APT31 TECHNİCAL ANALYSİS REPORT

@echocti @echocti echocti.com

Contents

Executive Summary

APT31 is a cyber threat actor believed to be backed by the Chinese government and has been conducting large-scale cyber espionage operations against many countries and industries around the world. The group is also known by names such as Zirconium and Judgment Panda, and specifically targets sensitive government information, strategic industrial secrets and innovative technologies. APT31 specialises in advanced phishing attacks, supply chain attacks and the use of malware.

In this report, APT31's identity, targeted countries and sectors, associated campaigns, attack methods used, and IoCs are comprehensively covered. The group organises attacks against strategic sectors in the United States, the European Union and the Asia-Pacific region, threatening economic and national security in these regions.

APT31's activities have caused significant damage, especially in the defence industry, government agencies, technology companies and the energy sector. The malware and techniques used by the group make it difficult to detect attacks, enabling long-term access and data exfiltration operations. Moreover, APT31's competence in supply chain attacks increases its success in cyber espionage operations.

The Mitre ATT&CK table presented in this report comprehensively analyses the tactics and techniques used by APT31. In addition, the IoCs identified provide important information for measures and defence strategies to be taken against APT31's cyber attacks. This report aims to provide security teams with the information they need to take more effective security measures against APT31.

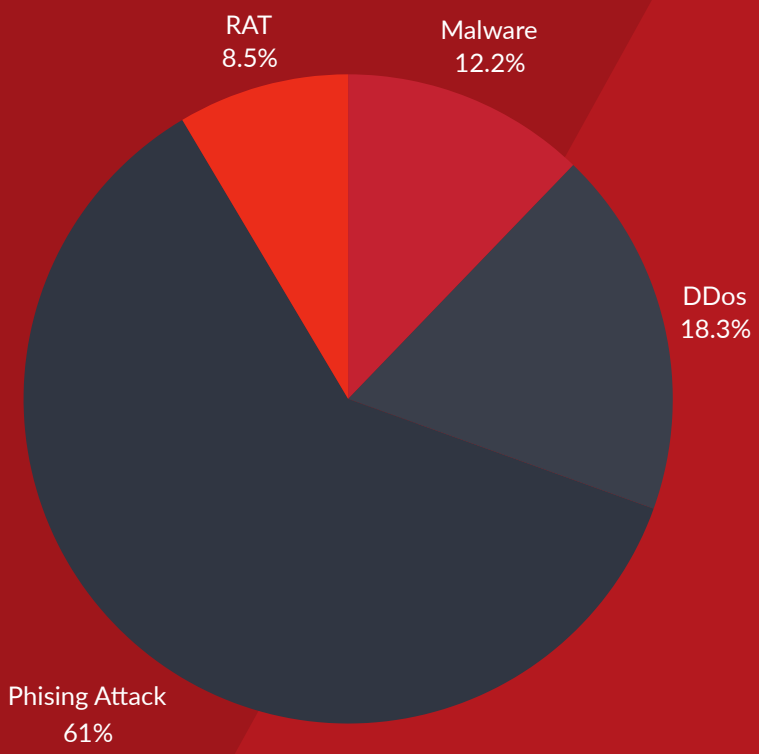
As a result, APT31's activities pose a serious threat not only to the targeted countries, but also to global cyber security. The findings and recommendations presented in this report provide guidance on measures to counter this threat.

Group Profile

This section provides detailed information about the general profile of APT31, who it is, the countries and sectors it targets.

Who is APT31?

APT31 is known as a state-sponsored threat actor based in China. The group's main activities include cyber espionage and intelligence gathering. APT31 organises long-term attacks against governments, military organisations and institutions operating in strategic sectors. This group, also known by other names such as Zirconium and Judgment Panda, aims to ensure persistence in the systems it infiltrates using advanced techniques. This threat actor uses advanced phishing techniques, malware and supply chain attacks, especially to access sensitive information and steal industrial secrets.



APT31 is an Advanced Persistent Threat group with an intelligence collection mission on behalf of the Chinese government. Similar to other nation-state actors, the group focuses on data of interest to the People's Republic of China and its strategic and geopolitical ambitions, rather than specific verticals. Chinese adversaries are considered some of the most prolific state-sponsored cyber actors in the world.

Targeted Countries and Sectors

Countries Targeted by APT31:

1. United States of America
2. European Union countries (especially France, Germany, United Kingdom, Finland)
3. Asia-Pacific region countries (Japan, South Korea, India)
4. It targets many countries around the world, including Australia.

Sectors Targeted by APT31:

1. Defence and Aerospace: Military technology, research and development activities.
2. Government Institutions: Diplomatic and national security information.
3. Technology and Telecommunications: Innovative technologies, communication networks.
4. Energy and Infrastructure: Strategic energy data and critical infrastructure.
5. Health Sector: Biotechnology and pharmaceutical research.

APT31 Tarafından Hedef Alınan Kurumlar

- **State Institutions**
  - White House
  - Ministries
  - Parliament
- **Military Institutions**
  - Naval Academy
  - US China Maritime Studies
  - US Navy
- **Informatics and Telekom**
  - Audio Technology Companies
  - MFA Companies
  - 5G Service Provider Company
- **Industry**
  - Steel Company
  - Various Companies in the Aviation Industry
- **Finance and Law**
  - International Law Firms
  - Financial Rating Companies
  - Management Consultancy Companies
- **Civil Society**
  - Various newspapers and academics
  - Policy Experts
  - Demokrasi Aktivistleri
- **Health**
  - Research Hospitals
  - Laboratory

Cyber Attacks Associated with APT31 Group

- In March 2021, an attack on the Finnish parliament was linked to the China-linked APT31 group.
- In July 2021, the APT31 cyber espionage group carried out ongoing attacks on numerous French organisations.
- In 2021 and 2022, it targeted the emails of British parliamentarians.
- In February 2022, the APT31 group carried out a phishing campaign targeting Gmail users linked to the US government.
- In July 2023, Attacks on Air-Gapped Systems in Eastern Europe were associated with the APT31 Group.
- In March 2024, it targeted US organisations operating in US critical infrastructure sectors.
- New CloudSorcerer attacks against government organisations in Russia in July 2024 were associated with APT31.

In March 2021, the Finnish parliament the attack was linked to the China-linked APT31 group

The cyber attack on the Finnish Parliament in March 2021 was attributed by the Finnish Police to the China-linked APT31 group.

The Finnish authorities investigated a number of offences in connection with the attack, including heavy espionage, illegal access to the information system and violation of communication confidentiality. The offences were committed between autumn 2020 and early 2021.

Police suspected the involvement of the China-linked cyber espionage group APT31 in the early stages of the investigation and confirmed this attribution after further investigation. In addition, police authorities announced that they had identified a suspect.

Chief Detective Inspector Aku Limnéll of the National Bureau of Investigation stated that this long-term investigation revealed a complex criminal infrastructure used by nation-state actors. During the investigation, the Finnish Police Service cooperated with international organisations and the Finnish Security and Intelligence Service.

At the same time, the US government announced sanctions against two Chinese hackers, allegedly members of the China-linked APT31 group. These sanctions targeted Zhao Guangzong and Ni Gaobin, who organised malicious cyber operations against US critical infrastructure sectors. The US Treasury Department also sanctioned the Wuhan Xiaoruizhi Science and Technology Company (Wuhan XRZ), which the Chinese Ministry of State Security used as a front for attacks on US critical infrastructure sectors.

In 2021 and 2022, he targeted the emails of British Parliamentarians

In 2021, the China-linked APT31 group is almost certainly responsible for a cyber attack on the email accounts of British parliamentarians. GCHQ's National Cyber Security Centre (NCSC) assessed that these attacks specifically targeted parliamentarians who drew attention to China's malicious activities. During the same period, the compromise of the UK Electoral Commission's computer systems between 2021 and 2022 was also attributed to a Chinese state actor. In these attacks, it was assessed that threat actors captured important information from the Electoral Commission and e-mail data and that this information could be used by Chinese intelligence services in espionage activities.

In February 2022, the APT31 group conducted a phishing campaign targeting Gmail users linked to the US Government

Google announced that it has blocked a phishing campaign run by the China-linked cyber espionage group APT31. This campaign targeted Gmail users associated with the US government. The phishing campaign took place in February and was detected by the Google Threat Analysis Group. The Threat Analysis team stated that the campaign was not linked to the ongoing invasion of Ukraine. Google TAG director Shane Huntley confirmed that the IT giant successfully detected and blocked all phishing messages.

Attacks on Air-Gapped Systems in Eastern Europe in July 2023 Associated with APT31 Group

A Chinese-linked group is believed to be behind a series of cyber attacks on industrial organisations in Eastern Europe. These attacks involved sophisticated methods specifically designed to steal data from air-gapped systems.

The malware used in the attacks was divided into three main categories: Gaining remote persistent access, collecting sensitive information, and transferring collected data. Among them, a modular malware that infects portable drives to exfiltrate data from air-gapped systems stands out. This software is capable of profiling portable drives and exfiltrating data from isolated networks through these drives. Other types of malware used to steal data from local computers and transfer that data through cloud services were also involved in these attacks.

The group used different malware families in the attacks. These included software that offered a wide range of functions, such as uploading and downloading files, executing commands, reverse shelling, and erasing their own traces. In addition, software used for remote access and initial data collection has the ability to list running processes, identify connected devices, perform file operations, take screenshots and update itself. The use of cloud services for command and control shows that such services are increasingly being abused by threat actors.

In these attacks, the group targeted not only Windows systems, but also Linux systems. In attacks against some companies in South Korea, it was found that despite its simple structure, a backdoor software was used that uses encryption to avoid network packet detection and performs various malicious functions. These attacks reveal that the group poses a complex and sophisticated threat on both Windows and Linux platforms.

Targeted US entities operating in US critical infrastructure sectors in March 2024

The US Treasury Department announced that it will impose sanctions on two Chinese hackers (Zhao Guangzong and Ni Gaobin) who were allegedly involved in attacks against US critical infrastructure sectors by the APT31 group. These hackers were reportedly linked to the Chinese Ministry of State Security and carried out these attacks through a shell company owned by Wuhan Xiaoruizhi Science and Technology Company Limited, a Wuhan-based technology company.

The US Department of Justice has indicted seven Chinese nationals, including two members of the APT31 group, on charges of computer intrusion and wire fraud. For nearly 14 years, the group has targeted dissidents, companies and political officials in the US and abroad in pursuit of China's economic espionage and foreign intelligence objectives.

APT31's cyber espionage programme, conducted as part of China's Ministry of State Security, targets political opponents both inside and outside China, government officials in the United States and elsewhere, candidates, campaign staff, and American companies. The group has conducted global hacking campaigns targeting thousands of individuals and companies, gaining long-term access to their networks, email accounts and phone call records.

EastWind campaign: New CloudSorcerer attacks on government organisations in Russia in July 2024 linked to APT31

In late July 2024, a series of ongoing targeted cyberattacks against Russian government organisations and IT companies were detected. These attacks were carried out through phishing emails containing malicious shortcut attachments. The attackers spread malware that sent commands to devices using the Dropbox cloud service, through which they downloaded additional payloads. This attack campaign was dubbed EastWind, and tools used by the APT31 group and an updated CloudSorcerer backdoor were detected in the attacks.

The malware used in the attacks was particularly associated with the APT31 group. One of the key tools detected in the EastWind campaign is a malware called GrewApacha, which has been in use since at least 2021. It was also found that the CloudSorcerer backdoor was updated by the attackers to use popular network services such as LiveJournal and Quora profiles as initial C2 servers. During the attacks, a new backdoor called PlugY was also discovered, which has a complex command set similar to the code of the DRBControl backdoor.

In the EastWind campaign, attackers were able to infiltrate organisations using spear phishing emails. These emails were sent with RAR archives and targeted organisations' email addresses. To hide their malicious activity, the attackers used popular network services such as GitHub, Dropbox, Quora, LiveJournal, and Yandex.Disk as C2 servers. These methods made attack traffic difficult to detect and increased the impact of the attacks.

The EastWind campaign shows that APT31 continues to use advanced cyber espionage techniques, targeting government and IT organisations in Russia. The updated and sophisticated nature of the tools used in the attacks reveals that these threat actors are constantly improving their methods and increasing the threat level to their targets.

APT31's Attack Tactic

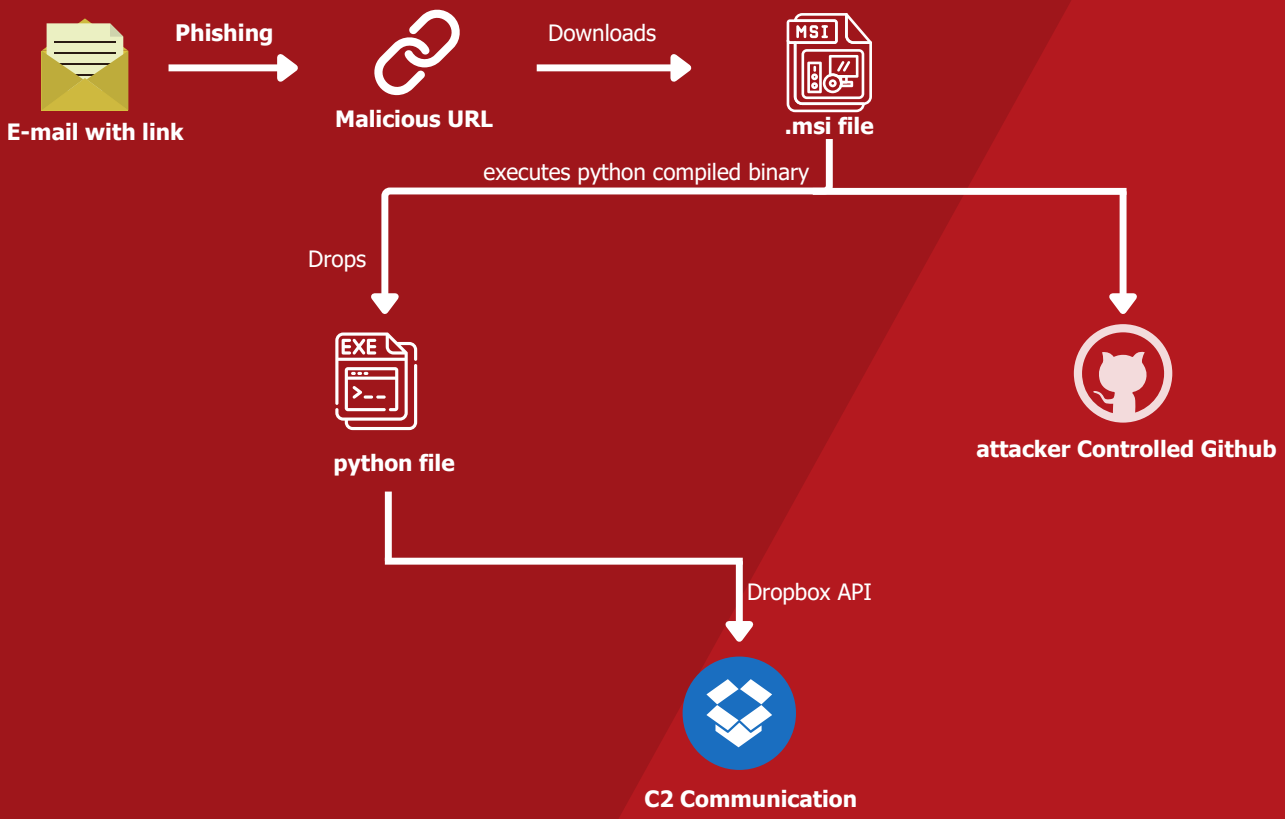
APT31 appears to have carried out its operations by adopting a two-stage strategy. In the first phase, victims were sent emails purporting to be from well-known US journalists. These emails contained excerpts from legitimate news articles and came with follow-up links. These links were most likely intended to lead to the original article. When victims clicked on these links, the attackers were able to gather preliminary information, such as the device on which the email was opened and the recipient's IP address. Between June and September 2018 alone, more than 10,000 such follow-up emails were sent.

The information gathered allowed attackers to launch direct attacks against victims' devices. In particular, APT31 targeted victims' family members, preferring to attack home routers rather than corporate networks protected by tighter security measures. The fact that APT31 carried out such attacks against home users was confirmed in a report published in December 2021.

As a tool, APT31 used a series of malware families in the first phase. This software was infiltrated into the system with DLL side loading technique. The attackers then turned to versions of CobaltStrike, a commercial penetration testing tool. For example, in one case, attackers targeted a subsidiary of a defence contractor that manufactures military flight simulators and gained access to the main network from this point. In this attack, a SQL injection was used after exploiting a local authorisation escalation zeroday vulnerability.

While it is noted that APT31 generally favours server-side exploits and minimises interaction with the victim, other activities targeting an activist group in Hong Kong indicate that attackers have also resorted to sending spoofed emails containing malicious attachments or links. It is also alleged that the attackers created fake Adobe Flash update pages to install malware. Another noteworthy detail is that APT31 has resorted to a strategy of using double-layered infections for some victims, regaining their access to the network even if the initial malware is detected.

APT31 Group's Attack Chain



ECHO

Mitre ATT&CK Table

Taktik	Teknik	Açıklama
Initial Access	Spear Phishing Attachment	Hedefli kimlik avı e-postalarıyla zararlı eklerin gönderilmesi.
Execution	PowerShell	PowerShell komutları kullanarak zararlı kod çalıştırma.
Persistence	Create Account	Hedef sistemde yeni kullanıcı hesapları oluşturma.
Privilege Escalation	Exploitation for Privilege Escalation	Sistem güvenlik açıklarını kullanarak yetki yükseltme.
Defense Evasion	Obfuscated Files or Information	Zararlı kodun algılanmasını zorlaştırmak için dosyaları gizleme.
Credential Access	Credential Dumping	Hedef sistemden kimlik bilgilerini toplama.
Discovery	System Information Discovery	Sistem bilgilerini toplama ve analiz etme.
Lateral Movement	Remote Services	Uzaktan erişim servislerini kullanarak sistemler arası hareket.
Exfiltration	Exfiltration Over C2 Channel	Komuta ve kontrol kanalı üzerinden veri sızdırma.

IoC's

IoC	Type
themicrosoftnow[.]com	URL
meeting[.]equitaligaiustizia[.]it	URL
137[.]74[.]76[.]92	IP
23[.]218[.]225[.]10	IP
28808164363d221ceb9cc48f7d9dbff8ba3fc5c562f5bea9fa3176df5dd7a41e	SHA256
e024fe959022d2720c1c3303f811082651aef7ed85e49c3a3113fd74f229513c	SHA256
d6b348976b3c3ed880dc41bb693dc586f8d141fbc9400f5325481d0027172436	SHA256
c0f93f95f004d0afd4609d9521ea79a7380b8a37a8844990e85ad4eb3d72b50c	SHA256
caeca1933efcd9ff28ac81663a304ee17bbcb8091d3f9450a62c291fec973af5	SHA256
de19e0163af15585c305f845b90262aee3c2bdf037f9fc733d3f1b379d00edd0	SHA256

How Can You Be Protected From Cyber Attacks?

If you want to ensure the security of your organisation in cyber space, there are some precautions to be taken.

Are There Vulnerabilities in the Software We Use?

If the software described as vulnerable is also used in your organisation, this software should be updated. If the software you use does not provide update support for a long time, a competing product should be used. Otherwise, attackers can access the network within the institution by taking advantage of these software vulnerabilities and damage the system by performing harmful behaviours on endpoint devices.

Has Personal Information of Our Employees Been Leaked?

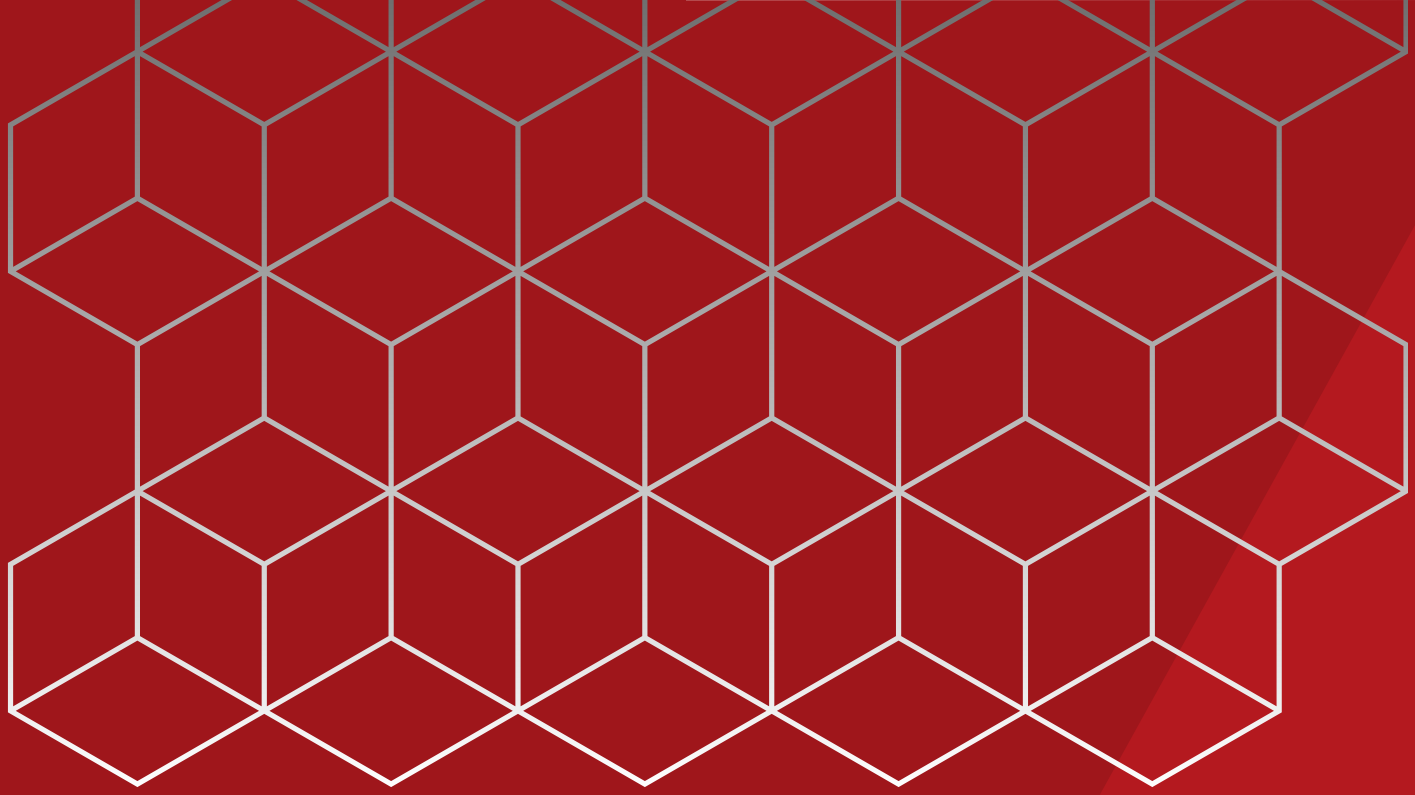
Especially corporate account information of corporate managers can be leaked due to third-party software. Phishing campaigns can be carried out using this leaked account information, or depending on the type and importance of the leaked account information, damage can be done to the organisation through the individual. In order to prevent these situations, personnel may be asked to change their corporate account passwords at certain periods.

Do Our Employees Have Sufficient Awareness on Cyber Security?

Perhaps the most important measure to be taken is human awareness. In particular, it is essential that employees who are relatively distant from the IT field but are in the same network receive cyber security awareness training. The defined employee profile is the first targets taken by cyber attackers. At this point, you can prevent this issue with awareness trainings.

To summarise,

Even in a situation where all precautions are taken, you may be cyber-attacked and damaged by this attack. The important thing is to minimise the potential damage.



ECHO

CYBER THREAT INTELLIGENCE