Incident Report: Conti Ransomware

Summary:

This report details a Conti ransomware attack based on a DFIR report. The attack involved the use of phishing emails with malicious attachments to gain initial access, followed by the deployment of IcedID malware and Cobalt Strike for lateral movement, privilege escalation, and ultimately, the encryption of systems across the network.

Attack Details:

The initial vector used by the threat actor was a zip file delivered through a phishing campaign. The zip file contained a JavaScript file that, when executed, downloaded the IcedID malware. The IcedID DLL was then executed using rundll32.exe, establishing command and control communication over port 443.

The IcedID malware exfiltrated various attributes, such as computer name and OS version, via encoded cookie values. After a period of two days, during which the malware remained dormant, a Cobalt Strike Beacon was dropped and executed on the compromised system.

Using the Cobalt Strike Beacon, the attackers performed discovery activities using native Windows utilities, such as nltest.exe, whoami.exe, and net.exe, to gather information about the system, user accounts, permission groups, and remote systems on the network.

The attackers then escalated privileges to SYSTEM using Cobalt Strike's built-in "named pipe impersonation" (GetSystem) functionality. With these elevated privileges, they moved laterally to the domain controllers using SMB and executed a Cobalt Strike Beacon.

From the compromised domain controllers, the attackers performed network scanning to identify open ports and enumerate networks present in the environment. They then used RDP and PsExec to move laterally to other systems, deploying Cobalt Strike Beacons on a large scale.

To maintain persistence and evade detection, the attackers modified Group Policy to disable Windows Defender across the network. They created a new domain user account, "nuuser," and added it to the Administrators group, ensuring continued access to the compromised network.

Finally, the attackers executed the Conti ransomware across the network using the deployed Cobalt Strike Beacons, encrypting systems and disrupting the organization's operations.