# APT31 Threat Group Profile

Fusion (FS) Cyber Espionage (CE)

Enterprise (EN)

April 26, 2016 09:16:00 AM, 16-00005410, Version: 2

## Executive Summary

APT31 engages in cyber operations where the goal is intellectual property theft, usually focusing on the data and projects that make a particular organization competitive within its field. Based on available data, we assess that APT31 conducts network operations at the behest of the Chinese government.

APT31 has targeted organizations headquartered in multiple countries, including the United States, Canada, and Sweden. They have targeted organizations in a range of industries, including aerospace, government, and telecommunications.

## Key Points

- APT31 engages in cyber operations where the goal is intellectual property theft, usually focusing on the data and projects that make a particular organization competitive within its field.
- Based on available data, we assess that APT31 conducts network operations at the behest of the Chinese government.

## Threat Detail

This report was originally published on the FireEye Intelligence Center portal on Nov. 17, 2015

### Targeting Patterns

Knowing the types of organizations, individuals, or data that a threat group targets provides insight into the group's motivations and objectives. Gathering this type of data about a group typically requires visibility into the group's operational planning; their initial attacks or infection attempts; or into actual victim environments. This data may take time, effort, and persistence to identify, accumulate, and analyze.

*Affected Industries*

This group has targeted organizations in the following industries:

- Aerospace and Defense
- Business and Professional Services
- Construction and Engineering
- Financial Services and Insurance
- High Tech and Information Technology
- Media and Entertainment
- Telecommunications

*Affected Countries*

This group has targeted organizations headquartered in the following countries:

- Canada
- Sweden
- United States

*Data Theft*

It may be difficult to estimate how much or what types of data a threat group has stolen during their intrusions for several reasons:

- Threat actors delete copies of files after they steal them, leaving little if any forensic evidence of the theft.
- Existing network security monitoring rarely records or identifies the data theft as it occurs.
- Data theft may occur using encrypted protocols (such as SSL) or through backdoors that use custom protocols, which are typically not decipherable to standard network monitoring tools even when they are present.
- The duration of time between the data theft and an investigation is often too great, and the trace evidence of data theft is overwritten during the normal course of business.
- Following a breach, some organizations focus on mitigation and recovery, so the full extent of the breach (and any data theft) is not fully investigated.
- Multiple threat groups may be present within a single organization, making it difficult to determine which group stole specific data.

APT31 has targeted company proprietary data, including financial data and client information. In at least one instance, APT31 actors specifically targeted information related to a company's sub-organization, before later compromising the sub-organization. APT31 stole credentials, VPN information, and communication data from the parent organization, and most likely used this data to gain access to the sub-organization.

- Data of Unknown Type or Category
- Information Technology, System, or Network Data
- Passwords, Certificates, or Credentials

*Context and Implications*

APT31 appears focused on obtaining information that would provide the Chinese government and state-owned enterprises with political, economic, and military advantages. Several organizations compromised by APT31 (particularly the national government agency, international financial organization, and aerospace and defense organizations) are suggestive of a nation state's political and military interests.

Chinese decision-makers can use political intelligence stolen during a compromise to inform their decisions. In one case, APT31 compromised an international financial organization while it was engaged in negotiations with its Chinese counterpart, suggesting that the compromise may have been intended to provide China with insider information that would give them an advantage in the talks.

APT31 also engages in activity suggestive of efforts to support China's state-owned organizations against global competitors. In one case, APT31 compromised an organization producing solar panels just as the U.S. Department of Commerce introduced a 31% tariff on solar products imported from China. In addition to the new tariff, the compromised company had also developed a product that posed a challenge to China's dominance of the solar panel manufacturing business. Given the timing of APT31's activity, the threat group may have sought to obtain information capable of supporting China's domestic solar panel manufacturers against increased foreign competition.

Finally, APT31's targeting of the aerospace and defense industry most likely contributes to China's efforts towards military modernization.

## Tactics, Techniques, And Procedures (TTPs)

The Attack Lifecycle is a framework used to describe the common "phases" of a typical attack or intrusion, as well as the specific techniques that may be used in each phase. In cases where we have obtained sufficient data, we have attempted to define alternate versions of the lifecycle for specific types or classes of threat groups, such as the Chinese APT Attack Lifecycle.

### *Initial Compromise*

The Initial Compromise stage of the Attack Lifecycle represents the methods used by a threat actor to penetrate a target organization's network environment.

APT31 has exploited vulnerabilities in applications such as Java and Adobe Flash to compromise victim environments.

### *Establish Foothold*

The Establish Foothold stage of the Attack Lifecycle involves actions that ensure continued control over a compromised system. Threat actors typically establish a foothold immediately after the initial compromise. The most common technique is installing a backdoor program that is able to persist between system reboots.

Some threat groups may initially install malware with limited functionality, such as downloaders or "toehold" backdoors that only support basic commands (such as "sleep" or "download a file"). These "first stage" tools are used to install more sophisticated backdoors as the group penetrates further into a victim network. Alternately, some groups may prefer to install more robust backdoors immediately following the initial compromise.

### *Escalate Privileges*

The Escalate Privileges stage of the Attack Lifecycle involves gaining permissions that may not be associated with an average user account. This may take the form of a privilege escalation exploit or discovering legitimate usernames and passwords for desired (usually administrator- or root-level) accounts. The most common technique is password hash dumping followed by password cracking or hash injection (pass-the-hash).

APT31 has used publicly available credential dumping tools such as GSECDUMP and Hashdump. The threat actors have also used SMB network shares to push files to remote hosts before remotely creating unnamed scheduled tasks to execute malicious binaries. For example, APT31 has used compromised domain user accounts to access remote systems. Once connected to the remote host, APT31 creates a scheduled task to execute a credential dumping utility and direct the output to a file. The threat actors then use the built-in Windows command "type" to view the contents of the newly created file.

In addition to extracting hashes from compromised systems, APT31 also attempts to locate credentials that may be stored in documents or located on file shares.

### *Internal Reconnaissance*

In the Internal Reconnaissance stage of the Attack Lifecycle, a threat actor takes steps to explore the victim environment. It is important for an intruder to understand the environment in order to know how to access systems, where key information is stored, and who has privileges to access that information. The most common techniques involve the use of built-in operating system commands (such as the Windows "net" commands).

APT31 uses built-in Windows commands to conduct reconnaissance and identify computers, accounts, and data of interest. We have also noted APT31 using the Microsoft SysInternal's tool AD Explorer to take Active Directory snapshots, which can then be viewed offline.

| | | |
|---|---|---|
| ADEXPLORER | Reconnaissance Tool | Publicly Available |

### *Lateral Movement*

In the Lateral Movement stage of the Attack Lifecycle, a threat actor takes steps to access additional systems within the network. The most common methods on Windows systems involve using built-in operating system tools (such as Task Scheduler or Remote Desktop) or publicly available remote execution tools like Microsoft (Sysinternals) PsExec.

APT31 relies on commonly used techniques such as scheduling jobs using Windows Task Scheduler, although the group will also typically use valid compromised credentials to move around a victim network or to access corporate resources such as VPNs.

### *Maintain Presence*

In the Maintain Presence stage of the Attack Lifecycle, a threat actor takes steps to ensure continued control over key systems in the network environment. These actions may be identical to those in the Establish Foothold phase; that is, any backdoors deployed in the Establish Foothold phase could also be used in this phase, and vice versa. However, a threat actor may also maintain presence (that is, continue to access the network) through other means, such as Virtual Private Network (VPN) access using legitimate, compromised credentials.

APT31 has used a variety of backdoors to compromise victims and maintain presence in the environment. For example, the group has used a Java exploit to deliver a SLOWGYRO backdoor, and an Adobe Flash exploit with a QUICKBALL payload. The group is one of many APT groups that use the SOGU backdoor.

In some cases, APT31 has used legitimate code signing certificates to sign their malware. APT31 has also installed multiple web shells in conjunction with their backdoors, most likely as a backup measure should responders detect their other methods of access.

APT31 has used backdoors that communicate via the UDP protocol. Some backdoors also use legitimate web services such as GitHub or Google Code as part of their communications, which helps them blend in with normal network traffic. APT31 will also use valid user credentials to obtain remote access to a victim environment, such as through a corporate VPN.

| | | |
|---|---|---|
| BANDCLOGS | Backdoor | Non-public |
| CITYWOK | Backdoor | Non-public |
| DUCKFAT | Backdoor | Non-public |
| DUCKWALK | Backdoor | Non-public |
| HOMEUNIX | Backdoor | Non-public / Confirmed Shared |
| LUCKYBIRD | Backdoor | Non-public |
| QUICKBALL | Backdoor | Non-public / Confirmed Shared |
| RAWDOOR | Backdoor | Non-public |
| SLOWGYRO | Backdoor | Non-public |
| SOGU | Backdoor | Non-public / Confirmed Shared |

### *Complete Mission*

In the Complete Mission stage of the Attack Lifecycle, a threat actor accomplishes his or her goal. The mission typically involves gathering and transferring information out of the target network, which may involve moving files through multiple systems before they reach their final destination. Threat actors may compress or encrypt files (for example, with a utility such as RAR) to make the process easier and more secure. Compression allows the attacker to transfer a smaller volume of data out of the environment. Encryption makes the stolen information difficult to identify while it is in transit.

Threat actors may use a variety of methods to move data out of the network, including staging data on a publicly facing web server where the data can be retrieved via HTTP, or using standard FTP to move files. Alternately, they may transfer files using encrypted network protocols (such as SSL or SSH), or via backdoors that use custom protocols. In both cases, the data transfer can be extremely difficult to detect.

APT31 typically uses password-protected RAR archives to collect data of interest and move it out of the victim network. APT31 appears to be very focused and selective in the data they steal, targeting specific types of data, rather than attempting to extract large amounts of diverse files.

RAR Archiver Publicly Available

### *Other*

Threat actors may use a variety of tools to conduct their activity. These tools do not always fit neatly into a specific phase of the attack lifecycle.

## Network Infrastructure

Network infrastructure refers to the computers, domain names, and online accounts that are acquired and maintained by a threat group to carry out their operations. These assets may be acquired legitimately (that is, by registering a domain name or buying access to a Virtual Private Server (VPS)) or they may be compromised assets that the group has hijacked, often without the knowledge of the legitimate owner.

### *Domains*

Threat actors often use domains for command and control (C2), particularly within malware. Because attackers can control the IP address to which a domain resolves, using domains gives them greater flexibility. If an infrastructure IP address is taken offline or discovered and blocked, the threat actor can simply update the DNS record to point to a new IP.

Attackers may register their own domains (zones and associated subdomains) through a domain registrar, either directly or using a third-party service or reseller. Alternately, threat actors may leverage dynamic DNS (DDNS) domains, where a DDNS provider allows customers to register a subdomain under a legitimate zone registered to the DDNS provider itself. These services often allow customers to register a certain number of subdomains free of charge, and provide software to allow customers to easily manage the DNS resolution of their domains.

Finally, threat actors may avoid registering domains and simply hijack legitimate domains for their own use. This is the case with strategic web compromises, but it may also include hosting malware on legitimate web sites where it can be retrieved by a first-stage downloader.

### *Domain Resolution*

Threat groups that use domains for command and control (C2) need to point their domains to IP addresses representing their infrastructure, typically using DNS A records. However, threat actors may also point their domains to innocuous IP addresses when the domains are not in use, in order to misdirect researchers and hide the true location of their infrastructure. Types of innocuous IPs may include:

- Non-routable IP addresses (including RFC1918, loopback, and broadcast IPs).
- Legitimate IP addresses, often belonging to well-known companies.

In addition, threat actor domains may resolve to other types of IP addresses:

- "Parking" IPs used by domain registrars to resolve domains that do not have a DNS A record.
- "Parking" IPs used by domain resellers who take over previously registered domains in an attempt to resell or otherwise monetize them.
- "Sinkhole" IPs used by security researchers who take over previously malicious domains in order to monitor network traffic to those domains.

For these reasons, not all IP addresses to which a threat group's domains resolve represent actual attacker infrastructure. However, the set of IP addresses and their locations still serves as a rough overview of threat actor activity.

| | |
|---|---|
| United States | 65% |
| Unknown | 8.5% |
| Japan | 8.1% |
| Russian Federation | 4.3% |
| United Kingdom | 3.0% |
| Germany | 2.6% |
| Korea, Republic of | 1.7% |
| China | 1.7% |
| Canada | 0.85% |
| Other | 4.3% |

*IP Addresses*

Identifying confirmed attacker infrastructure is a more complicated process than simply determining where threat actor domains have resolved. Valid infrastructure may be:

- inferred by the presence of hard-coded IP addresses within their malware or other tools
- identified through direct observation of threat actor activity
- identified through confirmed two-way communication with threat actor malware or tools (as opposed to mere beaconing)

It is also important to distinguish between infrastructure that is actually controlled by threat actors, as opposed to infrastructure that they use (such as TOR exit nodes).

IP addresses used for this group's infrastructure have been identified in the following countries:

| | |
|---|---|
| United States | 62% |
| United Kingdom | 12% |
| Singapore | 7.7% |
| Unknown | 7.7% |
| Korea, Republic of | 3.8% |
| Russian Federation | 3.8% |
| Thailand | 3.8% |

## First Version Publish Date

April 26, 2016 08:56:00 AM

## Version Information

Version:1.0, April 26, 2016 08:56:00 AM
APT31 Threat Group Profile

5950 Berkshire Lane, Suite 1600 Dallas, TX 75225

This message contains content and links to content which are the property of FireEye, Inc. and are protected by all applicable laws. This cyber threat intelligence and this message are solely intended for the use of the individual and organization to which it is addressed and is subject to the subscription Terms and Conditions to which your institution is a party. Onward distribution in part or in whole of any FireEye proprietary materials or intellectual property is restricted per the terms of agreement. By accessing and using this and related content and links, you agree to be bound by the subscription terms of service.

For more information on this or other FireEye products, please contact info@isightpartners.com.

For more information please visit: https://mysight.isightpartners.com/report/full/16-00005410