Cyber Security

Enterprise Security Challenges and Opportunities

- **Gulshan Gupta**
Scientist, Space Applications Centre,
ISRO, Ahmedabad

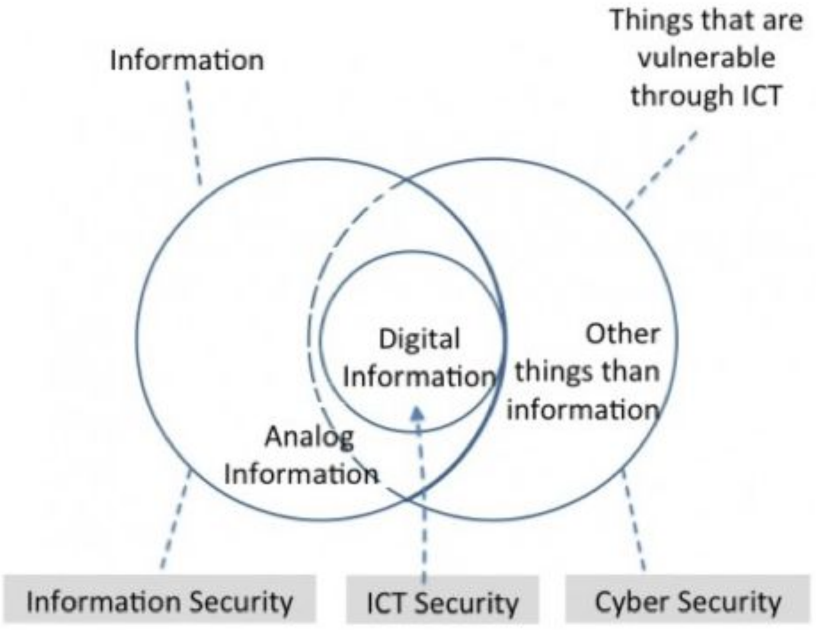
19 April, 2022 @ Sardar Patel College of Engineering, Vidyanagar

Outline

- ➢ Scope and Classification
- ➢ Current Situation: Impact and Statistics
- ➢ How / Why / Who
- ➢ Evolution / Technology / Cyber Threats
- ➢ Threat landscape
- ➢ Zero Day attacks
- ➢ Advanced Persistent Threat (APT)
  - ○ Execution Flow
  - ○ APT - Case Study
- ➢ Attack Vectors - Network, Email, Apps
- ➢ Email Security
  - ○ Phishing examples
  - ○ General Cautions
- ➢ Cyber Incident Reporting
- ➢ OWASP top 10
- ➢ Opportunities

Scope and classification

- Critical infrastructure security
- Network security
- Application security
- Cloud security
- Web security
- IoT security
- Perimeter security
- Cyber forensics and incident response
- Endpoint protection
- Compliance and governance
- Intrusion detection
- Malware/spyware analysis

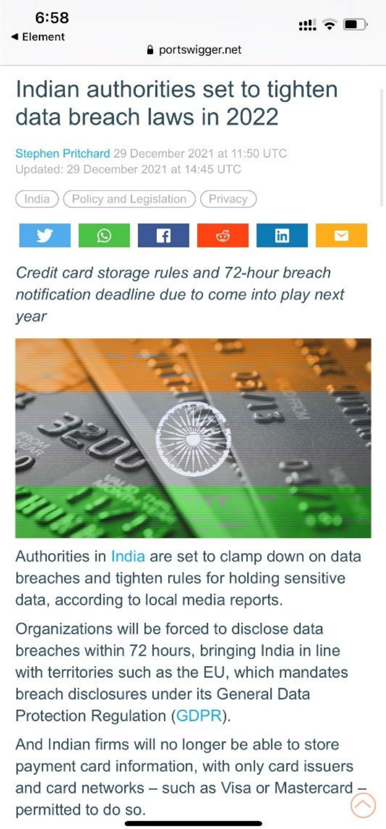


Current Era

- Digital World
  - Business, banking, healthcare, etc
  - Share of mobile in India’s digital media spends jumped to 76% in FY21 from 45% in FY19

- Crime is following the same trend
  - Worldwide Ransomware attacks (62% increase, 2019-2020)
  - High-profile hacks
  - More sophisticated phishing emails

- New privacy laws and regulations
  - Awareness on compliance



Indian authorities set to tighten data breach laws in 2022

Stephen Pritchard 29 December 2021 at 11:50 UTC
Updated: 29 December 2021 at 14:45 UTC

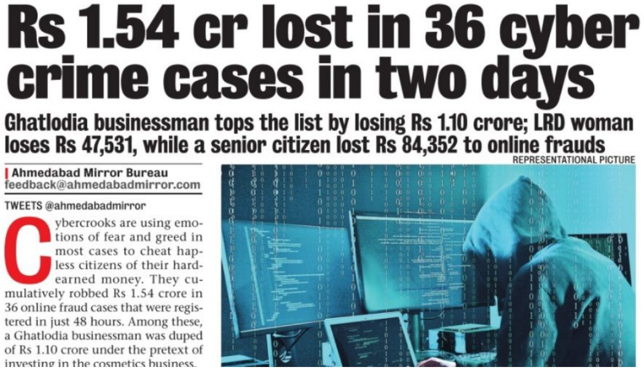
India | Policy and Legislation | Privacy

Credit card storage rules and 72-hour breach notification deadline due to come into play next year

Authorities in India are set to clamp down on data breaches and tighten rules for holding sensitive data, according to local media reports.

Organizations will be forced to disclose data breaches within 72 hours, bringing India in line with territories such as the EU, which mandates breach disclosures under its General Data Protection Regulation (GDPR).

And Indian firms will no longer be able to store payment card information, with only card issuers and card networks – such as Visa or Mastercard – permitted to do so.



Rs 1.54 cr lost in 36 cyber crime cases in two days

Ghatlodia businessman tops the list by losing Rs 1.10 crore; LRD woman loses Rs 47,531, while a senior citizen lost Rs 84,352 to online frauds

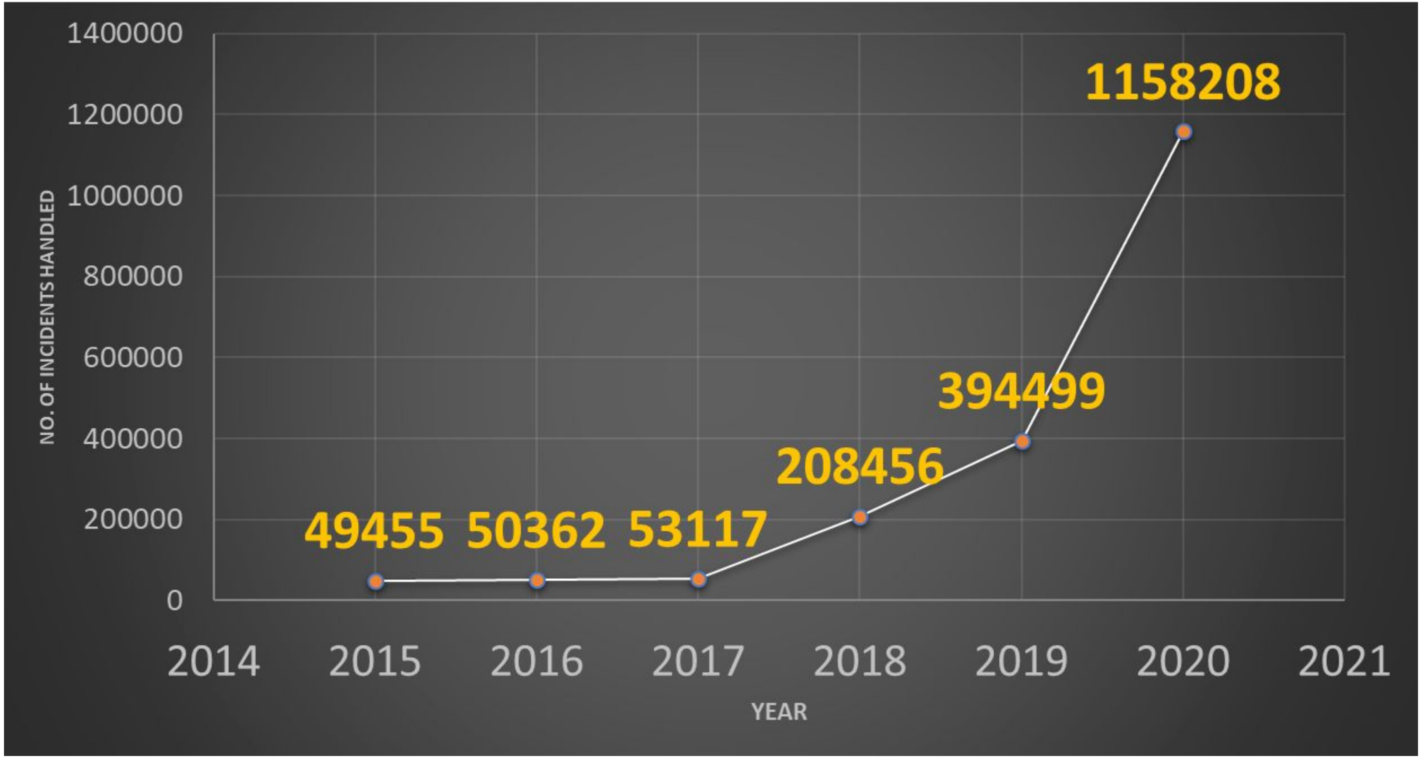
REPRESENTATIONAL PICTURE

Ahmedabad Mirror Bureau
feedback@ahmedabadmirror.com

TWEETS @ahmedabadmirror

Cybercrooks are using emotions of fear and greed in most cases to cheat hapless citizens of their hard-earned money. They cumulatively robbed Rs 1.54 crore in 36 online fraud cases that were registered in just 48 hours. Among these, a Ghatlodia businessman was duped of Rs 1.10 crore under the pretext of investing in the cosmetics business.

Cyber attacks in India grew by **194%** in 2020



Source: CERT-In Annual Report

How ?

- Global access to attacker
  - Much more access than physical security
  - Most of the systems online

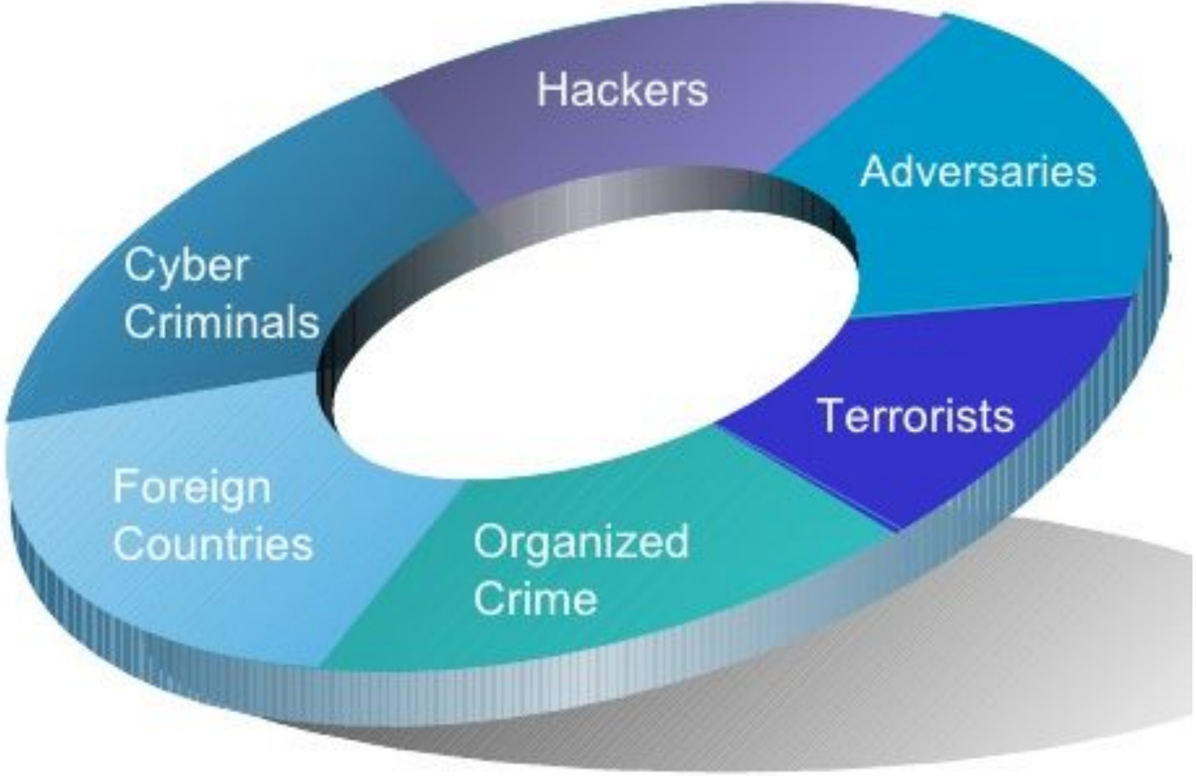
- Risks caused by poor security knowledge and practice:
  - Identity Theft
  - Monetary Theft
  - Legal Ramifications (for yourself and your organization)

- Attack Vectors/Vulnerabilities are easily available
  - Web Browser
  - IM Clients
  - Web or Mobile Apps
  - Excessive User Rights

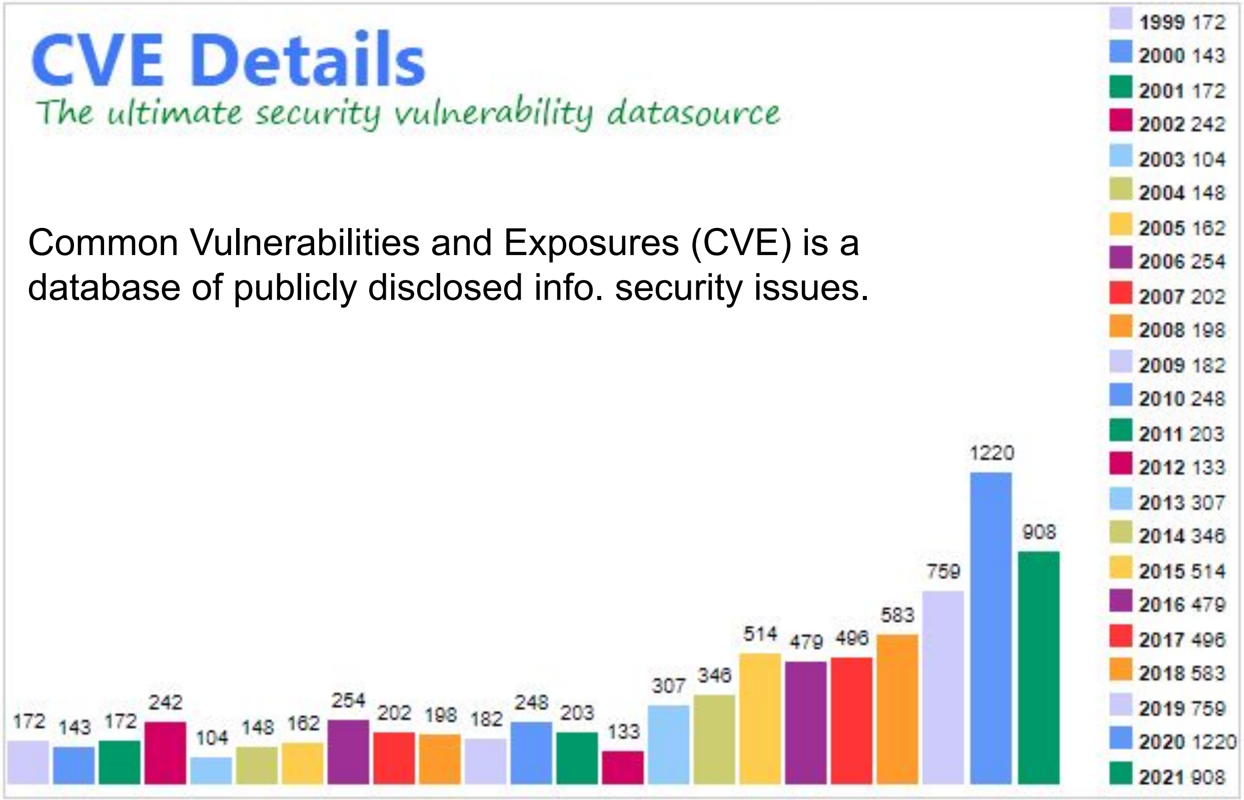
Why ?

- Names, phone numbers, email addresses
- Software & Hardware Info.
- Process Information
- Location Information
- Project Details
- Work Schedules
- Functional Hierarchy
- Establishment Details

Who ?


Hackers
Adversaries
Cyber Criminals
Terrorists
Foreign Countries
Organized Crime

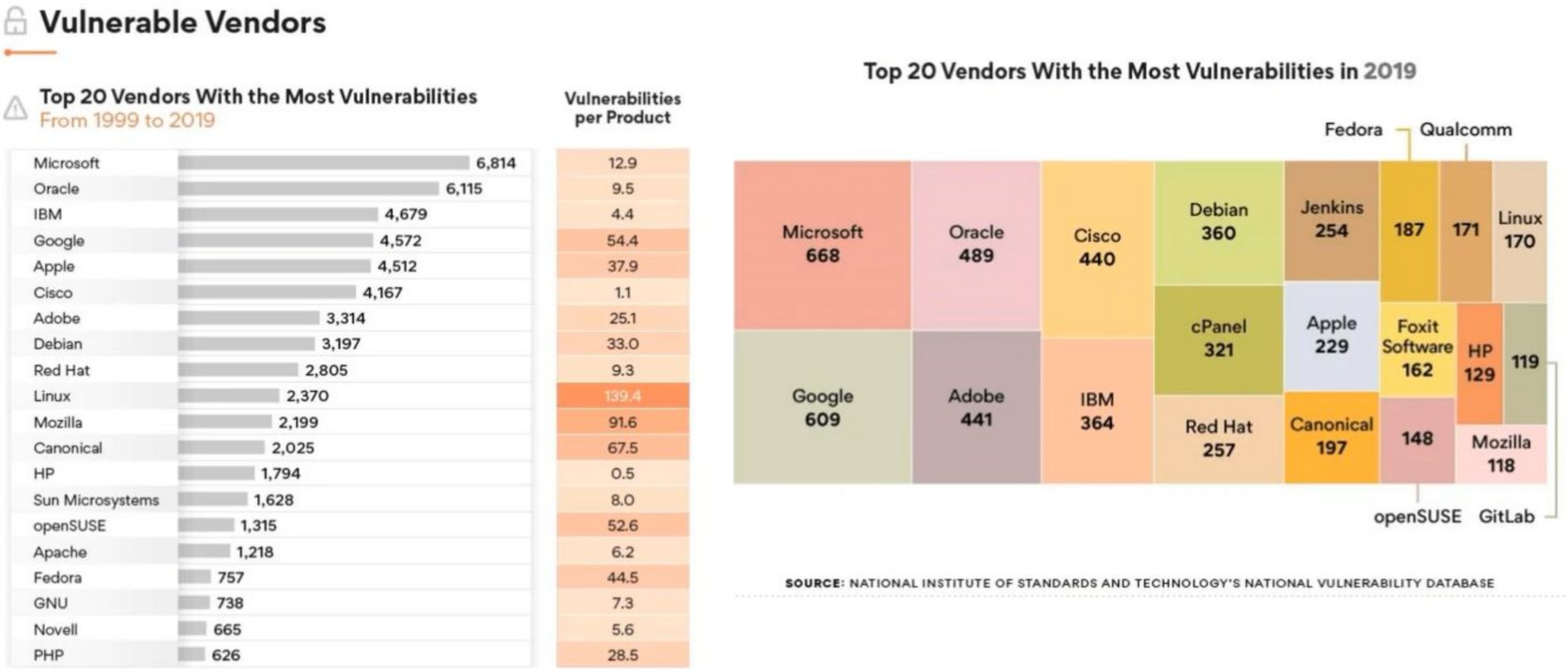
Vulnerabilities By Year



Common Vulnerabilities and Exposures (CVE) is a database of publicly disclosed info. security issues.

CVE Details- Security Vulnerability Data source

Vulnerabilities in Softwares



Vulnerable Vendors

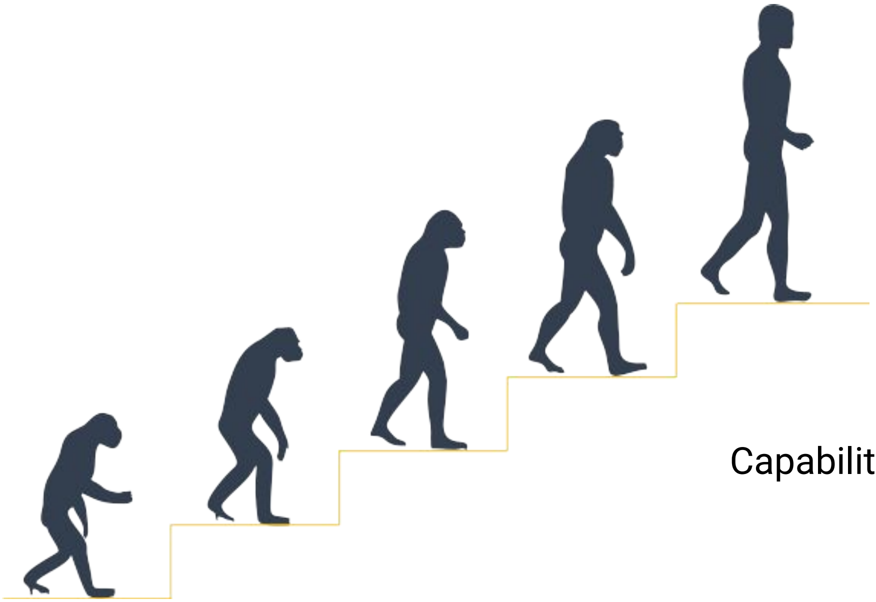
Top 20 Vendors With the Most Vulnerabilities
From 1999 to 2019

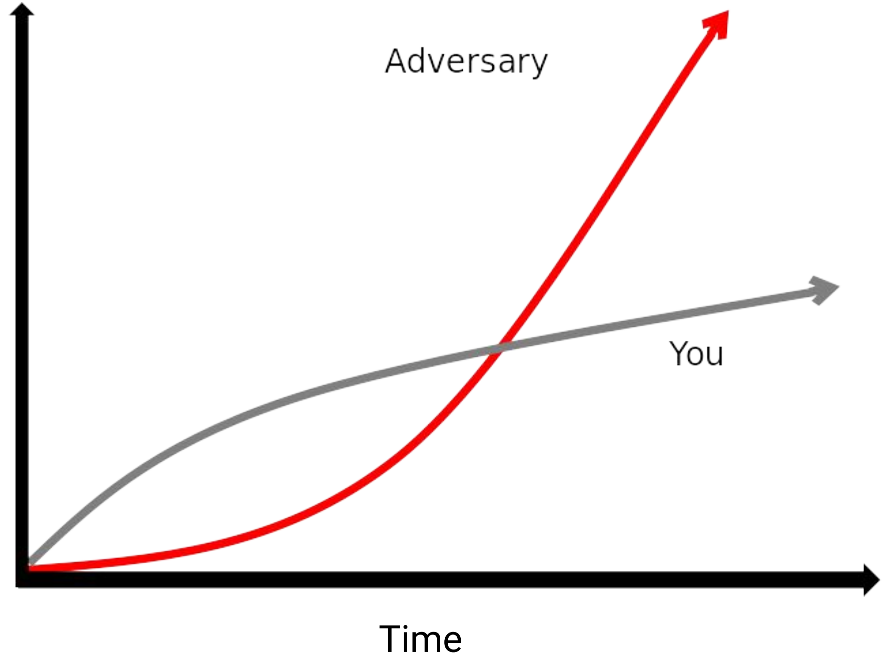
		Vulnerabilities per Product
Microsoft	6,814	12.9
Oracle	6,115	9.5
IBM	4,679	4.4
Google	4,572	54.4
Apple	4,512	37.9
Cisco	4,167	1.1
Adobe	3,314	25.1
Debian	3,197	33.0
Red Hat	2,805	9.3
Linux	2,370	139.4
Mozilla	2,199	91.6
Canonical	2,025	67.5
HP	1,794	0.5
Sun Microsystems	1,628	8.0
openSUSE	1,315	52.6
Apache	1,218	6.2
Fedora	757	44.5
GNU	738	7.3
Novell	665	5.6
PHP	626	28.5

Top 20 Vendors With the Most Vulnerabilities in 2019

SOURCE: NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY'S NATIONAL VULNERABILITY DATABASE

Evolution of Attacker

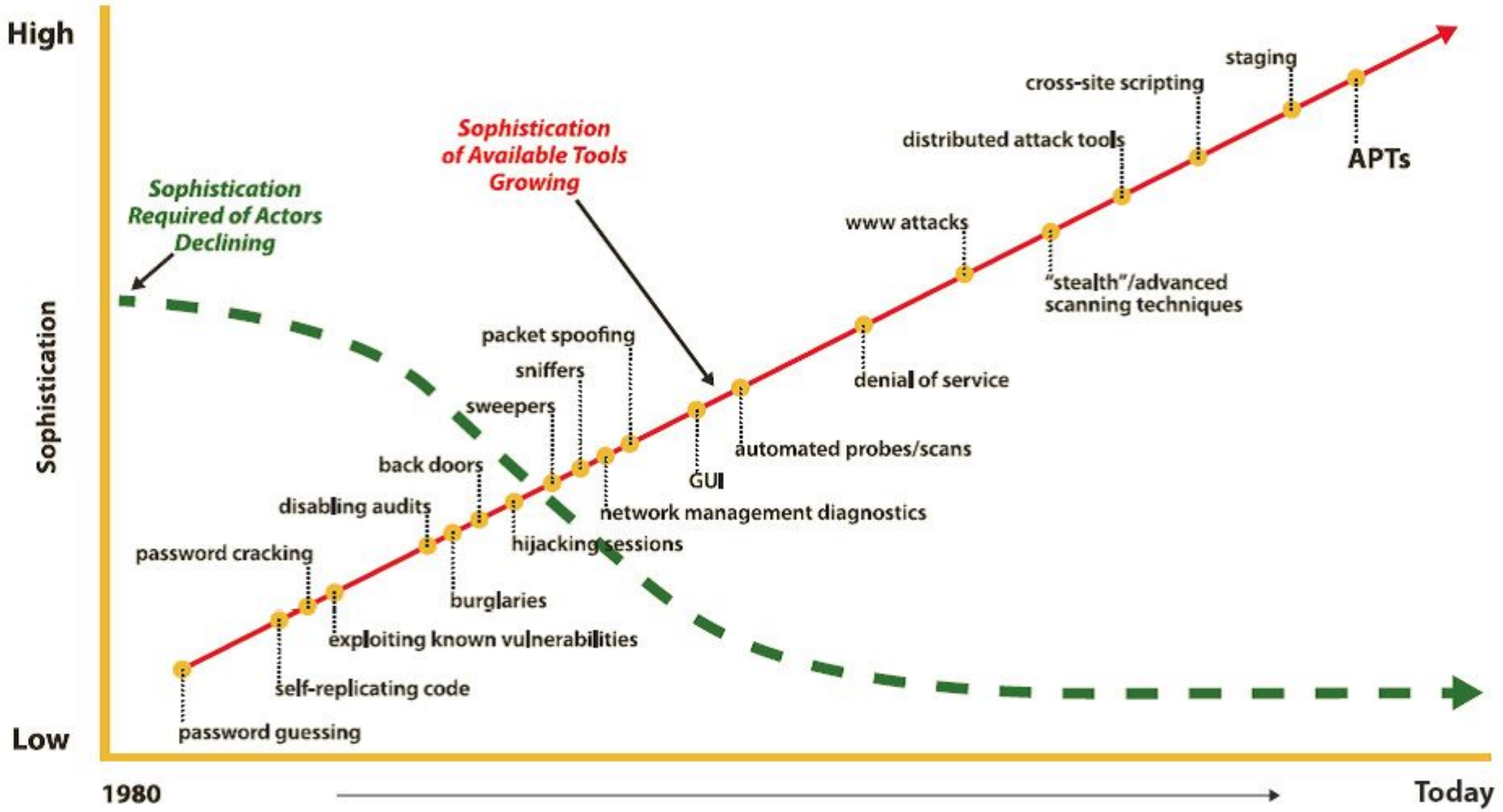




$445 billion industry

100+ nations

Evolution of Technology and Cyber Threats



MALWARE

What is it?

Any software intended to…

- Damage
- Disable
- Or give someone unauthorized access to your computer or other internet-connected device

Why should you care?

- Most cybercrime begins with some sort of malware. You, your family, and your personal information is almost certainly at risk if malware finds its way onto your computer or devices.

Examples

- Ransomware
- Adware
- Botnets
- Rootkits
- Spyware
- Viruses
- Worms

Known Threats

Threats about which information(IOC) is already available

- Hash
- URL
- IP/Domain
- DNS Query
- Regex
- CVE

Signatures exists for known threats

Unknown Threats

Known threats may be converted to Unknown by manipulating IOCs

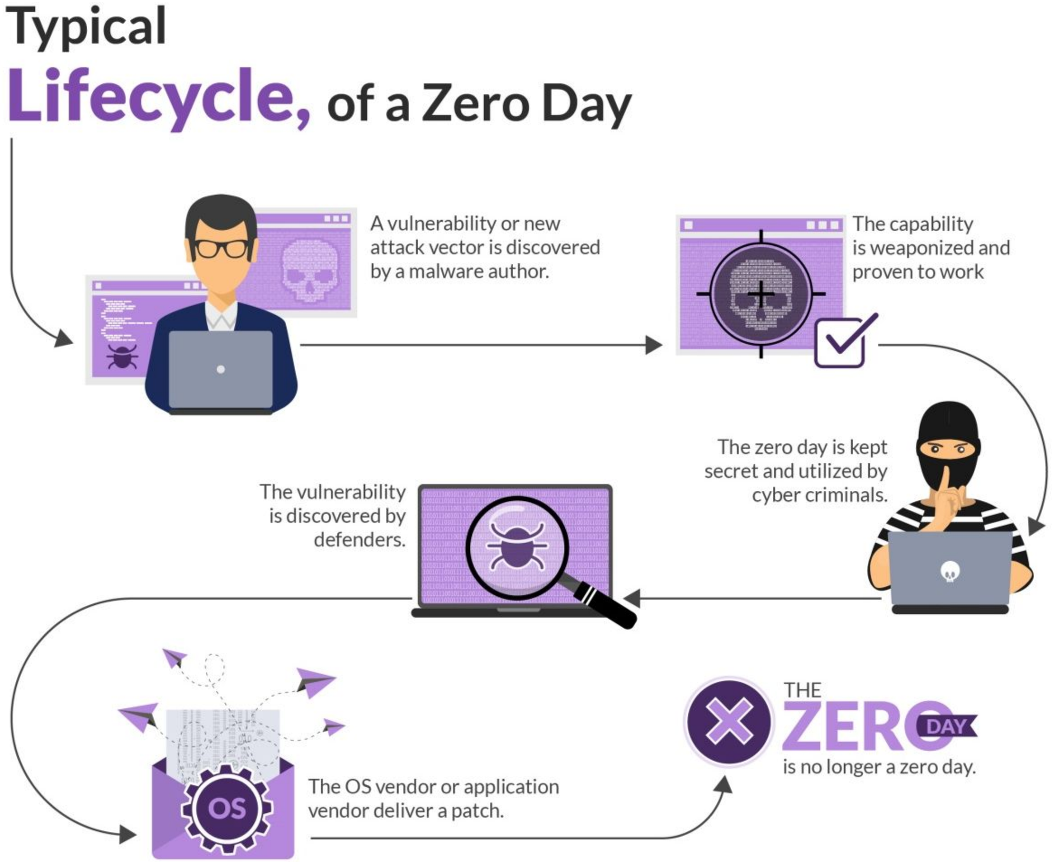
New Types of Attacks where technique unknown / undiscovered vulnerability.

- Ransomwares
- APT
- Zero day attacks
- Manipulated files/patterns
- Shared cloud IPs

Zero Day Attack

Vulnerability or attack vector is **known only to attackers,** so that it work without intervention from defenders.

At least **66 zero-days** have been found to be in use in 2021, which is almost double the number of such attacks recorded last year.



Typical **Lifecycle,** of a Zero Day

A vulnerability or new attack vector is discovered by a malware author.

The capability is weaponized and proven to work

The zero day is kept secret and utilized by cyber criminals.

The vulnerability is discovered by defenders.

The OS vendor or application vendor deliver a patch.

THE ZERO DAY is no longer a zero day.

Source: MIT Technology Review, 2021

Log4j Vulnerabilities- Recent Zero Day Attack

The Log4J vulnerability exploits, Log4Shell exploit.

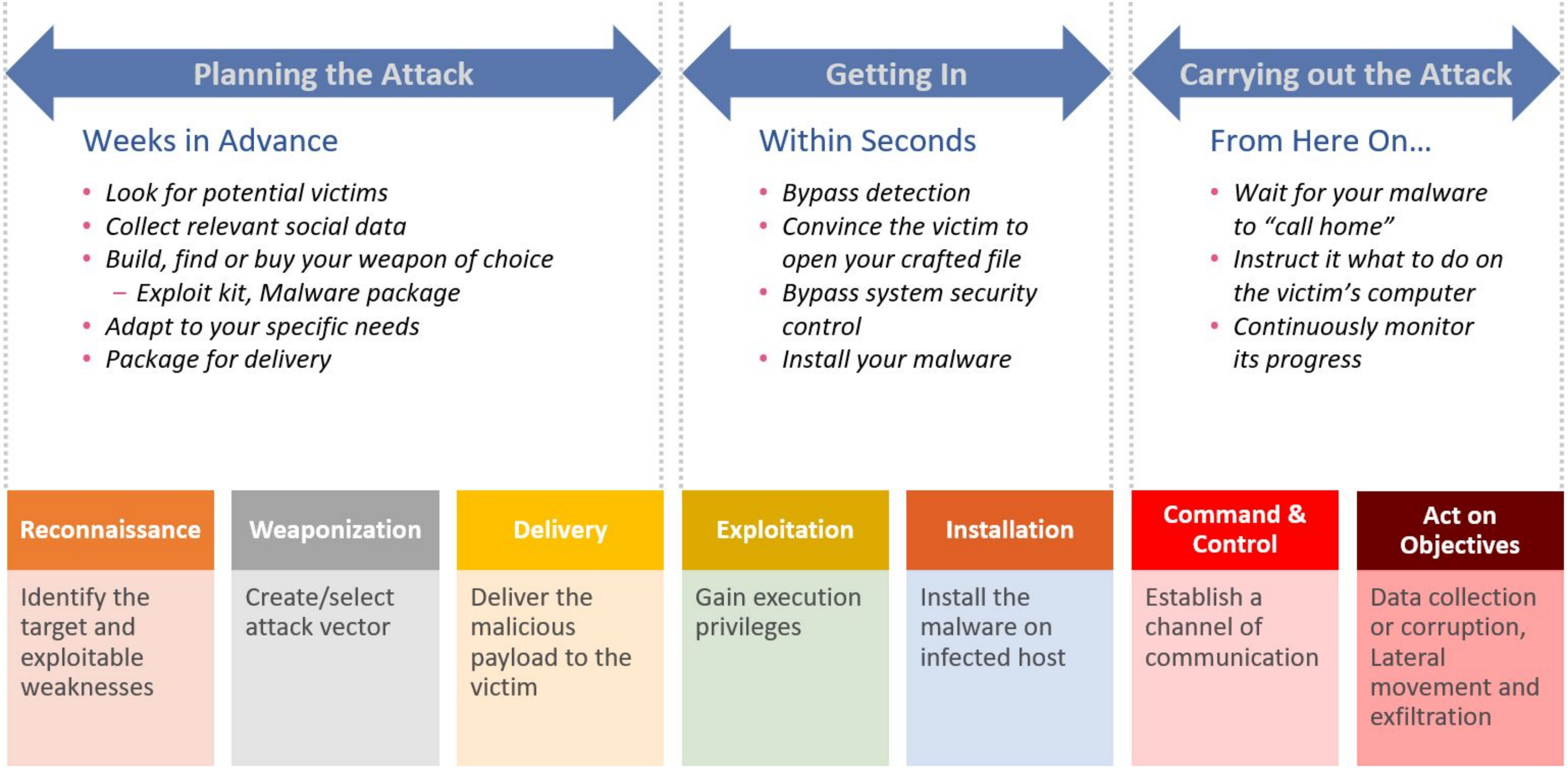
- CVE-2021-44228 (RCE)
- CVE-2021-45105 (DoS)
- CVE-2021-45046 (RCE)

Attack Vector:
Apache Log4j versions 2.16 and below fail to protect against attacker-controlled (Lightweight Directory Access Protocol) (LDAP) and other JNDI-related endpoints, according to the CVE description.

Mitigation:

- Update to 2.17.0
- Remove if not in use
- Workarounds to disable services?

Advanced Persistent Threat (APT)



Planning the Attack

Weeks in Advance

- *Look for potential victims*
- *Collect relevant social data*
- *Build, find or buy your weapon of choice*
  - *Exploit kit, Malware package*
- *Adapt to your specific needs*
- *Package for delivery*

Getting In

Within Seconds

- *Bypass detection*
- *Convince the victim to open your crafted file*
- *Bypass system security control*
- *Install your malware*

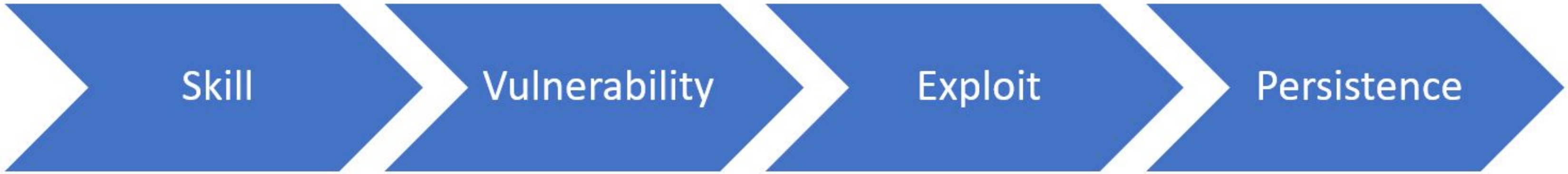
Carrying out the Attack

From Here On…

- *Wait for your malware to "call home"*
- *Instruct it what to do on the victim's computer*
- *Continuously monitor its progress*

Reconnaissance	Weaponization	Delivery	Exploitation	Installation	Command & Control	Act on Objectives
Identify the target and exploitable weaknesses	Create/select attack vector	Deliver the malicious payload to the victim	Gain execution privileges	Install the malware on infected host	Establish a channel of communication	Data collection or corruption, Lateral movement and exfiltration

Key Terms



Skill

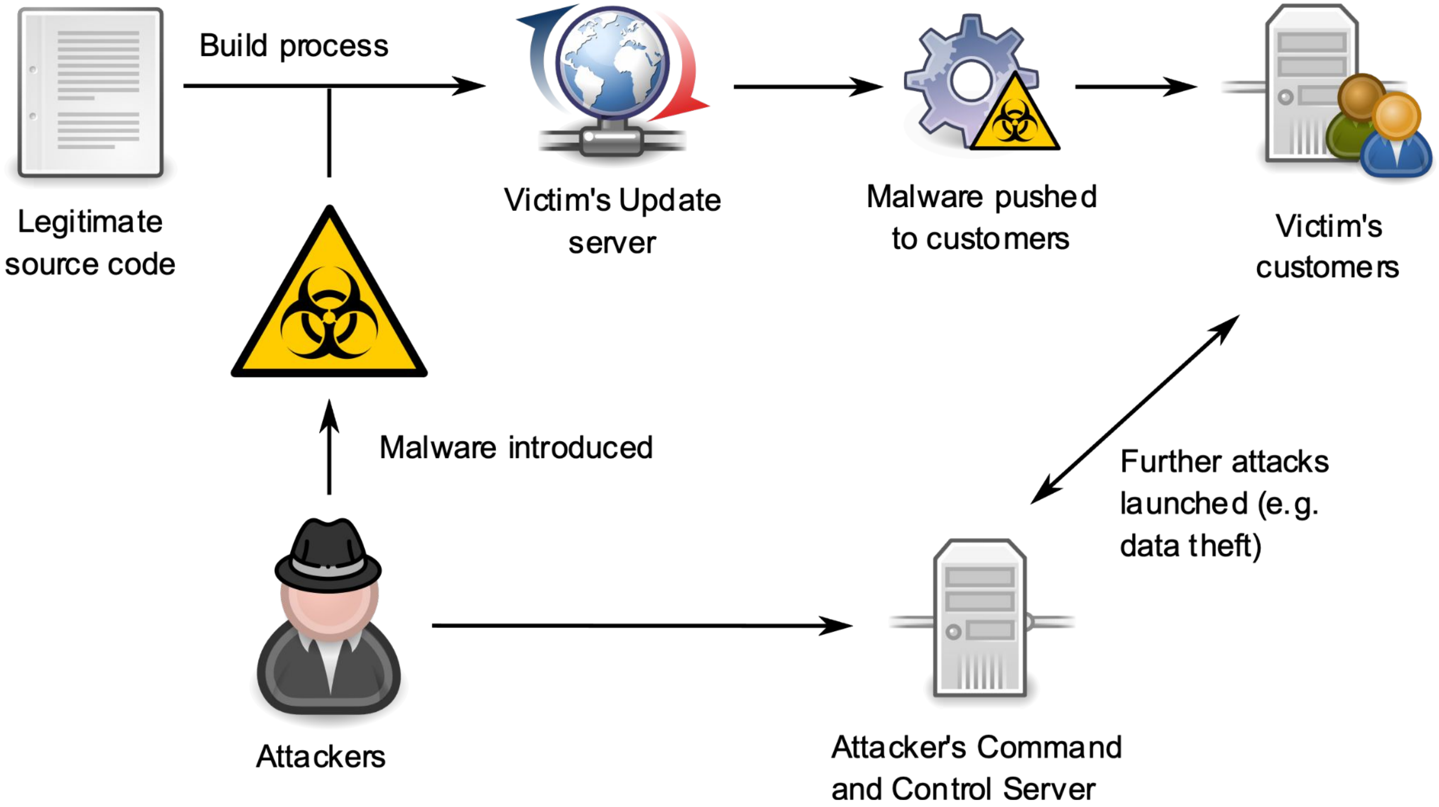
Vulnerability

Exploit

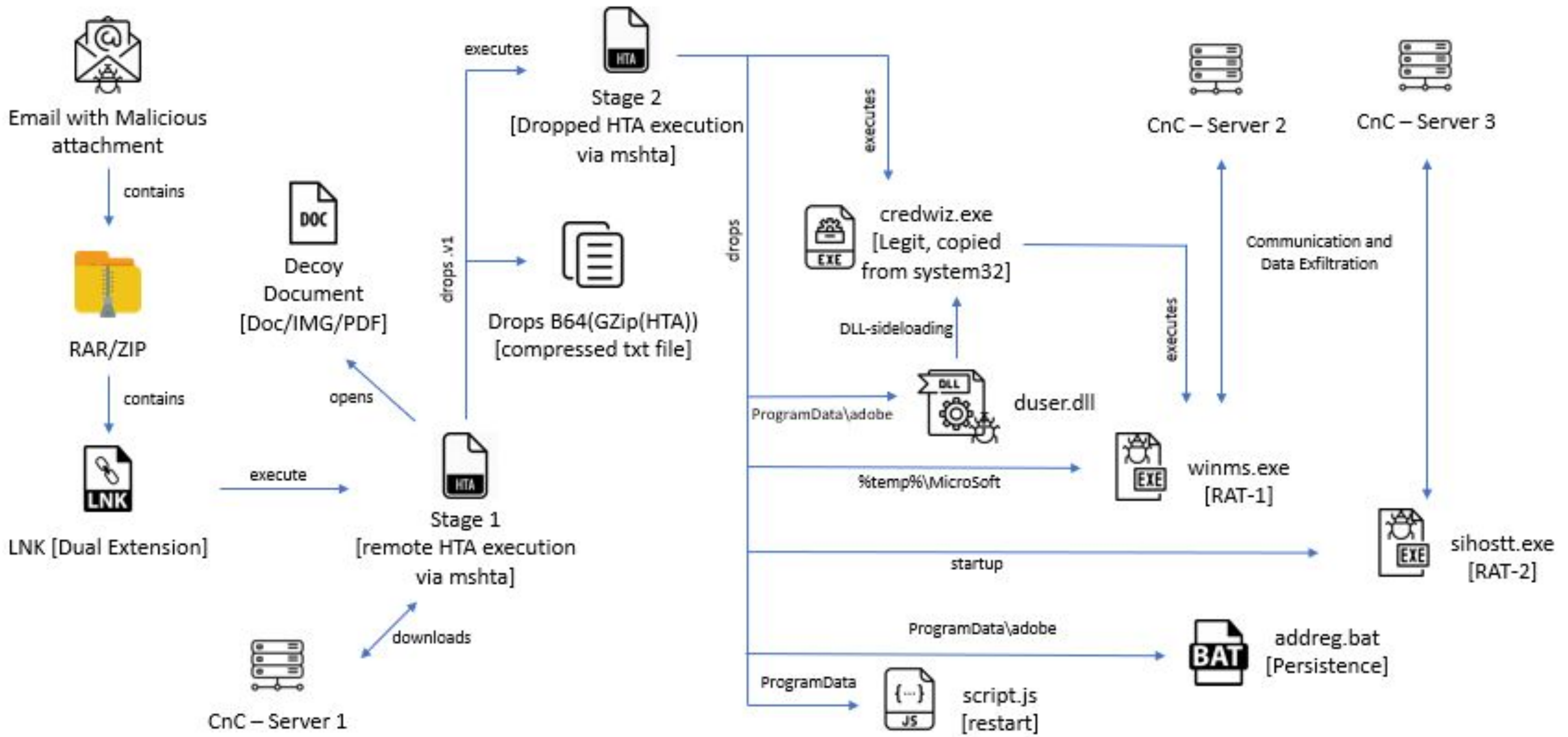
Persistence

Skill	Vulnerability	Exploit	Persistence
The key trait used to create the basis of the attack **Example:** Sharp Memory Coding Capabilities Automation	The Loophole/Gap Being Vulnerable means more prone to attacks ie exploitable Can be subverted by catching up/patching up	The attack itself which utilizes a vulnerability Can be multiple exploits for a single vulnerability OR a single exploit for multiple vulnerabilities	Remain in the ecosystem for greater gains without being noticed Defines the stealthiest of attacks

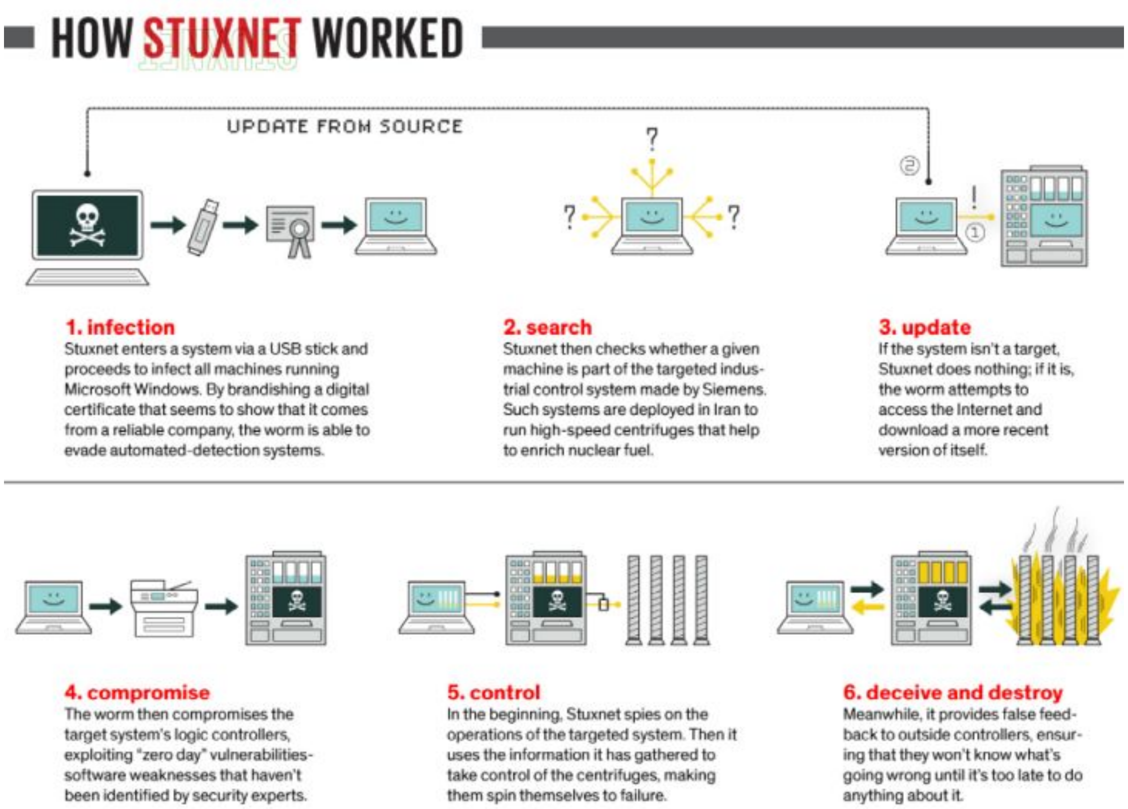
Supply Chain Attack


Build process
Legitimate source code
Victim's Update server
Malware pushed to customers
Victim's customers
Malware introduced
Further attacks launched (e.g. data theft)
Attackers
Attacker's Command and Control Server

Multi-staged APT Execution Flow



APT – Case Study



HOW STUXNET WORKED

1. infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update
If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

4. compromise
The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

5. control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

Uncovered in 2010 (2005); Four Zero Day Vulnerabilities Exploited

Target: Iran Nuclear Program, SCADA Systems

APT Propagation:

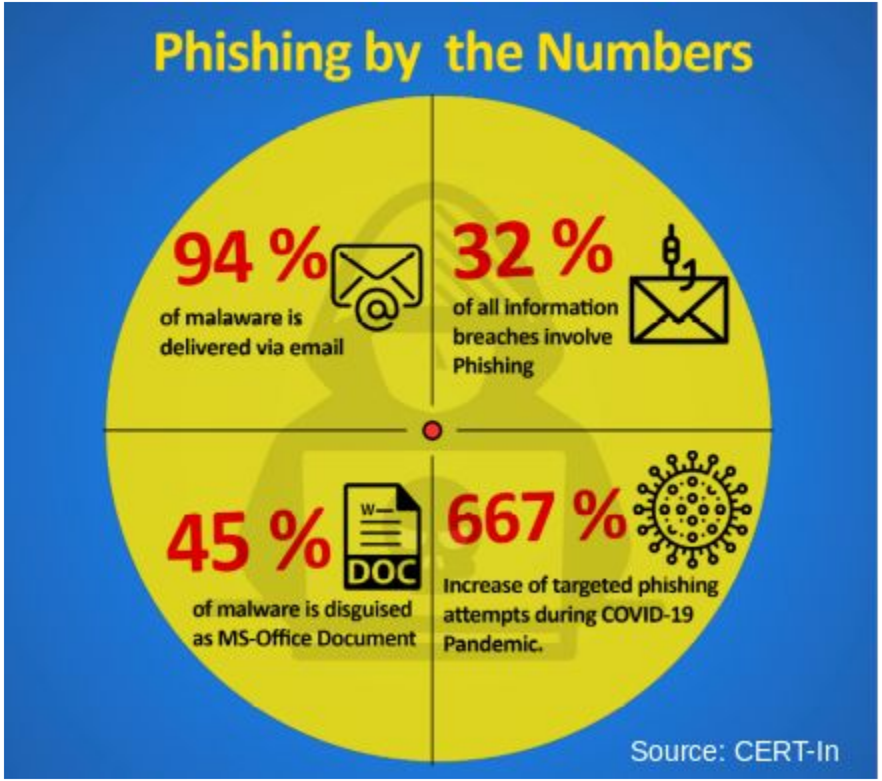
1. Introduce Malicious code into trusted process
2. Conceals malicious activity
3. Code with only minimal functionality
4. Remotely add new capabilities
5. Runs in the network's VM

Source: spectrum.ieee.org/telecom/security/the-real-story-of-Stuxnet/

Attack Vectors

- Brute force password attack
- Phishing attacks with malicious links
- An injection vulnerability
- Malicious software/application installation
- Supply chain attack
- Unhandled input / exception
- Weak / insecure / reused passwords

…………list is not exhaustive



Phishing by the Numbers

94 % of malaware is delivered via email

32 % of all information breaches involve Phishing

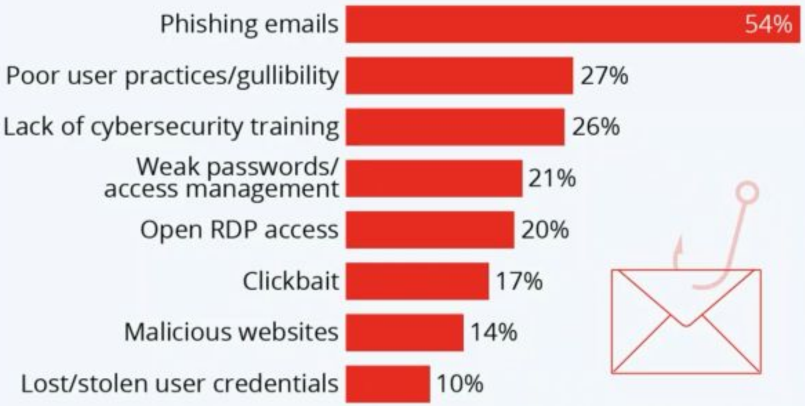
45 % of malware is disguised as MS-Office Document

667 % Increase of targeted phishing attempts during COVID-19 Pandemic.

Source: CERT-In

Phishing the Most Common Cause of Ransom Attacks

Leading causes of ransomware attacks reported by managed service providers in 2020

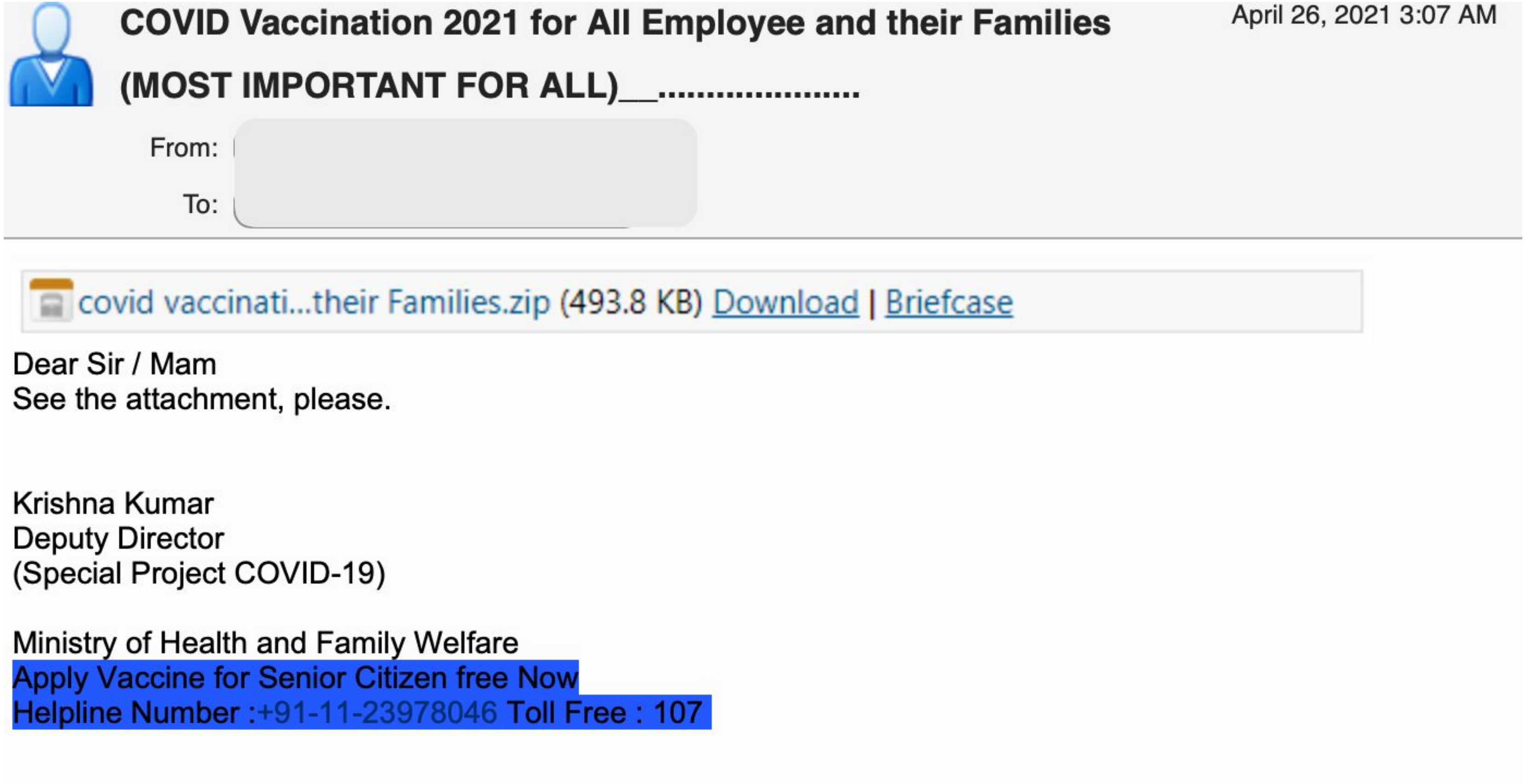


Based on a survey of 1,000+ managed service providers conducted in August 2020. Respondents were asked to pick three answers.

Source: Datto

Email remains as widely used attack vector

E-Mail Security



COVID Vaccination 2021 for All Employee and their Families (MOST IMPORTANT FOR ALL)__....................

April 26, 2021 3:07 AM

From: [redacted]

To:

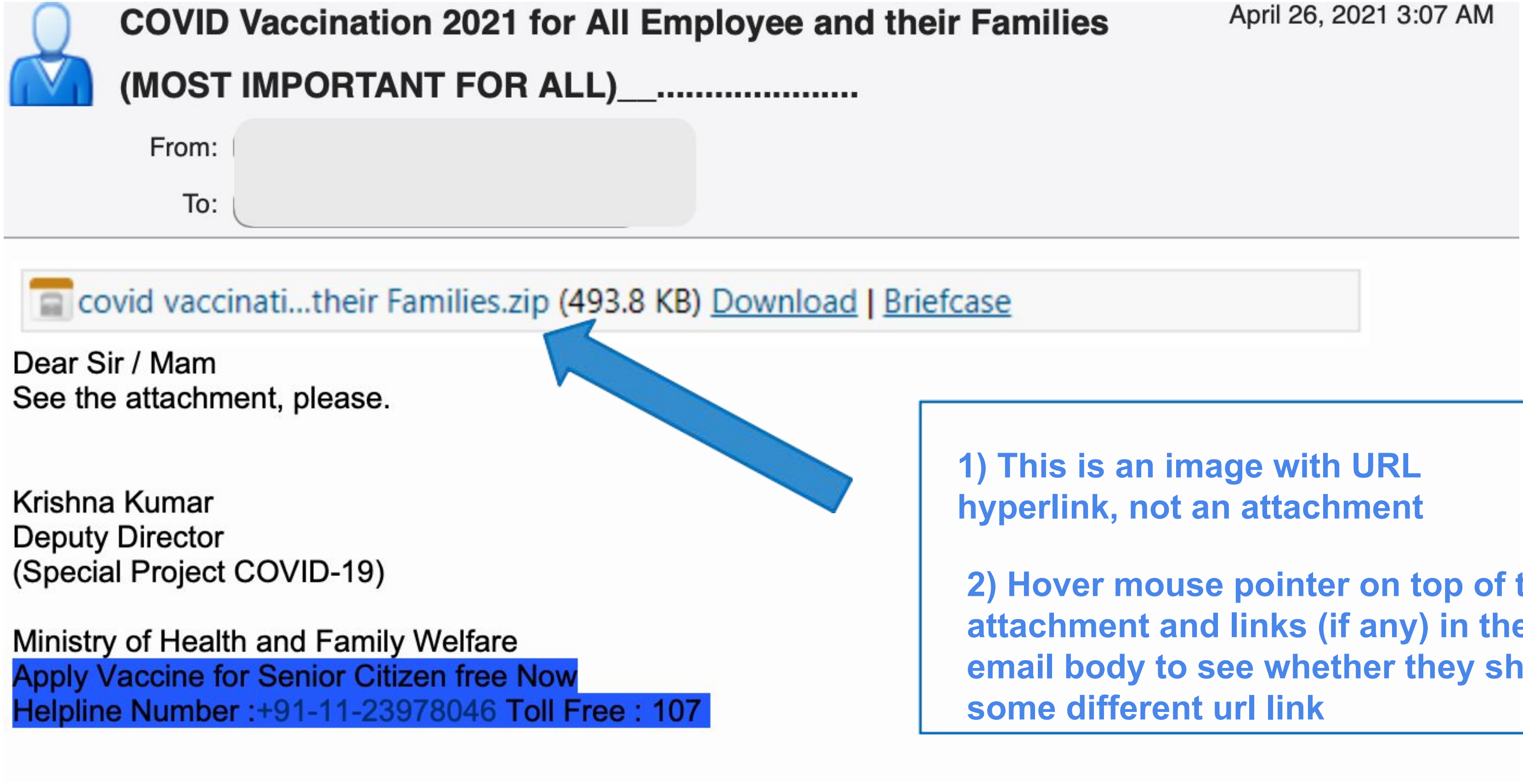
covid vaccinati...their Families.zip (493.8 KB) Download | Briefcase

Dear Sir / Mam
See the attachment, please.

Krishna Kumar
Deputy Director
(Special Project COVID-19)

Ministry of Health and Family Welfare
Apply Vaccine for Senior Citizen free Now
Helpline Number :+91-11-23978046 Toll Free : 107

Sample Phishing Email 1



COVID Vaccination 2021 for All Employee and their Families (MOST IMPORTANT FOR ALL)__....................

April 26, 2021 3:07 AM

From: [redacted]

To: [redacted]

covid vaccinati...their Families.zip (493.8 KB) Download | Briefcase

Dear Sir / Mam
See the attachment, please.

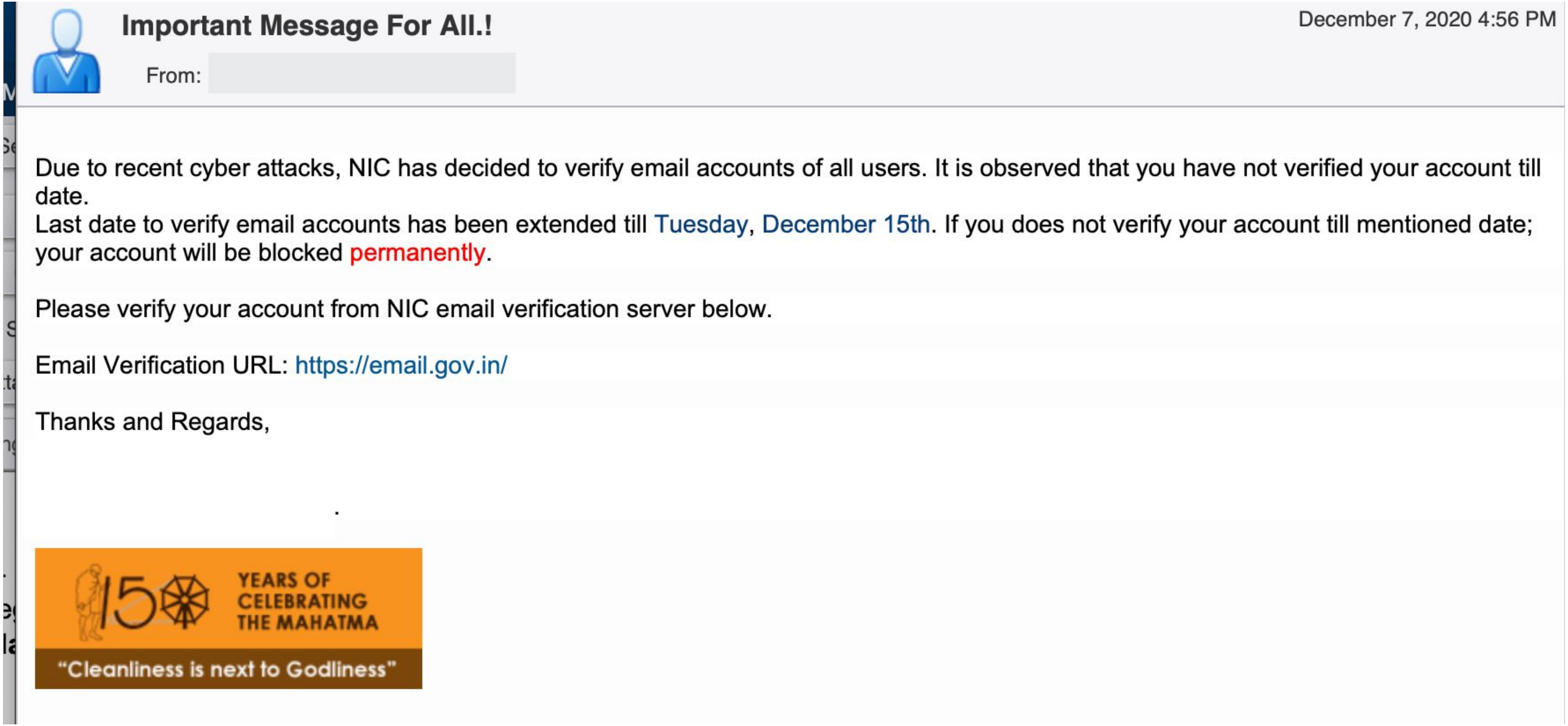
Krishna Kumar
Deputy Director
(Special Project COVID-19)

Ministry of Health and Family Welfare
Apply Vaccine for Senior Citizen free Now
Helpline Number :+91-11-23978046 Toll Free : 107

1) This is an image with URL hyperlink, not an attachment

2) Hover mouse pointer on top of the attachment and links (if any) in the email body to see whether they show some different url link

Sample Phishing Email 1



Important Message For All.!

December 7, 2020 4:56 PM

From: [redacted]

Due to recent cyber attacks, NIC has decided to verify email accounts of all users. It is observed that you have not verified your account till date.
Last date to verify email accounts has been extended till Tuesday, December 15th. If you does not verify your account till mentioned date; your account will be blocked permanently.

Please verify your account from NIC email verification server below.

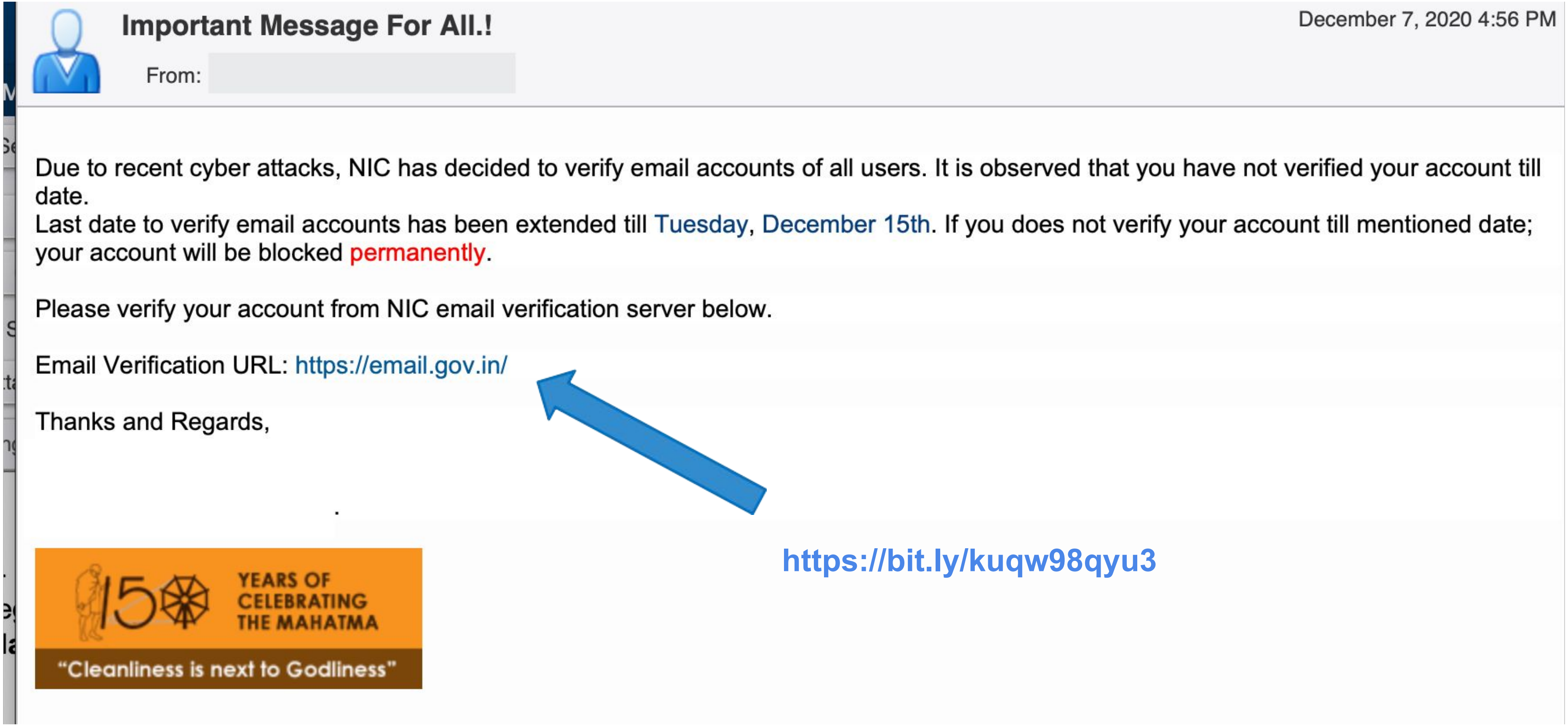
Email Verification URL: https://email.gov.in/

Thanks and Regards,

.

150
YEARS OF CELEBRATING THE MAHATMA
“Cleanliness is next to Godliness”

Sample Phishing Email 2



Important Message For All.!

December 7, 2020 4:56 PM

From: [redacted]

Due to recent cyber attacks, NIC has decided to verify email accounts of all users. It is observed that you have not verified your account till date.
Last date to verify email accounts has been extended till Tuesday, December 15th. If you does not verify your account till mentioned date; your account will be blocked permanently.

Please verify your account from NIC email verification server below.

Email Verification URL: https://email.gov.in/

Thanks and Regards,

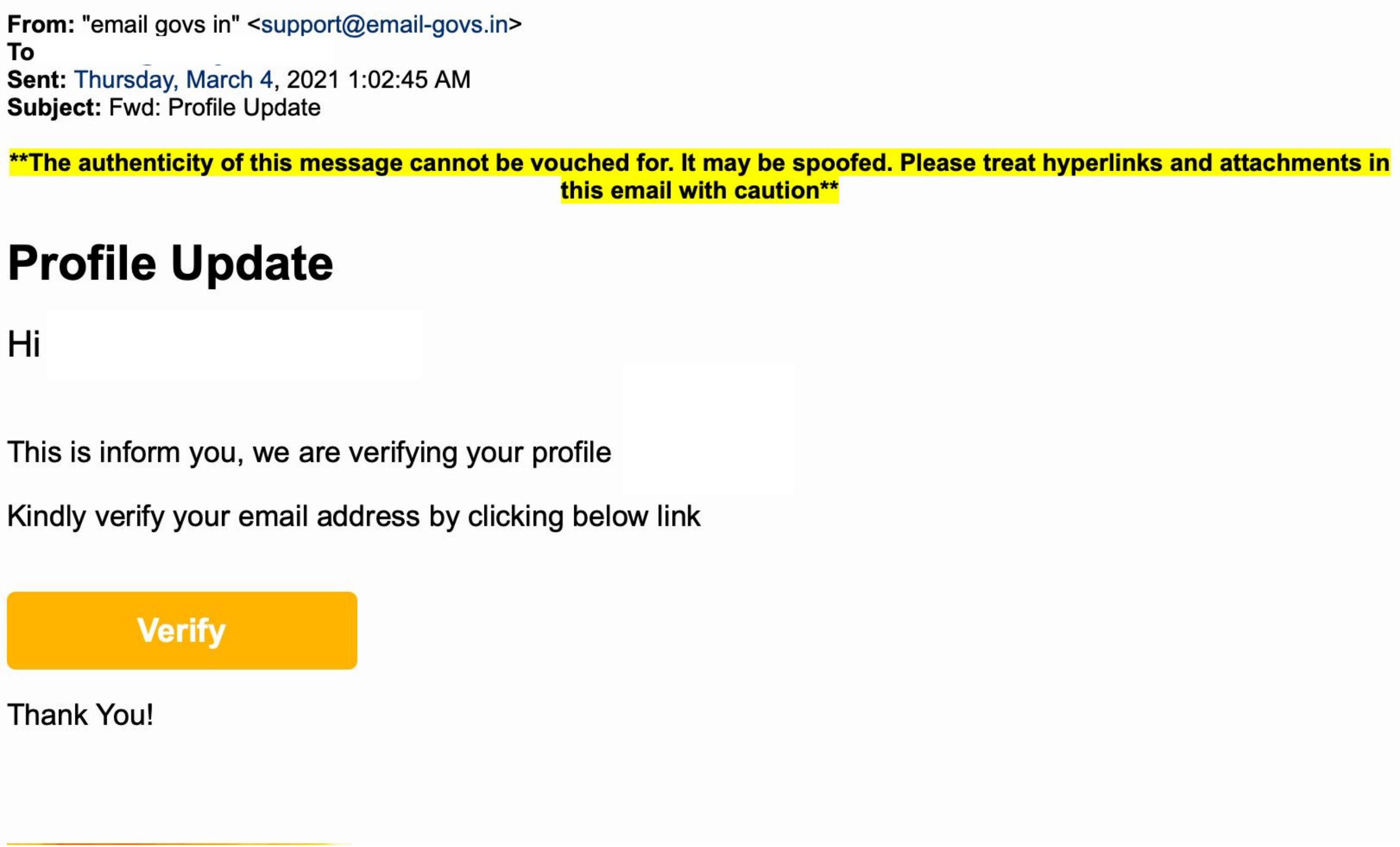
.

150
YEARS OF CELEBRATING THE MAHATMA
"Cleanliness is next to Godliness"

https://bit.ly/kuqw98qyu3

Sample Phishing Email 2

Sample Phishing Email 3



From: "email govs in" <support@email-govs.in>
To
Sent: Thursday, March 4, 2021 1:02:45 AM
Subject: Fwd: Profile Update

****The authenticity of this message cannot be vouched for. It may be spoofed. Please treat hyperlinks and attachments in this email with caution****

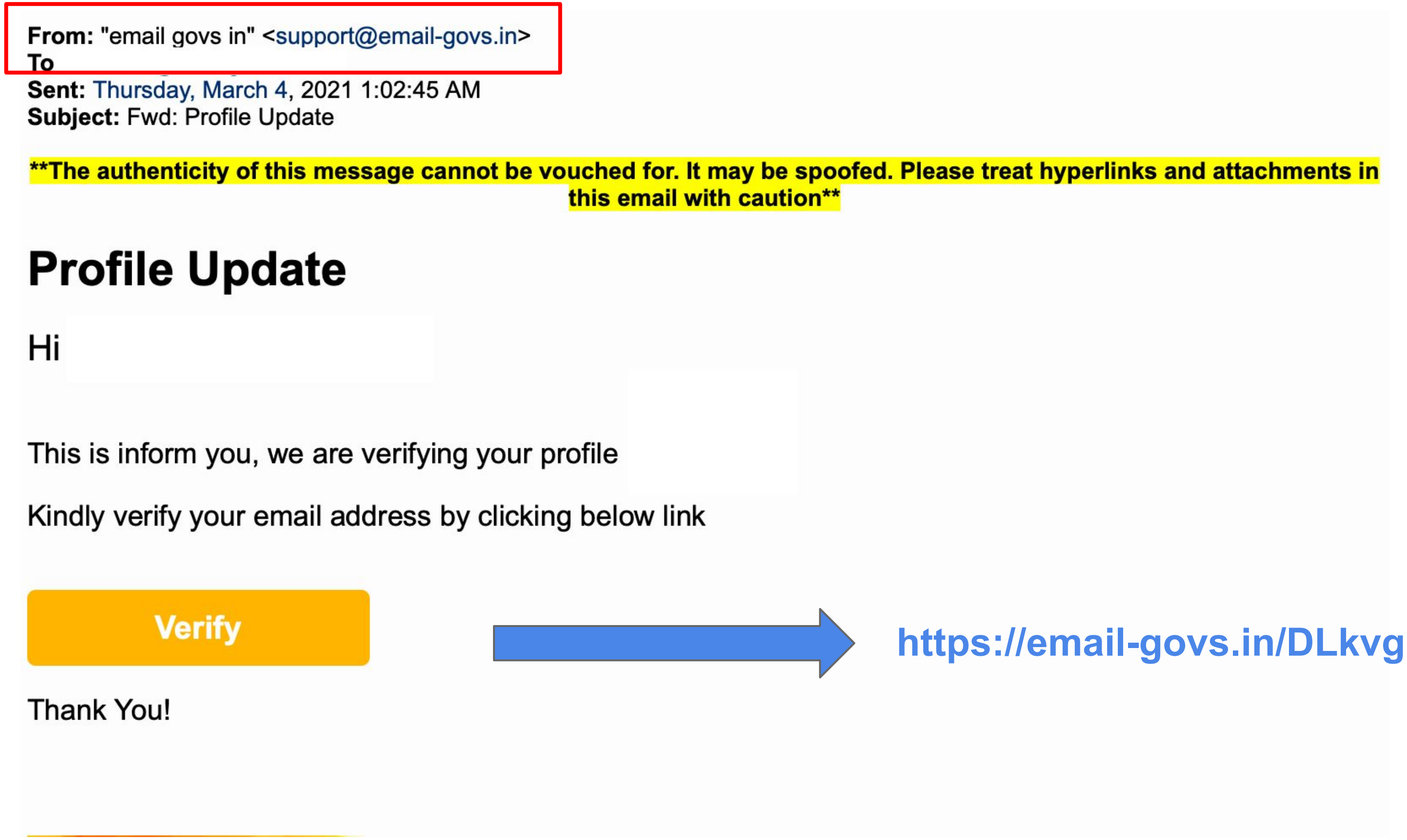
Profile Update

Hi

This is inform you, we are verifying your profile

Kindly verify your email address by clicking below link

Thank You!



From: "email govs in" <support@email-govs.in>
To
Sent: Thursday, March 4, 2021 1:02:45 AM
Subject: Fwd: Profile Update

****The authenticity of this message cannot be vouched for. It may be spoofed. Please treat hyperlinks and attachments in this email with caution****

Profile Update

Hi

This is inform you, we are verifying your profile

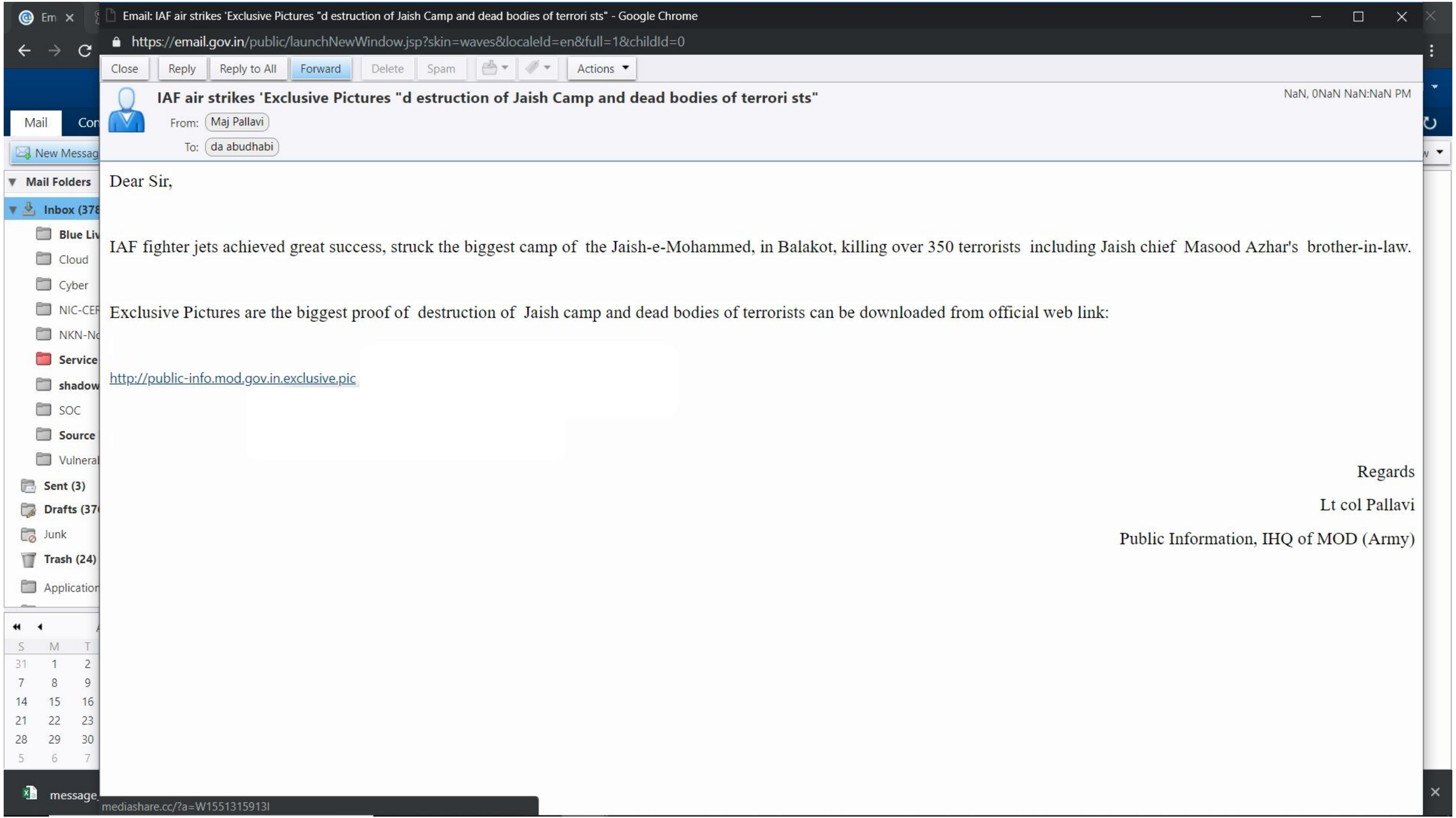
Kindly verify your email address by clicking below link

Thank You!

https://email-govs.in/DLkvgnVI

Sample Phishing Email 3

Sample Phishing Email 4



Email: IAF air strikes 'Exclusive Pictures "d estruction of Jaish Camp and dead bodies of terrori sts" - Google Chrome

https://email.gov.in/public/launchNewWindow.jsp?skin=waves&localeId=en&full=1&childId=0

IAF air strikes 'Exclusive Pictures "d estruction of Jaish Camp and dead bodies of terrori sts"

NaN, 0NaN NaN:NaN PM

From: Maj Pallavi

To: da abudhabi

Dear Sir,

IAF fighter jets achieved great success, struck the biggest camp of the Jaish-e-Mohammed, in Balakot, killing over 350 terrorists including Jaish chief Masood Azhar's brother-in-law.

Exclusive Pictures are the biggest proof of destruction of Jaish camp and dead bodies of terrorists can be downloaded from official web link:

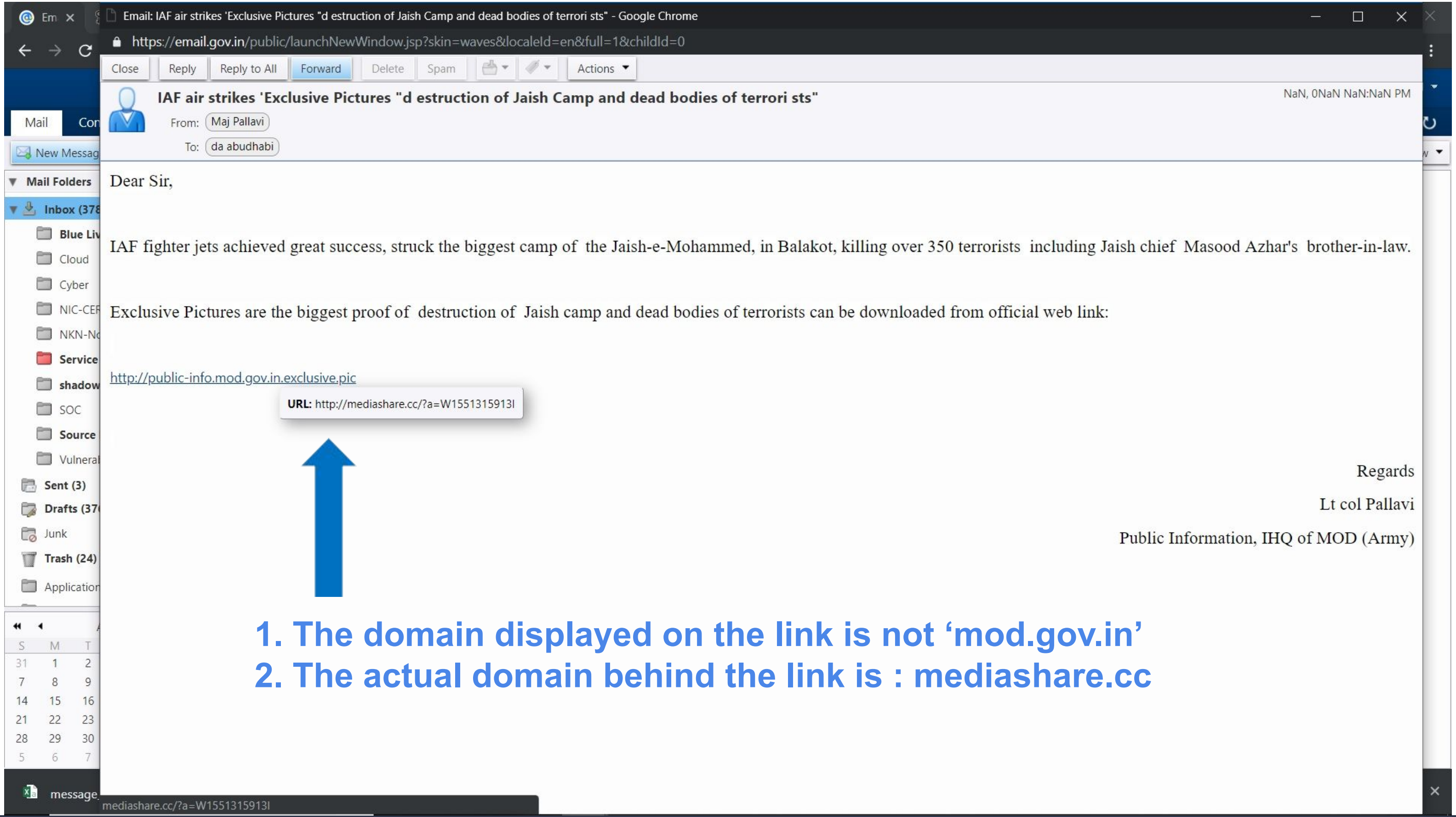
http://public-info.mod.gov.in.exclusive.pic

Regards

Lt col Pallavi

Public Information, IHQ of MOD (Army)

mediashare.cc/?a=W1551315913l


Email: IAF air strikes 'Exclusive Pictures "d estruction of Jaish Camp and dead bodies of terrori sts" - Google Chrome
https://email.gov.in/public/launchNewWindow.jsp?skin=waves&localeId=en&full=1&childId=0
Close
Reply
Reply to All
Forward
Delete
Spam
Actions
Mail
New Messag
Mail Folders
Inbox (378
Blue Liv
Cloud
Cyber
NIC-CER
NKN-Nc
Service
shadow
SOC
Source
Vulnera
Sent (3)
Drafts (37
Junk
Trash (24)
Application
message

IAF air strikes 'Exclusive Pictures "d estruction of Jaish Camp and dead bodies of terrori sts"

NaN, 0NaN NaN:NaN PM

From: Maj Pallavi

To: da abudhabi

Dear Sir,

IAF fighter jets achieved great success, struck the biggest camp of the Jaish-e-Mohammed, in Balakot, killing over 350 terrorists including Jaish chief Masood Azhar's brother-in-law.

Exclusive Pictures are the biggest proof of destruction of Jaish camp and dead bodies of terrorists can be downloaded from official web link:

http://public-info.mod.gov.in.exclusive.pic

URL: http://mediashare.cc/?a=W15513159131

Regards

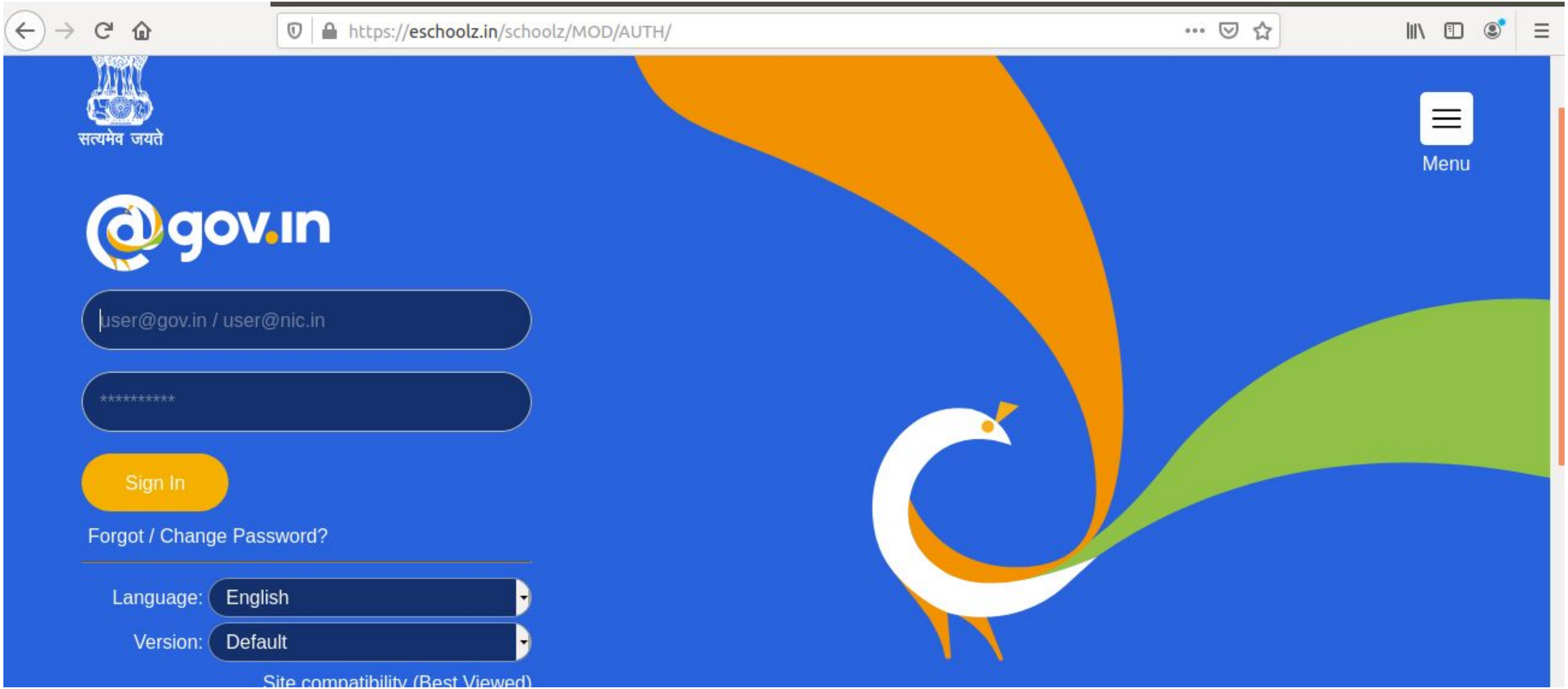
Lt col Pallavi

Public Information, IHQ of MOD (Army)

mediashare.cc/?a=W15513159131

1. The domain displayed on the link is not ‘mod.gov.in’
2. The actual domain behind the link is : mediashare.cc

Sample Phishing Email 4



https://eschoolz.in/schoolz/MOD/AUTH/

user@gov.in / user@nic.in

****

Language: English

Version: Default

Sample Phishing Page

Common Patterns in Phishing

- Phishing mail sent to targets with links of shortened urls, file sharing sites
- Mails with Password protected attachments. The password is provided in the mail body or in a separate attached text file
- Compromised accounts used to send phishing mail
- Recent events like covid, vaccination, Govt guidelines, 7th pay commission, salary/DA Arrears…etc., are used as phishing lures
- Links to files hosted on File Sharing sites/ Cloud storage (ex: google drive, onedrive..etc)
- Re-direction to external sites
- Mails sent to multiple recipients, mailing lists, bcc

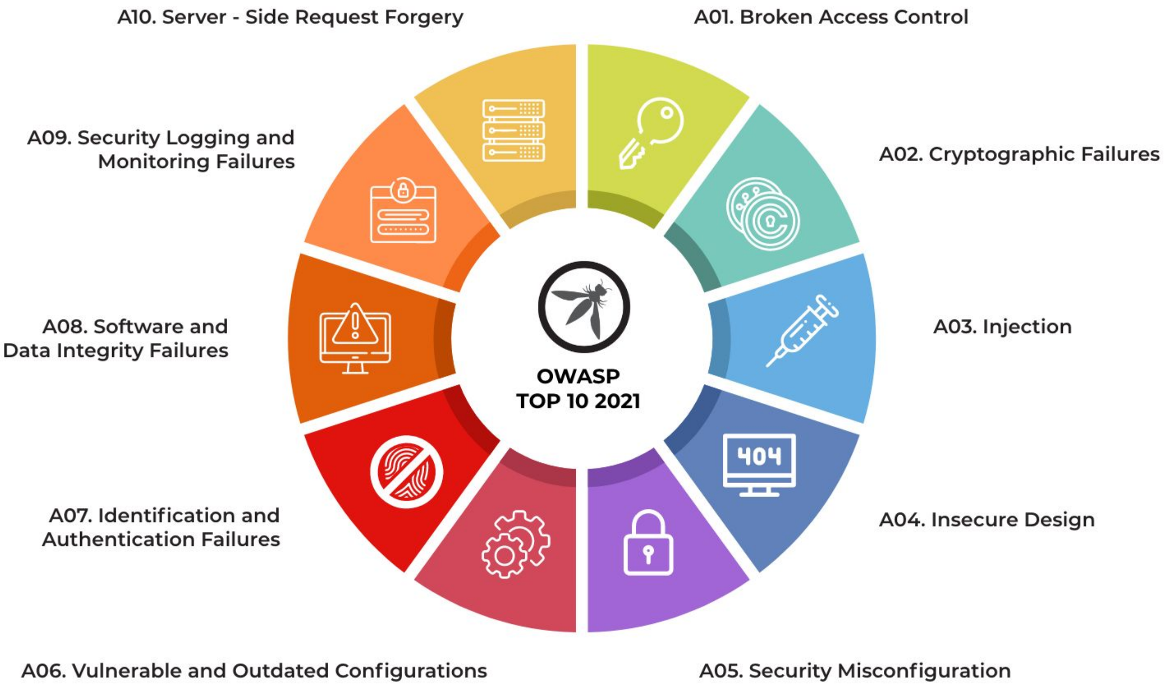
Cyber Incident Reporting

- **Notify** your organization’s help desk or the IT-Team immediately
- **Don’t attempt** to investigate or remediate the incident on your own.
- **Inform other users** of the system and instruct them to stop work immediately.
- Unless instructed, **do not power down** the machine.
- Unless instructed, **do not remove the system** from the network.
- Organization **CERT/security** team will contact you to **get additional information**
- Each organization is required to have a **specific plan to handle security incidents.**

Opportunities

- Security Architect / Security Engineer
- Ethical Hackers
- NW / System / DC Administrator
- Security Tester / VAPT specialist
- Security Auditor (OWASP, ISO/IEC 27001/2)
- Forensic Analyst
- OT/ICS/SCADA Security Specialists
- Researcher or an Educator

OWASP Top 10



A10. Server - Side Request Forgery

A01. Broken Access Control

A09. Security Logging and Monitoring Failures

A02. Cryptographic Failures

A08. Software and Data Integrity Failures

A03. Injection

A07. Identification and Authentication Failures

A04. Insecure Design

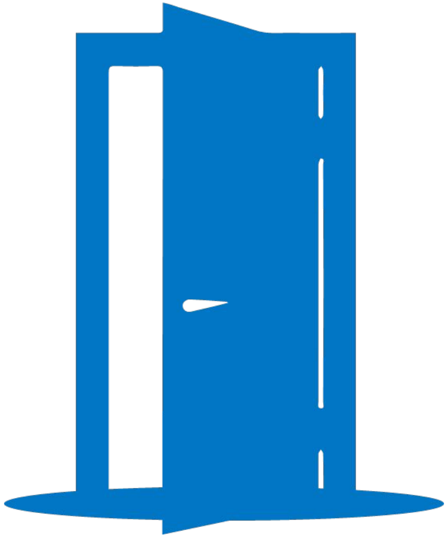
A06. Vulnerable and Outdated Configurations

A05. Security Misconfiguration

Thank you

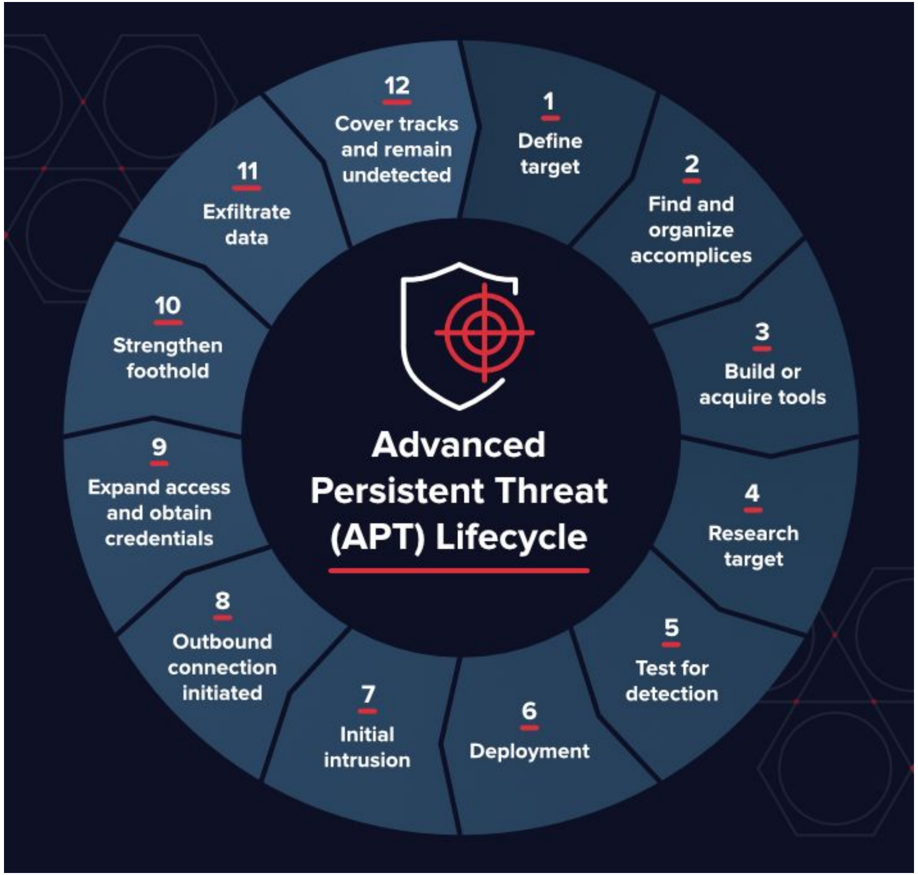
Gulshan Gupta
SAC-ISRO, Ahmedabad

For further queries/contact:
gulshang@sac.isro.gov.in



“Cyber Security should be built-in not bolted on”

Advanced Persistent Threat (APT)


Advanced Persistent Threat (APT) Lifecycle
1 Define target
2 Find and organize accomplices
3 Build or acquire tools
4 Research target
5 Test for detection
6 Deployment
7 Initial intrusion
8 Outbound connection initiated
9 Expand access and obtain credentials
10 Strengthen foothold
11 Exfiltrate data
12 Cover tracks and remain undetected

- ➢ **Advanced**: Full spectrum of intelligence gathering techniques
- ➢ **Persistent**: low-and-slow approach, Continuous monitoring and interaction
- ➢ **Threat**: specific objectives and coordinated human actions and well funded

Approach: Self-destructing malware and sniffers, small file size and common names don’t raise flags

Targets: .mil, .gov sites, defense, vendors, High profile Users and CEOs