NETWORK INTELLIGENCE

The Digital Security Company

June 2023, Edition

SECURITY ADVISORY DIGEST

IN THIS EDITION:

Security Advisory Listing

- Piramal Group hit by BianLian ransomware attack
- 100K+ compromised ChatGPT accounts for sale on the dark web
- BlackCat claims the Reddit February breach and threatens to leak stolen data
- CoWIN Data Breach: Sensitive Information of Citizens Available on Telegram

Also Inside

Security Patch Advisory

Critical High Low

Date: June 30, 2023

Piramal Group hit by BianLian ransomware attack

RECOMMENDATIONS

1. Audit and control the execution of remote access tools and software on your network.

2. Restrict usage of remote desktop services like RDP and enforce stringent security measures.

3. Limit PowerShell use, update to the latest version, and enable enhanced logging.

4. Regularly audit administrative accounts and employ the principle of least privilege.

5. Develop a recovery plan with multiple copies of data stored securely and offline.

6. Adhere to NIST standards for password management, including length, storage, reuse, and multi-factor authentication.

7. Regularly update software and firmware, segment networks for improved security, and actively monitor network activity.

8. Apply the principle of least privilege to all systems and services so that users only have the access they need to perform their jobs.

REFERENCES

Piramal Group Cyber Attack: BianLian Ransomware Gang Lists Group as Victim

INTRODUCTION

The Piramal Group is an Indian multinational conglomerate with a presence across various sectors such as healthcare, life sciences, drug discovery, financial services, alternative investment and real estate.

On June 28, the BianLian ransomware group added Piramal Group to its victim list on the data leak site. The BianLian gang claims to have stolen 870 GB of data such as Financial, Project, Technical, Personal and Accounting info. Three months ago, the organization was also identified as a victim of the LockBit ransomware group.

In May 2023, the FBI, CISA, and the ACSC published a joint technical report on the BianLian gang highlighting the gang's transition from a file-encrypting ransomware operation last year to a pure data exfiltration & extortion gang this year.

The group typically gains access to victim systems via valid RDP credentials obtained from initial access brokers or through phishing. Post access, the group installs a custom backdoor & RMM software and creates or activates local administrator accounts. Next, it uses PowerShell and Windows Command Shell to disable tamper protection, Windows Defender and AMSI.

The actors use PsExec and RDP with valid accounts for lateral movement; Advanced Port Scanner, SoftPerfect Network Scanner, SharpShares and PingCastle tools to learn about the victim's environment; and FTP, Rclone tool, or the Mega file hosting service to exfiltrate data.

To pressure the victim into paying the ransom, the BianLian gang employed additional techniques such as printing the ransom note to printers on the compromised network and threatening the employees of victim companies via telephone calls.

LESSON LEARNED

- Vulnerability or misconfiguration issues in software and inadequate security control, often allow attackers to have easy access to sensitive data or gain initial access to cause further damages to cloud-based or on-premises IT Infrastructure.

SECURITY ADVISORY

Date: June 21, 2023

100K+ compromised ChatGPT accounts for sale on the dark web

RECOMMENDATIONS

1. To mitigate the risks associated with compromised accounts, ChatGPT users should update their passwords regularly and implement two-factor authentication.

2. Provide awareness among employees and management staffs to not accidentally upload or leak sensitive information on AI chatbot platforms such as ChatGPT. Exposure of personal data can have serious consequences, including identity theft and financial fraud.

3. If possible, limit the length of questions submitted to ChatGPT.

4. It is strongly recommended to provide guidance for customers on identifying and avoiding fraudulent emails, websites, and calls, and urge them to immediately report any suspicious activities to the bank.

5. Stay vigilant on all your account activities. Sign up for SMS and email alerts that can raise red flags in case of suspicious activity.

6. Ensure to be more vigilant while communicating over email or phone call, to eliminate risk of social engineering like phishing.

7. Pay close attention to false sense of urgency, electronic communications impersonating one of the company's vendors, requests for wire transfers

INTRODUCTION

Researchers have identified over 100,000 accounts of OpenAI's ChatGPT service sold on underground hacking marketplaces over the past year. May 2023 was the peak, with more than 26,802 accounts being offered for sale.

As ChatGPT stores the history of user queries and AI responses by default, unauthorized access to accounts might expose confidential or sensitive information of companies and their employees.

The logs containing ChatGPT accounts on underground marketplaces reveal that the victim systems were infected with Raccoon, Vidar, and Redline information stealers.

Most affected regions: Asia-Pacific, Middle East and Africa, Europe, Latin America, North America and CIS.

Top affected countries: India, Pakistan, Brazil, Vietnam, Egypt, United States, France, Morocco, Indonesia and Bangladesh.

LESSON LEARNED

- Lack of timely and informed cyber security awareness among employees and management staffs might lead accidental uploading and leaking of confidential data on platforms such as ChatGPT, Bard, or other similar Large Language Models (LLMs).

REFERENCES

Over 100,000 Stolen ChatGPT Account Credentials Sold on Dark Web Marketplaces

Group-IB Discovers 100K+ Compromised ChatGPT Accounts on Dark Web Marketplaces; Asia-Pacific region tops the list

SECURITY ADVISORY

Date: June 20, 2023

BlackCat claims the Reddit February breach and threatens to leak stolen data

RECOMMENDATIONS

1. Ensure to be more vigilant while communicating over email or phone call, to eliminate risk of social engineering like phishing.

2. Educate employees in terms of protecting themselves from threats like phishing's/untrusted URLs.

3. Ensure Microsoft Windows Workstations, Microsoft Exchange Server and Microsoft IIS Server are updated with latest security patches.

4. Use role-based authentication with temporary tokens where possible.

5. Use strong passwords and enforce multifactor authentication wherever possible.

6. Control MFA push with features such as number matching to improve user sign-in security. (Ex: Number matching in Azure MFA and number matching in Duo called Duo Verified Push)

7. Configure user email alerts for new MFA and MDM device enrolments. Configure alert on volume of push attempts per account.

8. Implement a FIDO2-compliant security key for multi-factor authentication

9. Pay close attention to false sense of urgency, electronic communications impersonating one of the company's vendors, requests for wire transfers.

10.Apply the principle of least privilege to all systems and services so that users only have the access they need to perform their jobs.

INCIDENT BRIEFING

Reddit is an American social news aggregation, content rating, and discussion website.

On June 16, BlackCat/ALPHV data leak site added 'The Reddit Files' and stated that the BlackCat actors 'broke into Reddit on February 05, 2023'.

On February 09, Reddit faced a 'highly-targeted phishing attack' & had docs and source code stolen. The TTPs used in the attack appear very similar to ScatteredSpider/0ktapus campaigns:

- a landing page impersonating its intranet site
- stolen employees' credentials and 2FA codes
- used Microsoft-signed POORTRY malware for defence evasion

BlackCat actors claim to have stolen 80 GB of data from Reddit, demanded $4.5 million ransom for the data to be deleted, and after failed negotiations, it's now planning to leak the data on the dark web.

The hackers stole internal docs, source code, limited contact information for a small number of company contacts and employees, advertiser information, and some internal dashboards and business systems.

LESSON LEARNED

- Timely internal security audits and careful reviewing of the reports can help organizations in detecting unusual activity and intrusion beforehand and take necessary actions to mitigate the risk pose by malware attacks and cybercriminals.

- Lack of timely and informed cyber security awareness among employees and management staff, which allows attackers to take advantage of such gaps in cyber security awareness programs, to trick employees and management staff into installing malicious software and giving out sensitive information via social engineering attack like phishing email, scamming, etc.

REFERENCES

Reddit hackers threaten to leak data stolen in February breach

Reddit Files: BlackCat/ALPHV ransomware gang claims to have stolen 80GB of data from Reddit

SECURITY ADVISORY

Date: June 12, 2023

CoWIN Data Breach: Sensitive Information of Citizens Available on Telegram

RECOMMENDATIONS

1. Download COVID-19-related applications only from verified sources.

2. It is strongly recommended to provide guidance for users on identifying and avoiding fraudulent emails, websites, and calls, and urge them to immediately report any suspicious activities to the bank.

3. Ensure to follow best cloud security practices and assure they are timely reviewed to eliminate any risk caused by access control or misconfiguration issues.

4. Ensure Internet-facing web services have robust monitoring capabilities and log retention policies to assist in the event of an incident.
5. Ensure MySQL server, Apache HTTP server, Apache Tomcat server, Confluence Server and Data Center are updated with latest security patches.

6. Ensure to apply latest security patch or use latest version of the third-party software.
7. Implement Bot protection and device fingerprinting capabilities to overcome dynamic IP attacks and achieving improved bot detection and blocking.

8. Implement Anti-DDoS measures on both Onpremise and cloud for real-time DDoS attack prevention.

9. Perform scans of your organization's network from the outside and identify and lock down the ports commonly used by VNC, RDP, or other remote access tools. And ensure these remote services are only allowed through VPN tunnels.

INCIDENT BRIEFING

On June 12, TMC's leader Saket Gokhale tweeted that the CoWIN portal data leak incident exposed the personal information of Indian citizens.

Saket Gokhale shared screenshots of a Telegram chatbot that is revealing personal details (such as mobile numbers, Aadhaar numbers, Passport numbers, Voter ID, details of family members, etc.) of all vaccinated Indians.

The data leak incident is yet to be verified. Union Health Ministry stated that they are working on a detailed report. It is yet to be disclosed how the data leak happened on Telegram.

LESSON LEARNED

- Vulnerability or misconfiguration issues in software and inadequate security control, often allows attackers to have easy access to sensitive data or gain initial access to cause further damages to cloud-based or on-premises IT Infrastructure.
- The incident highlights the importance of cybersecurity measures and the need for government to take all necessary steps to protect the citizens data.

REFERENCES

CoWIN Data leak! Aadhaar, PAN Card info, shared on Covid vaccination portal, made public by Telegram: Report

TMC's Saket Gokhale alleges data breach of senior politicians, others on CoWin

SECURITY ADVISORY

Security Patch Advisory

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

12th June 2023 – 25th June 2023
TRAC-ID: NII23.06.0.3

UBUNTU

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
Ubuntu Linux	USN-6158-1: Node Fetch vulnerability	• Ubuntu 20.04 LTS • Ubuntu 18.04 ESM	Kindly update to fixed version
Ubuntu Linux	USN-6159-1: Tornado vulnerability	• Ubuntu 23.04 • Ubuntu 16.04 ESM	Kindly update to fixed version

PALO ALTO

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
PAN-OS software	CVE-2023-0010 PAN-OS: Reflected CrossSite Scripting (XSS) Vulnerability in Captive Portal Authentication	• PAN-OS 10.2 versions before 10.2.2 • PAN-OS 10.1 versions before 10.1.6 • PAN-OS 10.0 versions before 10.0.11 • PAN-OS 9.1 versions before 9.1.16 • PAN-OS 9.0 versions before 9.0.17 • PAN-OS 8.1 versions before 8.1.24	Kindly update to fixed version
GlobalProtect app on Windows	CVE-2023-0009 GlobalProtect App: Local Privilege Escalation (PE) Vulnerability	• GlobalProtect App 6.1 versions before 6.1.1 • GlobalProtect App 6.0 versions before 6.0.5 • GlobalProtect App 5.2 versions before 5.2.13	Kindly update to fixed version

SECURITY ADVISORY

Security Patch Advisory

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

12th June 2023 – 25th June 2023
TRAC-ID: NII23.06.0.3

ORACLE

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
Oracle Linux	ELSA-2023-3714	• Oracle Linux 9 (aarch64) • Oracle Linux 9 (x86_64)	**Kindly update to fixed version**
Oracle Linux	ELSA-2023-3741	• Oracle Linux 7 (aarch64) • Oracle Linux 7 (x86_64)	**Kindly update to fixed version**

VMWARE

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
VMware Tools	**VMware Tools update addresses Authentication Bypass vulnerability (CVE-2023-20867)**	• VMware Tools versions 12.x.x, 11.x.x, 10.3.x	**Kindly update to fixed version**

SECURITY ADVISORY