BLUE TEAM REPORT FOR THE APT 1:

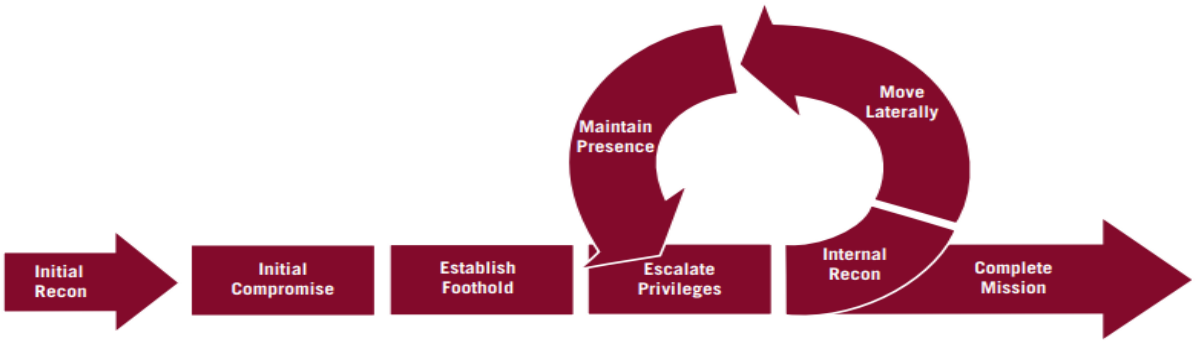
In a report revealing APT1's multi-year computer espionage effort, the Mandiant Intelligence Center made some previously unreleased information public.

The strategic monitors track hundreds of threat groups around the globe, including APT1. Regarding the quantity of information stolen, this should be regarded as one of the most precise estimates.

1. **How does this report better prepare you as a blue teamer?**

Using specific commands, the APT1 breaches organizations, then makes use of this data to run network operations. The APT1 has a well-established attack approach that it has evolved over time to steal enormous amounts of data and intellectual property. Starting with spearfishing, this is followed by the use of specialized digital weapons. They utilize this to deliver enormous amounts of compressed data in bundles to China. Then they begin the entire procedure over again. Due to their widespread distribution across the system and capacity to carry out these acts in the environment, they have shown to be successful in entrepreneurial settings.

The APT1 has a well-established attack approach that has evolved over time to steal enormous amounts of data and intellectual property. Starting with spearfishing, this is followed by the use of specialized digital weapons. They utilize this to deliver enormous amounts of compressed data in bundles to China. Then they begin the entire procedure over again. Due to their widespread distribution across the system and capacity to carry out these acts in the environment, they have shown to be successful in entrepreneurial settings.



As a blue team specialist, we are unable to locate the point of entry, which can be a phishing email or an external service. This is due to insufficient log information and the attacker's ability to hide their traces.

By looking at the lifecycle of the attacker, most of the security measures can be taken to avoid the possibility of a hack or compromise of the network/system. The operations performed by the APT1 are -

- **Account Discovery : local host** - To locate accounts on the system, APT1 utilized the commands net localgroup, net user, and net group.

  Mitigation : This can be done through the process of Operating System Configuration. Avoid listing administrator accounts when an application is elevated through UAC because doing so could reveal account names.

  Detection : Command Execution - Keep an eye out for actions that could be used to obtain information about accounts, such ag calls to cloud APIs that carry out account discovery, in logs and other sources of command execution history.

  More information about these scenarios is provided in the table below -

TECHNIQUES IMPLEMENTED	MITIGATION	DETECTION
Acquire Infrastructure	Since it relies on actions taken outside the purview of enterprise defenses and controls, this technique cannot be easily mitigated with preventive controls.	Keep an eye out for DNS registry data queries that could indicate a potential purchase, lease, or rental of targeting-related infrastructure. Detection efforts could concentrate on associated phases of the adversary lifecycle, such as command and Control.
Compromise Infrastructure : Domains	Due to the fact that this technique is predicated on actions taken outside the purview of business defenses and controls, it cannot be easily countered using preventive measures.	Keep an eye out for logged domain name system (DNS) information that could compromise external infrastructure that is used for targeting. Detection efforts could concentrate on associated phases of the adversary lifecycle, such as command and control.
Remote Services : RDP	Whenever possible, use multi-factor authentication for remote service logons.	Keep track of all commands and arguments that have been executed and may have been used to log into a service like telnet, SSH, or VNC that has been created specifically to accept remote connections. The opponent is then able to operate in the user's place.

These techniques would provide a better idea of how to work on the systems and would also give a perspective on the attacker's methodology. These mitigations can be used to improve security and create certain procedures to safeguard it.

How can you take the lessons learned in APT1 and apply them to other APT groups like Cozy Bear?

CozyBear, also known as APT29, is a Russian cyber espionage group. The group has been active since at least 2008 and is believed to be responsible for a number of high-profile cyberattacks, including the 2016 Democratic National Committee hack. APT29 is a much more sophisticated and advanced threat actor than APT1. APT29 has been active since at least 2008, and their tools and techniques have evolved over time. They are a highly skilled and experienced group that has successfully targeted a wide range of high-value targets.

The APT29 has a different set of groups that perform the operations, some of them are -

- IRON RITUAL
- IRON HEMLOCK
- NobleBaron
- Dark Halo

These groups are similar to those of APT1 and often perform espionage against large organizations that affect the economy.

The APT29 group has been known to use a variety of techniques to gain access to victim networks. Some of these techniques include:

1. Spear phishing: The group has been known to send carefully crafted emails that appear to come from a trusted source in order to trick victims into clicking on malicious links or attachments.

2. Watering hole attacks: The group has been known to compromise popular websites that their targets are likely to visit and embed malicious code that can infect visitors' computers.

3. Drive-by downloads: The group has been known to host malicious code on websites that can be downloaded and executed automatically when unsuspecting users visit the site.

4. Malicious document files: The group has been known to create document files that contain embedded malicious code that can be executed when the file is opened.

5. Malicious macros: The group has been known to create macro-enabled document and spreadsheet files that, when opened, will execute malicious code embedded within the file.

6. Remote access tools: The group has been known to use various remote access tools to gain unauthorized access to victim systems.

7. Custom malware: The group has been known to develop custom malware to carry out their attacks.

These attacks are similar to that performed by the APT1 group, and these can be mitigated by -

1. Use strong authentication methods, such as two-factor authentication, for all user accounts.

2. Use a centralized logging solution to monitor all activity on the network.

3. Use intrusion detection and prevention systems to monitor for and block suspicious activity.

4. Regularly update all software and systems to the latest version.

5. Educate employees on security risks and best practices.

What was the political response to this report? Did China debate its findings?

The Apt1 report from Mandiant has served as a wake-up call to the need for security measures to ward off Chinese and Russian hackers. The report included thorough details and information on the strategies and techniques used by the group of hackers. The report also emphasizes the demand for improvements in security in both the public and private sectors.

As the Mandiant Group published the report about APT1 in the January 2010 M-Trends report, they say that the Chinese government may have authorized this activity, but they also believe that there is no way to know their involvement. The evidence required has changed after three years. They say that the groups that are conducting this activity are based in China, and it is sure that the Chinese government knows about it and is aware of it.

TABLE 11: APT1 FQDNs have resolved to IP addresses within these Chinese net blocks

Number	Net block	Registered Owner
150	223.166.0.0 - 223.167.255.255	China Unicom Shanghai Network
68	58.246.0.0 - 58.247.255.255	China Unicom Shanghai Network
10	112.64.0.0 - 112.65.255.255	China Unicom Shanghai Network
7	114.80.0.0 - 114.95.255.255	China Telecom Shanghai Network
5	139.226.0.0 - 139.227.255.255	China Unicom Shanghai Network
4	222.64.0.0 - 222.73.255.25	China Telecom Shanghai Network
3	116.224.0.0 – 116.239.255.255	China Telecom Shanghai Network
16	Other (Non-Shanghai)	

Is APT1 hacking more or less? Why?

The Apt1 is a hacking espionage unit. The operations performed by the group have caused a lot of damage to organizations and resulted in many security issues. The APT1 resulted in many more issues such as data theft and resulted in -

- Information on system designs, product developments and simulation strategies.
- Emails of high ranking officials
- Business plans
- Network architecture information
- White papers and agendas

Although the group performs these operations to steal data, they can also perform certain deadly operations, such as -

- Deletion of files
- Credential Dumping
- Scripting
- Ransomware attacks
    - ★ It is recorded that the APT1 has stolen information as large as 6.5 terabytes from an organization in the span of 10 months. They also compromised many industries such as information technology, aerospace, public administration, energy, transportation, and entertainment.

REACTIONS TO THE REPORT :

Although the APT1 and APT29 are different from the origins, the operations performed by both of the hacking groups are similar to each other and the targeted systems are often compromised in the same way without any trace of the attackers identities.

One of the interesting facts about the APT1 is that the longest time it has had access to a victim is 4 years and 10 months, the group is highly sophisticated and one can assume how smart they were to be in a network for that long.

REFERENCES :

https://socradar.io/apt-profile-cozy-bear-apt29/

https://attack.mitre.org/groups/G0006/

https://attack.mitre.org/groups/G0016/

https://www.mandiant.com/resources/apt1-exposing-one-of-chinas-cyber-espionage-units

https://resources.sei.cmu.edu/asset_files/technicalreport/2014_005_001_90523.pdf

https://harrisbricken.com/chinalawblog/china-cybersecurity-no-place-to-hide/