what is the MITRE ATT&CK :

The MITRE ATT&CK™ framework is a comprehensive matrix of tactics and techniques designed for threat hunters, defenders and red teams to help classify attacks, identify attack attribution and objective, and assess an organization's risk. Organizations can use the framework to identify security gaps and prioritize mitigations based on risk.

What is APT 28 :

Fancy Bear aka APT28. Fancy Bear, also known as APT 28, Sofacy, or Swallowtail, is a cyberespionage group that is linked to the Russian government. The group has been in operation since 2008, **targeting the energy, government, media, aerospace, and defense sectors via phishing campaigns and credential harvesting**.

APT28 reportedly compromised the Hillary Clinton campaign, the Democratic National Committee, and the Democratic Congressional Campaign Committee in 2016 in an attempt to interfere with the U.S. presidential election.In 2018, the US indicted five GRU Unit 26165 officers associated with APT28 for cyber operations (including close-access operations) conducted between 2014 and 2018 against the World Anti-Doping Agency (WADA), the US Anti-Doping Agency, a US nuclear facility, the Organization for the Prohibition of Chemical Weapons (OPCW), the Spiez Swiss Chemicals Laboratory, and other organizations.Some of these were conducted with the assistance of GRU Unit 74455, which is also referred to as Sandworm Team.

the APT28 espionage movement has mostly targeted national critical infrastrucutre in the USA, Europe and the countries of the former Soviet Union, including governments and militaries, security organizations, media entities,and dissidents and entities with conflict with the current Russian Government

APT28 steals internal data after compromising the victim and sometimes pub-licize them. Up to now, this group has been involved in the Syrian conflict, NATO-Ukraine relations, the European Union refugee and migrant crisis, the 2016 Olympics and Paralympics Russian athlete doping scandal, public accusations regarding Russian state-sponsored hacking

APT28 TACTICS :

We have observed APT28 rely on four key tactics when attempting to compromise intended targets. These include sending spear-phishing emails that either deliver exploit documents that deploy malware onto a user’s systems, or contain a malicious URL designed to harvest the recipients’ email credentials and provide access to the their accounts. APT28 has also compromised and placed malware on legitimate websites

intending to infect site visitors, and has gained access to organizations by compromising their web-facing server

INFECTION WITH MALWARE VIA SPEAR PHISH :

- Craft exploit document with enticing lure content.
  - Send exploit document to victim.
  - Victim opens document, and malware is installed by exploiting a vulnerability
  - (e.g., ARM-NATO_ ENGLISH_30_NOV_2016. doc leveraged an Adobe Flash exploit, CVE-2016-7855, to install GAMEFISH targeted machine).

- Register a domain spoofing that of a legitimate organization (e.g.theguardiannews[.]org).
  - Send link mirroring structure of legitimate organization's site that is designed to expire once users clickit.
  - Victim goes to link and retrieves malicious document or is served a web-based exploit that installs malware.
  - (Flash Vulnerability CVE-2016-7855 and Windows Vulnerability CVE-2016-7255 were exploited as zero days to install malware on victims who visited a malicious URL).
- WEBMAIL ACCESS VIA SPEAR-PHISH
  - Register a domain spoofing a webmail service or an organization's webmail portal (e.g., 0nedrive-0ffice365[.]com)
    - Send email to targets instructing them to reset their passwords
    - Recipient visits fake login page and enters credentials.
      - Send email to victims warning of security risk and asking them to enable security service.
      - Person is asked to authorize application to view mail and gives access.
    - APT28 uses stolen credentials to access mailbox and read email
      - APT28 leverages Oauth privileges given to malicious application to read email.
- INFECTION WITH MALWARE VIA STRATEGIC WEB COMPROMISE (SWC)
  - Compromise a legitimate site and set up malicious iFrame.
  - Users of the site are redirected using malicious iFrame and profiled
  - (e.g, this technique was used to compromise and infect visitors to numerous Polish Government websites in 2014).
  - Exploit is served to users matching the target profile and malware is installed on their system.
- ACCESS THROUGH INTERNET-FACING SERVERS
  - Network reconnaissance to find vulnerable software.
  - Exploitation of previously known vulnerabilities present on unpatched systems.

- Leverage initial compromise to access other systems and move deeper into the victim network.

APT28 Malware Suite

Tools	Role	AKA
Chopstick	Backdoor	Xagent,webhp,SPLM(v2 fybis)
Evil Toss	Backdoor	sedreco, AZZY, Xagent, ADVSTORESHELL, NETUI
Gamefish	Backdoor	Sednit, Seduploader, JHUHUGIT, Sofacy
Sourface	Down loader	Older Version of CoreShell , sofacy
Oldbait	Credentials	Sasfis
Coreshell	Down loader	New version of Sourface, Sofacy

Leveraging zero-day vulnerabilities in Adobe Flash Player,Java, and Windows, including CVE-2015-1701, CVE-2015-2424,CVE-2015-2590, CVE-2015-3043, CVE-2015-5119, and CVE-2015-7645.

MITRE-Attack

What is APT 32 :

APT32 is a suspected Vietnam-based threat group that has been active since at least 2014. The group has targeted multiple private sector industries as well as foreign governments, dissidents, and journalists with a strong focus on Southeast Asian countries like Vietnam, the Philippines, Laos, and Cambodia. They have extensively used strategic web compromises to compromise victims.

APT32 regularly used stealthy techniques to blend in with legitimate user activity:

- APT32 was observed using a privilege escalation exploit (CVE-2016-7255) masquerading as a Windows hotfix.
- APT32 compromised the McAfee ePO infrastructure to distribute their malware as a software deployment task in which all systems pulled the payload from the ePO server using the proprietary SPIPE protocol.

- APT32 also used hidden or non-printing characters to help visually camouflage their malware on a system. For example, APT32 installed one backdoor as a persistent service with a legitimate service name that had a Unicode no-break space character appended to it. Another backdoor used an otherwise legitimate DLL filename padded with a non-printing OS command control code

APT32 Malware and Infrastructure :

APT32 appears to have a well-resourced development capability and uses a custom suite of backdoors spanning multiple protocols. APT32 operations are characterized through deployment of signature malware payloads including WINDSHIELD, KOMPROGO, SOUNDBITE, and PHOREAL. APT32 often deploys these backdoors along with the commercially-available Cobalt Strike BEACON backdoor. APT32 may also possess backdoor development capabilities for macOS.

WINDSHIELD:

- Command and control (C2) communications via TCP raw sockets
- Four configured C2s and six configured ports – randomly-chosen C2/port for communications
- Registry manipulation
- Get the current module's file name
- Gather system information including registry values, user name, computer name, and current code page
- File system interaction including directory creation, file deletion, reading, and writing files
- Load additional modules and execute code
- Terminate processes
- Anti-disassembly

KOMPROGO :

- Fully-featured backdoor capable of process, file, and registry management
- File transfers
- Running WMI queries
- Retrieving information about the infected system
- Creating a reverse shell

SOUNDBITE:

- C2 communications via DNS
- Process creation
- File upload
- Shell command execution

- File and directory enumeration/manipulation
- Window enumeration
- Registry manipulation
- System information gathering

PHOREAL:

- C2 communications via ICMP
- Reverse shell creation
- Filesystem manipulation
- Registry manipulation
- Process creation
- File upload

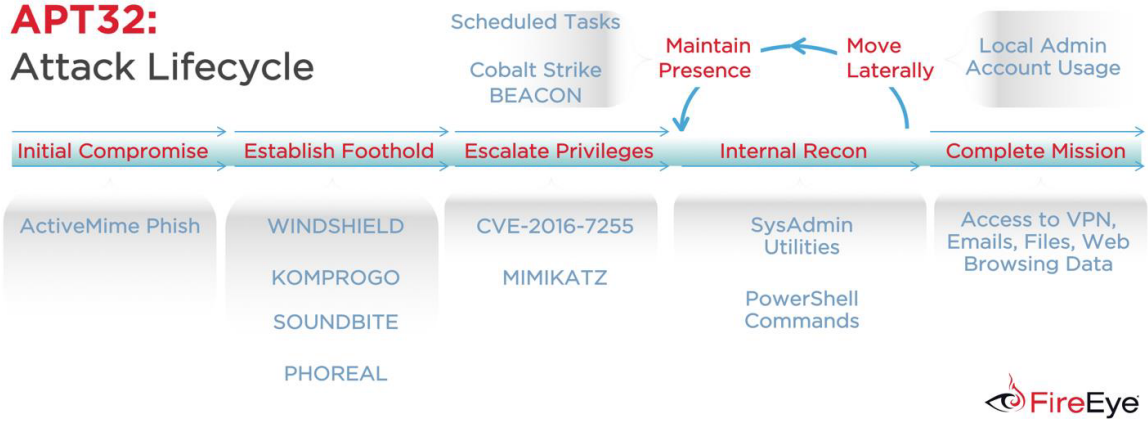
BEACON (Cobalt Strike) :

- Publicly available payload that can inject and execute arbitrary code into processes
- Impersonating the security context of users
- Importing Kerberos tickets
- Uploading and downloading files
- Executing shell commands
- Configured with malleable C2 profiles to blend in with normal network traffic
- Co-deployment and interoperability with Metasploit framework
- SMB Named Pipe in-memory backdoor payload that enables peer-to-peer C2 and pivoting over SMB

APT32 Malware and Capabilities :

APT32 operators appear to be well-resourced and supported as they use a large set of domains and IP addresses as command and control infrastructure. The FireEye iSIGHT Intelligence MySIGHT Portal contains additional information on these backdoor families based on Mandiant investigations of APT32 intrusions.

APT32:
Attack Lifecycle



FireEye