Department of Supervision, Central Office
Cyber Security and IT Risk (CSITE) Group

CONFIDENTIAL

Advisory No: 7/2024 **Dated: July 22, 2024**

Applicability: This advisory is applicable to Scheduled Commercial Banks (excluding Regional Rural Banks); Small Finance Banks; Payments Banks; Primary UCBs (Level 3&4)[1]; NBFCs (Medium, Top and Upper Layer)[2]; Credit Information Companies and All India Financial Institutions (EXIM Bank, NABARD, NaBFID, NHB and SIDBI).

Ransomware Incident

It has been brought to our notice that one of the Regulated Entities suffered a ransomware attack executed by the 'RansomHouse' group.

2. The incident details, modus operandi and recommendations are given as under:

a. Ransomware Attack exploiting MS-Exchange 'OWASSRF' vulnerability

The attack was carried out by leveraging MS-Exchange '**OWASSRF'** vulnerability (exploit method consisting of CVE-2022-41040 and CVE-2022-41082 to achieve remote code execution (RCE) through Outlook Web Access (OWA)).

b. Modus Operandi

- **Initial access:** The adversary gained initial access by obtaining valid credentials for Outlook Web Access (OWA), which was accessible from the internet, likely through brute force attacks or other infiltration techniques.
- **Exploitation:** Utilizing the compromised OWA credentials, the adversary exploited the OWASSRF vulnerabilities in Microsoft Exchange (CVE-2022-41040 and CVE-2022-41082). These vulnerabilities, involving a Server-Side

[1] As per RBI Circular DoS.CO/CSITE/BC.4083/31.01.052/2019-20 dated December 31, 2019 on 'Comprehensive Cyber Security Framework for Primary (Urban) Cooperative Banks (UCBs) – A Graded Approach'
[2] As per RBI circular DOR.CRE.REC.No.60/03.10.001/2021-22 dated October 22, 2021 on 'Scale Based Regulation (SBR): A Revised Regulatory Framework for NBFCs'

Request Forgery (SSRF) attack, allowed remote code execution under the elevated domain administrator privileges associated with the Exchange service account.

- **Backdoor Deployment:** After successful exploitation, the adversary executed encoded PowerShell commands via the Exchange Web process (`w3wp.exe`). This enabled to download and install Remote Monitoring and Management (RMM) tool 'TacticalRMM', ensuring persistent control within the compromised system.
- **Privileged Accounts Creation:** Leveraging the elevated existing Exchange service account (with domain administrator privileges), the adversary created new local and domain accounts. These accounts were added to privileged groups within the Exchange server and Active Directory, significantly expanding system access.
- **Lateral movement:** The adversary utilized Remote Desktop Protocol (RDP) and Windows Management Instrumentation Command-line (WMIC) to move laterally from the initially compromised Exchange server to other servers. Tools such as 'AnyDesk' and 'MeshAgent' were installed on the servers to solidify their foothold.
- **Command and Control (C2) Communication:** Using the deployed backdoors, the adversary established and maintained command and control channels. Additionally, no-profile PowerShell scripts were executed to establish communication with the threat actor's C2 infrastructure.
- **Network Scanning:** The adversary accessed Active Directory servers using WMIC and installed the 'Netscan.exe' tool. This enabled comprehensive network scans to identify additional targets and mapping out the network for further exploitation.
- **Malware Distribution:** Network shares on the Active Directory server were used to distribute malware to other windows servers within the network.
- **Data Exfiltration:** From the Active Directory server, the adversary accessed an internet-enabled server and deployed the 'Rclone' utility. This facilitated the systematic upload of critical data to adversary-controlled cloud storage.
- **Password Harvesting:** With administrative access to the backup application server, the adversary executed a PowerShell script to decrypt encrypted credentials using the Data Protection API (DPAPI). This provided credentials

used to connect to virtualization hosts such as vSphere, ESXi, and Hyper-V in plain text.

- **Remote Access to Virtualization hosts:** Using the obtained credentials such as 'root', the adversary achieved unauthorized SSH access to virtualization hosts.
- **Ransomware Payload Execution:** With root access on these virtualization hosts, the adversary executed ransomware payload.

3.IOCs

The IOCs pertaining to the incidents are given in **Annex I.**

4. Common Modus Operandi of Ransomware Attack and deficiencies

a. Entry Points

- Via-Exploiting the vulnerability of Internet facing asset, specifically web vulnerability in OWA. (Web application, Email)

b. Execution of Ransomware

- Fileless malware execution utilizing LOLBINs (Living Off the Land Binaries) – use of non-malicious binaries which are local to the operating system to camouflage their activities. (e.g., PowerShell, Regsvr32, Mshta, Certutil, Bitsadmin, Rundll32, WMIC, Cscript, WinRM, Macros, VBscript)
- Utilizing remote management and application deployment tools (e.g., 'Tactical RMM','MeshAgent')

5.Control Deficiencies

a. Lack of Multi-Factor Authentication (MFA):

- OWA access lacked MFA, enabling unauthorized access with compromised credentials.

b. Vulnerability Management:

- Failure to patch known vulnerabilities in Microsoft Exchange (CVE-2022-41040 and CVE-2022-41082) allowed exploitation via the OWASSRF vulnerability for initial access.

c. Access Controls:

- Inadequate protection of credentials led to unauthorized access to the backup application server.
- Role-based access management was not in place.
- Service accounts had elevated privileges, facilitating the creation of privileged accounts and lateral movement.

d. Network Segmentation:

- Lack of effective network segmentation allowed lateral movement from the Exchange server to other critical infrastructure.

e. Endpoint Detection and Response (EDR):

- Use cases were not configured in the SIEM system to identify specific threats and activities logged by the EDR system.
- EDR was not configured to alert the suspicious activities logged.

f. Logging and Monitoring:

- Installation of 'AnyDesk', 'rclone', and 'MeshAgent' was not reported or prevented by EDR or any other security tool.
- Inadequate logging and ineffective monitoring of RDP and SSH sessions, network scans, and data exfiltration activities.
- Appropriate SIEM use cases were not in place to detect 'creation of new local accounts and domain accounts', 'addition of users to privileged groups' and 'password harvesting attempts.'
- Scheduled tasks created by the adversary were not monitored, allowing automation of malicious activities and persistence without raising alerts.
- Failure to monitor SSH connections to virtualization hosts.
- Legitimate system tools like 'WMIC' and PowerShell were used to evade detection. These tools were not adequately monitored for suspicious use.

g. Network Security Controls:

- Network traffic was not adequately monitored to detect unforeseen network traffic and the spike in the network utilization during non-business hours.
- Internet access was enabled on servers, facilitating data exfiltration and communication with external command and control servers.
- Reverse connections from command and control (C2) servers were not adequately monitored, allowing persistent access and control over compromised systems.

6. Recommendations

i) [3]The RE's are advised to adhere to extant instructions.

ii) The IOCs specific to this incident are given in **Annex I**. A few Indicators of Attacks (IOAs) are detailed in **Annex II.** RE's are advised to leverage the information given

[3] Regulatory expectations in this color are already covered in the extant advisory digest or advisories issued in calendar year 2024.

in **Annexes (I and II)** and take proactive steps to monitor the network and secure the ecosystem.

iii) Conduct frequent reviews of 'active directory service accounts', 'privileged accounts', 'local accounts/groups', 'permitted network file shares and respective rights' to identify and mitigate security risks.

iv) Create separate role-based accounts for administration tasks and day-to-day operations to mitigate the risk of unauthorized access. This ensures a clear distinction of privileges for administrators.

v) Configure geo fencing wherever it is possible (such as firewall, email gateway, WAF, etc.) to restrict access based on geographic locations.

vi) Configure internet facing webserver service such as Exchange server with minimal "need to have" privileges.

vii) Enable comprehensive logging for all critical systems, including RDP sessions, network scans, and data access events. Implement and monitor Indicator of Attack (IOA) based use cases in SIEM.

viii) Monitor use of commands such as PowerShell, msbuild, wevtutil, psexec, wmic,certutil, bitsadmin, for abnormal usage with regard to time/workstation/user/process. Also check for unknown start up entries. Regularly update the detection rules to cover new 'LOLBin' techniques.

ix) Monitor and analyze network traffic for unusual patterns, such as spikes and large data transfers, by setting up alerts and investigating anomalies promptly.

x) Restrict internet access on servers. Restricted Internet access for whitelisted URLs through proxy may be given on need basis. Continuously monitor for internet connections initiated from servers.

Best Practices[4]

i) REs may consider implementing immutable backup solutions as per its risk assessment.

ii) REs may consider implementing whitelisting of applications at all servers as per its risk assessment.

[4] These are not mandatory. However, REs may consider implementing them

Annex I

<table>
<tr><th>Subject</th><th>Details</th></tr>
<tr><td>Suspected threat actor IP addresses</td><td>

85.239.54.103
45.66.249.226
188.34.207.137
172.64.162.16
172.64.163.16

</td></tr>
<tr><td>Suspected malicious file hashes</td><td>
<table>
<tr><td>0 c38c3147f25c450552ea9d9b54ad201e6201ed8</td></tr>
<tr><td>d4c3bdc6b0c1568553e2189f3aeac5b0851673af</td></tr>
<tr><td>24780657328783ef50ae0964b23288e68841a421</td></tr>
<tr><td>a5add09384665cee82c23dede6eb64c185cf953a</td></tr>
<tr><td>60854185f6338e1bfc7497fd41aa44c5c00d8f85</td></tr>
<tr><td>55447378c48561c35bad1317b58a34ee50c5072f</td></tr>
<tr><td>8a62d1fc576d963f388f2e137b0a1176e500108d</td></tr>
<tr><td>a279eb18dff8b3f0d8f27c1822ac7b2b9294a6ce</td></tr>
<tr><td>fe8cd9dce3f82e76f5a5651c60c72e638f826ade</td></tr>
<tr><td>1230ce6606fb20ae5d33c0c89f6a6f304dc997ff</td></tr>
<tr><td>92f14e8f4de6205818880d110b236e5f4f9d3b8a</td></tr>
<tr><td>f81ca755c559a50322a0aea959344c4c43e4d02e9616d40 61414675328dbbca1</td></tr>
<tr><td>753768cbba72d1054422caef2ace3bba944ac36e</td></tr>
<tr><td>3b345fe042442a8074039e76828213e289591b17</td></tr>
<tr><td>490e70172de71eeea57110e31bd7daf71fe83b08</td></tr>
<tr><td>af1c3816c62c5cf9abf1edf4662e4a9920d8ec3a</td></tr>
</table>
</td></tr>
<tr><td>Tools used during the attacks</td><td>

MeshAgent.exe
tacticalrmm.exe
AnyDesk.exe
new.exe
Setup.x86x64.Office2023Pro.exe
kitty_portable.exe

</td></tr>
</table>

	• netscan.exe • rsysdrv.exe • set.exe

IOCs of Ransomware attacks:

S.L No	IP Address
1	85.239.54.103
2	45.66.249.226
3	188.34.207.137
4	172.64.162.16
5	172.64.163.16
6	178.236.246.45
7	178.236.246.57
8	178.236.247.9
9	178.236.246.183
10	178.236.246.219
11	178.236.246.238
12	95.181.173.207
13	95.181.173.18
14	141.95.72.59
15	141.95.72.61
16	139.99.125.38
17	23.10.238.36
18	89.145.207.198

S. No.	C2 Domain
1	https://linkgostarbot[.dot]ir/bot/
2	5lvigv.dnslog[.]cn
3	663883c5.dnslog[.]store
4	mesh.accountsoutlook[.]com
5	http[:]//qualitygovt[.]ae/wp-includes
6	https[:]//transfer[.]sh/
7	https[:]//transfiles[.]ru/lxf03
8	https[:]//transfiles[.]ru/getFiles/3784421
9	remote.richardbate[.]com

Annex II

Possible Indicators of Attack (IoA)

a. Unauthorized Access and Privilege Escalation

- Multiple failed login attempts (Event ID 4625) indicate potential brute force attacks.
- Successful logins from unusual locations (Event ID 4624) suggest compromised credentials.
- Unexpected privilege assignments (Event ID 4672) indicate possible privilege escalation.
- Unusual account changes (Event IDs 4720, 4722, 4725, 4726) suggest unauthorized account activity.
- Unauthorized additions to privileged groups (Event IDs 4728, 4732, 4733) indicate potential backdoor creation.
- Changes in permission on sensitive objects. (Event ID 4670)

b. Persistence Mechanisms and Execution

- New unauthorized scheduled tasks (Event ID 4698) suggest persistence mechanisms.
- A typical process creation (Event ID 4688) indicates possible execution of malicious programs.
- PowerShell activity (Event ID 4104) indicates potential fileless malware execution.
- Loading of sensitive PowerShell modules (Event ID 4103).
- Unauthorized software installations (Event IDs 11707, 11724) suggest malicious tool deployment.
- Changes to audit policy settings (Event ID 4719) indicate attempts to evade detection

c. Network and Communication Anomalies

- Unexpected network connections (Event ID 5156) suggest command and control or data exfiltration.
- Unusual outbound data transfer using tools like ‘Rclone’ (Event ID 5158)
- Access to sensitive files by unusual users or processes (Event ID 4663) indicates potential data theft.

- Large outbound data transfers suggest data exfiltration (requires network monitoring).
- Outbound connections resembling reverse shell patterns indicate remote control attempts.
- Unusual or high internet activity by servers suggests data exfiltration or unauthorized communications.
- Suspicious DNS queries indicate potential attempts to contact malicious domains.
- Unusual ‘ICMP’ traffic from servers suggests potential reconnaissance or covert communication.

d. Evasion and Internal Scanning

- Use of legitimate processes like ‘w3wp.exe’ and ‘wuauclt.exe’ to run malicious PowerShell commands indicate sophisticated evasion techniques.
- RDP, SSH’, and ‘WMIC’ connection indicates unauthorized remote access attempts.
- High volumes of ‘SYN’ requests, failed connection attempts, and connections to unusual ports.