Response plays an equally important role as prevention and detection in case of APT. Prevention and detection plan gets strengthened from effective response strategy.

Mandiant M-trends 2014 report shows that 229 is the median number days a threat actor remains undetected. Even though there are multiple chances to detect an attack and prevent it from spreading across the network, it has become very difficult to detect attack frequently. It is often seen that organizations get to know about the attack through third parties such as cloud providers or content management service providers. Sometime organizations are often compromised earlier, and the attack is detected 6-9 months later. Incident Response is still very important at any stage of attack and although it's a reactive mechanism; it becomes very valuable to minimize the damage of attack. Incident response starts from the time attack is being detected and continues until the organization recover back to normal operation. It helps in recovering the organization back to normal state and ensure that the attack does not happen again. Since APT attacks are meant to be persistent, incident response becomes very vital to the organization in order to get rid of the attack quickly. (Mandiant, 2014)

Building incident response plan

"Failing to plan is planning to fail" – Alan Lakein

Like any other plan, incident response also requires a planned approach. Few important points are:

- Management role is important to identify a team of skilled staff members dedicated to incident response.
- Senior executives should also actively participate in understanding the critical infrastructure of company for risk assessment.
- A security metrics should be defined to measure the milestones of incident response. It is important to make an inventory of all devices and software.

- Corporate infrastructure must be hardened with secure configuration. There should be a guideline for incident response during various attacks with well-defined roles of staff and management.
- It is critical for any incident response plan to maintain the integrity of data by preserving and handling evidence through analysis and reporting.
- There should also be documented approach to use tools and techniques during various scenarios. Documenting the findings and validating the result is an important step in making response plan. Hence, it is important to document the process and overall progress.
- Since most of the attacks do involve law enforcement, it is important to remain in boundaries and perform the required task. (Eric Cole, 2012)

An incident response plan should deal with all adverse events faced by the organization along with prospective threats which can be equally damaging for the organization. The main goal of an incident plan is to make sure that whenever a damaging event takes place, which is of high impact to the company, actions should be taken to minimize the exposure and prevent any recurrence of the particular event.

Incident response during APT attacks

To deal with APT, the incident response plan should include multiple ways of prevention, detection and response methods. Furthermore, incident response should include techniques to manage new malwares, zero day vulnerabilities etc. If the organization is dealing with top secret data, then it must prioritize APT incident response as one of the key component in Information Security Program and business strategy.

System Admin, Audit, Networking, and Security (SANS) has specific checklist for Incident handling including APT incidents. These steps give directions to develop process for an Incident Response program.

1. *Preparation*

   Preparation is most important part of any attack or defense strategy but often it is overlooked. This will include identifying critical infrastructure and intellectual properties of organization. It is important to identify what kind of data is on stake. The ultimate goal of incident response is timely recovery and response. If the plan is practiced then it can be executed quickly with minimal mistakes. Forensic examination and malware analysis are vital for APT incident response, therefore it is important to build a team of capable resources specializing in these areas. Training the team is equally important to get used to stress situation and can also facilitate smooth communication among team.

2. *Identification*

   APT attacks are complex and attacker may use known or new attack tools for executing the plan. It is often seen that attackers use some kind of Remote Access Trojan to keep a backdoor and steal the data. Hence, organizations must possess required defense tools to identify such malwares and use computer driven network intelligence to discover malware. Additionally, it is essential to keep checking outside posted data on cloud services such as pastebin, news to find any suspicious information.

3. *Containment*

   Once the APT threat actors are identified, the next step can be, to either watch the activity and learn consequent goals or disconnect them. Once the adversary is identified,

organization should take the network traffic sample and scan full corporate network to identify other infected systems. If management decides to stop the attack, then organization should update IDPS signature to block the adversary from further damaging. Based on the information collected, organization should also try to block specific port, server, DNS or IP range from entering into corporate network. At the same time, they should start assessing what resources have been stolen and subsequent legal ramifications around it.

4. *Eradication*

   After identifying the attack, it is likely that organization start focusing on recovering back to normal while overlooking eliminating the risk. This might lead to reoccurrence of the same attack or attack with slight variation. Hence, it is critical to identify all the infected systems and isolate them to separate network. Once isolated, a comprehensive forensic exam should be carried on these infected systems to collect digital evidence of the incident.

5. *Recovery*

   Once the attack is identified and eradicated, the next step is to rebuild the systems and move them into production. Before deploying back to production, the organization must re-engineer the system and while putting data back, it should be ensured that attacker's code or infection cannot be reintroduced into system. Even after putting these machines back into production, regular monitoring must be done to safeguard that attacker does not successfully get back into system.

6. *Lessons learned*

A key to incident response is to learn from mistakes and improve techniques. This involves assessing losses, achievements and failures in detecting and handling the malware. This step will also lead to development of Threat Intelligence group to identify adversaries. Kill – chain model can be used to for counter intelligence activities.

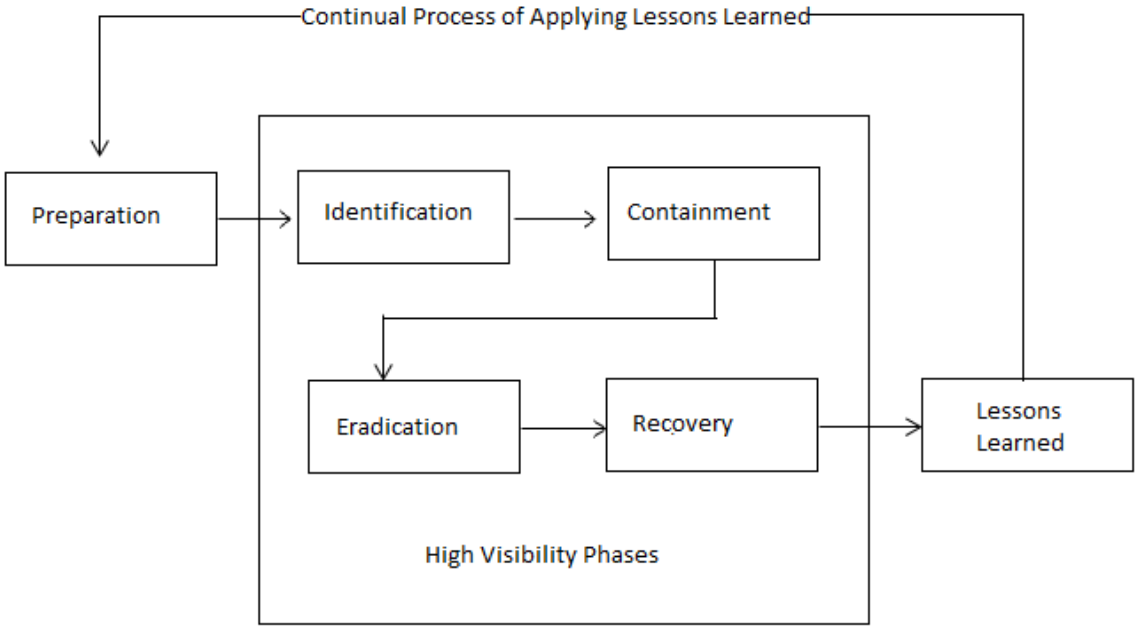

Figure 1.1 Six steps of incident response in APT, Source: Eric Cole "Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization"

The six steps for incident response can be pictorially represented in Figure 1. There is feedback loop from lessons learned into the preparation which shows that it's a continuous activity. Organization may focus on improving methods of incident response by developing active honey nets and deception capabilities. Correlation and aggregation of data is important for identifying APT. These might lead to adoption of SIEM tool and integrating various data resources such as

firewall, IDS, IPS, DMZ servers and network infrastructure. Security awareness campaign must be designed in view of APT since most of the APT attacks are based on spear phishing attack. Hence awareness among employees can become crucial in mitigating risk of APT. (Chris Crowley, Eric Cole, 2012)

Importance of Forensics in Incident Response

The main element of incident response is to know how the attack occurred and pattern of the attack on different systems. This can be achieved by conducting forensics tests on machines to analyze their logs and different processes running in the memory. Even a small change in the system alters the logs and one must have the eye to spot the different behavior or settings changed. Various memory and visualization forensic tools can be helpful to achieve the same.

The process of digital forensics

Collection

This involves Identification, labeling, recording and acquisition of data while preserving integrity.

Examination

It is the process of assessment of data manually or with help of automated tools to obtain data of particular interest while preserving its integrity.

Analysis

It involves analysis of examination results using legally justifiable methods and techniques.

Reporting

Once the analysis is complete, a report is created to describe methods used for obtaining data and subsequent results. It may also cover recommendations. (Karen Kent, Suzzane Chevalier, Tim Grance, Hung Dang, 2006)

Few cases involving application of computer forensics

Computer forensics plays an important role in uncovering the events by creating timeline of events and actions. A basic example of application of forensics is extraction of data from unallocated space. It is often noted in Mandiant's investigations that attackers collected the data and compressed it into a RAR archive and then transferred to command and control center. In this case, in order to recover the complete data, reconstruction of fragments is required. Reconstruction of fragments of files that have been deleted from drive is called as carving. When attackers delete the RAR archive, it is important for investigator to reconstruct the file from fragments in unallocated space. This is done by following header signature of RAR files. Investigators use forensics tools to carve data to reconstruct file. (Mary Singh, 2013)

Importance of malware analysis

There are various phases associated while analyzing a malware affecting the systems. At first, it is important to find how an unknown process is related to external environment and how is it

controlled. It is essential to understand how the malware works i.e. which processes trigger the malware and what data is being lost or damaged in the system. Malware analysis may include different steps like intensive, systematic, behavioral and code analysis. Code obfuscation and encryption techniques may cause delay in analysis as they take longer time than usual.

Using these results of malware analysis an organization can work upon remediation and prevention techniques from the same malware. It can also be used to detect the similar malware in other systems. (Anuj Soni, 2014)

Live Response and memory forensics

Sometimes it is required to perform forensic examination of a live machine where static copy of system cannot be obtained. Live response is collection of information from a live machine to find out if the incident has been occurred. This includes collection of data pertaining to running processes, connection information, resources used by processes, files opened by processes, log files, metadata of files etc. There are multiple tools available for collecting data during live response such as Volatility, EnCase Enterprise, Mandiant Redline for Intelligent purpose, The Windows Forensics Toolchest Helix3 enterprise etc. (Cal Waits, Joseph Ayo Akinyele, Richanrd Nolan, Larry Rogers, 2008)

1. *Redline*

   Mandiant Redline is a free tool that collects information from systems for analysis. It analyses the data and creates search collectors and checks if other systems in network are also displaying similar symptoms. It can identify malware and distinguish if the system is compromised. Since it is very difficult for an attacker to change memory footprint,

Redline create memory indicators for identifying attacks by checking the difference in memory footprint. (Mandiant, 2014)

2. *Volatility*

   The volatility framework is collection of open tools, implemented in Python for memory forensics. According to the tool definition, "The extraction techniques are performed completely independent of the system being investigated but offer unprecedented visibility into the runtime state of the system. The framework is intended to introduce people to the techniques and complexities associated with extracting digital artifacts from volatile memory samples and provide a platform for further work into this exciting area of research."(Volatility, 2014)

3. *Maltego*

   Maltego is an open source intelligence and forensic software developed by Paterva. It is used as visualization application for observing social network, companies, infrastructure, document and files etc. Maltego provides relationship of various components and their respective correlation. (Paterva, 2014)

There are various tools for detection and response of APT attacks. It is important for any organization to keep resources ready and analyze patterns of attack from the beginning.

APT in action

1. *GhostNet (2009)*

   Cyber spying operation originating from People's Republic of China compromised Computer systems belonging to embassies, foreign ministries and other government offices, and the Dalai Lama's Tibetan exile centers in India, London and New York City.

2. *Operation Aurora (2010*)

   Google discovered Google along with at least twenty other large companies from a wide range of businesses--including the Internet, finance, technology, media and chemical sectors have been similarly targeted to gain access of Gmail accounts of Chinese human rights activists.

3. *RSA (2011)*

   Cryptographic seeds for RSA SecurID were stolen and used to launch attacks against numerous defense contractors, including Lockheed Martin.

4. *APT1 (2013)*

   Mandiant reported that APT1, a Chinese cyber threat actor, has systematically stolen hundreds of terabytes of data from at least 141 organizations.

Conclusion

All attacks cannot be prevented and it is certain that incidents are going to occur. Hence it becomes very important to align incident response program according to different threat vectors. Advance Persistent attacks involve some level of sophistication, organization and resources very

specific to a target. APT employs zero day exploits, advance malware kits but these attacks are advanced in terms of resourceful and programmatic approach as well. A good APT defense should be able to detect APT at any stage and stop it. Enterprises need to adopt defense in depth effectively which should span across the attack surface. Intelligence-driven computer network defense can be used to map adversaries and identifying patterns. Conventional network defense tools such as firewall, Intrusion Detection and Prevention system can address the known vulnerabilities but correlating information and sharing intelligence information can reduce the threat on larger extent.

New age incident response has evolved from coming at the last moment for just documentation. But nowadays if organizations are able to pull off a good incident response method, that in a can be a proactive since organization will be well-prepared for new age attacks. Hence it is important to understand that keeping incident response plan is not enough but an organization need to keep it effective and up to date in accordance with threat profile and risk vectors. Feedback and lessons learned will hold key in making the incident response plan effective. An incident response plan will be called effective when it provides means to recover the organization back to normal state efficiently in less time and ensures that attack does not happen again.

REFERENCES LIST

Adnan Baykal. *Incident Response in the age of APT*. http://doa.alaska.gov/ets/security/Strategic Planning/MS-ISAC_IncidentResponse.pdf (accesses Apr 17, 2014)

Anuj Soni. *The Importance of Command and Control Analysis for Incident Response*. 2014. http://digital-forensics.sans.org/blog/2014/03/31/the-importance-of-command-and-control-analysis-for-incident-response (accessed Apr 17,2014)

Art Ehuan, Michael Gibbons, Gant Redmon. *Incident Response In The Age Of Nation State Cyber Attacks.* 2013. http://www.slideshare.net/JTroisi/incident-response-in-the-age-of-nation-state-cyber-attacks (accessed Apr 17, 2014)

Cal Waits, Joseph Ayo Akinyele, Richanrd Nolan, Larry Rogers. *Computer Forensics: Results of Live Response Inquiry vs. Memory Image Analysis.* http://resources.sei.cmu.edu/asset_files/ TechnicalNote/2008_004_001_14948.pdf (accessed Apr 17, 2014)

Chris Crowley. *APT Incident Handling Checklist*. 2012. https://www.sans.org/score/checklists/ APT-IncidentHandling-Checklist.pdf (Accessed Apr 17, 2014)

Cisco. *Cisco 2014 Annual Security Report*. 2014. https://www.cisco.com/web/offer/gist_ty2_ asset /Cisco_2014_ASR.pdf (accessed Apr 17, 2014)

Dell SecureWorks. *Advanced Persistent Threats*. http://www.secureworks.com/cyber-threat-intelligence/advanced-persistent-threats/ (accessed Apr 17, 2014)

EMC. The Critical Incident Response Maturity Journey. 2013. http://www.emc.com/collateral/ white-papers/h12651-wp-critical-incident-response-maturity-journey.pdf (accessed Apr 17, 2014)

Eric Cole. *Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization.* Syngress, 2012.

Eric M. Hutchins, Michael J. Cloppert, Rohan M. Amin, Ph.D. Lockheed Martin Corporation. *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*. http://www.lockheedmartin.com/content/dam/lockheed/data/corporate /documents/LM-White-Paper-Intel-Driven-Defense.pdf (accessed Apr 17,2014)

Jason Steer. *The Need for Incident Response*. 2013. http://www.fireeye.com/blog/corporate/2013 /11/the-need-for-incident-response.html (accessed Apr 17, 2014)

Karen Kent, Suzzane Chevalier, Tim Grance, Hung Dang. *Guide to Integrating Forensic Techniques into Incident Response.* 2006. http://csrc.nist.gov/publications/nistpubs/800-86/SP8 00-86.pdf (accessed Apr 17, 2014)

Mandiant. *Accelerated Live Response*. 2014. https://www.mandiant.com/resources/download/ redline ()

Mandiant. *APT1 Exposing One of China's Cyber Espionage Units. 2013*. http://intelreport. mandiant.com/Mandiant_APT1_Report.pdf (accessed Apr 17, 2014)

Mandiant. M-Trends 2014: Beyond the Breach. 2014. http://connect.mandiant.com/m-trends_ 2014?source=web (accessed Apr 17, 2014)

Mary Singh. *Carving Station – RAR Files*. 2013. https://www.mandiant.com/blog/carving-station -rar-files/ (accesses Apr 17, 2014)

Nelson Bill, Amelia Phillips, and Christopher Steuart. *Guide to Computer Forensics and Investigations.* Cengage Learning, 2010.

Nigel Willson. *APT Response Strategy – Part 1*. 2014. http://nigesecurityguy.wordpress.com/2014/01/21/apt-response-strategy-part-1/ (accessed Apr 17, 2014)

Paterva. *Maltego*. 2014. https://www.paterva.com/web6/products/maltego.php (accessed Apr 17, 2014)

Protiviti. Incident Response – Securing Executive Support to address security breaches effectively. 2011. http://www.protiviti.com/en-US/Documents/POV/POV-Incident-Response-APTs-Protiviti.pdf (accessed Apr 17, 2014)

Verizon. The 2013 Breach Investigation Report. 2013. http://www.verizonenterprise.com/DBIR/2013/ (accessed Apr 17, 2014)

Volatility. *The Volatility Framework*. 2014. https://code.google.com/p/volatility/ (accessed Apr 17, 2014)