

INDIA

THREAT LANDSCAPE REPORT

2020



CYFIRMA
DECODING THREATS



CONTENT

01 INTRODUCTION.....	3	07 TRENDS IN MALWARE.....	20
02 CYFIRMA'S METHODOLOGY.....	5	09 PHISHING ATTACKS DURING COVID PANDEMIC.....	25
03 EXECUTIVE SUMMARY.....	7	09 THREAT ACTORS TARGETING INDIA.....	29
04 DRIVING FACTORS IMPACTING INDIA THREAT LANDSCAPE.....	9	10 REPORTED CRITICAL INCIDENTS.....	32
05 REPORTED CAMPAIGNS.....	12	11 UPCOMING TRENDS.....	34
06 TOP ATTACK METHODS.....	15	12 RECOMMENDATIONS.....	39

01 INTRODUCTION

Welcome to CYFIRMA's India Threat Landscape Report 2020

In a year where the COVID-19 pandemic has been in all conversations, threat actors have been doing brisk business, with an abundance of malware attacks, and threat campaigns, leveraging on the COVID-19 theme, as well as other geopolitical triggers, in this highly volatile region (speaking in terms of the cyber landscape).

Here is a brief look into the cybersecurity challenges that will likely be witnessed across India in 2020 and beyond. We will delve further in the coming sections of this report.



Reported Campaigns

Facts and intelligence on the reported cyber-attack campaigns.



Top Attack Methods

Detailed information on the top attack methods observed.



Trends in Malware

Malware used by various hacker groups targeting South East Asia & India



Phishing Attacks During COVID-19 Era

Discuss the evolving situation of phishing attacks during Covid pandemic.



Threat Actors Targeting India

Threat actors targeting organizations in India & South East Asia.



Critical Incidents Reported

Top critical incidents reported during H1, 2020.



Upcoming Trends

Predict trends of upcoming cyber-attacks.



Recommendations

Prevent future attacks with security measures to safeguard the organization.

With its proprietary cloud-based threat discovery and cyber-intelligence platform, DeCYFIR, CYFIRMA is able to dive into the hackers' trenches to discover, analyse, correlate, and find the deepest insights from noisy data. These insights will help India-based businesses navigate their threat landscape better, anticipate incoming attacks, and avoid financial and reputation damages.

02 CYFIRMA'S METHODOLOGY

The information presented in this report is sourced from both the surface-web as well as CYFIRMA's proprietary cloud-based threat discovery and cyber-intelligence platform, DeCYFIR

The report is compiled based on the following principles:

Consumption Across the Organizational Hierarchy

The contents are designed to be consumed by all functions across the organization, from strategic intelligence for top management to tactical intelligence for operations. At its core, the onus is on decoding signals and intelligence, from the external threat landscape, and correlating and presenting them into consumable and multi-dimensional insights.

Threat Detection and Analytics Models

CYFIRMA's dedicated pool of security analysts and data scientists are adept at analysing large quantum of data, with assistance from DeCYFIR's machine learning and AI-driven routines, to identify threat actors, recognize trends in their activities, and their malicious objectives. For the purpose of this report, the top trending factors across each examined vertical have been represented. CYFIRMA encourages the reader to

source our other literature available on the public domain to gather in-depth insights where required.

The DeCYFIR Platform

CYFIRMA's proprietary cloud-based threat discovery and cyber-intelligence platform, DeCYFIR, especially its Threat Visibility and Intelligence module is the sonar-and-radar threat discovery system. The module unravels threats in the deepest trenches and highest vantage points by monitoring the external threat landscape (deep, dark webs, surface web, hackers' forums, closed communities, and other sources). It equips clients with early detection of potential threats.

Document Flow and Objectives

The purpose of this report is to offer a snapshot of the cybersecurity concerns likely to impact organizations in India through H2, 2020 and

beyond. This report presents and describes cybersecurity risks, methodologies, and tools, prevalent through H1, 2020 and likely to impact the operation, infrastructure, and reputation of such organizations.

Intended Audience

This report is intended for cybersecurity and threat intelligence personnel, security management teams, CISO, security operatives, and those managing their organization's cybersecurity posture. It is assumed that the reader has an above average understanding of cybersecurity related Tactics, Techniques and Procedures (TTP).

03

EXECUTIVE SUMMARY

India is a haven for start-ups, and a fertile ground for technological innovation, generating massive quantity of data that attracts cybercriminals



CYFIRMA
DECODING THREATS

© CYFIRMA 2020, ALL RIGHTS ARE RESERVED.



The digitally savvy, and youthful population lives the mobile-first, hyper-connected lifestyle that creates a big attack surface for cybercriminals

While digital adoption is breaking new grounds, the corresponding cyber maturity is low and not keeping pace with the technological strides. All these factors are prompting more nations – especially India's geopolitical foes – to partake in the cyber game targeting India. The Big 3 – namely China, North Korea, and Russia, authoritarian regimes that are suspected of aiding state sponsored cybercriminal activities – have shown interest in breaching India's security perimeters. This report highlights the various cybersecurity insights drawn from this region through H1 2020, with a roadmap stretching through the rest of the year, H2 2020. The report addresses the following in detail:

- **COVID-19 pandemic was abundantly leveraged as part of threat campaigns.** CYFIRMA uncovered the North Korean Lazarus group planning a large-scale phishing campaign targeting more than 5M individuals

and businesses across six countries and multiple continents, amongst other such campaigns.

- **Threat actors deployed attacks that maximized the exploitation of the organization's security errors and oversight.** Attack methods included abuse of Apache and IIS web servers, identifying loopholes to target Cloudflare-preferred safeguard for servers/websites, port scanning followed by brute forcing, etc.
- **Commodity malware is increasingly employed by state sponsored hacking groups.** The latter, including Stone Panda and Lazarus, are utilizing malware that are available for purchase, or as part of a licensing and delivery model, including Emotet, Ursnif, TrickBot, etc., increasingly as drivers of their campaigns.

- **Ransomware operators are adopting a 'name and shame' modus operandi.** All the major operators, including those managing NetWalker, Sodinokibi, Maze, DoppelPaymer, etc., are now exfiltrating data alongside the encryption of the victim's systems. This data is then used as leverage to force the victim to pay the ransom.
- **Phishing attacks have intensified and are targeting the 'unsupervised' workforce.** With the COVID-19 pandemic forcing employees to work from home, threat actors are keen to target them while they are away from their organization's security perimeters. In H1 2020, CYFIRMA has observed an entire range of phishing attacks employing a wide range of TTPs.

04 DRIVING FACTORS IMPACTING INDIA THREAT LANDSCAPE

India shares her borders with Pakistan and Afghanistan in the northwest, China (Tibet), Nepal and Bhutan in the north, and Myanmar and Bangladesh in the east.

Southern neighbours across the Indian ocean include Sri Lanka and Maldives. India is surrounded by neighbours whose relationships with her can be described as distrusting and adversarial, juxtaposed with periods of relative calm.

Having monitored India cyber threat profile throughout the course of COVID-19 pandemic, our researchers have observed hackers' increased interest towards India government agencies and conglomerates starting in February 2020.

India is an attractive target due to the following reasons:

Low cybersecurity awareness among its population

India has a young population where more than 50% are below the age of 25. Telecommunications and internet penetration are concentrated in the large cities but these have improved dramatically in recent years when rural populations leapfrog technology with mobile access. However, the lack of understanding of cyber risks have seen significant uptick of online frauds, scams and hoaxes, and the spread of fake news.

Low cybersecurity maturity among businesses

Businesses have traditional approach towards IT projects where resources are focused on building the digital systems, and cybersecurity requirements are relegated to an afterthought.

This presents profound challenges as frequently actions are only taken after a data breach or cyberattack has occurred.

The situation is compounded by the fact that over 46% of commercial businesses are operating on traditional legacy systems. These are aged technologies which are no longer supported by their vendors, and they present cybersecurity gaps, loopholes and vulnerabilities where hackers can exploit to gain entry to corporate networks.

Over 99.4% of Indian companies are categorized as micro, small, and medium businesses (source: MSME Ministry's FY19 annual report). These organizations are not aware of cyber risk, and its potential to upend businesses.

Digital Start-ups, unicorns, and powerhouses

Indian Industries which possess huge personal and customer identifiable information, such as telecommunication companies, online retailers, F&B, and financial institutions are attractive targets for hackers.

In addition, Indian IT services, digital companies, and start-ups unicorns possess vast amounts of personal, customer, and financial identifiable information. Gaining access to this treasure trove of data can fetch a handsome fee in dark web marketplaces.

Geopolitical Situation

Geopolitical situation around India, specially coming from two fronts - China and Pakistan – has seen increased tension and acrimony. China's expansionist push with its belt and road initiative has been accused of being debt traps for emerging countries while hostility between India and Pakistan remains a perennial issue. China viewed India's support for the Dalai Lama and her offer of asylum to Tibetan refugees as a provocation and this has been a thorny issue.

Based on our research, we have noticed state-sponsored and financially motivated hackers are particularly keen on India government agencies and Indian companies. Our research showed the suspected threat actors were mainly sponsored by China, Pakistan and North Korea.

The hackers' objectives were centred around smearing India's reputation, cause productivity loss, create operational damage and seek financial gains.

Lack of Cyber Intel Sharing – Inter and Intra Industry

To fight cyber-crime effectively, cyber-intelligence sharing amongst players operating within a specific industry or across multiple industries need to take place. This can create a common repository of known threats, malware, tactics, techniques, and procedures, giving organizations additional ammunition to mount more effective defence strategies.

Lack of nation-wide cyber-strategy, policies, and procedures

Regulations around data privacy and protection should be enacted and enforced as these measures will help businesses evaluate their cybersecurity posture and seek ways to improve.

Currently, incident reporting is not mandatory. By making it compulsory, there will be a body of research data which can provide insights on threats to India and inform the government on strategies it can undertake to strengthen the nation's cyber posture.

Lack of Cybersecurity Talent

While this is a global problem, the issue is particularly acute for India. Ranked third in the list of countries with the highest number of cyber threats, India faces an urgent need for cybersecurity talents and resources who can help fend off cyberattacks. The tertiary institutions have not included cybersecurity training, awareness, and education as part of their curriculum, and this could exacerbate the ongoing talent crunch problem.

05 REPORTED CAMPAIGNS

This section highlights the trending cyber threat campaigns that targeted India and the greater South East Asia region in 2020

A threat campaign is broadly defined as organized activities suspected to be carried out by threat actors using specific tactics, techniques, and procedures (TTP) with a clear motive and specific outcome.

CYFIRMA's Threat Visibility and Intelligence capability offers a view of how threat actors are exploiting vulnerabilities, including details about campaigns, their association with the external threat landscape, correlation with the threat actors, TTP, motivations, etc.

Global Covid 19 Related Phishing Campaign by Lazarus Group

Hacker groups planned a large-scale phishing campaign targeted at more than 5M individuals and businesses (small, medium, and large enterprises) across six countries and multiple continents. The hacking campaign used phishing emails under the guise of local authorities in charge of dispensing government-funded Covid-19 support initiatives. These phishing emails are designed to drive recipients to fake websites where they will be deceived into divulging personal and financial information.

- **Targeted Countries:** India, Japan, Singapore, South Korea, US, UK
- **TTPs:** Phishing Attack, Credential Harvesting, Impersonation, Website Spoofing, Data Exfiltration
- Security researchers of CYFIRMA conducted detailed technical analysis and North Korean state sponsored Lazarus

Group emerged as the prime suspect. There is a common thread across six targeted nations in multiple continents – the governments of these countries have announced significant fiscal support to individuals and businesses in their effort to stabilize their pandemic-ravaged economies.

- CYFIRMA Researchers first picked up the lead on June 1, 2020, and analysed the planned campaign, decoding the threats, and gathering evidence. Evidence points to hackers planning to launch attacks in six countries across multiple continents over a two-day period. Further research uncovered seven different email templates impersonating government departments and business associations.
- Researchers were able to intercept seven email templates impersonating government departments and institutions like the Bank of England, Singapore's Ministry of Manpower, Japan's Ministry of Finance etc. Aided by millions of email addresses and business contact details, Lazarus was planning to send emails that speak of new government-backed business support payment, and subsequently lead the targeted individual to a spoofed webpage.

Herein, the impersonated website will be used to trick the user out of personal and financial information.

- CYFIRMA also observed that hackers are planning to spoof or create fake email IDs impersonating various authorities. These are some of the emails discussed in their phishing campaign plan:
 - covid19notice@usda.gov
 - ccff-applications@bankofengland.co.uk
 - covid-support@mom.gov.sg
 - covid-support@mof.go.jp
 - ncov2019@gov.in
 - fppr@korea.kr

CYFIRMA also identified a few other noteworthy campaigns :

RedWall Campaign by Stone Panda

RedWall is a long-running Global Reconnaissance Campaign primarily carried out by Stone Panda (also known as APT10) with the aim to list vulnerable assets spanning potential

target organizations and affiliates. It is suspected that the vulnerable assets list sourced by RedWall is not only used by the campaign's instigator Stone Panda, but also by other Chinese state-sponsored hacking groups as well. The RedWall global reconnaissance campaign was also featured prominently as part of the plans of suspected Chinese threat actors that were looking to disrupt and delay the now postponed Tokyo 2020 Olympics, by exploiting the gaps in the games' security infrastructure. As per the latest information gathering, we have observed certain activities where attackers launched passive scans towards organization's assets, which we believe to be in the reconnaissance & enumeration phase of a long planned hacking activity. Recently, amid the COVID-19 outbreak and the global insistence on staying and working from home, Chinese cybercriminals dedicated a lot of focus towards VPN tools and the vulnerabilities lying within- the exploitation of which could allow them to attack remote desktops. In this regard, the RedWall campaign was leveraged to identify vulnerable devices, eventually listing as many as 7,300 VPN devices that were rendered publicly accessible.

- **Motive:** Primary motive is Data Exfiltration where hackers were interested to steal intellectual properties, copyrights, and trade secrets as part of corporate espionage activities leading to Operational Disruption & Reputational Damage.
- **Targeted Countries & Industries:** This campaign targets primarily India, South Korea, Japan, etc. RedWall primarily targets multinational companies across multiple industries, especially retail, supply chain transactions, ordering and invoicing systems, manufacturing, and Product / IT-based companies.
- **TTPs:**
 - Attack vectors are mostly phishing attacks followed by installing malware to exfiltrate sensitive data.
 - Hackers are interested to leverage Web and SSL based vulnerabilities.
 - Stone Panda has been observed using 'Living off the Land' tactics and techniques, which are often referenced in their group members' chats in dark web forums.



06 TOP ATTACK METHODS

CYFIRMA has witnessed a steady increase in attacks, particularly spanning the region, that leverage on the attack methods described here

Cybercriminals will seek out these attack methods when targeting India through H2 2020, and beyond.





Attack on Servers

Due to improper implementation of vulnerability management cycle, many organizations fail to patch their critical web servers or database servers in a timely manner. Threat actors always try to utilize this situation and keep looking for weak links on the servers.

- This year the focus has been on the Apache and IIS web servers. Threat actors tend to find out the version details on the open ports targeting HTTP & HTTPS [port 80, 443, 8080 or 8443]. The version details help to identify the associated CVE numbers along with the exploit details.
- Organizations have started using powerful applications like Cloudflare to safeguard their servers/websites from injection attacks or brute-force attacks. But in recent scenarios threat actors have been quite successful to find loopholes for targeting applications behind Cloudflare. The target methods include new set of injection payloads or some powerful tools written in python/Golang languages.



Attack on Linux Servers

Linux-based systems were considered to be one of the most secured assets in the past. However, we have observed the sudden increase in the malware attacks or hacking attempts because of severe vulnerabilities on the Linux servers in recent times.

We have categorized the trends as per our investigation on critical Incidents:

1. Cryptocurrency Mining
2. Dropping Ransomware and other Trojans to create Bots for DDOS Attacks
3. Ransomware Attacks
4. Using Ransomware and other Trojans for Data Exfiltration
5. Information Stealing, Data Theft

Threat Actors' Attribution:

1. We have observed the involvement of **Chinese** and **Russian** threat actors with most of the critical incidents and a few of them were responsible to leverage Linux vulnerabilities.
2. Infamous **North Korean Hacker group Lazarus** was linked to Dacls RAT for targeting Linux servers.
3. However, **Rocke Group, Pacha Group, Black Tech** were directly involved to deploy a few malware into the Linux devices.
4. We have seen involvement of **Stone Panda, Fin7, Mission2025, Fancy Bear** too leveraging Linux vulnerabilities to deploy malware after rigorous scanning and reconnaissance activities.

The Malicious Activities observed:

1. Remote/Arbitrary Code execution. [Ex: HiddenWasp Malware]
2. Exploit vulnerable system configuration and applications. [Ex: Golang Malware]
3. Act as a backdoor and spyware to steal data. [Ex: SpeakUp Backdoor]
4. Persistence, File upload and download capabilities. [Ex: TSCookie Malware]



Attack on SMTP Application & Email Servers

SMTP is mainly hosted on port number 25 and associated with port number 2525, 465 and 587. There have been a number of incidents where port scans were performed on these ports to identify the application and version details. Vulnerability on Mail Transfer Agents have been exploited too in the month of May and June this year.

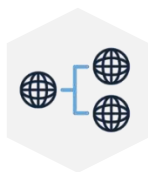
- CVE-2019-10149 has been heavily exploited by Sandworm threat actor group and others. Threat actors tried to send malicious emails to the SMTP server which could help them to execute arbitrary codes remotely further leading to command injection. They tried to add privileged users, disabled security settings and modified configurations to enable remote access, etc.
- We have observed SMTP relay attacks during this period as well. SMTP relays are useful to send mail via external servers, but these open relays had been mishandled by spammers and hackers for sending phishing & spam emails.
- Another critical vulnerability, tracked as CVE-2020-7247, impacted OpenSMTPD, was seen heavily being exploited since January 2020. Attackers tried to exploit this vulnerability by crafting and sending malformed SMTP messages to the vulnerable server. The motive was to execute arbitrary codes with root privileges.



Reconnaissance on Well-known Ports

- The port scanning activity along with directory brute forcing severely spiked in the month of April.
- The most targeted ports are:

SSH	22
telnet	23
SMTP	25, 465, 587
RDP	3389
HTTP/HTTPs	80, 443, 8080, 8443
NetBIOS/SMB	139, 445
SQL Server	1433, 1434



Subdomain Takeover Attacks

Subdomain takeover vulnerabilities occur when a subdomain points to a service or projects that has been ended or deleted but DNS entries still exist. The attacker can take over or seize the control of the organization's subdomain via various cloud services.

- There have been several incidents reported from the companies like Honeywell, Xerox, PwC, Hawaiian Airlines, Autodesk, UNESCO, Siemens, Volvo etc. where subdomains got hijacked for implanting malware or to host obscene materials etc. Most of those subdomains were hosted on Microsoft's Azure cloud.
- Tech Giant Microsoft was also notified of having close to 650+ vulnerable subdomains which could be hijacked by threat actors for malicious intentions.



Attack on Web Applications

In 2019, we experienced a wave where hackers were keen to target web applications for malicious intent. The primary motives were to look for sensitive information, credentials, API keys, critical server information or bypassing authentication etc.

In 2020, the trend continues & the top attacks on web applications identified are as follows:

1. Remote Code Execution
2. OS Command Injection
3. Account Takeover
4. Cross-site scripting
5. SQL Injection
6. File Inclusion Attacks
7. 2FA/MFA bypass
8. Server-side Request Forgery
9. DoS Attack
10. Exploitation of Third-party vulnerabilities

07 TRENDS IN MALWARE

A malware attack occurs when malicious software executes unauthorized actions on the victim's system

The malicious software encompasses many types of attacks such as ransomware, spyware, command and control (C2) software, and more.

Criminal organizations, state actors, and even well-known businesses have been accused of deploying malware while targeting India in H1 2020.

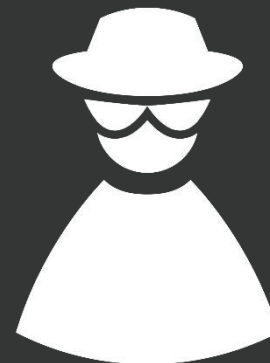
Listed here are malware trends with a likely impact on India through H2 2020 and beyond.

MIRAI BOTNET



-  Echobot
-  Mozi.m & Mozi
-  Compromised Network IoT Devices
-  LeetHozer

RANSOMWARE



-  NetWalker
-  Sodinokibi
-  Maze
-  DoppelPaymer
-  Nemty
-  Ryuk & WastedLocker

MIRAI BOTNET

There has been a spike in Mirai Botnet usage starting this year, an increase of over 2000 per cent since last year, and from February 2020 we saw many new variants of Mirai coming in. CYFIRMA has detected couple of Mirai variants described below:

- **Echobot** was one of the Mirai variants identified, which incorporated various exploits including those targeting enterprises and ICS products. The ICS-specific exploits started targeting CVE-2019-14931 and CVE-2018-7841 mostly.
- Several Mirai variants were identified which attempted to download files named "**Mozi.m**" and "**Mozi.a**" by exploiting vulnerabilities in IoT devices. It also targeted vulnerabilities in DSL modems and GPON routers, D-Link and NETGEAR, Huawei routers, and Realtek SDK etc.
- We found strong evidence suggesting that MISSION2025, one of the major Chinese nation-sponsored hacking groups, are using compromised network/IoT devices such as TVs, smart speakers, surveillance cameras, etc. for their Mirai Botnet campaign.
- Mirai Botnet is infamous for launching DDoS attacks. This year also it came up with new **LeetHozer** botnet variant which tries to exploit many different vulnerabilities and also tries to login via default credentials into the targeted device. LeetHozer sends the device information to its C2C server and waits for instructions to begin a distributed denial-of-service (DDoS) attack.

RANSOMWARE

2020 has been the year of Ransomware so far. We came across a number of different ransomware groups including Maze, NetWalker, Sodinokibi, Nemty, DoppelPaymer, Revil etc., creating their own websites to publish details about the breaches or data exfiltration activities. Details of some infamous ransomware groups are mentioned below:

NetWalker Ransomware

The NetWalker ransomware operators have established themselves as one of the most dangerous ransomware gangs. It is estimated that the operators of the NetWalker ransomware have received over \$25 million from ransom payments since March this year. While precise statistics are not available, the \$25 million figure places NetWalker close to the top of today's most popular ransomware gangs. The group received about 2,795 Bitcoin (BTC) from March 1, allegedly making it one of the cybercriminals' most profitable forms of ransomware. The Bitcoin transactions obtained

by the gang — where the sum is split between many separate addresses — indicate that NetWalker is a "ransomware-as-a-service" malware. A major reason why the gang has been so popular is also because of its "leak site" where the gang publishes names and releases victims' data who fail to pay their demand for ransoms.

Sodinokibi Ransomware

Operators of the Sodinokibi ransomware have tweaked their modus operandi in such a way that if the victim decides to not pay the ransom, the critical data compromised as part of the attack would be posted and sold on hacker forums for subsequent purchase and usage by the hacker community. The victim, already flustered by the attack and data breach, will usually pay the ransom to avoid an escalating series of attacks and compromise of organizational information. Recently the Sodinokibi Ransomware operators published over 12 GB of stolen data allegedly belonging to Brooks International for not paying the ransom.

Maze Ransomware

Maze Ransomware operators attacked IT services giant Cognizant in a series of data breach where unencrypted data was most likely accessed and stolen. They possibly exfiltrated a limited quantity of data from Cognizant's systems during the time they did have access. The Ransomware first spread across the network and steal unencrypted data before encryption. This stolen data is then used to threaten the victim with public disclosure unless the ransom is paid by the victim. CYFIRMA Intelligence and Research team suspects Maze ransomware has been leveraged as part of the joint campaign carried out by North Korean Threat Actor - Lazarus Group and Chinese Threat Actor - Gothic Panda. In addition to these groups, Russian Threat Actor - Cozy Bear (APT29), has been observed publicly reporting of using Maze Ransomware in their operations.

DoppelPaymer Ransomware

CYFIRMA Threat Intelligence team has observed a recent increase in activities related to DoppelPaymer ransomware this year. It is primarily suspected to be operated by threat actor group Indrik Spider, however, another financially motivated Russian group TA505 is also suspected of leveraging this tool. Indrik Spider is considered to be an affiliate of TA505. Along with usual encryption capability, this ransomware would also exfiltrate data from the infected systems. Moreover, DoppelPaymer operators have also launched a site called 'Dopple Leaks' with an intent to expose stolen files and shame non-paying victims. This could have enormous impact on the reputation as well as the finance of the affected entity. DoppelPaymer ransomware was seen to target organizations in multiple industries such as Manufacturing, Oil and Gas, Finance, Public Services, Retail, and others.

Nemty Ransomware

Operators behind the infamous Nemty ransomware started re-charting their operations. They have completely shut down their publicly available Ransomware-as-a-Service (RaaS) model

and are now dedicating all their attention on targeted attacks. Traditionally, Nemty is synonymous with the classic RaaS operation, and has been heavily advertised on underground Russian-speaking hacking forums since it first debuted in 2019. Nemty was popular amongst hackers owing to its monetization model - if ransoms were obtained, the Nemty operator kept 30% of the payment, while the distributors got 70% for their efforts.

Ryuk & WastedLocker Ransomware

Ryuk ransomware activities increased by leveraging Remote Desktop Services (RDS), Citrix devices and Pulse VPN. The actors behind the global campaign have been targeting the energy and utilities, technology, and manufacturing sectors. The motive behind the campaign is data encryption and exfiltration.

The WastedLocker ransomware was developed by the Russian cybercrime crew known as Evil Corp, which was behind Dridex Trojan, and multiple ransomware like Locky, Bart, Jaff, and BitPaymer. WastedLocker ransomware was used in highly targeted attacks, and threat actors also used

SocGhosh fake update framework and a custom version of the Cobalt Strike loader to spread the malware. After compromising the target networks, the attackers would attempt to deploy the ransomware to exhort multimillion-dollar payment. The attackers mainly targeted major corporations. The list of victims includes large private organizations, along with 11 listed companies, eight of which are part of Fortune 500.



08

PHISHING ATTACKS DURING COVID PANDEMIC

Phishing attacks have increased significantly this year and evolved correspondingly with new technologies and methodologies that came into the picture during this Covid-19 era.



CYFIRMA
DECODING THREATS

© CYFIRMA 2020, ALL RIGHTS ARE RESERVED.

During the pandemic, many organizations and government agencies opted for work from home.

This situation helps attackers to launch new spear-phishing attacks, BEC Attacks, phishing scams, etc. A few reported critical phishing incidents are highlighted here:

2020

January & February

- Chinese hackers' association
- Smishing attack
- AZORult & Emotet

April

- Unnamed Global Social Engineering Campaign
- TrickBot Malware Operation

June

- Lemon Duck Cryptominer Distribution
- Leveraging Training Programs

March

- Attacks on VPN
- North Korean Hackers' association
- TA542 association
- Zeus Sphinx Trojan Distribution

May

- Global phishing campaign targeting Microsoft Office 365 users



June 2020

Lemon Duck Cryptominer Distribution: Phishing email started spreading PowerShell script that distributes the Lemon Duck Cryptominer through a new propagation method - COVID-19-themed emails with weaponized attachments. This campaign targeted Garment, Real Estate, Health, Electronics, and Shipping/Logistics industries.

Leveraging Training Programs: The latest identified phishing campaign used a novel training program that is needed to comply with coronavirus legislation for commercial enterprise. The initiative, which targets Office 365 users, sends an email with a link to register for the professional development - "COVID-19 Employee Training: A Health Workplace Certificate". However, rather than a valid sign-up page, it directs users to a malicious website, in which they are required to enter their credentials.

May 2020

Global Phishing campaign targeting Office 365 Users: Microsoft Office 365 users were targeted by a global phishing campaign using bait messages camouflaged as notifications sent by their organization to update the VPN

configuration they would use to access company assets while working from home. The attackers were spoofing the sender email address in the phishing emails to match the domains of their targets' organizations and embed hyperlinks that instead of directing the recipients to new VPN configs, send them to phishing landing sites designed to steal their Office 365 credentials. The landing page was a cloned Office 365 login page hosted on the Microsoft-owned web.core.windows.net domain by abusing the Azure Blob Storage and came with a valid Microsoft certificate, making it a lot harder to detect the phishing attempt.

April 2020

Unnamed Global Social Engineering Campaign: There was an upward surge in global social-engineering lures in malicious emails that promise victims financial relief during the coronavirus pandemic. For an example, a large email campaign was uncovered targeting manufacturing, retail, energy, business services and hospitality companies. The campaign emails claim to be from a major (unnamed) United Kingdom bank. That then leads them to the attacker-controlled landing page that asks for their name, address, and credit-card number.

TrickBot Malware Operation: TrickBot malware operation has targeted multiple industry sectors with the highest number of unique COVID-19-themed malicious emails and attachments. This campaign used several hundreds of unique weaponized attachments in emails that pose as a message from a non-profit offering free COVID-19 test. Then the attackers attempted to monetize their efforts by deploying other payloads as well.

March 2020

Attacks on VPN: VPN applications have been badly affected by multiple phishing attacks launched by the hackers. Hackers tried to impersonate websites through registered domains targeting industries worldwide. The fake VPNs such as Swift VPN, Panda VPN, Shield Next etc. were distributed and created in China. These Fake VPN applications captured organization's internal application behaviour, stole credit card details, confidential information, etc. This data was further sent to three Command & Control servers, out of which two are in France and one is in South Korea.

North Korean Hackers' association: North Korean threat actor groups attacked R&D labs of Manufacturing, Food & Beverage, Retail, Energy, Media, etc. industries by creating COVID-19 phishing emails & websites with a motive of figuring out a way to take out their public tool information and exfiltrate information related to their research, Intellectual Property details.

Zeus Sphinx Trojan Distribution: CYFIRMA Researchers also observed Zeus Sphinx joining the growing fray of COVID-19 themed phishing and malspam campaigns ramping up worldwide. When infected users land on a targeted online banking portal, Sphinx dynamically fetches web injections from its C2 server to modify the page that the user sees, so that the information that the user enters into the log-in fields is sent to the cybercriminals.

January & February 2020

Chinese Hackers' association: Chinese Threat Actors such as Mustang Panda launched Coronavirus-related phishing attacks to target Taiwan.

Smishing Attack: Coronavirus-related SMS phishing attack or "smishing" attack was on rise to steal credentials by redirecting the victims to malicious websites.

AZORult & Emotet: Cybercriminals started sending out phishing emails about coronavirus to the global sectors enticing victims to open attached Microsoft Word document which installs the AZORult information stealer.

09 THREAT ACTORS TARGETING INDIA



Lazarus Group

The North Korean Threat Actor group increased their activities in 2020 which involved “fileless attack”, spreading new malware samples, attacking cryptocurrency businesses, and a lot more.

CYFIRMA Threat Intelligence observed the recent increase of “fileless attack” operated by Lazarus Group where they would install Anchor backdoor using TrickBot trojan. They would also target the cryptocurrency business with augmented abilities as part of Operation AppleJeus Sequel. We noticed a trend where tools such as BISTROMATH RAT, HOPLIGHT, SLICKSHOES Dropper, CROWDEDFLOUNDER RAT, HOTCROISSANT RAT, ARTFULPIE Malware, BUFFETLINE RAT would be used by this group. They are believed to use a few new malware variants known as COPPERHEDGE RAT to target cryptocurrency exchanges. TAINTEDSCRIBE and PEBBLEDASH malware have the capability to download, upload, delete, execute files, allow Windows CLI access, create and terminate processes, and

carry out target system inventory reconnaissance.

The threat actor group was also suspected of targeting users in South Korea by leveraging HWP documents containing COVID-19 contents. It is suspected that a certain backdoor gets installed to carry out remote action once the attacker gains access to the victim's system.

They leveraged a new variant of Dacls RAT specially crafted to target macOS systems. The previous version of this RAT targeted Windows and Linux systems. The new variant of the RAT had been distributed through a malicious two-factor authentication application known as MinaOTP. The new RAT variant could perform Command Execution, File Management, Traffic Proxying, and Worm Scanning.



APT36

**a.k.a Operation
Transparent Tribe,
ProjectM, Mythic Leopard**

This Pakistan government-backed hacker group has targeted Indian diplomats in the past to collect sensitive data like emails, passwords, and location data. In 2020, this threat actor was noticed to have impersonated the Indian government to send emails containing malware to victims, mostly Indians. The emails typically contained bogus health advisories on coronavirus. Victims who click on the attached document activate a malware that gives the hacker access to sensitive and important information like passwords, credit card information and location data stored on a user's browser. Additionally, a number of other intrusions have been detected including a spear-phishing campaign aimed at computers belonging to the Indian Railways. Pakistan's conflict with India has been ongoing and APT36's activities are a continuity of those hostilities.



Mission2025

This group is suspected to be Chinese state-sponsored threat actors and have been active as early as 2012. MISSION2025 is suspected of carrying out various campaigns against multiple industries such as Automotive, Retail, Healthcare, Energy, Hi-Tech, Media, Finance, Healthcare, Telecom, Supply Chain, Travel. The group is believed to target nations such as US, UK, Japan, India, France, South Korea, Hongkong, Thailand for financial gains and/or corporate espionage.

They have been observed implanting trojan and backdoor to steal sensitive information from organizations as part of their cyber-espionage campaigns. These campaigns could possibly be carried out to assist the local Chinese companies as part of the "Made in China 2025" vision. This involves the possible theft of IP, Trade Secrets, and Blueprints, with the likely intent of either Information Exfiltration, Corporate Espionage, or Financial Gains via sale across the Deep/Dark web.



Stone Panda, a.k.a menuPass, APT 10, Cloud Hopper

This Chinese threat actor group has traditionally shown interest in stealing international trade data and supply chain information from various enterprises across several countries such as India, Japan, Canada, Brazil, etc. The group has shown a tendency to target Managed Service Providers (MSP), alongside Government agencies, Financial institutions, and entities in the Energy & Resources domain. The group is motivated by financial gains and to cause reputational damage.

Stone Panda has been observed using Windows default commands and management frameworks for their malware installation; internal reconnaissance in victim environment; and lateral movement. In terms of their proficiency in spear phishing, they execute very high-level reconnaissance followed by credential dumping and further followed by theft of trade secrets and critical business information etc. They use tools like ChChes, EvilGrab, PowerSploit, RedLeaves etc. for executing high level information stealing operations. These situations lead to data

breaches and reputation damage. In the threat actor's recent campaigns; they are potentially using commodity malware including Phorpiex and Sohanad. Most of the observed variants have the capability to download other malware such as advanced backdoor for further campaign operations. CYFIRMA suspects the intent of using commodity malware/pup is to avoid security researchers/analysts attributing the campaign to them at the initial compromise stage.



10 REPORTED CRITICAL INCIDENTS

India-China Border Conflict

Background: India and China have always been uneasy neighbours, while also being two of the biggest economic powers in the Asian continent. Recently, geopolitical tensions between the two countries hit peak levels after a border issue escalated into India's hard stand against Chinese interests and investments in the Indian market, including the banning of a multitude of China origin mobile applications citing security concerns. CYFIRMA's surveillance virtual agents in the Deep/Dark Web and Hackers' forums picked up chatter amongst Chinese threat actor groups about potential retaliatory attacks against India.

Observations: CYFIRMA Research recorded extended conversations in the Chinese hacking communities discussing ways to 'teach India a lesson'. Hackers expressed frustration with India and statements such as "this is one nation who doesn't listen to us" was observed.

The cyber criminals were discussing, in Mandarin, the following targets:

- Press and media companies
- Telecommunication companies (private and public)
- Government websites including defence-related agencies
- Indian Pharma companies
- Smartphones manufacturers
- Construction and tires companies

CYFIRMA's research identified that the following exploits were likely:

- Defacing websites using weakness in web applications
- Data exfiltration using specialized malware
- Denial of Service
- Impersonating companies' website and launching malicious phishing campaigns

Motivation: Naming and shaming, Reputation damage, and Exfiltration of sensitive information including trade secrets.

Analysis: In the hackers' conversations, IP addresses were shared and discussed. Our analysis of these IP addresses attributed Gothic Panda and Stone Panda to be behind these potential hacking campaigns. These are two prolific hacking groups with close association with the Chinese Government.

Reporting & Impact: CYFIRMA's early warning reports about these findings were enthusiastically received by both the government and private sector entities in India with substantial air-time and newsprint dedicated to the same. Indian organizations and entities in the firing line were encouraged to be vigilant and to implement robust mitigation tools and protocols to avoid potential attacks.

11 UPCOMING TRENDS

UPCOMING TRENDS



Ransomware Activities



Reconnaissance
Activity



Phishing and Other Social
engineering attacks



Brute Force &
DDoS Attacks



Continuation of
Commodity
Malware Usage



Ransomware Activities

We notice that the ransomware groups are improving their tactics and have become quite desperate. They do not depend on any particular attack vector or attack method but combine different approaches. Healthcare, government agencies, banks, manufacturing, retail, IT service providers and ecommerce platforms will likely be on their radar for the rest of the year. The planning might have started long before the actual deployment of the malware, thus it is important to stay alert and take all necessary precautions. We could see files getting frequently published on their data leaks sites for groups like Maze, as part of their new 'name and shame' modus operandi. The new 'Ransomware as a Service' (RaaS) model will influence a lot of new age cybercriminals onto hacking as a means for quick money. Data exfiltration, reputation damage & financial gains are the primary motives here.



Phishing and Other Social engineering attacks

We expect this particular trend to continue through this year and the next as well. Data breaches have been more evident only because of different social engineering attacks. Cybercriminals prefer to impersonate and trick the victims to share credentials or engage them in some malicious payment activities. Legitimate companies never ask for critical information over unsolicited emails. Phishing emails would usually contain tell-tale signs as such discrepancy in the "From" address, the use of signature subject lines like "your account will be closed" or "your account will be compromised" etc. These emails are designed to lure the victim to click on malicious hyperlinks or go to phishing websites which would have fake login pages. These fake login pages are created to steal credentials. Sometimes phishing emails have spelling mistakes or poor graphics but due to the lack of user awareness, victims fail to distinguish between an authentic email and a phishing email.



Reconnaissance Activity

Organizations are now deploying smart security tools and implementing proper incident response mechanism to avoid cyber mishaps. So, these days, the greatest challenge for an attacker is to bypass a target's security controls to achieve a successful compromise. When target systems are located on a secure network then the attacker needs to be very careful while bypassing IDS, IPS, firewalls, proxies, and any other elements of a defence-in-depth architecture. Herein, reconnaissance becomes very important for the initial planning. Reconnaissance helps further to gather the intelligence for better visibility on how a target works and what can be the potential vulnerabilities. In our reported campaigns we have always noticed the tendency of port scanning and information harvesting activities which indicate the motives for the threat actors. The attack on port 22, 25, 445, 3389 etc. will likely continue for the foreseeable future.



Brute Force & DDoS Attacks

DDoS & Brute-force activities have increased significantly in comparison to 2019, especially during April to June as per CYFIRMA's recent investigation. According to an Amazon report, the largest DDoS attack took place earlier this year on AWS, the infrastructure was hit with 2.3 TBPS DDoS attack. Starting in 2019, Mirai gathered a lot of infamy in the cyberworld for targeting IOT devices. Not only Mirai but Kaiji malware also joined the notorious list this year, successfully targeting Linux and IoT devices. This will continue along with other generic brute force activities where hackers try to crack credentials via guest, admin, root & some common user id – password combination. The usual process which we noticed showed hackers trying to find information on vulnerabilities which could be leveraged for large scale DDoS attacks. They use several compromised servers, and malware hosting assets to launch attacks. Also, the recent discovery of the NXNSATTACK technique validates our findings. The DDoS attacks

have been more complex, lasted for longer time and mostly targeted critical business, financial business, retail industry etc. Moreover, during this COVID-19 pandemic, we expect RDP brute force scenario to become more obvious. Weak passwords, exposed WordPress container or database servers are the reasons behind these attacks.













Continuation of Commodity Malware usage

CYFIRMA has reported about the commodity malware findings several times. The nation-sponsored hacking groups are still using commodity malware for their campaigns continuously. From our latest observations and investigations, Lazarus Group & Stone Panda have often utilized these malware variants for the initial intrusion stage in many of their campaigns. The observed TTPs are persistence mechanism via service creation, process injection into svchost,

antivirus evasion, usage of unsigned fake applications, dynamic DNS for C2 communication etc. We recommend monitoring and detection of these activities using behaviour-based monitoring systems like EDIR or SIEM.

12 RECOMMENDATIONS

RECOMMENDATIONS

-  **Educate staff** to be wary of unsolicited emails containing attachments – they should not open these emails as they could contain malicious attachments.
-  **Enable emerging security solutions** like deception technology powered with machine learning helps in real-time breach detection and prevention.
-  **Employ backup systems to restore data** in the event of ransomware attacks. Ideally, these backup systems should not be attached or connected to the main network.
-  **Conduct Educational trainings** on social engineering attacks and conduct social Engineering Tests (SET).
-  **Ensure** the email security gateways, Email SPF, DKIM, DMARC, Advanced Threat protection systems, Firewall rules and network proxy controls are configured appropriately to detect the attacks in real time.
-  **Employ a multi-layered threat detection and mitigation approach** to effectively detect and block threats that manage to sneak into your organizational setup.
-  **Manage Supply Chain Risk** by ensuring there is information security policy and process for vendor management, and third-party management.
-  **Implement robust security protocols and encryption**, including authentication or access credentials configurations, to secure critical information stored in databases/servers.
-  **Plan periodic Red Team exercises** to measure the effectiveness of people, process and technology related to defending the organization. Red Team exercise helps organizations to improve security controls, enhance defensive capabilities, and measure the overall effectiveness of existing security operations.
-  **Ensure that all applications/hardware are updated** to their latest versions - this is the best way to flush out exploitable vulnerabilities.

ABOUT CYFIRMA

Headquartered in Singapore and Tokyo, CYFIRMA is a leading threat discovery and cybersecurity platform company. Its cloud-based AI and ML-powered cyber intelligence analytics platform helps organizations proactively identify potential threats at the planning stage of cyberattacks, offers deep insights into their cyber landscape, and amplifies preparedness by keeping the organization's cybersecurity posture up-to-date, resilient, and ready against upcoming attacks. CYFIRMA works with many Fortune 500 companies. The company has offices and teams located in Singapore, Japan, and India.

Official websites:

<https://www.cyfirma.com/>
<https://www.cyfirma.jp/>



[Linkedin.com/company/cyfirma](https://www.linkedin.com/company/cyfirma)



[facebook.com/Cyfirma/](https://www.facebook.com/Cyfirma/)



[twitter.com/cyfirma](https://www.twitter.com/cyfirma)