Hash: d14b48bae7484afe7942b7f21830a9561e8c49cb4cf4fa9ebbc1dc5b4573a375

Malicious Detections: 31

Malware Information:

Malware Analysis Summary:

Type: The malware is primarily identified as a Trojan and RTF (Rich Text Format) exploit. It is likely a dropper that exploits vulnerabilities in Microsoft Office to install additional payloads.

Detection Rate: The malware is detected by 31 out of 31 antivirus engines on VirusTotal, indicating a high detection rate among security vendors.

Behavior: The malware appears to exploit a vulnerability in RTF files, potentially using it to drop additional payloads on the victim's system. The exploit may use known vulnerabilities such as CVE-2015-1641 and CVE-2012-1856.

Potential Impacts: The malware can potentially lead to the installation of additional malicious payloads, which could include ransomware, spyware, and other types of malware. This could result in data theft, system compromise, and disruption of critical services.

Recommended Actions for Mitigation:

1. Ensure that Microsoft Office and associated software are up-to-date with the latest security patches.

2. Implement a robust antivirus solution and keep it updated to detect and remove the malware.

3. Use secure protocols for email attachments and limit the execution of macros from unknown sources.

4. Limit user privileges to prevent the malware from installing additional payloads.

5. Conduct regular system backups to ensure data integrity and availability in case of an infection.

6. Educate users on safe email practices and the risks associated with opening suspicious attachments.

7. Consider implementing a network intrusion detection system to identify and block suspicious traffic.

Hash: 01ec7b1066df7c55e262dc375bff5fd13a1fc9706c3db4b3522ac8b9d2453b52

Malicious Detections: 62

Malware Information:

Malware Analysis Summary:

Type:

The malware is primarily identified as a Trojan with various classifications, including detection of MSIL (Microsoft Intermediate Language), agent-based threats, and behavior associated with information stealers.

Detection Rate:

The detection rate is remarkably high, with 67 out of 67 vendors identifying the malware as malicious, and many assigning specific classifications and threat names.

Behavior:

The behavior of the malware is typically related to Trojans, which suggests that the malware may engage in malicious activities such as data theft, keylogging, and potential dropper functionality for additional malicious payloads.

Potential Impacts:

The potential impacts of this malware include the unauthorized collection and exfiltration of sensitive data, keylogging, and the potential deployment of additional malicious payloads.

Recommended Actions for Mitigation:

To mitigate the risks associated with this malware:

- Immediately quarantine or remove the malware from the system.
- Deactivate and re-scan the system using up-to-date anti-malware software.
- Change passwords, as the malware may have compromised login credentials.
- Implement stronger security controls, including firewalls, intrusion detection systems, and employee education on safe computing practices.
- Update all other software with the latest security patches and definitions.
- Perform a complete system scan and remediation to ensure no additional malicious files are present.
- Analyze network traffic for potential data leakage or malicious communication.
