GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Hacker Tools, Techniques, and Incident Handling (Security 504)"
at http://www.giac.org/registration/gcih

Finding the Advanced Persistent Adversary

GIAC (GCIH) Gold Certification

Author: Fayyaz Rajpari, frajpari@gmail.com
Advisor: Richard Carbone

Accepted:
September 29, 2014

Abstract

The Advanced Persistent Threat is a commonly used term by security practitioners all over the world. Many believe these threats are in the form of hidden backdoors, stealthy credential stealers, and other crafty hacking tools. This is partially true, but it is a small component of the Advanced Persistent Threat. This generic term would be better described by the term, Advanced Persistent Adversary. It is the actor or groups behind these tools that are the real problem. Preventative security software will not stop the Advanced Persistent Adversary (APA). In this paper, we will explore the actions behind the APA and how they are continuously successful. The motivations behind these groups will be discussed, and how to find them with a mature incident response lifecycle. This is a real world approach to live response and forensics in any large organization.

© 2014 The SANS Institute Author retains full rights.

1. Introduction

The Advanced Persistent Threat was born long before the days of computers. However, the security industry has brought more emphasis to this "scare-word". Its first real use as the term APT came from the US Air force in 2006 due to the sole fact that nation state and government backed espionage turned to significantly more advanced attacks. The term was coined by the USAF to describe any well-funded, organized attack groups that have interest in data theft for various reasons. This includes, but not limited to economic growth, gathering intelligence, intellectual property, design plans, and/or personal information. Therefore, Advanced Persistent Adversary is a term that can be used to describe the above as it accurately depicts not only the threat, but the threat actors as well. Merriam Webster dictionary defines the term adversary as "one that contends with, opposes, or resists: enemy". By substituting the word "adversary" in place of "threat," one can better grasp the idea that it is the human behind the threat that is of importance. The Adversaries can be categorized into three motivational objectives: Political, Financial, and Economic (Bejtlich, 2010). The terms APA, advanced attack group, and threat actor group will be used interchangeably throughout this paper.

Live response and forensics is a key element used after the identification stage during the incident response (IR) lifecycle. Live response is an important aspect of IR for examining the impact of a breach. It is in this stage that the investigation starts and the true extent of the breach is uncovered. The next step is to contain compromised assets. During containment, a security team needs to understand the impact to the business. Leadership buy-in is crucial for this step; otherwise, it can severely hinder the operations to an organization. If the step is not enforced, an organization may suffer large financial loss due to nefarious APA activity leading to data exfiltration. Company reputation and brand damage may suffer as well if an organization continues without completing this necessary step during and/or after response. The use of forensic tools is critical when responding to advanced attacks so organizations can understand the human element of the attack. The resolution and recovery in IR are equally important. These steps allow an organization to monitor for the re-occurrence of adversarial activity, while validating they

© 2014 The SANS Institute Author retains full rights.

are out of the environment. Figure 1 is an example of the Incident Response workflow and forensics as part of the investigative process.

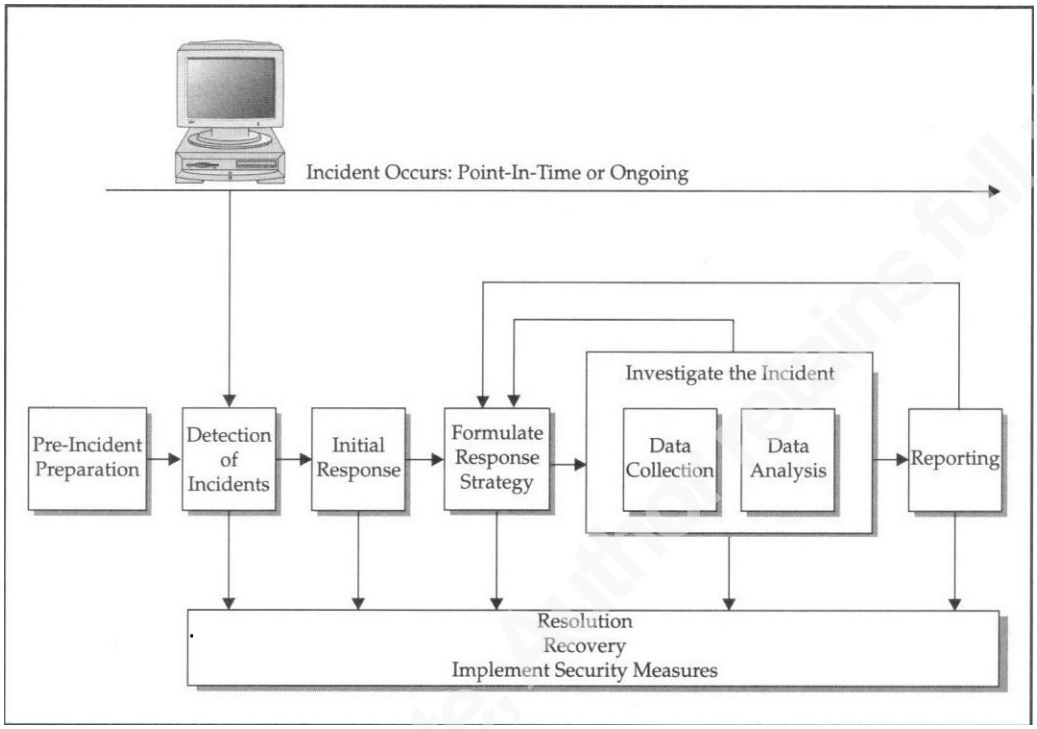


Figure 1 - Incident Response and Forensics Workflow (Prosise and Mandia 2003)

2. APA Motivation and TTP (Tools, Techniques, Procedures)

An organization's Computer Incident Response Team (CIRT) will be effective in the IR lifecycle by any intelligence they can obtain on the APA. Therefore, it is critical to understand these motivations by APA groups in the world. The primary threat actor groups that will be analyzed are Chinese and Middle Eastern. These examples are highlighted due to the distinct motivations each group had in recent years. Of course, this does not assume that these are the only APA groups. They are examples derived through research work published from various sources including KPMG, BBC, USA Today, CNN, Economist Intelligence Unit, Mandiant, Kaspersky, Symantec, and McAfee.

© 2014 The SANS Institute Author retains full rights.

2.1. China

The first major APA from China came out in 2009, dubbed "Operation Aurora" by McAfee. Initially it was reported the attack was towards Google, but later it was discovered that numerous businesses were attacked. Some of the major organizations attacked were Adobe, Juniper, Symantec, Northrop Grumman, and Morgan Stanley. The aim was to steal company secrets from emails and source code.

After a growing number of attacks were identified as originating from China, the U.S. government stated "China's economic espionage has reached an intolerable level and I believe that the United States and our allies in Europe and Asia have an obligation to confront Beijing and demand that they put a stop to this piracy" (Rogers, 2011). China later responded by stating, "It is unprofessional and groundless to accuse the Chinese military of launching cyber-attacks without any conclusive evidence" (Chinese Defense Ministry, 2013).

Working with the U.S. government, Mandiant released a 76 page public report discussing in great length, a specific military unit in China, PLA Unit 61398, and its attack activities. The activities in this report help bring some validity in the allegations made by the U.S. Government. The key findings of the APT1 Report by Mandiant were as follows:

1. Unit 61398 was considered to be a state secret by China and traced to four large networks in Shanghai;
2. The APT1 group has systematically stolen hundreds of terabytes of data from at least 141 organizations, while maintaining access for an average of 365 days to the victim networks;
3. APT1 controls thousands of systems in support of their computer intrusion activities;
4. The size of APT1's infrastructure implies a large organization with at least dozens, but potentially hundreds of human operators;
5. The industries APT1 targets match industries that China has identified as strategic to their growth, including four of the seven strategic emerging

© 2014 The SANS Institute Author retains full rights.

industries that China identified in its twelfth Five Year Plan (discussed in further detail in the following section).

One theory behind China's motivation for attacks against numerous industries is related to their five-year economic plans. In 1953, China adopted its first five-year plan. These plans establish a foundation and guiding principle for China's economic growth. Currently, China is on its twelfth five-year plan. The main goals are for a higher quality of growth, boosting GDP, and ensuring long-term prosperity to the nation. At this time, China's five-year plan focuses on the industries outlined below in Figure 2 and therefore these industries have a higher likelihood of being targeted by Chinese APA groups.



China's 12th Five-Year Plan: Seven Priority Industries

1. **New energy**
   - Nuclear, wind and solar power
2. **Energy conservation and environmental protection**
   - Energy reduction targets
3. **Biotechnology**
   - Drugs and medical devices
4. **New materials**
   - Rare earths and high-end semiconductors
5. **New IT**
   - Broadband networks, internet security infrastructure, network convergence
6. **High-end equipment manufacturing**
   - Aerospace and telecom equipment
7. **Clean energy vehicles**

© 2011 KPMG Advisory (China) Limited, a wholly foreign owned enterprise in China and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. Printed in China.

Figure 2 - China's 12th Five Year Plan: Seven Priorities (KPMG, 2011)

A representation of China's growth is depicted in the graph below comparing the eleventh and the current twelfth 5-year plan. Their growth is targeted to remain at approximately 7%, but as seen in Figure 3, it is consistently higher than the target growth year over year.

© 2014 The SANS Institute Author retains full rights.

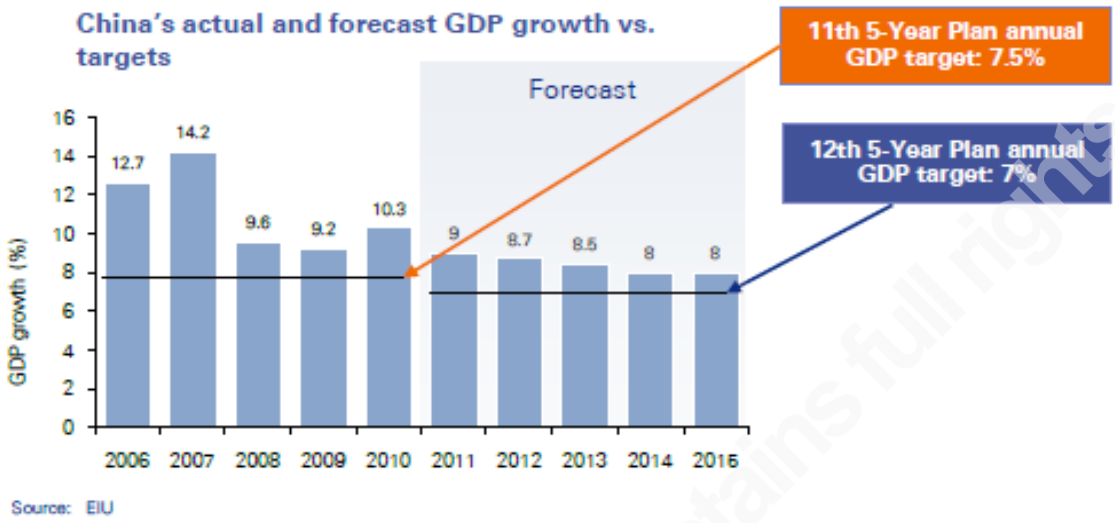


Figure 3 - China's Actual and Forecast GDP growth vs. Target growth (KPMG, 2011)

Further, the International Monetary Fund forecasts China's economic growth in 2014 at 7.5%, nearly triple the 2.8% growth forecast for the United States (McDonald, 2014). The same study depicts China as the leader when compared against other countries as seen in Figure 4 below.

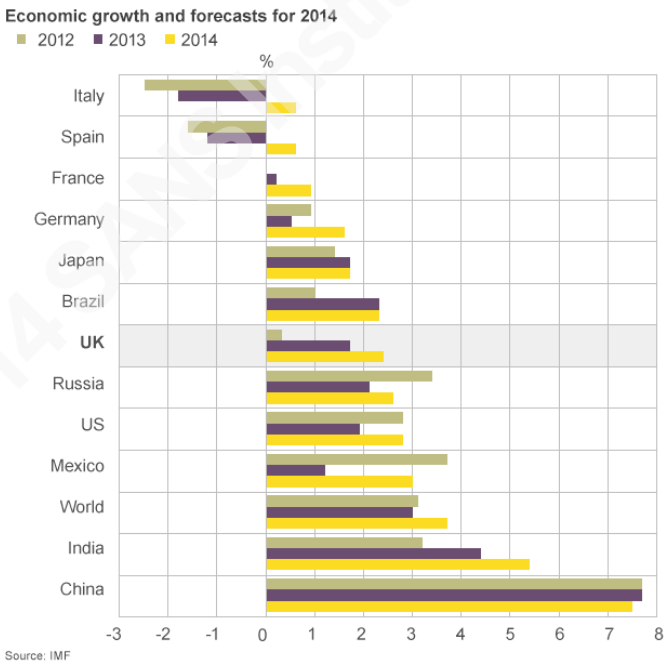


Figure 4 - Economic growth and forecasts for 2014 (International Monetary Fund, 2014)

Fayyaz Rajpari, frajpari@gmail.com

© 2014 The SANS Institute Author retains full rights.

The research and development of China's seven priorities and to create such growth is a costly venture. It is also resource intensive and can take several years to develop. This would require hiring skilled resources to conduct lengthy research and development of these initiatives. However, nation sponsored APA groups can be hired at a fraction of the cost and therein lies the motivation behind China's attacks against various industries throughout the globe.

Reconnaissance and infiltration can be achieved through tactics like strategic web compromise and spearfishing attacks. As stated in Mandiant's report, "this translates into data theft that goes far beyond the core intellectual property of a company, to include information about how these businesses work and how executives and key figures make decisions" (Mandiant M-Trends, 2014).

2.1.1 Tools used by APT1

The APT1 Appendix by Mandiant highlights the Chinese APA as using an arsenal of malware families. An array of custom backdoors is used by this threat group. A Remote Access Trojan known to be in existence for over 8 years was one of the tools used by APT1 to control victim computers. Even though this is very well known, it continues to be a successful tool used by APA groups. Figure 6 shown is an image of the Poison Ivy functionality. Each item on the left is a clickable action that can be executed on the victim system.

© 2014 The SANS Institute Author retains full rights.

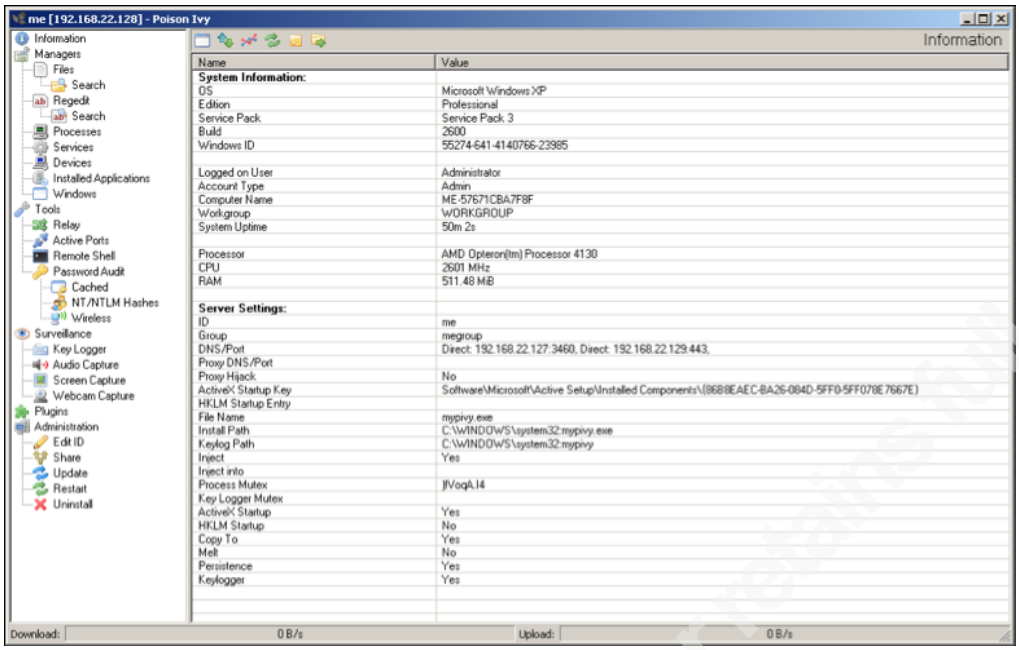


Figure 6 – Poison Ivy Remote Access Trojan

Symantec and McAfee have released reports on the same APA group with different names. APT1 is known by Symantec as Comment Crew and by McAfee as Operation Shady RAT. Both reports can give additional insight into the group's tools, techniques, and procedures.

2.2 Middle East

Increased activity out of this region has made this APA group a growing threat and a target. The complex computer worm, Stuxnet, targeted Iran's nuclear program and reportedly disrupted almost 20% of Iran's centrifuges in the Natanz nuclear enrichment facility. There is speculation that this APA was United States and Israeli government sponsored activity. Moreover, due to this activity, other Middle Eastern APA groups were identified in mainstream media. The Syrian Electronic Army is a prime example of Middle Eastern APA with non-financial related motivations.

Middle Eastern APA groups have numerous levels of cyber operations in command. Their main goals are to confront enemies and critics of the Islamic regime. Their motivations are political with religious influence, while tendencies appear to be espionage related activities against western countries.

Fayyaz Rajpari, frajpari@gmail.com

© 2014 The SANS Institute Author retains full rights.

According to the BBC Persian, Iran's Cyber Warfare Structure is as follows:

1. High Council of Cyberspace – High-level policy creation consisting of the president and heads of various government entities such as the parliament, the police, ministers of intelligence, etc.
2. Cyber Defense Command – Created in response to Stuxnet. Consists of armed forces and government ministries. Their main goal is defend against probable wars for damage control against the country's infrastructure.
3. Cyber Army – Iran's elite hacker group with possible connections to Iran's military force, but no official registration to the Iranian government. They have known to hack into foreign media outlets including Twitter and other government sites in western countries. This can be considered advanced attack group due to the offensive skillset.
4. Basij Paramilitary Force – Members of the IRGC (Islamic Revolution Guards Corps.). This force is responsible for cyber warfare with groups against the Iranian regime.
5. FETA Police – Specialized group formed under the Iranian Police in 2009 to confront internet crimes like fraud, information theft, and other internet threats. Main activity of this group has grown to battling internet crimes with hired hackers for vulnerability research against government sites so they can be remediated.
6. Syrian Electronic Army – Strong supporter and ally of Iran. Several incidents from this group attacking western media outlets have been reported including, but not limited to Reuters, NPR, The Guardian, The Onion, and Harvard University.

The above structure illustrates Iran's tenacity of having an organized cyber task force that aligns with their motivations. Below are key findings in the M-Trends 2014 Report on Iranian threat actors:

1. Use of the same DDOS tool used in 2012 attacks on US Banking institutions;
2. Use of English command web shells translated into Farsi;
3. ¼ of systems infected with malware;

Fayyaz Rajpari, frajpari@gmail.com

© 2014 The SANS Institute Author retains full rights.

4. 150 gigabytes of data consisting network diagrams, user accounts and passwords exfiltrated;
5. Creation of exploits used in intrusion activities identified as coming from Tehran.

Even with the above data points, it is important to note that Mandiant observed this APA group to be have a weaker skillset than other groups. However, due to Stuxnet and the historical tension between Iran and Western countries over the nuclear program, they should be regarded as highly capable.

In recent news, the Syrian Electronic Army (SEA) has been very active. This is a prominent APA in the Middle East supporting the President of Syria, Bashar Al-Assad. Al-Assad's main goal is to reform and defend Syria against Israeli occupation. The SEA and its supporters feel that the western media and their support of Israel are detractors of Bashar Al-Assad, resulting in continuous reported attacks in 2014. Figure 7 below shows tools, techniques, and procedures of the SEA in a 3 day attack timeline on a western news agency.

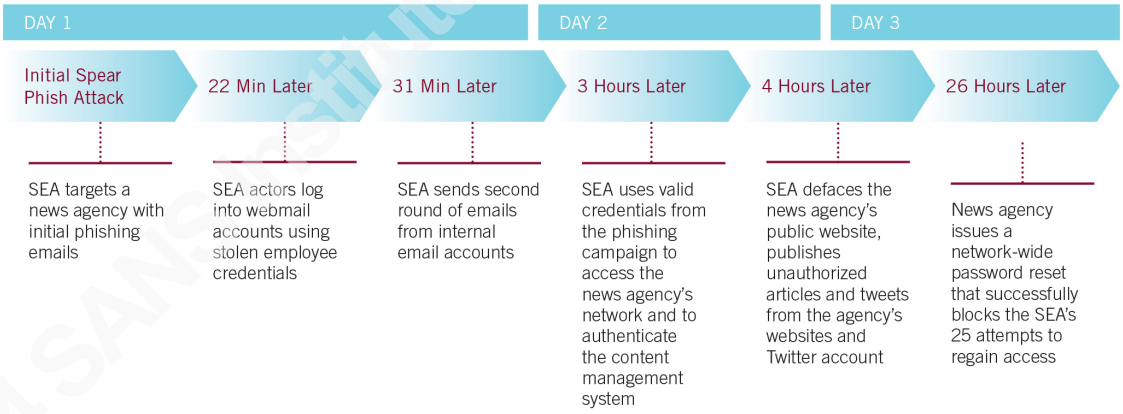


Figure 7 - Tools, Techniques, and Procedures of the SEA during 3 day attack timeline (Mandiant M-Trends, 2014)

2.2.1 Tools used by the Syrian Electronic Army

Common tools used by the SEA include:

1. DarkComet RAT – Trojan horse steals credentials, captures webcam footage, and log key strokes. Consists of a client/server architecture commonly

© 2014 The SANS Institute Author retains full rights.

deployed on Windows 7 operating systems. All of its functionality is referenced in Figure 8.

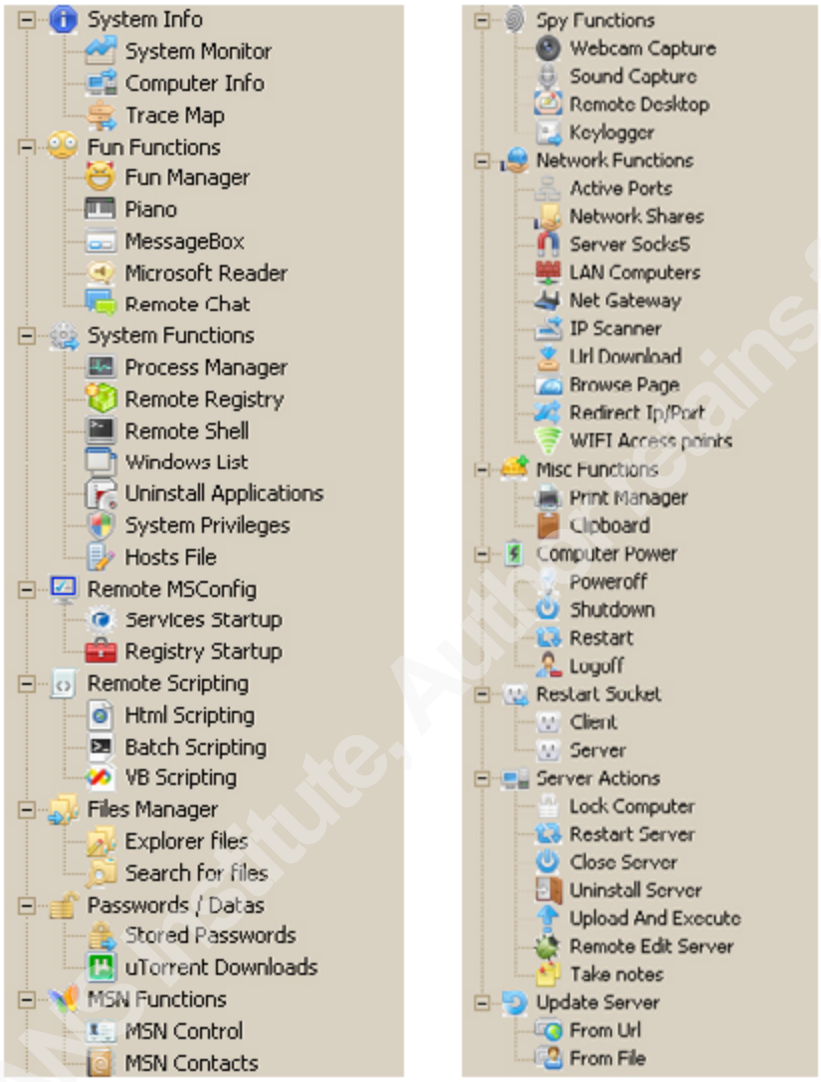


Figure 8 – DarkComet Remote Access Trojan Control Panel and Functionality (Kaspersky Lab, 2014)

2. Xtreme RAT – Trojan horse logs the victims' screenshots and key strokes. Figure 9 shows the tool being used along with attack delivered through a Word document format and a campaign code of "IDF" for tracking purposes of the target victims (Villeneuve and Bennett, 2014).

© 2014 The SANS Institute Author retains full rights.

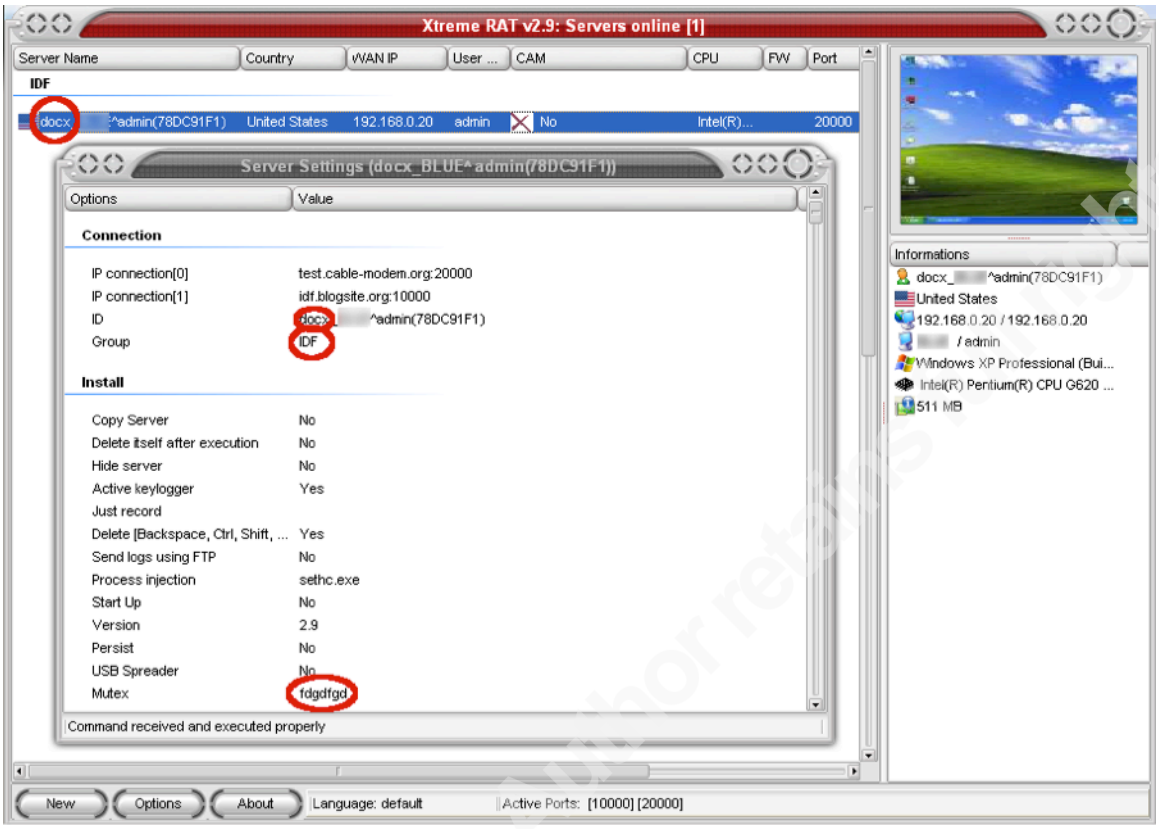


Figure 9 – XtremeRat with weaponized Word document (FireEye, 2014)

Further details by Kaspersky shows activity of Remote Access Trojans, including Xtreme RAT used in Middle Eastern countries (Figure 10).

© 2014 The SANS Institute Author retains full rights.

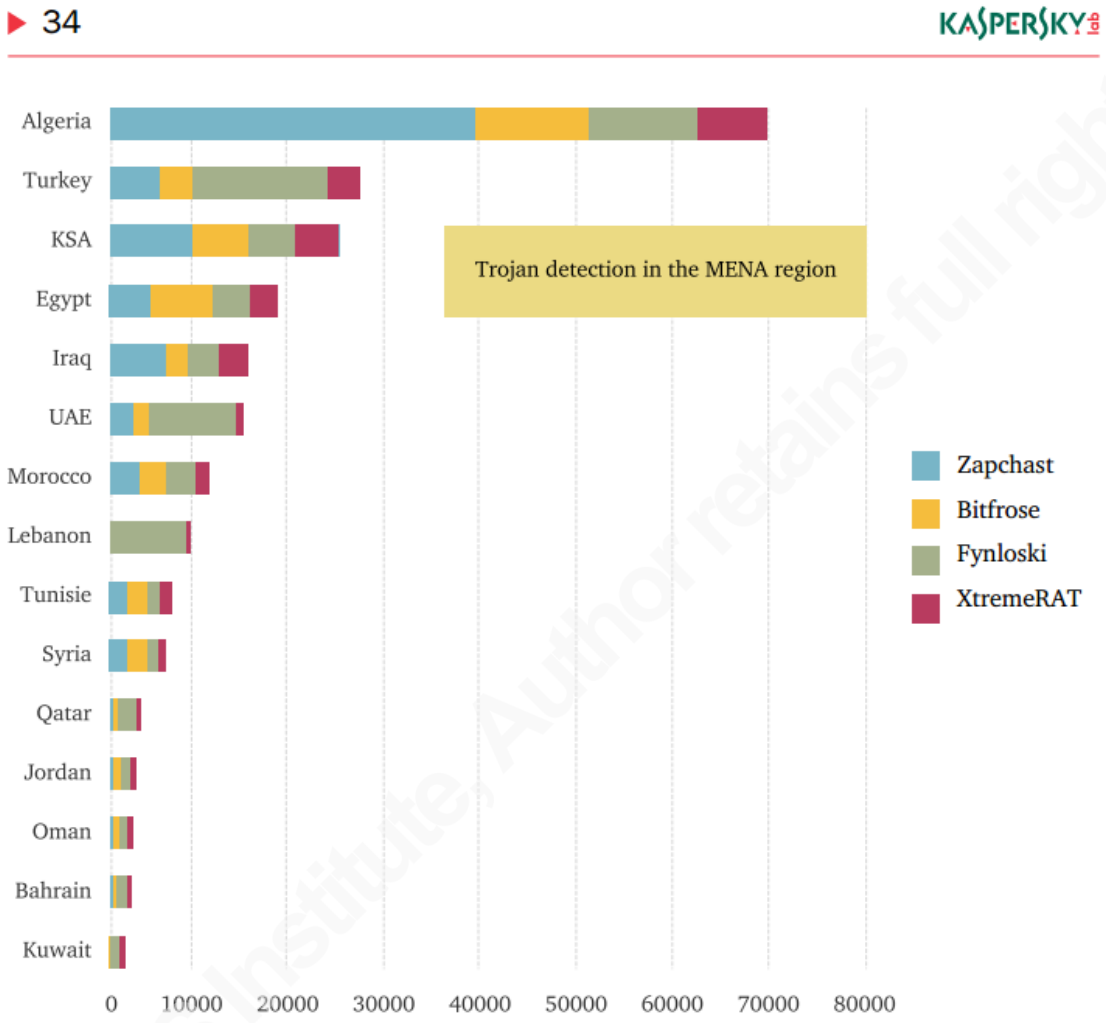


Figure 10 - Trojan detection in the Middle Eastern Region (Kaspersky Lab, 2014)

Based on the this research and data provided from the 2014 Mandiant M-Trends report, below are some observations on tools, techniques and procedures (TTP) in the Middle East.

1. They utilize a set of publicly available tools, with only a few being custom.
2. They utilize the same infrastructure for a year or longer, including IP and Domain information. This behavior degrades their success.
3. Minimal obfuscation techniques have been used.
4. APA has used common tools to exploit known web based vulnerabilities on public facing sites.

Fayyaz Rajpari, frajpari@gmail.com

© 2014 The SANS Institute Author retains full rights.

2.3 TTP Summary

Tools, techniques, and procedures can be further described through an attack lifecycle diagram, as represented in Figure 11. Web, email, and/or external storage devices combined with social engineering are common techniques during the "Initial Compromise" stage. They can also be referred to as an attack vector. During this stage, a payload is delivered through a weaponized file format that exploits the vulnerability, ultimately to "establish afoothold." Immediately after software is installed, it may run as the user, preferably as a system account that has escalated privileges. If the APA does not have the necessary privileges, full privileges to the system must be gained to move deeper within the network. These privileges are escalated through other vulnerabilities in the underlying software. Further instructions can be delivered by command and control (C2) activity performed by the malicious actor in a remote location. Additional binaries can be dropped by the attacker to evade traditional security measure and to "maintain a presence." The use of common Microsoft Windows administration tools can be used to move throughout the network for additional reconnaissance. This can be classified as a procedure the adversary must go through to understand where the data resides. Throughout the lifecycle, there is a variety of tools used as highlighted in gray below. The tools are used up to the point of data exfiltration and finally to "complete the mission."

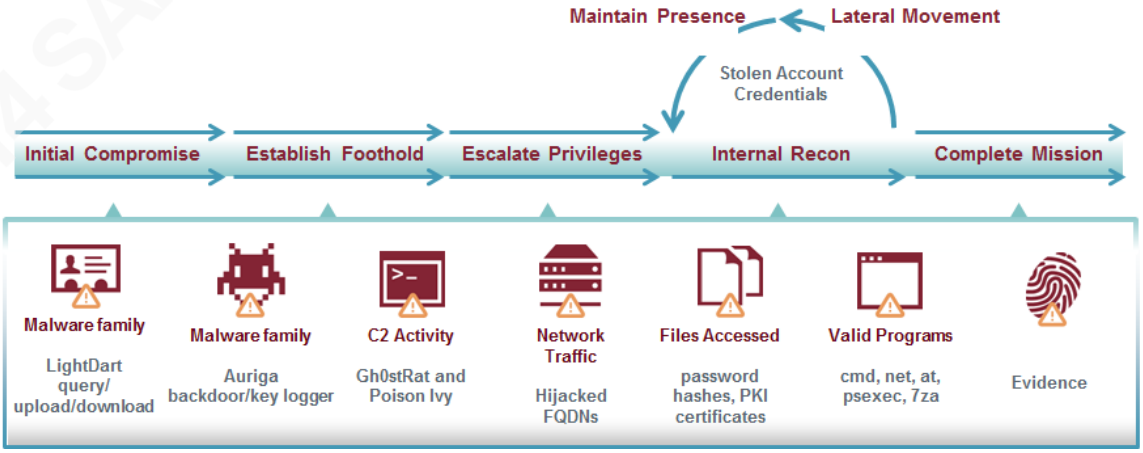


Figure 11 - Attack Lifecycle (Mandiant)

© 2014 The SANS Institute Author retains full rights.

3. Security Monitoring Techniques

Security monitoring can give a great depth of visibility to the attack lifecycle in any organizations' CIRT. These techniques will help the CIRT understand how far an attacker has made it within the organization during a breach. For example, is the adversary only at the first stage or are they past the initial stages of compromise and approaching the end of their mission to exfiltrate data?

Two main approaches to security monitoring can be classified as Continuous Monitoring and Network Security Monitoring. Security monitoring techniques are essential in an incident response program. It is important to apply both techniques from the early phases of preparation and through the detection and analysis. Continuous Monitoring is a vulnerability centric approach focused on assets, configuration weaknesses, and vulnerabilities. Network Security Monitoring is a threat centric approach. It is focused on adversarial activity with alignment towards finding the APA (Bejtlich, 2013, p. 9)

3.1 Continuous monitoring

The CAESARS Framework Extension, created by National Institute of Standards and Technology (NIST) and the efforts comprised of members from the National Security Agency (NSA), Department of Homeland Security (DHS), and National Institute of Standards (NIST) is a defensive monitoring approach, termed "Continuous Monitoring." The system configurations are checked on a more frequent basis than it would be traditionally, thus the term "Continuous." Determination against these systems as non-standard and to check against controls for compliance defines "Monitoring."

The resulting goal of this framework is provide organizations an early warning system on situational awareness through security monitoring and analysis of data through a variety of security tools.

Continuous Monitoring External Data Domains as categorized by NIST Interagency Report 7756:

1. Vulnerability Management;
2. Patch Management;
3. Event Management;

© 2014 The SANS Institute Author retains full rights.

4. Incident Management;
5. Malware Detection;
6. Asset Management;
7. Configuration Management;
8. Network Management;
9. License Management;
10. Information Management;
11. Software Assurance.

In a mature organization, each domain above will be monitored and maintained. If this can be achieved successfully, the organization's risk level of having adversary activity can drop. Furthermore, the above categories can be applied through the use of the Security Content and Automation Protocol (SCAP) revision 2 that is referenced in the NIST Interagency Report 7800 as below.

1. Asset Reporting Format (ARF) – format for assets;
2. Common Configuration Enumeration (CCE) – unique identifiers to configuration;
3. Common Vulnerability Enumeration (CVE) – unique identifiers to known vulnerabilities;
4. Common Platform Enumeration (CPE) – description and identifiers to classes of applications, operating systems, and hardware devices;
5. Extensible Checklist Configuration Description Format (XCCDF) – Language for configuration and system state;
6. Open Vulnerability and Assessment Language (OVAL) – Language used for determination of vulnerabilities existing on a system.

3.2 Network Security Monitoring

Most traditional security mechanisms have a common goal of blocking, filtering, or denying. The Network Security Monitoring (NSM) approach does none of the above. The one goal of NSM is to provide maximum visibility to a network. Although there are numerous security controls that block, filter, and deny threats, the need for full visibility

© 2014 The SANS Institute Author retains full rights.

still necessary. There is no security solution or combination of solutions that is bulletproof and can stop every malicious threat and more importantly the actors behind it. Therefore, when security mechanisms fail to stop the APA, NSM can greatly increase visibility of these security controls and the attack lifecycle flow. The implementation of NSM will give an enterprise the ability to accomplish key steps in an IR workflow. The APA will eventually fail if the organization's CIRT can interrupt the attack flow and/or have the common goal of stopping data exfiltration.

The amount of data provided by NSM can be overwhelming. There are numerous ways to monitor for analysis. In depth deployment strategies, along with rich examples of its use can be further explored in Richard Bejtlich's book, The Practice of Network Security Monitoring. Below are a list of NSM data types and tools to use for capture and analysis of the data. Most tools outlined are included in the open source Ubuntu distribution, Security Onion:

- *Full content data* - Copy of all network data on the wire (Network Sniffer, Wireshark);
- *Extracted content data* - Data streams including files, images, and media from source to destination. No network level detail like MAC addresses or IP addresses (Wireshark, Xplico);
- *Session Data* – Network activity details of who, when, how, and amount of data transferred (Sguil, Argus);
- Transaction Data – Additional detail in regards to session data, exchanged between two devices (Bro http.log);
- *Statistical Data* – Information about a network capture, file size, network data size, capture duration, etc. (Capinfos);
- *Metadata* - Ownership of data, domain name information, routing data, etc. (whois.net);
- *Alert Data – Messages* reported through automated traffic analysis based on patterns, counts and signatures (Snort, Suricata).

One approach to using NSM and finding APA can be categorized into the necessary data collection along the "Intrusion Kill Chain" referenced in a paper written

© 2014 The SANS Institute Author retains full rights.

by Lockheed Martin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains" (Table 1). The authors further classify indicators into three types: Atomic, Computed and Behavioral. Examples of each are IP and email addresses, hashes, and a combination of both respectively. Table 1 depicts the stages of the Kill Chain with detection and correlation to monitoring for each phase.

© 2014 SANS Institute, Author retains full rights.

© 2014 The SANS Institute Author retains full rights.

Table 1- The Intrusion Kill Chain vs Detection Mechanism

Phase	Detect (NSM and Endpoint)
Reconnaissance	Transaction Data
Weaponization	Extracted Content
Delivery	Session Data, Endpoint monitoring
Exploitation	Endpoint monitoring
Installation	Endpoint monitoring
C2	Transaction Data
Actions and Objectives	Endpoint monitoring

4. Live Response with Forensics

Security monitoring is an ongoing process that will ultimately lead to data that may conclude findings of compromised assets. Live response is the act of responding to these compromised assets and understanding the questions pertaining to "what happened, how, and where?" When it comes to live response, the two key aspects in an enterprise incident response program is the time until remediation and to understand the full impact of the breach.

Traditional cyber forensics can be used to understand the impact; however, it is a time consuming task, with several hours spent in collection of memory and full disk images. Afterwards, the analysis stage can take just as long or longer. Thus, in traditional IR programs, many times forensics is overlooked and only used when required for litigation matters. However, this approach can leave out key elements and details in a compromise, ultimately keeping organizations in a breached state with a false sense of security. Ultimately, live response with forensics can reduce the overall time spent in IR, while expanding the visibility to APA activity. The approach is to collect only relevant data rather than gathering a full memory or disk images. Windows native command line tools and others like WMIC and SysInternals' PsExec are instrumental to finding pertinent details when IR is invoked. Free tools like Redline are also available for download and use in single machine incidents. In enterprise environments it is most sensible to use automation with scripts when dealing with APA and understanding the full compromise of a network. Enterprise grade tools like Mandiant for Intelligent

© 2014 The SANS Institute Author retains full rights.

Response can query thousands of systems at once for forensic artifacts reducing overall response time.

To find APA, the security team must go beyond traditional detection mechanisms to look for hostile activity. Similar to how data collection is done through scripts and tools, the adversary will also prefer to use scripts, tools, and native command line execution to evade detection from traditional security. The wiki below provides a comprehensive list of typically used Windows commands. As these commands are executed, forensic artifacts can be searched upon and used in hunting for the adversary through Windows queries or custom Indicators of Compromise (IOCs). It is important to understand TTP used by the threat actor group so an appropriate and a relevant hunting strategy can be used during incident response.

Windows commands commonly used by APA typically include the following (skullsecurity.org):

net use \\<target> “” /u:”” – establish a null session
net user – listing users
dir /s - full directory listing
sc query – list running services
nslookup – look up dns records
at – run or view scheduled tasks
reg query – query a key
reg add - add a key
netstat –an | find <port> - find port #
ipconfig /displaydns or /flushdns – display or flush dns

How is this applied in the real world? Let us look at the registry as an example. The Windows registry is very dynamic and forensic artifacts can be gleaned from it. If an adversary wants to compromise a network, they will not stand still on one system. A common tactic is to move laterally within the organization and hop from one point to another for various purposes including reconnaissance, infiltration, and data exfiltration. The below query is used to get information on what other systems an endpoint may have mapped sessions to. This can give more insight to the security team as to what possible

© 2014 The SANS Institute Author retains full rights.

hop points the adversary may have used. If the adversary is using malware with worm-like attributes, the infection vector can spread in seconds to minutes throughout an enterprise when network shares are enumerated. This is called lateral spread. If it gets worse if this then an advanced attacker is in your network. The APA's main goal is to go undetected, so a common tactic is not to use malware once inside the network. A commercial Antivirus (AV) scanner may end up detecting the lateral spread of some of files deemed as malicious on the drives. What's more important is investigating the types of files that AV did not detect.

Figure 12 shows a simple registry query done by the adversary to show mount points on the endpoint:

```
C:\Users\frajpari>reg query hkcu\software\microsoft\windows\CurrentVersion\Explorer\mountpoints2

HKEY_CURRENT_USER\software\microsoft\windows\CurrentVersion\Explorer\mountpoints2\##192.168.1.210#backup
HKEY_CURRENT_USER\software\microsoft\windows\CurrentVersion\Explorer\mountpoints2\##192.168.1.210#mp3s
HKEY_CURRENT_USER\software\microsoft\windows\CurrentVersion\Explorer\mountpoints2\##192.168.1.210#pictures
HKEY_CURRENT_USER\software\microsoft\windows\CurrentVersion\Explorer\mountpoints2\##192.168.1.210#Share
HKEY_CURRENT_USER\software\microsoft\windows\CurrentVersion\Explorer\mountpoints2\##192.168.1.210#upnpav
```

Figure 12 – Registry query command for mountpoints

When the attacker is moving through these shares and using Windows commands like "net use" or copy to stage his own utilities or creating innocuous folders and files, it is called lateral movement. A copy process of attacker tools dumped to a legitimate network share is shown below:

```
C:\Users\frajpari>net use \\192.168.1.210
The command completed successfully.

E:\>copy "\Attack Tools"\*.* \\192.168.1.210\backup\software /Y
\Attack Tools\7za.exe
\Attack Tools\BasicInfo.exe
\Attack Tools\fciv.exe
\Attack Tools\lads.exe
\Attack Tools\PI2.3.2.rar
\Attack Tools\PsExec.exe
\Attack Tools\rcat.exe
        7 file(s) copied.
```

Figure 13 – Lateral movement with Windows commands

The above-copied executables are not likely to be detected by most antivirus solutions, as many are native Windows tools while others are others legitimate tools used in Windows administration. Rcat, a variant of netcat, is a common backdoor utility that can open and listen for any ports on the victim system. It can be further used to pass through commands such as a Windows command shell! Thus, this can be classified as a

© 2014 The SANS Institute Author retains full rights.

Trojan that goes undetected by numerous antivirus solutions because of its obfuscation. PI2.3.2 is commonly used amongst APA, known as Poison Ivy Remote Access Trojan. The tool has many nefarious functions such as screen capture, key stroke logging, and listing all services just to name a few. Notice this is in RAR format; it is also encrypted to evade antivirus detection.

Registry queries can be useful to give the computer incident response team (CIRT) information on remote shares and mount points that are in use so that attention can be focused there if necessary. To make this operation quicker, the use of IOCs can alert the CIRT only when the IOC is triggered.

An example IOC looking for specific network files is shown in the following figure:

© 2014 The SANS Institute Author retains full rights.

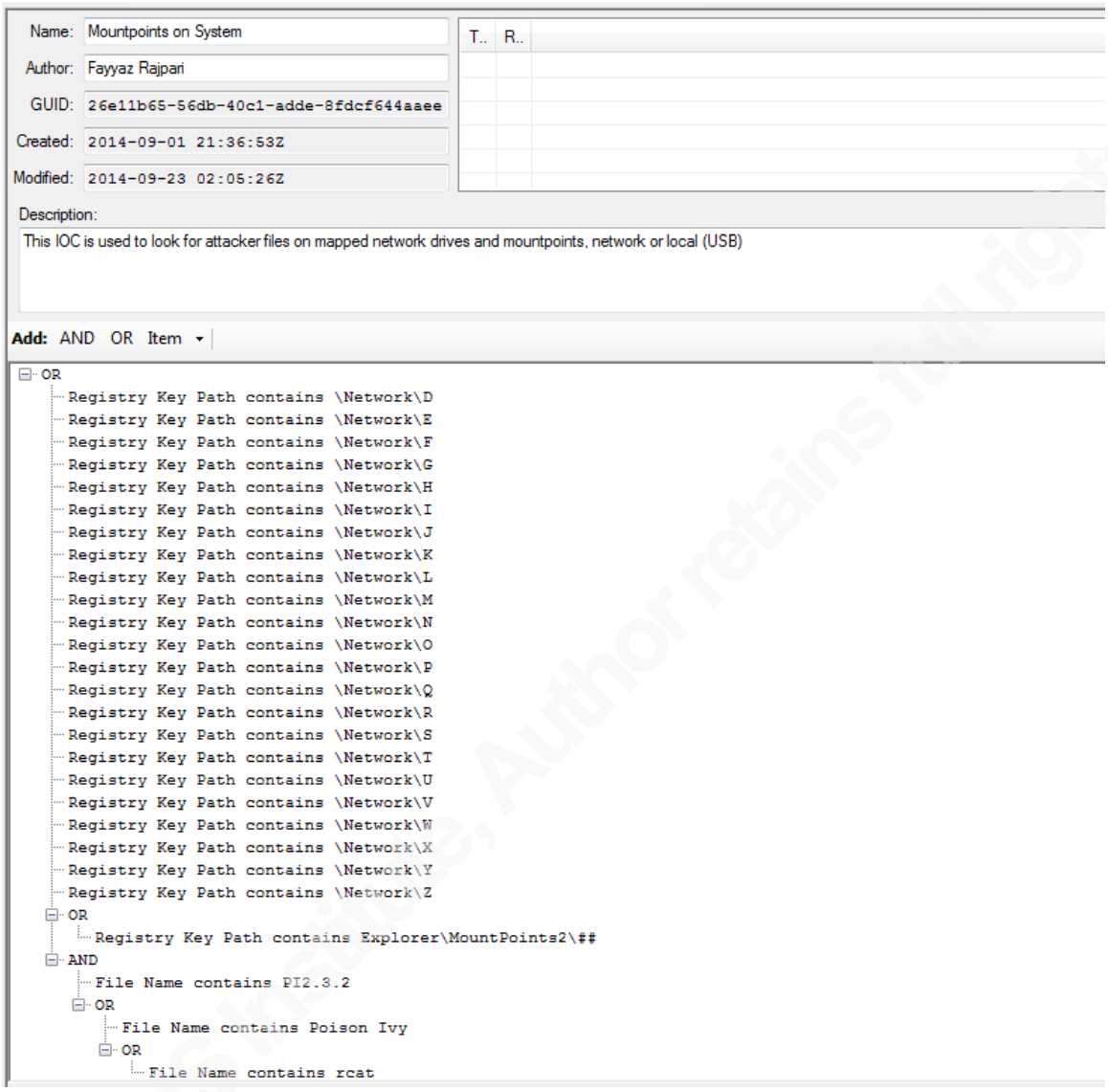


Figure 14 – Indicator of Compromise with network drives and file names

As additional items are found on systems, the CIRT can quickly uncover Adversary TTPs. For example, this attacker likes to use PsExec and Rcat as tools to move laterally within the organization. Another IOC can be written to look for file attributes including MD5 hash, size, name, and owner details. These IOCs should be used across the enterprise to sweep hosts for evidence of further compromise. The cycle described and detailed above can be repeated numerous times until all suspect assets have been identified and scoped. Figure 15 depicts the investigative lifecycle used by a CIRT.

Fayyaz Rajpari, frajpari@gmail.com

© 2014 The SANS Institute Author retains full rights.

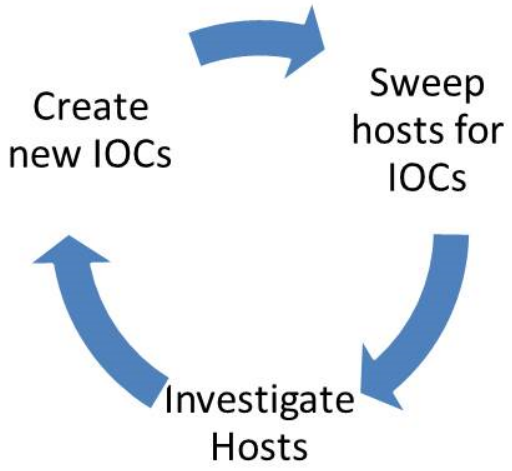


Figure 15 - Investigative lifecycle with Indicators of Compromise

5. Conclusion

Finding the Advanced Persistent Adversary is a growing concern among organizations and nations alike. It requires not only skill, but also a mature incident response program to find the human element of the attack. APA groups all have different motivations and intent for compromising organizations. Each organization must take a strategic and knowledgeable approach when hunting for the APA. Uncovering the full scope of a breach in the least amount of time is essential when doing live response with forensics. The good news is that it can be achieved through a combination of applying intelligence of the APA's tools, techniques, and procedures in the IR lifecycle along with sound hunting strategies with security monitoring. Organizations will fall behind if they rely on the traditional security mechanisms as the main approach for detection and response. A proactive method must be enforced to hunt for the Advance Persistent Adversary.

Fayyaz Rajpari, frajpari@gmail.com

© 2014 The SANS Institute Author retains full rights.

6. References

Alperovitch, D. (1 August 2011). Revealed: Operation Shady RAT. Retrieved September 2, 2014, from www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf

APT1: Additional Comment Crew Indicators of Compromise. (25 February 2013). Retrieved September 2, 2014, from http://www.symantec.com/connect/blogs/apt1-additional-comment-crew-indicators-compromise

APT1: Exposing One of China's Cyber Espionage Units." Mandiant. (18 February 2013). Retrieved September 1, 2014 from http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

BBC Persian. Structure of Iran's Warfare. Retrieved September 1, 2014, from http://nligf.nl/upload/pdf/Structure_of_Irans_Cyber_Operations.pdf

Bejtlich, R. (16 January 2010). TaoSecurity*: What Is APT and What Does It Want?* Retrieved May 13, 2014, from http://taosecurity.blogspot.com/2010/01/what-is-apt-and-what-does-it-want.html

Bejtlich, R. (2013). *The Practice of Network Security Monitoring Understanding Incident Detection and Response.* San Francisco: No Starch Press.

Brown, E. (14 January 2012). NIST Publishes Draft Implementation Guidance for Continuously Monitoring an Organization's IT System Security. Retrieved August 24, 2014, from http://www.nist.gov/itl/csd/monitoring-012412.cfm

China's 12th Five Year Plan: Overview. (5 March 2011). Retrieved September 11, 2014, from http://www.kpmg.com/CN/en/IssuesAndInsights/ArticlesPublications/Publicationseries/5-years-plan/Documents/China-12th-Five-Year-Plan-Overview-201104.pdf

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer Security Incident Handling Guide. *National Institute of Standards and Technology, 800-61*(2).

FireEye Special Report: Assessing Damage and Extracting Intelligence (2014) http://www.fireeye.com/resources/pdfs/fireeye-poison-ivy-report.pdf

Kaspersky Lab, Global Research and Analysis Team. (1 August 2014). Syrian Malware, the ever-evolving threat. Retrieved September 1, 2014, from https://securelist.com/files/2014/08/KL_report_syrian_malware.pdf

McDonald, J. (30 April 2014). Report: China to overtake U.S. economy this year. Retrieved September 1, 2014, from

Fayyaz Rajpari, frajpari@gmail.com

© 2014 The SANS Institute Author retains full rights.

http://www.usatoday.com/story/money/business/2014/04/30/china-us-top-economy/8538689/

M-Trends Threat Report: Attack the Security Gap. (April 2013). Retrieved September 1, 2014 from https://www.mandiant.com/resources/mandiant-reports/#

M-Trends Threat Report: Beyond the Breach Mandiant. (April 2014). Retrieved September 1, 2014 from https://www.mandiant.com/resources/mandiant-reports/#

Prosise, C., & Mandia, K. (2003). *Incident response & computer forensics* (2nd ed.). New York: McGraw-Hill/Osborne.

Rogers, M. (U.S. Rep) (4 October 2011). Economic Espionage. *Court Hearing*. Lecture conducted from Chairman of House Permanent Select Committee.

Sanger, D. (31 May 2012). Obama Order Sped Up Wave of Cyberattacks Against Iran. Retrieved August 26, 2014, from http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=4&

Schwartz, M. (21 May 2013). Google Aurora Hack Was Chinese Counterespionage Operation. Retrieved September 28, 2014.

Villeneuve, N., & Bennett, J. (19 February 2014). XtremeRAT: Nuisance or Threat? Retrieved August 26, 2014, from http://www.fireeye.com/blog/technical/2014/02/xtremerat-nuisance-or-threat.html

Windows Commands. (11 January 2011). Retrieved September 16, 2014, from https://wiki.skullsecurity.org/Windows_Commands

Yan, H., Ahmed, A., & Jamjoom, M. (7 January 2013). Al-Assad touts plan for resolution, says enemies of Syria 'will go to hell' Retrieved August 31, 2014, from http://www.cnn.com/2013/01/06/world/meast/syria-civil-war

Zetter, K. (10 January 2011). Google Hackers Targeted Source Code of More Than 30 Companies | WIRED. Retrieved September 27, 2014.

© 2014 The SANS Institute Author retains full rights.