Credit: The Cyberthrone

Who is Fancy Bear?

Fancy Bear is a notorious state-sponsored hacking group that has been active since at least 2008. The group is believed to be associated with the Russian military intelligence agency. It has played a part in campaigns against businesses and organisations all around the world. The **_secpro** readership really picked a great (in a bad way...) APT for us to investigate next!

Known for using sophisticated and targeted techniques to infiltrate computer systems and steal sensitive information, the group has been linked to high-profile cyberattacks. This includes the 2016 attack during the U.S. presidential election.

This group is also known as APT28, Pawn Storm, Sednit, Strontium, and Sofacy.

Who did Fancy Bear attack?

They have been linked to a number of high-profile cyberattacks, including:

- The Democratic National Committee (DNC) in the United States in 2016 during the U.S. presidential election.
- The World Anti-Doping Agency (WADA) after it exposed a state-sponsored doping program in Russia.
- The German parliament, between 2015 and 2017.
- Emmanuel Macron's 2017 presidential campaign.
- The Organization for Security and Co-operation in Europe (OSCE), a target in 2016.

Just to be clear, this is not an exhaustive list. They have probably targeted many other organizations and high-profile individuals. That includes a 2020 attack on the Norwegian Parliament.

While the exact motivation behind Fancy Bear's cyberattacks is not always clear. The group is believed to have strong ties to the Russian government. Some experts suggest that the group focuses on gathering intelligence and disrupting the activities of foreign governments and organizations.

What tools and techniques do the Fancy Bear use?

Here are some of the tools and techniques that Fancy Bear uses, with reference to the MITRE ATT&CK framework:

Spearphishing (MITRE ATT&CK – T1566.002)

Fancy Bear uses spearphishing emails to deliver malware to their targets. They often use social engineering techniques to make the emails appear legitimate and convincing.

PowerShell (MITRE ATT&CK – T1059.001)

They use PowerShell to execute commands and download and execute malware on compromised systems. This technique is difficult to manage because PowerShell is a legitimate tool that is commonly used by system administrators.

Mimikatz (MITRE ATT&CK – T1003.001)

The threat agents use Mimikatz to harvest credentials from compromised systems.

Rundll32.exe (MITRE ATT&CK – T1218.011)

Fancy Bear has been known to use `rundll32.exe` to execute malicious code. Rundll32.exe is a legitimate Windows utility that is often used to load and execute DLLs, making it a useful tool for attackers to use to hide their malicious activity.

Remote Access Trojans (RATs) (MITRE ATT&CK – T1020)

Fancy Bear has been known to use RATs, such as XtremeRAT and Gh0st RAT. This is how they gain remote access to compromised systems.

DLL Side-Loading (MITRE ATT&CK – T1073.004)

Fancy Bear has been known to use DLL side-loading to execute malicious code on compromised systems. This technique involves replacing a legitimate DLL with a malicious one that is designed to execute the attacker's code.

Command and Control (C2) Infrastructure (MITRE ATT&CK – T1102)

Fancy Bear has been known to use multiple C2 servers to communicate with their malware on compromised systems. This makes it more difficult to detect and disrupt their operations.

What others groups use similar tools and techniques to Fancy Bear?

There are several APT groups that use similar tools and techniques to Fancy Bear. Some view this as a potential connection or shared tactic.

1. APT29 (Cozy Bear): APT29, also known as Cozy Bear, is another Russian APT group that is believed to have been active since at least 2008. Like Fancy Bear, APT29 has been known to use spearphishing, PowerShell, and DLL side-loading in their attacks.

3. Lazarus Group: The Lazarus Group is a North Korean APT group that has several high-profile cyberattacks to their name. Like Fancy Bear, the Lazarus Group uses spearphishing, RATs, and custom malware in their attacks.

4. Comment Crew: Comment Crew is a Chinese APT group that has been linked to a variety of cyberattacks, including the 2010 Google Aurora attack. Comment Crew has been known to use spearphishing, RATs, and custom malware in their attacks.

Overall, these APT groups share some similarities in their tactics, techniques, and procedures. This suggests that they may be a connection. However, it's worth noting that attribution of cyberattacks can be difficult and complex. Definitive links between different APT groups may not always be clear.

How closely do Fancy Bear and Cozy Bear work together?

Fancy Bear and Cozy Bear are both believed to be Russian APT groups that have been linked to various cyber espionage activities. They target similar industries and organizations, including government agencies. Some security researchers think that Fancy Bear and Cozy Bear may be different teams within the same Russian intelligence agency.

How do Fancy Bear differ from Cozy Bear?

While Fancy Bear and Cozy Bear share some similarities in their tactics and targets, there are also some clear differences.

Targeting

While both APT groups have been known to target government agencies, political campaigns, and technology companies, they have also had some differences in their specific targets. For example, Fancy Bear has been known to target Olympic organizations and anti-doping agencies, while Cozy Bear has been linked to cyber espionage activities targeting the US government and military.

Techniques

All three APT groups have been known to use spearphishing and custom malware in their attacks. But Fancy Bear has been known to use DLL side-loading to execute malicious code, while Cozy Bear uses zero-day exploits.

Attribution

While all three APT groups are believed to have links to the Russian government, there has been some debate among security researchers about the exact nature of these links. For example, some researchers have suggested that Fancy Bear and Cozy Bear may be different teams within the same Russian intelligence agency, while others have suggested that they may be separate groups with different objectives.

Are Fancy Bear worth worrying about?

Fancy Bear is a highly sophisticated APT group that has been conducting cyber-espionage campaigns for more than a decade. The group's ties to the Russian government remain a subject of debate. But, its tactics, targets, and malware are similar to other suspected Russian intelligence agencies. Fancy Bear is probably behind many high-profile attacks and continues to be a significant threat today. As such, it is crucial for organizations to remain vigilant and take steps to protect themselves from the group's tactics. This includes implementing robust cybersecurity measures and employee training programs.

In short: yes, absolutely.
