Incident Report: Cobalt Kitty Campaign

Summary:

This report details the Cobalt Kitty campaign conducted by the OceanLotus threat group, also known as APT32, Ocean Buffalo, SeaLotus, TIN WOODLAWN, and APT-C-00. The campaign, which is believed to have begun in 2012, targeted multiple private sector industries, foreign governments, dissidents, and journalists, with a strong focus on Southeast Asian countries. The primary objective of the campaign was to collect information related to perceived threats to the Vietnamese government, with possible geopolitical and economic espionage objectives as well.

Attack Details:

OceanLotus used various initial access techniques to compromise their targets, including spearphishing links that directed victims to malicious sites downloading fake Flash Installers containing Cobalt Strike beacons and spearphishing attachments in the form of Word documents with malicious macros that downloaded Cobalt Strike payloads.

Once initial access was gained, the attackers used obfuscated and XOR-encoded PowerShell scripts to download additional obfuscated PowerShell payloads and Visual Basic scripts. These scripts were used to establish persistence through various means, including:

1. Creating scheduled tasks that downloaded additional payloads
2. Modifying Windows Registry Autoruns to execute VBScript and PowerShell scripts residing in the ProgramData folder
3. Implanting payloads in NTFS Alternate Data Streams for hidden execution
4. Creating scheduled tasks that loaded malicious PowerShell payloads using DLL hijacking with a Google Update binary
5. Creating and modifying Windows services to load PowerShell scripts
6. Utilizing malicious Outlook backdoor macros for C2 communication and data exfiltration

The attackers also employed DLL side-loading techniques, implanting a malicious DLL file that would be loaded by the Windows Search Service. This DLL then used Regsvr32.exe to download COM scriptlets for malicious execution.

To establish command and control, the attackers used various techniques, including:

1. Cobalt Strike's malleable C2 profiles to impersonate Amazon, Google Safe Browsing, Pandora, and OSCP traffic
2. DNS tunneling for C2 communication and data exfiltration
3. Malicious Outlook macros to utilize email for C2 communication and data exfiltration

OceanLotus conducted extensive reconnaissance on the compromised networks using built-in Windows tools to gather information on the environment's users, network configurations, open ports, services, and operating systems.

To harvest credentials, the attackers used a modified version of Mimikatz to dump credentials from the LSA Secrets. These credentials were then used to perform pass-the-hash and pass-the-ticket attacks for lateral movement.

Lateral movement was conducted using a combination of Windows Management Instrumentation (WMI), 'net user' commands, and SMB/Windows Admin Shares. The attackers also used RDP to move laterally to multiple hosts on the network.