सत्यमेव जयते
GOVERNMENT OF INDIA

INDIAN CYBER CRIME COORDINATION CENTRE (I4C)

MINISTRY OF HOME AFFAIRS

RANSOMWARE

-A MAJOR CYBER THREAT

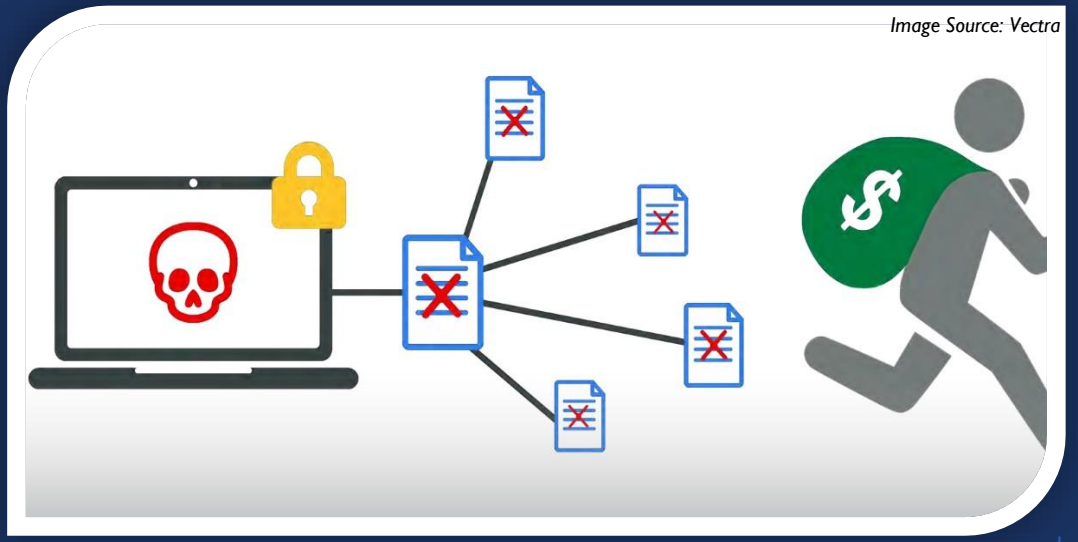


Image Source: Vectra

RESTRICTED CIRCULATION

Ransomware is a flourishing criminal industry that not only risks the personal, professional and financial security of individuals and organizations but can also threaten human lives and national security.

Good day. Your computer has been locked by ransomware, your personal files are encrypted and you have unfortunately "lost" all your pictures, files and documents on the computer. Your important files encryption produced on this computer: videos, photos, documents, etc.
Encryption was produced using unique public key RSA-1024 generated for this computer. To decrypt files you need to obtain the private key.
All encrypted files contain MW_
Your number: 93999135000121
To obtain the program for this computer, which will decrypt all files, you need to pay
3 bitcoins on our bitcoin address 1EhKNQirrpVUK9dyELt1Gks8oaeB1RqFXi (today 1 bitcoin was 260 USA dollars). Only we and you know about this bitcoin address.
You can check bitcoin balanse here - https://www.blockchain.info/address/1EhKNQirrpVUK9dyELt1Gks8oaeB1RqFXi
After payment send us your number on our mail ttk@ruggedinbox.com and we will send you decryption tool (you need only run it and all files will be decrypted during 1...3 hours)
Before payment you can send us one small file (100..500 kilobytes) and we will decrypt it - it's your garantee that we have decryption tool.
And send us your number with attached file.

We dont know who are you. All what we need - it's some money.
Don't panic if we don't answer you during 24 hours. It means that we didn't received your letter (for example if you use hotmail.com or outlook.com
it can block letter, SO DON'T USE HOTMAIL.COM AND OUTLOOK.COM. You need register your mail account in www.ruggedinbox.com (it will takes 1..2 minutes) and write us again)
You can use one of that bitcoin exchangers for transfering bitcoin.
https://www.unocoin.com
https://btcxindia.com
https://www.bitquick.in
https://buysellbitco.in
https://localbitcoins.com/country/IN
You dont need install bitcoin software - you need only use one of this exchangers or other exchanger that you can find in www.google.com for your country.
Please use english language in your letters. If you don't speak english then use https://translate.google.com to translate your letter on english language.

Figure: Ransomware message displayed on the users system.

RANSOMWARE

Ransomware is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files until a ransom is paid.

Ransomware is a flourishing criminal industry that not only risks the personal, professional and financial security of individuals and organizations but can also threaten human lives and national security.

RANSOMWARE IN THE PANDEMIC

The COVID-19 pandemic has elicited the largest numbers of employees working from home, which has revealed vulnerabilities in the underlying IT infrastructure and has increased the attack surface of many organizations.

A surge in Ransomware attacks is observed in the last couple of years.

Source: https://www.techtarget.com/searchsecurity/feature/Ransomware-trends-statistics-and-facts

RANSOWARE HEADLINES

PCI Security Standards Council (PCI SSC).

India among top 3 countries most affected by ransomware attacks

ANI | Updated: Mar 10, 2022 09:06 IST

India tops the list in ransomware attacks amid digital push

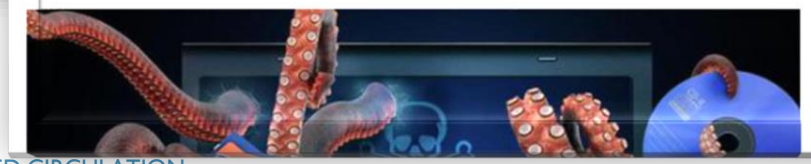
BS Business Standard

India tops ransomware attacks globally with 68% entities impacted: Sophos

Info-tech

Three-fourths of organisations in India have been hit by ransomware threat this year: Report

BL Mumbai Bureau | Mumbai, Dec 18 | Ransomware Attacks | Updated On: Dec 18, 2021



Cost organisations nearly $2 million on average

Indian Container Terminal Diverts Ships Due to Ransomware Attack

Jawaharlal Nehru Port reported handling 5.6 million TEU in 2021 at the five container terminals in the port near Mumbai (Jawaharlal Nehru Port Trust)

PUBLISHED FEB 22, 2022 8:17 PM BY THE MARITIME EXECUTIVE

THE TIMES OF INDIA

Ransomware hits Telangana and Andhra Pradesh power department websites

Mahesh Buddi / TNN / Updated: May 3, 2019, 14:44 IST

SOME STATISTICS / TRENDS

- As per Checkpoint Report, Indian education sector faced 5,196 cyber attacks very week in July 2021
- As per CrowdStrike Global Security Survey 2021, India and Asia pacific region has been heavily affected by ransomware
- Open Source indicates the increase in Ransomware incidents in the country
- Various Sector such as Power, Education, Health, etc. are major targets

Ransomware is **part of 10% of all breaches**.

- **Ransomware attacks doubled** in frequency in 2021, according to the 2021 "Verizon Data Breach Investigations Report."
- Approximately **37% of global organizations** said they were the victim of some form of ransomware attack in 2021,
- **95% of all the ransomware samples are Windows-based** executable files -- or dynamic link libraries -- according to VirusTotal.

RANSOMWARE TRENDS

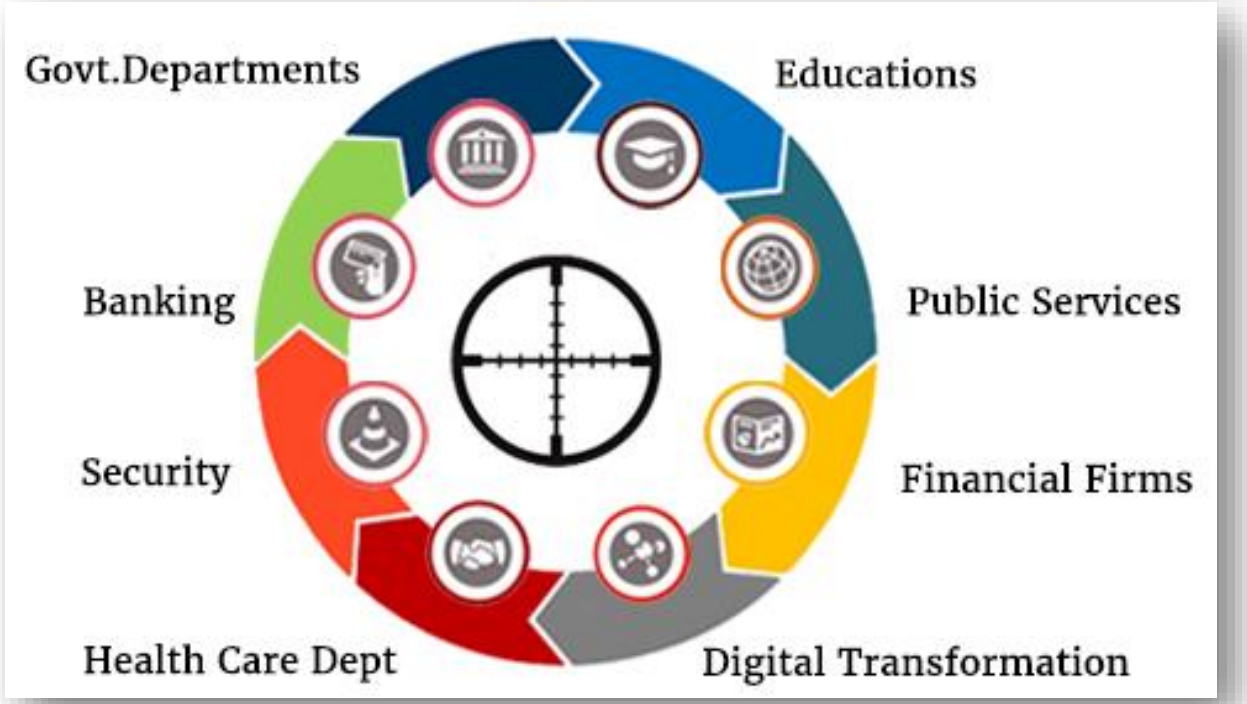
- "Micro, Small & Medium Enterprises (MSME) and individuals" are impacted by ransomware threats.
- In the case of individuals, the main ransomware family is "DJVU/STOP." A new variant of this ransomware variant is extension ".ghsd".
- Most of the reported ransomware attacks primarily used two methods "phishing and vulnerability exploitation" in addition to other techniques to compromise the system.

Some of the recently reported ransomware based on open source information and CERT-In are:

a. Lockbit (Ransomware as a service model, Double extortion technique)
b. ReVIL (Ransomware as a service model, Double extortion technique)
c. AvosLocker (Double extortion technique)
d. Conti Ransomware

RANSOMWARE TARGETS

Today any enterprise, organisation or individuals users, big or small, is vulnerable to ransomware attack. The possibility of a it depends upon how attractive and important data your organization possess.

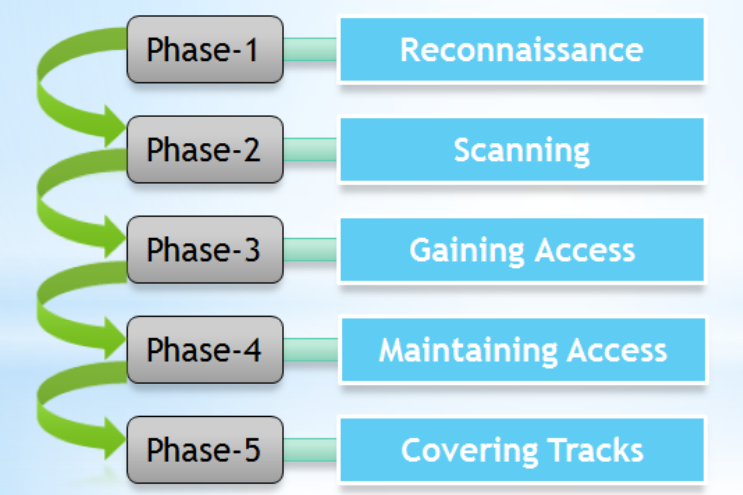


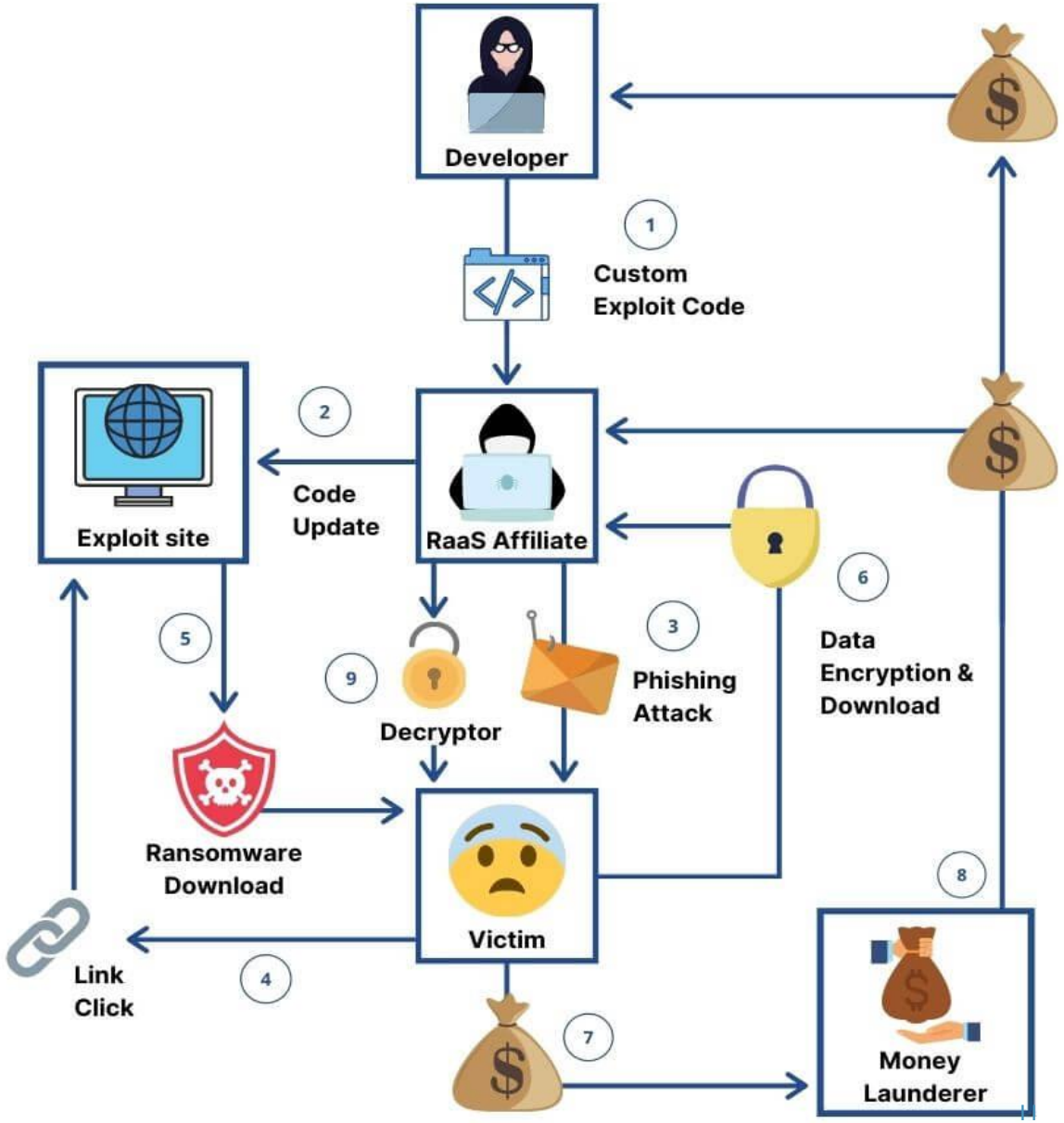
EVOLUTION

- Trend from floppy disks distributed via snail mail changed with the tide as the internet and then blockchain technologies and cryptocurrencies respectively
- Hundreds of different **Ransomware families** are active
- Notable Ransomware Families
    - Conti, REvil, Babuk Locker, DarkSide, LockBit, Nefilim, Ryuk, Sodinokibi, Stop, Petya, Wcry, etc.
- Vulnerabilities associated with Ransomware on increase
- Number of new APT groups are exploiting such vulnerabilities to mount attacks
- Notable Ransomware variants extensions
    - Pcqq, nusm, paas, pahd, zqqw, reqg, nusm, etc.

RANSOMWARE AS A SERVICE

In recent years, ransomware has become a big criminal enterprise. Several forums operate as **Ransomware as a Services (RaaS)** recruit hackers/affiliates and discuss ransomware operations business model, profit sharing, rent, sell etc.





UpGuard

RANSOMWARE ATTACKING METHODS

There are a number of vectors ransomware can take to access a users device/computer.

- EXPLOITING THE VULENRABILTIY : A cyber-security term that refers to a flaw in a system that can leave it open to attack.
- PHISHING E-Mails : Crafted malicious emails embedded with decoy attachments and payloads
- MALICIOUS UPDATES/INSTALLERS : Fake applications, update, advertisements
- STOLEN/REUSED CREDENTIALS : Harvesting credentials from open source or darkweb and using compromised account credentials as weapon
- MALICIOUS LINKS IN CHAT : Sending mass phishing or short-url in SMS, Internet messengers, Groups etc.
- **EXPLOIT KITS :** Malicious codes, PowerShell, scripts, remote desktop attacks etc.

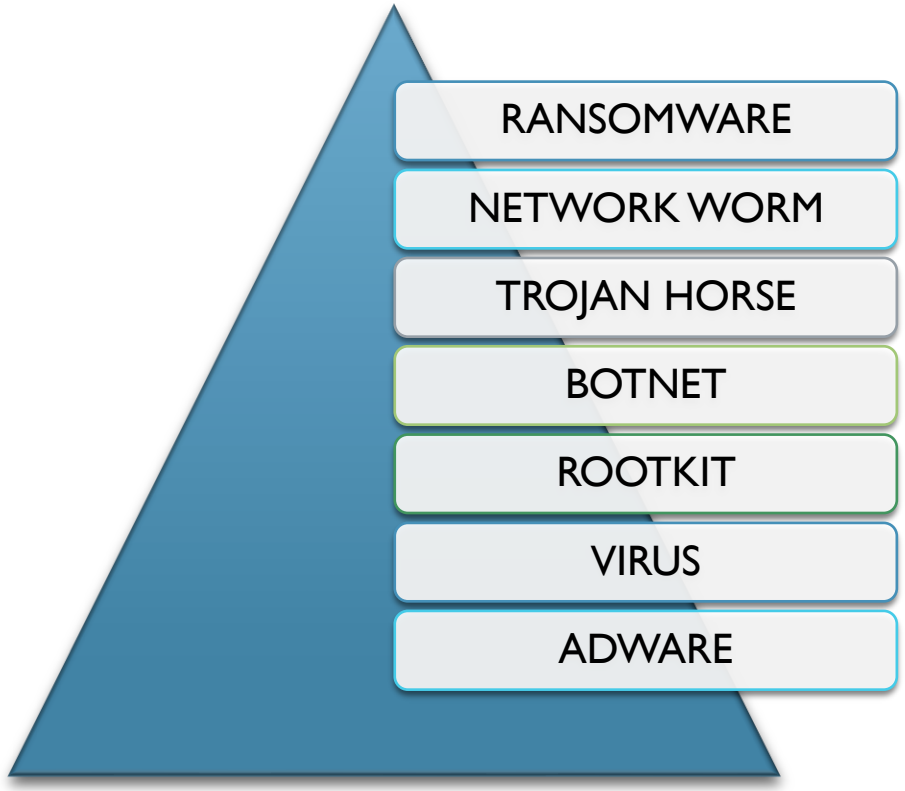
IMPACTS OF CYBER ATTACKS

Ransomware can cause major damage to organizations or systems, as well as to business reputation and consumer trust.

Some potential results include:

- Sabotage
- Data breach.
- Financial loss.
- Reputational damage.
- Legal consequences.

Types of Malicious Code Continued

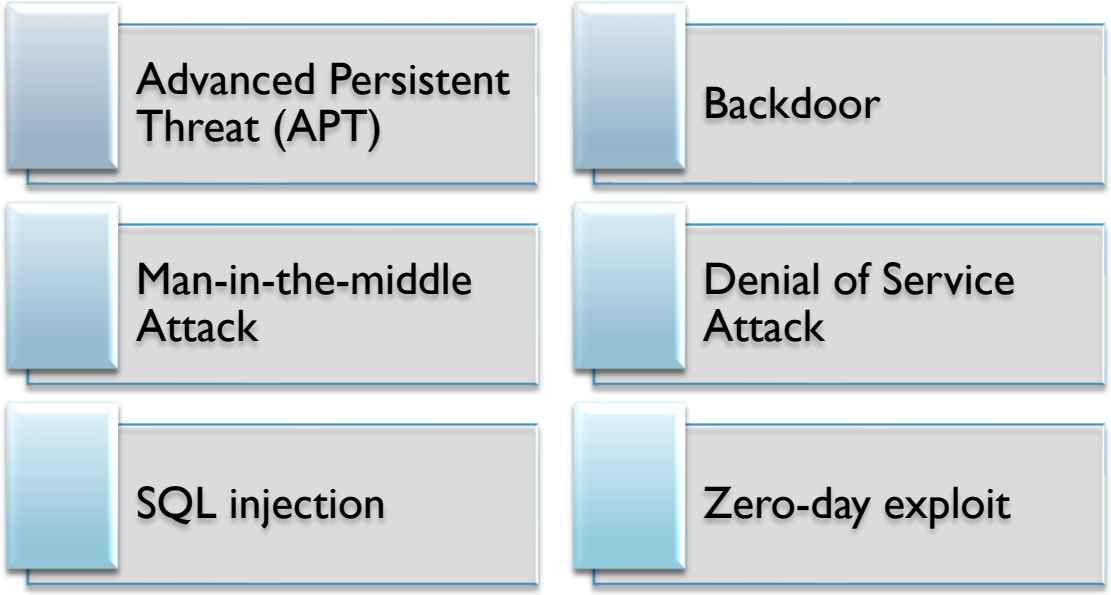


SOURCES OF CYBER THREATS

Cyber threats can come from a wide variety of sources, some notable examples include:

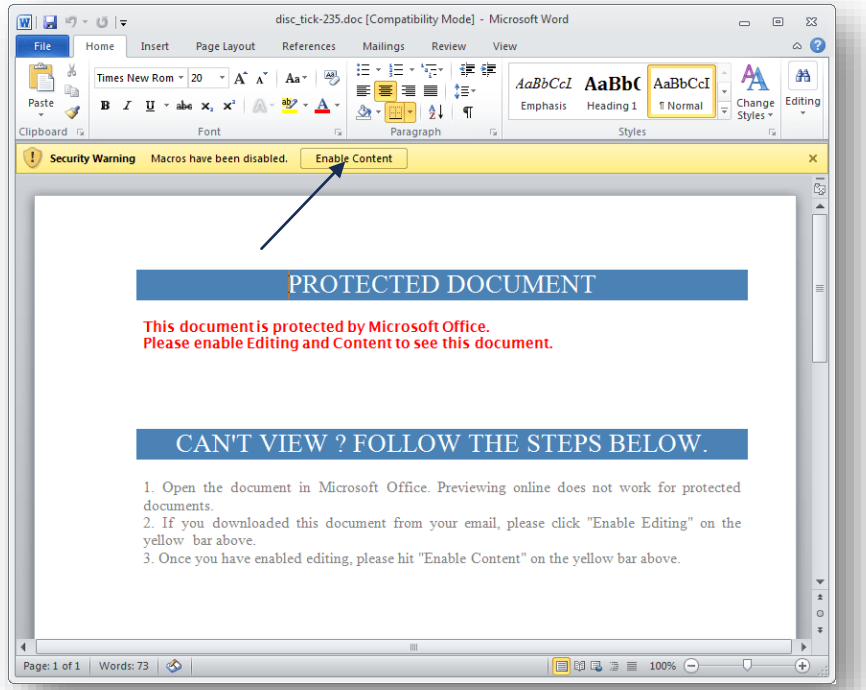
- National governments.
- Terrorists.
- Industrial secret agents.
- Rogue employees.
- Hackers.
- Business competitors.
- Organization insiders.

SOME MAJOR Types of Cyber Attacks



SAMPLE MALICIOUS RANSOMWARE MAIL/ATTACHMENT

Sample of phishing email



Sample malicious document, ask user to "Enable content"

	Hyderabad Breaking News | Hyderabad News - Eenadu Online Telugu Newspaper	1	11	12:09:09	http://www.eenadu.net/hyderabad-news.aspx
	Telugu Movies|Latest Telugu Movies News in Telugu|Tollywood new in Telugu|Telugu Cinema News|New Movies - Eenadu	1	11	12:17:29	http://www.eenadu.net/telugumovies/cinemanews.aspx?item=cinema&no=4
	Rediff.com: Online Shopping, Rediffmail, Latest India News, Business, Bollywood, Sports, Stock, Live Cricket Score, Money, Movie Reviews	1	11	12:10:18	http://www.rediff.com/
	Yahoo	3	11	12:12:37	http://www.yahoo.com/
	Yahoo	4	11	12:12:37	https://in.yahoo.com/?p=us
	Download Baahubali (2015) - [PreDVD - x264 - 1CD - (Tamil + Telugu + Hindi) - AC3 - 900MB][LRanger] Torrent - Kickass Torrents	1	11	12:34:17	https://kat.cr/baahubali-2015-predvd-x264-1cd-tamil-telugu-hindi-ac3-900mb-lranger-t10926142.html
	Torrentz Search Engine	1	11	12:33:51	https://torrentz.eu/
	Torrentz Search Engine	1	11	12:33:51	https://torrentz.in/
	www.TamilRockers.com - Baahubali (2015) - [PreDVD - x264 - 1CD - (Tamil + Telugu + Hindi) - AC3 - 90 Download	1	11	12:34:14	https://torrentz.in/583e4e66f76ae9097eaafb51a477a19a3ffa7887
	telugu movies 2015 download	1	11	12:34:01	https://torrentz.in/search?q=telugu+movies+2015
		1	11	12:26:09	https://www.google.co.in/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#q=ortas

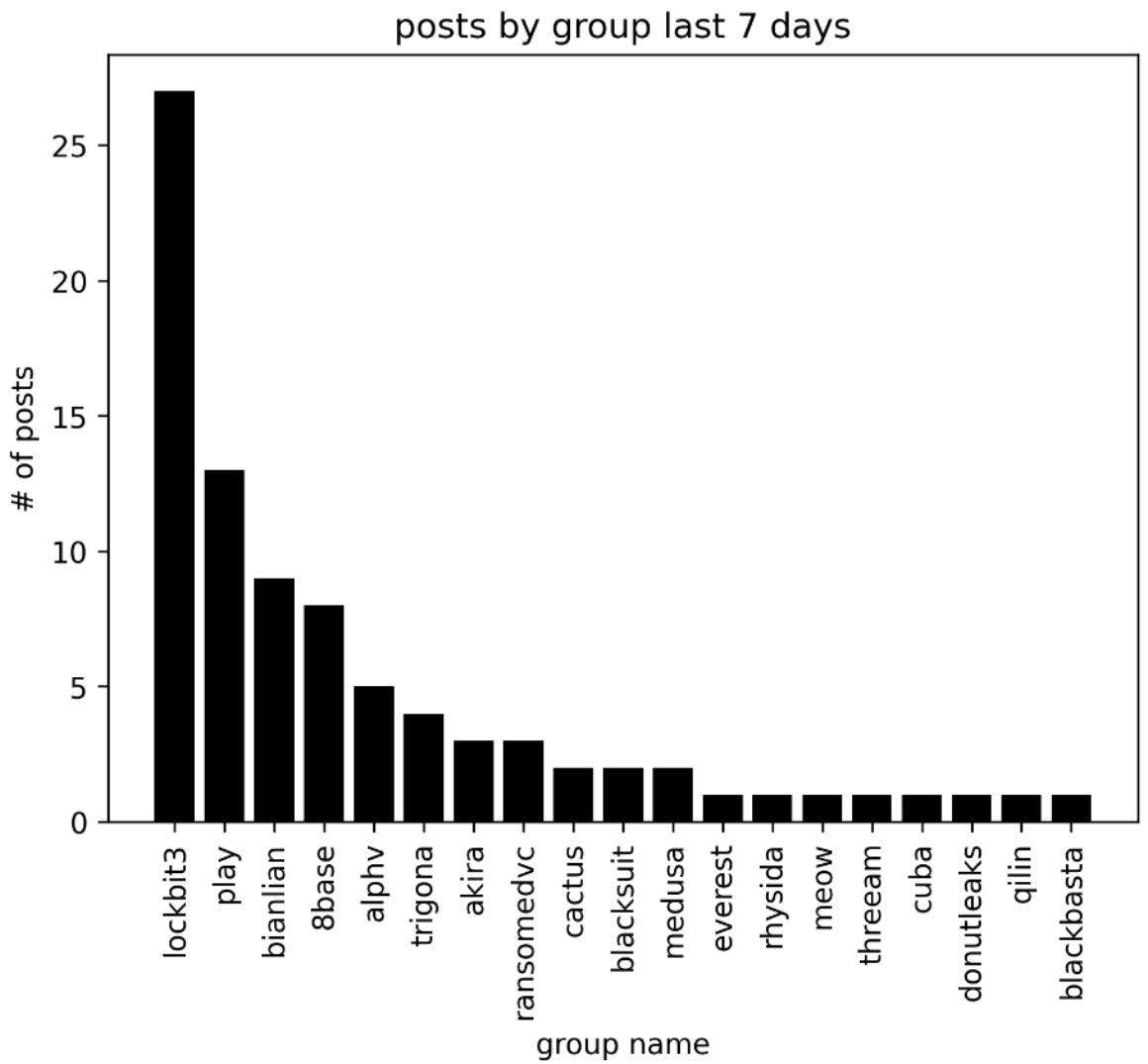
Figure: Browsing torrent activities

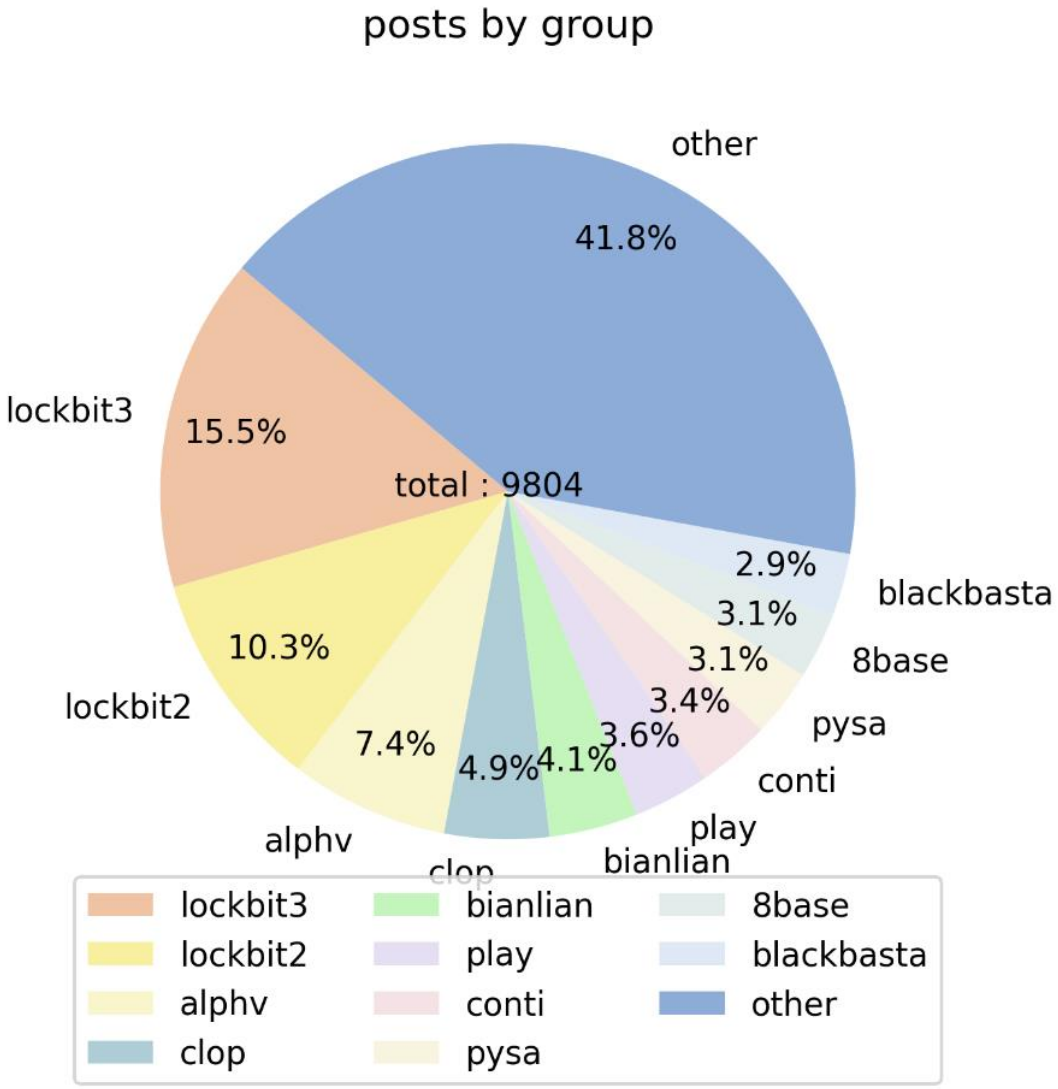
RANSOMWARE THREATS

- Ransomware attacks cause downtime, data loss, reputational damage, intellectual property theft, etc.
- Threats to Critical Information Infrastructure (CII)
- Terror Financing from Ransomware Proceeds
- Organizations losing access to their systems and sensitive data, and privacy breaches
- The risk of data leaks and permanent data loss
- Downtime and disruption of routine work and loss of reputation
- Insider Threats

Ransomware Threats

- Ransomware attack can target both **individuals and organizations.**
- Rapid growth of cryptocurrency worldwide has fueled the ability of ransomware actors to readily monetize their activity.
- Most ransomware activity emanates from a small number of nations who appear unwilling or unable to crack down on this criminal activity – or who may be complicit in and benefit from it.
- And increasingly, the line between a Nation-State (Advanced Persistent Threat) attack and one mounted by a criminal enterprise is fast getting blurred.


posts by group last 7 days
# of posts
group name
lockbit3
play
bianlian
8base
alphv
trigona
akira
ransomedvc
cactus
blacksuit
medusa
everest
rhysida
meow
threeam
cuba
donutleaks
qilin
blackbasta


posts by group
other
41.8%
lockbit3
15.5%
total : 9804
2.9%
blackbasta
3.1%
8base
3.1%
pysa
3.4%
conti
3.6%
play
4.1%
bianlian
4.9%
clop
7.4%
alphv
lockbit2
10.3%
lockbit3
lockbit2
alphv
clop
bianlian
play
conti
pysa
8base
blackbasta
other

date	title	group
2024-02-06	spbglobal.com\$81.4M\Spain\706GB\<1%DISCLOSED	cactus
2024-02-05	Virgin Islands Lottery	play
2024-02-05	Ready Mixed Concrete	play
2024-02-05	Premier Facility Management	play
2024-02-05	Perry-McCall Construction	play
2024-02-05	Northeastern Sheet Metal	play
2024-02-05	McMillan Pazdan Smith	play
2024-02-05	Mason Construction	play
2024-02-05	Leaders Staffing	play
2024-02-05	Hannon Transport	play
2024-02-05	Greenwich Leisure	play
2024-02-05	Douglas County Libraries	play
2024-02-05	Albert Bartlett	play
2024-02-05	Asecos	blackbasta
2024-02-05	www.commonwealthsign.com	qilin
2024-02-05	themisbourne.co.uk	lockbit3
2024-02-05	Vail-Summit Orthopaedics & Neurosurgery (VSON)	alphv
2024-02-05	http://tobaccofreekids.org	blacksuit
2024-02-05	hutchpaving.com	lockbit3
2024-02-05	davis-french-associates.co.uk	lockbit3
2024-02-05	VCS Observation	akira
2024-02-05	noe.wifi.at	lockbit3
2024-02-05	ksa-architecture.com	lockbit3
2024-02-05	GRTC Transit System	bianlian

https://ransomwatch.telemetry.ltd/#/recentposts

Incident 1

ALPHV | Blog | Collections

SOLAR INDUSTRIES INDIA WAS HACKED. MORE THAN 2TB SECRET MILITARY DATA LEAKED

1/26/2023, 9:39:03 AM

Because of low security, more than 2TB of sensitive data related to weapons production was stolen from Solar Industries India Limited.

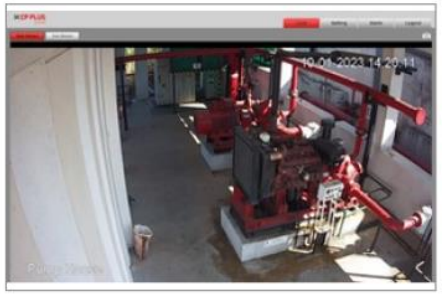
The data leakage affected all products and classified documents of the company. The data includes full descriptions of engineering specifications, drawings, audits of many weapons, among others:

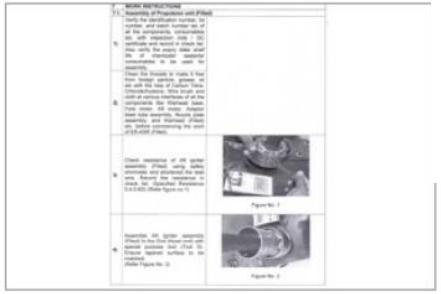
- Rocket Pinaka MK-1 ADM-1
- Propellant Pinaka MK-1 Enhanced
- Proppelant Pinaka MK-2 Guided
- Proppelant Akash Booster
- Proppelant RTRS
- Proppelant Astra MK-2
- Proppelant PSOM-XL
- Proppelant SkyRoot
- Proppelant Star Booster
- Proppelant HEMRL(PJ-10)
- Proppelant BramhMos
- Proppelant A1-P(P1 & P2)
- Warhead: Konkur, Invar, ATGM MK-2, MPBX Blocks
- Mines: Vibhav, Vishal, Adrashy
- Bomb: PGB 450, GP 250

And much more.

Also among the data contain:

- Personal information about the company's employees and customers
- Armament supply chains to various sources
- Blueprints and engineering documentation





eeficvtfgqgpzlvunkwnvrjpkmwmrdjyakdvw4jkklgfukcpfzig54qd.onion

Index of /

../		
03 Dec 22/	18-Jan-2023 18:58	-
09 Sales Register Dec 22/	18-Jan-2023 19:12	-
20.07.22 Cali/	11-Jan-2023 12:14	-
Defense/	18-Jan-2023 18:25	-
ICICI Personal Ln Doc/	18-Jan-2023 19:07	-
Mediclaim/	18-Jan-2023 19:07	-
PF Document/	18-Jan-2023 20:30	-

eeficvtfgqgpzlvunkwnvrjpkmwmrdjyakdvw4jkklgfukcpfzig54qd.onion/09 Sales Register Dec 22/

Index of /09 Sales Register Dec 22/

../		
01 ETPL Sales Register Dec 22.xlsx	18-Jan-2023 19:12	323565
02 EEL Sales Register Dec 22.xlsx	18-Jan-2023 19:12	2213924
03 SIIL Sales Register Dec 22.xlsx	18-Jan-2023 19:12	8066428
Final Summery Dec 22.xlsx	18-Jan-2023 19:12	40121
SIIL Mega Details Dec 22.xlsx	18-Jan-2023 19:12	1333081
SIIL Transit sale Qtr-3 (1).xlsx	18-Jan-2023 19:12	2542718
Sale In Tranist 02.01 (1).XLSX	18-Jan-2023 19:12	1924593

Darkweb URLS of weblinks

Incident 2

Two Wheelers · 2 Min Read

Suzuki Motorcycle India halts operations due to cyberattack

Manufacturing was reportedly halted since May 10, and it is estimated that since then the company lost production of over 20,000 vehicles. The company has not revealed the origin of the attack or when it will resume production.

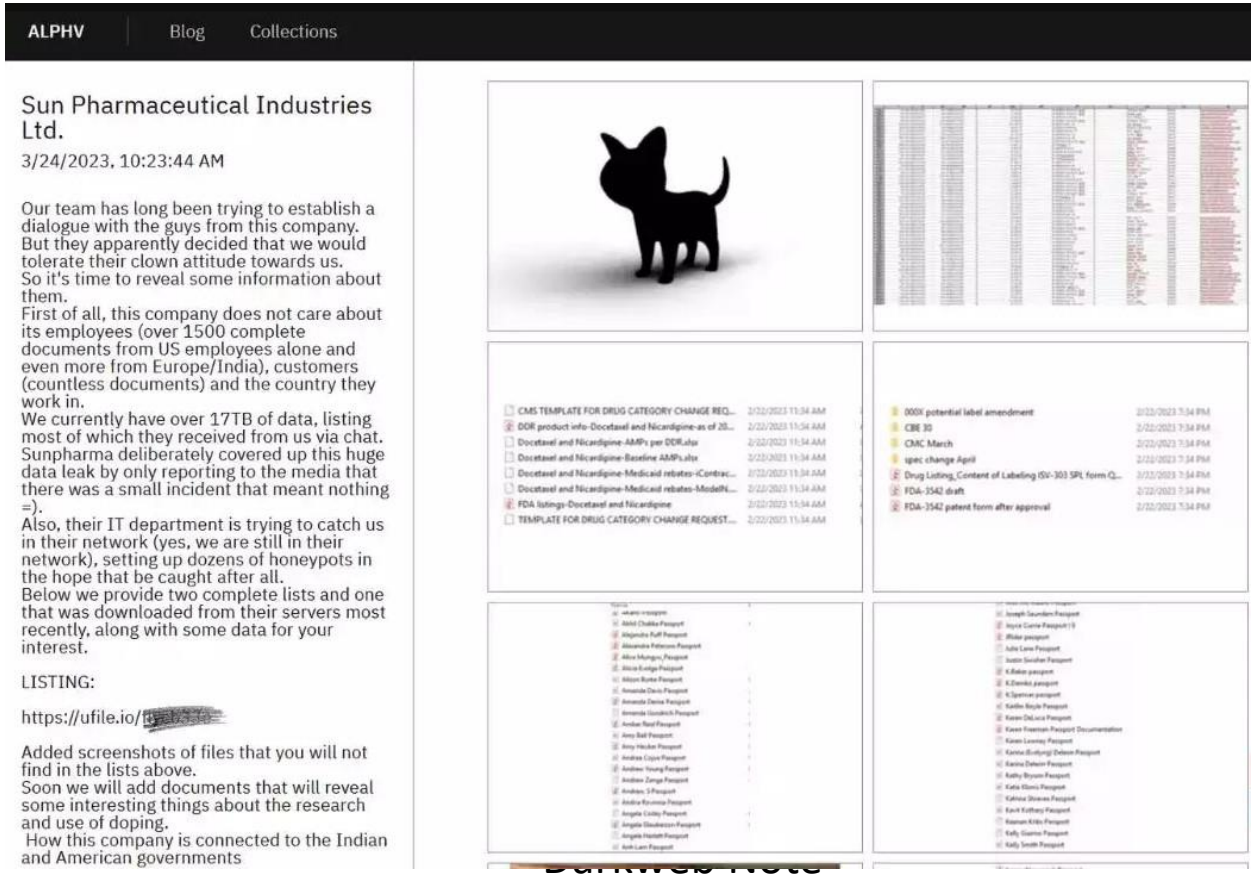
Biplab Das · ETAuto
Updated On May 19, 2023 at 08:44 PM IST

Incident 3

SUN PHARMACEUTICAL INDUSTRIES LTD

Ransomware : ALPHV (BLACKCAT)

Date: 25 March 2024



CHALLENGES

Technical Challenges	Legal Challenges
Identifying Ransomware Infrastructure	Investigation of Ransomware attacks
Misuse of Cryptocurrency	Lack of universal legal framework
Blockchain & Darkweb Analysis	Unclear jurisdiction
Diplomatic Challenges	**Training Challenges**
Coordination among countries	Lack of response capacity and trained manpower
Coordination among Agencies	Forensic and investigative skills
Lack of universal framework	Lack of digital forensic equipment