Incident Report Analysis

Incident reported by

Full Name:	Craig Smith
Position:	SOC Analyst
Date:	11/11/23
Email:	securityteam@stc.com

Details of Incident

Incident No.	0001 (Conti Lab)
Date of Incident:	8th September 2021
Client Name:	Joes Fishshop
Type of Incident:	Data Breach, Ransomware, Phishing Attack

Incident Summary:

On September 8, 2021, an incident occurred on the network of WIN-AOQKG2AS2Q7.bellybear.local, indicating a security breach. The incident involves a sophisticated attack leveraging various techniques to compromise the system's integrity, confidentiality, and availability. The attack appears to follow a complex multi-stage process allowing the attacker to eventually encrypt the systems data whilst then deploying ransomware on the user's system. After careful research it is to my belief that the attack is known as Conti Ransomware and is used by Russia’s Wizard Spider Advanced Persistent Threat group (APT)

Incident Timeline:

1. **Initial Access:**
    - A malicious link was downloaded from a phishing email on the WIN-AOQKG2AS2Q7.bellybear.local system
2. **Execution:**
    - Powershell.exe was executed by NT AUTHORITY\SYSTEM to download an executable file that initiated a reverse connection to a C2 server
3. **Persistence, Defensive Evasion:**
    - Scheduled job was added to execute at a routine interval on the infected system to provide persistence, also in order to reduce the chance of detection the registry was modified.
      Scheduled Task/Job Execution - T1053 – Attempted to modify Windows Defender.
      Alert - The attackers created and modified Windows Services
      – Persistence – New Service (T1050)
      – Persistence – Modify Existing Service (T1031)
4. **Credential Access, Discovery:**
    - The attacker proceeded to extract OS credentials by retrieving memory from LSASS.exe, followed by traditional network traffic sniffing to detect other online systems. “whoami” executed by NT AUTHORITY\SYSTEM. Potentially gathering information about the current user, potentially for privilege escalation.
    - Net1.exe executed and to add the user ("securityninja") to the "Remote Desktop Users" group.
5. **Lateral Movement:**
    - Change Default File Association - T1042 - Unsecapp.exe created cmd.exe in the Administrator's documents folder.
    - Alert - DefaultUserModified

6. **Collection, Exfiltration:**

- Emails and local files were collected and prepared for exfiltration. MsMpEng.exe initiated a DNS query for detectportal.firefox.com. MsExchangeFrontendTransport.exe attempted a connection to port 25 (SMTP) from port 8940 to 10.10.10.6.

7. **Command & Control :**
    - The files were encoded and transmitted to the C2 server, which subsequently uploaded them to an external system controlled by the attacker
    - Alert – Metasploit - w3wp.exe initiated a connection to port 444 on 10.10.10.6
8. **Impact – Deployment Of Ransomware:**
    - Cmd.exe created readme.txt in C:\Users\Default\AppData\Roaming. The file confirmed the ransomware and provided instructions to move forward.
    - The ransomware was activated to disrupt the operations of the targeted organization

Attack Methodology Summary:

The cyberattack started with a phishing email that triggered the download of a malicious link. Using this initial access, the attackers established persistence by modifying the system's registry and creating scheduled tasks. They then proceeded to extract OS credentials and conduct lateral movement to expand their foothold within the network. This involved modifying default file associations and user privileges. Following this, they collected and prepared data for exfiltration, transmitting it to a command-and-control server controlled by the attackers. Finally, they deployed ransomware, causing significant disruption to the organization's operations.

Notes

Malicious File Activity

Numerous instances of file creation were observed, including the generation of potentially malicious files such as cmd.exe and readme.txt. Notably, cmd.exe, typically located in the system32 folder, was anomalously created within the administrator's directory. Subsequently, readme.txt was copied across various directories, containing information about the ransomware itself and instructions for the user to make payment. Objective being to get as much attention as possible

Network Connections

Suspicious network connections, especially outbound connections from critical system processes like w3wp.exe and MsExchangeFrontendTransport.exe suggested critical data was being transferred to an external server. Most likely used as blackmail for the ransomware

User Account Manipulation:

Unauthorized addition of a user ("securityninja") to the "Remote Desktop Users" group was identified. Evidence suggested that the default user account was modified