NETWORK INTELLIGENCE

The Digital Security Company

March 2023, Edition 1.0

# SECURITY ADVISORY DIGEST

## IN THIS EDITION:

Security Advisory Listing

- Dissecting LimeRAT – A Simple yet Powerful Remote Access Trojan
- Indian pharma giant Sun Pharmaceutical Industries hit by security breach incident
- Team Mysterious Bangladesh launched cyberattacks against various Indian entities
- LastPass breach update: Hackers compromised DevOps engineers, installed a keylogger & stole password vault data

Also Inside

**Security Patch Advisory**

Critical High Low

Date: March 29, 2023

# Dissecting LimeRAT – A Simple yet Powerful Remote Access Trojan

## RECOMMENDATIONS

1. Block the threat indicators at their respective controls.

2. Disable unused remote access/Remote Desktop Protocol (RDP) ports and monitor remote access/RDP logs.

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

4. Ensure anti-virus and endpoint detection products are up to date with the latest signatures.

5. Refrain from opening untrusted links and email attachments without first verifying their authenticity.

6. Educate employees in terms of protecting themselves from threats like phishing/untrusted URLs.

7. Avoid downloading files from unknown websites.

8. Turn on the automatic software update feature on your computer, mobile, and other connected devices.

9. Use strong passwords and enforce multi-factor authentication wherever possible.

10. Enable Data Loss Prevention (DLP) Solutions on the employees' systems.

11.Keep all systems and software updated to the latest patched versions.

12.Prior to allowing VPN connections from remote endpoints, ensure that posture checking is configured to enforce a baseline set of security controls.

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

## INTRODUCTION

- LimeRAT is a Remote Access Trojan (RAT) that is designed to give attackers control over an infected system while evading traditional antivirus solutions.

- The malware is versatile and can perform various malicious activities such as keylogging, stealing passwords, capturing screenshots, executing arbitrary commands, downloading and uploading files, using the infected machine for crypto-mining or DDoS attacks.

- LimeRAT's code is obfuscated, making it unreadable, and contains a configuration class that appears to be encoded and encrypted. • LimeRAT's decryption algorithm involves generating a key by computing the MD5 hash of another string from the configuration class, copying the first 15 bytes and then the first 16 bytes of the computed hash to an array, and then decoding and decrypting the original string using the Base64 algorithm and the AES256-ECB algorithm.

- After decrypting the LimeRAT string, the malware can execute the instructions contained within it, including downloading additional malware, executing arbitrary commands, and stealing sensitive data.

## URL

https[:]//pastebin[.]com/raw/sxNJt2ek

## IP

20[.]199[.]13[.]167

SECURITY ADVISORY

Date: March 29, 2023

# Dissecting LimeRAT – A Simple yet Powerful Remote Access Trojan

## HASH (SHA-256)

| HASHES | DETECTED BY ANTIVIRUS | | | | | |
|---|---|---|---|---|---|---|
| | Symantec | TrendMicro | McAfee | Sophos | Microsoft | SentinelOne |
| 6d08ed6acac230f41d9d6fe2a26245eeaf08c84bc7a66fddc764d82d6786d334 | YES | YES | YES | YES | YES | YES |

## REFERENCES

LimeRAT Malware Analysis: Extracting the Config

SECURITY ADVISORY

Date: March 21, 2023

# Indian pharma giant Sun Pharmaceutical Industries hit by security breach incident

## RECOMMENDATIONS

1. Keep all operating systems and software up to date. Prioritize patching known exploited vulnerabilities.

2. Ensure to have a decent Antivirus program installed on computer.

3. Refrain from opening untrusted links and email attachments without first verifying their authenticity.

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

5. Avoid downloading files from unknown websites. 6. Use conditional access policies to prevent from attacks that leverage stolen credentials and session cookie by enabling policies such as compliant devices or trusted IP address requirements.

7. Continuously monitor for suspicious signin attempts with suspicious characteristics (for example, location, ISP, user agent, use of anonymizer services).

8. Monitor for unusual mailbox activities such as the creation of Inbox rules with suspicious purposes or unusual amounts of mail item access events by untrusted IP addresses or devices.

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

10.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).

## INCIDENT BRIEFING

Sun Pharmaceutical Industries Limited (d/b/a Sun Pharma) is an Indian multinational pharmaceutical company headquartered in Mumbai that manufactures and sells pharmaceutical formulations and active pharmaceutical ingredients (APIs) in more than 100 countries across the globe.

The Pharmaceutical giant disclosed in a BSE filing on March 2, 2023, that an information security incident has occurred at the company, and the impacted IT assets have been isolated. The company stated that the incident had not impacted core systems and operations. The company added that it is investigating the matter, and appropriate containment and remediation actions are being taken in a controlled manner to address the incident.

Currently, Sun Pharma hasn't disclosed details like how the breach happened, the attack vectors, the threat actor details and whether any data was stolen or not.

## LESSON LEARNED

Lack of endpoint security, use of admin account, using unpatched operating system, usage of commonly used passwords, reuse of same passwords across different platforms and failed to comply with security practices, often allows attackers to gain initial access onto the organization network and cause further damage

## REFERENCES


- Sun Pharma reports security breach, isolates impacted assets
- Sun Pharma reports "information security incident"; isolates impacted IT assets


SECURITY ADVISORY

Date: March 13, 2023

# Team Mysterious Bangladesh launched cyberattacks against various Indian entities

## RECOMMENDATIONS

1.Ensure Internet-facing web services have robust monitoring capabilities and log retention policies to assist in the event of an incident.

2. Send relevant log files from Internet-facing web servers to a SIEM or Syslog server.

3. Monitor child processes of web application processes for suspicious processes.

4. If possible, implement IP address access control lists (ACLs) in order to restrict access to Internet-facing systems.

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. Run regular dork queries to discover loopholes and sensitive information before attacks occur.

8. Do not store unencrypted secrets in .git repositories.

9. Securing APIs by filtering paths, understanding XML and JSON schemas for enforcement, and activity tracking mechanisms to trace bots and guard internal resources.

10. Implement Bot protection and device fingerprinting capabilities to overcome dynamic IP attacks and achieving improved bot detection and blocking.

11.Implement Anti-DDoS measures on both On-premise and cloud for real-time DDoS attack prevention.

12.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.

## INTRODUCTION

Team Mysterious Bangladesh, a group of pro-Bangladesh hacktivists, have targeted several Indian government and private entities in a wave of cyberattacks under the #OpIndia operation.

The threat group more likely used HTTPFLOOD (aka "./404FOUND.MY") and Raven-Storm tools to conduct DDoS attacks against Indian entities.

The HTTPFLOOD tool uses the HTTP flooding attack technique to manipulate and post unwanted requests to bring down a web server or application. The tool has been built in Python, and it takes the following three inputs: a target URL, a Proxy list and a number of threads (i.e. count of requests to be sent to the server).

The Raven-Storm tool uses multi-threading to send multiple packets at a single moment and get the target down. This tool is capable of server takedown, wifi attacks, and application layer attacks.

In December 2022, Team Mysterious Bangladesh claimed to have compromised the CBHE Delhi, India and leaked information about students from 2004 to 2022. The threat actors gained unauthorized access to the exposed admin panel of the CBHE Delhi (https[:]//www[.]cbhedelhi[.]com/) site using Google Dorking. The incident exposed sensitive information such as the name, Aadhar number, IFSC code, and other PII details of numerous individuals.

## REFERENCES


1. Team Mysterious Bangladesh planning another tide of attack over Indian entities
2. Indian Central Board of Higher Education Compromised by Team Mysterious Bangladesh
3. Bangladeshi hacktivist group targeting Indian govt websites, servers


SECURITY ADVISORY

Date: March 2, 2023

# LastPass breach update: Hackers compromised DevOps engineers, installed a keylogger & stole password vault data

## RECOMMENDATIONS

1. LastPass recommends customers to follow best practices around setup and configuration of LastPass.

2. Enable multi-factor authentication on your LastPass accounts so that threat actors won't be able to access your account even if your password is compromised. If MFA is already enabled, LastPass is recommending to regenerate MFA shared secrets in LastPass account settings.

3. It is recommended to reset LastPass master password and ensure that the master password isn't reused.

4. Review and Increase the iteration count settings for master password (minimum recommendation is 600000 rounds) via Account settings -> General -> Show Advanced Settings -> "Security" section -> Password Iterations field

5. If master password strength or iteration count were previously insufficient, LastPass suggests to temporarily disable the 2FA/MFA configuration -> delete the TOTP entry in the LastPass Authenticator -> re-enable 2FA/MFA configuration and -> re-enroll LastPass Authenticator

## INTRODUCTION

LastPass has provided a significant update on the investigation into the two security breaches it disclosed last year, in August and December.

During the two breaches, the threat actor stole 14 of 200 software repositories, internal scripts from the repositories containing LastPass secrets and certificates, technical information about the operation of the development environment, DevOps Secrets, cloud-based backup storage, backup of LastPass MFA/Federation Database and encrypted password vault data with decryption keys.

LastPass says that after the August incident, the threat actor behind the hack used the exfiltrated information to target one of its senior DevOps engineers. This attack leveraged a remote code execution exploit in a third-party media software toolkit to install a keylogger on the engineer's personal laptop.

Using the keylogger, the threat actor successfully captured the engineer's master password for the LastPass corporate vault, from where the actor stole passwords for the company's corporate network and AWS accounts.

The attackers used the stolen credentials to access the shared cloud-storage environment and exfiltrate sensitive data, including some of its customers' encrypted password vaults. Even if some LastPass cloud resources were encrypted, the company says the threat actor managed to obtain decryption keys from the engineer's device and password vault.

## REFERENCES


1. LastPass: DevOps engineer hacked to steal password vault data in 2022 breach

2. LastPass Reveals Second Attack Resulting in Breach of Encrypted Password Vaults


SECURITY ADVISORY

# Security Patch Advisory

| Severity Matrix | | | |
|---|---|---|---|
| L | M | H | C |
| Low | Medium | High | Critical |

20th March 2023 – 26th March 2023
TRAC-ID: NII23.03.0.3

## UBUNTU

| TECHNOLOGIES | ADVISORIES | AFFECTED PRODUCTS | RECOMMENDATION |
|---|---|---|---|
| Ubuntu Linux | USN-5963-1: Vim vulnerabilities | • Ubuntu 22.10<br>• Ubuntu 22.04 LTS<br>• Ubuntu 20.04 LTS<br>• Ubuntu 18.04 LTS<br>• Ubuntu 16.04 ESM<br>• Ubuntu 14.04 ESM | Kindly update to fixed version |
| Ubuntu Linux | USN-5964-1: curl vulnerabilities | • Ubuntu 22.10<br>• Ubuntu 22.04 LTS<br>• Ubuntu 20.04 LTS<br>• Ubuntu 18.04 LTS | Kindly update to fixed version |

## F5 NETWORKS

| TECHNOLOGIES | ADVISORIES | AFFECTED PRODUCTS | RECOMMENDATION |
|---|---|---|---|
| BIG-IP SPK, F5OS-A, F5OS-C, | K000133094: cURL vulnerability CVE-2020-8177 | • BIG-IP SPK 1.5.0 - 1.7.0<br>• F5OS-A 1.3.0 - 1.3.2<br>• F5OS-C 1.5.0 - 1.5.1 , 1.3.0 - 1.3.2 | Kindly update to fixed version |
| F5OS-A, F5OS-C | K000133092: cURL vulnerability CVE-2022-43552 | • F5OS-A 1.4.0 , 1.3.0 - 1.3.2<br>• F5OS-C 1.5.0 - 1.5.1, 1.3.0 - 1.3.2 | Kindly update to fixed version |

SECURITY ADVISORY

# Security Patch Advisory

| Severity Matrix | | | |
|---|---|---|---|
| L | M | H | C |
| Low | Medium | High | Critical |

20th March 2023 – 26th March 2023
TRAC-ID: NII23.03.0.3

## ORACLE

| TECHNOLOGIES | ADVISORIES | AFFECTED PRODUCTS | RECOMMENDATION |
|---|---|---|---|
| Oracle Linux | ELSA-2023-1403 | Oracle Linux 8 (aarch64)<br>Oracle Linux 8 (x86_64) | **Kindly update to fixed version** |
| Oracle Linux | ELSA-2023-1407 | • Oracle Linux 9 (aarch64)<br>• Oracle Linux 9 (x86_64) | **Kindly update to fixed version** |

## REDHAT

| TECHNOLOGIES | ADVISORIES | AFFECTED PRODUCTS | RECOMMENDATION |
|---|---|---|---|
| Red Hat Enterprise Linux | **RHSA-2023:1368** | • Red Hat Enterprise Linux for x86_64 9 x86_64<br>• Red Hat Enterprise Linux for IBM z Systems 9 s390x<br>• Red Hat Enterprise Linux for Power, little endian 9 ppc64le<br>• Red Hat Enterprise Linux for ARM 64 9 aarch6 | **Kindly update to fixed version** |

SECURITY ADVISORY