Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No.:104 **11-Sep-2020**

Name: High rise in the Targeted Ransomware Attacks on Critical infrastructure

Threat Classification: Ransomware

Summary:

According to recent Cybersecurity researches, there has been a huge increase in the number of Ransomware attacks with a seven-fold rise in campaigns compared with the last year. NetWalker, also known as Mailto, is a sophisticated family of Windows ransomware that is actively targeting Corporate networks, including the Government organizations and critical infrastructures. Two of the most common Vulnerabilities exploited reportedly are Pulse Secure VPN (CVE-2019-11510) and Telerik UI (CVE-2019-18935).

Indicators of Compromise (IOCs):

- https://image.communications.cyber.nj.gov/lib/fe3e15707564047c7c1270/m/2/FBI+FLASH+-+7.28.2020.pdf
- https://www.cynet.com/attack-techniques-hands-on/netwalker-ransomware-report/
- https://otx.alienvault.com/pulse/5e7921852f87a3cfbb4b2e6c

Recommendations:

- It is strongly recommended that the organization's **Security team** must perform **IOC sweeping** on every system running in enterprise environment as per above mentioned IOCs.
- **Backups, including offline backups of all critical servers and information systems** should be maintained. Ensure that an efficient Data Backup strategy is in place and practiced. e.g. backup copies of critical data should be maintained with 3-2-1 Backup Strategy, i.e. 03 Total copies of data, 02 of them Local on different Media's and 01 copy at a secure Remote/ DR site.

a. For Prevention:

- **Execution of PowerShell encoded and malformed commands or windows PowerShell altogether** must be blocked, if not required.
- Execution of **qeSw.exe, pw.exe, Invoke-Mimikatz.ps1, mimikatzN.exe, CORONAVIRUS_COVID-19.vbs, wce.exe, Invoke-mimikittenz.ps1, mimikatz.exe, t.exe, pwdump7.exe, dl.exe, rz.ps1**, **mshta.exe**, **cscript.exe** and **wscript.exe** files must be blocked on every system running in enterprise environment.
- **Execution of unsigned executables** from sensitive webservers and endpoints must be blocked.
- Implement strict **Software Restriction Policies/ Application Whitelisting** to **block unsigned executables** running from %**AppData**%, ***\StartMenu\Programs\Startup* and** %**TEMP**% paths.
- **Block Tor** (The Onion Router) **Gateways** as they are the primary means for ransomware threats to communicate with their C&C servers.
- Suspicious email attachments should be strictly monitored and blocked and the gateway level.
- **It is mandatory to enable 2-factor authentication** on every system running in enterprise environment.
- Apply **Geo-fencing** wherever possible.
- All updates and SCCM (Configuration Manager Servers if any) need to be hardened on priority based on industry best practices.
- **Privileged rights on Updates Servers, Domain Controller, Email Servers, Application Servers, Antivirus Servers** should be reviewed and reassigned only on need to know basis.
- Only whitelisted addresses of update portals, e.g. Microsoft, Kaspersky, CISCO etc. Firewalls should be allowed, with Deny all approach.
- **Only whitelisted software should be allowed to be used** within the environment and every software should have business justification and department head authorization before allowing into production use.
- Up-to-date and **Advanced Antimalware solution** should be in place for Enhanced Safety **enabled with Ransomware protection feature**.
- All antivirus/antimalware clients should be regularly check on host machines for their up and running state.
- All changes on end user machines should be restricted (e.g. installing software, giving admin rights and similar).
- **All unnecessary ports, protocols and services on end user machines and servers should be blocked**.

- Passwords of all privileged accounts (admin, root, super users etc.) need to be changed.
- Passwords change routine should be followed on all Access Points.
- Weak/ Insecure network protocols, and vulnerable applications should not be used.
- **Regular OS, Software, VPN and System Security patching** should be applied.
- **Regular awareness sessions** for the organization need to be planned especially on phishing and ransomware.

b. For Detection:

- All critical servers should have vulnerability assessment done and remediation for all critical, high and medium vulnerabilities should be done on priority.
- All **critical servers, information systems servers, privileged users and end machines/laptops should be monitored** for any abnormal activity or other signs of compromise.
- All critical Operating Systems, Services or Applications and Network device **Security logs should be retained (archived)** on a regular basis, and retention period should be in accordance with organization's Information Security policy and/ or obligations.

c. For Incident Response:

- In case of any similar incident, professional partner/vendor services should be available through service contract, NDA (Non-disclosure agreement) or similar.
- **Incident response Play books need to be prepared** for critical servers and need to be tested for any worst situation.