APT1

Overview

APT1 is a Chinese threat group that has been attributed to the 2nd Bureau of the People's Liberation Army (PLA) General Staff Department's (GSD) 3rd Department, commonly known by its Military Unit Cover Designator (MUCD) as Unit 61398.

Tactics

APT1's strategy is to conduct long-term cyber-espionage against targeted organizations through Advanced Persistent Threat (APT) tactics. They use spear phishing attacks to gain initial access and maintain persistence to steal large amounts of sensitive information.APT1 focuses on industries of strategic interest to China, particularly English-speaking businesses, to conduct systematic intellectual property theft while remaining hidden through sophisticated infrastructure.

Techniques

1. **Techniques Used**: Account Discovery: Local Account, Acquire Infrastructure: Domains, Archive Collected Data: Archive via Utility, Automated Collection, Command and Scripting Interpreter: Windows Command Shell, Compromise Infrastructure: Domains, Data from Local System, Email Collection: Local Email Collection, Email Collection: Remote Email Collection, Establish Accounts: Email Accounts, Masquerading: Match Legitimate Name or Location, Network Share Discovery, Obtain Capabilities: Malware, Obtain Capabilities: Tool, OS Credential Dumping: LSASS Memory, Phishing: Spearphishing Attachment, Phishing: Spearphishing Link, Process Discovery, Remote Services: Remote Desktop Protocol, System Network Configuration Discovery, System Network Connections Discovery, System Service Discovery, Use Alternate Authentication Material: Pass the Hash
2. **Software used**: BISCUIT, Cachedump, CALENDAR, GLOOXMAIL, gsecdump, ipconfig, Lslsass, Mimikatz, Net, Pass-The-Hash Toolkit, PoisonIvy, PsExec, pwdump, Seasalt, Tasklist, WEBC2, xCmd

Procedures

APT1 attacks first unfold via spear phishing emails with malicious attachments that exploit known vulnerabilities (e.g. CVE-2012-0158) for code execution. After successful intrusion, APT1 will install backdoor software, such as WEBC2, to communicate with command and control servers via HTTPS to maintain persistent access privileges.APT1 will further use batch scripts and remote desktop protocols to collect system information including network topology, user credentials, and so on. Their goal is to steal sensitive corporate information such as business plans, technical designs, email content, etc. APT1's infrastructure consists of servers around the globe that regularly change communication nodes to evade detection and support long-term and stealthy attack campaigns.