

# APT 32: Operation Cobalt Kitty

## Attack Lifecycle

### Background

- APT 32 (OceanLotus Group)
  - Operations coincide with Vietnamese state interests
- Targets:
  - private sector organizations
  - foreign governments
  - dissidents
  - Journalists
- [Cybereason Attack Lifecycle Publication](#)
- This attack was after trade secrets and proprietary information

### Attack Lifecycle Phases

- Penetration
- Foothold and persistence
- Command & control and data exfiltration
- Internal reconnaissance
- Lateral movement

### Penetration

- Obtained through social engineering
- Two types of spear-phishing attacks in email form
  - Link to site that downloads to a malicious fake Flash Installer that delivers a [Cobalt Strike Beacon](#) (Downloads encrypted payload with shellcode)
  - Word documents containing malicious macros which download Cobalt Strike payloads (Created two scheduled tasks that download additional payloads)
    - Scheduled tasks are run to establish CS Beacon
  - [Comparison to previous APT 32 attacks](#)

### Foothold

- Three main techniques used for persistence
  - Windows Registry Autorun
  - Windows Services
  - Windows Scheduled Tasks
- Windows Registry Autorun
  - VBScript and Powershell scripts were placed in the ProgramData folder
  - Scripts are being used to launch Cobalt Strike PowerShell scripts to establish a beacon to command & control server
  - Payloads were being hidden through NTFS Alternate Data Stream
  - A separate Outlook backdoor macro was established

- Used to communicate with the C2
  - To ensure this connection ran, a registry value was edited ("HKEY\_CURRENT\_USER\Software\Microsoft\Office\14\Outlook")
- Windows Services
  - Created and/or modified Windows Services to ensure the loading of the PS script
  - Exploited SearchIndexer.exe and SearchProtocolHost.exe (part of Windows Search Service) using [Phantom DLL Hijacking](#)
    - Dynamic Link Library (DLL) files contain a library of functions and other information that can be accessed by a windows program
    - Malicious "msfte.dll" file was placed in the system32 folder, the location of the vulnerable applications (allows for the malicious file to be loaded every time Windows Search Service launched)
- Windows Scheduled Tasks
  - Utilized scheduled tasks to ensure malicious payloads ran at specific times (less suspicious)
  - Google Update
    - Exploited the Google Update DLL
    - Inserted a malicious DLL (goopdate.dll) to run under the GoogleUpdate.exe which uses a scheduled task to look for new updates for google (each time the GoogleUpdate.exe was executed, the malicious file was executed as well)

## Communication

- Attackers used different techniques and protocols to communicate with the Command & Control servers:
  - Cobalt Strike Fileless Infrastructure (HTTP)
  - Cobalt Strike Malleable C2 Communication Patterns
  - Variant of Denis Backdoor using DNS Tunneling
  - Outlook Backdoor Macro as C2 Channel
  - Custom NetCat
- Cobalt Strike Fileless Infrastructure (HTTP)
  - Multi-stage payload delivery in the first phase of the attack
  - Low forensic footprint since most payloads are downloaded from the C&C and executed in-memory without touching the disk
  - Second stage is either Powershell or COM scriptlet:
    - Powershell downloader - a Powershell one-liner downloads and executes a Powershell payload from the C&C server
    - Regsvr32.exe downloader command - COM scriptlet is downloaded using regsvr32.exe
- Cobalt Strike Malleable C2 Communication Patterns
  - Analysis of the network traffic
- Variant of Denis Backdoor using DNS Tunneling

- Disguises the real IP and domain of the C&C server by having the backdoor communicate with known DNS servers (such as Google's 8.8.8.8 DNS server or OpenDNS's server)
- Doesn't communicate directly with the C&C servers
- Ensures that the backdoor's traffic won't be filtered by firewalls and other security products since most organizations don't tend to block common DNS servers
- Outlook Backdoor Macro as C2 Channel
  - Third phase of attack
  - Turns Microsoft Outlook into a C2 channel by replacing its original VbaProject.OTM macro container with a malicious one containing a backdoor functionality
  - Attackers are then able to send system commands via emails to exfiltrate data
  - Decoded malicious macro constantly looks for incoming emails containing specific strings
- Custom NetCat
  - Custom version of NetCat
  - Uses the previously installed backdoor to upload and execute this custom version of NetCat
  - To look less suspicious, the NetCat binary is renamed to something resembling a Windows update file or something similar

## **Internal Reconnaissance**

- Internal Network Scanning
  - Network scanning against entire ranges as well as specific machines
  - Attackers look for open ports, services, OS finger-printing, and common vulnerabilities
- Information Gathering Commands
  - Attackers use tools built into Windows to gather information on the environment's network and users
  - Tools include:
    - netsh
    - ipconfig
    - netstat
    - arp
    - net user/group/localgroup
    - nslookup
    - Windows Management Instrumentation (WMI)
- Vulnerability Scanning using PowerSploit
  - After Cobalt Strike Beacon is installed, attackers search for privilege escalation vulnerabilities to exploit on the compromised hosts
  - Utilizes parts of the PowerSploit project (which is no longer supported)

## **Lateral Movement**

- Obtaining Credentials

- Mimikatz
  - Gaining Outlook Credentials
- Pass-the-hash and Pass-the-ticket
- Propagation via Windows Admin Shares
- Windows Management Instrumentation (WMI)