



# Report for Information on Advanced Persistent Threats (APT1)

01.24.2024

---

## Overview

Since 2004, a threat intel group has been collecting information on breaches all across the world. None other than APT 1 who has amassed a large amount of exfiltration data since their inception. Since 2010 said group called Madiant has been filing a case against them on their attacks worldwide. Three years later, they have piled a ton of evidence against the Advanced Persistent Threat linking them to attacks worldwide, building a case that they are in fact involved with the Chinese Government. This report is about the most legendary group of all APT 1. There is a reason they are the first. It is one of 20 other groups that originate out of China. This group has been at it since 2006, gaining infamy for the sheer size of data stolen that compelled us to write this report.

We shall be going over a small quantity of their attacks and their TTPs (Tactic, Techniques, and Procedures) to emulate how they went about their business in breaching an estimated 150 organizations and it is quite unknown it is possible it could be significantly more that we even know about. In our research we were able to track four possible networks in Shanghai that may be connected to the group . Two of which are in the proximity of the Pudong New Area. They are not ghosts nor shadows but actual individuals behind the keyboards being ordered by a higher officer likely the CCP (Chinese Communist Party) to continue launching these attacks on targeted networks to gain strategic advantages of their nation state adversaries. Thus it is considered a persistent threat because they are state sponsored and have large amounts of resources to initiate these attacks. In our research we were able to find strong correlation with the People's Liberation Army (PLA) Unit 61398 is very similar to APT 1 in its objectives and capabilities. PLA Unit 61398 is also located where APT 1 allegedly originated from.

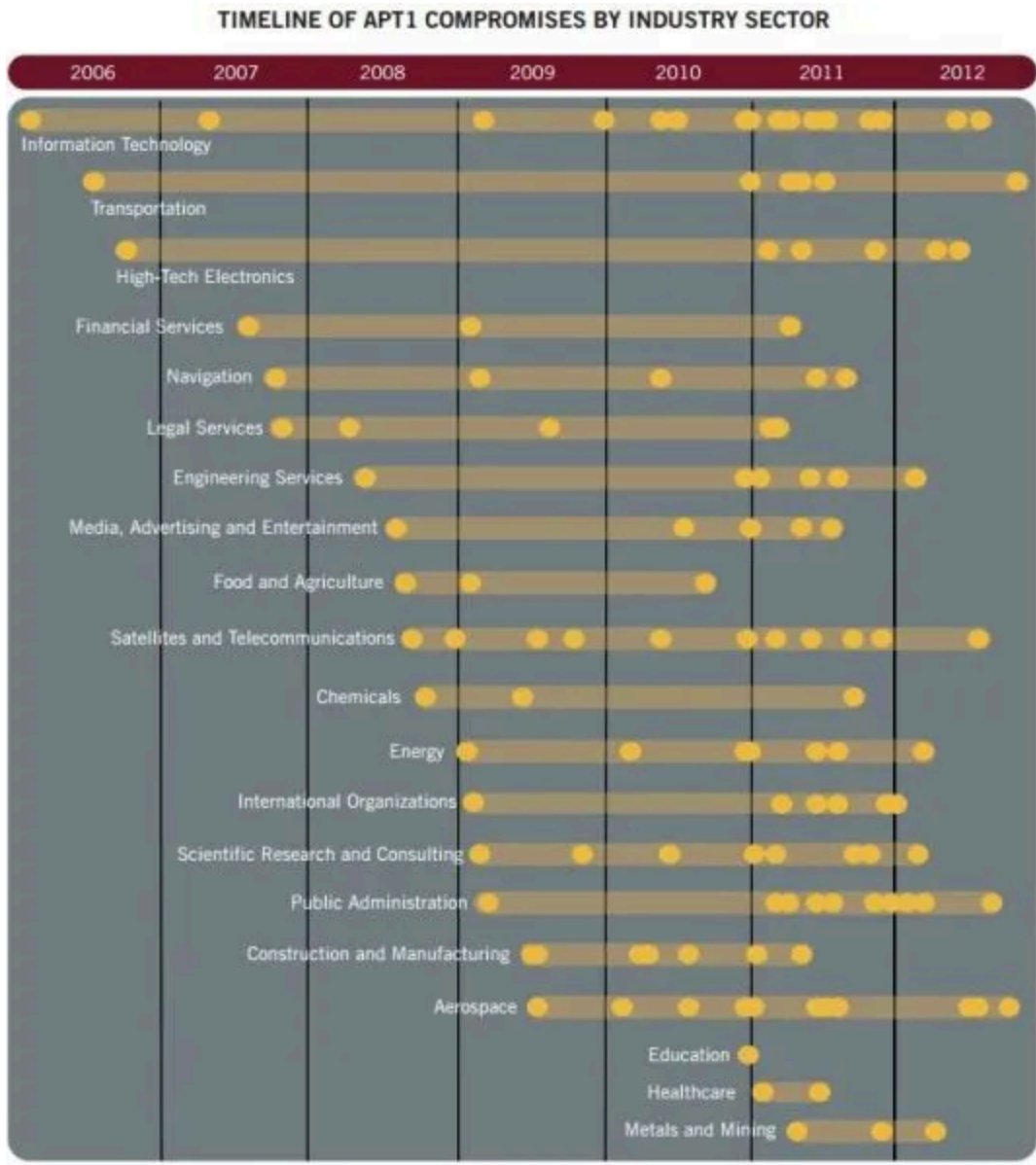
## Goals

1. APT1 has honed a large attack methodology in which they hone themselves to Intellectual Property from their victim organizations in an attempt to steal sensitive data in regards to their IP.
2. Of the 141 APT1 targets about 87% of them reside in an area where the English language is their native language meaning western nations.

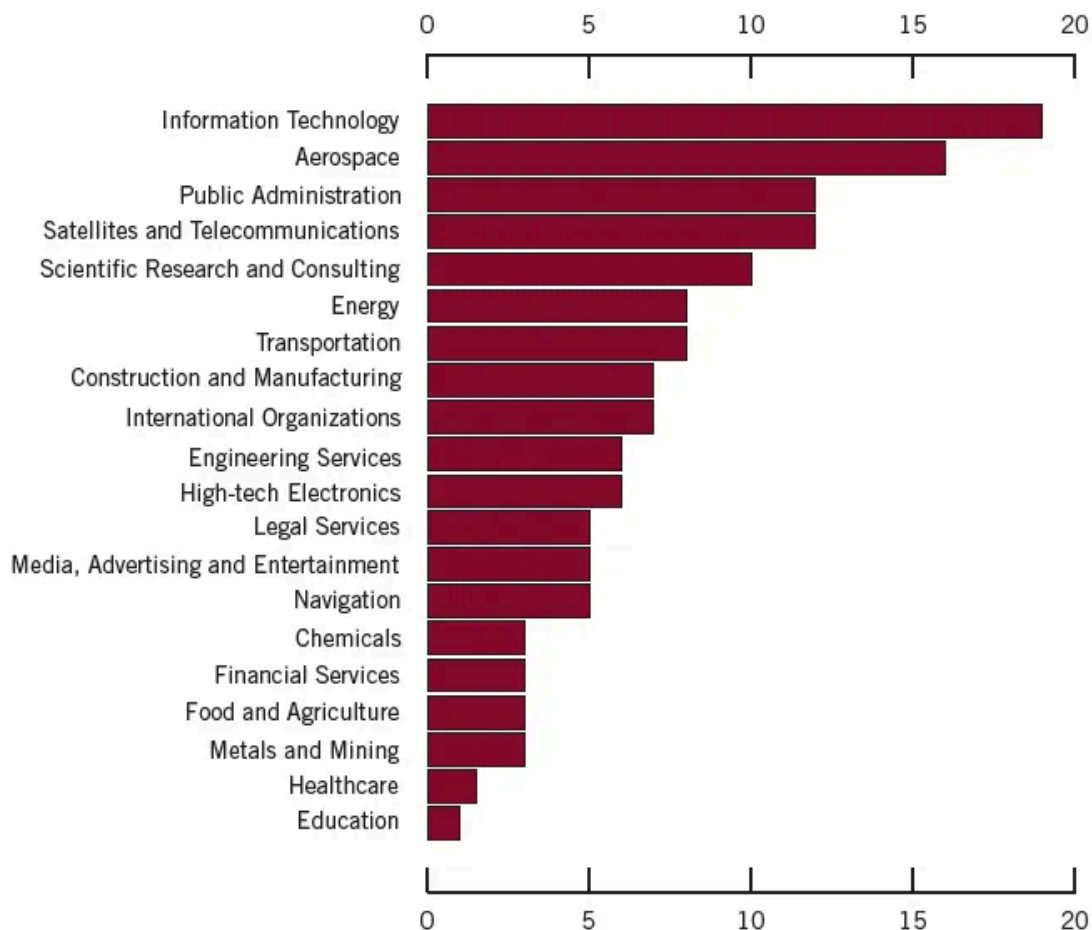
- 3. They specialize in staying persistent in the target network and staying there for as long as possible being hidden for about an average of about a year. The longest being 4 years and 10 months being persistent on a network.
- 4. They weren't always active daily. They were strategic for when they would show themselves to exfiltrate data in the background while evading detection.
- 5. APT1 whose purpose seems to be extremely broad. It doesn't seem to be targeting a specific industry as shown in the second infographic down below. It would tend to target more industries than others as shown in the third infographic below.



Shows APT1's victims. It even shows victims with a multinational presence who have headquarters outside of their respective countries.



The dots show a range from when APT1 started attacking that particular industry.



## Impact OBJ

APT1 attacks steal a wide range of data inside them containing information relating to:

1. As mentioned before Intellectual Property sensitive data including: product development, info on test results, system designs, product manual, part lists, and simulation tech
2. Manufacturing procedures, such as proprietary processes, standards and waste management processes
3. Business plans like information or contract negotiation positions and product pricing, legal events, mergers, joint ventures, and acquisitions.
4. Policy positions and analysis: such as white papers, and notes from meetings with high ranking personnel
5. Emails of important personnel belong to the victim organization
6. User credentials and network architecture information

It is estimated that APT1 has likely stolen hundreds of terabytes from its victims. The largest being about 6.5 terabytes within 10 months being in their networks.

## APT1 Attack Vectors

APT1 has honed their attack methodology and have perfected it over the years designed to steal large amounts of Intellectual property data. They begin with an aggressive spear phishing attempt, then proceed to deploy custom malware to get around their network to eventually end off exfiltrating as much sensitive data as possible while maintaining persistence.

They have fluent English with acceptable amounts of slang to get a victim to fall prey to the spearfish to gain initial access. They tend to have consistently updated their initial access tools to be more effective when inside their victims network as well. For example:

Date: Wed, 18 Apr 2012 06:31:41 -0700

From: Kevin Mandia

Subject: Internal Discussion on the Press Release


Hello, Shall we schedule a time to meet next week? We need to finalize the press release. Details [click here](#).

Kevin Mandia

With an adobe pdf document at the bottom intelligently obfuscated to deceive the victim into thinking it's not malware but actually a legitimate email coming from the CEO. The file would look something like this.

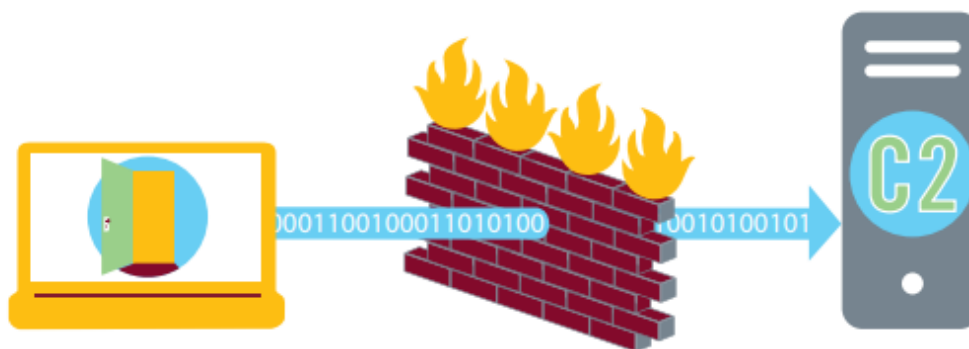
**Would you click on this?**

Some APT1 actors have gone to the trouble of making the malicious software inside their ZIP files look like benign Adobe PDF files. Here is an example:

Name	Type
 employee benefit and overhead adjustment keys.pdf ...	Application

This is not a PDF file. It looks like the filename has a PDF extension but the file name actually includes 119 spaces after ".pdf" followed by ".exe" — the real file extension. APT1 even went to the trouble of turning the executable's icon to an Adobe symbol to complete the ruse. However, this file is actually a dropper for a custom APT1 backdoor that we call WEBC2-QBP.

Once they get the victim to click and open the document they will begin to establish a foothold and deploy a backdoor. A backdoor is a software that allows an intruder to send commands to the system remotely. In almost every case, APT backdoors initiate outbound connections to the attackers command and control center(C2) server. Firewalls are adept at keeping malware outside the network from communicating inside the network but not so much if the malware is already inside the network from communicating outside as shown below.



**FIGURE 17: Backdoors installed on compromised systems usually initiate connections with C2 servers**

While APT1 intruders occasionally use publicly available backdoors such as Poison Ivy and Gh0st RAT, the vast majority of the time they use what appear to be their own custom backdoors. We have documented 42 families of backdoors in “Appendix C: The Malware Arsenal” that APT1 uses that we believe are not publicly available. In addition we have provided 1,007 MD5 hashes associated with APT1 malware in Appendix E. We will describe APT1’s backdoors in two categories: “Beachhead Backdoors” and “Standard Backdoors.”

APT1s backhead doors are notoriously named WEBC2 backdoors. WEBC2 backdoors are well known to be used by APT1. How it works is the backdoor is designed to retrieve a webpage from a C2 server. It excerpt the webpage to contain special HTML tags: the backdoor will interpret the data within the tags as HTML commands. They have been deploying WEBC2 backdoors since 2004. It appears they may have direct access to developers of the continually released variants overtime.

WEBC2 backdoors typically give APT1 attackers a short and simple set of commands to issue to victim systems like

1. Open an interactive command shell (usually Windows’ cmd.exe)
2. Download and execute file
3. Sleep (remain inactive) for a set period of time

The APT1 attacker has the option to tell the victim machine to download a specific malware of their liking. WEBC2 backdoors work for their intended purposes, but they generally have fewer features than the “Standard Backdoors”.

Once they are inside their networks they will attempt to move laterally within their victim’s systems. Escalating privileges involves acquiring credentials that will allow for them to have

complete access to their compromised network. APT1 predominantly uses publicly available tools to dump password hashes from victim systems in order to obtain legitimate user credentials. APT1 has used these privilege escalation tools:

**TABLE 6: Publicly available privilege escalation tools that APT1 has used**

Tool	Description	Website
<b>cachedump</b>	This program extracts cached password hashes from a system's registry	Currently packaged with fgdump (below)
<b>fgdump</b>	Windows password hash dumper	<a href="http://www.foofus.net/fizzgig/fgdump/">http://www.foofus.net/fizzgig/fgdump/</a>
<b>gsecdump</b>	Obtains password hashes from the Windows registry, including the SAM file, cached domain credentials, and LSA secrets	<a href="http://www.truesec.se">http://www.truesec.se</a>
<b>lsisass</b>	Dump active logon session password hashes from the lsass process	<a href="http://www.truesec.se">http://www.truesec.se</a>
<b>mimikatz</b>	A utility primarily used for dumping password hashes	<a href="http://blog.gentilkiwi.com/mimikatz">http://blog.gentilkiwi.com/mimikatz</a>
<b>pass-the-hash toolkit</b>	Allows an intruder to "pass" a password hash (without knowing the original password) to log in to systems	<a href="http://oss.coresecurity.com/projects/pshtoolkit.htm">http://oss.coresecurity.com/projects/pshtoolkit.htm</a>
<b>pwdump7</b>	Dumps password hashes from the Windows registry	<a href="http://www.tarasco.org/security/pwdump_7/">http://www.tarasco.org/security/pwdump_7/</a>
<b>pwdumpX</b>	Dumps password hashes from the Windows registry	The tool claims its origin as <a href="http://reedarvin.thearvins.com/">http://reedarvin.thearvins.com/</a> , but the site is not offering this software as of the date of this report

Once they are inside a victims network they proceed to what is called Internal Reconnaissance. The Intruder that is APT1 collects information about the target system by using custom built commands to explore a compromised system and its environment. Sometimes, even using a bash script to run a variety of commands quickly to automate the task.



```
@echo off
ipconfig /all>>"C:\WINNT\Debug\l.txt"
net start>>"C:\WINNT\Debug\l.txt"
tasklist /v>>"C:\WINNT\Debug\l.txt"
net user >>"C:\WINNT\Debug\l.txt"
net localgroup administrators>>"C:\WINNT\Debug\l.txt"
netstat -ano>>"C:\WINNT\Debug\l.txt"
net use>>"C:\WINNT\Debug\l.txt"
net view>>"C:\WINNT\Debug\l.txt"
net view /domain>>"C:\WINNT\Debug\l.txt"
net group /domain>>"C:\WINNT\Debug\l.txt"
net group "domain users" /domain>>"C:\WINNT\Debug\l.txt"
net group "domain admins" /domain>>"C:\WINNT\Debug\l.txt"
net group "domain controllers" /domain>>"C:\WINNT\Debug\l.txt"
net group "exchange domain servers" /domain>>"C:\WINNT\Debug\l.txt"
net group "exchange servers" /domain>>"C:\WINNT\Debug\l.txt"
net group "domain computers" /domain>>"C:\WINNT\Debug\l.txt"
```

---

### 8: An APT1 batch script that automates reconnaissance

This script performs the following functions and saves the results to a text file:

- » Display the victim's network configuration information
- » List the services that have started on the victim system
- » List currently running processes
- » List accounts on the system
- » List accounts with administrator privileges
- » List current network connections
- » List currently connected network shares
- » List other systems on the network
- » List network computers and accounts according to group ("domain controllers," "domain users," "domain admins," etc.)

Once an APT attacker has a good idea of the system and acquires legitimate credentials, it is not difficult for the attacker to move undetected.

- » They can connect to shared resources on other systems
- » They can execute commands on other systems using the publicly available "psexec" tool from Microsoft Sysinternals or the built-in Windows Task Scheduler ("at.exe")

These normal processes are hard to distinguish because actual system administrators also use these techniques to perform actions around the network.

## Maintain Persistence

In this stage, the intruder will continue to stay hidden in the network and will want to find a way to communicate from outside the network. Like mentioned before, they might want to install a C2 server or perhaps they would like to have multiple ways of getting back into the system by installing additional backdoors to maintain persistence. APT1 has been known to do this.

They also actively try to steal legitimate user credentials to impersonate them. APT1 has been seen using stolen credentials to log into victim systems using VPNs that are only protected by a single-factor authentication. They are allowed to access whatever that user is given privileges to see. They will try everything as well to access web portals within the network or web based emails systems such as Outlook Web Access.

## Completing the Mission

Once APT1 finds files of interests they pack them into archive files before stealing them. APT intruders most commonly use the RAR archiving utility for this task and ensure that the archives are password protected. They might use a BASH script to automate the process as well.

```
@echo off
cd /d c:\windows\tasks
rar.log a XXXXXXXX.rar -v200m "C:\Documents and Settings\Place\My
Documents\XXXXXXXX" -hpsmy123!@#
del *.vbs
del %0
```

Sometimes attackers will transfer files via traditional routes like using File Transfer Protocol(FTP) or existing backdoors. Sometimes files are so large that they get split up by however much is needed to avoid suspicion. For example being split up into 200mb portions.

## Defense Strategies against APT1

### I. Defense Against APT1

APT 1 can be defended against by having threat intelligence personnel in place to research on this adversary and how they operate but studying up on their TTPs. Knowing what we know about their attack vector they like targeting users via Spear Phishing campaigns. It's imperative that we educate these users on how they try to fool the victims via impersonation. Cultivating a security conscious environment is of

utmost importance in defending against APT1 because once they are inside your network they are difficult to find and get rid of. A remediation technique that is also effective is by having role based access control to limit a users ability to have much access than what they need. A user might not only need a certain amount of access to do their job preventing APT1 access from having lateral movement within our network. Preventative measures that may be put into place is by deploying Endpoint Detection and Response alongside an IDS Intrusion Detection System to find these adversaries and begin to eradicate them from your network as soon as possible if detected. Their sole goal is to exfiltrate data. They will fight to stay inside by finding their backdoors and closing them. They will be found and high alert with the security team will be placed provoking an incident response plan to be executed.

## II. Incident Response against APT1

At this stage, we are in the recovery phase, we must begin system hardening. Implement the necessary security controls to strengthen the infrastructure. Run some forensic analysis to understand how our organization was compromised. Document the findings and implement configurations and policies based on our findings. Afterwards, there will need to be continuous improvement to preventive measures because the next attack could be a ransomware attack and we must be prepared for everything.

## Framework Alignment

### 1. NIST Cybersecurity Framework:

The NIST Cybersecurity Framework is a widely recognized and adopted framework that provides a set of guidelines and best practices to improve cybersecurity risk management. The APT1 defense strategies align with the NIST framework in the following ways:

- Identify (NIST CSF Core Function): Risk assessment, asset inventory, and establishing an incident response team aligned with the "Identify" function.
- Protect (NIST CSF Core Function): Access control, network segmentation, encryption, and endpoint protection align with the "Protect" function.
- Detect (NIST CSF Core Function): Network monitoring, intrusion detection, and endpoint detection and response align with the "Detect" function.
- Respond (NIST CSF Core Function): Incident response planning, communication plan, and containment align with the "Response
- " function.

- Recover (NIST CSF Core Function): Data restoration, system hardening, and continuous improvement align with the "Recover" function.

## 2. ISO 27001:

ISO 27001 is an international standard for information security management systems (ISMS). The APT1 defense strategies align with ISO 27001 in the following ways:

- Risk Assessment (ISO 27001 Clause 6): Conducting a risk assessment aligns with ISO 27001 requirements for risk management.
- Access Control (ISO 27001 Clause 9): Implementing the principle of least privilege aligns with ISO 27001 access control requirements.
- Incident Response (ISO 27001 Clause 16): Developing an incident response plan aligns with ISO 27001 requirements for managing information security incidents.

## Insights into the impact of emerging technologies like AI on APT1 methodologies and defenses

AI is a double edged sword in the context of APT1. While it may empower the defender with advanced capabilities for threat detection and response, it also poses challenges as an attacker because it will enhance the ability of an attacker to launch a sophisticated attack with all the data that a machine learning AI may have. It might have a stronger capability of creating a strong attack proposition. Whereas, in being in the situation of being an defender it might be susceptible to more mistakes that an attackers AI may exploit in theory.

### Projections on the evolution of APT1

The whereabouts of APT1 are unknown. Ever since the mandiant report they have shut down their operations. They are more than likely under one of 20 other APT groups who belong to the Chinese. Due to their culture being very submissive in following orders they will continue being a threat and I foresee them continuing to grow under another pseudonym. More than likely leveraging AI! In the near future to launch even more sophisticated attacks it's up to the defenders to counteract and perfect their own AI to be able to keep up, that is if...

References():

<https://www.mandiant.com/sites/default/files/2021-09/mandiant-apt1-report.pdf>