ISACA®

Bangalore Chapter

INFOCITY AUDITOR

ISACA Bangalore Chapter-News Letter

Q1 – 2023 ISSUE

ISACA
Bangalore Chapter

Nodesec

GTB Technologies
Data Security that Works™

GTB ADVANCED DLP

Control,Protect,Discover,Classify & Audit.

- Data Classification
- Network DLP
- Endpoint DLP
- Data Discovery
- Compliance & Regulatory Data Protection
- Intellectual Property Data Protection

Free Demo

- Fully Managed service (MSSP) or Hybrid MSP
- Annual options
- On-premises or in the cloud (AWS, Azure, Rackspace, and the like)
- GTB Hosting options available

www.nodesectech.com

www.gttb.com

+91-9748200550

FORTINET | savex TECHNOLOGIES

Security-Driven Networking, everywhere you need it.

Protect the possibilities with Secure SD-WAN.

For details contact:
india_marketing@fortinet.com
www.fortinet.com

CONTENT

04

Articles

05

Crossword

06

Support from ISACA
Bangalore Chapter

FROM THE DESK OF THE PRESIDENT

Dear Members,

Greetings of the day to you !!!

Many thanks for the renewal of your membership and certification(s) for 2023; we are sure that all of you are getting continuous benefits and support from ISACA HQ and our chapter.

Change is a concept that is particularly pertinent to cybersecurity, where technological innovation and evolving cyber-attack techniques mean industry professionals constantly need to adapt their practices. The third generation of an unsupervised language model developed by AI, Chat GPT-3, is already a game changer, capable of offering responses that are so convincing that they are able to trick humans, and this is one of the most highly discussed subjects in the internet space. Cybersecurity professionals will witness more radical changes that are going to come due to this unsupervised language model.

Coming back to our regular update on chapter activities, four CPE sessions were delivered as part of CPE and one CPE was delivered during the morning session, which was well received by all members. CISM and CRISC batching were completed in February 2023. A new CISA batch started with more than 15 members. Based on the demand, CDPSE classes have been scheduled, and we would request all members take advantage of this opportunity and share these details with their friends and colleagues.

As part of the SheLeadsTech 2023 program, an in-person event with leading women speakers from various industries is planned as part of International Women's Day on March 11, 2023, at Chancery University. This is a full-day program with 6CPE credit, and this is the first time the Bangalore chapter is organizing a full-day program. The spotlight theme for the event will be an individual session, fireside chat, and panel discussion with leading and empowering women leaders who have made their mark in career and ICT fields. We are excited and honored to invite all of you to this full day program.

Post our new office registration (Solus B 10) on December 15, 2022, we have pursued with the BBMP authority and got the Khatha certificate in the name of ISACA Bangalore Chapter. We are fully geared to start the chapter's operations during the month of March 2023. Please do watch out our communication on the ceremony for the official, and your presence will be highly inspirational for all of us.

We launched a yearly feedback survey for our members' valuable feedback. Some of the improvement actions taken were also highlighted as part of the survey.

The ISACA Bangalore Chapter intended to add more accredited trainers for the chapter review classes, and the chapter requested eligible candidates submit applications. We have gotten a good response and hope we will be able to get more ATP trainers to strengthen our review classes.

Thank you once again for the renewal of your ISACA membership and certification and for supporting the chapter to maintain its leading status in terms of membership. Still, 50% of the renewal has been achieved, and a continued follow-up is being done with other members to achieve maximum renewals

Regards,

Rajasekharan. K R, CISM, CDPSE, CRSIC ®, PMP, ISO 27001 LA, ITIL (E), CSM, COBIT- 5(F)

President

MESSAGE FROM THE VICE PRESIDENT

Dear Members,

I am sure this message will find you in the best of your health & spirits.

By now many of you should be aware that our SheLeadsTech in the banner program of One in Tech, will be held in person on March 11, 2023, and on the same day we will also commemorate International Women's Day.

We have organized a full-day event that will earn 6 CPE. We request all of you to join us for this in-person event. The Board of Directors and I are excited about the opportunity to see you in person!

We have a great line-up of experts who will share their insights on the trends in Technology and its impact on the careers of professionals and their organizations. The event will also feature a wellness session with prominent women leaders from the field and a session on handwriting analysis!

I along with our Board thank the sponsors for their continued support and participation in our Chapter events.

March is a time of optimism, a time to look ahead and making the time ahead more productive.
We will have our inaugural ceremony of our new office at SOLUS JAIN on 19th March 2023 and it can be rewarding. The invite will be rolled out soon.

Your contributions and efforts are much appreciated!

Best regards,

VIJAYAVANITHA. S ,CISA,CIA,MBA,M.COM

Vice President

MESSAGE FROM THE SECRETARY

Dear Members,

I extend a very warm greeting to all of you. This is our special edition of the newsletter for celebrating the International Women's Day on the 11th of March 2023. We have arranged for a full day program for the day.

As we all know International Women's Day is a global celebration of the social, economic, cultural and political achievements of women. We are celebrating this day by hosting a panel discussion featuring prominent women in IT, highlighting their successes and challenges. Also, other programs are scheduled to keep the members engaged for a full day program.

Overall, celebrating International Women's Day in respect of Bangalore Chapter of ISACA is an opportunity for us to recognize the important contributions of women in the technology field, and to work towards creating a more diverse and inclusive industry for all.

Also, I would like to inform all the members that furnishing of the new Office building is nearing completion.We would like to call upon all the members to actively participate in the opening ceremony of the office wherein we expect a dignitary from the HQ to participate. With the inauguration of the new office, we will be centrally located and hope to see greater member participation in the activities of the chapter.

Also, I would like to inform all the members that furnishing of the new Office building is nearing completion.We would like to call upon all the members to actively participate in the opening ceremony of the office wherein we expect a dignitary from the HQ to participate. With the inauguration of the new office, we will be centrally located and hope to see greater member participation in the activities of the chapter.

We still remain the largest chapter in India but our gap to the next largest chapter Mumbai is down to less than a hundred. We request upon all the members who have not renewed their membership to renew membership to enjoy all the membership privileges extended by ISACA and to grow in their career and recognition in the community as leaders in the IT space.

Looking forward to meeting you all in person on the 11th March.

With Best wishes for the year ahead,

R S UPADHYA
Secretary

ISACA
Bangalore Chapter

RENEWAL OF ISACA MEMBERSHIP FOR THE YEAR 2023

Warm Greetings from ISACA Bangalore Chapter!!

We thank you for your continued support and commitment to professional excellence by earning one or more of ISACA Certifications.

Use your ISACA® membership and ISACA certification(s) as the platform for your growth by utilizing the opportunities for professional development. As you would have experienced, your ISACA membership and certification(s) increase your advancement opportunities by keeping you informed of standards and good practices in the fields that matter most to you and providing access to leading edge research and knowledge through Journals, Webinars, Blogs, ISACA e-library, local chapter events and many more.

Also, you are aware ISACA Bangalore Chapter provides significant benefits and local networking opportunities to its members. The chapter has been in the forefront and served its members in their quest for acquiring professional knowledge by conducting regular CPE Sessions, Webinars, Conferences and other professional development programs. At the chapter it is our endeavor to bring to the table the most relevant of the current topics and encourage active participation of members.

Visit www.isacabangalore.org for more information.

Now it is time for renewing your ISACA® membership for 2023 if not already done. Please ensure to renew your membership before the PURGE to ensure the benefits arising out of continued membership.

Please click below to renew (login with your ISACA username and password to renew)
http://www.isaca.org/renew

In case you need any assistance, please do not hesitate to reach out to Chapter Office at chapter@isacabangalore.org

For your information, the membership dues are indicated here below:
International Membership Dues: $135.00
ISACA Bangalore Chapter Dues: $10.00
Total Dues for 2023 membership renewal: US$ 145.00

Note: Apart from the above, certification maintenance dues may apply as per the certifications held.

Contributions to ISACA Bangalore Chapter Newsletter

Dear Members,

The ISACA Bangalore Chapter Quarterly Newsletter covers the updates on chapter events, technical articles and whitepapers related to the areas of emerging technologies, IT Governance, Audits and Cybersecurity. In this regard, we encourage our chapter members to send your technical articles and whitepapers to us.

You can send your articles / whitepapers to our chapter email address: chapter@isacabangalore.org

Regards,
Director - Newsletter, ISACA Bangalore Chapter

Support from ISACA Bangalore Chapter
Website: https://engage.isaca.org/bangalorechapter/home

Chapter Office Address:

Solus Jain Heights
Unit No: B10, 10th Floor, 1st Cross.
J.C Road, Bangalore-560 002

S-13, 2nd Floor ,Priya Chambers
Dr.Rajkumar Road, Opp. St. Theresa's Hospital,
2nd Stage, Rajajinagar,Bangalore-560010

T: 080-41514331/ 98865 08515 / 080-23377956
Email: chapter@isacabangalore.org
Telegram Channel: https://t.me/joinchat/AAAAAEt42QAUpWHucyNyJA
LinkedIN: https://www.linkedin.com/company/isacabc/
Facebook: https://www.facebook.com/ISACABC/

ISACA Bangalore Chapter

1.Topic: Debunking Common Myths About Cloud Security

Speaker : Prateek Bhajanka, Technology Strategist, Sentinel One

Date : 7th January 2023 (Saturday) Time: 5:30pm to 7:30pm IST

2. CPE Credit offered

Speaker Profile:

Mr. Prateek Bhajanka is a Technology Strategist, Former Gartner Analyst and CybersecurityResearch Analyst. Prateek' s expertise in Security Operations, Vulnerability Management, Penetration Testing, Endpoint Security (EPP/EDR), Digital Forensics and Incident Response, etc. He advises cybersecurity vendors on their Product Messaging and Positioning, Go ToMarket strategy, Licensing, Product Strategy. Presently Prateek manages Technology Strategy for Sentinel One as his role is Technology Strategist- APJ Lead for Sentinel One

2.Topic: Cybercrime - Security Trends and Observations from the field

Speaker : Chitresh Pandit – Sr Consultant - Microsoft

Date : 28th January 2023 (Saturday) Time: 5:30pm to 7:30pm IST

Free Attendance - 2 CPE Credits offered

Speaker Profile:

Chitresh Pandit is a Sr. Consultant Cybersecurity with Security Service Line Microsoft Services, has been with Microsoft for 7 years majorly working with customers during a Security Incident for Compromise Recovery and containment. In addition, he has been working on Security and Identity Modernization, Azure Security, Solution Architecture and Design of Security landscape (Defender Suite, Azure Sentinel) for enterprises and additionally assisting enterprises with cyber security risk assessment and proactive and reactive threat hunting

3.Topic: Managing application layer security for containers

Speaker :Mr. Giri Radhakrishnan, Technical Product Marketing Manager at Tigera (USA)

Date :25th February 2023 (Saturday) Time:11:00am to 1:00pm IST

Free Attendance - 2 CPE Credits offered

Speaker Profile:

Andrey Prozorov, CISM, CIPP/E, CDPSE, LA 27001 is a cyber security and privacy expert with 15+ years of experience and his main areas of expertise are information security and privacy management systems, and methodology (ISO27001, ISO27701, GDPR, KATAKRI, COBIT, ISF SOGP, NIST, IAEA guides, PMBOK). Presently Andrew is a Technical Compliance Manager at Finn play.

Topic Summary:

Agenda:

Observability and security for containers is a challenge especially when it comes to service-service communication. The most used method to solve this problem is using a service-mesh. But operating a service-mesh itself brings its own set of challenges. The session will discuss and demonstrate how to come up with a way to solve this problem.

Speaker Profile:

Giri Radhakrishnan is a Technical Product Marketing Manager at Tigera. He is responsible for GTM activities, product positioning, and messaging for Calico security solutions, focusing on zero trust and container security. Giri has more than 11 years of experience working with networking and security products, with a focus on technical enablement, customer experience, competitive analysis, and product marketing

4.Topic: Acing your Vulnerability Management Program: Policy to Practice

Speaker :Dr Sashank Dara, CTO, CISO & Cofounder at Seconize

Date : 4th March 2023 (Saturday) Time: – 5:30pm to 7:30pm IST

Free Attendance - 2 CPE Credits offered

Topic Summary:

Modern vulnerability management is a tedious, resource-consuming effort. This talk will provide practical advice on how to ace your vulnerability management programs, right from getting the policies in place, adopting mature methodologies, identifying risks, building automation for remediation, and adhering to compliance requirements.

All of them have "Risk Based Principles" at their core.

The session will cover:

1. Basics of Risk Based Vulnerability Management
2. Myths and Pitfalls of modern vulnerability management
3. Adopting mature practices with less resources

Speaker Profile:

Dr Sashank Dara, CTO, CISO & Cofounder at Seconize

As Chief Architect and Technology Officer, he is building next generation automated and intelligent IT Risk and compliance management products. This involves inventing and building relevant cutting edge IT Risk Enumeration, Rating and Quantification technology. This helps CISOs/CIOs translate technical IT risks to measurable potential business impact and embrace a Risk driven approach for derisking their Organizations from Cyber Threats.

As Chief Information Security Officer (CISO) , he is also responsible for overall IT security and compliance at Seconize.

5.SheLeadsTech program 2023 as part of International Women's Day 11th March – In person event – Hotel Chancery Pavilion, Residency Road, Bangalore.

Date :11th March 2023 (Saturday) Time:10:00am to 4:00pm IST

Registration open for all - 6 CPE Credits offered

Venue :The Chancery Pavilion, Residency Road, Bangalore.

Speakers and Panelist:

1. Ms. Anamika Singh, VP, Standard Chartered
2. Ms. Anuradha Lipare,CISO
3. Ms. Smitha Menon , Director, Campgemini
4. Mr. Vaidhyanathan Iyer, COO IBM Cyber Security Command Center

ISACA Bangalore Chapter

PERFORMING A CLOUD AUDIT

INTRODUCTION

In my last article, we understood the various risks involved in Cloud Audit.We discussed on Data Security Risks,Regulatory Risks, Backup Risks, Disaster Recovery Risks, Technology risks, Accountability Risks amongst others. One should also look at these risks from the angle of how they are deployed and serviced.For instance, back up risk in case of an Infrastructure as a Service (IaaS) would be different from that of Software as a Service (SaaS) or Platform as a Service (PaaS). But the bigger question is, how does one audit the Cloud and how do you ensure the risk is within the organization's appetite? This article explores a few of these aspects.

AUDITING THE CLOUD

Given the fact that cloud can be deployed in multiple ways (Public, Private, Hybrid, community etc.) and serviced in different models (IaaS, PaaS or SaaS), auditors need to understand the risks in each scenario. A general one size fits all approach may not be of much relevance as each organization has adopted to the cloud in a unique manner.

The first step would be to check the deployment and service model of the Cloud and understand the SLAs in place between the customer and the Cloud Service Provider (CSP). The following are a few pertinent questions:

a. What is the deployment model chosen by the customer and is that in line with the organization / regulatory expectations?

To recollect the popular deployment models are Public, Private, Community or Hybrid

A company in the BFSI or Healthcare space may prefer a Private Cloud (On Premise or Third Party managed) in contrast to a Public Cloud. On the contrary a company in the hospitality space, may be open to Public Cloud, but with an additional layer of encryption if necessary.

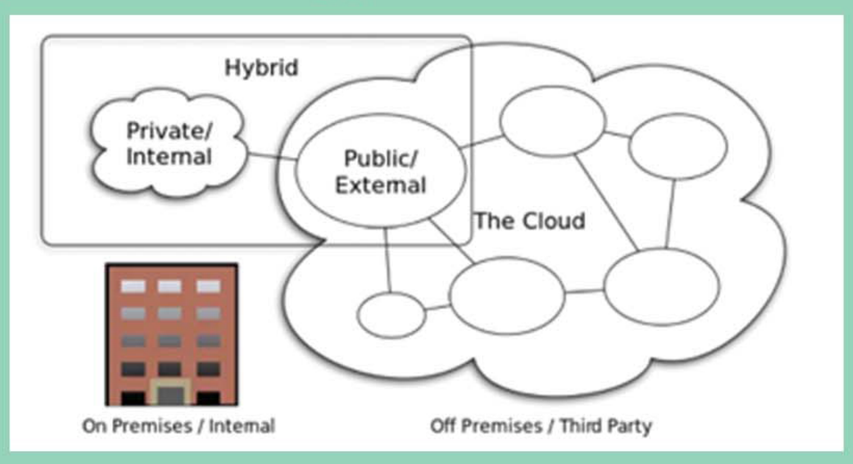


Fig 1 – Different models of deploying Cloud

b. What is the Cloud service model used by the organization?

As discussed in the previous articles, the popular cloud Service are Infrastructure as a Service (IaaS), Platform as a Service (PaaS) or Software as a Service (SaaS).

A company having a dedicated tech team, might prefer going for an Infrastructure as a Service (IaaS), where only the infrastructure (i.e., Physical network,data center) is shared by CSP, and Operating system, network, applications, is designed and developed by the company. In this case as auditors, all the traditional domains are to be looked into, except for physical security and environmental controls. The below are a few areas to be examined:

i. Compatibility of applications once they have migrated from On-premises to IaaS

ii. How have the Infrastructure and Virtualization Security been enabled?

iii. How is the network, VPN set up? How is the firewall configured to permit the incoming and outgoing traffic?

iv. How are the change management practices followed for the infrastructure?

v. How are the root accounts (super use account in cloud) protected?

vi. Whether the vulnerability and penetration testing (ethical hacking) of the infrastructure was performed to identify technical weaknesses?

vii. How is encryption enabled?

viii. How are access to make Infrastructure changes managed?

ix. How are logs configured and retained?

x. Is there a centralized Cloud infra team who manages the overall infrastructure? Does it include how it is designed and operated?

xi. Are there standard ways in which software development takes place on the Cloud?

On the contrary, a company may alternatively be using a SaaS solution developed by a CSP. In this case most of the technical controls are the responsibility of the SaaS solution provider and the auditor must focus on the customers responsibilities which include the following:

i. How was the data migrated into the SaaS solution? Is there means to ensure integrity and completeness?

ii. Who has access to the data from the CSP's team and from the client's end? How are those managed?

iii. Is the access subject to periodical review and revocation?

iv. How are users identified and authorized into the SaaS solution? Are there multi-factor authentications in place?

v. Who is responsible for periodical backing up data? Is the data back up in line with the organization needs? For instance, organization has a backup requirement for four times a day,whereas the SaaS solution could be backing up the data only once a day!

vi. How is Disaster Recovery System enforced? How can it impact the clients' business?

vii. Whether super user has access to delete production data and backup data?

viii. How is the data classified within the SaaS Application? Does it have Personally Identifiable data, Sensitive Data, highly confidential data etc.?

ix. How is each category of data treated and secured? Are there mandatory encryptions in place?

x. Where is the data hosted? Are there geographical barriers?

xi. Who and how is the process of access grant, revocation and modification monitored?

Therefore, as auditors, each Cloud deployment model has unique questions to answer. The below Figure is another reminder to understand the unique responsibilities in different service models.

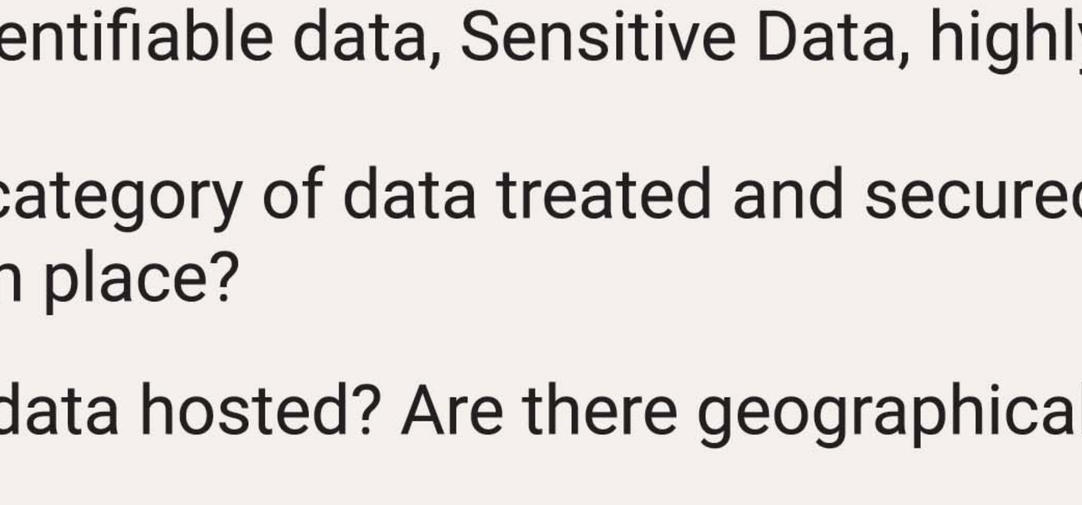


Fig 2 – Responsibilities in a different Cloud Models

c. Other common audit questions in all the Cloud Models

The following are few of the common area's auditors should focus in addition to above:

i. Understanding the SLAs in place and how they are monitored?

ii. What is the extent of customization performed by CSP for the customer? Often, the CSP does not customize as it makes it difficult for the CSP to manage those customizations.

iii. What are the security frameworks the CSP is adhering to? ISO 27001, ENISA Cloud governance framework, Cloud Control Matrix (CCM) by Cloud Security Alliance (CSA), SOC 2 Type 2 are few standard reports which are worthy for CSPs.

iv. Ensuring back up policy is consistent between customer requirement and what the CSP offers?

v. How are changes to application and infrastructure performed? What is the extent of sharing of the roles and responsibilities between the CSP and customer?

vi. Has the CSP mandated encryption for all customers or is it only based on request?

vii. Does CSP have access to the customers data and how is that monitored?

viii. How is multi-tenancy of cloud customers managed?

ix. Is there a Cloud Escrow agreement in place? An Escrow Agreement is a simple tri-party arrangement with mutually agreed terms between the CSP, customer and trustee. Under the terms of the Agreement, the CSP deposits the materials required to access, restore or rebuild the Cloud with the trustee and in the event CSP failing to operate or closing down the business, the customer can make use of the information with the trustee and suffer minimal losses

x. Are the backups subject to same level of protection as the production environments?

xi. Whether the data is hosted within the geographical boundaries of the customer? Are there any regulatory requirements in storing the data locally?

xii. Is the Disaster Recovery / back up stored in the same geographical location or stored in different location? (A different location is preferred as it reduces the risk in case the primary center is not accessible.)

xiii. Who invokes the Disaster recovery and under what circumstances are these invoked? Is it only when all the CSP or majority of the CSP customers have an outage or when even when one customer is having a challenge?

xiv. Are there additional methods of access restrictions such as IP based restrictions, browser-based restrictions, device-based restrictions, geography / country / region-based restrictions, time-based restrictions etc.

Common issues noted in Cloud Audits:

Based on my experience, below are a few common issues noticed in Cloud Audits:

In General

• Lack of awareness of responsibilities towards key risk (e.g., Who must take backup, who will test it) / Shared Responsibility
• SLA Compliance and tracking (for CSP and Third Party)
• Understanding of Backup, Restoration, BCP and Disaster Recovery requirements and responsibilities

In case of IaaS / PaaS audits

• Network Security, VLAN, subnets, firewall rules (Ingress and egress) having incorrect configuration, open firewall ports,
• Incorrect parameters configured for Virtualization Layer, permitting unapproved ports, Web Application Firewall WAF not configured, IDS / IPS not configured.
• Ownership of deployment between centrally controlled cloud architects versus platform / department autonomy, creating conflicting rules.
• Failure in DR / Backup restoration, lack of segregation of duties at Customer set up (e.g., User having access to delete production data and cloud backup)

In case of SaaS Audits

- Absence of SOC 2 Report Type 2 – No visibility of CSP operations
- Incorrect data classification principles followed by Customer (PII, Health, SPDI hosted in Cloud) without assessing the risk
- SOC 2 report covers different locations, Customer data hosted in different location
- Absence of User access review performed by Customer / CSP for the services provided
- Lack of Change Management review by Customer in a highly customized environment.
- Extent of access to CSP and their team

Concluding Thoughts

Auditing the cloud requires comprehensive understanding of the customer, the CSP practices and how the integration between them. One should also be clear on the shared responsibilities and to what extent these overlap or override. As auditors, it is important that cloud is assessed independently from the angle of how it is deployed, serviced and more importantly to the extent it is used by the organization.

About the Author

CA Narasimhan Elangovan, Partner, KEN & Co. and Sr. Advisor, Digital Security Services in Crowe Advisory Services (India) LLP.
B.COM, FCA, CS, DISA, DIPIFR(UK), CISA(USA), LLB, CDPSE (USA), ISO 27001 Lead Auditor
Email: narasimhan@ken-co.in

ISACA
Bangalore Chapter

The Third-Party Remote Access Security & applying Digital Trust

Information aware attackers are more common. They have observed an increase in the number of businesses using outside providers to swiftly and effectively scale their modus operandi. They've come to the conclusion that they can potentially acquire access to several well-known organizations by concentrating their efforts on a single small third-party vendor as opposed to one single corporation. They have not only discovered yet another backdoor, but also a backdoor that opens a number of further backdoors.

High-profile data breaches at Marriott, YouTube, and Tesla over the past three years have all been connected weaknesses in third party connected environments. Also, the researchers found that more than 50% of firms had dealt with a third-party-caused data breach.

In addition to the fact that third parties are a common attack vector, a recent study found a worrying gap between an organization's perception of the threat posed by third-party access and the security solutions it uses.

The solution for third party remote access risk is simply to start putting basic resources and required controls behind validating your third party and other partners and implementing security measures that go beyond just implicit trust. Here are three starting points for assessing and shoring up your own third-party access security

NETWORK ASSETS, CONNECTIVITY, AND ITS TRANSPARENCY

As part of basic change management process measures, the first step is to evaluate the exposure and take asset inventory of your current third-party access. Based on the recent survey report, nearly 50% say that they have full inventory of third parties with approved network access. Surprisingly, nearly other 50% don't have any visibility into vendor access and their network permissions.

An initial inventory of vendor access can make the transition to a third-party vendor management system much more straightforward, which can significantly mitigate the risk of a third-party breach. A platform designed to manage vendor access not only offers the ability to easily see who has access and how much, but also can log who accessed your systems, when they did it, and what they did. As they say, knowing is half the battle.

An initial inventory of vendor access can make the transition to a third-party vendor management system much more straightforward, which can significantly mitigate the risk of a third-party breach. A platform designed to manage vendor access not only offers the ability to easily see who has access and how much, but also can log who accessed your systems, when they did it, and what they did. As they say, knowing is half the battle.

Access based Zero Trust Network

The accurate inventory of access is difficult and this experienced outcome of majority surveys, they say that they are unable to provide the appropriate amount of access to their vendors based on the inventory. There is a challenge more than the most error is giving vendors too much access for indefinite period, and then trusting that their vendor doesn't suffer a breach of their own. With third-party breaches on the rise, trusting your vendors to limit breaches into your own systems just isn't no more enough.

Best way to implement a third-party vendor management platform, which allows the implementation of a much more secure Zero Trust Network Access model. Implicit trust in a vendor must be replaced with explicit trust like multi-factor verification and privileged access management. Any time a vendor needs access to your systems, they must verify who they are, and once verified, only have access to exactly what they need to know or have.Trust can be abused; however, verification cannot.

Auditing Third Party Security process

Management of independent contractors is harder than it seems. Companies are finally realising that managing vendor access belongs to the security and ICT teams rather than the legal, compliance, and procurement departments. And when that duty changes, ICT departments are suddenly in charge of more than a few hundred vendors, which overwhelms them.

Implementing a third-party vendor management platform can make it easier to handle the normally arduous process of keeping track of third-party access, establishing network permissions, and keeping an eye on activity. This in turn makes it simpler to add new security measures as well as to keep track of who has access.

A third-party management system can provide the protection and transparency you need to know you're safeguarded against any breaches, as opposed to simply giving a new vendor access and crossing your fingers and wishing for the best.

Signed contracts, reputations, and compliance checklists are no longer sufficient due to the increasing number of hackers focusing on third-party vendors. Happily there exist technologies to make vendor administration simpler and more safe; the decision to invest resources in one is now required.

Every interaction is based on trust. Third party relationships, businesses,and transactions trustworthy is key for establishing and maintaining the digital trust Trust is defined as "certain reliance on the competence, strength, or veracity of someone's relationship in business. Third party access is one the key parameters for establishing trust. Digital trust places a strong emphasis on relationships, interactions, and transactions,which cover a wide range of contexts and interaction rates. Asset Management, establishing a framework for zero trust and ensuring the asset & its process are working against the established baseline will increase the confidence of business relationships.

Developing digital trust is a continuous process; the notion of digital trust emphasizes both the construction and upkeep of a reliable digital ecosystem.

RAJASEKHARAN. K R , CISM, CDPSE, CRSIC ®, PMP, ISO 27001 LA, ITIL (E), CSM, COBIT- 5(F)

TABLE OF CONTENTS

INTRODUCTION

This whitepaper describes the importance of EDR security and gives a quick glimpse of EDR evasion techniques. The objective of this paper is to provide insights on endpoint security as an increasingly vital component of any organization's cybersecurity strategy.

ABBREVIATION

Sl No	Acronyms	Full Form
1	EDR	Endpoint Detection and Response
2	AV	Antivirus
3	IOC	Indicator of compromise

MARKET TRENDS & CHALLENGES

EDR evasion capabilities have grown significantly in the past several years. It is easy to find many publicly available approaches for defeating EDR tools. A strong endpoint security is an increasingly vital component of any organization's cybersecurity strategy. The information available on existing EDR evasion capabilities will be explored as this can aid threat hunters in detection. Deploying an effective EDR security solution is essential to protecting enterprises/organizations from cyber threats.

Let us look at the current methods that hackers use to evade EDR detection:

DIFFERENT METHODS TO EVADE EDR DETECTION:

Bloating: EDRs do not scan files beyond a certain file size. By increasing the file size of the malicious file, attackers can evade the EDR detection

IOC Manipulation: One of the other methods to avoid detection is modifying the malicious file such that it removes IOC used by security products to detect malware.

Certificate Spoofing: Spoofing the code signing certificate and signing the malicious certificate to evade EDR and security products

1. BLOATING:

Cyber attackers can evade EDR detection by increasing the file size of the malicious file as EDRs do not scan files beyond a certain file size

2. IOC MANIPULATION:

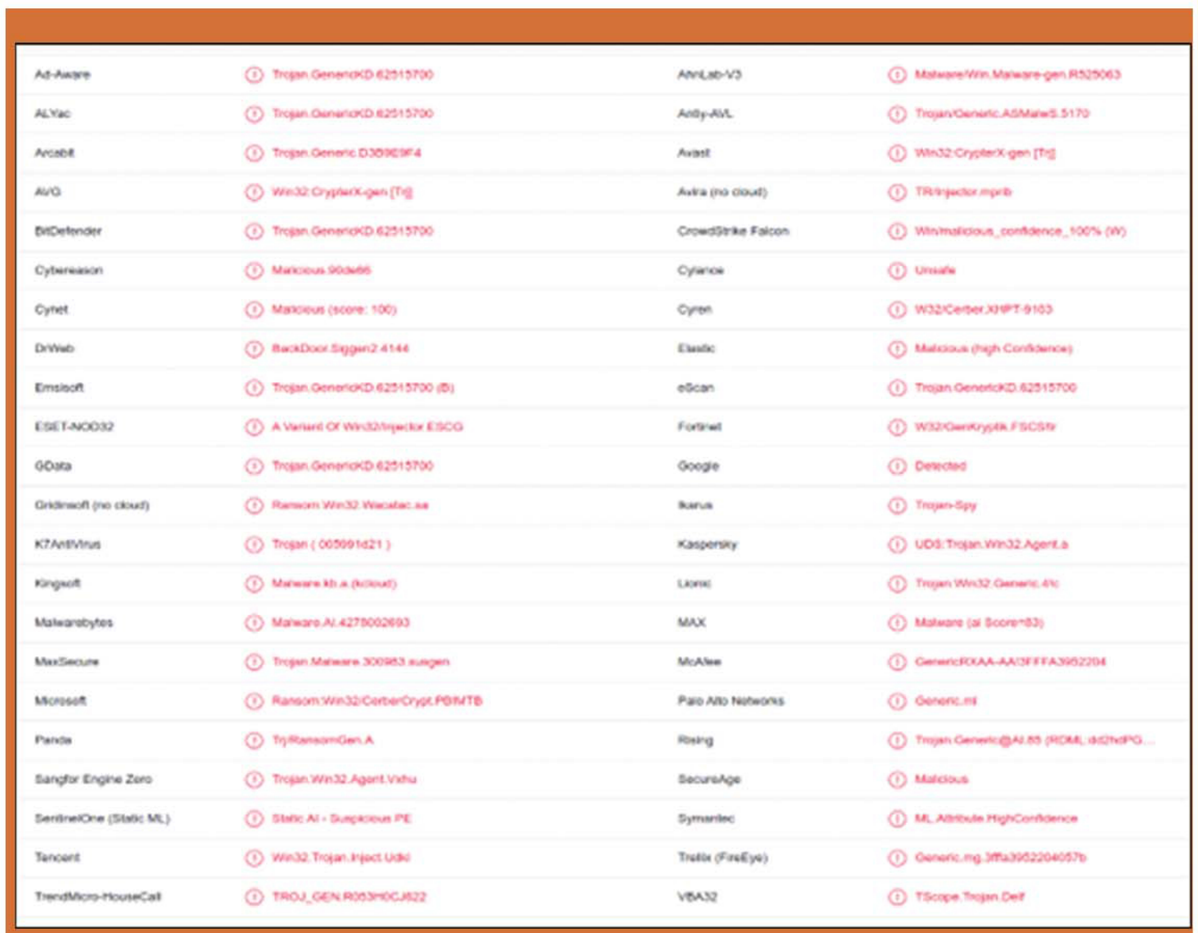
Attackers also use other methods such as modifying the malicious files in a manner that it removes IOC used by security products to detect the malware .

3. CERTIFICATE SPOOFING:

Hackers also spoof code signing certificates and sign malicious files to evade EDR and security products

SHOWN BELOW ARE SOME SAMPLE SCREENSHOTS OF THE VARIOUS STAGES OF EDR EVASION

1) Detection before bloating (Fig 1)

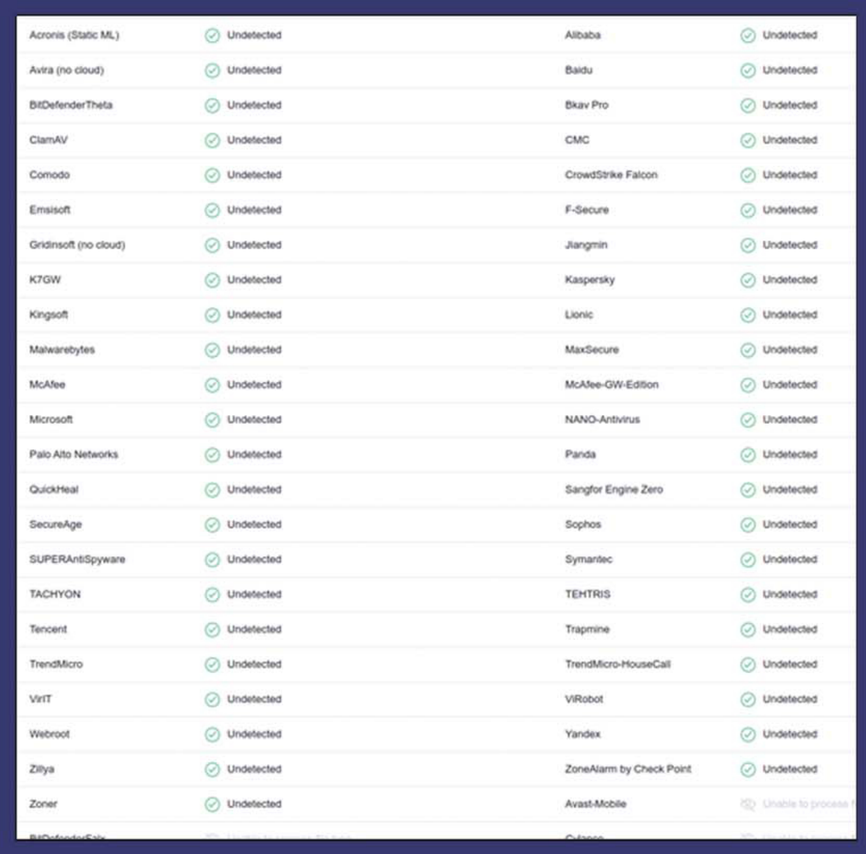


Ad-Aware	Trojan.GenericKD.62515700	AhnLab-V3	Malware/Win.Malware-gen.R525063
ALYac	Trojan.GenericKD.62515700	Antiy-AVL	Trojan/Generic.ASMalwS.5170
Arcabit	Trojan.Generic.D3D9E9F4	Avast	Win32:CrypterX-gen [Trj]
AVG	Win32:CrypterX-gen [Trj]	Avira (no cloud)	TR/Injector.mprib
BitDefender	Trojan.GenericKD.62515700	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cybereason	Malicious.90de66	Cylance	Unsafe
Cynet	Malicious (score: 100)	Cyren	W32/Cerber.XHPT-9103
DrWeb	BackDoor.Siggen2.4144	Elastic	Malicious (high Confidence)
Emsisoft	Trojan.GenericKD.62515700 (B)	eScan	Trojan.GenericKD.62515700
ESET-NOD32	A Variant Of Win32/Injector.ESCG	Fortinet	W32/GenKrypt!k.FSCS!tr
GData	Trojan.GenericKD.62515700	Google	Detected
Gridinsoft (no cloud)	Ransom.Win32.Wacatac.sa	Ikarus	Trojan-Spy
K7AntiVirus	Trojan (005091d21)	Kaspersky	UDS:Trojan.Win32.Agent.a
Kingsoft	Malware.kb.a.(kcloud)	Lionic	Trojan.Win32.Generic.4!c
Malwarebytes	Malware.AI.4278002693	MAX	Malware (ai Score=83)
MaxSecure	Trojan.Malware.300983.susgen	McAfee	GenericRXAA-AA!3FFFA3952204
Microsoft	Ransom:Win32/CerberCrypt.PBMTB	Palo Alto Networks	Generic.ml
Panda	Trj/RansomGen.A	Rising	Trojan.Generic@AI.85 (RDML:dd2NdPG...
Sangfor Engine Zero	Trojan.Win32.Agent.Vxhu	SecureAge	Malicious
SentinelOne (Static ML)	Static AI - Suspicious PE	Symantec	ML.Attribute.HighConfidence
Tencent	Win32.Trojan.Inject.Udkl	Trellix (FireEye)	Generic.mg.3ffa3952204057b
TrendMicro-HouseCall	TROJ_GEN.R053H0CJ522	VBA32	TScope.Trojan.Delf

2) Bloating the infected file (Fig 2)

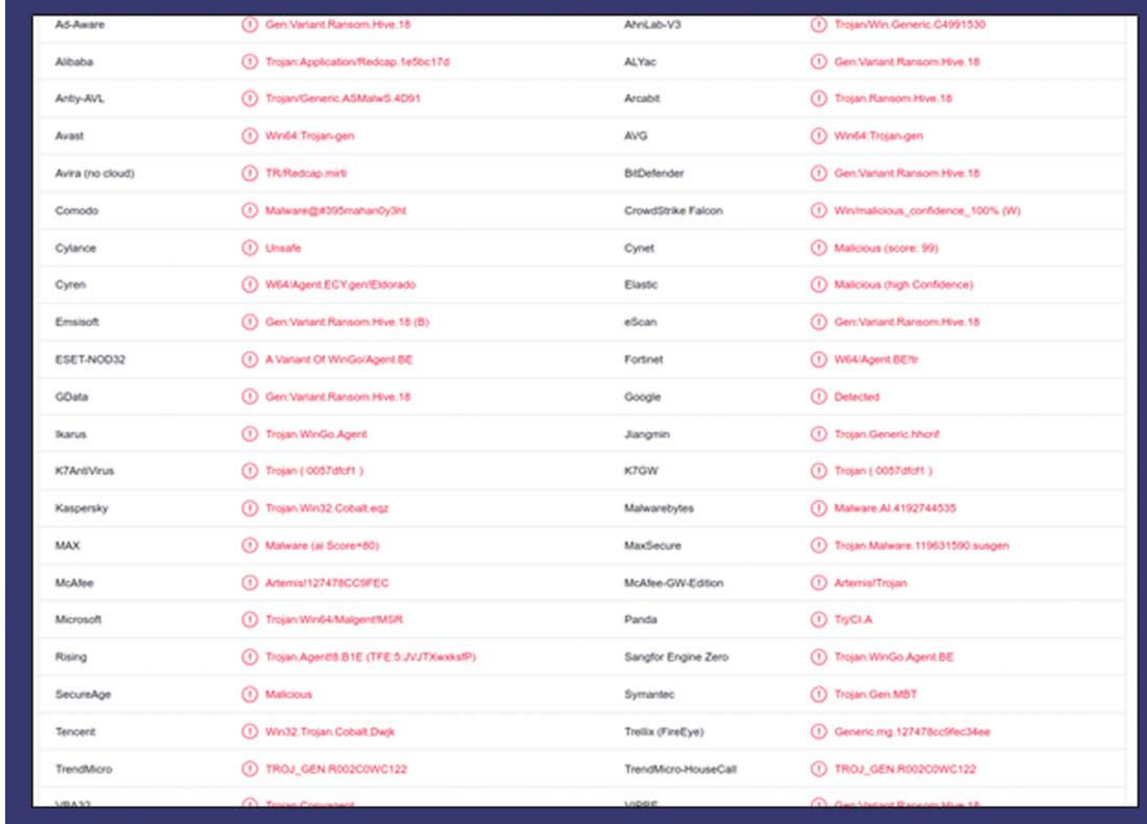
```
mc@mc:/tmp/ezr$ ls -lh
total 7.0M
-rwxrwxr-x 1 mc mc 2.3M Oct  7 21:39 ezr
-rw-r--r-- 1 mc mc 4.8M Oct  7 15:05 infected
mc@mc:/tmp/ezr$ ./ezr --input infected --output infected_bloated --bloat 100

mc@mc:/tmp/ezr$ ls -lh
total 112M
-rwxrwxr-x 1 mc mc 2.3M Oct  7 21:39 ezr
-rw-r--r-- 1 mc mc 4.8M Oct  7 15:05 infected
-rwxrwxr-x 1 mc mc 105M Oct  7 21:40 infected_bloated
mc@mc:/tmp/ezr$
```

3) After bloating (Fig 3)



Acronis (Static ML)	Undetected	Alibaba	Undetected
Avira (no cloud)	Undetected	Baidu	Undetected
BitDefenderTheta	Undetected	Bkav Pro	Undetected
ClamAV	Undetected	CMC	Undetected
Comodo	Undetected	CrowdStrike Falcon	Undetected
Emsisoft	Undetected	F-Secure	Undetected
Gridinsoft (no cloud)	Undetected	Jiangmin	Undetected
K7GW	Undetected	Kaspersky	Undetected
Kingsoft	Undetected	Lionic	Undetected
Malwarebytes	Undetected	MaxSecure	Undetected
McAfee	Undetected	McAfee-GW-Edition	Undetected
Microsoft	Undetected	NANO-Antivirus	Undetected
Palo Alto Networks	Undetected	Panda	Undetected
QuickHeal	Undetected	Sangfor Engine Zero	Undetected
SecureAge	Undetected	Sophos	Undetected
SUPERAntiSpyware	Undetected	Symantec	Undetected
TACHYON	Undetected	TEHTRIS	Undetected
Tencent	Undetected	Trapmine	Undetected
TrendMicro	Undetected	TrendMicro-HouseCall	Undetected
VirIT	Undetected	ViRobot	Undetected
Webroot	Undetected	Yandex	Undetected
Zillya	Undetected	ZoneAlarm by Check Point	Undetected
Zoner	Undetected	Avast-Mobile	Unable to process f

4) Before IOC Evasion (Fig 4)



Ad-Aware	Gen:Variant.Ransom.Hive.18	AhnLab-V3	Trojan/Win.Generic.C4991530
Alibaba	Trojan:Application/Redcap.1e5bc17d	ALYac	Gen:Variant.Ransom.Hive.18
Antiy-AVL	Trojan/Generic.ASMalwS.4D91	Arcabit	Trojan.Ransom.Hive.18
Avast	Win64:Trojan-gen	AVG	Win64:Trojan-gen
Avira (no cloud)	TR/Redcap.mirti	BitDefender	Gen:Variant.Ransom.Hive.18
Comodo	Malware@#395mahan0y3nt	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cylance	Unsafe	Cynet	Malicious (score: 99)
Cyren	W64/Agent.ECY.gen!Eldorado	Elastic	Malicious (high Confidence)
Emsisoft	Gen:Variant.Ransom.Hive.18 (B)	eScan	Gen:Variant.Ransom.Hive.18
ESET-NOD32	A Variant Of WinGo/Agent.BE	Fortinet	W64/Agent.BE!tr
GData	Gen:Variant.Ransom.Hive.18	Google	Detected
Ikarus	Trojan.WinGo.Agent	Jiangmin	Trojan.Generic.hhcnf
K7AntiVirus	Trojan (0057dfcf1)	K7GW	Trojan (0057dfcf1)
Kaspersky	Trojan.Win32.Cobalt.esz	Malwarebytes	Malware.AI.4192744535
MAX	Malware (ai Score=80)	MaxSecure	Trojan.Malware.119631590.susgen
McAfee	Artemis!127478CC9FEC	McAfee-GW-Edition	Artemis!Trojan
Microsoft	Trojan:Win64/Malgent!MSR	Panda	Trj/CI.A
Rising	Trojan.Agent!8.B1E (TFE:5:JVJTXwxksfP)	Sangfor Engine Zero	Trojan.WinGo.Agent.BE
SecureAge	Malicious	Symantec	Trojan.Gen.MBT
Tencent	Win32.Trojan.Cobalt.Dwjk	Trellix (FireEye)	Generic.mg.127478cc9fec34ee
TrendMicro	TROJ_GEN.R002C0WC122	TrendMicro-HouseCall	TROJ_GEN.R002C0WC122
VBA32	Trojan.Convagent	VIPRE	Gen:Variant.Ransom.Hive.18

5) Performing IOC Evasion (Fig 5)

```
mc@mc:/tmp/ezr$ ls -lh
total 4.5M
-rwxrwxr-x 1 mc mc 2.3M Oct  7 21:39 ezr
-rw-r--r-- 1 mc mc 2.3M Oct  7 16:35 infected
mc@mc:/tmp/ezr$ ./ezr --input infected --output infected_evaded --ioc

mc@mc:/tmp/ezr$ ls -lh
total 6.7M
-rwxrwxr-x 1 mc mc 2.3M Oct  7 21:39 ezr
-rw-r--r-- 1 mc mc 2.3M Oct  7 16:35 infected
-rwxrwxr-x 1 mc mc 2.3M Oct  7 22:10 infected_evaded
mc@mc:/tmp/ezr$
```

ISACA Bangalore Chapter

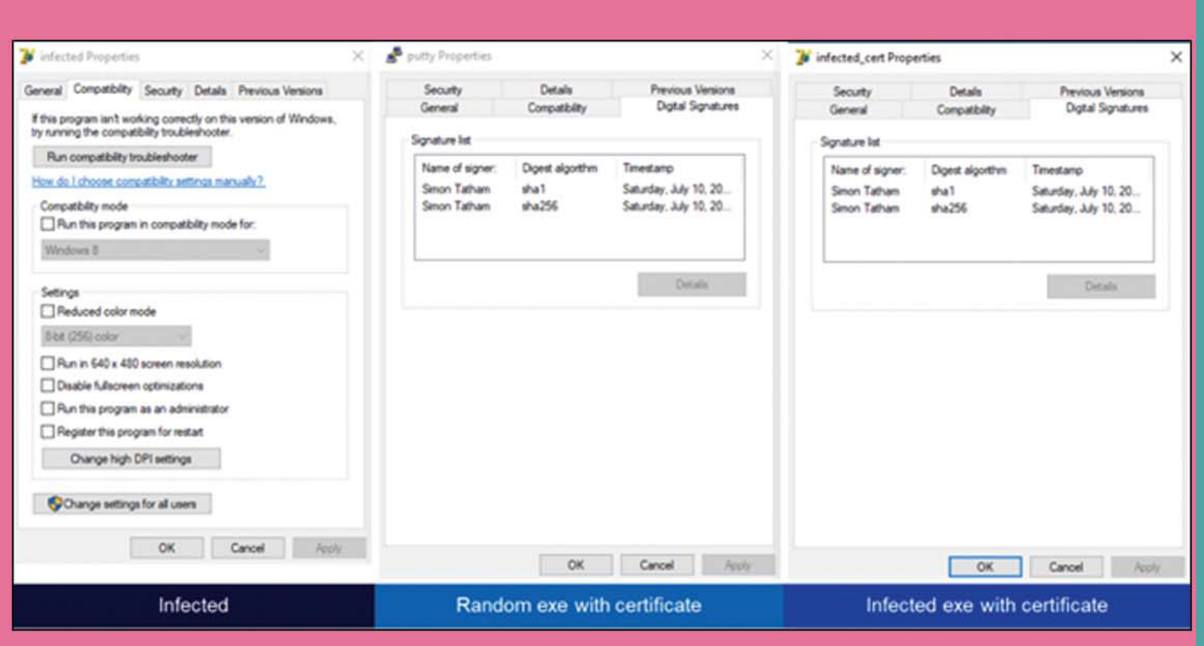
THE FOLLOWING IMAGES SHOW HOW HACKERS ENCRYPT THE PAYLOAD/SHELL CODE USING XOR

6) After IOC Evasion (Fig 6)

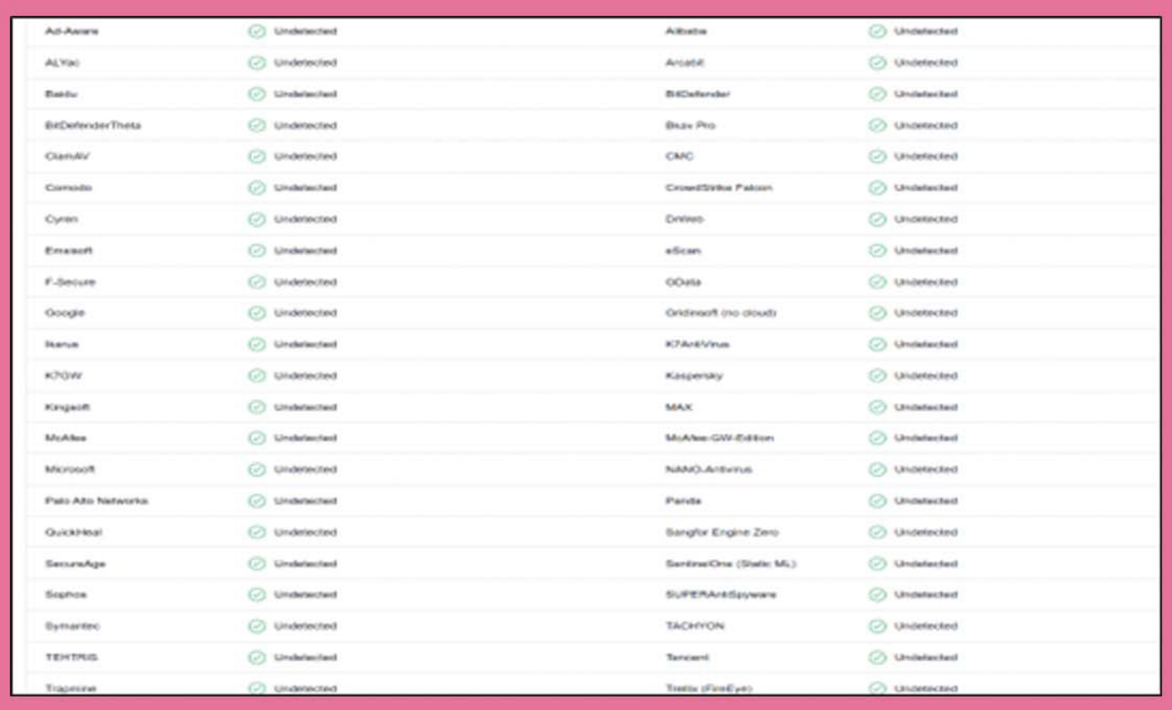
Ad-Aware	Undetected	Alibaba	Undetected
ALYac	Undetected	Antiy-AVL	Undetected
Arcabit	Undetected	Avast	Undetected
AVG	Undetected	Baidu	Undetected
BitDefender	Undetected	BitDefenderTheta	Undetected
Bkav Pro	Undetected	ClamAV	Undetected
CMC	Undetected	Comodo	Undetected
CrowdStrike Falcon	Undetected	Cybereason	Undetected
Cylance	Undetected	DrWeb	Undetected
Emsisoft	Undetected	eScan	Undetected
F-Secure	Undetected	GData	Undetected
Gridinsoft (no cloud)	Undetected	Ikarus	Undetected
K7AntiVirus	Undetected	K7GW	Undetected
Kingsoft	Undetected	Lionic	Undetected
MAX	Undetected	McAfee	Undetected
McAfee-GW-Edition	Undetected	NANO-Antivirus	Undetected
Palo Alto Networks	Undetected	Panda	Undetected
QuickHeal	Undetected	Sangfor Engine Zero	Undetected
SentinelOne (Static ML)	Undetected	Sophos	Undetected
SUPERAntiSpyware	Undetected	Symantec	Undetected
TACHYON	Undetected	TEHTRIS	Undetected

7) Faking certificate (Fig 7)

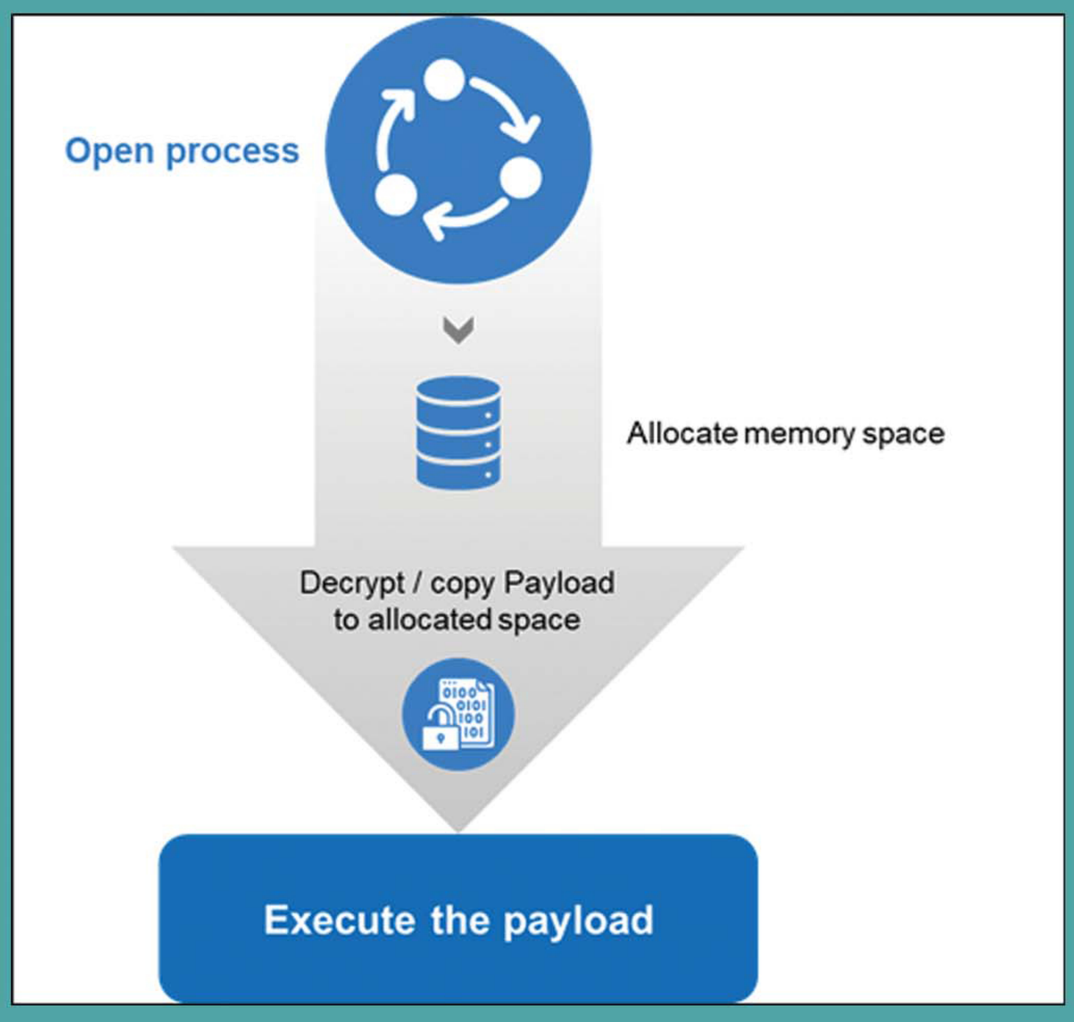
```
mc@mc:/tmp/ezr$ ls -lh
total 8.2M
-rwxrwxr-x 1 mc mc 2.3M Oct  7 21:39 ezr
-rw-r--r-- 1 mc mc 4.8M Oct  7 15:05 infected
-rwxrwxrwx 1 mc mc 1.3M May 12 12:54 putty.exe
mc@mc:/tmp/ezr$ ./ezr --input infected --output infected_cert --cert-file putty.exe

mc@mc:/tmp/ezr$ ls -lh
total 13M
-rwxrwxr-x 1 mc mc 2.3M Oct  7 21:39 ezr
-rw-r--r-- 1 mc mc 4.8M Oct  7 15:05 infected
-rwxrwxr-x 1 mc mc 4.8M Oct  7 21:51 infected_cert
-rwxrwxrwx 1 mc mc 1.3M May 12 12:54 putty.exe
```



8) After certificate spoof (Fig 9

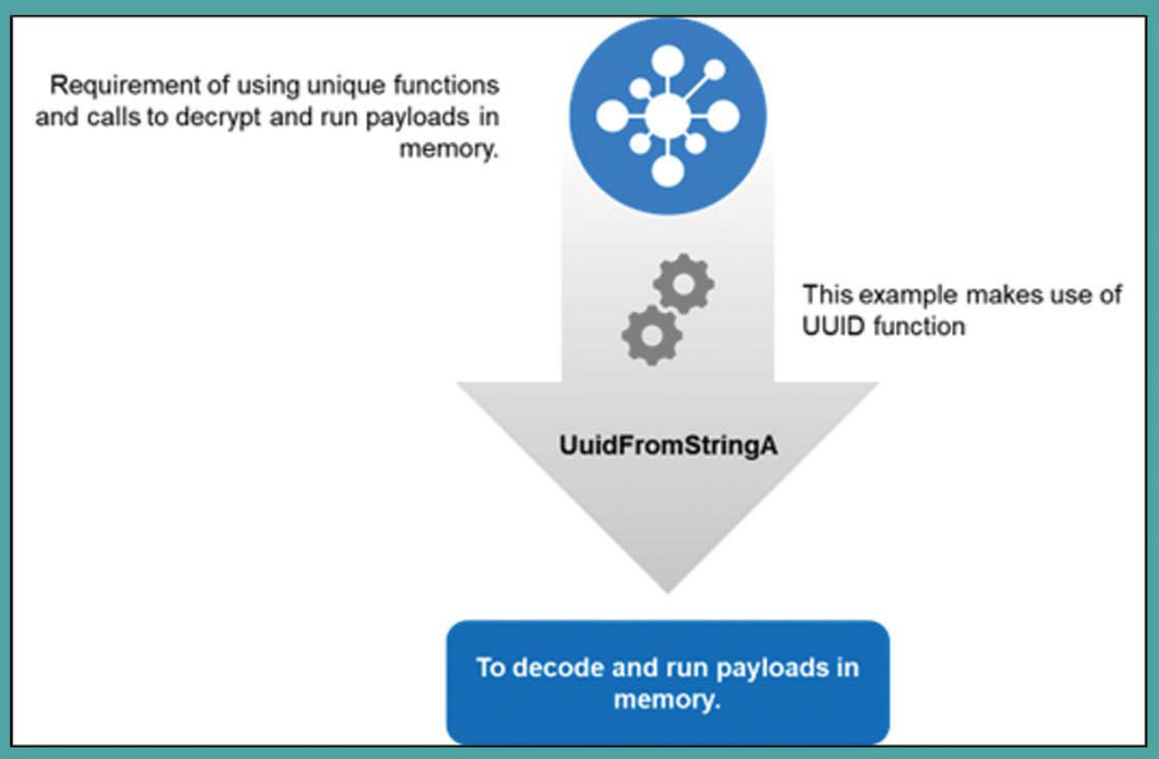


9) Common AV/EDR evasion methods for XOR shellcode (Fig 10)

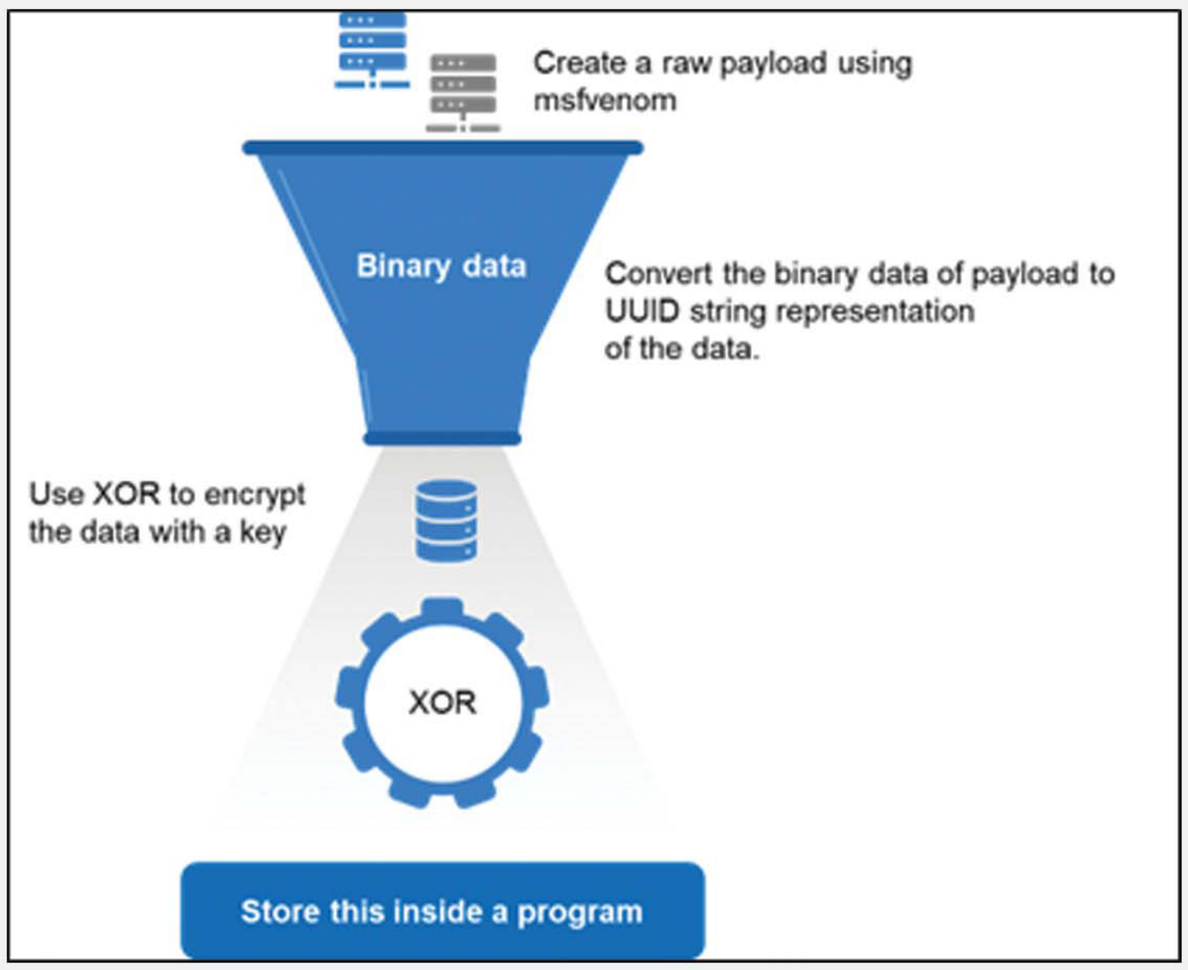


The drawback however is that common functions like memcpy, Write Process Memory are now detected on dynamic analysis by most AV's.

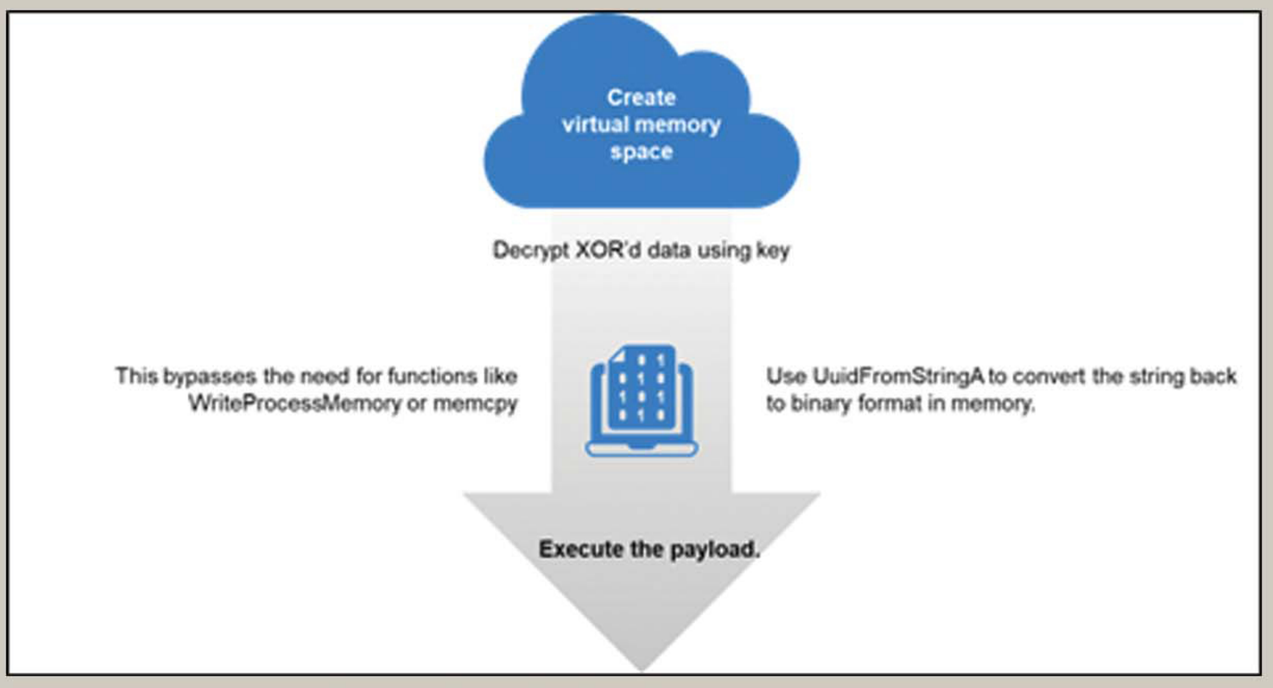
10) How the hackers encrypt the Payload/ Shell code using XOR (Fig 11)



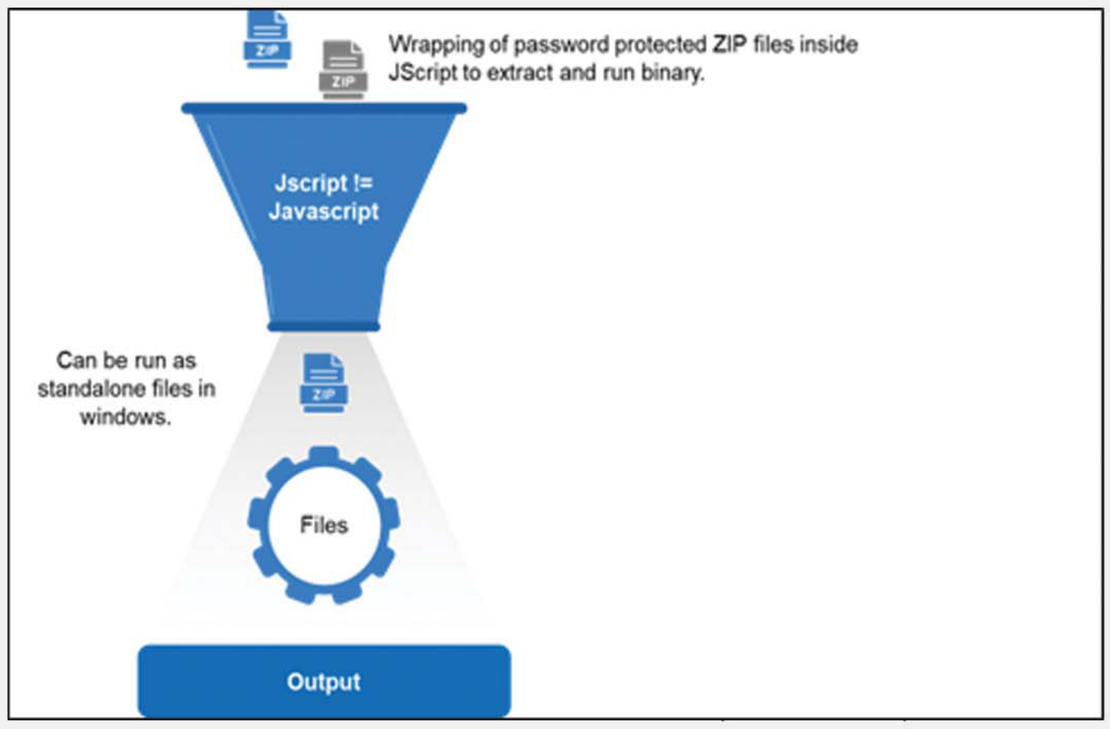
11) Steps to create the same (Fig 12)

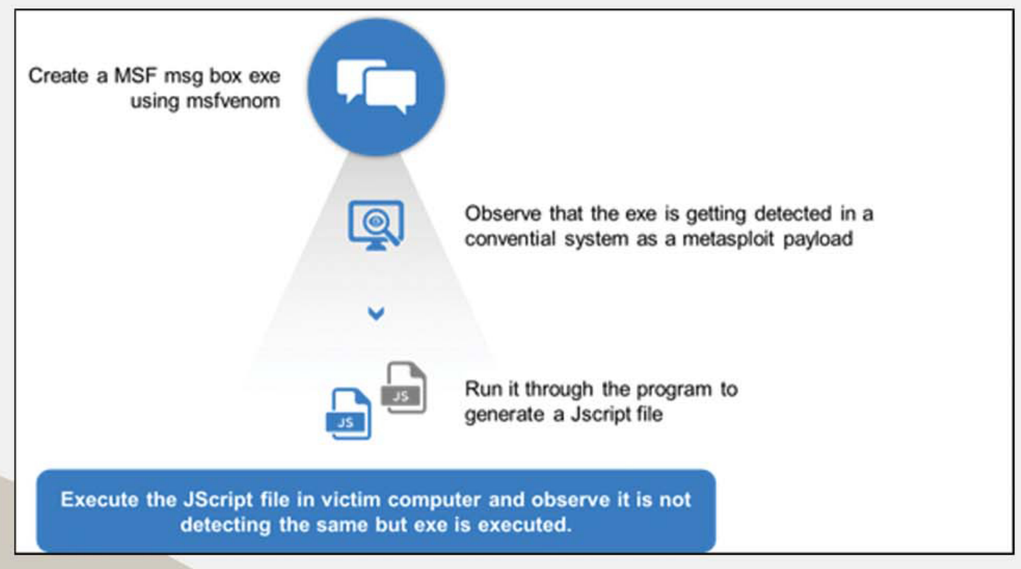


12) Steps to execute payload from within program (Fig 13)

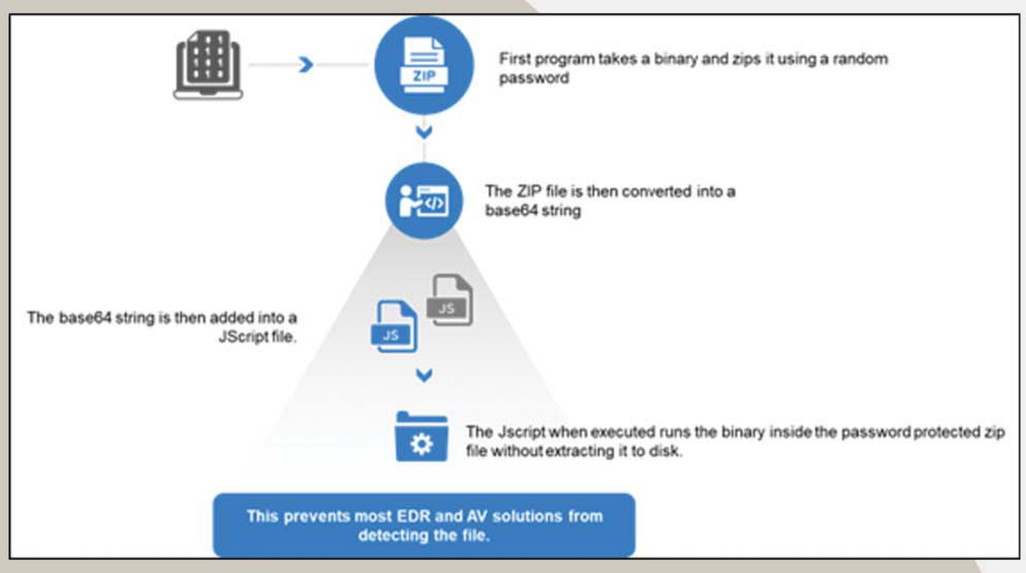


13) Next few screenshots show how an executable is converted to an embedded zip file inside JScript (Fig 14)





How the JScript code works (Fig 16)



ANALYSIS

Detection rate dropped from 18 to 5.	Not detected by many major Antivirus.	What is being detected is the Jscript code not the binary.	If the Jscript is rewritten from scratch it will likely make the code undetectable by all AV's and EDR's.

CONCLUSION

To summarize, malicious actors are taking advantage of the situation, exploiting an unprecedented opportunity to breach organizations worldwide using endpoints as the top attack vector. As a result, the endpoint security solution should be based upon best practices for protecting organizations from preventing the most imminent threats to the endpoint.

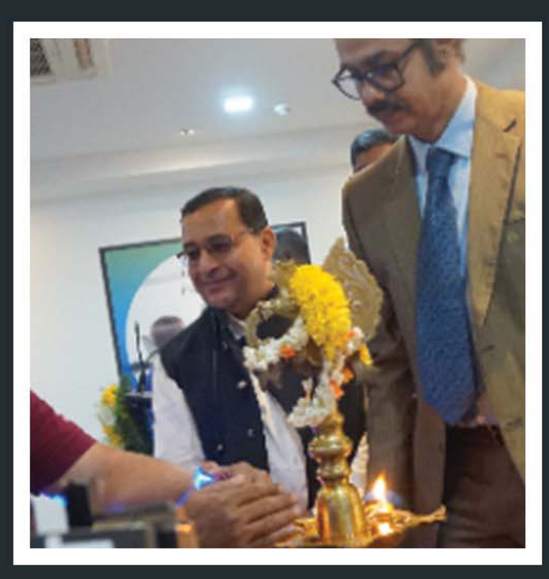
Author Info

Mr. Suriya Prakash
Head-DARWIS SFS & Threat Intel API
CySecurity Corp

Mr. Sabari Selvan
Security Architect
CySecurity Corp

Pictorials

Office Pooja & Inauguration




Become a part of

SheLeads Tech

PROGRAM CALENDAR – IWD 2023
11TH MARCH 2023 | THE CHANCERY PAVILION | 10:00 TO 05:00 PM

ONE IN TECH™

SheLeadsTech

Building global inclusion and equity for the advancement of women in cybersecurity and IT audit.

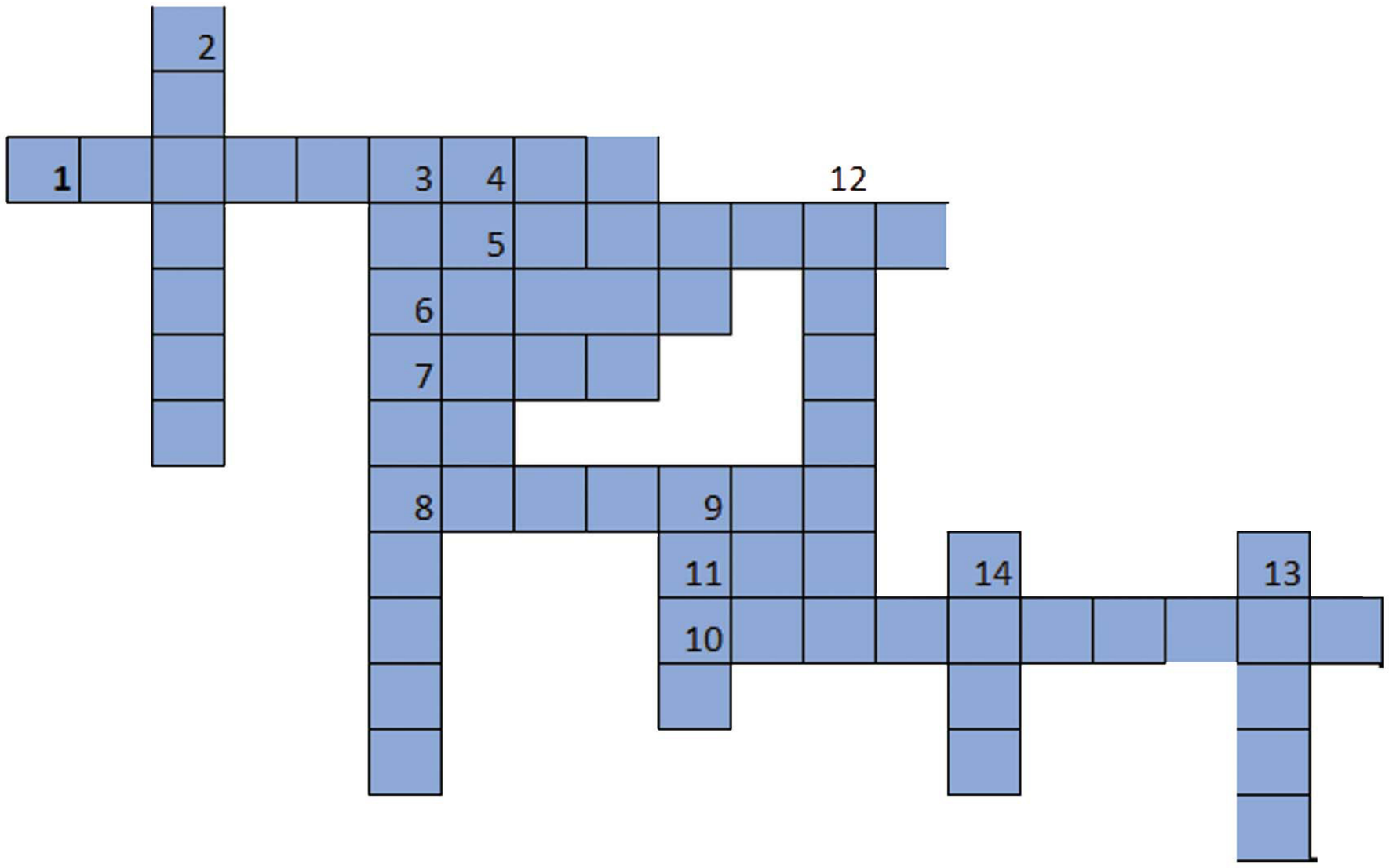
ISACA Bangalore Chapter

Event Partner
VALUE POINT
A NOVENTIQ Company

Time - IST	Session
09:00 - 09:50	Delegate registration
10:00 – 10:05	Invocation Ms. Vijay Vanitha – ISACA BC Vice President
10:05 -10:10	Welcome address by ISACA President Mr. Rajasekharan KR
10:10 - 10:15	SheLeadsTech welcome address by ISACA BC SIG Director - Ms. Lalitha Satheesh
10:20 -10:25	Lighting the lamp by Chief Guest/Keynote Speaker/Women Leaders
10:25 -10:45	Keynote address Mr. Mahadesha / Program Director & CISO, CeG
10:45 - 11:45	**Panel Discussion:** **"How to embrace IT advancement through upskilling and cross learning and be prepared to face the challenges".** • Ms. Anamika Singh, VP, Standard Chartered • Ms. Anuradha Lipare, CISO • Ms. Smita Menon, Director, Capgemini • Mr. Vaidyanathan Iyer, COO IBM Cybersecurity Command Center
11:45- 12:00	Networking break
12:00 - 13:00	Correlational Analysis of Handwriting and Personality Aparna and Dr. Nootan, Write Strokes with Right Thoughts
13:00 -14:00	Lunch
14:00 - 14:45	Governance, Compliance, and Security in Cloud Ms. Shikha Saxena, Sr. Enterprise customer engineer, Google
14:45 – 15:30	**Fireside chat: "Digital Trust Transformation- Pushing the boundaries of audit"** Ms. K R Praveena, Senior Consultant & ED, MaGC Ms. Smitha Sathyanarayana, Internal audit & Risk analysis, SAP
15:30 – 15:45	Networking break
15:45 – 16:45	Wellness Being Ms. Jolly, Infosys
16:45 – 17:00	Ending note and vote of thanks

TIME(IST)	AGENDA (NEW OFFICE INAGURATION)
10:15 - 10:55	Registration and **Welcome Tea & Coffee Assemble in the Terrace**
10:55 - 11:00	Welcome remarks by the Master of Ceremony
11:00 - 11:20	**Inauguration** of SOLUS JAIN - Ribbon Cutting Ceremony by Mrs. Emily Bastedo in presence of esteemed members and building committee
11:20 - 11:25	**Lamp Lighting** & Invocation song
11:25 - 10:30	**Welcome Address** by ISACA BC President
11:30 - 12:00	Address/Remarks by group of invited Building Committee Members
12:00 - 12:30	**Keynote Address by** Mrs. Emily Bastedo, ISACA HQ (Chief Guest) - Global Government Relations and Public Affairs Director
12:30 - 12:40	Address by ISACA Regional Ambassador
12:40 - 13:25	**Address** by Vice President & recognizing Building Committee Members
13:25 - 13:30	**Vote of Thanks**
13:30 Onwards	**Lunch & Networking** **Assemble in the Terrace**

CROSS WORD



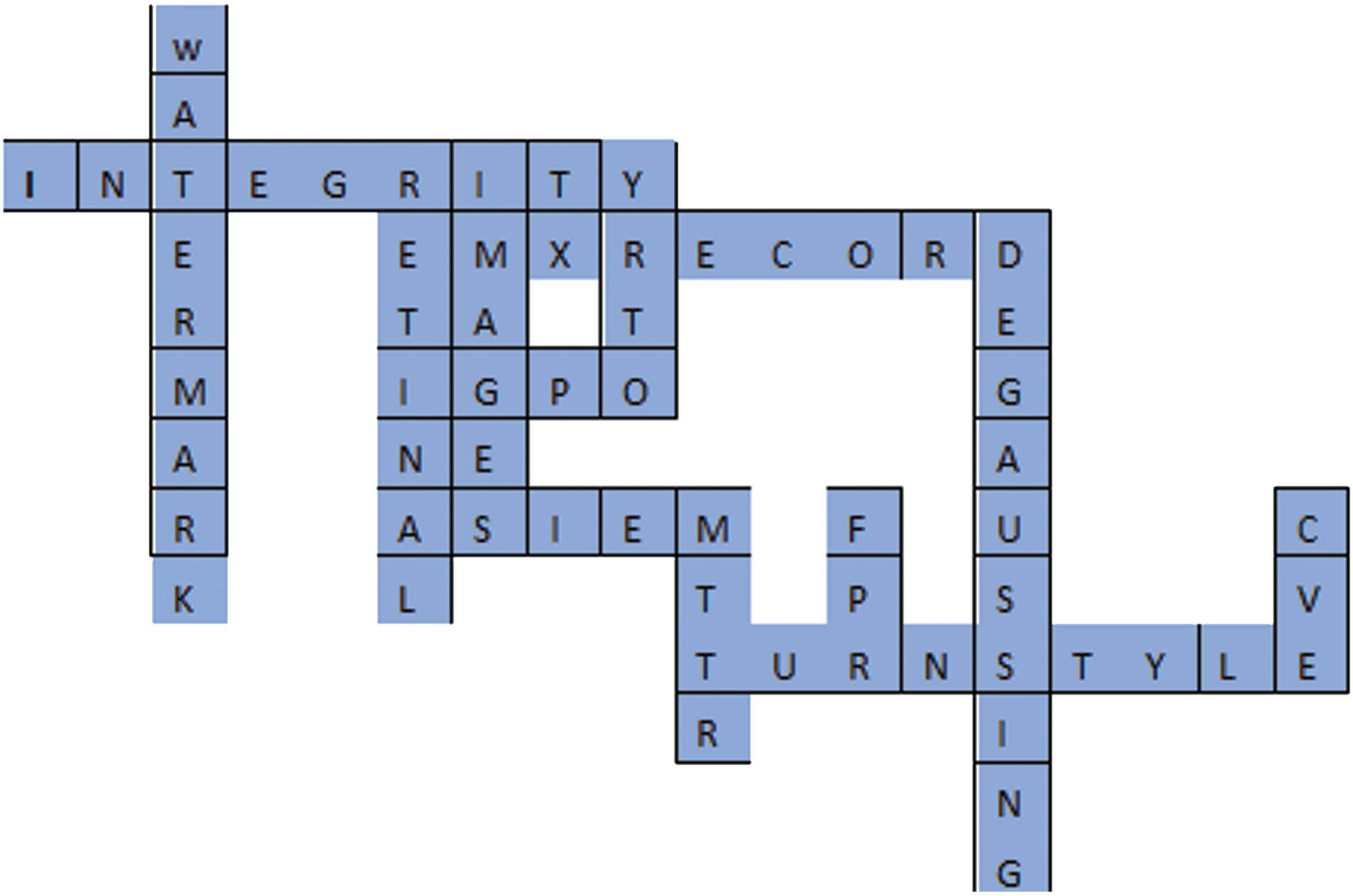
Across

1 ____ board
5 Being honest
7 Provides security to web and non web application
6 Low cost, but is it high enough quality?
8 "Critical element to consider when considering protection of customer's information"
10 "command that's used to find the path between two systems on a network entering a facility at a time"
11 Commonly used transport mechanism

Down

2 System design that duplicates components to provide alternatives in case one component fails
3 Method of making data transfers more secure
4 " computer and communications system"
9 Attack type very active in the pharmaceuticals and biotechnology industry
12 substance composed of two or more elements
13 ____UDP as its transport protocol.
14 IT Related

Answers for Q4 2022 crossword



ISACA
Bangalore Chapter

FREE STUDENT MEMBERSHIP

Make connections that will inspire and shape your future

Attention all students, for a limited period ISACA International will be waiving the US 25 student membership fee.

*Terms & Conditions apply

Become an ISACA student member, today!

ISACA is excited to invite you to join ISACA at no cost for the 2023 membership year. Joining ISACA will provide you with access to member-exclusive opportunities such as:

- Discount on world-renewed exam prep and certification fees
- Access to exclusive content and thought leadership.
- Access to our ISACA global network of 16K digital + professionals
- Access to the ISACA Mentorship Program
- Opportunity to network and learn with the local chapter & Free access to monthly CPE sessions.

Steps to enroll free 2023 membership:

- Confirm your college participation.
- Provide the number of students details who would like to enroll for free.

For more information contact – communications@isacabangalore.org

080-23377956/9886508515

ISACA®

Bangalore Chapter

26th Annual Karnataka Conference

A Hermit out of it's Shell:The Digitization ,Privacy, Cybersecurity & Current Threats.

Venu : The LaLiT Ashok Bangalore

Date : 28th & 29th Jul 2023

For Registration & more details
Watch out Chapter Website,Social Media channel & Communication

If undelivered please return to :

ISACA®
Bangalore Chapter

S-13, 2nd Floor ,Priya Chambers
Dr.Rajkumar Road, Opp. St. Theresa's Hospital,
2nd Stage, Rajajinagar,Bangalore-560010
Phone No:080-23377956
Email:chapter@isacabangalore.org

Solus Jain Heights
Unit No: B10, 10th Floor, 1st Cross.
J.C Road, Bangalore-560 002
Phone No:080-41514331

Printed @ Cauvery Ent. © 22128682

Chapter Reg No : 433/2002-2003