|  |  |  |  |
| --- | --- | --- | --- |
|  |  | Malware Analysis  Otis Smith / Cybersecurity Professional / 11.28.23 |  |
|  |  |  |  |
| Pipette dropping liquid in a petri dish | | | |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | |
|  |  | TABLE OF CONTENTS |  |
|  |  | Summary …………………………..  Discovery……………………………  Vulnerability……………………….  Exploitation………………………..  References.………………………..  Mitigation………………………….. |  |



|  |  |  |
| --- | --- | --- |
| Summary |  | |
| The malware analysis focused on isolating and inspecting malware using virtual machines (VMs) and various analysis tools. The analysis involved setting up a Windows 10 VM and a REMnux VM, configuring network settings, and using tools such as Wireshark, Pestudio, and CyberChef to dissect and understand the behavior of a malicious Word document (REP\_89419812646634117.doc).  A hand holding a glowing city  Description automatically generated | |  |
| Discovery   1. VM Setup:  * Downloaded and imported MSEdge on Win10 and REMNUX VMs into VirtualBox. * Click on this link “[**MSEdge on Win10 (x64) Stable 1809**](https://drive.google.com/file/d/1cybdluIseTL48gwwh7uPt6k81CdvnRt1/view?usp=sharing)” to download the package.   A screenshot of a computer  Description automatically generated  Verify the file is loaded into the download folder.  A screenshot of a computer  Description automatically generated  Open “**Oracle VM VirtualBox Manager**” and click on “**File**” and “**Import Appliance….”** A screenshot of a computer  Description automatically generated  Review the inputs and hit on “**Finish**”  A screenshot of a computer  Description automatically generated  The new “**MSEdge-Win10**” has been created.  A screenshot of a computer  Description automatically generated  REMNux  Click on the link”[**this malware analysis VM (REMNUX)**](https://app.box.com/s/wf8pxzgo5cvrirglmeieqsrqkncera5c)” to download the file. A screenshot of a computer  Description automatically generated  Click on the “**Download**” and “**remnux-v7-focal-virtualbox.ova**” has been successfully downloaded in the download folder. A screenshot of a computer  Description automatically generated  Open “**Oracle VM VirtualBox Manager**” and click on “**File**” and “**Import Appliance….”A screenshot of a computer  Description automatically generated**  Review the inputs and hit on “**Finish**”  A screenshot of a computer  Description automatically generated  The new “**REMnux v7**” has been created.     * Configured network settings to create a controlled environment.   **MSEdge-Win10**  Put Windows VM in **Host-Only** mode.  Made sure the “**MSEdge-Win10**” is off and click on “Settings”A screenshot of a computer  Description automatically generated  Selected “**General**” on the left-hand side menu and click the “**Advanced”** and made show the “**Shared Clipboard**” and “**Drag’nDrop**” are set to “**Disabled**”A screenshot of a computer  Description automatically generated  Selected “**Network**” on the left hand side menu and click the “**drop down arrow”** , selected “**Host-only Adapter**” and “**Ok**”  A screenshot of a computer  Description automatically generated  The outcome information.A screenshot of a computer  Description automatically generated  **REMnux v7**  Move over the “REMnux” VM just to setup the “Network” Selected “**Network**” on the left hand side menu and click the “**drop down arrow”** , selected “**Host-only Adapter**” and “**Ok**”  A screenshot of a computer  Description automatically generated  The outcome information  A screenshot of a computer  Description automatically generated   * Modified default gateway and DNS settings for Windows VM to route through REMnux.Network Scanning:   Set both the “**Gateway**” and “**DNS with the “REMnux ip address**” of “**172.28.201.3**” then click “**OK**”  A screenshot of a computer  Description automatically generated  To verify the connection: open up a CMD command prompt in the Windows VM and ping the REMnux VM  Open command prompt and ran the ping command “**172.28.201.5**” and was successful.  A screenshot of a computer  Description automatically generated  Did the command “**ipconfig /all**” just to view the overall settings of the “**Host Name**”, “**IP**”, “**Subnet Mask**”, “**Default Gateway**”, “**DNS Servers**”. A screenshot of a computer  Description automatically generated   1. Windows VM Configuration:  * Disabled real-time protection in Windows Defender.   Click on the “**Show hidden Icons**” on the bottom righthand corner of the screen then select the “**Actions needed**” **Windows defender icon**”. A screenshot of a computer  Description automatically generated  Now, on the “**Windows Security**” window. Click on the “**Virus & threat protection**” icon. A screenshot of a computer  Description automatically generated  Scroll down to “**Virus & threat protection settings**” and click on “**Manage settings**”  A screenshot of a computer  Description automatically generated  Now, on the **Virus & threat protection settings**”, scroll down to Real-time protection and click is “**on**” to “**off**”.  Note: This is done due to prevent windows firewall for stopping or delecting the malware malicious file”A screenshot of a computer  Description automatically generated  This message will come up and click yes.  A screenshot of a computer  Description automatically generated  The Real-time protection is now turned to “**off**” then close all the boxes. A screenshot of a computer  Description automatically generated   * Extracted and examined the contents of the malicious ZIP file.   Right click on the folder and select “**Extract All..**”A screenshot of a computer  Description automatically generated  Double click on the shortcut to open the file **pestudio.exe file**. A screenshot of a computer  Description automatically generated  Open the **REP\_894198**  A screen shot of a computer  Description automatically generated  Click and drag the file into “**pestudio**” boxA screenshot of a computer  Description automatically generated  The file information is displayed in hashes. A screenshot of a computer  Description automatically generated  Next, select “**indicators (5)\***” to view the information. After reviewing the information. Noticed the file size was too large with “**5265 bytes**”A screenshot of a computer  Description automatically generated   * Analyzed the first 4 bytes of the malware file using HxD.      1. Malware Analysis with Pestudio:  * Overcame SmartScreen issues to run Pestudio.   By moving the file itself from the desktop and returning it back to its original location. Created a shortcut icon back to the desktop to ran the file successfully.  A screenshot of a computer  Description automatically generated   * Extracted **hash**, **indicators**, and **strings** from the malware.   **Hashes**  A screenshot of a computer  Description automatically generated  **Indicator Detail**  A screenshot of a computer  Description automatically generated  **Strings**    A screenshot of a computer  Description automatically generated   * Identified suspicious macros, including **'Macros/VBA/Frjpossu**,' **'Macros/VBA/Xhrcwkmbidam**,' and **'Macros/VBA/Xhrcwkmbidam**.'   A screenshot of a computer  Description automatically generated   1. Macro Analysis with CyberChef:  * Decoded and analyzed the obfuscated PowerShell commands.   A screenshot of a computer  Description automatically generated   * Split, decoded, and formatted the commands for better readability.   A screenshot of a computer  Description automatically generated | |  |
|  | |  |

|  |  |  |
| --- | --- | --- |
| Vulnerability |  | |
| 1. PowerShell Commands:  * PowerShell commands executed on Windows showed attempts to connect to suspicious URLs.   A screenshot of a computer program  Description automatically generated   * Encoded payloads indicated potential malicious activities.   A screenshot of a computer  Description automatically generated   1. Network Traffic:  * Analyzed network traffic using Wireshark, revealing connections to domains like **'amelano.net**,' **'911concept.com**,' **'ayonschools.com**,' **'beech.org**,' and **'firelabo.com**.' * Open a new terminal using the command “**Wireshark**” to open WireShark.   A screenshot of a computer  Description automatically generated   * Simulated internet traffic with **Inetsim** and observed DNS requests via **Fakedns**.   A screenshot of a computer  Description automatically generated | |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Exploitation | | |  | |
| 1. Fiddler Analysis:  * Monitored HTTP traffic with Fiddler, highlighting connections to the aforementioned suspicious domains.   A screenshot of a computer  Description automatically generated   * Examined requests for HTML documents from the simulated **INetSim HTTP server**.   Click on “**Website**” tab to view where it was directed to, and it show “**This is the default HTML page for INetSim HTTP server fake mode. This file is an HTML document**”A screenshot of a computer  Description automatically generated   1. Inetsim Simulation:  * Simulated internet traffic to emulate network interactions by starting **Inetsim**.   Use the command “**Inetsim**” to setup a fake internet simulator.  A screenshot of a computer  Description automatically generated   * Checked the report generated by **Inetsim** to analyze connection attempts and their destinations.   A screenshot of a computer screen  Description automatically generated | | | |  |
| References |  |  | |  |

1. Tools Used:

* VirtualBox, Wireshark, Pestudio, HxD, CyberChef, Fiddler, Inetsim.

1. Commands:

* Various commands executed, such as 'ipconfig,' 'ifconfig,' 'sshd status,' 'sshd start,' and others.

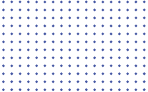
1. Files Analyzed:

* REP\_89419812646634117.doc and related extracted files.

1. Network Domains:

* amelano.net, 911concept.com, ayonschools.com, beech.org, firelabo.com.

.

Mitigation: 

1. Endpoint Protection:
   * Real-time Protection: Ensure that real-time protection features of endpoint security solutions are enabled to detect and block malicious activities.
   * Regular Updates: Keep endpoint protection software up-to-date to ensure the latest threat intelligence is applied.
2. Network Security:
   * Firewall Configuration: Implement and configure firewalls to monitor and control incoming and outgoing network traffic.
   * DNS Filtering: Employ DNS filtering to block access to known malicious domains and prevent connections to suspicious URLs.
3. User Awareness:
   * Security Training: Provide regular cybersecurity awareness training to educate users about the risks associated with opening suspicious email attachments and enabling macros.
   * Phishing Simulations: Conduct phishing simulation exercises to train users on identifying and avoiding phishing attempts.
4. Macro Security Settings:
   * Disable Macros by Default: Configure macro settings in office applications to disable macros by default, allowing them only from trusted sources.
   * Digital Signatures: Encourage the use of digital signatures on macros to verify their authenticity.
5. PowerShell Execution Policies:
   * Restricted Execution Policy: Enforce a restricted PowerShell execution policy to prevent the execution of PowerShell scripts without proper authorization.
   * Application Whitelisting: Implement application whitelisting to allow only authorized applications to run on endpoints.
6. Email Filtering:
   * Email Gateway Security: Deploy advanced email filtering solutions to scan and filter email attachments for malicious content before reaching end-users.
   * Attachment Sandboxing: Use email security solutions that sandbox and analyze attachments in a secure environment before delivery.
7. Incident Response:
   * Response Plan: Develop and regularly update an incident response plan to efficiently respond to and mitigate security incidents.
   * Monitoring Tools: Implement continuous monitoring tools to detect and respond to malicious activities in real-time.
8. Network Traffic Analysis:
   * Behavioral Analysis: Utilize network traffic analysis tools to identify abnormal patterns and behavior indicative of malicious activities.
   * Intrusion Detection Systems (IDS): Implement IDS to detect and alert on suspicious network activities.
9. Virtual Machine Security:
   * Isolation: Ensure proper isolation of virtual machines to prevent the lateral movement of malware within the network.
   * Snapshot and Restore: Regularly create snapshots of VMs before conducting malware analysis to facilitate quick restoration in case of issues.
10. Security Tool Validation:
    * Regular Testing: Validate the effectiveness of security tools through regular testing and validation exercises.
    * Tool Integration: Integrate different security tools to provide comprehensive coverage and enhance the overall security posture.
11. Continuous Learning and Research:
    * Stay Informed: Regularly update cybersecurity professionals on the latest malware trends, techniques, and tools through continuous learning and research.
    * Collaboration: Foster collaboration with the cybersecurity community to share threat intelligence and best practices.
12. Data Backup and Recovery:
    * Regular Backups: Implement regular data backups to ensure critical data can be restored in case of a malware attack.
    * Offsite Backups: Store backups in an offsite location to prevent data loss in the event of a network compromise.

By implementing these mitigation measures, organizations can enhance their overall cybersecurity posture, reduce the risk of malware infections, and improve their ability to detect and respond to malicious activities effectively. Regular training, proactive defense mechanisms, and a well-defined incident response plan contribute to a more resilient cybersecurity environment.

Report:

This analysis provided insights into the behavior of malware, potential vulnerabilities, and the network infrastructure exploited by the malicious document. It serves as a foundation for further investigation and mitigation strategies.