India Ransomware Report 2022

Enhancing Cyber Security in India

At a Glance

The prevalence of Ransomware threats continued its upward trajectory in the year 2022. In 2022, Ransomware gangs broadened their attacks across critical sectors with increased frequency and complexity. New ransomware variants emerged last year, as several profit-driven cyber criminals started their own campaigns aided by leaked source codes of established groups and the availability of readymade tool kits. Ransomware As A Service (RAAS) ecosystem with financial motive is becoming prominent with double and triple extortion tactics to cause successful business disruption, thereby forcing the victim to the pay ransom. Not only money, but Geo political conflicts also influenced ransomware attacks this year. This trend may continue further when Ransomware broadens its spectrum beyond financial aspects and becomes an arsenal for cyberwarfare's.

With phishing being the major pivot point for network initial access, attackers are continuing to exploit known vulnerabilities of public exposed applications and also focusing on acquiring valid credentials / session cookies of remote access services mainly through infostealer logs available in the dark web and underground forums. In addition, system misconfigurations, brute force attacks, unmanaged devices, insider threats and supply chain attacks are becoming concerning risk factors.

Much emphasis is required on ransomware prevention as the time, cost and efforts involved may become quite significant in responding and recovering from ransomware incidents. It is crucial to develop cyber resiliency with well-prepared & tested disaster recovery (DR) and business continuity plans (BCP) to avoid major business operational disruption in ransomware crisis times.

This report is focused on presenting the latest ransomware trends and attack methodologies pertaining to Indian cyberspace, which CERT-In has observed in the year 2022. The actionable preventive measures are discussed to improve ransomware resiliency and avoid significant business risks.

We hope, this report helps in reassessing the ransomware resiliency capabilities with a focus on defense in depth.

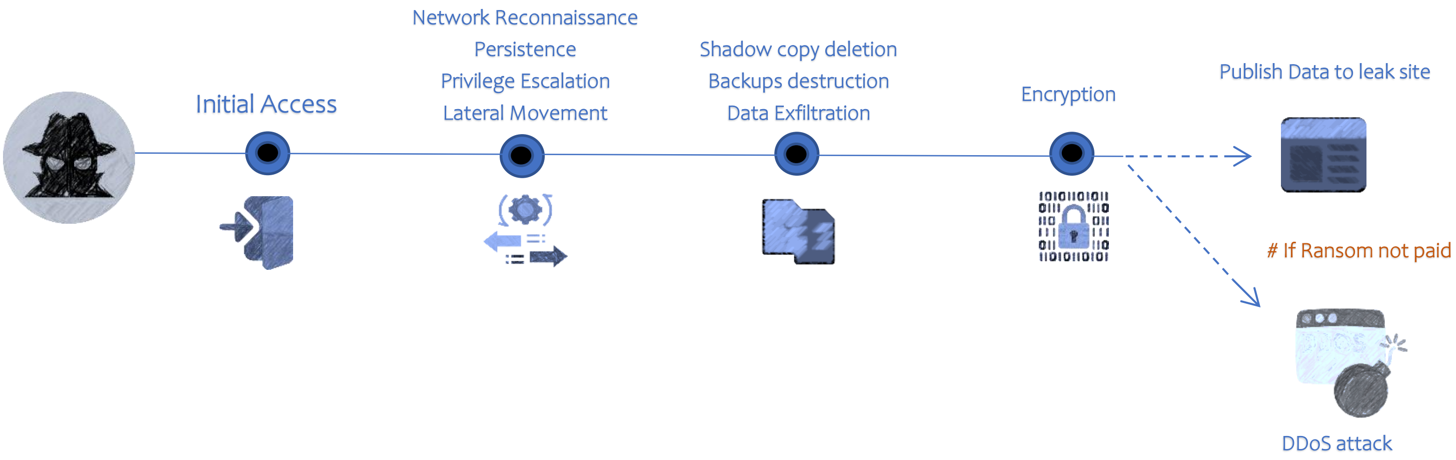
Ransomware - Introduction

Ransomware is a category of malware that gains access to systems and makes them unusable to its legitimate users, either by encrypting different files on targeted systems or locking the system's screen unless a ransom is paid. Ransomware actors also threaten to sell or leak any exfiltrated data, if the ransom is not paid.

Although there are countless strains of ransomware, they mainly fall into two main categories.

- *Crypto Ransomware* encrypts files on a computer so that they become unusable.
- *Locker Ransomware* blocks standard computer functions from being accessed.

Advanced Ransomware attacks follow several stages –



Initial Infection methods

For Organisations

⚠ Exploiting vulnerabilities in Internet-facing systems [Ex: VPN, Firewalls, Mail & Web servers]
⚠ Compromised credentials/Cookies
⚠ Phishing campaigns
⚠ Supply chain attacks
⚠ Insider Threats

For Individuals

⚠ Drive by Download, particularly from pirated/crack software advertising websites
⚠ Phishing/Spam Emails

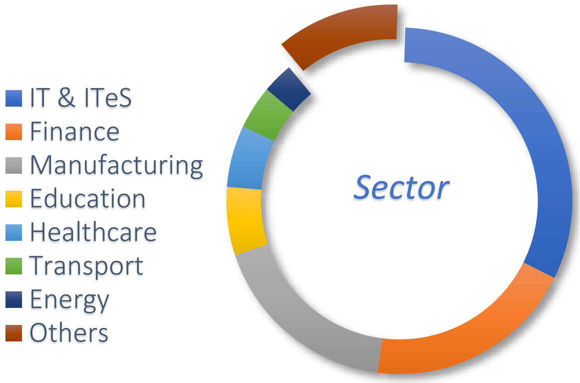
Ransomware -Trends

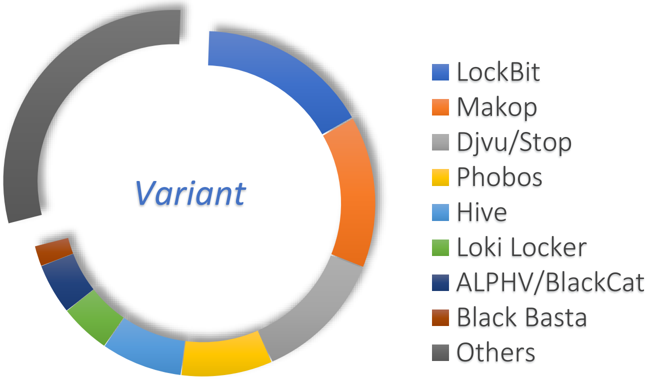
Sectors & Variants

Overall, there is **53%** increase in Ransomware incidents reported in 2022 Year over Year.

IT & ITeS was majorly impacted sector followed by Finance and Manufacturing. Ransomware players targeted critical infrastructure organisations and disrupted critical services in order to pressurise and extract ransom payments.

Variant wise, Lockbit was majorly seen variant in the Indian context followed by Makop and DJVU/Stop ransomware. Many new variants were observed in 2022 such as Vice society, BlueSky etc. Leaked Ransomware source codes are getting forked to launch new Ransomware brands.





At large enterprise level, Lockbit, Hive and ALPHV/BlackCat, Black Basta variants became major threats, whereas Conti which was very active in the year 2021 became extinct in the first half of the year 2022. Makop and Phobos Ransomware families mainly targeted medium and small organisations. At individual level, Djvu/Stop variants continued dominance in attacks over the past few years.

Ransomware -Trends

Vulnerabilities exploited

Most of the Ransomware groups are exploiting known vulnerabilities for which patches are available. Some of the product wise vulnerabilities being exploited are:

Microsoft Exchange:

CVE-2021 -34523: Proxyshell
CVE-2021 -34473: Proxyshell
CVE-2021 -31207: Proxyshell
CVE-2021 -26855: ProxyLogon

Citrix:

CVE-2020-8195: Unauthenticated Authorization Bypass
CVE-2020-8196: Improper access control
CVE-2019-19781: Directory Traversal
CVE-2019-11634: Incorrect Access Control

Fortinet:

CVE-2020-12812: Improper authentication
CVE-2019-5591: Information Disclosure
CVE-2018-13379: Directory traversal

SonicWall:

CVE-2021-20016: SQL injection
CVE-2020-5135: Buffer Overflow
CVE-2019-7481: SQL injection

Sophos:

CVE-2020-12271: SQL injection

Zoho:

CVE-2021-40539: Authentication bypass

Pulse Secure VPN:

CVE-2021 -22893: Authentication bypass
CVE-2020-8260: Remote Code Execution
CVE-2020-8243: Arbitrary Code Execution
CVE-2019-11539: Code Execution
CVE-2021 -11510: Arbitrary File Reading

Palo Alto:

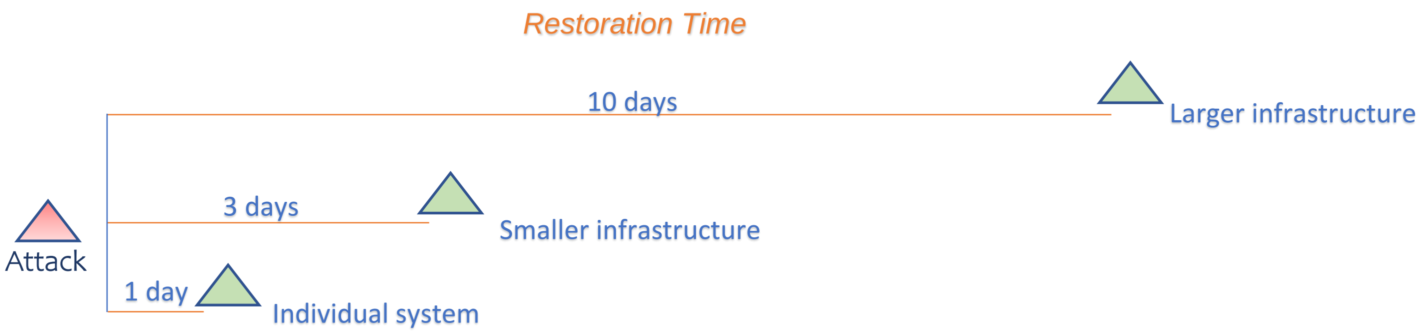
CVE-2020-2021: Authentication Bypass
CVE-2019-1579: Remote Code Execution

Ransomware -Trends

Restoration & Recovery time

Ransomware restoration & recovery time is dependent upon multiple factors like level of infection, affected applications, availability of backups & images, and Business Continuity preparedness. Time, efforts and cost involved are very much significant even with the availability of safe backups. It is essential to have tested Business Continuity Plan (BCP) to avoid major operational disruption. When Ransomware strikes, many organisations are clueless about scope of infection/blast radius. Lack of an updated IT inventory list, improper network segmentation and visibility gaps are the main reasons for ascertaining the level at which the infection has spread across the organisation, leading to enormous efforts in sanitisation of each and every system in the affected network. Also, rebuilding the applications may take considerable time, if golden images/backups are unavailable or inaccessible.

On an average, the restoration time is about 10 days for infections in reasonably large infrastructure networks. For smaller network/ infrastructure, the restoration time is around 3 days and for individual systems it is 1 day.



As Ransomware incident is a business risk, organisations must prepare themselves to face this havoc in an efficient manner-

1. Maintain current asset inventory to assist in determining components and devices that support critical operations
2. Plan how to continue operations if a critical system gets compromised
3. Develop work arounds or manual controls to ensure business operations
4. Regularly test Business Continuity Plans (BCP) including Disaster Recovery (DR) & backup procedures.
5. Incorporate automation in BCP and Recovery phases.

Ransomware -Trends

Ransomware gangs are becoming innovative in their approach to improve attack operational efficiency. Ransomware builders are focusing on speed and performance. Instead of encrypting entire file, a portion of file is getting targeted for encryption to save time. Multithreading is getting leveraged for faster encryption and decryption of files.

Attackers are using already existing Living Off the Land Binaries (LOLBINS) and legitimate tools available in sources like Github during the infection phases. In this way, they are successfully able to blind security solutions and disable the anti-malware applications, which makes their life easy for deployment and execution of encryptors. Safe boot restart is another technique adopted by Ransomware gangs in this context. Also, data exfiltration is getting destinated to reputed cloud storage to avoid flagging by firewall devices.

Prominent RAAS groups like LockBit are using novel methods such as launching bug bounty programs, to improve the quality of the malware. These groups are releasing new toolkit versions on regular basis with enhanced capabilities. Malware authors are using heavy obfuscation techniques to bypass static signature detections and hinder reverse engineering. Notable techniques include command line-based Ransomware execution using unique string argument for each victim entity. Ransomware authors are choosing light weight cryptographic algorithms to make the encryption process faster and efficient. Some Ransomware authors are switching to "Rust", a cross platform language to evade AV detections and enhance concurrency for encryption process.

Some groups are rebranding themselves and some are carrying out only low-profile attacks to avoid the attention of law enforcement.

As threat actors become sophisticated and swift in the attack process, organisations must level up their capabilities for monitoring and early detection of Ransomware infection.

As prevention is better than cure, it is desirable to understand the attack surface and ensure hardening of all internet-exposed assets and improve security posture to minimize the Ransomware attack probability. Targeted Ransomware attacks may not immediately disrupt the systems. Threat actors take time during attack phases for activities such as network enumeration, lateral movement. So, it gives the targeted entities an opportunity for threat hunting and detection of the intrusion at early stages. Early detection and mitigation of the Ransomware threat can minimize the impact and avert a crisis situation.

Rasomware –Trends

Legitimate tools & LOLBINs

Most of the Ransomware groups are trying to leverage already available legitimate tools and Living Off the Land Binaries (LOLBins) during the attack phases. This way, they are able to blind the security controls in the victim environment. After disabling end point Antivirus/EDR functionality, in later stages Ransomware custom encryptor is being dropped for execution.

Attack phases of network enumeration, persistence, lateral movement are mainly through already available tools in the operating system or via legitimate / open-source applications sourced from code repositories such as Github.

In many cases, Usage of post exploitation tool "Cobalt Strike" has become a common practice. Brute Ratel is also becoming a favourite choice apart from Cobalt Strike.

Ransomware gangs are commonly using Microsoft Sysinternals utilities such as PsExec for lateral movements.

Threat actors also started using tools like "Non Sucking Service Manager (nssm)" to install an executable as a service. nssm monitors the running service and will restart it if it dies.

Some of the observed LoLBINs and Legitimate tools were:

- Network enumeration
  Commands - net, ping, whoami, systeminfo
  Light weight tools - Advanced IP scanner, Netscan, Adfind, PinginfoView
- Persistence
  AnyDesk, ngrok, FRP (fast reverse proxy)
- Credential Dumping
  Mimikatz, quarks pwdump

It is recommended to refer to the following website for a list of "Living Off The Land Binaries, Scripts and Libraries"

- https://lolbas-project.github.io/

Defence -Active Directory

Active Directory is a directory service developed by Microsoft for Windows domain networks, which contains critical information about all users, endpoints, applications, and servers. Active directory sits at the heart of most organisations and would be considered a crown jewel information system. Threat actors always focus on reaching Active Directory (AD) after the initial compromise. Once privileged access is achieved in the domain controller, ransomware can easily target and attack the AD controlled assets through methods like logon scripts via a Group Policy Object (GPO), by leveraging WMI. Attackers generally try to leverage Active Directory database "ntds.dit" and SYSVOL for further attacks.

It is very important to protect Active Directory to the greatest extent possible. It helps in deterring Ransomware lateral movements and reduce the scope of infection.

Some of the hardening measures:

- Implement Principles of Least Privilege in AD Roles and Groups
- Restrict the use of privileged AD accounts and consider Multi Factor Authentication (MFA) for privileged AD accounts
- Disable the Local Administrator Account on all systems
- Consider using Local Administrator Password Solution (LAPS), if required
- Regularly audit security changes across Active Directory and Azure AD environments
- Implement Active Directory tiered administration model
- Use dedicated work station with secured configuration for Active directory
- Clean-Up Inactive User Accounts in AD
- Limit the software and roles installed on domain controllers

Refer:

https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory

May explore free AD security assessment tools like Ping castle, Purple Knight etc. to analyse the AD risks and for further closure of the security gaps.

- https://www.pingcastle.com/
- https://www.purple-knight.com/

But make sure to completely remove these tools and related files post assessment, as in the future these may become weapons for use by threat actors, if somehow they get access to the Active directory.

Defence -Network

It is very important to have organisation network level visibility to monitor and detect any malicious or suspicious network connections. Appropriate controls must be deployed to monitor perimeter level network traffic as well as within the internal networks.

- Maintain perimeter level security controls firewall/IDS/IPS with latest versions, updated signatures and fine-tuned rules
- Implement Geo-based traffic filtering, if feasible
- Ensure firewall configurations with features like Botnet filter, DPI-TLS inspection and sandboxing
- Block or restrict RDP and other non-essential ports, protocols & services at the network level
- Review and revamp the network architecture from a security preceptive:
- Segment the network using appropriate controls such as VLANs, internal firewalls, ACLs, SDN. Segment wireless LAN to separate internal network from guest users.
- Define zone to zone interaction so that only specific traffic allowed to pass between the zones.
- Ensure to implement secured remote access as per business requirement
- Maintain the network logs and monitor for alerts for any malicious or dark web traffic or unusual data egress traffic. Especially, keep a watch on network sessions involving newly registered domains
- Ensure restricted access to network level routers, switches, firewalls and other elements with strong authentication policy
- Based on the threat intel feeds, monitor or block malicious domains and IP addresses at appropriate levels of firewall, proxy server, DNS server etc. In case of identification of historical connections towards any malicious IP or domain, immediately trace out the possibly compromised host and investigate
- Deploy Anti-DDoS controls as some ransomware incidents may get associated with DDoS attack

May explore free tools like Real Intelligence Threat Analytics (R-I-T-A) to identify any suspicious network beacons, long connections and DNS tunnelling for further investigations. Threat actors generally attempt to initiate outbound connectivity from the compromised hosts to evade detection by security controls such as firewall. In such cases, usage of tools like R-I-T-A can be handy for network level threat hunting.

RITA framework ingests Zeek logs or PCAPs converted to Zeek logs for analysis.

- https://www.activecountermeasures.com/free-tools/rita/

Defence -Email

Email based phishing is one of the most prominent initial infection vectors in ransomware infections. Ransomware threat actors frequently engage in spear-phishing and Business Email Compromise (BEC) to harvest user & application credentials for obtaining access to organisation's network infrastructure. Also, visiting email embedded malicious domains or accessing malware attachments in emails may lead to ransomware infection.

Email security controls play crucial role in stopping malicious inbound emails.

- Implement Email security protocols:
  - Sender Policy Framework (SPF)
  - DomainKeys Identified Mail (DKIM)
  - Domain-Based Message Authentication, Reporting & Conformance (DMARC)
- Enable Multi Factor Authentication (MFA) for email access to deter Business Email Compromise (BEC)
- Configure native security settings, when using Microsoft 365 Exchange or Google Workspace
- Implement security features in Email gateway applications such as:
  - Anti-phishing
  - Anti-spam
  - Email content & attachment scanning
  - URL scanning & domain reputation scanning
  - Attachment sandboxing

Awareness is the key factor in defending against phishing campaigns.
There are multiple platforms that offer free phishing simulations to test staff preparedness

- KingPhisher: https://github.com/rsmusllp/king-phisher
- Gophish: https://getgophish.com/

Defence -Backups

To ensure ransomware resiliency, a backup maintenance policy plays a crucial role. Backups can be considered as the last line of defence against ransomware.

After initial access, Ransomware actors actively enumerate and infect/destroy any online backups to build pressure on the victim for negotiations on ransom payments. It is not only important to have latest offline backups but also regular testing is essential to ensure flawless quick recovery from safe backups.

The 3-2-1 backup rule may be adopted for data retention and storage:

- Keep at least three (3) copies of data.
- Store two (2) backup copies on different storage media.
- Store one (1) backup copy offsite.

As per the business case, one may opt for

1. External hard drives and disks
2. Tape Libraries
3. NAS Backup servers and solutions
4. Cloud storage

✓ Immutable WORM (Write Once Read Many) based backup solutions with delete protection are preferable.
✓ Maintenance of Snapshots with versioning can reduce recovery times (RTOs and RPOs).
✓ Golden image must be maintained for all critical applications
✓ Consider anti-malware controls in backup environment
✓ Consider placing backup servers in off-domain, workgroup mode, with a unique set of access credentials

Defence -End points

In targeted attacks, once Ransomware gains initial access to the network, it attempts enumeration, privilege escalation and lateral movement. In individual attack cases, the execution of encryptor happens by targeting files with certain extensions.

End point level some baseline controls must be enforced.

- Install and maintain updated Antivirus/EDR with scheduled scan settings
- Use standard user accounts and disable administrative rights, wherever possible
- Block/restrict RDP, SMB, PowerShell and other unwanted services
- Enable & configure Ransomware protection with Controlled folder access in window-based systems
- Keep the operating system, third party applications (MS office, browsers, browser Plugins) up-to-date with the latest patches
- Consider configuring the host firewall for controlling network traffic
- Ensure web browser protection controls
- Consider whitelisting the applications using Software Restriction Policy (SRP) and AppLocker
- Implement a strict External Device (USB drive) usage policy.
- Enforce baseline security policies for Bring Your Own Device (BYOD)
- Ensure to encrypt critical data both at rest and in transit
- Consider implementing Data Leak Prevention

Defence -Hypervisors

CERT-In has observed a rise in Ransomware attacks targeting virtualised infrastructure where in a single shot several VMs hosted critical applications can be disrupted to cause a major impact. Data centres with virtualised infrastructure deployment like VMWare ESXI and Hyper-V may face severe downtime, if sufficient measures are not undertaken.

Threat actors often use vCenter/ESXi command line interface “esxcli” to enumerate and shutdown the virtual machines to start the encryption process.

- Avoid usage of root access credentials
- Close active remote shells whenever not in use
- Restrict access to all management interfaces with proper segmentation and MFA
- Restrict/Disable SSH access to ESXi hosts and block unused ports
- Consider using ESXi Lockdown mode
- Enable “execInstalledOnly” to prohibit execution of custom code inside ESXi
- Consider disabling AD accounts for admin level access to ESXi
- Consider UEFI Secure Boot on the physical servers
- Avoid exposure of vCenter/ESXi hosts to internet

Defence -End users

Without awareness among End users /Employees & Third parties, no security control will be enough to protect the digital assets.

- Educate the end users on cyber hygiene, digital privacy, password management, safe browsing & remote work practices
- Train the end users on usage of AV/EDR tool that is installed in the systems
- Regularly conduct training and simulation sessions on topics like social engineering, phishing, Ransomware and Drive by download campaigns
- Intimate the employees about their roles and responsibilities in cyber security and process to detect and report the incidents

Defence-Access control

Credential compromise due to Info-stealer malwares is a growing concern as it is becoming a network access opportunity for RAAS affiliates. Initial access brokers (IAB) are advertising network access in dark web/underground forums, mainly sourced through stealer malware associated campaigns.

- Enforce Password change policies, Idle session timeouts, especially for accessing internet facing applications
- Enforce Multi Factor Authentication for access to critical assets
- Implement Least Privilege Access
- Avoid usage of common passwords
- Maintain strong password policy

Defence-Cloud

Threat actors are actively targeting publicly accessible cloud workloads with the objective of data exfiltration and subsequent data wiping. It is essential to understand the shared responsibility model to secure the cloud hosted resources.

- Regularly audit for misconfigurations & insecure default settings in the cloud infra
- Set strong IAM policies with principle of least privilege
- Set up the ability to recover apps and data in the cloud
- Update instances and container images regularly
- Monitor the cloud instances with appropriate security controls

Defence-Policies & Procedures

- Plan and implement policies for
    - Inventory management -Software & Hardware level
    - Patch management –
      Prioritize patching of public facing applications, specifically for
        - VPN/RDP applications
        - Firewalls
        - Email servers
        - Endpoint Management platforms
        - Web servers
    - Identity & Access management
    - Business Continuity Planning & Backup management
    - Third party risk management

Ransomware Incident Response

- Organisations should develop and test Ransomware Incident Response plan
- For necessary guidelines on Ransomware crisis response measures, the following resources may be referred.
  - *https://www.csk.gov.in/documents/RANSOMWARE_Report_Final.pdf*
  - *https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2022-0023*

Be prepared to face the Ransomware crisis with defence in depth approach and tested incident response plan

Report Ransomware incidents to CERT-In and other applicable regulatory / law enforcement agencies

Contact & Coordinate with CERT-In to get support in Ransomware incident response

For more information & technical assistance

Contact

Indian Computer Emergency Response Team
E-mail: incident@cert-in.org.in
Phone: 1800-11-4949
FAX: 1800-11-6969
Web: https://www.cert-in.org.in