INDIA

RANSOMWARE

REPORT

H1-2022

Table of Contents

At a Glance

Ransomware incidents continue to grow in the year 2022 with attacks across multiple sectors including critical infrastructure. Threat actors are continuing to modernise their attack tool kits with high impact strategies. Ransomware As A Service (RAAS) eco system is evolving with sophisticated double and triple extortion tactics [Data exfiltration, DDoS] and wide range of ransomware campaigns through affiliates. This is leading to higher probability of monetization and further rise in attack campaigns. Post covid accelerated digitalization and hybrid work culture are also aiding this threat emergence.

Threat actors are continuing to exploit known vulnerabilities, compromised credentials of remote access services and phishing campaigns for initial access into the infrastructure of organizations as well as citizens.

This present report covers the ransomware latest tactics and techniques along with sector wise trends observed in the first half of year-2022, specific to Indian cyber space. Also ransomware specific Incident response remediation and mitigation measures are covered as per the current threat landscape.

Ransomware Statistics

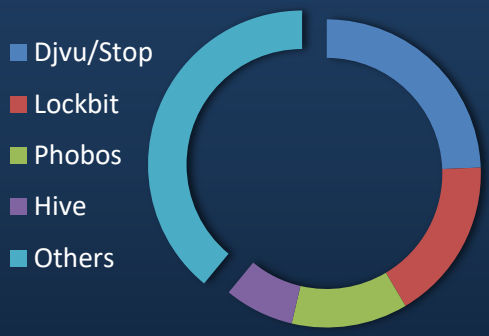
51% ▲

Overall, there is 51% increase in ransomware incidents reported in 2022-H1 compared to previous year [2021].

Prominent Ransomware Families observed in H1 2022

- Djvu/Stop – Citizen centric attacks
- Lockbit [2.0 & 3.0] – Targeted attacks

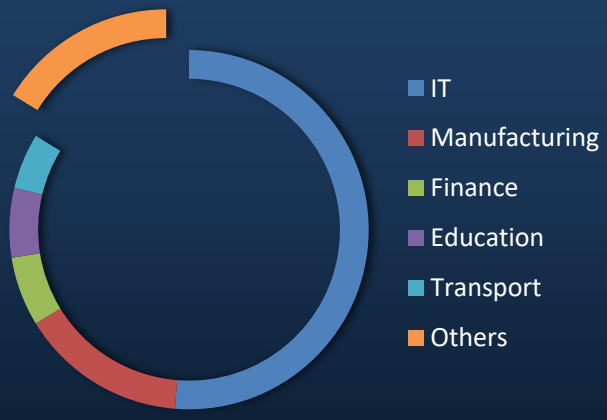
- Phobos is actively involved in both citizen centric and targeted attack campaigns
- Hive group activity is observed in targeted attacks
- Apart from these, the following are some of the variants observed in H1 2022



- ALPHV
- ReVil
- Ragnar Locker
- Conti
- Makop

Major sectors affected in H1 2022

- Majority of the attacks are observed in Datacentres/IT/ITeS sector followed by Manufacturing and Finance sectors.
- Ransomware groups have also targeted critical infrastructure in H1 2022 including Oil& Gas, Transport, Power



Ransomware Trends

Initial Infection

- [T1190]
  Ransomware gangs are focusing on known unpatched vulnerabilities of public-facing applications for initial entry into the network, such as-

  - CVE-2019-19781
    Vulnerability in Citrix Application Delivery Controller (ADC) and Gateway 10.5, 11.1, 12.0, 12.1, and 13.0

  - CVE-2021-40539
    Vulnerability in Zoho ManageEngine ADSelfService Plus version 6113 and prior

- [T1133]
  Compromised credentials of remote access services [VPN/ RDP] are being used by threat actors to gain entry into the network

- [T1566]
  Targeted Phishing campaigns with embedded payloads like Emotet are also witnessed in H1-2022 for further ransomware infections

- [T1189]
  "Drive by download" is the common tactic in citizen-centric ransomware cases

Ransomware Trends

Living off the Land

- Threat actors are leveraging what is already available in the target environment instead of deploying custom tools and malware
- In this way, malicious actions are less likely to flag security controls such as AV/EDR

Windows Binaries

- CMD.exe
- PowerShell
- Task Scheduler
- WinRm
- WMI/WMIC
- Rundll32

Threat actors are either using already available tools or deploying light weight tools during the attack. Fileless payloads became favourite choice for threat actors.

Internal Reconnaissance

- Advanced IP scanner
- Netscan
- AdFind
- PingInfoVeiw

Credential dumping

- MimiKatz and its obfuscated versions
- quarks pwdump

Lateral Movement

- Cobalt Strike
- WinRM
- PsExec

- Ransomware attacks are evolving with increased use of legitimate tools like "AnyDesk" for remote administration, which ensure continued command and control by the attacker

- By executing scripts (ex: .bat) to reboot victim machines in safe mode, threat actors are able to evade installed security solutions and carryout further activities.

- Development of customised payloads along with cross platform functionality to target multiple platforms
  - Linux based Operating Systems
  - Virtualised environment [vCenter, ESXI etc.]
  - Backup storages [NAS]
  - Cloud Environments [Ex: MongoDB instances]

- For cloud-based systems, ransomware groups are wiping the data instead of encrypting, after data exfiltration

* The above tool list is not exhaustive

Ransomware Attack-Response

In case of any suspected ransomware incident, the following steps may be followed, as appropriate

Step 1: Disconnect

- Immediately disconnect and isolate infected systems from the network. If several systems or subnets appear impacted, take the infected network offline at the switch level
- Disconnect all external storage: memory sticks, attached phones/cameras, external hard drives, USB drives
- Turn off any wireless functionality: Wi-Fi, Bluetooth, NFC
- Isolate backups immediately, if any connected to network
- Consider temporarily disabling any external facing remote connectivity service [VPN/RDP]

Report the incident to CERT-In and other regulatory authorities and lodge FIR with law enforcement agencies

Step 2: Determine the scope of Infection for unauthorised access & signs of encryption

- Mapped or shared drives /folders and Network storage devices of any kind
- External Hard Drives and USB storage devices of any kind (USB sticks, memory sticks, attached phones/cameras)
- Connected networks through MPLS, Internet leased lines etc. including the infrastructure situated at different geographic locations
- Cloud based storage services: Google Drive, Drop Box etc.

Step 3: Determine the ransomware strain

- Check for the ransomware type by evaluating encrypted file extension, ransom note /Lock screen.

Step 4: Response

- Preserve the logs of security devices, End points for necessary analysis
- It is recommended to backup the encrypted files, in case a decryptor becomes available
- Scan the working systems with updated Antivirus applications such as “Microsoft Safety Scanner” to determine the malicious binaries. Consider scanning the systems with multiple AV vendor applications to rule out any possible infection
- Patch any existing vulnerabilities and harden the applications /infrastructure
- Consider resetting all the account credentials that are possibly compromised and implement Privileged Access Management (PAM)
- Implement proper network segmentation with controlled access to services/ applications and disable unnecessary services & ports

Ransomware Attack-Response

- Consider enabling multi-factor authentication, especially for public facing services/remote access applications
- Deploy appropriate security controls such as latest AV/EDR, Firewall, IDS for monitoring and mitigating the cyber threats

The following URL may be referred for other relevant measures specific to Ransomware threat
https://www.csk.gov.in/alerts/ransomware.html

Restoration

- It is recommended to rebuild all the infected systems with fresh installations. Make sure to rigorously sanitize the infected systems/applications/devices before bringing back into the network.
- In case of Active Directory compromise, consider rebuilding all the systems under that domain with known good backup source.
  Ensure to follow the best security practices as listed in the below URL for AD rebuilding:
  https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory
- Monitor the network for any suspicious/ anomalous behaviour

It is not recommended to Negotiate and/or Pay the Ransom

Data Recovery

- Check availability of the decryptors from trusted sources such as:
  https://www.nomoreransom.org/en/decryption-tools.html
  In case of availability, try recovering the corrupted files in isolated environment
- Restore the corrupted files from known good backup source, if available
- Check for Shadow Copies if possible
- Check for any previous versions of files that may be stored on cloud storage, e.g., Drop Box, Google Drive etc.

Contact CERT-In for any Technical Assistance

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