Aug 2024 - Sep 2024

Tactical Intelligence Development Report

TechGuard Inc., a major cybersecurity solutions provider with a diverse client base spanning financial services, healthcare, and critical infrastructure sectors, has recently been hit by a sophisticated and multi-faceted cyber attack. The attack appears to be part of a large-scale, coordinated campaign orchestrated by a well-resourced advanced persistent threat (APT) group known as "Specter."

Part 1

Investigation of the specific behaviors and techniques used by:

- **SpecterDrop**

When the victim clicks the malicious link of a phishing email, it deploys the multi-stage malware. The first and initial malware is ”SpecterDrop”, a Remote Access Trojan (RAT) malware, the attacker uses to gain full administrative privileges and remote control of a target computer. It also helps gain access to corporate accounts using sophisticated social engineering techniques, to bypass Multi-Factor Authentication. It establishes a persistent backdoor, allowing the attackers to maintain remote access even after the initial infection. This could involve modifying system settings or creating hidden processes.

Once the RAT is deployed inside the system it gets connected to the command-and-control server, which is controlled by the attacker, in this case, Specter Group. This connection is made possible by compromising an Open TCP port on the victim's machine. While SpecterDrop is inside the system, it is designed to communicate and deploy other malware, such as ShadowFrost.

- **ShadowFrost**

ShadowFrost is deployed on a victim's machine with the help of SpecterDrop. The purpose of this malware is also exactly designed to exfiltrate sensitive data and conduct lateral movement across the network. The malware uses a combination of legitimate administrative tools and custom exploitation techniques to escalate privileges and evade detection.

Exfiltration is made possible by using encrypted channels to avoid detection. For lateral movement inside the network, it may have used various techniques, such as exploiting vulnerabilities in network devices or exploiting compromised credentials.

ShodowFrost was responsible for deploying another malware, FrostLock, which is ransomware, encrypting critical files and demanding a ransom.

Analyzing malware impact on different parts of the organization's network and systems.

As the employees of the finance and operation department are targeted, the financial transaction systems, customer databases, and internal communication channels are showing signs of unauthorized access and data manipulation.

The combined actions of ”SpecterDrop” and ”ShadowFrost” had a significant impact on various parts of the organization's network and systems:

- **Compromised Accounts:** The initial compromise in employee accounts has led an unauthorized access to sensitive data of an organization.
- **Lateral Movement:** The ability to move laterally across the network allows the attackers to spread the infection and gain access to additional systems and cover from security.
- **Data Theft:** The exfiltration of sensitive data has resulted in financial loss, reputational damage, and legal consequences.
- **Disruption of Operations:** The ransomware attack and sabotage of backup systems have caused significant disruptions to the organization's operations.
- **Long-Term Consequences:** The attack has long-term consequences, such as more security spending, loss of customer trust, penalties, and fines.

By understanding the specific behaviors and techniques used by ”SpecterDrop” and ”ShadowFrost,” organizations can improve their security and prevent similar attacks in the future.

Part 2

Developing a tactical intelligence report that provides immediate response actions for mitigating the malware's effects:

No way completely ensures the protection from malware, precautions be adapted to reduce the probability of malware attack. So there must be a 'defence-in-depth' plan to give an immediate response to the breach. It will help to detect malware and stop it before it causes harm to the organization The following tactics will ensure to reduction of the impact and offer an immediate response to malware:

1. As soon the security analyst recognizes that a computer got infected, he/she must disconnect the system by:
    - Disabling its network approach.
    - Applying firewall rules to block all incoming and outgoing network traffic and data.
    - If immediately possible place the system in VLAN isolation.
    - Powering the system off.
2. If the attack is found in lateral movement, turn off Wi-Fi, disable the main network connection, and disconnect the internet. Also, segmentation of the network should be made immediately.
3. Immediately back up the data, assume that the attack could be ransomware, and store it in a safe location.
4. After understanding the motives and approaches of the threat actor, immediately place the backup server out-of-network site, assume that backup data might get infected, and apply the documented procedures for response.
5. Document all response actions, evidence, and decisions for legal and regulatory purposes.

High alerts and immediate actions must be ensured so that malware cannot communicate with its command-and-control servers. Strategies should be applied to give a hard time to threat actors.

Planing for addressing the ransomware component, decryption strategies, and recovery options:

Addressing

Usually, ransomware can not be detected and mitigated very easily, a analyst realizes the security alerts and patterns for identifying ransomware. The attacks occur in a matter of seconds, in about 43 minutes it can encrypt 100,000 files, so fast techniques should be employed to detect the ransomware before it's too late.

Ransomware and its components can be identified by following the techniques:

- A malware always carries some information with it like IP address, domains, and some other indicators, often called ”Signatures”. **Signature-based detection** which contains a library of signatures of malware, can be used at the right time to identify malware. However, this method can not be helpful when malware uses a completely new signature of malware.
- Ransomware behavior helps in detecting it. Normally, this behavior involves opening the files, and replacement of files with encrypted ones. **Behaviour-based detection** contains a detailed list of those behaviors and alerts the analyst when found and recognizes one.
- Ransomware not only encrypts the data but also steals it. This exfiltration may occur through the network channels, which can be identified. **Channel-based detection** can help in identifying those channels of abnormal traffic and create alerts to disconnect those channels.

The ransomware type and name can be identified by encrypted file extensions, like .aes-ni, Alcatraz, and .encrypted, etc

Decryption and Recovery

Relying on the attacker for the decryption key after paying for ransom, must be not adopted, as it is not guaranteed that the attacker communicate back after paying ransom in bitcoin, a normal ransom payment method, which has no trace back. So some strategies can be used to decrypt and restore the infected data.

It is not guaranteed that encrypted data could be decrypted without the key but still, strong technical methods can have a chance to decrypt it. Certain decryption tools, available on the internet, can be used to decrypt the data back if the ransomware is a common one. If not, a cryptographer expert can try reversing the encryption. Unfortunately, most of the time, both methods failed.

The last resort, contact the attacker which is, again, not recommended. Or use the backup data.