✏️

# APT -1

중국 인민해방군 유닛 61398

APT1 is a Chinese threat group that has been attributed to the 2nd Bureau of the People's Liberation Army (PLA) General Staff Department's (GSD) 3rd Department, commonly known by its Military Unit Cover Designator (MUCD) as Unit 61398.

**ID:** G0006

**Associated Groups**: Comment Crew, Comment Group, Comment Panda

**Version**: 1.3

**Created:** 31 May 2017

**Last Modified:** 22 October 2020

## Threat Actor Profile

**Origin**: China, 2006

**Aliases**: Comment Crew, Comment Group, Comment Panda, Byzantine Candor, GIF89a, Group 3, TG-8223, Unit 61398

**Key Target Sectors**: Manufacturing, Information Technology, Healthcare, Finacial Services, Government, Transportation, Communication, Energy and Power

**Attack Vectors**: Spear-phishing, Unauthorized Access, Data Theft

**Target Region**: Eastern Asia, North America

**Malware Used**: Downbot, Ecltys, Seasalt, Barkfork, Poison Ivy, Mimikatz, WakeMinap, Dalbot, Revird, Badname, Cachedump, Wualess, Calendar, GlooXmail, WEBC2

**Tools Used**: Mimikatz, Cachedump, Gsecdump, IPconfig, Lslsass, Pass-The-Hash Toolkit, Net, PsExec, Pwdump, Tasklist, and xCmd

---

# Discovery

## ID: T1135

**Sub-techniques:** No sub-techniques

**Tactic:** Discovery

**Platforms:** Linux, Windows, macOS

**Permissions Required:** User

**Data Sources:** Command: Command Execution, Process: OS API Execution, Process: Process Creation

**CAPEC ID:** CAPEC-643

**Contributors:** Praetorian

**Version:** 3.0

**Created:** 14 December 2017

**Last Modified:** 29 December 2020

**APT1 listed connected network shares.**

# Network Share Discovery

Adversaries may look for folders and drives shared on remote systems as a means of identifying sources of information to gather as a precursor for Collection and to identify potential systems of interest for Lateral Movement. Networks often contain shared network drives and folders that enable users to access file directories on various systems across a network.

File sharing over a Windows network occurs over the SMB protocol. [1] [2] Net can be used to query a remote system for available shared drives using the `net view \\remotesystem` command. It can also be used to query shared drives on the local system using `net sh`

## ID: T1057

**Sub-techniques:** No sub-techniques

**Tactic:** Discovery

**Platforms:** Linux, Windows, macOS

**System Requirements:** Administrator, SYSTEM may provide better process ownership details

**Permissions Required:** Administrator, SYSTEM, User

**Data Sources:** Command: Command Execution, Process: OS API Execution, Process: Process Creation

**CAPEC ID:** CAPEC-573

**Version:** 1.2

**Created:** 31 May 2017

**Last Modified:** 26 March 2020

**APT1 gathered a list of running processes on the system using tasklist /v.**

## Process Discovery

Adversaries may attempt to get information about running processes on a system. Information obtained could be used to gain an understanding of common software/applications running on systems within the network. Adversaries may use the information from Process Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

In Windows environments, adversaries could obtain details on running processes using the Tasklist utility via cmd or `Get-Process` via PowerShell. Information about processes can also be extracted from the output of Native API calls such as `CreateToolhelp32Snapshot`. In Mac and Linux, this is accomplished with the `ps` command. Adversaries may also opt to enumerate processes via /proc.

## ID: T1016

**Sub-techniques:** T1016.001

**Tactic:** Discovery

**Platforms:** Linux, Windows, macOS

**Permissions Required:** User

**Data Sources:** Command: Command Execution, Process: OS API Execution, Process: Process Creation, Script: Script Execution

**CAPEC ID:** CAPEC-309

**Version:** 1.2

**Created:** 31 May 2017

**Last Modified:** 24 April 2021

**APT1 used the ipconfig /all command to gather network configuration information.**

## System Network Configuration Discovery

Adversaries may look for details about the network configuration and settings of systems they access or through information discovery of remote systems. Several operating system administration utilities exist that can be used to gather this information. Examples include Arp, ipconfig/ifconfig, nbtstat, and route.

Adversaries may use the information from System Network Configuration Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

## ID: T1049

**Sub-techniques:**  No sub-techniques

**Tactic:** Discovery

**Platforms:** IaaS, Linux, Windows, macOS

**Permissions Required:** Administrator, User

**Data Sources:** Command: Command Execution, Process: OS API Execution, Process: Process Creation

**Contributors:** Praetorian

**Version:** 2.2

**Created:** 31 May 2017

**Last Modified:** 08 March 2021

# System Network Connections Discovery

Adversaries may attempt to get a listing of network connections to or from the compromised system they are currently accessing or from remote systems by querying for information over the network.

An adversary who gains access to a system that is part of a cloud-based environment may map out Virtual Private Clouds or Virtual Networks in order to determine what systems and services are connected. The actions performed are likely the same types of discovery techniques depending on the operating system, but the resulting information may include details about the networked cloud environment relevant to the adversary's goals. Cloud providers may have different ways in which their virtual networks operate.[1][2][3]

Utilities and commands that acquire this information include netstat, "net use," and "net session" with Net. In Mac and Linux, netstat and `lsof` can be used to list current connections. `who -a` and `w` can be used to show which users are currently logged in, similar to "net session".

**APT1 used the net use command to get a listing on network connections.**

## ID: T1007

**Sub-techniques:**  No sub-techniques

**Tactic:** Discovery

**Platforms:** Windows

**Permissions Required:** Administrator, SYSTEM, User

**Data Sources:** Command: Command Execution, Process: Process Creation

**CAPEC ID:** CAPEC-574

**Version:** 1.1

**Created:** 31 May 2017

**Last Modified:** 15 March 2020

## System Service Discovery

Adversaries may try to get information about registered services. Commands that may obtain information about services using operating system utilities are "sc," "tasklist /svc" using Tasklist, and "net start" using Net, but adversaries may also use other tools as well. Adversaries may use the information from System Service Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

**APT1 used the commands net start and tasklist to get a listing of the services on the system.**

---

# Collection

## ID: T1119

**Sub-techniques:** No sub-techniques

**Tactic:** Collection

**Platforms:** Linux, Windows, macOS

**System Requirements:** Permissions to access directories and files that store information of interest.

**Permissions Required:** User

**Data Sources:** Command: Command Execution, File: File Access, Script: Script Execution

**Version:** 1.0

**Created:** 31 May 2017

**Last Modified:** 31 March 2020

## Automated Collection

Once established within a system or network, an adversary may use automated techniques for collecting internal data. Methods for performing this technique could include use of a Command and Scripting Interpreter to search for and copy information fitting set criteria such as file type, location, or name at specific time intervals. This functionality could also be built into remote access tools.

This technique may incorporate use of other techniques such as File and Directory Discovery and Lateral Tool Transfer to identify and move files.

**APT1 used a batch script to perform a series of discovery techniques and saves it to a text file**

## ID: T1005

**Sub-techniques:** No sub-techniques

**Tactic:** Collection

**Platforms:** Linux, Windows, macOS

**System Requirements:** Privileges to access certain files and directories

**Data Sources:** Command: Command Execution, File: File Access

**Version:** 1.2

**Created:** 31 May 2017

**Last Modified:** 26 May 2020

## Data from Local System

Adversaries may search local system sources, such as file systems or local databases, to find files of interest and sensitive data prior to Exfiltration.

Adversaries may do this using a Command and Scripting Interpreter, such as cmd, which has functionality to interact with the file system to gather information. Some adversaries may also use Automated Collection on the local system.

**APT1 has collected files from a local victim**

# Soft Ware

# Modus Operandi

A typical APT1 cyber-attack begins by sending spear phishing emails to the victim. These emails have official language and themes to make them look authentic but carry a malicious attachment. When a victim opens the attachment, the backdoor provides control of the targeted machine to the APT1. Once they gain access to the network, they can visit any targeted system at any time. The group remains latent for very long durations, sometimes over several months or even years, without victims having any hint about the intrusion.

They target intellectual property, like proprietary manufacturing processes, technology blueprints, test results, pricing documents, business plans, emails and contact lists, and partnership agreements from the victim organizations. The group maintains access to victim’s networks for an average of 356 days. The group also installs new backdoors to the already infected systems in the environment. In such a scenario, even if one backdoor is detected and deleted, they still have other backdoors that can be used.

# Known tools and malware

APT1 is known to use multiple families of backdoors and Trojans to infiltrate into the targeted network. Along with using several backdoors and Trojan, the group also uses various open-source utility tools in their cyber attack campaigns.

**Malicious programs used by APT1**

- **Downbot** Trojan horse that comes hidden in malicious programs.
- **Ecltys** Trojan horse that opens a backdoor on the victimized computer system.
- **Seasalt** Adware that comes with an excessive display of advertisements.
- **Barkfork** Backdoor that comes hidden in malicious programs.
- **Poison Ivy** - Remote Access Trojan (RAT), designed with spying capabilities.
- **WakeMinap** Trojan horse that opens a backdoor on the compromised computer.
- **Dalbot** Trojan horse that opens a backdoor on the compromised computer.

- **Revird** Trojan horse that opens a backdoor on the compromised computer.
- **Badname** Trojan horse that can gain remote unauthorized access and control over the affected computer.
- **Wualess** Trojan horse that opens a backdoor on the compromised computer.
- **Biscuit** It is a backdoor that has been used by APT1 since as early as 2007.
- **Calendar** It is malware that mimics legitimate Gmail Calendar traffic.
- **GlooXmail** It is a malware that mimics legitimate Jabber/XMPP traffic.
- **WEBC2** A backdoor that is used to retrieve a Web page from a predetermined C2 server.

Other prominent malware used by APT1 are Auriga, Bangat, Bouncer, Combos, Cookiebag, Dairy, Getmail, Gdocupload, Goggles, Greencat, Hackfase, Helauto, Kurton, Lightbolt, Lightdart, Longrun, Manitsme, Mapiget, Miniasp, Newsreels, Starsypound, Sword, Tabmsgsql, Tarsip-eclipse, Tarsip-moon, Warp, Webc2-adspace, Webc2-ausov, Webc2-bolid, Webc2-clover, Webc2-cson, Webc2-div, Webc2-greencat, Webc2-head, Webc2-kt3, Webc2-qbp, Webc2-rave, Webc2-table, Webc2-ugx, Webc2-y21k, Webc2-yahoo and Webc2-tock.

**Known Commercial/Open Source tools used by APT1**

- **Cachedump** It is a publicly-available tool that extracts cached password hashes from a system’s registry.
- **Gsecdump** It is a publicly-available credential dumper, used to obtain password hashes and LSA secrets from Windows operating systems.
- **IPconfig** A Windows utility that can be used to find information about a system's DNS, DHCP, TCP/IP, and adapter configuration.
- **Lslsass** A publicly-available tool that can dump active login session password hashes from the Lsass process.
- **Mimikatz** It is a credential dumper capable of obtaining plaintext Windows account logins and passwords.
- **Pass-The-Hash Toolkit** - A toolkit that allows an attacker to "pass" a password hash (without knowing the original password) to login to systems.

- **Net** This utility is a component of the Windows operating system.
- **PsExec** A command-line tool that lets its user execute processes on remote systems. It is used by IT administrators and attackers.
- **Pwdump** A credential dumper tool to dump passwords.
- **Tasklist** A utility that shows a list of services and applications with their Process IDs (PID) for every task running on either a remote or local computer.
- **xCmd** An open source tool that allows the user to execute applications on remote systems.

# Mimikatz

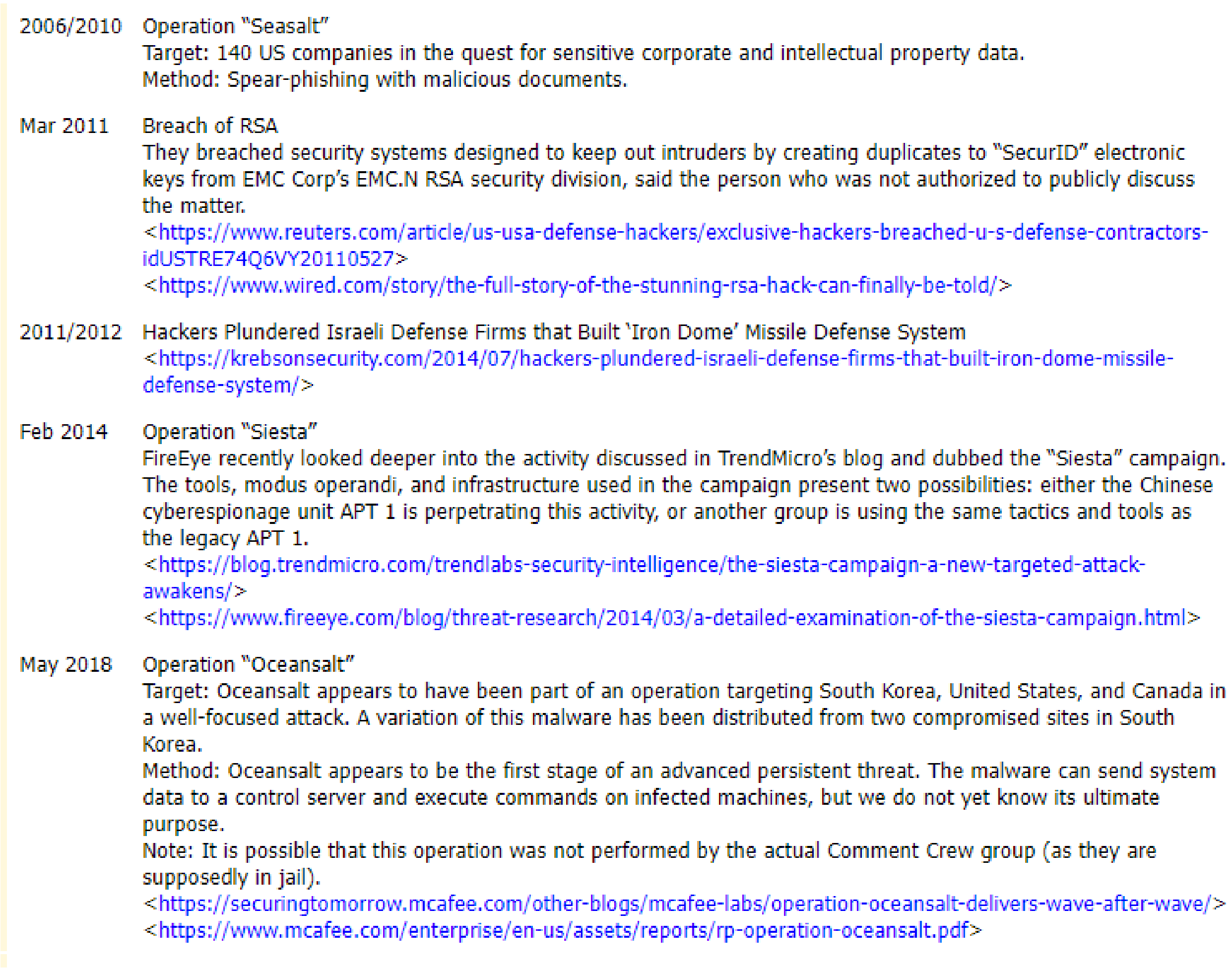
Mimikatz is a great post-exploitation tool written by Benjamin Delpy (gentilkiwi). After the initial exploitation phase, attackers may want to get a firmer foothold on the computer/network. Doing so often requires a set of complementary tools. Mimikatz is an attempt to bundle together some of the most useful tasks that attackers will want to perform.

Fortunately, Metasploit has decided to include Mimikatz as a meterpreter script to allow for easy access to its full set of features without needing to upload any files to the disk of the compromised host.

**Note:** The version of Mimikatz in metasploit is v1.0, however Benjamin Delpy has already released v2.0 as a stand-alone package on his website. This is relevant as a lot of the syntax has changed with the upgrade to v2.0.

## more information

https://www.offensive-security.com/metasploit-unleashed/mimikatz/



2006/2010 Operation "Seasalt"
Target: 140 US companies in the quest for sensitive corporate and intellectual property data.
Method: Spear-phishing with malicious documents.

Mar 2011 Breach of RSA
They breached security systems designed to keep out intruders by creating duplicates to "SecurID" electronic keys from EMC Corp's EMC.N RSA security division, said the person who was not authorized to publicly discuss the matter.
<https://www.reuters.com/article/us-usa-defense-hackers/exclusive-hackers-breached-u-s-defense-contractors-idUSTRE74Q6VY20110527>
<https://www.wired.com/story/the-full-story-of-the-stunning-rsa-hack-can-finally-be-told/>

2011/2012 Hackers Plundered Israeli Defense Firms that Built 'Iron Dome' Missile Defense System
<https://krebsonsecurity.com/2014/07/hackers-plundered-israeli-defense-firms-that-built-iron-dome-missile-defense-system/>

Feb 2014 Operation "Siesta"
FireEye recently looked deeper into the activity discussed in TrendMicro's blog and dubbed the "Siesta" campaign. The tools, modus operandi, and infrastructure used in the campaign present two possibilities: either the Chinese cyberespionage unit APT 1 is perpetrating this activity, or another group is using the same tactics and tools as the legacy APT 1.
<https://blog.trendmicro.com/trendlabs-security-intelligence/the-siesta-campaign-a-new-targeted-attack-awakens/>
<https://www.fireeye.com/blog/threat-research/2014/03/a-detailed-examination-of-the-siesta-campaign.html>

May 2018 Operation "Oceansalt"
Target: Oceansalt appears to have been part of an operation targeting South Korea, United States, and Canada in a well-focused attack. A variation of this malware has been distributed from two compromised sites in South Korea.
Method: Oceansalt appears to be the first stage of an advanced persistent threat. The malware can send system data to a control server and execute commands on infected machines, but we do not yet know its ultimate purpose.
Note: It is possible that this operation was not performed by the actual Comment Crew group (as they are supposedly in jail).
<https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/operation-oceansalt-delivers-wave-after-wave/>
<https://www.mcafee.com/enterprise/en-us/assets/reports/rp-operation-oceansalt.pdf>

# Reference

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

https://mitre-attack.github.io/attack-navigator/

https://www.fireeye.com/blog/threat-research/2014/05/the-pla-and-the-800am-500pm-work-day-fireeye-confirms-dojs-findings-on-apt1-intrusion-activity.html

https://cyware.com/research-and-analysis/apt1-a-nation-state-adversary-attacking-a-broad-range-of-corporations-and-government-entities-around-the-world-3041