



Proceedings of
**Webinar on Emerging Cyber
Security Challenges**

(August, 2021)

**NATIONAL CYBER CRIME RESEARCH & INNOVATION CENTRE (NCR&IC)
BUREAU OF POLICE RESEARCH AND DEVELOPMENT
Ministry of Home Affairs, Government of India**



Proceedings of Webinar on Emerging Cyber Security Challenges

June 30th, 2021 (Through Cisco WebEx)

NATIONAL CYBER CRIME RESEARCH & INNOVATION CENTRE (NCR&IC)
Bureau of Police Research & Development
NH-8, Mahipalpur, NewDelhi - 37

(August 2021)

वरुण सिंधु कुल कौमुदी, भा.पु.से.
महानिदेशक

VSK Kaumudi, IPS
Director General

Tel. : 91-11-26781312 (O)
Fax : 91-11-26781315
Email : dg@bprd.nic.in



पुलिस अनुसंधान एवम् विकास ब्यूरो
गृह मंत्रालय, भारत सरकार
राष्ट्रीय राजमार्ग-8, महिपालपुर,
नई दिल्ली-110037

Bureau of Police Research & Development
Ministry of Home Affairs, Govt. of India
National Highway-8, Mahipalpur,
New Delhi-110037

Message



Cyber space is changing and evolving dynamically with the advancement of technologies like Artificial Intelligence (AI), Machine Learning (ML), Automation, Virtualization, Blockchain Networks, Big Data, Internet of Things (IoT), Internet of Senses, Cloud and Quantum Computing etc. With these technologies, 5G and the fast expanding cyber space, it is the need of an hour to dive deeper and to know the emerging cyber security challenges, so that gaps can be bridged faster.

With a view to assess such challenges and to evolve mitigating strategies and techniques, a National Level Webinar on '**Emerging Cyber Security Challenges**' was organized by NCR&IC, BPR&D, on June 30, 2021 at the BPR&D Hqrs. The distinguished speakers from Law Enforcement, Academia and Industry delivered talks on evolving security challenges, cyber crimes and appropriate measures to be adapted and developed to avert them. The Webinar was well attended by more than 400 participants from LEAs.

I congratulate Dr. Karuna Sagar, IPS, IG/Director (Modernization) and his Team comprising of Sh. B S Jaiswal, DIG (Mod), Dr. Manjunath M Gosal, SSO (T) and NCR&IC Professionals on successful conduct of this Webinar.

I believe, the proceedings of this webinar will be very useful for our Police Forces and will go a long way in stimulating new dimensions of resilience and technical upgradation to overcome the challenges and will provide great stimulus to cyber crime prevention and investigation.

(V. S. K. KAUMUDI)

"Promoting Good Practices and Standards"

नीरज सिन्हा, भा.पु.से.
अपर महानिदेशक

Neeraj Sinha, IPS
Additional Director General

Tel.: + 91 11 26781344 • Fax: 91 11 26782201
Email: adg@bprd.nic.in • Website: www.bprd.nic.in



पुलिस अनुसंधान एवम् विकास ब्यूरो
गृह मंत्रालय, भारत सरकार
राष्ट्रीय राजमार्ग-8, महिपालपुर,
नई दिल्ली-110037

Bureau of Police Research & Development
Ministry of Home Affairs, Govt. of India
National Highway-8, Mahipalpur,
New Delhi-110037

Message



Cyber-crime has emerged as a significant road block for the Law Enforcement Agencies around the world. New technologies have continued to challenge the skills and learnings of police investigators.

In the background of emerging concerns relating to cyber-crime, it is heartening to note that Modernization Division of the BPR&D is publishing the proceedings of a National webinar, organized (June 30, 2021) on 'Emerging Cyber Security Challenges'. Words of wisdom of domain experts from law enforcement, academia and industry, on evolving security and cyber-challenges, would be of considerable interest of professionals in the field.

I acknowledge the efforts of the Modernization Division team led by Dr. Karuna Sagar, IPS, IG, Shri B. S. Jaiswal, IPS, Dr. Manjunath M Gosal, SSO (T) and the professionals of National Cyber Research & Innovation Centre (NCR&IC) in the endeavour.

(Neeraj Sinha)

Place: New Delhi.

Date: August 19, 2021

डॉ. करुणा सागर, भा.पु.से.
महानिरीक्षक / निदेशक (आधुनिकीकरण)

Dr. Karuna Sagar, IPS
Inspector General/Director (Modernisation)

Tel. : 91-11-26782023
91-11-26782030 (F)
Email : igmod@bprd.nic.in



पुलिस अनुसंधान एवम् विकास ब्यूरो
गृह मंत्रालय, भारत सरकार
राष्ट्रीय राजमार्ग-8, महिपालपुर,
नई दिल्ली-110037

Bureau of Police Research & Development
Ministry of Home Affairs, Govt. of India
National Highway-8, Mahipalpur,
New Delhi-110037

Executive Summary



Realizing the fact of ever-increasing cases of Cyber Crimes and the need to evolve effective strategies for prevention and investigation of crimes taking place in cyberspace, the National Cyber Research and Innovation Centre (NCR&IC), a component under the 14C Scheme of the MHA, setup at the BPR&D, New Delhi organized a webinar on “Emerging Cyber Security Challenges” on June 30, 2021, at the BPR&D Headquarters, New Delhi. More than 400 Police Officials from State/UTs, CAPFs, CPOs and other Police Forces attended the webinar. This webinar was aimed to provide an interactive digital platform for LEAs to learn from the country’s best cyber experts.

The webinar was addressed by eminent subject matter experts from Academia, Industry and Law Enforcement Agencies. The webinar offered a rich insight to Law Enforcement Officers on emerging cyber security challenges from three different perspectives.

Sh. Neeraj Sinha, ADG, BPR&D in his inaugural remarks highlighted the need of organizing webinars on the latest developments taking place in cyber security avenues. He also urged all the participants to learn new ideas and wisdom from the distinguished speakers present in the webinar.

Sh. Madan Modan Oberoi, IPS, Executive Director, Technology and Innovation, INTERPOL delivered his talk on ‘*Combating Cyber Crime - Trends, Issues and Role of Interpol*’. He shared the incidents of latest trends in cyber-attacks from around the world and informed the participants about the initiatives being taken by INTERPOL in the field of joint investigations and capacity building of law enforcement officials viz a viz prevention and investigation of cyber crimes.

“Promoting Good Practices and Standards”



Sh. Venkata Satish Guttula, Director - Security, Rediff.com spoke at length on his topic '*Anatomy of Phishing Attacks*'. He explained various types of phishing and spear-phishing attacks and the methods to investigate them.

Dr Sandeep Shukla, Joint Coordinator, C3i Center and The National Blockchain Project, Indian Institute of Technology, Kanpur delivered his talk on a very important and crucial topic '*Cyber Security as a National Security Issue*'. He emphasized the need of upgrading the skills and knowledge to identify, prevent and investigate cyber-attacks and Cyber Crimes. He also informed the participants about various initiatives of R&D in cyber security being undertaken by C3i Center, IIT Kanpur.

The officials participating in the webinar got a good opportunity to learn and upgrade their knowledge in emerging cyber security challenges. They actively took part in Q&A sessions followed by each talk and enriched their awareness. Overall, it was an interactive and informative webinar about cyber-attacks and Cyber Crimes. The need for a 'proactive intelligence approach' for LEAs in combating emerging Cyber Crimes and the methods to identify and investigate phishing attacks were two main takeaway messages from the webinar.

(Dr. Karuna Sagar)
Director/IG (Mod)

CONTENTS

Agenda cum Minute to Minute Programme	x
Webinar on Emerging Cyber Security Challenges	1
PROCEEDINGS	1
Session - I: Combatting Cyber Crime – Trends, Issues, and Role of INTERPOL	3
Session – II: Anatomy of Phishing Attacks	46
Session III: Cyber Security as a National Security Issue	71
Concluding remarks and Vote of Thanks	98



AGENDA CUM MINUTE TO MINUTE PROGRAMME WEBINAR ON EMERGING CYBER SECURITY CHALLENGES

June 30th, 2021 (Through Cisco WebEx)

Time	Sessions
10:00AM-10:10AM	Inaugural Address – ADG, BPR&D
10:10AM-10:40AM	<p><i>Session 1:</i></p> <p>Dr. Madan M. Oberoi, IPS, Executive Director, Technology & Innovation, Interpol</p> <p>Topic – Combatting Cyber Crime – Trends, Issues, and Role of INTERPOL</p>
10:40AM-10:50AM	Q&A
10:50AM-11:20AM	<p><i>Session 2:</i></p> <p>Sh. Venkata Satish Guttula, CISM, CDPSE, CDPP Director - Security, Rediff.com India Ltd.</p> <p>Topic – Anatomy of Phishing Attacks</p>
11:20AM-11:30AM	Q&A
11:30AM-12:00PM	<p><i>Session 3:</i></p> <p>Dr. Sandeep Shukla Joint Coordinator, C3i Center and The National Blockchain Project, Department of Computer Science and Engineering Indian Institute of Technology, Kanpur Kanpur, India.</p> <p>Topic – Cyber Security as a National Security Issue</p>
12:00PM-12:10PM	Q&A
12:10PM-12:15PM	Vote of Thanks - DIG (Mod)



Webinar on ‘Emerging Cyber Security Challenges’

June 30th, 2021

PROCEEDINGS

The National Cyber Research & Innovation Centre (NCR&IC), a unit under the I4C Scheme of MHA, established at Bureau of Police & Research Development (BPR&D), New Delhi has organized a One Day Webinar on ‘Emerging Cyber Security Challenges’ on June 30, 2021 (Through Cisco WebEx) at BPR&D HQrs. The objective of the Webinar was to provide an interactive digital platform and interactive session for Law Enforcement Agencies on emerging cybercrimes, new techniques and methodologies for investigation, prevention and modern-day challenges and to learn from the country’s best cyber security experts.

The Webinar was organized on a high level and chaired by Shri Neeraj Kumar Sinha, ADG, BPR&D. More than 400 participants from States, UT, CAPFs, CPOs and other Govt. Departments attended the Webinar. Following were three esteemed speakers one each from LEAs, industry and academia who delivered their talk:

- Sh. Madan M. Oberoy, IPS,**
Executive Director,
Technology & Innovation, Interpol
- Sh. Venkata Satish Guttula, CISM, CDPSE, CDPP**
Director - Security,
Rediff.com India Ltd.
- Dr Sandeep Shukla**
Joint Coordinator, C3i Center and The National Blockchain Project,
Department of Computer Science and Engineering
Indian Institute of Technology, Kanpur
Kanpur, India.

Following session wise topics were selected for delivering the Presentations/Talk by the Panellists/guest speakers: -



- Session I** - Combatting Cyber Crime – Trends, Issues, and Role of INTERPOL
- Session II** - Anatomy of Phishing Attacks
- Session III** - Cyber Security as a National Security Issue

Sh. B. S. Jaiswal, DIG (Mod), BPR&D and NCR&IC moderated the session and started the proceeding of the webinar by welcoming Sh. Neeraj Sinha, ADG, BPR&D as the chief guest of the event. DIG (Mod) explained the purpose of starting the webinar series and introduced NCR&IC to the participants. He informed the participants that NCR&IC is one of the seven verticals of the Indian Cyber Crime Coordination Center (I4C) Scheme and it has got three mandates and they are as follows:

- a) Identify present problems regarding cyber-crime of LEAs, which need research-based solutions
- b) Track emerging technological developments, proactively predict potential vulnerabilities, which can be exploited by cyber criminals
- c) Disseminate the knowledge and experience of LEAs in areas of cyber-crime by creating a strategic partnership with stakeholders in academia, private sector or inter-governmental organization

He informed that the next webinar of this series will be conducted with a different topic related to cyber-crime.

Sh. Neeraj Sinha, ADG, BPR&D delivered an inaugural address by welcoming all the participants and the distinguished speakers. He expressed his compliments to the NCR&IC team, Modernisation Division and DIG (Mod) for organizing a webinar on important topics of cyber security and cyber crime. He informed that as the rapid advancement and development are taking place in cyber space so are the adversaries upgrading their modus operandi in committing cybercrimes. He emphasized the importance of understanding the new challenges cyber space is throwing before law enforcement agencies and gave examples that how cyber warfare has evolved in a manner in which one can wreak havoc into the land of adversaries without even dirtying his/her hands. ADG, BPR&D urged all the participants to learn new ideas and wisdom from the distinguished speakers present in the webinar.

SESSION - I:

Combatting Cyber Crime – Trends, Issues, and Role of INTERPOL

Sh. Jaiswal, DIG (Mod) introduced the first speaker of the webinar, Dr M M Oberoi before the participants. Dr Madan M Oberoi, IPS (AGMUT, 1992) is the Executive Director of Technology and Innovation at Interpol. Dr Oberoi is a Fullbright scholar in the area of cyber security from the University of Washington and holds a PhD in the area of cybercrime from IIT Delhi. He was instrumental in setting up the Indian Cybercrime Coordination Center, I4C Scheme of the Ministry of Home Affairs, Govt of India.



(Dr M.M. Oberoi, IPS)

Dr M.M. Oberoi gave his talk on the topic “Combating Cyber Crime, Trends, Issues and Role of INTERPOL”. The talk was spread across five different agendas as mentioned below:

- i) Technology Radar, ii.) Cybercrime Trends, iii) LEA Issues, iv.) Action Pillars, v.) INTERPOL Support

Dr Oberoi shared his wisdom on the Technology Radar by covering the following verticals:

- a. Connectivity - Cloud Computing, Big data, Internet of things
- b. Digital Disruption- Dark Web, Blockchain Technologies, 3D Printing
- c. Artificial Intelligence (AI) – Deepfake, AI Designed Malware,
- d. Autonomous Machines – Robotics, Drones, Unmanned Vehicles
- e. Simulations- Virtual Reality, Augmented Reality, Digital Twins

Dr Oberoi explained the LEA’s way of looking into emerging technologies. He explained emerging technology may be looked into three aspects viz. The threat, Evidence and Tool. They utilize systems and intelligence to counteract threats, tool aspect is used by Law Enforcement to assist in operational and investigative duties. Similarly, the aspect of Evidence is related to the recovery of data and identifiers. Explaining the broad implications of technological development taking place around



the globe, Dr Oberoi further informed the participants that Data tsunami, Digital disruption, Digital Insecurity, Alternate Anonymous Digital Economy, and Third-Party Policing are the various facets that require the attention of LEAs. He further emphasized that Collection, Collation and Analysis of data is very important for LEAs to manage a large amount of data being generated because of IoT and 5G components. This may help LEAs noise separation from a large amount of data and management of helpful information extracted from a large amount of data. Digital Disruption is caused by the advent of cryptocurrencies, the dark web and drones. Large scale security breaches happening across the spectrum of cyber space is affecting the trust of the common citizen. The usage of cryptocurrency has affected the traditional approach of police in following the currency flow. Since there is anonymity in the ecosystem of cryptocurrencies, the traditional approach of following the movement of currency cannot be done any longer.

While explaining the Cybercrime trends, Dr Oberoi explained that the biggest trend in cybercrime is the increasing incidents of ransomware attacks. Another type of trending cyber crime is Business E-mail Compromise cases which causes tremendous losses in terms of monetary values. Distributed Denial of Services attacks also called DDoS attacks are another cause of great concern as this type of attack takes place on critical infrastructures like power and water supplies. Dr Oberoi continued sharing the news items of high profile cyber-attacks from across the globe. He also highlighted the fact that ransomware attacks have become a sort of cottage industry where cybercriminals are selling the ransomware scripts to other parties and the entire ecosystem has become something called Ransomware as a Service (RaaS). He also said that according to the official data on cybercrime in India, the country has lost Rs 1.25 Lakh Crores due to cybercrimes.

Dr Oberoi also shared the success stories of law enforcement agencies in combating cybercrime. He emphasized the fact that the reason behind these successes is the proactive use of traditional policing methods rather than over-reliance on technology solutions.

Dr Oberoi continued his talk discussing the LEAs issues with regard to combating cybercrime. He discussed at length about following issues:

- i. Intelligence
- ii. Skill & Infrastructure Gaps
- iii. E-evidence Management
- iv. Multi-jurisdictional Collaboration
- v. Reactive Approach

He emphasized the need for a proactive intelligence approach for LEAs in combating emerging cybercrimes.

The fourth agenda of the talk was on Action Pillars. Dr Oberoi mentioned that the Indian Cybercrime Coordination Center (I4C) is founded with the idea of strengthening action pillars in the following areas:

- i. Actionable Intelligence

- ii. Forensics
- iii. Capacity Building
- iv. Strategy & Outreach
- v. Reporting, Investigation & Prosecution
- vi. Research & Innovation

The final and fifth agenda of the talk was on Interpol's support to LEAs in combating cybercrime. Dr Oberoi explained that INTERPOL is having their own Technology Radar under which they research emerging technologies and how they are impacting the crimes happening in cyber space. He informed the participants that INTERPOL is also managing online communities to keep theme-based discussions. They also have developed an INTERPOL Global Knowledge Hub to share and disseminate knowledge in cyber space. He urged the LEAs to join the Global Knowledge Hub and become part of the global learning ecosystem. They have been conducting virtual courses offered free of cost for LEAs. The application for enrolment may be forwarded through CBI. Interpol also runs INTERPOL virtual academy in which more than 90 e-learning modules are created and has more than 20,000 participants on board. Interpol also runs a Cybercrime Operational Coordination centre to coordinate with LEAs of member countries in investigating cybercrimes.

A copy of the presentation may be seen as follows: -



Combating Cyber Crime

Trends, Issues, and Role of INTERPOL

Dr. Madan Oberoi, IPS (AGMUT:1992)
Executive Director (Technology and Innovation), INTERPOL

30 June, 2021

Our way of looking into emerging technologies

THREAT
Utilizing systems and intelligence to counteract threats

TOOL
The use of tools by law enforcement to assist in operational and investigative duties

EVIDENCE
The recovery of data and identifiers

30/6/2021

Technology Radar

- Connectivity**
 - Cloud Computing
 - Big Data
 - Internet of Things
- Digital Disruption**
 - Dark Web
 - Block Chain Technologies
 - 3D Printing
- Artificial Intelligence**
 - Deep Fakes
 - AI Designed Malwares

Other technologies shown include: Autonomous Machines, Robotics, Drones, Unmanned Vehicles, Simulation, Digital Twins, Augmented Reality, and Virtual Reality.

30/6/2021

Broad Implications

- 01 Data Tsunami
- 02 Digital Insecurity
- 03 Digital Disruption
- 04 Alternate Anonymous Digital Economy
- 05 Third Party Policing

7



Ransomware as a service is the new big problem for business

Easy-to-use ransomware as a service schemes are booming, accounting for almost two-thirds of ransomware campaigns during the past year, warn researchers.

By Danny Palmer | March 4, 2021 – 12:31 GMT (20:31 SGT) | Topic: Security

Ransomware as a service is proving effective for cyber criminals who want a piece of the cyber-extortion action but without necessarily having the skills to develop their own malware, with two out of three attacks using this model.

Ransomware attacks are still proving extremely lucrative, with the most well-organised gangs earning millions per victim, so many cyber criminals want to cash in – but don't have the ability to code and distribute their own campaigns.

30/6/2021 <https://www.zdnet.com/article/ransomware-as-a-service-is-the-new-big-problem-for-business/?tag=ASIS&aff=64>

Europol: "Virtually All" Crime Now Has a Digital Element

James Coker
Reporter, Infosecurity Magazine
Follow @ReporterCoker

"Virtually all" criminal activities have an online component to them, while many have fully migrated online, according to a new report by Europol.

The 2021 *Serious and Organised Crime Threat Assessment* (SOCTA) highlighted how criminals are increasingly incorporating digital technologies into their activities, a trend that has been exacerbated in the last year amid COVID-19 lockdowns. This includes in areas like communication and finances, making crimes harder for law enforcement agencies to detect and track down.

The growth of encrypted communication channels and social media has made it easier cyber-criminals to advertise their services to a wider range of people, while the shift to online shopping has "entailed a steep increase in the use of small parcels, via postal or express courier services, to distribute illicit goods." The study additionally noted that new money laundering techniques involving cryptocurrencies have proliferated recently.

Related to This Story

- 21% of UK Workers Feel More Vulnerable to Cybercrime During COVID-19
- Elderly People in the UK Lost Over £4m to Cybercrime Last Year
- Global Public-Private Partnerships Key to Fighting Cybercrime

<https://www.infosecurity-magazine.com/news/europol-crime-has-digital-element/>

Apple supplier is the latest target of a \$50 million ransomware hack

The attackers are threatening to leak blueprints.

J. Fingas | 04.21.21
@jxfingas

Devindra Hardawar/Engadget

The **REvil ransomware gang** has found a fresh target. **BleepingComputer** and **BleepingSecurity** report the group is threatening Apple after one of the tech giant's key **MacBook** suppliers, **Quanta**, allegedly refused to pay a \$50 million ransom following a hack targeting its systems. The attackers disclosed their efforts alongside **Apple's spring event** after Quanta reportedly signaled that it wouldn't pay by the April 27th deadline, and

<https://www.engadget.com/apple-quanta-ransomware-hack-139453046.html>



US fuel pipeline hackers 'didn't mean to create problems'

By Mary Ann Rasmus
Business reporter, BBC News
10 May



A cyber-criminal gang that took a major US fuel pipeline offline over the weekend has acknowledged the incident in a public statement.

"Our goal is to make money and not creating problems for society," DarkSide wrote on its website.

The US issued emergency legislation on Sunday after Colonial Pipeline was hit by a ransomware cyber-attack.

The pipeline carries 2.5 million barrels a day - 45% of the East Coast's supply of diesel, petrol and jet fuel.

<https://www.bbc.com/news/business-57050680>

Fujifilm becomes latest ransomware victim as White House urges business leaders to take action

The National Security Council's top cyber official, Anne Neuberger, released an open letter warning businesses that every organization is at risk.

EXECUTIVE SUMMARY

Ransomware: One of the biggest menaces on the web
Everything you need to know about ransomware: how it started, why it's booming, how to protect against it, and what to do if your PC's infected.
[Read More](#)

In a statement, the company said it was investigating unauthorized access to its servers and had no choice but to shut down its network. On Tuesday evening, the company said it became aware that it was being hit with ransomware and spent the last two days trying to "determine the extent and the scale of the issue."

The photography and medical imaging giant said the attack had affected all of its external communications, including email and phone services. BleepingComputer spoke with Advanced Intel CEO Vitali Kremez, who said Fujifilm had been hit with the Qbot trojan in May and added that the people behind Qbot have been working with the REvil ransomware gang as of late.

REvil caused outrage again this weekend after they were implicated in a ransomware attack on JBS, one of the world's largest meat processors and a company providing about one-fourth of the beef and pork in the US. They previously shut down Colonial Pipeline, causing gas shortages on the East Coast and national outrage that sparked more attention on pharmaceutical multinationals for the situation.

<https://www.sdnet.com/article/fujifilm-becomes-latest-ransomware-victim-as-white-house-urges-business-leaders-to-take-action/#tag=R33d7f948>

Support the Guardian
Available for everyone, funded by readers
Contribute → Subscribe →

Sign in The Guardian
The 200th Years


News Opinion Sport Culture Lifestyle

Coronavirus World UK Environment Science Global development Football Tech More

Cybercrime
This article is more than 1 month old

Colonial Pipeline confirms it paid \$4.4m ransom to hacker gang after attack

The company's CEO authorized the payment as a means to restart the pipeline's systems quickly and safely



A cyberattack forced the shutdown of 5,500 miles of Colonial Pipeline's sprawling interstate system. Photographs: Jim Lis/Sources/EP4

<https://www.theguardian.com/technology/2021/may/19/colonial-pipeline-cyber-attack-ransom>

Swedish Health Agency shuts down SmiNet after hacking attempts

By Sergiu Galian
May 21, 2021 12:38 PM



The Swedish Public Health Agency (Folkhälsomyndigheten) has shut down SmiNet, the country's infectious diseases database, on Thursday after it was targeted in several hacking attempts.

SmiNet, which is also used to store electronic reports with statistics on COVID-19 infections, was shut down on Thursday to investigate the attacks and was brought back online on Friday evening.

<https://www.bleepingcomputer.com/news/security/swedish-health-agency-shuts-down-sminet-after-hacking-attempts/>

30/6/2021

BLEEPINGCOMPUTER

NEWS - DOWNLOADS - VIRUS REMOVAL GUIDES - TUTORIALS - DEALS - FORUMS - MORE

Food giant JBS Foods shuts down production after cyberattack

By Sergio Gattin | May 21, 2021 | 10:57 AM

JBS Foods, a leading food company and the largest meat producer globally, had to shut down production at multiple sites worldwide following a cyberattack.

The incident impacted multiple JBS production facilities worldwide over the weekend, including those from the United States, Australia, and Canada.

<https://www.bleepingcomputer.com/news/security/food-giant-jbs-foods-shuts-down-production-after-cyberattack/>

Info-tech

PTI services disrupted after massive ransomware attack on servers

PTI New Delhi | Updated on October 25, 2020 | Published on October 25, 2020

Ransomware attack on news service provider

Several servers of Press Trust of India (PTI) were infected with ransomware. As a result of the malware encrypting on data and applications, subscribers did not receive news for few hours. LockBit ransomware was used to execute this attack. The news agency did not heed to ransomware demands. Their engineers worked to restore operations in a phased manner. The entire operations were made possible in a couple of hours.

Sopra Steria hit by new version of Ryuk ransomware

IT services company Sopra Steria says it has contained the ransomware virus, but systems will take a few weeks to be fully operational

By Karl Flanders, Emsa Content Editor, Computer Weekly | Published 27 Oct 2020 11:55

European IT services company ransomed

French IT services company Sopra Steria suffered a ransomware attack recently and informed that they will be running below operational capacity, until normalcy is restored. The company has also mentioned that their investigation has not revealed leakage of data or damages to their customers' information systems. They are working with security product companies to identify and isolate the malicious code. Ryuk ransomware was reportedly used to execute this attack. This ransomware has been linked to several major security incidents in the last few months, including an attack on Philadelphia-based eResearch Technology, which provides clinical trial oversight software to drug makers and testing firm. Sopra Steria employs more than 40,000 employees and is one of the largest IT services and consulting groups in Europe.

THE TIMES OF INDIA

GADGETS NEWS

Grocery app BigBasket hacked, data of 2 crore users leaked; What you should do to stay safe

Data breach of online supermarket portal

The personal data of around 2 crore users of online supermarket BigBasket have reportedly been breached. Stolen data include name, contact address, mobile number, passwords, Date of Birth (DOB) and IP address of logins and other information. It is alleged that this data was sold for \$40,000 (approximately 30 lakh rupees). Customers of this online supermarket portal have been advised to change passwords of internet banking accounts, PIN of UPI apps used to order from the app, and as well as replace their passwords used in this app, if the same password is used for their email ids and other services. The company has registered a complaint with the Cyber Cell in Bangalore police and claimed that the financial information of their customers are secure.



Haldiram's servers get hit by ransomware attack, hackers demand \$750,000

Haldiram's servers were affected with the ransomware attack and the hackers are demanding a ransom of USD 750,000.

India TV Tech Desk
New Delhi
Published on: October 18, 2020 16:38 IST

ET CIO.com

From The Economic Times

Noida cyber cell probing Haldiram ransomware attack

The Noida Police are investigating a 'ransomware' attack on the servers of popular food chain Haldiram.

IANIS • October 20, 2020, 12:29 IST

Sour moments for Haldirams and Mithaas

Sweets and snacks manufacturer Haldiram's has been hit by ransomware. This attack affected the critical data on the company's sales and finance. Unidentified hackers also demanded a sum of USD 750.000 (equals to 55 lakh rupees approximately) to release the stolen data. In another incident, restaurant chain Mithaas also be-came a victim of ransomware. This attack has not resulted in any financial loss to the company as per their statement. Noida police have registered a case on both ransomware incidents and are investigating it.

CBS NEWS

Justice Department to prioritize ransomware attacks on same level as terrorism

BY JEFF PEQUER
UPDATED ON: JUNE 3, 2021 / 7:51 PM / CBS NEWS

DOJ to prioritize ransomware on same level as...

BREAKING NEWS
DOJ TO PRIORITIZE CYBERATTACKS ON SAME LEVEL AS TERRORISM

<https://www.cbsnews.com/news/ransomware-cyberattacks-terrorism-doj/>

Money-go-round: The booming cottage industry behind ransomware

Too many people stand to make too much money from ransomware attacks. That has to change, warn EU lawmakers.

The problem is larger than cybercriminals seeking corporations and governments to gain access to their own data | Image via Shutterstock

BY LAURENS CERULLUS
May 18, 2021 / 5:43 pm

30/6/2021 https://www.politico.eu/article/ransomware-attacks-booming-cottage-industry/?utm_source=RSS_Feed&utm_medium=RSS&utm_campaign=RSS_Syndication

BBC NEWS

Bristol company hosted notorious child-abuse site

By Jon Vois
Child-abuse
02 June 2021

A Bristol-based company is being criticised for hosting a website known for sharing child-sex-abuse material.



REUTERS

Latin American crime cartels turn to cryptocurrencies for money laundering

By Diego Ove

MEXICO CITY (Reuters) - In April 2019, Mexican police arrested suspected human trafficker Ignacio Santoyo in a plush area of the Caribbean resort of Playa del Carmen after linking him to a prostitution racket extending across Latin America.

Yet it was not the 2,000 women Santoyo is alleged to have blackmailed and sexually exploited that ultimately led to his capture, but the bitcoin he is suspected of using to help launder the proceeds of his operations, officials said.

The cryptocurrency is emerging as a new front in Latin America's struggle against gangs battling for control of vast criminal markets for sex, drugs, guns and people, according to law enforcement authorities.

"There's a transition to committing crimes in cyberspace, like acquiring cryptocurrencies to launder money ... and the pandemic is accelerating it," said Santiago Nieto, head of the Mexican finance ministry's financial intelligence unit (UIF).

<https://www.reuters.com/article/mexico-bitcoin-insight/latin-american-crime-cartels-turn-to-crypto-to-clean-up-their-cash-idUSKBN2811KD>

Hackers are targeting telecom companies to steal 5G secrets

Cybersecurity researchers at McAfee detail an ongoing cyber-espionage campaign that is targeting telecom companies around the world.

By Danny Palmer | March 16, 2021 - 15:55 GMT (23:55 SGT) | Topic: Security

A cyber-espionage campaign is targeting telecoms companies around the world with attacks using malicious downloads in an effort to steal sensitive data – including information about 5G technology – from compromised victims.

Uncovered by cybersecurity researchers at McAfee, the campaign is targeting telecommunications providers in Southeast Asia, Europe and the United States. Dubbed Operation Diànxùn, researchers say the attacks are the work of a hacking group working out of China.

<https://www.xinnet.com/article/hackers-are-targeting-telecoms-companies-to-steal-5g-secrets/?tag=RSS&off=68>

Tesla Model X hacked and stolen in minutes using new key fob hack

Tesla is rolling out over-the-air software updates this week to prevent the attack from hijacking owner key fobs.

- A Belgian security researcher has discovered a method to overwrite and hijack the firmware of Tesla Model X key fobs, allowing him to steal any car that isn't running on the latest software update.
- The attack takes only a few minutes to execute and requires inexpensive gear

The steps of the attack are :

- Attacker approaches the owner of Tesla Model X vehicle.
- The attacker needs to get as close as 5 meters to the victim in order to allow the older modified ECU to wake up and ensnare the victim's key fob.
- The attacker then pushes the malicious firmware update to the victim's key fob.
- This part requires around 1.5 minutes to execute
- Once a key fob has been hacked, the attacker extracts car unlock messages from the key fob.
- The attacker uses these unlock messages to enter the victim's car.

<https://www.xinnet.com/article/tesla-model-x-hacked-and-stolen-in-minutes-using-new-key-fob-hack/?tag=RSS&off=68>

Phishing sites now detect virtual machines to bypass detection

By Lawrence Abrams

Phishing sites are now using JavaScript to evade detection by checking whether a visitor is browsing the site from a virtual machine or headless device.

Cybersecurity firms commonly use headless devices or virtual machines to determine if a website is used for phishing.

To bypass detection, a phishing kit utilizes JavaScript to check whether a browser is running under a virtual machine or without an attached monitor. If it discovers any signs of analysis attempts, it shows a blank page instead of displaying the phishing page.

<https://www.bleepingcomputer.com/news/security/phis-hing-sites-now-detect-virtual-machines-to-bypass-detection/>

BLEEPINGCOMPUTER

NEWS + DOWNLOADS + VIRUS REMOVAL GUIDES + TUTORIALS + DEALS + FORUMS + MORE

Hackers scan for vulnerable devices minutes after bug disclosure

By Ionut Bascu

May 15, 2021 08:37 AM



Every hour, a threat actor starts a new scan on the public web for vulnerable systems, moving at a quicker pace than global enterprises when trying to identify serious vulnerabilities on their networks.

The adversaries' efforts increase significantly when critical vulnerabilities emerge, with new internet-wide scans happening within minutes from the disclosure.


<https://www.bleepingcomputer.com/news/security/hackers-scan-for-vulnerable-devices-minutes-after-bug-disclosure/>

Report: Russian Dark-Web Site Responsible for Massive Drug Deals

Published: 05 June 2021 12:11 PM UTC

Share 10 Like 54 Tweet 100 Print

Western risk intelligence companies monitoring threatening activity on the internet claim that Hydra, a Russian language site hosted on the Dark Web, is responsible for facilitating some US\$1.37 billion worth of drug deals.



“Hydra acts as a host for sellers to set up and run their own narcotics shops, with Hydra profiting as the intermediary for all executed transactions conducted,” a recent joint report by Flashpoint and Chainalysis, revealed.

“Due to its reputable narcotics products and wide range of sellers, Hydra serves an increasingly diverse buyer clientele, ranging from larger wholesale narcotics buyers to individual recreational users, including students and young people,” it said.

The dark web marketplace only broke onto the scene in 2015, but in the six years since its inception it has exploded in popularity, taking the place of a former competitor, the Russian Anonymous Marketplace RAMP, which was shut down by Russian authorities in 2017.

“RAMP was notorious for taking down its competition by conducting DDoS attacks and reporting names and IP addresses of competitor operators,” the report said.

Unlike other dark-web illegal marketplaces which are sometimes run by a single or small group of hackers, Hydra is believed to have dozens of employees keeping it up.

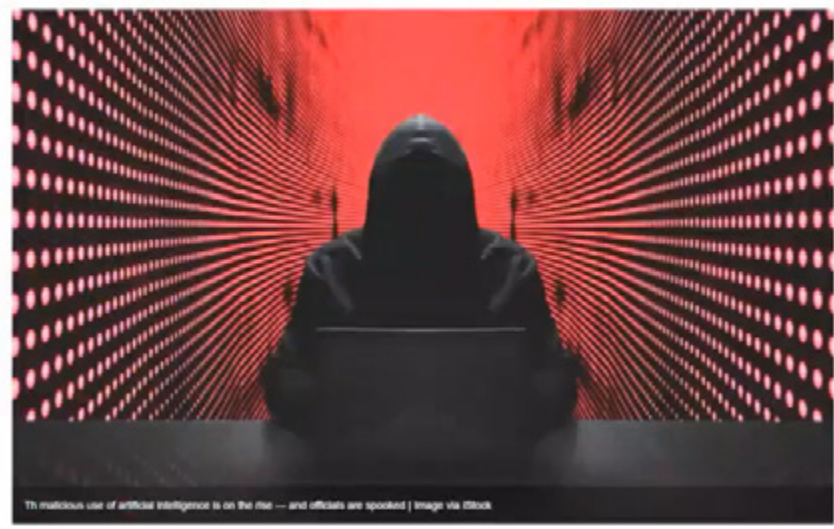
According to flashpoint and chainalysis “Hydra entered the market with a business model related to its mythical namesake: if you cut off one head, two more will grow back in its place,” the report said.

To that end, the site has made a name for itself due to its strict security policies, offering greater anonymity than other dark web marketplaces. While most trades are conducted online through crypto currencies, Hydra actually requires its sellers to take their ultimate profits out in Russian flat currency, which makes them particularly hard to track.

<https://www.ecorp.org/en/daily/14539-report-russian-dark-web-site-responsible-for-massive-drug-deals>

One group that's embraced AI: Criminals

From deepfakes to enhanced password cracking, hackers are discovering the power of AI for malicious use.



The malicious use of artificial intelligence is on the rise — and officials are spooked | Image via iStock

BY LAURENS GERLUS


May 30, 2021 1:50 PM

<https://www.politico.eu/article/artificial-intelligence-criminals/>

FBI warns of scammers targeting families of missing persons

By Sergiu Gatlan

May 17, 2021 12:27 PM



The Federal Bureau of Investigation (FBI) warned that scammers actively target the vulnerable families of missing persons attempting to extort them using information shared on social media.

<https://www.bleepingcomputer.com/news/security/fbi-warns-of-scammers-targeting-families-of-missing-persons/>

Cyber crimes in India caused Rs 1.25 lakh crore loss in 2019: Official

By PTI | October 20, 2020 8:48 PM

Industry expert said that there are only a few Indian companies who are making some of the cyber security products and there is a big vacuum in the sector.

THE WEEK

- 7 of 10 Indian companies saw increase in cyber attacks since lockdown
- India was the third most cyber-attacked nation in the world

By K. Sushil Kumar | October 22, 2020 12:28 PM

Estimating cybercrime losses in India

India's cybersecurity co-ordinator Lt Gen (Retd) Rajesh Pant has said that cybercrimes are responsible for causing a loss of RS 1.25 lakh crore in 2019. He made this remark while speaking at an industry event organised by the Federation of Indian Chambers of Commerce & Industry (FICCI). Besides, he mentioned that the National Cyber Security Strategy (NCSS) will ensure a safe, secure, trusted, resilient and vibrant cyberspace for India and the policy is pending final approval. He has also said that India is now the third most cyber-attacked country in the world.

Info-tech

Cyber frauds to see an uptick in India in 2021: Report

Hemani Sheth | Mumbai | Updated on November 24, 2020 | Published on November 24, 2020

Cyber frauds in India

Kaspersky's security bulletin has predicted a spike of cyber frauds in India around 2021 due to the continuous digitalization of economy. The bulletin also discusses UPI-related frauds in India and the related advisories issued by Indian banks. They have recommended strengthening of security infrastructure at Micro Small and Medium Enterprises (MSME) which are increasingly digitalizing their operations. In addition, the bulletin mentions that the healthcare sector in India faces several cyber risks and makes reference to the recent attacks in Dr Reddy's Laboratories and Lupin pharmaceuticals.

India is second in global ransom payouts for cyberattacks: Survey

TOI

Chennai: Indian organisations were worst hit by ransomware attacks among all Asia Pacific (APAC) nations during the pandemic, and globally, India too stood second when it came to ransom pay-outs and more than a third paid between \$1 million — \$2.5 million to hackers for such cyberattacks. 74% organisations in India suffered a ransomware attack this year compared to 67% of Australia's companies, 52% in Japan, and 46% in Singapore.

Indian companies ransom payout

Ransomware attacks had the worst impact on Indian organisations among all nations in the Asia Pacific during this pandemic. More than a third (34%) of them paid between \$ 1 million to \$ 2.5 million to malicious actors to recover their data and regain system access over the past 12 months. This is one of the key findings of CrowdStrike's '2020 Global Cyber Security Attitude Survey.' The survey's respondents - 2200 senior IT decision makers and IT security professionals - were interviewed during August and September this year. The survey also revealed that nation-state actors are the biggest concern this year, according to 51% of Indian companies. Indian companies were rated second in ransom payouts as compared to nations across the globe.

NEWS

Data Of 10 Cr Digital Payments Transactions Leaked After Attack On Juspay's Server

Harshit Rakheja
Inc42 Staff
03 Jan'21 • 7 min read

- The data includes information about credit and debit cardholders and is being sold on the dark web
- The data, which is in the form of a data dump, appears to have been leaked through a compromised server of payments company Juspay
- Names of issuing bank, expiry date, masked credit/debit card numbers, names, customer ID and merchant account ID have been leaked among several other details

Indian card holders' data leaked

The data of more than 10 crore Indian cardholders has allegedly been leaked in the Dark Web and is also available for sale for an undisclosed amount. The database is reported to have sensitive information like user's card brand (VISA/Mastercard), card expiry date, the last four digits of the card, the masked card number, the type of card (credit/debit), the name on the card, card fingerprint, card ISIN, customer ID and merchant account ID, among other details. It is alleged that this data dump has leaked from a compromised server of Bengaluru-headquartered mobile payment solutions company Juspay.



72% of Covid-related cyberattacks coming via fake emails in India

72 per cent of Covid-19-related attacks today are scamming or spear-phishing which is the fraudulent practice of sending emails ostensibly from a known or trusted sender

Topics
Coronavirus Tests | Coronavirus Vaccine

COVID-19 related fake emails

COVID-19 related cyber-attacks in India make use of scamming and spear phishing techniques. While the spear phishing attacks on compromised accounts are 13%, scammers account for 36% of cyber-attacks. The cumulative percentage of these **attacks through fake emails is 72%**. These were some of the findings of a study by Barracuda Networks. The study also found a huge spike in Business email compromise (BEC). Another finding of the study is that 71% of spear phishing attacks included malicious links, whereas 30% of BEC attacks included malicious link. Similarly, BECs account for 12 % of the spear-phishing attacks and it has increased from 7 % as found in the last year. The emails discuss fake cures and donations to compromise email accounts in Indian organisations.

NEWS • LIVE TV INDIA TODAY
APP MAGAZINE

HOME MY FEED MALAYALAM INDIA CORONA GAMING FACT CHECK

News | India / Mega Mumbai power outage may be result of cyber attack, final report awaited

Mega Mumbai power outage may be result of cyber attack, final report awaited

A malware attack is suspected to be the reason behind Mumbai's power outage last month. The case is being probed by the state's cyber department and the final report is awaited.

Sahil Joshi • Divyesh Singh
Mumbai
November 20, 2020 UPDATED: November 20, 2020 13:06 IST

Mumbai's power outage

Malware **attack** seems to have caused the **power outage that disrupted normal life and business in Mumbai for more than two hours on October 13** of this year. The incident is under investigation with **Maharashtra cyber cell** and their interim findings have **reportedly traced the malware to Padgha-based state load dispatch centre**. The center manages power transmission and load dispatch to areas in Mumbai and Navi Mumbai. The centre works on automated system and monitors data. Investigations have also revealed that the attacks have originated from China. The final outcome of the report is awaited.

mint

Restructuring of networks amid pandemic exposed India to cyber attacks: Report

2 min read • Updated: 20 Dec 2020, 06:48 PM IST

According to the report, India was ranked second after the US among the top 5 countries most affected by ransomware attacks in the third quarter

The sudden rush to provide remote access to employees by restructuring network and security systems during the lockdown made India vulnerable to ransomware attacks in the third quarter of current year, according to cyber security firm Check Point Software Technologies.

Due to the immediate push, several IT companies were unable to scale up their cloud security postures which led to increased opportunity for **cyber criminals to carry out attacks**, Check Point Software

Indian organisations' exposure to cyber-attacks during the pandemic

Due to the lockdown announced in India at the beginning of last year to prevent the spread of COVID-19 virus, many organisations restructured network and security fabrics overnight. In a rush to get work done through **remote access**, some even allowed connectivity from home personal computers for official work. Those computers **often lacked basic cyber hygiene** and did not use updated software patches and anti-malware programs. These made Indian users vulnerable to ransomware attacks, according to a report by **Check Point**. Their survey also **ranks India in the second place after US among the top 5 countries affected by ransomware attacks** in the third quarter of 2020.

Info-tech

Cybercriminals abusing legitimate cloud hosting services in malware campaigns, warns Microsoft

Hemani Sheth | Mumbai | Updated on November 27, 2020 | Published on November 27, 2020

Cyber criminals misusing cloud-hosting services

Cyber criminals are **making use of legitimate hosting services for their malware campaigns**. Microsoft has mentioned that some of the known malwares like BazarLoader, Zloader, Lightbot, Hancitor and others are using this technique. Microsoft's experts have alerted that these email campaigns use topics like threats of job dismissal, exposing of illegal activity and other fear tactics. Downloading and opening the links to malicious document or file hosted on legitimate service leads to payload. Users should avoid clicking on suspicious links.

KrebsOnSecurity
In-depth security news and investigation

ADVERTISING

21 GoDaddy Employees Used in Attacks on Multiple Cryptocurrency Services

NOV 20

Fraudsters redirected email and web traffic destined for several cryptocurrency trading platforms over the past week. The attacks were facilitated by scams targeting employees at GoDaddy, the world's largest domain name registrar, KrebsOnSecurity has learned.

The incident is the latest incursion at GoDaddy that relied on tricking employees into transferring ownership and/or control over targeted domains to fraudsters. In March, a voice phishing scam targeting GoDaddy support employees allowed attackers to assume control over at least a half-dozen domain names, including transaction brokering site [escrow.com](#).

And in May of this year, GoDaddy disclosed that 28,000 of its customers' web hosting accounts were compromised following a security incident in Oct. 2019 that wasn't discovered until April 2020.

This latest campaign appears to have begun on or around Nov. 13, with an attack on cryptocurrency trading platform [nxtqd.com](#).

"A domain hosting provider 'GoDaddy' that manages one of our core domain names incorrectly transferred control of the account and domain

15 SolarWinds Hack Could Affect 18K Customers

DEC 26

The still-unfolding breach at network management software firm SolarWinds may have resulted in malicious code being installed to nearly 18,000 customers, the company said in a legal filing on Monday. Meanwhile, Microsoft should soon have some idea which and how many SolarWinds customers were affected, as it recently took possession of a key domain name used by the intruders to control infected systems.

On Dec. 13, SolarWinds acknowledged that hackers had inserted malware into a service that provided software updates for its Orion platform, a suite of products heavily used across the U.S. federal government and Fortune 500 firms to monitor the health of their IT networks.

In a Dec. 14 filing with the U.S. Securities and Exchange Commission (SEC), SolarWinds said roughly 33,000 of its more than 300,000 customers were Orion customers, and that fewer than 18,000 customers may have had an installation of the Orion product that contained the malicious code. SolarWinds said the intrusion also compromised its Microsoft Office 365 accounts.

The initial breach disclosure from SolarWinds came five days after cybersecurity incident responder FireEye announced it had suffered an intrusion that resulted in the theft of some 300 proprietary software tools the company provides to clients to help secure their IT operations.

On Dec. 13, FireEye published a detailed writeup on the malware infrastructure used in the SolarWinds compromise, presenting evidence that the Orion software was first compromised back in March 2020. FireEye didn't explicitly say its own intrusion was the result of the

Here's a simple explanation of how the massive SolarWinds hack happened and why it's such a big deal

ISABELLA JILIAN | DEC 24, 2020, 2:58 PM

Solar Winds Hack

Software patches update systems and protect them from potential hacks and infections. But, what if the patches contain malicious codes and hacking tools? This was the case of a recent attack on Solar Winds, an American company that develops software for businesses to help manage their networks, systems, and information technology infrastructure.

Suspected Russian hackers were found to have infiltrated malicious code into Orion IT platform; an application provided by Solar Winds, used to manage IT resources, targeting in the process to hack several national agencies and private companies in the US.

As per current reports, several technology companies including Intel, Cisco, VMware and Nvidia suffered Solar Winds hack. Cybersecurity and Infrastructure Security Agency (CISA) of the US government, and FireEye Inc were the first to report these attacks.

30/6/2021

12 SolarWinds: What Hit Us Could Hit Others

JAN 21

New research into the malware that set the stage for the megabreach at IT vendor SolarWinds shows the perpetrators spent months inside the company's software development labs honing their attack before inserting malicious code into updates that SolarWinds then shipped to thousands of customers. More worrisome, the research suggests the insidious methods used by the intruders to subvert the company's software development pipeline could be repurposed against many other major software providers.

In a blog post published Jan. 11, SolarWinds said the attackers first compromised its development environment on Sept. 4, 2019. Soon after, the attackers began testing code designed to surreptitiously inject backdoors into Orion, a suite of tools used by many Fortune 500 firms and a broad swath of the federal government to manage their internal networks.

Attack Timeline - Overview

According to SolarWinds and a technical analysis from CrowdStrike, the intruders were trying to work out whether their "Sunspot" malware - designed specifically for use in undermining SolarWinds' software development process - could successfully insert their malicious "Sunburst" backdoor into Orion products without tripping any alarms

18 VMware Flaw a Vector in SolarWinds Breach?

U.S. government cybersecurity agencies warned this week that the attackers behind the widespread hacking spree stemming from the compromise at network software firm SolarWinds used weaknesses in other, non-SolarWinds products to attack high-value targets. According to sources, among those was a flaw in software virtualization platform VMware, which the U.S. National Security Agency (NSA) warned on Dec. 7 was being used by Russian hackers to impersonate authorized users on victim networks.

On Dec. 7, 2020, the NSA said "Russian state-sponsored malicious cyber actors are exploiting a vulnerability in VMware Access and VMware Identity Manager products, allowing the actors access to protected data and abusing federated authentication."

Russian State-Sponsored Actors Exploiting Vulnerability in VMware® Workspace ONE Access Using Compromised Credentials

Summary

Russian state-sponsored malicious cyber actors are exploiting a vulnerability in VMware® Access and VMware Identity Manager® products [1], allowing the actors access to protected data and abusing federated authentication. VMware released a patch for the Command Injection Vulnerability reported as CVE-2020-4006 on December 3rd 2020. NSA encouraged National Security System (NSS), Department of Defense (DoD), and Defense Industrial Base (DIB) network administrators to prioritize mitigation of the vulnerability on affected servers.

Privileged access to the web-based management interface of the device is required to exploit the vulnerability, so using a strong and unique password lowers the risk of exploitation. The risk is lowered further if the web-based management interface is not accessible from external. The vulnerability affects the following products [2]:

- VMware Access™ 20.01 and 20.10 on Linux®
- VMware vCenter™ 6.5 U1, 6.5 U2, and 6.5 U3 on Linux
- VMware vCloud Connector™ 3.3.1, 3.3.2, 3.3.3, 4.0.0
- VMware vCloud Foundation™ 4.x
- VMware vSphere® Suite Lifecycle Manager™ 4.x

VMware released a software update to plug the security hole (CVE-2020-4006) on Dec. 3, and said it learned about the flaw from the NSA.

The 3 Most Common Types of BEC

CEO fraud: In this instance, attackers will pose as a company CEO or other company executive in an attempt to fool any level of employee — from intern to an accountant to human resources and everything in between — into executing unauthorized wire transfers or sending out confidential tax information. Often, there can be crossover here into social engineering attacks, which use psychological manipulation to trick people into divulging confidential information or providing access to funds.

Usually, CEO fraud phishing emails are social engineering, but they sometimes can be spear-phishing attacks (that is, the attacker spoofs the CEO asking an employee to download a file).

Account compromise: As mentioned above, one of the biggest goals for cyberattacks is account takeover. This is one of the most devastating forms of BEC attacks and involves using phishing emails to hack an executive or employee account and then uses those qualifications to request invoice payments to vendors. Interestingly, this dovetails with reports that more than 56% of organizations report falling victim to a breach caused by their vendor.

Account takeovers may not be seen as destructive as ransomware or malware attacks, but they can cause huge financial loss to companies. They also almost always start with a social engineering attack, asking recipients for unspecified tasks or for compromising information. Then criminals often lurk for months undetected in the back end of systems, learning communication patterns they can later exploit. This ecosystem is clearly still extremely vulnerable to hacking and phishing attacks, leaving a ripe opening for cybercriminals to abuse.

False invoice scheme: The FBI lists false invoice schemes as one of the top five major types of BEC scams. These attacks commonly target someone who works in a business's financial department, such as an accountant. Savvy attackers will alter a legitimate invoice's bank account numbers but leave the rest of the invoice unchanged, making it difficult to detect that it's fraudulent. The possibilities from there are numerous: Some attackers increase the payment amount or create a double payment, among many strategies.

However it happens, the false invoice scheme involves using phishing emails to impersonate the accountant, the vendor, or both. These techniques are replicable in other prominent billing schemes, such as creating shell companies or making fraudulent purchases with organizational funds.

THREAT INTELLIGENCE

1/18/2021 08:05 PM

SolarWinds Attack Underscores 'New Dimension' in Cyber-Espionage Tactics

Meanwhile, Malwarebytes is the latest victim, Symantec discovers a fourth piece of malware used in the massive attack campaign, and FireEye Mandiant releases a free tool to help spot signs of the attack.

The complex cyberattack campaign against major US government agencies and corporations including Microsoft and FireEye has driven home the reality of how attackers are setting their sights on targets' cloud-based services such as Microsoft 365 and Azure Active Directory to access user credentials — and ultimately the organizations' most valuable and timely information.

Today Malwarebytes revealed that it, too, was compromised by the same attackers who infected SolarWinds' Orion network management software to reach many of the targets in the campaign — but via a different attack vector that gained privileged access to 365 and Azure. "After an extensive investigation, we determined the attacker only gained access to a limited subset of internal company emails. We found no evidence of unauthorized access or compromise in any of our internal on-premises and production environments," said Marcin Kleczynski, CEO and co-founder of Malwarebytes, said today in a blog post disclosing the breach, noting that Malwarebytes is not a SolarWinds customer.

Security researchers and incident responders investigating the massive attacks — believed to be the handwork of Russia's nation-state hacking machine — meanwhile continue to find new weapons used in the campaign, even as new victims come forward.

IBM Trusteer Exposes Massive Fraud Operation Facilitated by Evil Mobile Emulator Farms

December 15, 2020 | By Shachar Gritzman co-authored by Limor Kessem | 7 min read

IBM Security Trusteer's mobile security research team has recently discovered a major mobile banking fraud operation that managed to steal millions of dollars from financial institutions in Europe and the US within a matter of days in each attack before being intercepted and halted.

This is the work of a professional and organized gang that uses an infrastructure of mobile device emulators to set up thousands of spoofed devices that accessed thousands of compromised accounts. In each instance, a set of mobile device identifiers was used to spoof an actual account holder's device, likely ones that were previously infected by malware or collected via phishing pages. Using automation, scripting, and potentially access to a mobile malware botnet or phishing logs, the attackers, who have the victim's username and password, initiate and finalize fraudulent transactions at scale. In this automatic process, they are likely able to script the assessment of account balances of the compromised users and automate large numbers of fraudulent money transfers being careful to keep them under amounts that trigger further review by the bank.

Mobile emulators help steal millions of dollars

Twenty emulators were used in the spoofing of over 16,000 compromised mobile devices and swindle millions of dollars from financial institutions in Europe and US. Each of these attacks were conducted in a few days before being intercepted and halted. Malicious actors used mobile emulators to set spoofed devices which in turn accessed thousands of compromised accounts. These attacks were discovered by IBM Security Trusteer's mobile security research team and is reported to be one of the severest and largest incident as on date.

OVER 20 MILLION GIONEE PHONES WERE FOUND TO BE 'INTENTIONALLY INFLICTED' WITH MALWARE

TECH2 NEWS STAFF DEC 07, 2020 13:47:15 IST

A Chinese court has charged Gionee for intentionally installing malware on its smartphones. Between December 2018 and October 2019, Gionee was found to be infecting over 20 million smartphones with Trojan Horse via an app, according to a report by China Judgment Document Network. Reportedly, the app was being used as a tool to profit from users via unsolicited ads, and other illegal means. As per the report, the app was automatically installed on Gionee users' phones without their consent.

Gionee fined for infecting 20 million smartphones

Gionee, Chinese mobile phone maker was fined by a Chinese court for infecting over 20 million smartphones with a Trojan horse malware. The court found that Gionee's subsidiaries colluded to implant the malware in Gionee phones through an app update. Upon automatically updating the Story Lock Screen app, a plug-in called Dark Horse Platform was installed on the phones. Between December 2018 and October 2019, unsolicited ads were also showed to affected users to make financial gains to the tune of 30 crore rupees. It is not clear from available news reports if Gionee phones sold in India were among those affected by this malware.

30/6/2021

EUROPOL

THE CYBER BLUE LINE – THE NEW LAW ENFORCEMENT FRONTIER

28 June 2021
Press Release

Join the Discussion

Europol spotlight report

It all started in 1854 at the battle of Balaklava during the Crimean War when a red-uniformed Scottish Highland Regiment formed a long line and extraordinarily halted a Russian cavalry charge. This act of bravery inspired a phrase still in use today – the thin red line, which is echoed in the term thin blue line often used in the context of law enforcement. As a thinly stretched resource, resisting far greater forces. The thin blue line flag graphic has appeared on everything from police coffee cups to COVID-19 masks.

The 'cavalry charge' is now taking place in cyberspace, as a significant and ever increasing aspect of police work today is dedicated to providing safety and security online. This not only means protecting the rule of law and victims online, but also serving the online community. In doing so, law enforcement is confronted with a number of challenges that, at their core, link to the question on where to draw the thin blue line in cyberspace.

Published today, the Cyber Blue Line report – the latest publication in the Europol Specialist Reporting series, highlights these challenges and identifies a number of pertinent issues which require debate, and thought leadership.

JOIN THE DISCUSSION

From the thin red line, to the thin blue line, to the Cyber Blue Line. Where does responsibility now lie when it comes to maintaining secure and safe societies in cyberspace?

The two authors of the report – Prof. Dr. Mary Aiken and Dr. Philipp Amann, explore the changing ways in which policing could be approached, in the real world and cyberspace, in a continuously evolving technological landscape.

Prof. Dr. Mary Aiken is a world leading expert in Cyberpsychology – the study of the impact of technology on human behaviour. She is a Professor of Cyberpsychology and Department Chair at Capital Technology University Washington DC, a Professor of Forensic Cyberpsychology at the University of East London, and an Adjunct Professor at the Geary Institute for Public Policy, University College Dublin, Ireland. Prof. Dr. Aiken is an Academic Advisor to Europol's European Cybercrime Centre (ECC). Prof. Dr. Aiken holds a PhD in Law from the University of Cambridge, and a MSc in Cyberpsychology.

A Need to Re-examine the Social Contract

Therefore, police leadership, policymakers and society should explore the challenges and opportunities of existing and emerging technologies. Additionally, the social contract that has evolved over hundreds of years of policing should perhaps be re-examined and redrawn? The need for protection in technology environments should also be debated and re-evaluated. How does the thin blue line transposed to cyberspace manifest, and when conceptualising new demarcation in cyberspace where does responsibility lie in terms of maintaining secure and safe societies? Policing bodies worldwide need to work out where on the spectrum of total order and total disorder they position their activities.

<https://www.europol.europa.eu/newsroom/news/cyber-blue-line-162760789-new-law-enforcement-frontier>

EUROPOL

THE CYBER BLUE LINE – THE NEW LAW ENFORCEMENT FRONTIER

28 June 2021
Press Release

Join the Discussion

Europol spotlight report

It all started in 1854 at the battle of Balaklava during the Crimean War when a red-uniformed Scottish Highland Regiment formed a long line and extraordinarily halted a Russian cavalry charge. This act of bravery inspired a phrase still in use today – the thin red line, which is echoed in the term thin blue line often used in the context of law enforcement. As a thinly stretched resource, resisting far greater forces. The thin blue line flag graphic has appeared on everything from police coffee cups to COVID-19 masks.

The 'cavalry charge' is now taking place in cyberspace, as a significant and ever increasing aspect of police work today is dedicated to providing safety and security online. This not only means protecting the rule of law and victims online, but also serving the online community. In doing so, law enforcement is confronted with a number of challenges that, at their core, link to the question on where to draw the thin blue line in cyberspace.

Published today, the Cyber Blue Line report – the latest publication in the Europol Specialist Reporting series, highlights these challenges and identifies a number of pertinent issues which require debate, and thought leadership.

JOIN THE DISCUSSION

From the thin red line, to the thin blue line, to the Cyber Blue Line. Where does responsibility now lie when it comes to maintaining secure and safe societies in cyberspace?

The two authors of the report – Prof. Dr. Mary Aiken and Dr. Philipp Amann, explore the changing ways in which policing could be approached, in the real world and cyberspace, in a continuously evolving technological landscape.

Prof. Dr. Mary Aiken is a world leading expert in Cyberpsychology – the study of the impact of technology on human behaviour. She is a Professor of Cyberpsychology and Department Chair at Capital Technology University Washington DC, a Professor of Forensic Cyberpsychology at the University of East London, and an Adjunct Professor at the Geary Institute for Public Policy, University College Dublin, Ireland. Prof. Dr. Aiken is an Academic Advisor to Europol's European Cybercrime Centre (ECC). Prof. Dr. Aiken holds a PhD in Law from the University of Cambridge, and a MSc in Cyberpsychology.

A Need to Re-examine the Social Contract

Therefore, police leadership, policymakers and society should explore the challenges and opportunities of existing and emerging technologies. Additionally, the social contract that has evolved over hundreds of years of policing should perhaps be re-examined and redrawn? The need for protection in technology environments should also be debated and re-evaluated. How does the thin blue line transposed to cyberspace manifest, and when conceptualising new demarcation in cyberspace where does responsibility lie in terms of maintaining secure and safe societies? Policing bodies worldwide need to work out where on the spectrum of total order and total disorder they position their activities.

<https://www.europol.europa.eu/newsroom/news/cyber-blue-line-162760789-new-law-enforcement-frontier>

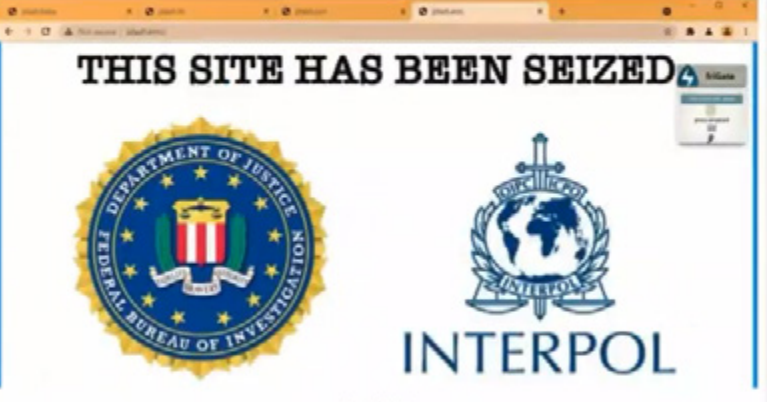
2A

Successes in Combating Cybercrime



FBI & Interpol disrupt Joker's Stash, the internet's largest carding marketplace

By Caitlin Ciampini for Zero Day | December 18, 2020 - 17:30 GMT (09:30 SGT) | Topic: Security



Officials from the US Federal Bureau of Investigation and Interpol have seized a small number of servers used by Joker's Stash, the internet's largest marketplace for buying & selling stolen cards, temporarily disrupting the site's activity.

<https://www.sdmnet.com/article/fbi-interpol-disrupt-jokers-stash-the-internets-largest-carding-marketplace/?tag=RSS&id=68>

Police smash 'world's most dangerous' cybercrime malware tool

International police have disrupted the "world's most dangerous" cybercrime malware tool used to break into computer systems, law agencies announced on Wednesday.

The illicit tool called EMOTET was operated as a so-called botnet, software that infects a network of computers and allows them to be remotely controlled, Europol and its judicial sister agency Eurojust said.

Police based in Britain, Canada, Germany, Lithuania, the Netherlands, Ukraine and the United States teamed together to infiltrate EMOTET's infrastructure.

<https://www.france24.com/en/live-news/20210127-police-smash-world-s-most-dangerous-cybercrime-malware-tool>

KrebsOnSecurity

18 **Joker's Stash Carding Market to Call It Quits**

JAN 21

Joker's Stash, by some accounts the largest underground shop for selling stolen credit card and identity data, says it's closing up shop effective mid-February 2021. The announcement came on the heels of a turbulent year for the major cybercrime store, and just weeks after U.S. and European authorities seized a number of its servers.

The Russian and English language carding store first opened in October 2014, and quickly became a major source of "dumps" — information stolen from compromised payment cards that thieves can buy and use to create physical counterfeit copies of the cards.

But 2020 turned out to be a tough year for Joker's Stash. As cyber intelligence firm Intel 471 notes, the curator of the store announced in October that he'd contracted COVID-19, spending a week in the hospital. Around that time, Intel 471 says many of Joker's loyal customers started complaining that the shop's payment card data quality was increasingly

Then on Dec. 16, 2020, several of Joker's long-held domains began displaying notices that the sites had been seized by the U.S. Department of Justice and Interpol. The crime shop quickly recovered, moving to new infrastructure and assuring the underground community that it would continue to operate normally.

Gemini estimates that Joker's Stash generated more than a billion dollars in revenue over the past several years. Much of that revenue came from high-profile breaches, including tens of millions of payment card records stolen from major merchants including Saks Fifth Avenue, Lord and Taylor, Bebe Stores, Hilton Hotels, Jason's Deli, Whole Foods, Chipotle, Wawa, Sonic Drive-In, the Hy-Vee supermarket chain, Buca Di Beppo, and Dickey's BBQ.

Joker's Stash routinely teased big breaches days or weeks in advance of selling payment card records stolen from those companies, and periodically linked to this site and other media outlets as proof of his shop's prowess and authenticity.


Like many other top cybercrime bazaars, Joker's Stash was a frequent target of phishers looking to rip off unwary or unsophisticated thieves. In 2018, KrebsOnSecurity detailed a vast network of fake Joker's Stash sites set up to steal login credentials and bitcoin. The phony sites all traced back to the owners of a Pakistani web site design firm. Many of those fake sites are still active (e.g. jokerstash[.]su).

As noted here in 2016, Joker's Stash attracted an impressive number of customers who kept five and six-digit balances at the shop, and who were granted early access to new breaches as well as steep discounts for bulk buys. Those "partner" customers will be given the opportunity to cash out their accounts. But the majority of Stash customers do not enjoy this status, and will have to spend their balances by Feb. 15 or forfeit those funds.

Law enforcement take down three bulletproof VPN providers

The three VPN services provided safe haven for cybercriminals to carry out ransomware attacks, web skimming operations, spearphishing, and account takeovers.

By Caitlin Ciampini for Zero Day | December 22, 2020 - 12:55 GMT (20:55 SGT) | Topic: Security





Secure Comms: Cracking the Encrypted Messages of Balkan Crime Gangs

By Ivana Jeremic, Belgrade, Biliv, April 12, 2021 06:42

Among the evidence gathered against a notorious Serbian crime gang rounded up in February were gruesome photos sent via an encrypted messaging app popular with drug smugglers. The downfall of Sky ECC and EncroChat has been a boon for police in Europe and the US, but raises a host of questions going forward.

When Serbian police arrested the leaders of a notorious crime gang in the first few days of February this year, in the search for evidence they seized 44 mobile phones equipped with an encrypted messaging app created by Canada-based Sky ECC.

Sky ECC described itself as "a global leader in secure messaging technology", helping to keep a host of industries safe from identity theft and hacking. Law enforcement authorities in the United States and Europe, however, say it was created with the sole purpose of facilitating drug trafficking and had become the messaging app of choice for transnational crime organisations.

Using equipment that President Aleksandar Vucic said Serbia had "borrowed from friends", police managed to access the app. What they found was gruesome, and damning – photos of two dead men, one of them decapitated.

<https://balkaninsight.com/2021/04/12/secure-comms-cracking-the-encrypted-messages-of-balkan-crime-gangs/>

First verdict against managers of the FIN7 gang: 10 years in prison

Fedir H. was arrested in Dresden in 2018. In Seattle, the online thief has now been sentenced to 10 years. The confessor is responsible for billions in damages.

Reading time: 3 min. Save to Pocket

From 2013 onwards, the FIN7 gang used sophisticated phishing attacks and malware to infiltrate bank servers, ATMs and payment terminals around the world. In 2015, the machinations of the criminal gang, also known as the Carbanak gang, were exposed for the first time - it was the largest online crime to date. Four of the gang members were arrested in Europe in 2018, including Fedir H. in Dresden. The Ukrainian was extradited to the USA and is now the first member of the gang to be convicted in Seattle.

The verdict is ten years in prison and \$ 2.5 million in redress. The court does not impose a fine due to the fact that it cannot be collected. With a confession, H. saved himself an extensive legal process and an even harsher judgment, because the prosecution dropped dozens of charges in return. Should H. have assets, 85 percent of the reparation goes to American Express.

In 2015, investigators from Kaspersky, Europol, Interpol and other institutions assumed that the damage would amount to a billion US dollars - but the US federal attorney's office is now talking of more than three billion dollars. The gang is said to have had more than 70 members. First, they made it easier for over 100 financial institutions in 40 countries to manipulate accounts and ATMs.

Thousands of payment terminals at chains attacked

In 2015, the gang started to infiltrate the payment terminals of other companies in order to access payment card data. The victims included restaurants belonging to the US chain Chipotle Mexican Grill, where FIN7 used malware to steal credit card data from the computer register. FIN7 then sold the card data underground to other criminals who went shopping with card clones.

<https://translate.google.co.uk/translate?hl=en&sl=de&url=https://www.heise.de/news/Erstes-Urteil-gegen-Manager-der-FIN7-Bande-10-Jahre-Knast-6020791.html&prev=search&pt=au>

First verdict against managers of the FIN7 gang: 10 years in prison

Fedir H. was arrested in Dresden in 2018. In Seattle, the online thief has now been sentenced to 10 years. The confessor is responsible for billions in damages.

Reading time: 3 min. Save to Pocket

From 2013 onwards, the FIN7 gang used sophisticated phishing attacks and malware to infiltrate bank servers, ATMs and payment terminals around the world. In 2015, the machinations of the criminal gang, also known as the Carbanak gang, were exposed for the first time - it was the largest online crime to date. Four of the gang members were arrested in Europe in 2018, including Fedir H. in Dresden. The Ukrainian was extradited to the USA and is now the first member of the gang to be convicted in Seattle.

The verdict is ten years in prison and \$ 2.5 million in redress. The court does not impose a fine due to the fact that it cannot be collected. With a confession, H. saved himself an extensive legal process and an even harsher judgment, because the prosecution dropped dozens of charges in return. Should H. have assets, 85 percent of the reparation goes to American Express.

In 2015, investigators from Kaspersky, Europol, Interpol and other institutions assumed that the damage would amount to a billion US dollars - but the US federal attorney's office is now talking of more than three billion dollars. The gang is said to have had more than 70 members. First, they made it easier for over 100 financial institutions in 40 countries to manipulate accounts and ATMs.


Thousands of payment terminals at chains attacked

In 2015, the gang started to infiltrate the payment terminals of other companies in order to access payment card data. The victims included restaurants belonging to the US chain Chipotle Mexican Grill, where FIN7 used malware to steal credit card data from the computer register. FIN7 then sold the card data underground to other criminals who went shopping with card clones.

<https://translate.google.co.uk/translate?hl=en&sl=de&url=https://www.heise.de/news/Erstes-Urteil-gegen-Manager-der-FIN7-Bande-10-Jahre-Knast-6020791.html&prev=search&pt=au>

£3.7m dark web drug dealers jailed after using auto 'bot' for orders

Their app gave customers regular updates, even apologising for supply issues during the Covid-19 pandemic



Two dealers who set up a £3.7 million dark web drugs ring were so inundated with customers they set up an automated "bot" to take orders.

Jehanzeb Amar, 29, and Salahydn Warsame - jailed for a total of 24 years on Wednesday - were part of an organised crime network supplying cocaine, ecstasy and LSD across Britain.

Scotland Yard were tipped off about an online social media site called "LetsWork" advertising Class A drugs in February 2020.

<https://www.standard.co.uk/news/crime/jehanzeb-amar-salahydn-warsame-jailed-dark-web-drug-auto-bot-6932509.html>



Man convicted after FBI alert Cork gardaí he accessed child pornography on dark web

Detective Sergeant Kevin Long of Cork West Divisional Protective Services Unit based in Donemoney said they received information from the FBI identifying a person in their area accessing an online site dedicated to child exploitation. File photo: iStock

<https://www.irishexaminer.com/news/courtdorona/aid-40284074.html>

Arrested in Palma for possession of child pornography videos

The police discovered it when they had his computer repaired and numerous files with sexually exploited children appeared

Drafting

Palma | 08 - 05 - 21 | 12:02 | updated at 12:10 PM

Arrested in Palma for possession of child pornography videos / NATIONAL POLICE

Agents of the National Police in Palma have proceeded to the arrest of a Colombian man, for his alleged participation in the commission of a crime of corruption of minors after it was discovered that he had a large number of images of child pornography on his computer.

30/6/2021 <https://www.diariodemallorca.es/success/2021/05/08/detenido-palma-posesion-video-pornografia-51478333.html>

BBC NEWS

Home Coronavirus Video World Asia UK Business Tech Science Stories Entertainment & Arts

World Africa Australia Europe Latin America Middle East US & Canada

Child sexual abuse: Four held in German-led raid on huge network

German authorities said the platform had more than 400,000 users

German police have arrested three men and a fourth is being held in Paraguay for allegedly running one of the world's biggest online networks for sharing images of child sex abuse.

Climate action is still hotly contested in Australia

<https://www.bbc.com/news/world-europe-56968414>

Ukraine arrests Clop ransomware gang members, seizes servers

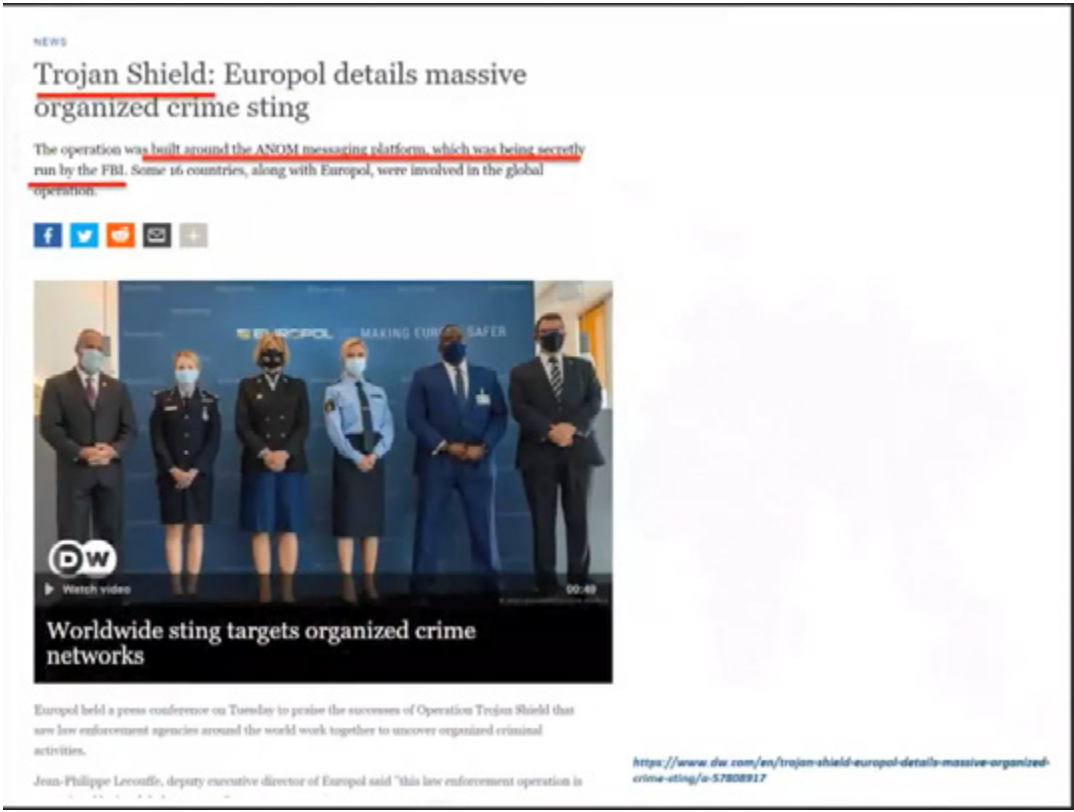
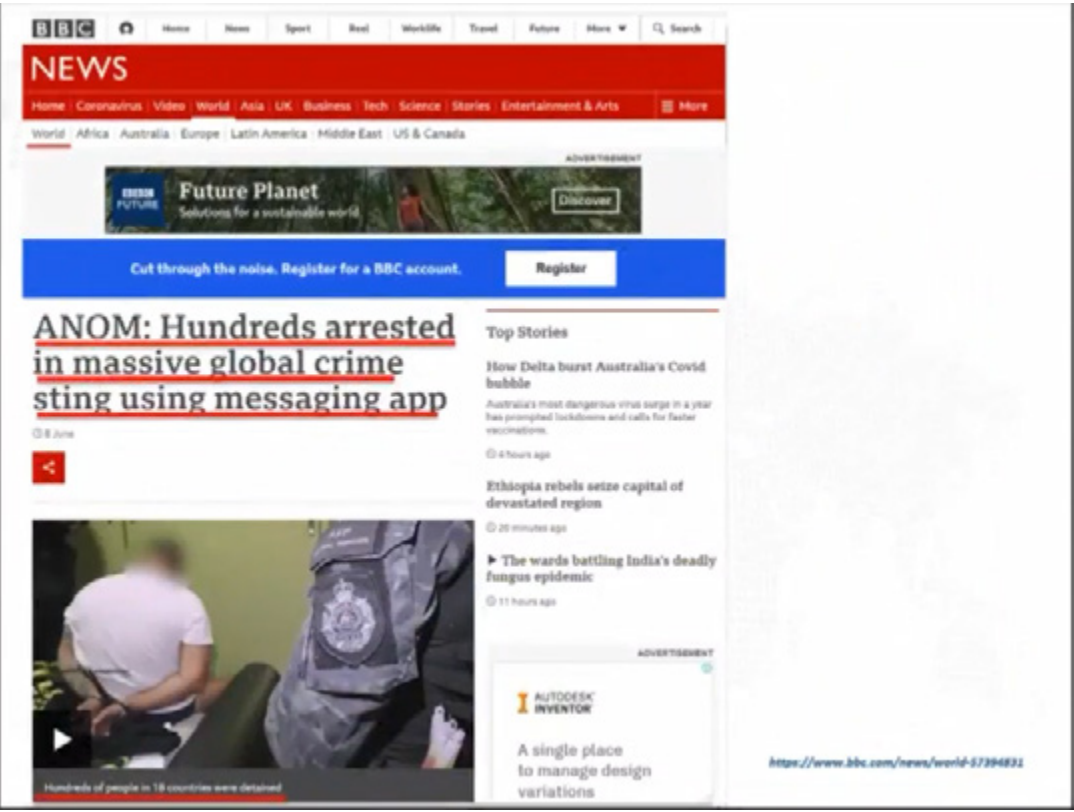
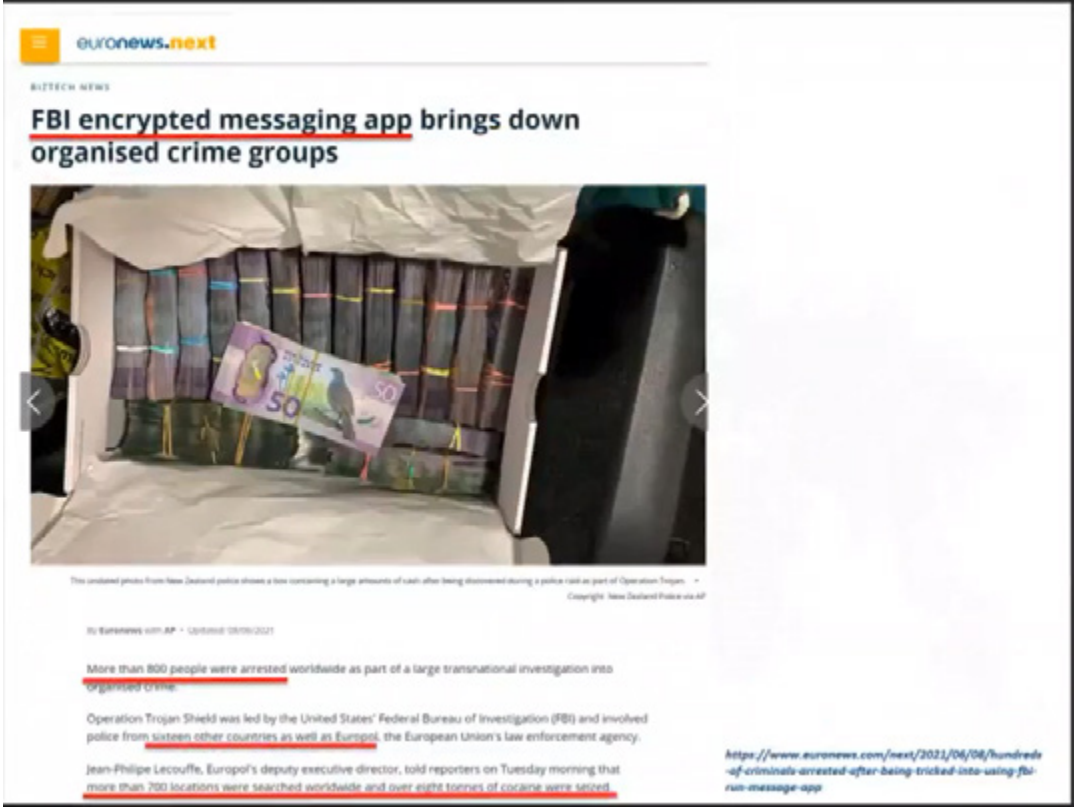
By Sergiu Gatlan

June 15, 2021

Ukrainian law enforcement arrested cybercriminals associated with the Clop ransomware gang and shut down infrastructure used in attacks targeting victims worldwide since at least 2019.

According to the Cyberpolice Department of the National Police of Ukraine the ransomware group is behind total financial damages of roughly \$500 million.

<https://www.bleepingcomputer.com/news/security/ukraine-arrests-clop-ransomware-gang-members-seizes-servers/>





Thornberg: Anom "a formidable gold mine"

TT News Agency 2021-06-15

Anom
 Krypterad tjänst som använts på **12 000 enheter**
 av personer i mer än **300 kriminella nätverk**
 i minst **100 länder**

MORE FROM MSN
 Stefan Löfven meeting with you
 Anna Book police report
 Alexandra thrown out

Thanks to Anom, the Swedish police have reached a new level of leadership in the criminal food chain.
 National Police Chief Anders Thornberg now reiterates the demands to be able to listen more - and emphasizes that more "ordinary" drug buyers must see their part in the serious violence in Sweden.
 Just over a week ago, police around the world, including Sweden, carried out one of the most extensive operations to date.

<https://www.msn.com/en-se/nyheter/nyheter/thornberg-anom-en-formidabel-guldgruva/er-AA1483z>

HAMBURG & SCHLESWIG-HOLSTEIN

Encrochat data leads to around 300 investigations

Published on 06/01/2021 | Reading time: 2 minutes

Hamburg (dpa / lno) - The decryption of the Encrochat network used by criminals by French investigators poses enormous challenges for the Hamburg police and public prosecutor. The Senate therefore decided on Tuesday to create 32 new positions in the investigative authorities, 28 of these are to be created by courts and public prosecutors, and another 34 temporarily by the police, as Justice Senator Anna Gallina (Greens) explained. Nine million euros are to be provided for the increase in staff.

The encrypted cell phones, the app and the chats of the communication service provider Encrochat were mainly used by criminals for the arms and drug trade. French authorities managed to crack the code last year.

Europe was able to skin off millions of secret messages, it said. It is about the smuggling of cocaine in the ton range. "The dimensions are breathtaking," said Gallina. The data sets that were sent to the Hamburg authorities have so far led to around 300 investigations by the public prosecutor and the police. Charges have already been brought in 50 cases. According to Interior Senator Andy Grote (SPD),

<https://www.welt.de/regionales/hamburg/article231521713/Encrochat-Daten-fuehren-zu-rund-300-Ermittlungsverfahren.html>

DARKMARKET: WORLD'S LARGEST ILLEGAL DARK WEB MARKETPLACE TAKEN DOWN

12 January 2023
 Press Release

DarkMarket, the world's largest illegal marketplace on the dark web, has been taken offline in an operation involving law enforcement agencies from Denmark, Moldova, Ukraine, the United Kingdom, the National Internet Agency and the FBI, and also Estonia, supported the takedown with specialist operational analysis and coordinated the cross-border collaborative effort of the countries involved.

DarkMarket in figures:

- almost 500 000 users;
- more than 2 400 sellers;
- over 320 000 transactions;
- more than 4 650 bitcoin and 12 800 monero transferred.

At the current rate, this corresponds to a sum of more than €140 million. The vendors on the marketplace mainly traded all kinds of drugs and sold counterfeit money, stolen or counterfeit credit card details, anonymous SIM cards and malware.

How Police Secretly Took Over a Global Phone Network for Organized Crime

In only one country it led to:

- Arrest of more than 100 suspects
- Seizure of more than 8000 KG of Cocaine
- Seizure of more than 1200 KG Crystal Meth
- Dismantling of 19 Synthetic Drug Labs
- Seizure of more than 20 M Euros in cash

Police monitored a hundred million encrypted messages sent through Encrochat, a network used by career criminals to discuss drug deals, murders, and extortion plots.

Because the messages were encrypted on the devices themselves, police couldn't tap the group's phones or intercept messages as authorities normally would. On Encrochat, criminals spoke openly and negotiated their deals in granular detail, with price lists, names of customers, and explicit references to the large quantities of drugs they sold, according to documents obtained by Motherboard from sources in and around the criminal world.



More than 20,000 arrests in year-long global crackdown on phone and Internet scams
9 December 2020

Home > News and Events > News > 2020 > More than 20,000 arrests in year-long global crackdown on phone and Int...

Targeting rising trends in telephone and online scams, Operation First Light intercepted over 150 million dollars in illicit funds.

LYON, France: A year-long investigative clampdown on criminal networks coordinated by INTERPOL has demonstrated the scale of phone and online frauds worldwide. Codenamed First Light, the operation officially concluded in November with the following results:

- 10,380 locations raided
- 21,549 operators, fraudsters and money launderers arrested
- 310 bank accounts frozen
- USD 153 973 709 worth of illicit funds intercepted.

This latest edition of Operation First Light marked the first time law enforcement has coordinated with INTERPOL on a global scale to combat telecoms fraud, with operations taking place on every continent.

What, in terms of law enforcement strategy, is common in these success stories

422 ARRESTED AND 4 031 MONEY MULES IDENTIFIED IN GLOBAL CRACKDOWN ON MONEY LAUNDERING
02 December 2020
Press Release

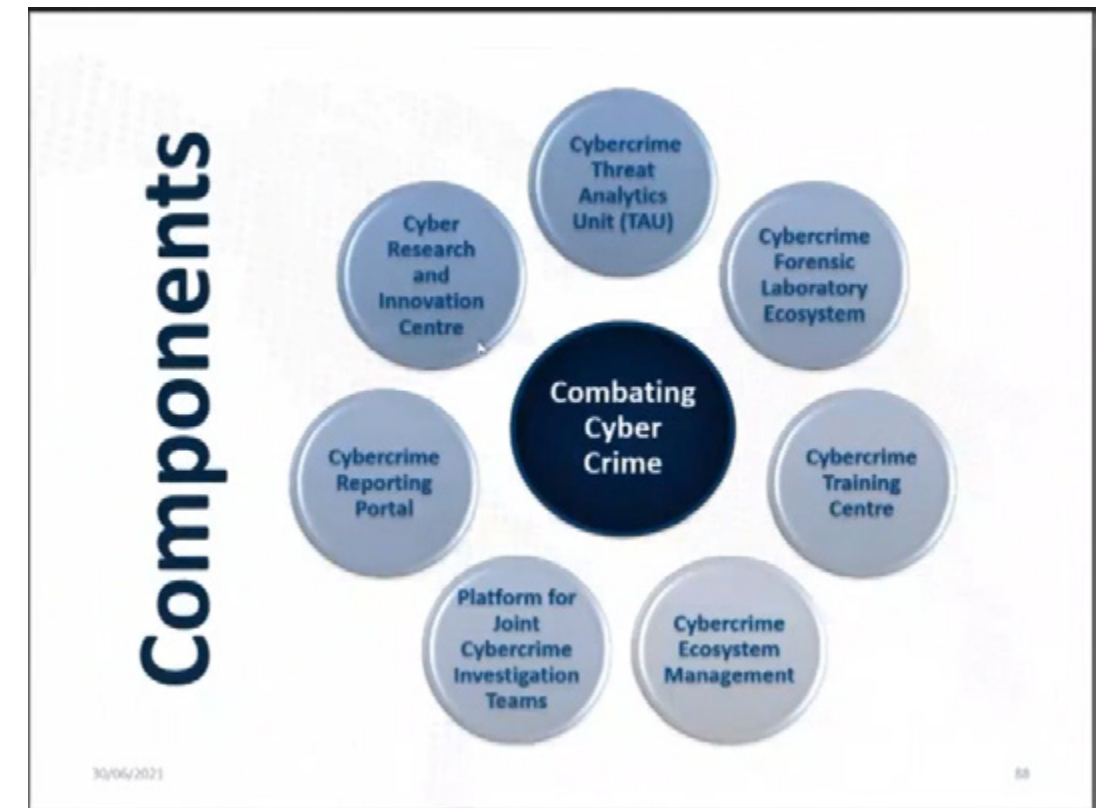
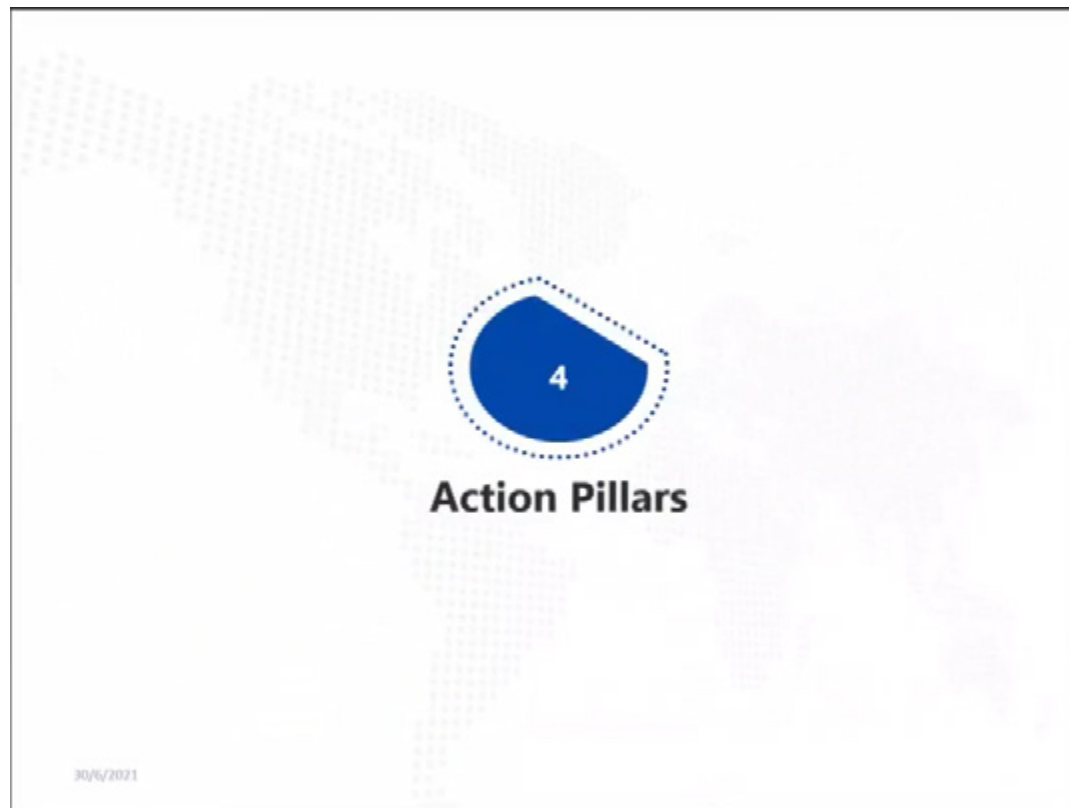
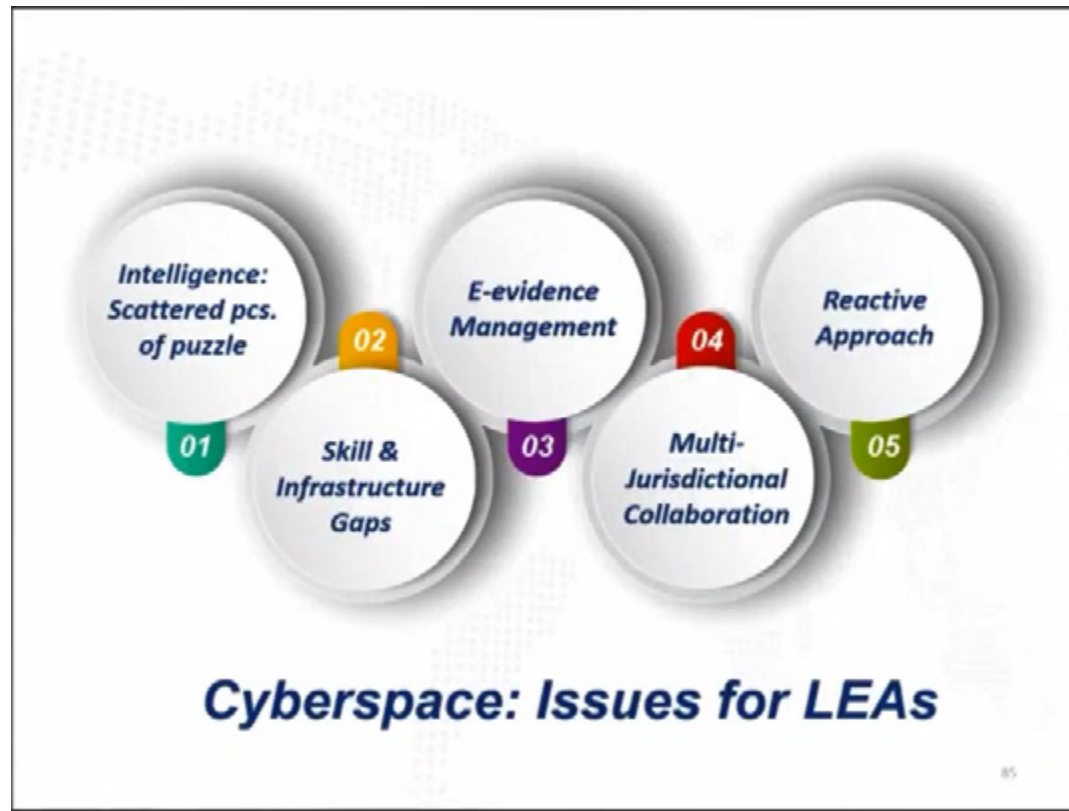
Today, law enforcement authorities from 26 countries and Europol announce the results of the European Money Mule Action 'EMMA 6', a worldwide operation against money mule schemes. Between September and November 2020, EMMA 6 was carried out for the sixth consecutive year with the support of the European Banking Federation (EBF) or FinTech FinCrime Exchange (INTERPOL) or Western Union. As a result, 4 031 money mules were identified alongside 227 money mule recruiters, and 422 individuals were arrested worldwide.

During the span of the operation, 1 529 criminal investigations were initiated. With the support of the private sector including more than 500 banks and financial institutions, 4 942 fraudulent money mule transactions were identified, preventing a total loss estimated at €33.5 million.

3

LEA Issues

30/6/2021





Aim:

Objective
Enable
Research based
response

Objectives:

- i. Create strategic partnerships
- ii. Identification of Research Problems based on the inputs from field
- iii. Leverage the strength and expertise of all such entities
- iv. Examine and recommend measures to strengthen Legal and Strategic framework

INTERPOL Technology Radar

Radar Base Features

INTERPOL Technology Radar

Radar Base Features

- Communities section with an overview of all existing communities (closed groups)
- Possibility to join one or more of them, depending on users' interests and work needs

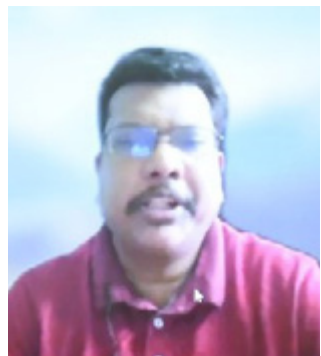


INTERPOL Support



SESSION – II:

Anatomy of Phishing Attacks



(Sh. Venkata Satish Guttula)

The next speaker, **Sh. Venkata Satish Guttula, CISM, CDPSE, CDPP Director – Security, Rediff.com India Ltd** elaborated the detailed anatomy of Phishing Attacks, their types and measures to prevent such attacks. The statistics of cyber-attacks using phishing techniques has increased steeply during the last few years. More than 90% of targeted cyber-attacks used Spear-Phishing in the initial phase to gain entry to the organization’s network.

The use of Phishing URLs in Emails has been increased tremendously in the previous few years and one-third of the data breaches that happened in this time frame involved phishing attacks. To instantiate some are the ones faced by Maersk due to which it lost the business of about \$200 million to \$300 million due to NotPetya Ransomware received from an Email. Business Email Compromise fraud saw significant losses and COVID-19 related Email attacks increased by 667% and 18 million such Emails were seen in just 1 week during April last year(2020).

Phishing attacks and the underneath techniques used have also been explained in detail. Phishing is a technique used by cyber-criminals to send genuine-looking Emails and make the user take action. These actions can be replying with personal information or clicking the link in the Email and doing some transactions etc. Attackers also take advantage of natural disasters, epidemics, pandemics to send malicious Emails under the pretext of local authorities that are in charge of dispensing various help, aids or have been offering other support initiatives.

Types of Phishing involves **Mass phishing** which is a type of large volume attack intended to reach as many people as possible. **Spear phishing** is a targeted attack directed at specific individuals using gathered information to personalize the emails and to make the attack more difficult to detect. **Whaling** is a type of spear-phishing attack that targets “big fish,” including high profile individuals or those with a great deal of authority or access. Then comes another variant of phishing which is **Clone phishing** involves a spoofed copy of a legitimate and previously delivered Email, with original attachments or hyperlinks replaced with more attractive versions, which is sent from a forged Email address therefore it appears to be from the original sender or another legitimate source. **Advance fee scams** are also there which requests the target to send money or bank details which can be misused through phishing techniques.

Common Baiting Tactics are also used to trap people and get their significant information like Notification from a help desk or system administrator asks you to take action to resolve an issue with your account (e.g., Email account has reached its storage limit), which often includes clicking on a link and providing the requested information. Advertisement for immediate weight loss, hair growth or fitness prowess, serves as a ploy to get one to click on a link that will infect a computer or mobile device with malware or viruses. Attachment labelled “invoice” or “shipping order” contains malware that can infect computer or mobile device if opened. It may contain what is known as “ransomware,” a type of malware that will delete all files unless a person pays a specified sum of money. It involves the use of notifications from what appears to be a credit card company indicating someone has made an unauthorized transaction on a persons account and if the link to log in to verify the transaction is clicked, then important information like username and password is collected by the scammer. A fake account on a social media site mimics a legitimate person, business or organization or organization linked with an online game, quiz or survey to collect information from personal accounts.

Punycode is a representation of Unicode with the limited ASCII character subset used for Internet hostnames is also explained. Using Punycode, hostnames containing Unicode characters are transcoded to a subset of ASCII consisting of letters, digits, and hyphens, which is called the Letter-Digit-Hyphen subset.

To detect a Phishing Scam, one can notice things like spelling errors (e.g., “pessward”), lack of punctuation or poor grammar, hyperlinked URL which can be different from the one displayed, or it is hidden, threatening language that calls for immediate action, requests for personal information, announcement indicating a prize or a lottery won or requests for donations etc.

Email Spoofing is also a technique used for phishing. In this fraudulent Email activity, the sender address and other parts of the Email header are altered to appear as though the e-mail originated from a different source.

An **Email header should be viewed** as a safeguard measure to detect phishing. To view the Email header in Rediffmail one should open an Email. Find and click “See Details”, then click “Show full headers” and to View, an Email header in Gmail one should open an Email and then find “More” (three vertical dots), choose “Show original”. Viewing an email header in Outlook involves opening an Email and then find “More actions” (three horizontal dots), choose “View message source” and viewing an Email header in Yahoo involves opening an Email and then find “More actions” (three horizontal dots), choose “View raw message.”

An **Email can be traced to its IP address** through header information but due to recent changes in the privacy policy knowing the exact IP address has become tedious. Some software tools can also be used to get header information or delivery information.

Some **Compliance and Mechanisms** can be incorporated into the mail system to strengthen security. Some such instances are the use of SPF, DKIM, DMARC etc.

Sender Policy Framework (SPF) is an Email authentication technique used to prevent spammers from sending messages on behalf of one domain. With SPF, an organization can publish details of authorized mail servers. SPF is a DNS text entry that shows a list of servers allowed to send mail for a specific domain. The domain owners/administrators are the only people allowed to add/

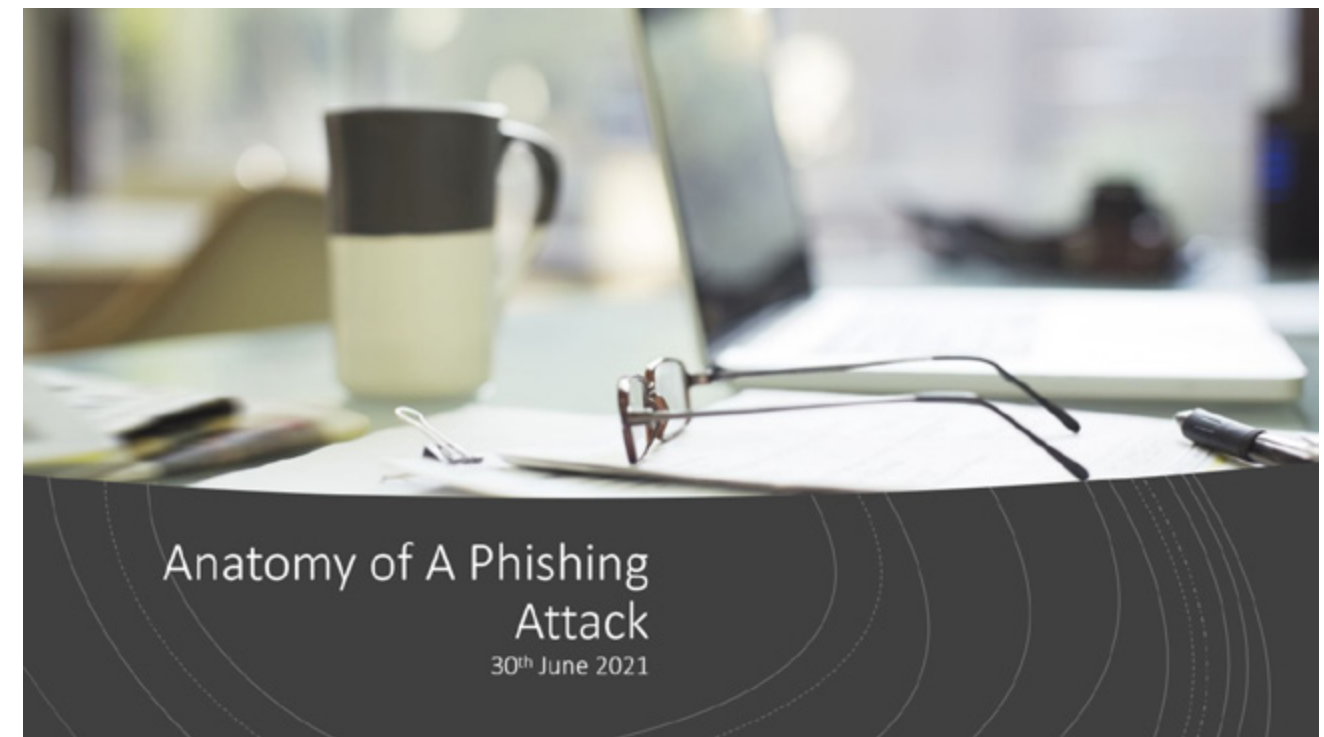


change the main domain zone. Hence SPF in a DNS entry can be considered a way to enforce the fact that the list is authoritative.

Domain Keys Identified Mail (DKIM) is an Email authentication technique that allows the receiver to check that an email was indeed sent and authorized by the owner of that domain. This authentication is done by giving the Email a digital signature. The recipients can know if the message has not been faked or altered in transit.

DMARC, which stands for “Domain-based Message Authentication, Reporting & Conformance”, is an email authentication, policy, and reporting protocol that is designed to detect and report Email spoofing. It builds on the widely deployed SPF and DKIM protocols, adding linkage to the author, domain name, published policies for recipient and handling of authentication failures, and reporting from receivers to senders, to improve and monitor the protection of the domain from fraudulent Emails. **BIMI** (Brand Indicators for Message Identification) and **SMIME** can also be used by organizations for further security to avoid such attacks.

The slides of his presentation are as follows: -

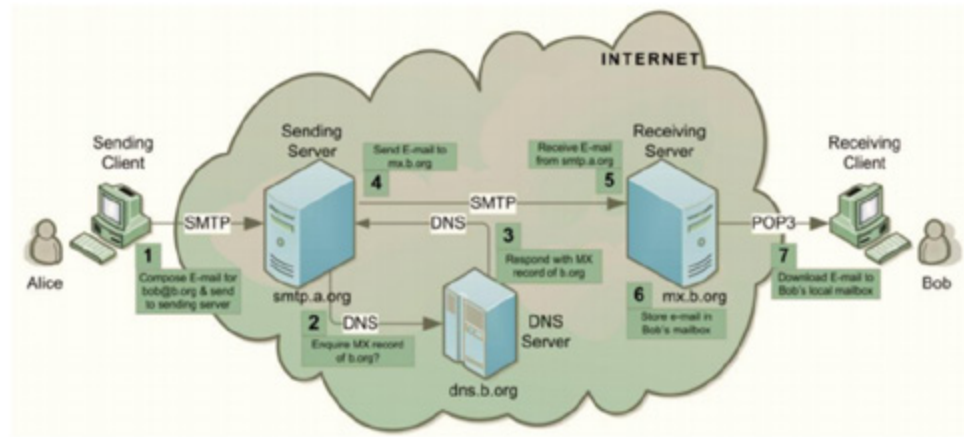


How Email Works





E-mail communication between a sender 'Alice' and recipient 'Bob'



Some statistics around cyberattacks involving email



- More than 90% of targeted cyberattacks used spear-phishing in the initial phase to gain entry to the organization's network
- In 2018, phishing URLs in the emails detected to be more than 269% than in the previous year of 2017.
- One-third of the data breaches that happened in 2018 involved phishing attacks.



Some statistics around cyberattacks involving email



- Maersk lost the business of about \$200 million to \$300 million because of NotPetya Ransomware received from an email.
- Business Email Compromise or CEO Fraud saw losses of about \$676 million
- COVID-19 related email attacks up by 667% and 18 million such emails were seen in just 1 week during April 2020.



Phishing

Phishing is a technique used by cybercriminals to send genuine-looking emails and make the user take actions. These actions can be replying with personal information or clicking the link in the email and doing some transactions etc.

- Take advantage of natural disasters, epidemics, pandemics, health scares, political elections or timely events
- Attackers are sending malicious emails under the pretext of local authorities that are in charge of dispensing government-funded COVID-19 support initiatives.

Common Baiting Tactics

- **Notification from a help desk or system administrator**
Asks you to take action to resolve an issue with your account (e.g., email account has reached its storage limit), which often includes clicking on a link and providing requested information.
- **Advertisement for immediate weight loss, hair growth or fitness prowess**
Serves as a ploy to get you to click on a link that will infect your computer or mobile device with malware or viruses.
- **Attachment labeled "invoice" or "shipping order"**
Contains malware that can infect your computer or mobile device if opened. May contain what is known as "ransomware," a type of malware that will delete all files unless you pay a specified sum of money.
- **Notification from what appears to be a credit card company**
Indicates someone has made an unauthorized transaction on your account. If you click the link to log in to verify the transaction, your username and password are collected by the scammer.
- **Fake account on a social media site**
Mimics a legitimate person, business or organization. May also appear in the form of an online game, quiz or survey designed to collect information from your account.

Types of Phishing

- Mass Phishing** – Mass, large-volume attack intended to reach as many people as possible
- Spear Phishing** – Targeted attack directed at specific individuals or companies using gathered information to personalize the message and make the scam more difficult to detect
- Whaling** – Type of spear phishing attack that targets "big fish," including high-profile individuals or those with a great deal of authority or access
- Clone Phishing** – Spoofed copy of a legitimate and previously delivered email, with original attachments or hyperlinks replaced with malicious versions, which is sent from a forged email address so it appears to come from the original sender or another legitimate source
- Advance-Fee Scam**: Requests the target to send money or bank account information to the cybercriminal

Punycode

Punycode is a representation of Unicode with the limited ASCII character subset used for Internet hostnames. Using Punycode, host names containing Unicode characters are transcoded to a subset of ASCII consisting of letters, digits, and hyphen, which is called the Letter-Digit-Hyphen subset.

Brand	What the user sees	The Punycode
IKEA	ikea.com	xn--iea-f6a.com
Lidl	lidl.com	xn--lid-xbb.com
Milka	milka.com	xn--mlka-lza.com
Milka	milka.de	xn--mlka-lza.de

Detect a Phishing Scam

- Spelling errors (e.g., "pessward"), lack of punctuation or poor grammar
- Hyperlinked URL differs from the one displayed, or it is hidden
- Threatening language that calls for immediate action
- Requests for personal information
- Announcement indicating you won a prize or lottery
- Requests for donations

Can You Spot All of the Errors in This Phishing Email?

1 Payment Declined -- Update Required Immediately!

2 Sense of urgency
Fear tactics

3 Imitating known brand
Fake email address

4 Impersonal

5 Urgency
Punctuation and grammar mistakes

6 Rollover shows malicious link

7 Scare tactics

8 Impersonal
Not real customer service

9 Copyright date is incorrect
Location is incorrect

ZIP file

Copyright © 2012 Apple Inc.
All rights reserved
3 Loop, Madisonville KY 42001

apple-invoice.zip Download

Can You Spot All of the Errors in This Phishing Email?

1 Payment Declined -- Update Required Immediately!

2 From: **ApplePay Support** <customer_support_ref_@apple.com>

3 Dear Apple User,

4 It has come to our attention that you're recent payment was declined. An update is required immediately..

To make this change, visit the support section at the link below.

5 <https://www.applepay.com/subscriptions/payment-update>
http://944.535.32/index/apple.html

6 **If you do not update your payment information in the next 24 hours, your account will be deactivated.**

7 Regards
ApplePay Support

8 Copyright © 2012 Apple Inc.
All rights reserved
3 Loop, Madisonville KY 42001

9 apple-invoice.zip Download

How to Spot a Malicious Landing Page

1 http://appel-pay.com

2 ApplePay

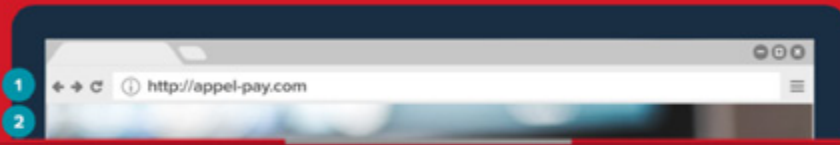
3 Apple ID

4 Password

Sign in

I forgot my Apple ID or password

How to Spot a Malicious Landing Page



- 1 Not a legitimate Apple website address
- 2 Missing navigation bar and footer
- 3 "Apple Pay" is misspelled
- 4 Apple ID homepage doesn't require password



Sample Phishing Email

Subject: EMAIL domaintech [redacted] VERSION UPGRADE

[redacted] <admin@mailbox.com>

Sent: Wed, 5 Aug 2020 20:04:57 GMT+0530

To: [redacted]

Show full headers | Mark as safe

Note: Please be careful while downloading attachments or clicking on links in Junk emails as they can be dangerous.

ATTENTION: This email is sent by an external sender. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Dear ,
Your email account currently needs the annual email version upgrade.

NB : Your account will soon be blocked from sending message if not Upgraded to the New Email version .
Please click on the below Server Link to complete the new email version upgrade

[GET VERSION 5.0.3](#)

Sample Phishing Email

Subject: This Is Little Harshan's Last Chance At Life, He Needs A Heart Surgery Urgently

Harshan <panel@realtredefined.co.in>

Sent: Wed, 29 Jul 2020 09:22:58 GMT+0530

To: [redacted]

Show full headers | Mark as safe | View blocked images

Note: Please be careful while downloading attachments or clicking on links in Junk emails as they can be dangerous.

ATTENTION: This email is sent by an external sender. Do not click links or open attachments unless you recognize the sender and know the content is safe.

This Is Little Harshan's Last Chance At Life, He Needs A Heart Surgery Urgently

"My baby's heart is failing," Hemlatha says, her grim face wet with tears. "The doctors say that his heart hasn't developed properly. I don't know what I did wrong that my child is suffering."

Right after baby Harshan was born, he started gasping for air. He couldn't get enough oxygen because of which his body started turning blue.

Sample Phishing Email

Your account has been suspended (Ref - 83783745690)

Yahoo/Inbox

service@paypal.com <of3vbxr2ktrjfn-hrkyhhsz...@paypal.com>
To: [redacted]@yahoo.com

Sat, Aug 1 at 5:47 PM



Dear Customer,

Your PayPal account has been temporarily restricted. We have found suspicious activity on credit cards linked to your PayPal account. You must confirm your identity to confirm that you own the credit card.

To maintain account security, please provide documents that confirm your identity.

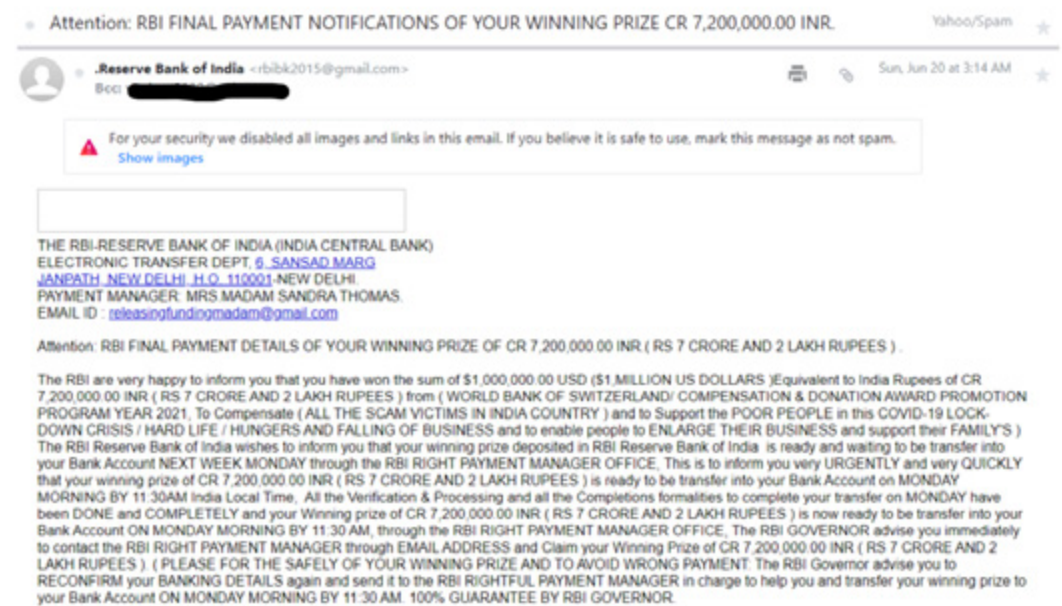
[Log in to PayPal](#)

After you complete the requested task, we will review the account and contact you about its status within 5 working days.

Thank you for your attention to this problem.



Sample Phishing Email



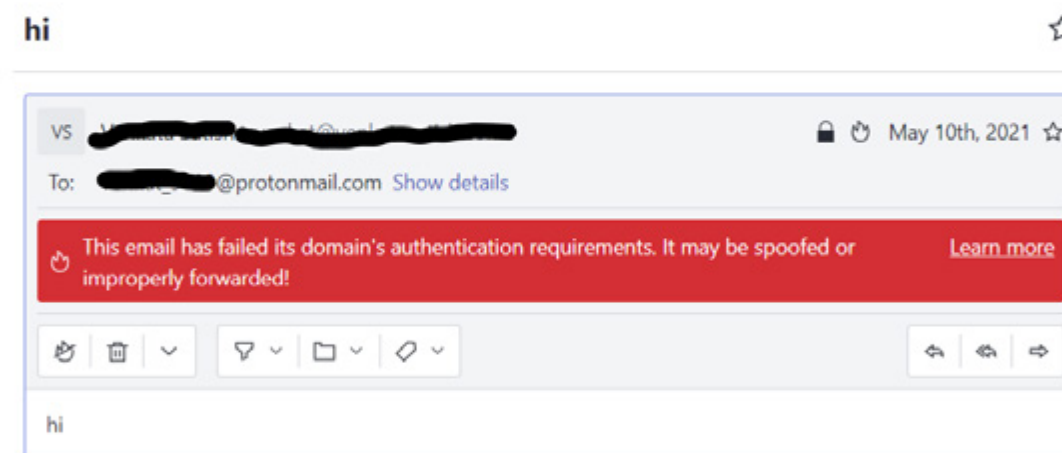
Email Spoofing

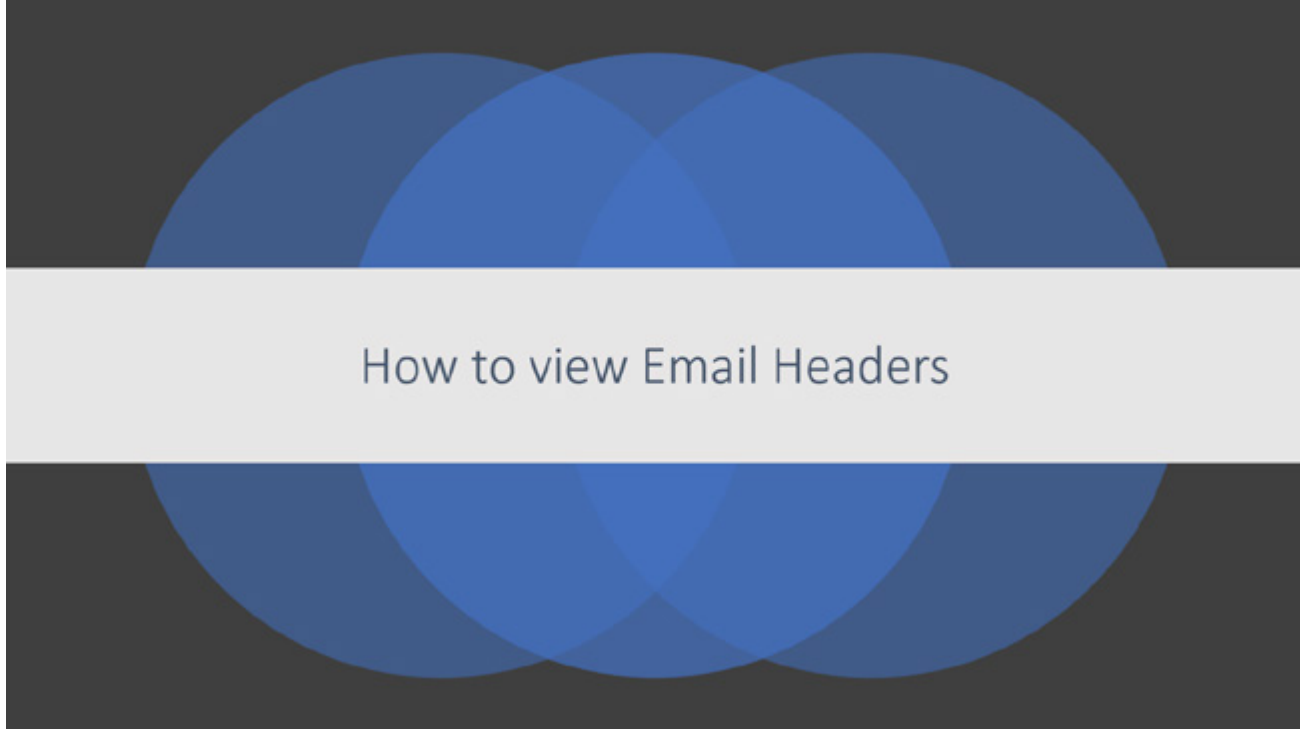
- **e-mail spoofing:** fraudulent e-mail activity in which the sender address and other parts of the e-mail header are altered to appear as though the e-mail originated from a different source

Sample COVID-19 themed phishing email



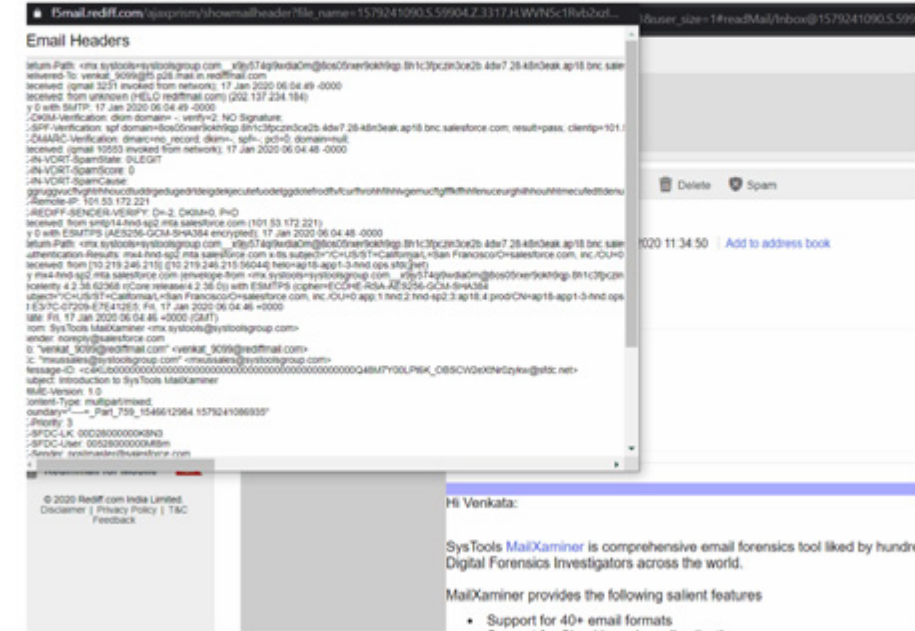
Sample Spoof Email





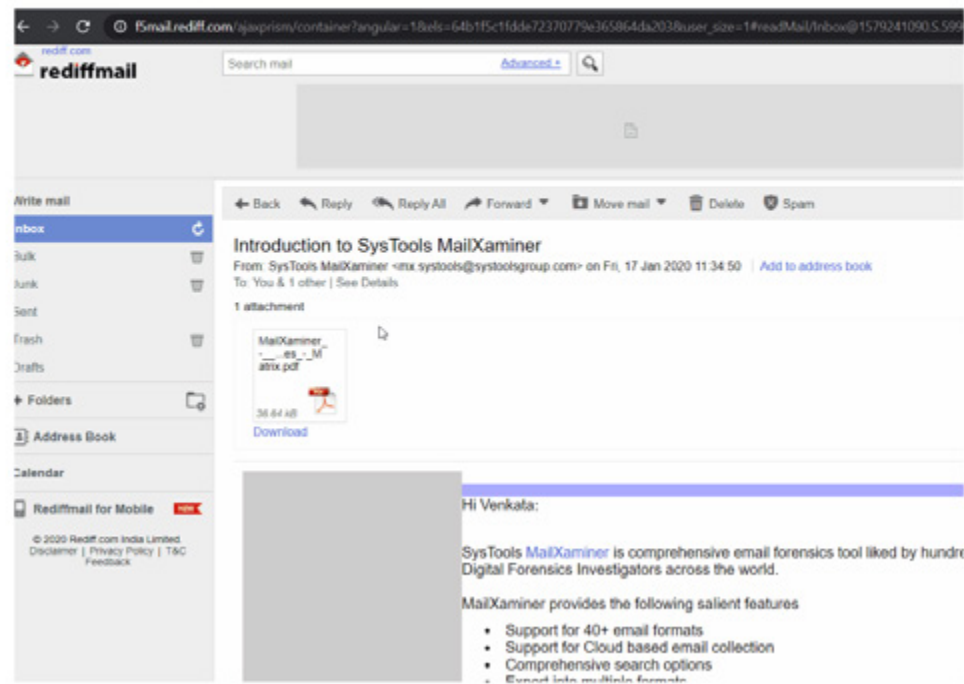
Viewing an email header in Rediffmail

Open an email. Find and click "See Details", then click "Show full headers"



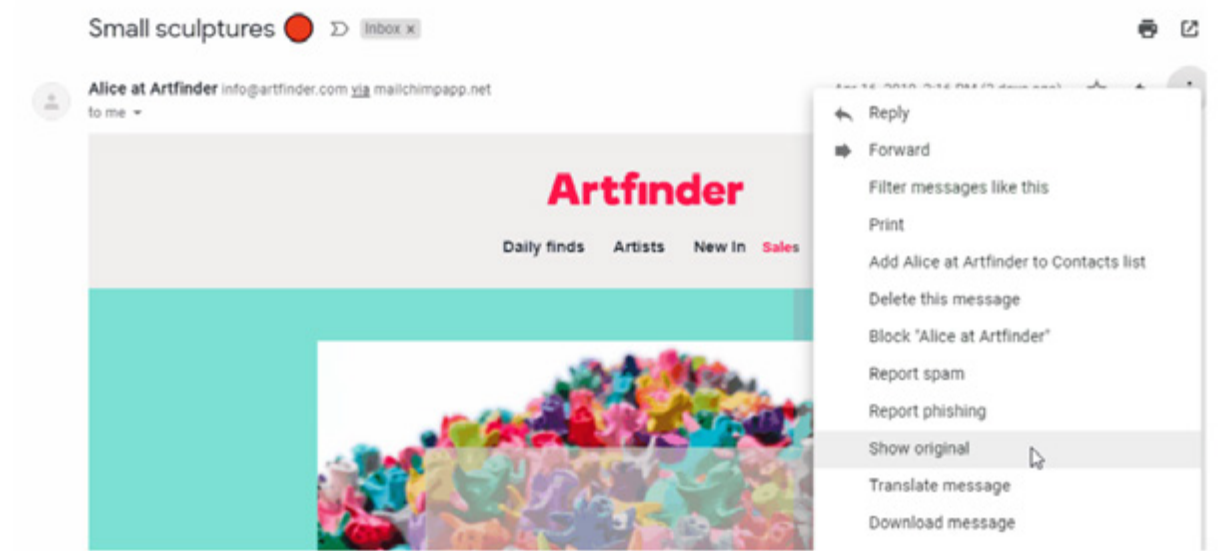
Viewing an email header in Rediffmail

Open an email. Find and click "See Details", then click "Show full headers"



Viewing an email header in Gmail

Open an email. Find "More" (three vertical dots), choose "Show original."



Viewing an email header in Gmail

Open an email. Find "More" (three vertical dots), choose "Show original."

Original Message

Message ID: <cab05aa04fc6aa9576d99dc3562c439adb2.20190416111249.5b2cd047c8.137e6b43@mail34.suw17.mcsv.net>
Created at: Tue, Apr 16, 2019 at 2:13 PM (Delivered after 182 seconds)
From: Alice at Artfinder <info@artfinder.com> Using MailChimp Mailer - **CID5b2cd047c862c439adb2**
To: roman1tkachev@gmail.com
Subject: Small sculptures
SPF: PASS with IP 198.2.181.34 [Learn more](#)
DKIM: 'PASS' with domain mailchimpapp.net [Learn more](#)

[Download Original](#)

[Copy to clipboard](#)

Viewing an email header in Outlook

Open an email. Find "More actions" (three horizontal dots), choose "View message source."

Message source

Received: from VE1EUR01HT137.eop-EUR01.prod.protection.outlook.com (2603:10a6:644:14) by DB6PR0402MB2870.eurprd04.prod.outlook.com with HTTPS via DB6PR01CA0073.EURPRD01.PROD.EXCHANGELABS.COM: Thu, 18 Apr 2019 08:31:28 +0000

Received: from VE1EUR01FT055.eop-EUR01.prod.protection.outlook.com (10.152.2.53) by VE1EUR01HT137.eop-EUR01.prod.protection.outlook.com (10.152.3.89) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384) id 15.20.1771.16: Thu, 18 Apr 2019 08:31:28 +0000

Authentication-Results: spf=pass (sender IP is 198.2.140.131) smtp.mailfrom=mail11.mcsignup.com; outlook.com: dkim=pass (signature was verified) header.d=deathtothestockphoto.com; outlook.com: dmarc=bestguesspass action=none header.from=deathtothestockphoto.com; Received-SPF: Pass (protection.outlook.com: domain of mail11.mcsignup.com designates 198.2.140.131 as permitted sender) receiver=protection.outlook.com; client-ip=198.2.140.131; hello=mail11.mcsignup.com;

Received: from mail11.mcsignup.com (198.2.140.131) by VE1EUR01FT055.mail.protection.outlook.com (10.152.3.104) with Microsoft SMTP Server id 15.20.1771.16 via Frontend Transport: Thu, 18 Apr 2019 08:31:27 +0000

Yacinine.Touhied@Extranet

Viewing an email header in Outlook

Open an email. Find "More actions" (three horizontal dots), choose "View message source."

Outlook interface showing the "More actions" menu for an email from "Death to The Stock Photo". The "View message source" option is highlighted in the menu.

Viewing an email header in Yahoo

Open an email. Find "More actions" (three horizontal dots), choose "View raw message."

Yahoo! email interface showing the "More actions" menu for an email from "Architectural Digest". The "View raw message" option is highlighted in the menu.



Viewing an email header in Yahoo

Open an email. Find "More actions" (three horizontal dots), choose "View raw message."

```
X-Apparently-To: romis_gomis@yahoo.com; Thu, 18 Apr 2019 09:06:46 +0000
Return-Path: cv-mmhkpd_f1hebdcmg_gakbdpjm_gakbbjhe_a@bounce.newsletters.archdigest.com
Received-SPF: pass (domain of bounce.newsletters.archdigest.com designates 74.112.65.117 as permitted sender)
X-YMail150: FRvIX5gMLDt_8YhN3R4zPLQ5vUFIzhd101EYDP34nI2085
i7Hgy265B6uIzsum5Fennb0hY1k3JdxcCjBhYQI4R5g_Qvnr6y_5Lbn6YY
RxdP1Vh7T_hfhH160167a9.q1653kd60vsvKxah6520ParL3VpHhVcZkFC
Yn3luqvRyScaR17uBh3FTT9YA3Ye2T7Jd8hYjVt_bvBd3H86PNI_HPH8cvf
0ur630x6d8e4Uu4HLGx36kyUsIoQp2SYbTeuIoLAGF1m1EVXIA70Lp4zoha
IuIHNA.od11w3jR70d47w0XmgahzYb3kx3RngK7xkjt2iq5_A2v8XA1qQf
Y6Fnk1AnocfKvg_550kzTgkX7.Y0tT3VvSP48nCh9Fozzi1Q_m00skaxZeYK
hhfSuc78oQ4u7DF75Ur6g0a_vQdZ9HO37Ev0hPhcFUBID70v9azcQ8u3Tq
kshToGUnAs1.h85bBZRuA0GL.Q.s32g4g02fPiHa619_d6_1ZI3QE5oDbwQ
u6UeInS1CUUZTr726oGLQ8hu3oZuz9K11ZfEncck0h3upcHX051hvbR1K
QoAIXImpePfXafh7Kfc4ivdgn3wCvq5QotJf_Op0ucasYgjiyeb3hpX7A1QYr
_SShrDEgv_VnJt4v1bV1UUr000wCw3mo_mptd0e31ZazYh7o8xAgRiJDoznT
vR7qeu33EL0VLc3_a5itnarYvFOQgr_hHECR0Vf6y0u0c2CSRquaefhixpt
ccrDux4HsImGh0g_NYZmqkHMGsHpp6j7Xfo7oZGR3bTuukdUmr803k4mZ5
FX.16fASAS5L8AigrUrI0IV15dQcs5kVw8000t0tAt1sofyEP.Z3zBgD4b9
n6pwVrhT5juYrp7uaAhuao_oh_hVR1ksr014Eov082z.9D.r04C_243H9
hi4yXia8_mLZgeL0vsl_1Kfm0ZV2Cduvkb86b0VhVhLnoQIN0PepIHIvOun
1fn57bjk.dn7kbSLjRRref_rnhH_r9Om3iJ.9jpcdUn1DvF0kAcefV2mkJ0Ze
Hu7tScUu4puHuh_T.z8Dci04VjipxLHsp9kqipAge1j1vAhrN1.3dHAY5
YuQ0zAD7YA6gzmcuHd6SA4IqR8zInHgJFD76GAN11bQ0jaq/KdIP88YvKk_
OEHVBUe1kcwT5fnL0nzv9fYKcN480p67wUBE3N4eoBLvd2ABETHa1jJhY5
TgVc2nHnFFfhmoBUECTevq5QeVOCAD=8jbyFXI8NwTsvJlXPKA1_vU1JUS
vJ5mCCf2jvnBRQ_yVh0XVEZXF0pv57c6kzu-
X-Originating-IP: [74.112.65.117]
Authentication-Results: mta4424.mail.ne1.yahoo.com
header.i@archdigest.messages2.com; header.s=spop1024; dkim=pass (ok)
Received: from 127.0.0.1 (EHO mail15694.archdigest.mkt6293.com) (74.112.65.117)
by mta4424.mail.ne1.yahoo.com with SMTPS; Thu, 18 Apr 2019 09:06:45 +0000
DKIM-Signature: v=1; a=rsa-sha1; c=relaxed/relaxed; s=spop1024; d=archdigest.messages2.com;
h=Date:From:Reply-To:To:Message-ID:Subject:MIME-Version:Content-Type:List-Unsubscribe; i=email@archdigest.messages2.com;
bh=U3aQqQ3v8mYASk8itIalIn70b+;
b=H6dnay21sha1k82SynIihuZVhalmd6nPsuEh1162AbR4Uho09dfqt4a3txaievHhHhB5pIA
```

Trace an Email

Trace Email (Header Analyzer)
Analyze the email headers and trace the email sender IP location and IP Whois easily.

Copy and paste the email message source below to trace the sender.

```
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
h=feedback-id: list-unsubscribe: list-unsubscribe-post: precedence
:mime-version: to: reply-to: from: subject: date: message-id
: domainkey-signature: dkim-signature;
bh=JQGFkxozhg8LWnG97eSM+1HXGRYAKaK+3zB4pWw=;
```

Email Source Ip Info	
Source IP Address	64.20.61.75
Source IP Hostname	apps.11x1.in
Country	United States
State	New Jersey
City	Secaucus
Zip Code	07094
Latitude	40.7861
Longitude	-74.0743
ISP	Interserver, Inc
Organization	Interserver, Inc
Threat Level	low



mxtoolbox.com/Public/Tools/EmailHeaders.aspx?huld=78fa005a-10ff-4b9b-9f18-a85e4d82c272

MxTOOLBOX

SuperTool | MX Lookup | Blacklists | DMARC | Diagnostics | Email Health | DNS Lookup | Analyze Headers

Header Analyzed
Email Subject: Hi

Delivery Information

- > DMARC Compliant
- > ✔ SPF Alignment
- > ✘ SPF Authenticated
- > ✘ DKIM Alignment
- > ✘ DKIM Authenticated

Relay Information

Received Delay:	8 seconds
-----------------	-----------

What does SPF ?

A kind of reverse MX ...

Allows the owner of a domain to specify which mail servers are allowed to send mail on behalf of the domain.

The domain owner publish a record in DNS specifying which mail servers are authorized to send mail for his domain.

When a mail server receives a message claiming to be from that domain, it looks up the spf record for that domain and it checks if it came through one of the allowed mail servers.

Sender Policy Framework (SPF)

Domain Keys Identified Mail (DKIM)

DKIM

- **Domainkeys** was first introduced by yahoo in a private agreement with paypal and ebay, then since 2007 a draft RFC
- **DKIM** took the main concepts from the yahoo proposal, incorporated some cisco ideas and appeared as an RFC in the same year, last version is RFC6376 Sep 2011

Domain-based Message Authentication, Reporting & Conformance (DMARC)



Why DMARC?

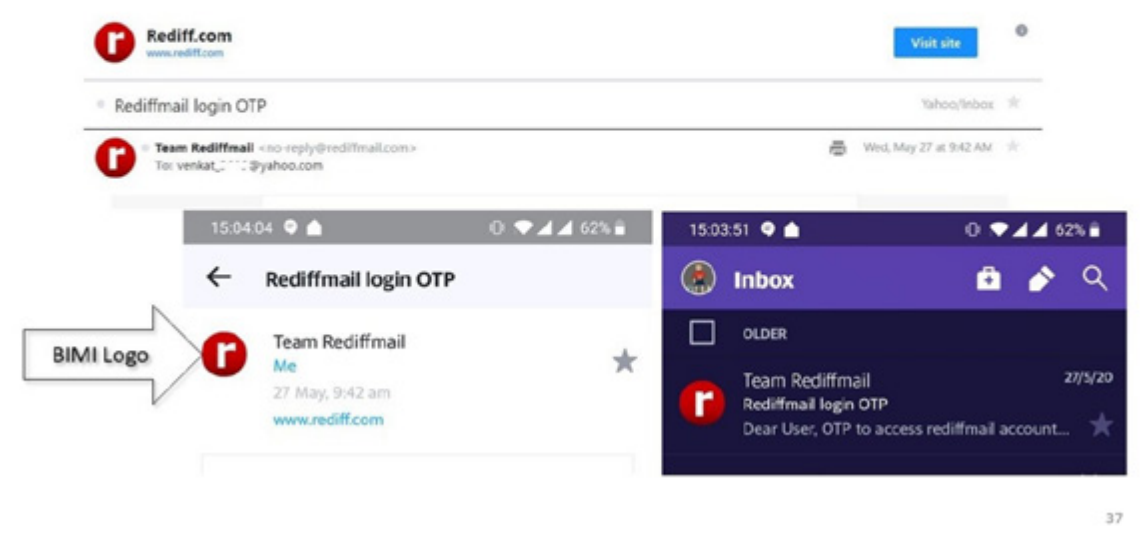
What is DMARC?

DMARC or Domain-based Message Authentication, Reporting and Conformance is

- an email-validation system designed to detect and prevent email spoofing
- It can also help combat phishing and thus protect your reputation
- a framework that works on top of Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM)

DMARC is not just for outbound emails but it is for inbound emails also

BIMI (Brand Indicators for Message Identification)

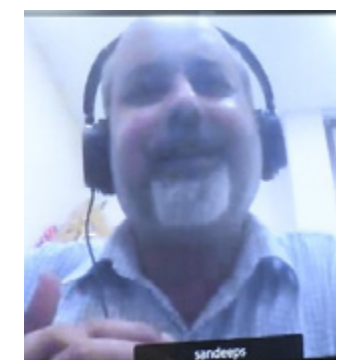


SMIME



SESSION III:

Cyber Security as a National Security Issue



(Dr. Sandeep Shukla)

Dr Sandeep Shukla started his talk on Cyber Security as a National Security Issue by introducing the difference between cyber crimes and cyber attacks. He explained that cyber crime may be defined as crimes that are taking place through the internet, computers and smart devices. Cyber crime may or may not be carried through cyber attacks. Whereas cyber attacks are online attacks performed to compromise confidentiality, integrity or availability of systems and information. Cyber-attacks may be used to commit cyber crime or create civil and administrative problems.

Dr Shukla further shed some light on IT Act and its role in bringing cyber criminals to justice. He further discussed the reporting of cyber crime to CERT-IN and NCIIPC.

Dr Shukla mentioned multiple examples of such Cyber Crimes such as:

- i. Jaamtara Gang and Financial fraud on unaware citizen
- ii. Impersonation on social media – use of simple passwords by users, not using 2-factor authentications
- iii. Honey Trapping on social media – completely a social engineering-based crime
- iv. Child Pornography creation and exchange
- v. Taking over someone's WhatsApp account – done through social engineering
- vi. The promise of employment on social media and then requesting the job seeker to pay fees
- vii. Deep fake videos, images, voice recordings
- viii. Ransomware attack on individuals for money
- ix. Blackmailing based on content leaked

He further discussed the strategies for fighting Cyber Crimes including, Cyber Forensic capability, Insider intelligence, Tracing IP addresses, Tracking cryptocurrency movement through blockchain analytics, AI/ML capabilities to detect deep fakes, Extensive information on mapping



IP addresses and their activities, Counter Hacking capabilities, Spreading awareness extensively. Cyber Attacks are done by exploiting vulnerabilities in the network, hardware, O/S, Firmware and Applications, which involves, Cyber Attacks that can breach confidentiality (Privacy), Breach integrity (change data – false data injection), reach availability (denial of service). Cyber Attacks can also be used in cybercrime, and Cyber Attacks can also damage systems including IT Systems and Industrial Control Systems.

Dr Shukla discussed many incidents related to Cyber Attacks on IT Systems and Industrial Control Systems, including:

- Targeting the Indian Power Sector
- Cyber Attack causing the Mumbai Power Outrage
- Cyber Attacks on Global Power Grids
- Track Malware Attack on India's largest Nuclear Plant
- Attacks on Nuclear Fuel Enrichment Program

Dr Shukla also discussed the actors who are Attacking our Cyber Space. He mentioned the role of Nation-State Actors, Terror outfits, Criminal Gangs (esp. Ransomware gangs), Hobby Hackers, Script kiddies etc. in attacking our Cyber Space. Some examples of State-Sponsored Threat Actors are:

- Target Sector – high-tech sectors, IP stealing
 - Spear-phishing to drop rootkits, keyloggers, credential stealers
- Target Sector – Engineering and Defense
 - Poses as prominent individual and spear-phish
- Target Sector – telecom, travel industry, IT firms, High-Tech Industry
 - Spear-phishing and penetrating vulnerable web servers
- Target Sector – Financial Institutions
 - Custom malware families – backdoors, tunnelers, data miners, destructive malware, ransomware
- Target Sector – various industry verticals in South Korea, Japan, Vietnam, Middle East
 - Word Processor, Adobe Flash, Web site compromise etc
- Target Sector – IT, High-Tech Industries, Governments, R&D organizations, Education
 - Spear-Phishing

He discussed our Cyber Security Philosophy, mentioning about Perimeter Security is not enough, which includes, Firewall misconfiguration and breaches, Authentication bypass, Insider Threat, Social Engineering, Phishing, Smishing, Vulnerabilities in Commercial Perimeter Defence etc. Moreover, he pointed out that Resilient Design is a must, that involves:



- Continuous Penetration Testing, Patching and Testing Cycles
- Threat Intelligence-based monitoring and IDS Technologies
- Fast Detection, Containment and Islanding mechanism
- Development of robust protocols and Software solutions
- Development of effective and useful SIEM Solutions
- Awareness and vigilance training

He further discussed the NIST Cyber Security Framework that includes identifying, protect, detect, respond and recover. He briefly discussed the C3i Center Research and Development for Securing Power Grid at functioning in IIT Kanpur. The centre involves various labs and activities like testbeds, National Vulnerability Database, design and development of Intrusion Detection System, Malware and Botnet Detection, Malware Analysis, Siemens PLC honeypot, Anomaly Detection in Physical Dynamics under attack.

Finally, Dr Shukla summarized his talk including the following key points: Critical Infrastructures (Power Grid, Water/Sewage Plants, Railways, Air Traffic Control, Traffic Systems) are ripe targets for APTs and State Actors. If drastic actions are not taken fast – we might be sitting on a ticking time bomb, and C3i Center and C3i Hub are engaged in doing their part but more research, development, courses, awareness programs and systematic efforts are required.



Cyber Security as a National Security Issue

Sandeep K. Shukla

Interdisciplinary Center for Cyber Security and Cyber Defense of Critical Infrastructure
IIT Kanpur



Cyber Crime vs Cyber Attacks

- ▶ **Cyber Crime**
 - ▶ Crime committed with cyber means
 - ▶ Through Internet
 - ▶ Through Computers, Smart Devices
 - ▶ May or may not be carried out via cyber attacks
- ▶ **Cyber Attack**
 - ▶ Attack to compromise confidentiality, Integrity or Availability of Systems and Information
 - ▶ Attack against Computers, Devices, Networks
 - ▶ May be used to commit cyber crime or create problems

IT Act and Cyber Crime

- ▶ The current IT Act conflates the concept of cyber attack and cyber crime
- ▶ IT Act defines the following as punishable
 - ▶ Act of accessing computers/information systems without permission of the owner
 - ▶ Act of downloading, copying or accessing without permission
 - ▶ Denying access to lawful user of a computer system
 - ▶ Impersonating through unlawfully using someone's password/electronic signature
 - ▶ Publicizing someone else's electronic signature information and identity theft
 - ▶ Putting virus or malicious programs on someone's computing system
 - ▶ Leaking confidential information
 - ▶ Failure to protect adequate measure to protect confidential data
- ▶ Quantum of punishment more for threatening national security, any of the above in case of CII
- ▶ Reporting to CERT-IN and NCIIPC
- ▶ Certain Civil Liabilities for Companies

Examples of Cyber Crimes

- ▶ Jaamtara Gang and Financial fraud on unaware citizen
- ▶ Impersonation on social media - use of simple passwords by users, not using 2 factor authentications
- ▶ Honey Trapping on social media - completely a social engineering-based crime
- ▶ Child Pornography creation and exchange
- ▶ Taking over someone's whatsapp account - done through social engineering
- ▶ Promise of employment on social media and then requesting the job seeker to pay fees
- ▶ Deep fake videos, images, voice recordings
- ▶ Ransomware attack on individuals for money
- ▶ Blackmailing based on content leaked



Fighting Cyber Crimes

- ▶ Cyber Forensic capability
- ▶ Insider intelligence
- ▶ Tracing IP addresses
- ▶ Tracking cryptocurrency movement through blockchain analytics
- ▶ AI/ML capabilities to detect deep fakes
- ▶ Extensive information on mapping IP addresses and their activities
- ▶ Counter Hacking capabilities
- ▶ Spreading awareness extensively



Cyber Attacks

- ▶ Cyber Attacks are done by exploiting vulnerabilities in network, hardware, O/S, Firmware and Applications
 - ▶ Cyber Attacks can breach confidentiality (Privacy)
 - ▶ Breach integrity (change data - false data injection)
 - ▶ Breach availability (denial of service)
- ▶ Cyber Attacks can be used in cyber crime
- ▶ Cyber Attacks can also damage systems
 - ▶ IT Systems
 - ▶ Industrial Control Systems

China-linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions

FEBRUARY 28, 2021 • INSIKT GROUP®

CHINA

Insikt Group®

Global Power Grids Are Becoming Increasingly Vulnerable to Cyber Attacks

March 4, 2021



Email This | Subscribe to Newsletter





Suspected Pakistani Actor Compromises Indian Power Company With New ReverseRat

by Black Lotus Labs Posted On June 22, 2021



Hack attack causes 'massive damage' at steel works

22 December 2014



The Real Story of Stuxnet

How Kaspersky Lab tracked down the malware that stymied Iran's nuclear-fuel enrichment program

By David Kushner

Computer cables snake across the floor. Cryptic flowcharts are scrawled



Saudi Aramco sees increase in attempted cyber attacks

Mervin Rashid 3 MIN READ

RIYADH (Reuters) - Saudi Aramco has seen an increase in attempted cyber attacks since the final quarter of 2019, which the company has so far successfully countered, the state oil giant's chief information security officer



Threat Research Blog

Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor

December 13, 2020 | by FireEye

FIREEYE | EVASION | SUPPLY CHAIN

Florida Cyber Attack Raises Alarm Over Security of Water Treatment Plants

By Tamara Lush, Alan Suderman and Frank Bajak | February 11, 2021

Email This | Subscribe to Newsletter



Article

1 Comment

A hacker's botched [attempt to poison the water supply](#) of a small Florida city is raising alarm about just how vulnerable the public water systems may be to attack...



Colonial hack: How did cyber-attackers shut off pipeline?

By Joe Tilly

Cyber reporter

10 May



India targeted through cyber intrusions by RedFoxtrot linked to Chinese military

NS - Last Updated: Jun 17, 2021, 03:44 PM IST

SHARE | FONT SIZE | DATE

Synopsis

Active since 2014, RedFoxtrot predominantly targets aerospace and defense, government, telecommunications, mining, and research organizations in Afghanistan, India, Kazakhstan, Kyrgyzstan, Pakistan, Tajikistan, and Uzbekistan, aligning with the operational remit of PLA Unit 69010.





Who are Attacking our Cyber Space?

- ▶ Nation State Actors
- ▶ Terror outfits
- ▶ Criminal Gangs (esp. Ransomware gangs)
- ▶ Hobby Hackers
- ▶ Script kiddies

More Examples of threat actors

- ▶ APT 38 - attributed to North Korea
 - ▶ Target Sector - Financial Institutions
 - ▶ Custom malware families - backdoors, tunnelers, dataminers, destructive malware, ransomware
 - ▶ Similar to Lazarus group (also attributed to North Korea)
- ▶ APT 37 - attributed to North Korea
 - ▶ Target Sector - various industry verticals in South Korea, Japan, Vietnam, Middle East
 - ▶ Hangul Word Processor, Adobe Flash, Web site compromise etc
- ▶ APT 1 - attributed to Unit 61398 China's PLA
 - ▶ Target Sector - IT, High-Tech Industries, Governments, R&D organizations, Education
 - ▶ Spear-Phishing

Source: FireEye

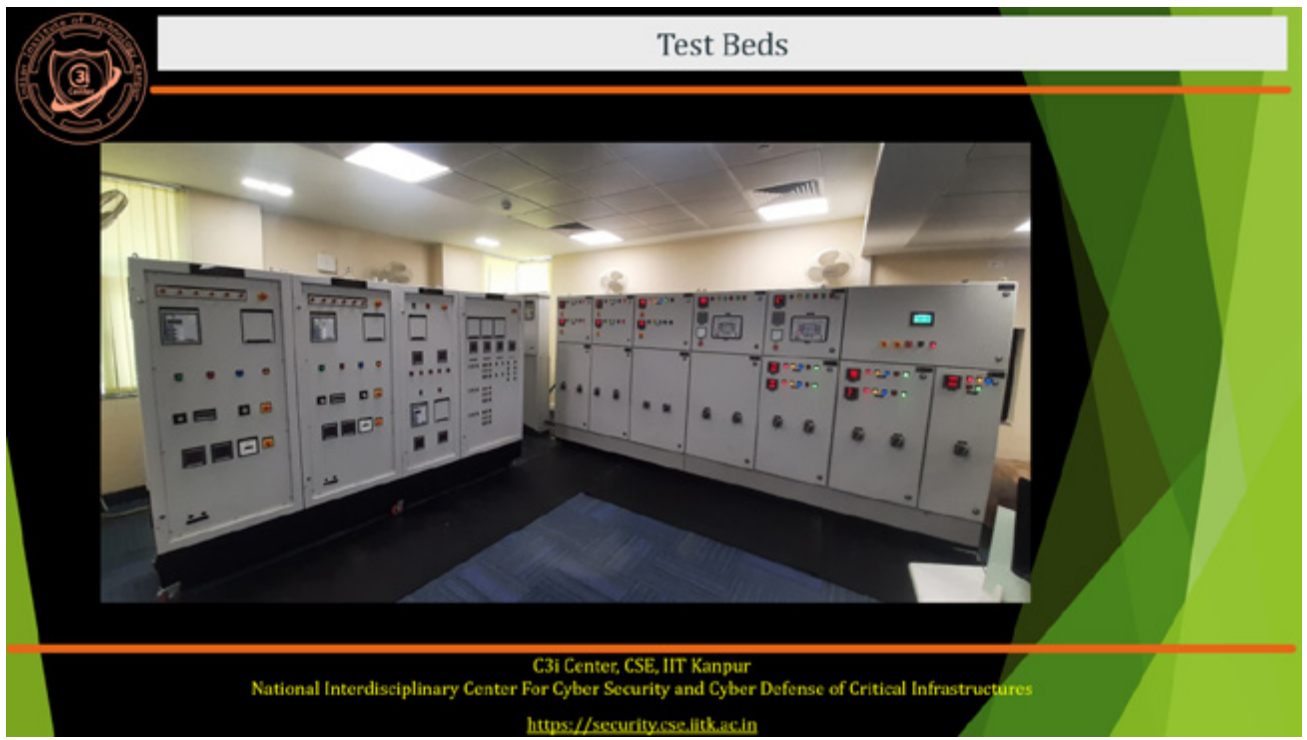
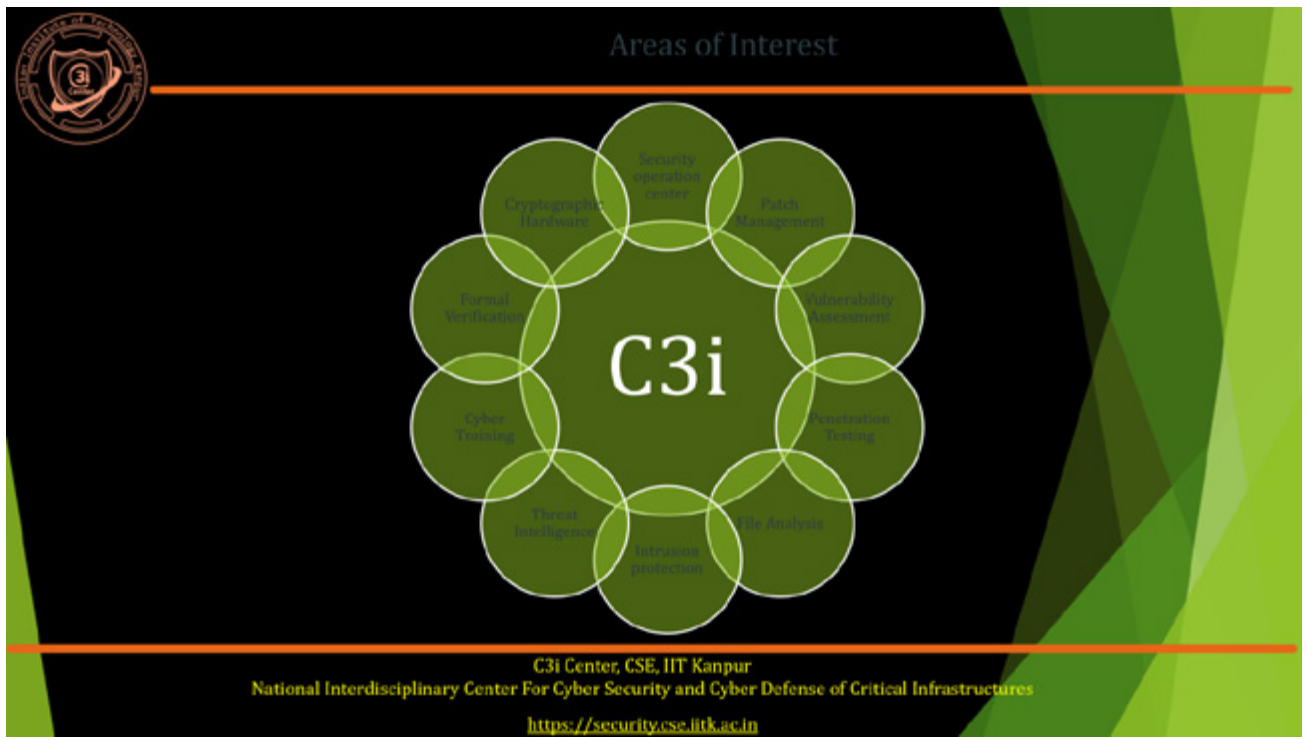
Examples of State Sponsored Threat Actors

- ▶ APT 41 - attributed to China
 - ▶ Target Sector - high-tech sectors, IP stealing
 - ▶ Spear-phishing to drop rootkits, keyloggers, credential stealers
- ▶ APT 40 - attributed to China
 - ▶ Target Sector - Engineering and Defense
 - ▶ Poses as prominent individual and spear-phish
- ▶ APT 39 - attributed to Iran
 - ▶ Target Sector - telecom, travel industry, IT firms, High-Tech Industry
 - ▶ Spear-phishing and penetrating vulnerable webservers

Source: FireEye


Our Cyber Security Philosophy

- ▶ Perimeter Security is not enough
 - ▶ Firewall misconfiguration and breach
 - ▶ Authentication bypass
 - ▶ Insider Threat
 - ▶ Social Engineering
 - ▶ Phishing, Smishing
 - ▶ Vulnerabilities in Commercial Perimeter Defence
- ▶ Resilient Design is a must
 - ▶ Continuous Penetration Testing, Patching and Testing Cycles
 - ▶ Threat Intelligence based monitoring and IDS Technologies
 - ▶ Fast Detection, Containment and Islanding mechanism
 - ▶ Development of robust protocols and Software solutions
 - ▶ Development of effective and useful SIEM Solutions
 - ▶ Awareness and vigilance training






Test Beds




C3i Center, CSE, IIT Kanpur
National Interdisciplinary Center For Cyber Security and Cyber Defense of Critical Infrastructures
<https://security.cse.iitk.ac.in>

Test Beds




C3i Center, CSE, IIT Kanpur
National Interdisciplinary Center For Cyber Security and Cyber Defense of Critical Infrastructures
<https://security.cse.iitk.ac.in>

Test Beds




C3i Center, CSE, IIT Kanpur
National Interdisciplinary Center For Cyber Security and Cyber Defense of Critical Infrastructures
<https://security.cse.iitk.ac.in>

Test Beds



C3i Center, CSE, IIT Kanpur
National Interdisciplinary Center For Cyber Security and Cyber Defense of Critical Infrastructures
<https://security.cse.iitk.ac.in>

Test Beds



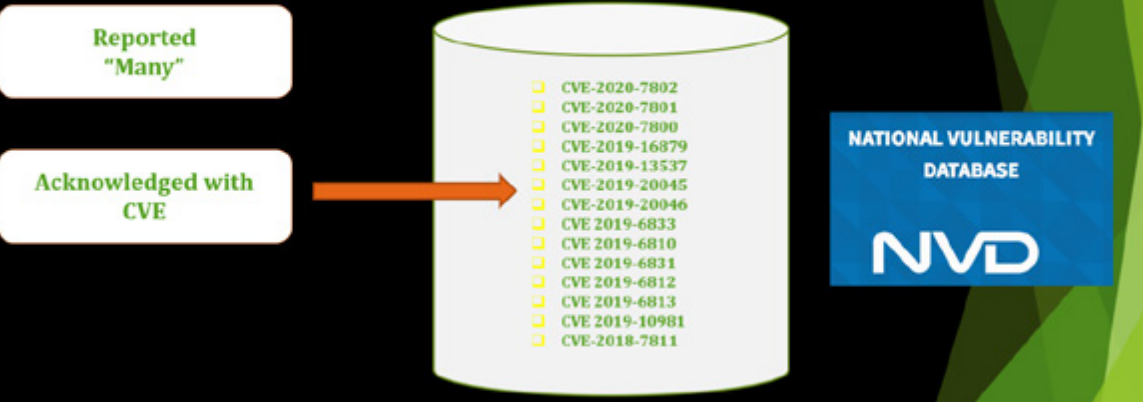
C3i Center, CSE, IIT Kanpur
National Interdisciplinary Center For Cyber Security and Cyber Defense of Critical Infrastructures
<https://security.cse.iitk.ac.in>

VAPT

VAPT • Tools and techniques for vulnerability detection

Reported "Many"

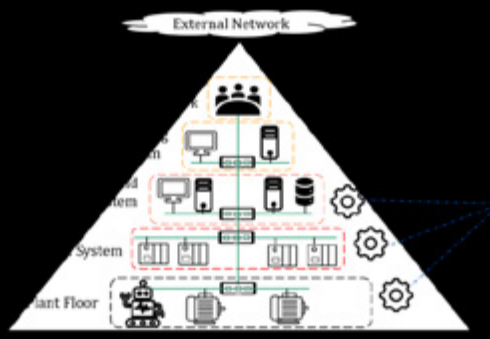
Acknowledged with CVE



NATIONAL VULNERABILITY DATABASE
NVD

- ☐ CVE-2020-7802
- ☐ CVE-2020-7801
- ☐ CVE-2020-7800
- ☐ CVE-2019-16879
- ☐ CVE-2019-13537
- ☐ CVE-2019-20045
- ☐ CVE-2019-20046
- ☐ CVE-2019-6833
- ☐ CVE 2019-6810
- ☐ CVE 2019-6831
- ☐ CVE 2019-6812
- ☐ CVE 2019-6813
- ☐ CVE 2019-10981
- ☐ CVE-2018-7811

C3i Center, CSE, IIT Kanpur
National Interdisciplinary Center For Cyber Security and Cyber Defense of Critical Infrastructures
<https://security.cse.iitk.ac.in>

External Network

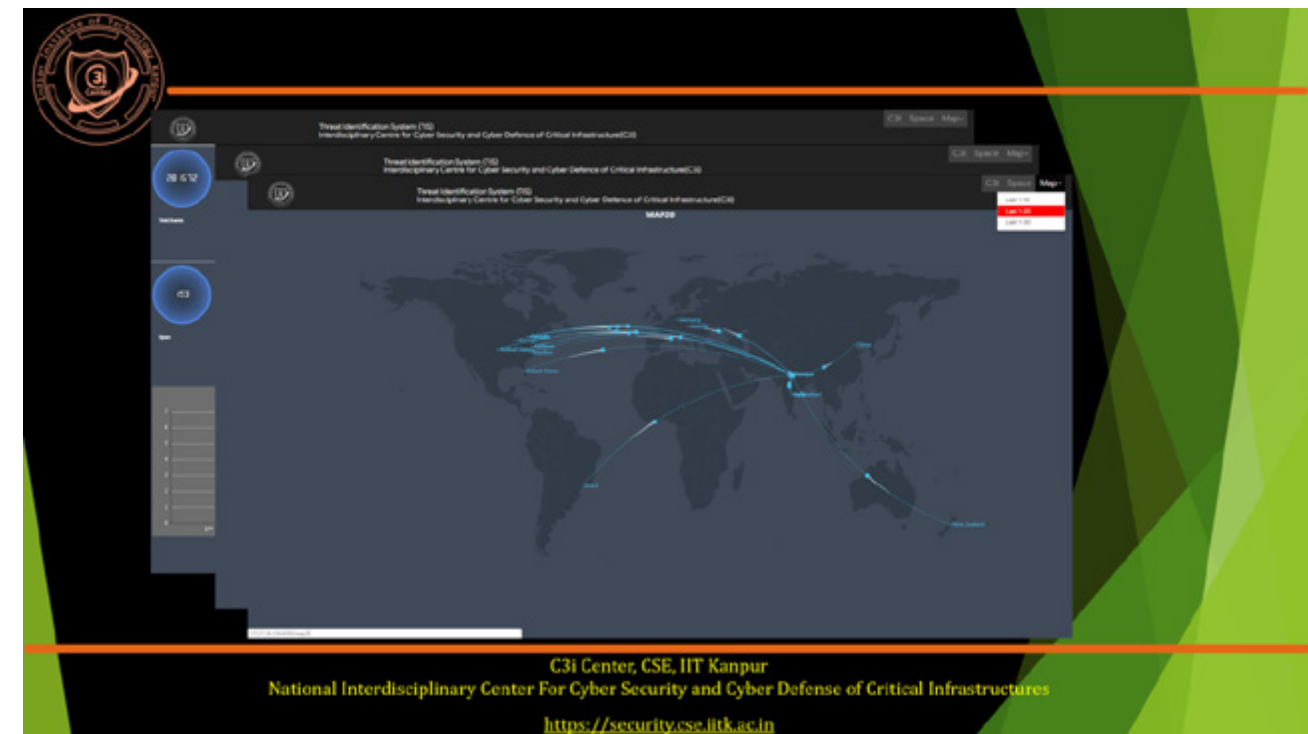
System

Smart Floor

Design and development of Intrusion Detection System

- ☐ Host
- ☐ Network
- ☐ Physical Dynamics

C3i Center, CSE, IIT Kanpur
National Interdisciplinary Center For Cyber Security and Cyber Defense of Critical Infrastructures
<https://security.cse.iitk.ac.in>



Malware and Botnet Detection

- P2P Botnet Detection
- Malware Detection and Classification
- Anomaly Detection in Physical Dynamics

```

mallab@mallab-BM1AF-BP1AF-BM6AF: ~
File Edit View Search Terminal Help
192.168.1.2      P2P_host detected      P2P_BOT detected
10.0.2.15      Non_P2P_Host Detected
172.27.22.206  P2P_host detected      P2P_BOT detected
172.27.28.106 Non_P2P_Host Detected
192.168.6.2    Non_P2P_Host Detected
172.27.22.206 P2P_host detected      P2P_BOT detected
192.168.4.2    P2P_host detected      P2P_BOT detected
172.27.28.106 Non_P2P_Host Detected
192.168.2.2    P2P_host detected      P2P_BOT detected
192.168.2.2    P2P_host detected      P2P_BOT detected

```

Malware Analysis

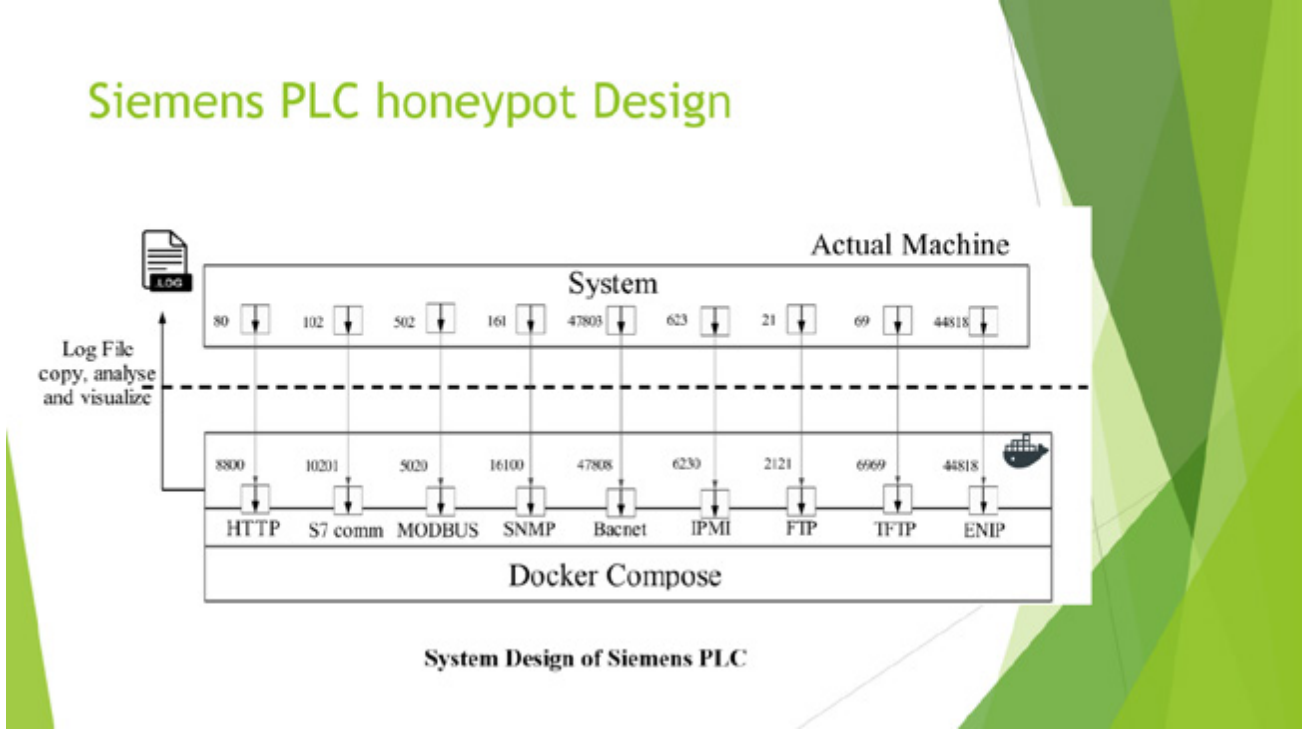
22,50,000+

Malicious File

- Image representation
- Evading API call sequences
- Early stage behaviour classification
- Memory Forensics
- Android Malware classification

- Detection and Classification Tool Development
 - Platform: Windows / Linux / Android
 - Extension: PDF, JPG, docx...

C3i Center, CSE, IIT Kanpur
National Interdisciplinary Center For Cyber Security and Cyber Defense of Critical Infrastructures
<https://security.cse.iitk.ac.in>



An IDS for PLC

C3i CENTER IIT KANPUR
Thu Sep 12 2019 - 11:14:35 AM
OPERATOR crack-PCtrack

PERMISSIVE CHECK C3

VICTIM 220.00

MODE REMOTE MODE

VOLTAGE 216.17

FREQUENCY 49.99

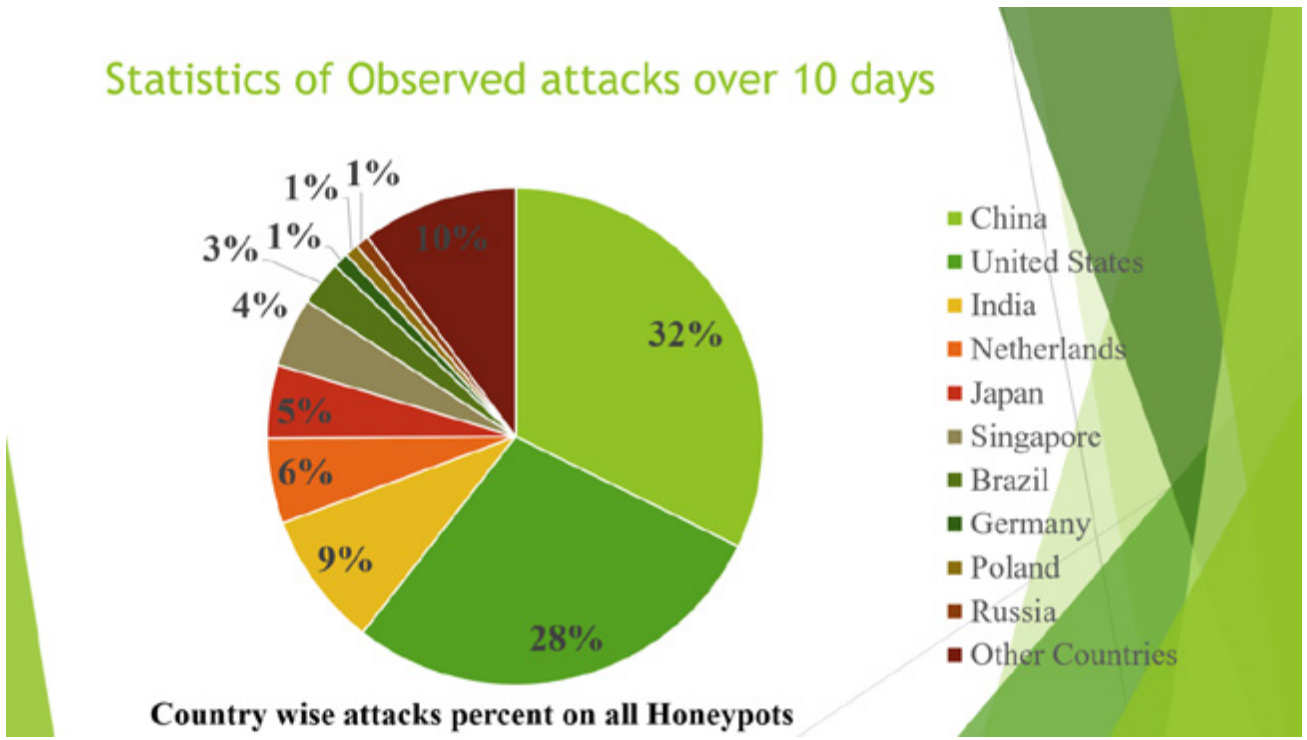
CURRENT 0.00

AUTO

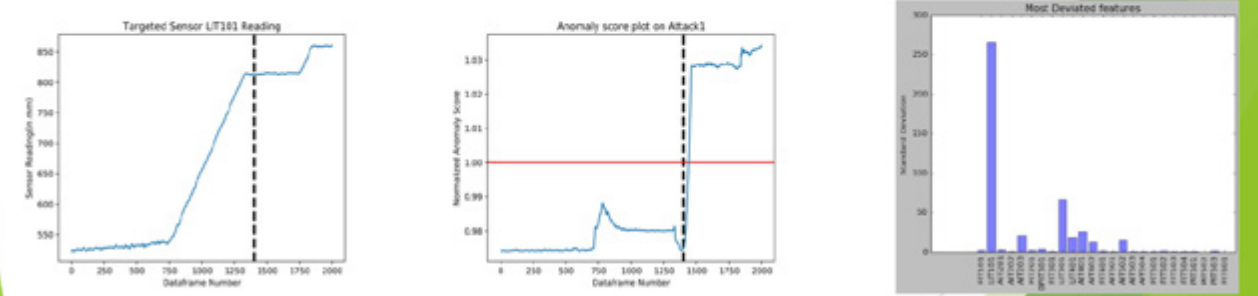
MANUAL

INTRUSION DETECTION					
Auto Mode	Manual Mode	START CMD (PC)	STOP CMD (PC)	START CMD (AUTO)	STOP CMD (AUTO)
OVER VOLTAGE (STATUS)	UNDER VOLTAGE (STATUS)	OVER CURRENT INST (STATUS)	OVER CURRENT TD (STATUS)	OVER FREQ (STATUS)	UNDER FREQ (STATUS)
OVER CURRENT INST (SET POINT)	OVER CURRENT TD (SET POINT)	OVER VOLTAGE (SET POINT)	UNDER VOLTAGE (SET POINT)	OVER FREQ (SET POINT)	UNDER FREQ (SET POINT)

SET POINTS					
Minimum Freq	Maximum Freq	Minimum Voltage	Maximum Voltage	Maximum Load TD	Maximum Load Inst
49.00	51.00	180.00	240.00	1.75	1.70

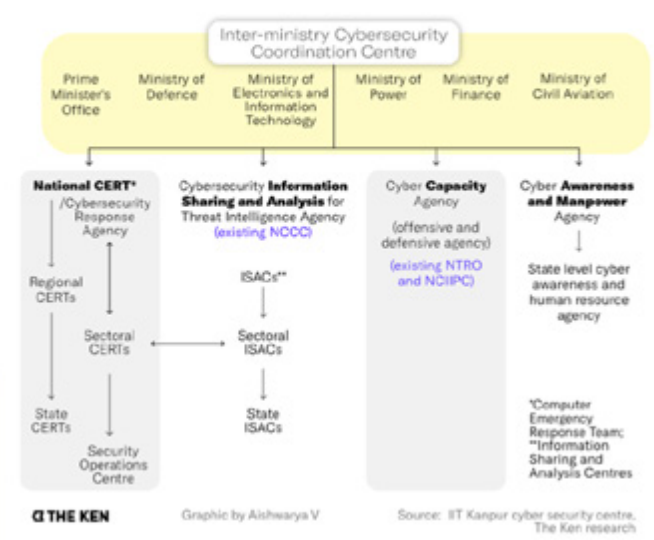


Anomaly Detection in Physical Dynamics under attack



Straight from the shoulder

A streamlined cybersecurity strategy would have a strong central agency as an anchor, with a set of institutions downstream that execute and enforce



Our Proposed Cyber Security Governance Structure

Too many cooks

Various agencies have the charter for cyber security but they are all disjointed with no clear delineation of roles and responsibilities



India's Cyber Security Governance Structure

Final Words

- ▶ Critical Infrastructures (Power Grid, Water/Sewage Plants, Railways, Air Traffic Control, Traffic Systems) are ripe targets for APTs and State Actors
- ▶ Absence of a regulation for Cyber Security Control and lack of funds
- ▶ Lack of a proper cyber security governance structure
- ▶ Lack of a federated cyber security protection, monitoring and response structure
- ▶ **Lack of Manpower and Awareness**
- ▶ Supply chain risk
- ▶ Lack of push from the cyber security leadership
- ▶ If drastic actions are not taken fast - we might be sitting on a ticking time bomb -
- ▶ C3i Center and C3i Hub is engaged in doing our part but more research, development, courses, awareness programs are required



CONCLUDING REMARKS AND VOTE OF THANKS

In the end, Sh. B. S. Jaiswal, DIG, (Mod), BPR&D proposed a Vote of Thanks to the Chair, Speakers and overwhelming participation of more than 400 from State/UTs Police and CAPFs/CPOs. He mentioned that the knowledge shared by respected experts/speakers on the various aspects of cyber security, cyber crime prevention and cyber crime investigation has greatly benefited all the participants in the creation of new ideas and stimulation to be carried forward and adapted to create new dimensions of enhancement in their day to day practices to deal with the Cyber Security Challenges to combat cyber crime.

The Organizing Team for the webinar:

1. Sh. B. S. Jaiswal, DIG (Mod)
2. Dr Manjunath M Gosal, SSO (T)
3. Dr Sarabjit Kaur, NCR&IC
4. Sh. Farhan Sumbul, NCR&IC
5. Sh. Pankaj Choudhary, NCR&IC
6. Sh. Gaurav Chaurasia, NCR&IC
7. Sh. Malladi Krishna, NCR&IC
8. Sh. Amit Giri, NCR&IC
9. Sh. Rushikesh Aghav, NCR&IC


 officialBPRDIndia


 BPRDIndia

 Bureau of Police Research & Development India

 bprdIndia

 www.bprd.nic.in

 Cyberdost

 www.cybercrime.gov.in



NATIONAL CYBER CRIME RESEARCH & INNOVATION CENTRE (NCR&IC)
BUREAU OF POLICE RESEARCH AND DEVELOPMENT

Ministry of Home Affairs, Government of India
NH-8, Mahipalpur, New Delhi-110037