Work from Home (WFH) During the Pandemic: A Study of Situational Crime - Vulnerabilities, Threats and Countermeasures

Eswara Sai Prasad Chunduru[1], Nagendar Rao Koppolu[2]

[1]Assistant Director, Digital Forensic Division, Central Forensic Science Laboratory, Hyderabad
[2]Inspector of Police (In-charge State Cyber Vertical), Telangana Police Department, Hyderabad

---

Abstract: *The concept of Working From Home (WFH) is not a new one, but due to the current COVID-19 situation, WFH has gained a lot of attention. Several organizations have migrated their workforce to work from home to achieve their business goals without any or minimum disruption while safeguarding their workforce from the COVID-19 situation. However, due to the lack of policies, technology, and training to secure this remote workforce, it became a challenge for organizations to manage their valuable information resources. This paper showcases the various vulnerability factors, associated threats, attack vectors, and prevention measures in the situational crime scenario (Work from Home (WFH).*

Keywords: Work From Home, Situational Crime, Measures of Prevention, Cyberspace, Trends, Pandemic Countermeasures.

1. INTRODUCTION

1.1. Work From Home (WFH):

Work from home (WFH) is defined as work done remotely, mainly from residence, instead of at an office. The concept of WFH is not a new practice and many organizations, particularly IT-based ones, are allowing their employees to choose this model when there is a difficulty or when the situation demands it. WFH is not too familiar or a day-to-day routine but applied in particular conditions faced by employees, such as health issues, family difficulties, and maternity issues. Only under such circumstances do organizations generally permit their employees. It is generally a temporary arrangement.

1.2. Why Work From Home:

The workforce of organizations occasionally chooses WFH for many reasons. For example, to meet the targets and timelines, family difficulties, health issues, maternity issues (particularly for women), freelancing, infrastructure renovation, and other situational compulsions.

1.3. Advantages of WFH:

There are many advantages to WFH for both the employee and the employer. Some are –

a. Minimum distractions and increased output.
b. Organizations benefit from the remote workforce by getting the tasks completed faster with possible minimum mistakes.
c. Less commutating and time saver.
d. More productivity because of less human interaction.
e. Happier, improved work-life balance and dynamic routine.
f. Saves physical office space and expenditure of the organization.
   Examples: food, stationery, water, electricity, and other physical infrastructural resources.
g. An increased overview into other markets.
h. Longevity of work period.
i. Increased loyalty.
j. Wide spectrum of available employees for hiring across the Globe.

k. Lucrative freelancing opportunities for the employees.

1.4. Disadvantages of WFH:

While there are various advantages, as mentioned above, making organizations encourage WFH, the obverse side is not rosy. Being said that, some of the shortcomings of WFH are –

a. Lack of community and lack of opportunity of working in diversified working cultures and missing tight-knit camaraderie.
b. Communication muddle.
   Ex: delayed tech and other support.
c. Procrastination and less accountability.
d. Payment logistics such as international transfers to confusing tax laws.
e. Managing productivity
f. Security concerns:
   i. Physical Security Concerns:
      1) The loss of computing devices is catastrophic.
      2) Damage to the hardware.
   ii. Cyber Security Concerns:
      1) Possibility of leakage of sensitive data
      2) Potential frauds associated with online financial transactions.
      3) Maintaining the CIA (Confidentiality, Integrity and Authenticity) of the information while storing, accessing, and transmission.
      4) Loss of payment credentials and multimedia data leakage, over ongoing virtual meetings.
      5) Volunteered or un-volunteered Cyber-attacks arising from unsafe and open networks.
      6) Unnoticed privilege escalations.
      7) Data loss arising from unreliable networks.
      8) Data theft arising from Fake VPNs, Encryption Software, Phishing, Shoulder Surfing.
      9) Distinguished cyber laws of the land.

The following figures (Fig - 1, 2, 3) are a representation of the advantages, disadvantages, and Cyber Security concerns of WFH:

Fig – 1: Advantages of WFH (Source: https://public.tableau.com/profile/meera6133#!/)

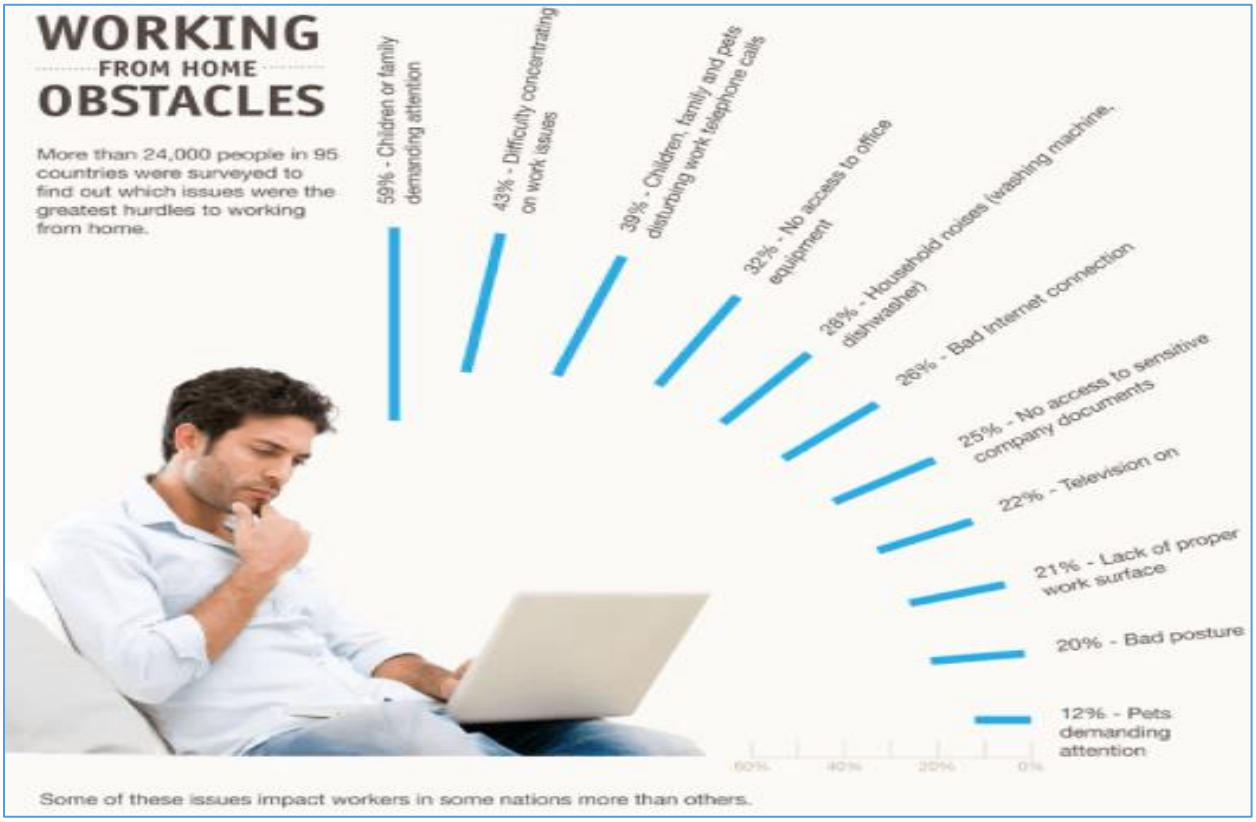

Fig – 2: Disadvantages of WFH (Source: https://cdn.lifehack.org/wp-content /uploads/2013/05/)

Fig – 3: Cyber Security Issues [9]

The below figures (Fig. 4, 5) represent the percent of the working population people across the World and India who think work from home is a new normal.

Fig – 4: Working Population Across the World [21]

Fig – 5: Working Population In India [21]

1.5. Corona Virus Disease -19 (COVID-19):

COVID-19, a. k. a. Novel Corona Virus, is a deadly, contagious, swiftly hiking, primarily affecting the body through the respiratory system that causes a human to approach death in a short span. As per World Health Organization (WHO), it spreads by coughing, sneezing, and contacting the person affected by the virus. In most scenarios, with the proper initial assessment and care, people infected with the COVID-19 virus can recover without special treatment. Older adults, and those with co-morbidities like cardiovascular disease, diabetes, chronic respiratory disease, and cancer, etc., are more likely to develop severe illnesses. For now, the COVID-19 pandemic is first a health and humanitarian crisis. Human contact and congregation can enormously favor the spread of the virus. With the spread of the second wave across the Globe and with the slow pace of vaccination, it appears that till mid-2022, the risk of the pandemic threatens humans. The below Figures (Fig. 6, 7) shows the trend of COVID-19 positive infections, daily change across the World and in India:

Fig – 6: COVID-19 positive infections Across the World (Source: Wikipedia)

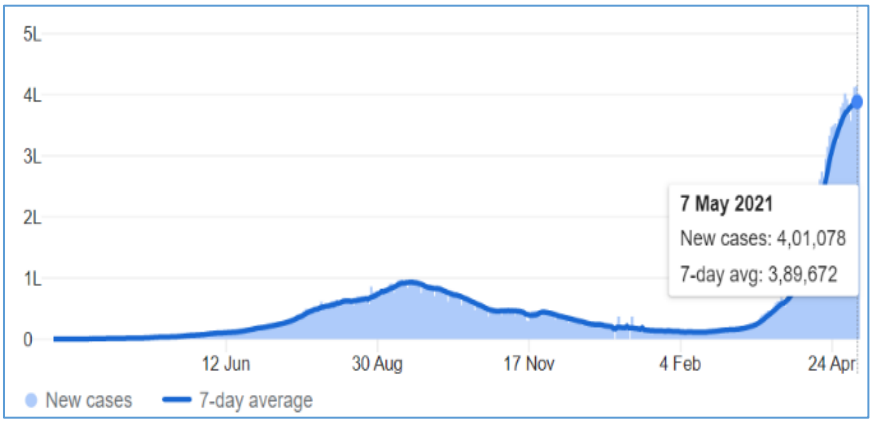

Fig – 7: COVID-19 positive infections In India (Source: Wikipedia)

1.6. Situational Crime:

A particular instance of the crime resulting from a state favoring less effort, more damages, hefty rewards, and possible legal cleansing. WFH is favoring crimes, especially in the virtual space, arising from the unique situation of COVID-19. The disadvantages associated, as mentioned above, with WFH favors a Situational Crime and the review of the cyber incidents in the past few months suggest the same [5]. The below Figures (Fig. 8, 9, 10) shows the trend of Cybercrime Incidents and timeline in the last few months and its timeline–

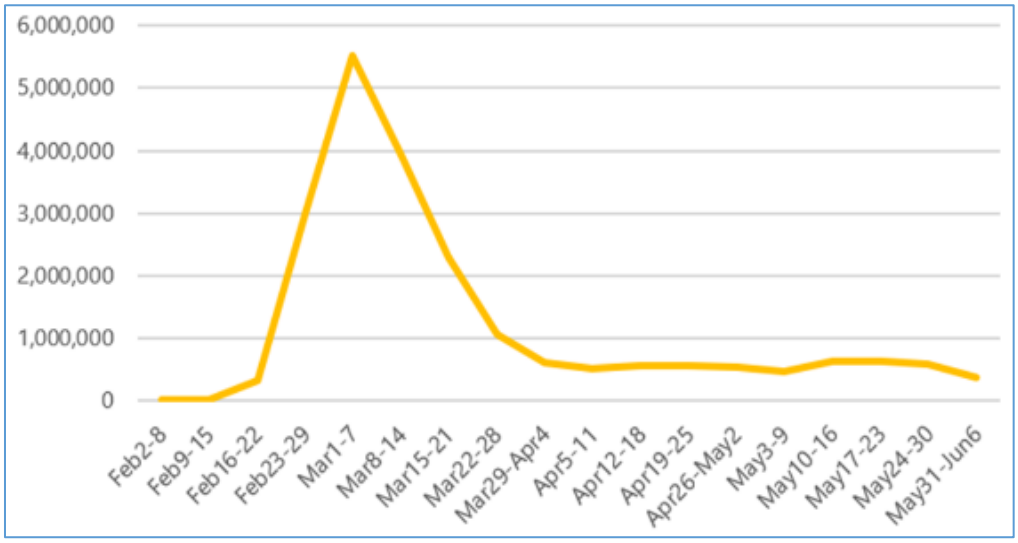

Fig – 8: The trend of COVID-19 themed attacks

(Source: https://www.forbes.com/sites/leemathews/2020/06/17/microsoft-covid-19-cyber-attacks-peaked-in-march-and-fell-off-quickly/?sh=1b227343c9aa)

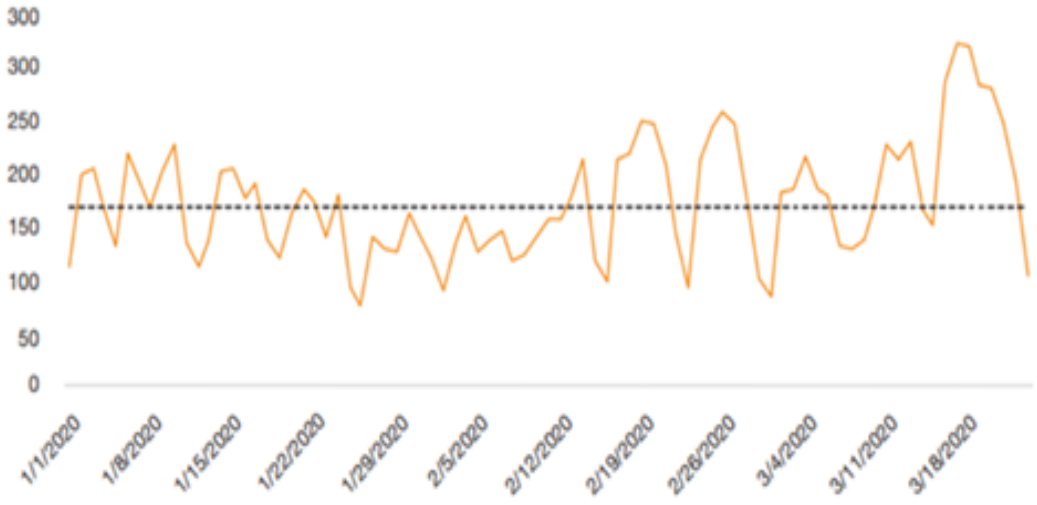

Fig – 9: Volume of attacks (Source: PwC India Cyber Protection Centre)

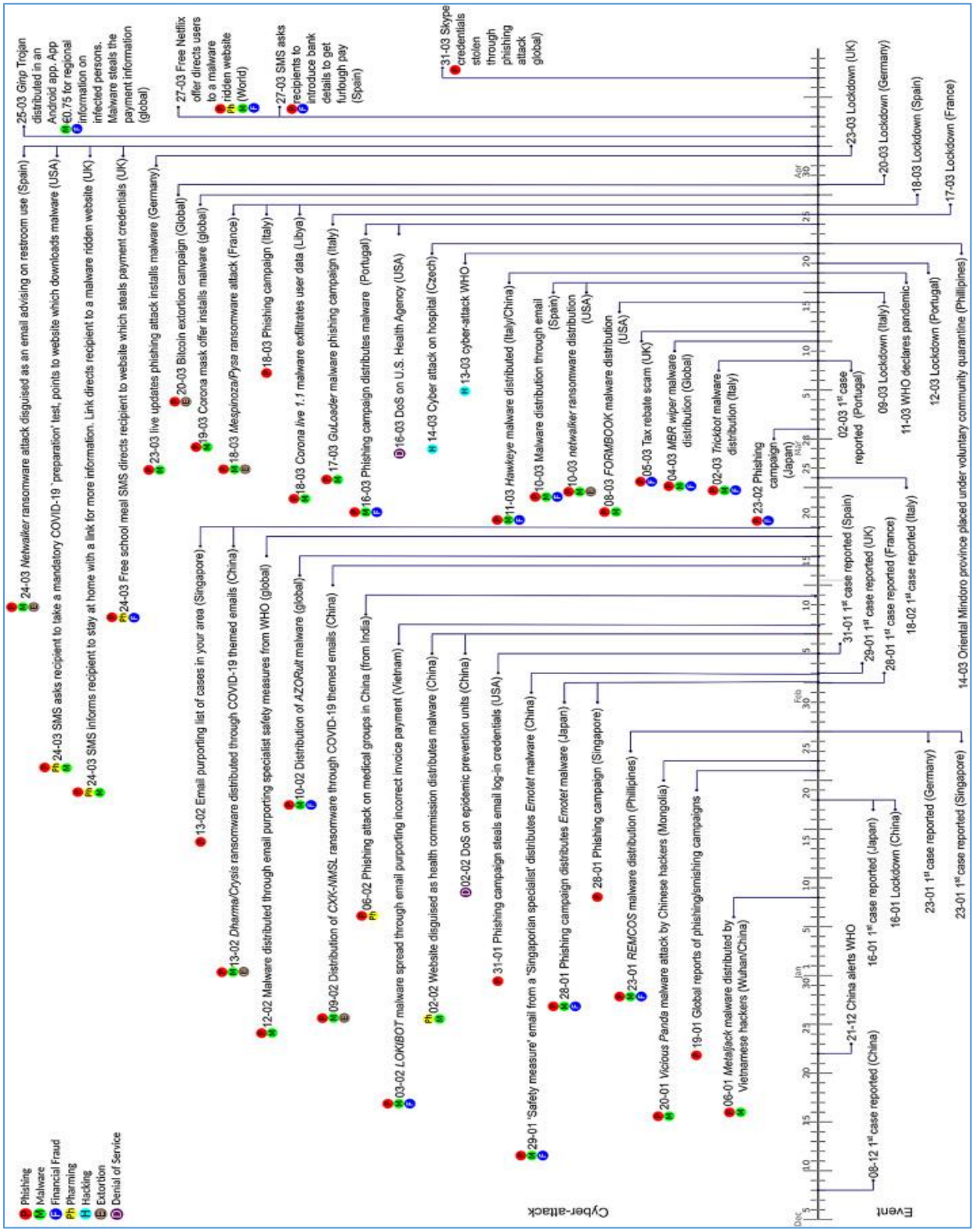

Fig – 10: Timeline of Attacks [6]

2. A Study of Work from Home (WFH) as a Situational Crime

As discussed in the introduction, the unique situation of COVID-19 mandates WFH, a new standard and way of life for the time being. This particular situation associated with the negative factors, apart from the virtues, favors the various Situational Crimes, especially Cybercrimes. The recent Cybercrime trends related to the COVID-19 pandemic are nothing but a class of Situational Crime. The factors that favor these incidents suggest that the disadvantages associated with WFH are the motivation. We will discuss these favorable factors and the various Cybercrime trends observed during the pandemic and explore the measures to combat these situations.

3. WFH – Cybercrime Trends

A report by Microsoft Inc. indicates approximately 9,000 plus attacks themed on coronavirus were noticed in India between February and May 2020. They include Malware or URL or an attachment or a phishing email using COVID-19 as a lure for compromising the information resources. Employees in WFH are the most targeted ones in these attacks by Cybercriminals. These attacks are targeting vulnerable places like healthcare organizations, state and local governments, and critical infrastructure. COVID -19 themed attacks saw a rise by 7% during the first two quarters of 2020; hackers also capitalized on the increased adoption of Microsoft Office with 22% of malicious Microsoft Office files and 11% of all PDF files, making up 33% of all newly identified Malware. It has been observed that 12,910 new variants of Malware in the first six months of 2020 (Report by SonicWall). The below illustration indicates the trend of malware attacks in the recent past under the pandemic [1][3].

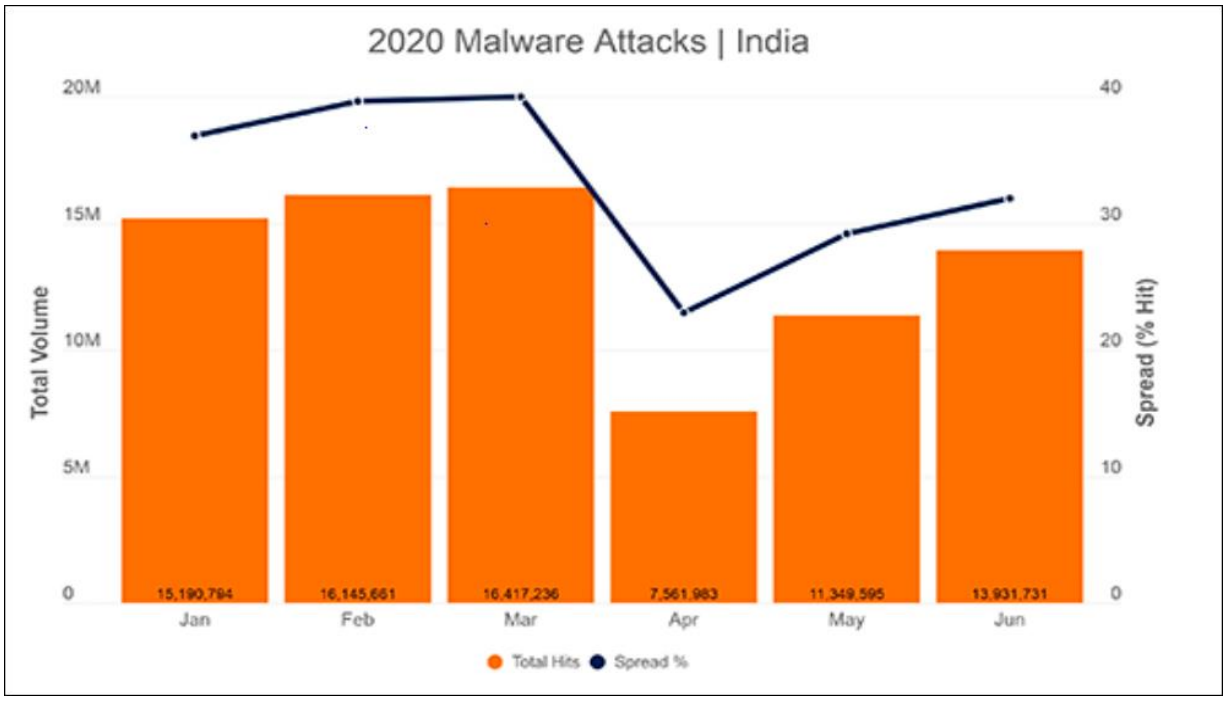

Fig – 11: Trends of Malware Attacks [22]

Further, there is a 50% rise in IoT malware cases, indicating hackers are trying to get into sensitive data through sensors in devices such as refrigerators, baby cameras, doorbells, and gaming consoles. Hence unchecked IoT devices can provide Cybercriminals with an opening into secure infrastructure. The above illustration shows the trend of Malware Attacks in India for the last few months. Also, increased use of non-standard ports has been observed to evade detection and deployment of Malware by Cybercriminals. The above data indicate that the attackers are now taking advantage of businesses adopting WFH.

A report from Kaspersky detected 93 coronavirus-related Malware in Bangladesh, 53 in the Philippines, 40 in China, 23 in Vietnam, 22 in India, and 20 in Malaysia [8].

Similarly, research conducted by Fortinet, an American Cybersecurity Enterprise, shows that every day an average of about 600 new phishing campaigns are being run. While they have identified 119 major coronavirus campaigns that were run globally, the most recent campaign, according to them, was detected on 24th March 2020. The phishing email was sent to the Canadian government health department and contained an RTF phishing lure that came from a spoofed address, noreply@whoint. Recently, Indian government agencies had to clarify malicious emails and messages disseminated on WhatsApp, claiming that the government provides Rs 1,000 under the fake *Corona Sahayata Yojana Scheme*. Press Information Bureau (PIB) clarified that both the claim and link were fraudulent and warned people against clicking on them. Also, fake accounts are circulated on the pretext of the Prime Minister's Citizen Assistance and Relief in Emergency Situations Fund (PM-CARES Fund). Also, phony ransom-seeking email scams are growing. Computer Emergency Response Team of India (CERT-In) has alerted users about such emails. This scam is an ongoing 'fake' email campaign that claims to have recorded a user's video that could be published if a ransom amount in CryptoCurrency is not paid. According to Fortinet, the first quarter of 2020 registered a 17 percent increase in virus attacks for January. February then saw a 52 percent increase which further increased to an alarming figure of 131 percent in March as compared to the corresponding period in 2019.

Another small-scale survey by the Cybersecurity firm Check Point endorses that organizations see a rise in security threats and attacks. According to the survey, 71 percent of the Information Technology (IT) and security professionals who were surveyed reported an increase in security threats or attacks. In addition to this, 61 percent of respondents said that they were apprehensive of the security risks that emerged from changes made to enable remote work. Phishing attempts (55 percent) and websites claiming helpful information on coronavirus (32 percent) have emerged as dominant threats to the organizations, the respondents said. For example, a bad actor steals sensitive information in phishing attacks by luring people to open an email, instant message, or text message containing malicious links or attachments. Also, a spike in the number of Zoom domains; around 1700 of them are newly registered since the advent of the pandemic and spotted malicious files targeting people in WFH [7].

The COVID-19 Pandemic, with the dramatic changes in working practices and the technologies used by organizations, has created a perfect ecosystem for Cybercriminals to capitalize on the latest trends to boost the success rates of attacks.

4. Vulnerabilities and Attacks associated with WFH

Various factors associated with online work increase cybersecurity risks. As the WFH involves multiple tasks such as meetings related to technical and administrative reviews, skill development, transactions relating to administration, maintenance, monitoring, finance, support, etc., it must be pursued remotely via online. These tasks must be performed without the security protections an office system/s affords us – such as firewalls and blacklisted IP addresses. Also, increased reliance on technology renders far more vulnerable to various cyber-attacks [4]. While WFH may offer a certain level of ease and familiarity, most people's personal computers, smartphones, and other devices, used in WFH are not secure beyond a simple anti-virus program or firewall [10]. Most organizations are not prepared for such a condition. International Association of IT Asset Managers (IAITAM) also warned government agencies, businesses, and other organizations of the risks involved in letting employees work from home without secure devices. The vulnerabilities experienced with WFH are as follows:

4.1 Poor Network Connectivity with use of misconfigured or inadequately configured Open/closed network connection without any security scrutinizing favors various network attacks, such as

i. Denial of service attack
ii. Man-in-the-middle attack (MiTM) [2].
iii. Encryption Attacks.
iv. Nmap scans, intense scans.

v. Doxware attacks.

4.2 Accessing websites without secure socket layer (SSL) protection, i.e., using websites starting with HTTP:// rather than HTTPS://, untrusted websites with Web-based Application flaws and Browser-based Vulnerabilities favors attacks like:

i. Social Engineering Attacks
ii. Phishing
iii. Spear phishing
iv. Vishing
v. SMShing
vi. Website defacement attacks.

4.3 Use of Personal Computer Systems by other family members for various activities like installing/downloading unwanted media, software files with the knowledge of the owner of the device or without by the intervention of the peers, i.e., kids, family, neighbors, etc. pave a freeway to several attacks [11], which include:

i. Worms
ii. Viruses
iii. Trojan horses
iv. Spyware attacks
v. Ransomware attacks
vi. Crypto Ransomware attacks
vii. Crypto Jacking attacks

4.4 Violation of data leakage/loss program (DLP) implemented by the organization (or) jailbreaking/ overriding the DLP for the malicious usage/ personal usage/injudicious usage of organizations' resources, property, software, data which will cause many computer-related offences such as:

i. Computer-related fraud or forgery
ii. Email spoofing
iii. Domain name spoofing
iv. Malicious usage of employee credentials
v. Unwanted privilege escalations.
vi. Cyber-enabled intellectual property theft.
vii. Motivated local attacks.
viii. Forced local attacks causing cyberstalking, cyber harassment, cyberbullying, etc. [12]

4.5 The other Vulnerabilities that add to the menace are:

i. No regular System Updates.
ii. Outdated and improperly configured Anti-Virus and Firewall.
iii. Accessing various online resources from the same system.
iv. Inability to remediate security incidents on remote workstations.
v. Heightened reliance on endpoint protection software.
vi. Inability to harden and ensure proper IT hygiene on home computers [15].

The above indicates that WFH indirectly facilitates the perpetuation of SITUATIONAL CRIME, with all the factors (Vulnerabilities) and the associated Attacks (Crimes). The below illustration depicts the impending threats in the post-COVID-19 pandemic:

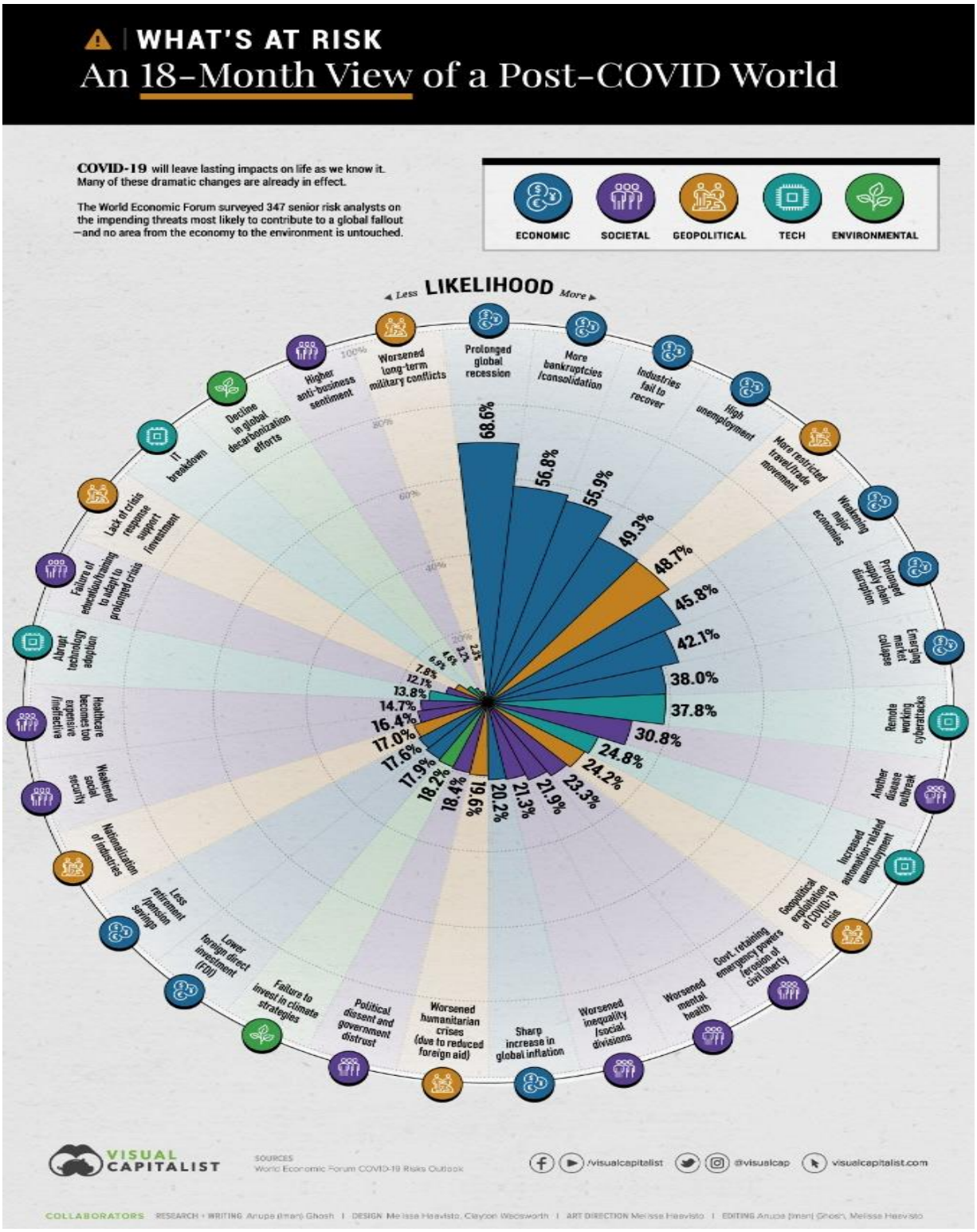

Fig – 12: Impending Threats in the post-COVID-19 pandemic [20]

5. Prevention of Situational Crime

It was introduced by Cornish & Clarke in the year 2003, presenting few techniques, categorized into five steps, which tend to prevent situational crime. Situational crime prevention seeks to reduce the harms caused by crime through altering primary or situational factors in the environment where crime regularly occurs [14].

Those are natured into two intentions i.e.

a. *Hard intentions*: Make it impossible for an offender to commit a crime.
b. *Soft intentions*: Decrease an offender's motivation for committing a crime.

Prevention of the Crime is the primitive footstep in showcasing criminal justice in action. Situational Crime Prevention (SCP) employs preventive approaches by focusing on methods to reduce the opportunities for crime. The five strategies of SCP that are employed in dealing with the above two intentions are:

a. Increasing the effort the offender must make to carry out the crime.
b. Increasing the risks the offender must face in completing the crime.
c. Reducing the rewards or benefits the offender expects to obtain from the crime.
d. Removing excuses that offenders may use to "rationalize" or justify their actions.
e. Reducing or avoiding provocations that may tempt or incite offenders into criminal acts.

The SCP can be applied as a cybercrime prevention measure in cybersecurity practice and is applicable in the WFH scenario. When used, SCP measures focus on reducing and/or denying cybercriminals opportunities for offending and impeding their ability to offend [16].

Below is a brief of the measures that can be initiated by various organizations in respect of the first three strategies, by way of hardening the targets and preventing the offenders, in stopping the cyber-attacks/frauds committed by individuals (external or internal employee)/hacker groups or state actors against customers and the organizations [19].

5.1 Increasing the effort the offender must make to carry out the crime:

i. The workforce should be forced to use strong passwords with possible maximum length containing numeric, lower- and upper-case alphabets, special characters, etc. As a result, it becomes challenging for the offenders to guess or crack them easily by automated attacks.
ii. Increased security awareness for the workforce by special security awareness and training modules so that they do not disclose any personal details and other confidential details, thereby preventing data or account compromise attempts.
iii. Implementing advanced security procedures like Two Factor Authentication and/or OTP channels.
iv. E.M.V. Chip-based Credit/Debit cards with no permanent PIN.
v. Implementing Hardware Tokens for high net worth financial transactions.
vi. Strengthened the IT infrastructure in terms of People, Policies and Technology to reduce the threats that originate from external and internal sources and increase the offender's effort to commit a crime by following the information security best policies such as ISO 27001 & 27002.
vii. Implementing Demilitarized zones (DMZ) concept, network segmentation, Identity and Access management; conducting Vulnerability & Penetration testing on applications and Web servers, etc.,
viii. Implementing security perimeter devices such as Load Balancer, Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Firewall, etc., for detection, warning, and containment.
ix. Stopping phishing emails targeted against the workforce by implementing SPAM filters.
x. Hardening the computer systems, by implementing Antivirus and Patch management, via online scanning of the systems used in WFH.

xi. Implementing Data Leakage Prevention Solutions (DLP) and encrypting the data end-to-end.
xii. Implementing privilege and access management solutions, i.e., role-based approach – thereby minimizing the individuals' interactions with the data.
xiii. Improved monitoring capability of the network from illegal intrusions by implementing "Next Generation" Security Operation Centre (SoC) based on AI and Machine Learning.

5.2 Increasing the risks, the offender must face in completing the crime :
i. Implementing virtual surveillance and monitoring systems in and off the premises of operations.
ii. Develop and implement the Standard Operating Procedures (SOPs) to log activities, maintenance, preservation, collection, and analysis.
iii. Information exchange about cybercrime offenders, methodologies.
iv. Performing data mining and analytics on the data transactions and identifying anomalies.
v. Deploying honeypots on the networks managed by the organization.

5.3 Reducing the rewards or benefits the offender expects to obtain from the crime [17] :
i. Implement a Transaction monitoring & Fraud Risk Management (FRM) solution with velocity checks, geolocation checks, etc., and block the accounts where required.
ii. Implementing cross-verification procedures for high volume transactions such as mail/voice verifications and block unauthorized transactions, especially SWIFT transactions.

5.4 Apart from the above measures, the measures suggested by NIST Special Publication 800-46 Revision 2 (Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security) may help in safeguarding the WFH situation [17]. They include deploying some or all the following security measures:

i. Developing and enforcing a telework security policy, such as having tiered levels of remote access.
ii. Requiring multi-factor authentication for enterprise access.
iii. Using validated encryption technologies to protect communications and data stored on the client devices.
iv. Ensuring that remote access servers are secured effectively and kept fully patched.
v. Securing all types of telework client devices, including desktop and laptop computers, smartphones, and tablets, against common threats.

6. Top FIVE attacks during the PANDEMIC in the backdrop of WFH

We try to discuss the top FIVE attack patterns during the COVID-19 pandemic in the background of WFH [13].

6.1 Intrusion attacks on Windows:

Intrusion attacks attempt to exploit vulnerabilities in applications, services and operating systems remotely through a network to achieve arbitrary code execution and perform unauthorized network activity. Below are some examples of intrusion attacks and probable remedies to counter them.

a. Intrusion.Win.MS17-010 (. o, p):
   i. Exploits server message block (SMB) network vulnerabilities.
   ii. SMB operates over TCP ports 139 and 445, used for file and printer sharing and remote services access.
   iii. These exploits were used in WANNACRY and EXPetr ransomware attacks.

   SOLUTION: Implementing security patch released by Microsoft security bulletin MS17-010.

b. Intrusion.Win.NETAPI.bufferoverflow.exploit:
   i. Successful exploitation can result in remote code execution on target machines, which allows the attacker to load Malware and propagate it to other vulnerable hosts on a network.

ii. Attempts to exploit a flaw in path canonicalization parser of the server service net API library through a specially crafted Remote Procedure Call (RPC) request.
iii. Operates over the TCP on ports 139, 445.
iv. Networm.Win32.kido malware used a Net API buffer overflow exploit to spread on a network.

SOLUTION: Implementing security patch released by Microsoft bulletin MS08-67.

c. Intrusion.Win.CVE-2017-0147.sa.leak:
i. Attack aimed at SMBv1 server in Windows.
ii. The vulnerability allows an attacker to use specially created packages to get important information from memory processes.
iii. These can trigger a WANNACRYPT type attack.

6.2 Bruteforce attacks:

A brute-force attack is an attack for guessing a password or an encryption key that involves trying all possible password combinations character by character until one is matched. An example of such type of attack and the possible remedy is as follows:

a. Bruteforce.Generic.Rdp (.d,.a,.c):

i. Successful Bruteforce attack allows obtaining valid user credentials.
ii. Rdp to find valid RDP login credentials by checking possible passwords until the correct one is found.
iii. Successful Bruteforce.Generic.Rdp allows gaining remote access to the targeted host computer.

SOLUTION:
1. Frequent changing of passwords.
2. Putting strong passwords to guess.
3. Do not install unwanted and untrusted software, applications.
4. Improving the security of Remote Desktop Service
5. Implementing Transport Layer Security (TLS) with high levels of encryption and enforce Network Level Authentication (NLA).

6.3 Scanning/Enumeration attacks:

Enumeration is the first stage of hacking, in which complete information regarding the target system is acquired. For example, the Operating System, version, active ports, IP, etc., of the target system. Below is an example of such type of attack and the possible remedy:

a. Scan.Generic.Portscan (.UDP, .TCP):
i. Port scanning determines which ports on a computer are active by sending them requests.
ii. Port status is determined by sending a TCP, UDP packets.

SOLUTION:
1. Using personal trusted VPN.
2. Disabling unwanted ports.
3. Terminating unwanted, suspicious software applications running in the background can be controlled in the windows task manager.

6.4 Denial of Service Attack (DoS):

DoS attack consumes all available resources of a server and makes it unavailable for legitimate traffic. Below is an example of a DoS attack and the suggested remedy:

a. Dos.Generic.flood.TCPSYN:
   i. By repeatedly sending an initial connection request (SYN), the attacker can overload all available ports of the target server, thus slowing down or preventing a server response to legitimate traffic.

SOLUTION:

1. Use of anti-virus and firewall software.
2. Install software from trusted sources.
3. Remove software after your purpose is served.

6.5 Trojan attacks:

Malicious programs of this family are used to destroy, block, modify or copy data or disrupt computers or networks' performance. Some of such attacks and the possible solutions are as below:

a. Trojan.Win32.Agentb.gen:
   i. The presence of the following files indicates the infection due to infected mails:
      1. iexplore.scr
      2. Isas.exe
      3. svhost.exe
   ii. As this is generic detection, in most instances, alert notifications from installed anti-virus software may be the only other symptoms.
   iii. They drop additional Malware; they could be any of the attacker's choosing and could include:
      1. Trojan: Win32/Hocomrac.A
         A. Copies itself to %windir%\svhost.exe.
         B. The Malware modifies the following registry entries to ensure that its copy executes at each Windows start:
            I. Adds value: "$$config"
            II. With data: "c:\windows\svhost.exe"
            III. Tosubkey: HKCU\Software\Microsoft\windows\currentversion\run

         C. The Malware creates the following files on an affected computer:
            I. %windir%\svhost.dll - detected as Trojan: Win32/Coremhead
            II. Backdoor: Win32/Beastdoor.DL A trojan that allows unauthorized remote access and control to the affected computer. It also modifies certain settings on the computer.

      2. PWS: Win32/QQ Rob:
         Family of programs that steals user input for QQ messenger. It also terminates or disables security-related processes and downloads and executes files from specific websites.

      3. Backdoor: Win32/Hupigon:
         Main backdoor component of Win32/Hupigon, a family of backdoor Trojans. TrojanDropper: Win32/Hupigon registers this component as a service. The service then opens a backdoor server that allows other computers to connect to and control the infected computer in various ways.

      4. Worm: Win32/Autorun:
         A worm that disables certain Windows utilities and spreads via removable and network drives [18].

5. Trojan: MSIL/ Agent:
   Malicious programs of this family are used to destroy, block, modify, or copy data or disrupt computers or networks' performance.

6. Trojan.Script.Generic
   A. This family includes programs that have characteristics typical of malicious trojan scripts.
   B. Previously used in HEUR: Trojan.Script.Generic

7. Trojan.Win32.AutoItscript.gen [18]:
   A. This family includes trojans that are binary files compiled from AutoIt scripts.
   B. It launches the system command interpreter "cmd.exe" with the following parameters /C AT /delete /yes. This cancels all scheduled tasks in the windows task scheduler.
      I. /C AT 9:00 /interactive /EVERY: m,t,w,th,f,s,su % system% svchost.exe, every day at 9:00 windows task scheduler will launch a copy of trojan.
   C. It creates the directory-
      I. %system%<rnd>, where <rnd> is a random 5-digit decimal number.
   D. It attempts to connect to the following HTTP servers.
      I. 87.***.14
      II. 69.***.224

8. Trojan-spy.MSIL.Noon.gen:
   This family includes malicious software programs that steal passwords from web browsers and record keystrokes on the user's computer.

9. Trojan-Downloader.Script.Generic: Programs of this family are malicious scripts that download and run other malicious software to the user's system

10. Dangerous.Object.Multi.Generic:
    A. It is a script that shows similarities to a Trojan.
    B. Possessing this script shows the following symptoms:
       I. Run in the background and connect C2 server controlled by hackers.
       II. Harvests banking information, saved passwords, browsing history.
       III. Logs keystrokes use a video camera, take screenshots regularly.
       IV. Create backdoor access and lead to ransomware or other virus infections, etc.
    C. Antivirus shows:
       I. Artemis!63116D7AD2F2
       II. Trojan.Gen.2
       III. Gen:Variant.Symmi.2215
       IV. VBS/Dldr.Rowm.A
       V. Script.Trojan.Suspic.Pdcl
       VI. Trojan.Script.Siggen.degalj
       VII. Script.Trojan.Agent.FZPT9I
       VIII. JS:Downloader-BSP [Trj]
       IX. VBS/Agent.NCO
       X. VBS.Downloader.Trojan

XI. Trojan.MSIL.Agent.QOJ
XII. MSIL/Agent.QOJ!tr
XIII. Trojan/Win32.Agent, etc.

11. Trojan.Multi.preqw.gen:
This family consists of POST requests made to malicious websites

12. Trojan.Script.Miner.gen
A. This Trojan is responsible for blocking web pages, sites, and shows denied pop-ups.
B. Possible date expiration check exits too soon after checking local time
C. Reads data out of its binary image
D. A process created a hidden window
E. Drops a binary and executes it
F. The binary likely contains encrypted or compressed data.
G. The executable is compressed using Ultimate Packer for Executables (UPX.)
H. Uses Windows utilities for basic functionality
I. Deletes its original binary from disk
J. Creates a hidden or system file
K. Network activity detected but not expressed in API logs
L. A possible crypto mining command was executed
M. Anomalous binary characteristics.

13. Trojan.Script.Redirector.gen:
This detection identifies a large group of programs or scripts that redirect web page visitors to another unsolicited website.
14. Trojan-Spy.JS.Agent.n:
It is a massive family of trojans written in JavaScript and is spyware.

15. Trojan-Downloader. VBS.Sload.gen:
This family consists of malicious VBScript scripts that are used for downloading additional malware modules using Powershell. These scripts contain encrypted PowerShell scripts that are subsequently decrypted and passed to PowerShell as arguments.

16. Trojan.Script.Iframer:
A. Slows down your PC speed notably.
B. Add other dangerous Trojan or Spyware to your system secretly.
C. Allow the hacker to access your entire system.
D. Collect all your personal information and transfer it to a remote hacker.
E. Destroys critical system files and makes PC unstable.

SOLUTIONS:
1. Keep software up to date.
2. Be wary of links and attachments
3. Pirated material on compromised websites.
4. Do not attach unfamiliar removable devices.
5. Use a non-administrator account.

6. Run full anti-virus scans regularly.
7. Check extensions when you install/run programs from unwanted files.
8. Always prefer a virtual keyboard over a physical keyboard.
9. Run system in safe mode, run Command Prompt (CMD) and try <cd restore> method.
10. Install software from only trusted sites.

7. CONCLUSIONS

WFH is the new normal and will be the future of work culture. Therefore, organizations cannot avoid WFH. Personnel belonging to an organization may be seen as a weak link by external threat actors, who may employ social engineering, phishing, and other methods to target and manipulate personnel into divulging sensitive information or even unintentionally installing backdoors to their networks. However, IT security and constant vigilance by well-trained IT security personnel help mitigate problems emanating from human resources.

Policies and best practices should be tailored and adopted by organizations such that IT security is seen as an integral aspect of an organization's infrastructure. Failure in systems security, resulting in a data breach or any other such situation, may cause catastrophic consequences to an organization's existence. Information Security is not an add-on subsystem that can be appended to an organization's internal resources but is integral to the functioning of an organization. Hence, budgets should be allocated to ensure that best-of-the-breed software and hardware technologies are integrated. These require commitment from top management onwards.

REFERENCES

[1] MORPHISEC'S 2020 WFH Employee Cybersecurity THREAT INDEX
[2] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-1794
[3] https://unit42.paloaltonetworks.com/how-cybercriminals-prey-on-the-covid-19-pandemic/
[4] https://smefutures.com/covid-19-ignites-a-firestorm-of-cyber-attacks/
[5] https://www.pwc.in/assets/pdfs/services/crisis-management/covid-19/covid-19-00crisis-the-impact-of-cyber-security-on-indian-organisations.pdf
[6] Harjinder Singh Lallie, Lynsay A. Shepherd, Jason R.C. Nurse, Arnau Erola, Gregory Epiphaniou, Carsten Maple, Xavier Bellekens, Cybersecurity in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic, Computers & Security, Volume 105, 2021, 102248, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2021.102248.(https://www.sciencedirect.com/science/article/pii/S0167404821000729)
[7] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains
[8] https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats#:~:text=Malware%2C%20spyware%20and%20Trojans%20have,their%20computers%20or%20mobile%20devices.
[9] https://amtrustfinancial.com/blog/small-busines/coronavirus-best-practices-work-from-home-policy
[10] https://analyticsindiamag.com/increasing-cybersecurity-threat-during-work-from-home-for-organisations/
[11] https://www.entrepreneur.com/article/348346
[12] https://cyberexperts.com/work-from-home-cyber-risks%EF%BB%BF/
[13] https://www.itgovernance.co.uk/top-5-remote-working-cyber-security-tips-infographic
[14] https://www.cisco.com/c/en_uk/products/security/ciso-benchmark-report-2020.html
[15] https://www.itgovernance.co.uk/blog/the-cyber-security-risks-of-working-from-home#:~:text=Online%20work%20increases%20cyber%20security,our%20tasks%20are%20conducted%20online.
[16] https://study.com/academy/lesson/situational-crime-prevention-definition-strategies.html

[17] https://oxfordre.com/criminology/view/10.1093/acrefore/9780190264079.001.0001/acrefore-9780190264079-e-3
[18] https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Worm:Win32/Autorun.WT
[19] https://www.securitymagazine.com/articles/91990-nist-cybersecurity-recommendations-for-working-from-home.
[20] https://www.visualcapitalist.com/whats-at-risk-an-18-month-view-of-a-post-covid-world/
[21] https://public.tableau.com/profile/rowena.lai#!/vizhome/WorkFromHomeDashboard/Dashboard1
[22] https://www.techcircle.in/2020/07/28/malware-attacks-drop-65-in-india-hackers-focus-on-iot-covid-19-emails-sonicwall

AUTHORS' PROFILES:

1. **Mr. Eswara Sai Prasad Chunduru** pursued M.Sc. (Physical Chemistry), M.Sc (IT) and Criminal Justice and Data Analytics from IIT, Kanpur. He is currently working as Assistant Director and Scientist C in Digital Forensic Division of CFS, GoI, Hyderabad. During his tenure of 22 years, he has analyzed more than 1500 cybercrime cases. He is a Guest Faculty at various organizations. He is co-author of the book - "Handbook on Cybercrime Investigation."

2. **Mr. Nagendar Rao Koppolu** joined Police Service as Sub-Inspector in the year 1998. He served in Law Enforcement, Bureau of Immigration (IB), Central Bureau of Investigation (CBI) (Anti-Corruption Wing), State Intelligence Department, and State Information Technology Cell. He pursued M.Tech (CSE), M.Sc. (IT), and Criminal Justice Data Analysis (IIT Kanpur). He is a certified Cyber Security Professional and ISO 27001 ISMS Lead Auditor. He co-authored two books on cybercrime. Presently, he is Inspector (in-charge) of State Cyber Vertical, Telangana.