Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No.:113 **18-11-2020**

Name: Targeted Ransomware attacks on Web Hosting Providers

Threat Classification: Ransomware

Summary:

There has been a huge increase in the number of Ransomware attacks with a seven-fold rise in campaigns compared with the last year. It has recently been reported that one of the biggest providers of managed web hosting solutions, has taken down all its servers in order to deal with a ransomware attack. The attack impacted the company's public-facing web hosting systems, **resulting in customer sites having their data encrypted**.

Indicators of Compromise (IOCs):

A list of recent Ransomware IOCs and top most exploited vulnerabilities are available at following links:

- https://cis.verint.com/2020/08/17/global-ransomware-attacks-in-2020-the-top-4-vulnerabilities/
- 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/

Recommendations:

- It is strongly recommended that the organization's **Security/Technical team** must perform **IOC sweeping** on every system running in enterprise environment as per above mentioned IOCs links.
- **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

© Copyright 2020, Pakistan Telecommunication Authority. All Rights Reserved.
Unauthorized use, dissemination or modification of this document is strictly prohibited.

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:

- **Configure the host OS so that temporary files created by the Web server application are restricted to a specified and appropriately protected subdirectory and to the service processes that created the files.**
- **Configure the Web server so that only processes authorized for Web server administration can write Web content files.**
- **Dedicate a single hard drive or logical partition for Web content and establish related subdirectories exclusively for Web server content files, including graphics, but excluding scripts and other programs.**
- **Define a single directory exclusively for all external scripts or programs executed as part of Web server content (e.g., CGI, ASP).**
- **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.
- **All unnecessary ports, protocols and services on end user machines and servers should be blocked or disabled**.
- All updates and SCCM (Configuration Manager Servers if any) need to be **hardened on priority based on industry best practices**.
- **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.
- **Privileged rights on Updates Servers, Domain Controller, Email Servers, Application Servers, Antivirus Servers** should be reviewed and reassigned only on need to know basis.

© Copyright 2020, Pakistan Telecommunication Authority. All Rights Reserved.
Unauthorized use, dissemination or modification of this document is strictly prohibited.

- 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 checked on critical servers for their up and running state.
- All changes on end user machines should be restricted (e.g. installing software, giving admin rights and similar).
- Passwords of all privileged accounts (admin, root, super users etc.) need to be changed.
- 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 assets 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, please report to this office.

© Copyright 2020, Pakistan Telecommunication Authority. All Rights Reserved.
Unauthorized use, dissemination or modification of this document is strictly prohibited.