eForensics

VOL. 11
NO. 11

ISSN 2300-6986

BEST OF 2023

SENSORY-BASED **DECEPTION ATTACKS** TO THWART DRONE FORENSIC

HOW **AI COPILOTS** CAN **REVOLUTIONIZE** DIGITAL FORENSIC

DIGITAL FORENSIC ANALYSIS USING **AUTOPSY**

HOW **AI** AND **ML** CAN BE USED TO **COUNTER RANSOMWARE**

EDITOR’S WORD

Dear readers

We all eagerly anticipate New Year, as it provides us with the opportunity to spend precious time with our loved ones. We wish you all a wonderful and joyful season, filled with love and respect. Moreover, we hope that you are surrounded by warmth and peace. As we approach the start of a new year, we send our best wishes for success, hope, and courage in the year ahead. We hope that the coming year brings you exciting and life-changing experiences and that your dreams come true. We wish you a very Merry Christmas and a prosperous New Year!

Best regards,

Ewa Dudzic
ewa.dudzic@eforensicsmag.com

PS. As December comes to an end, we prepare to welcome January. This month, the two issues of eForensics will be released. The first issue, titled “The Best of 2023” is already out and available for reading. The second issue, focusing on satellite forensics, will be released in the last week of December. You can find a table of contents for this issue on the next pages, which includes 31articles about digital forensics. I highly recommend reading all of them, as they covervarious aspects of digital analysis and provide useful strategies and tools. You can become an expert in digital forensics and take your skills to the next level. So, have fun reading and expanding your knowledge!

EDITOR-IN-CHIEF
JOANNA KRETOWICZ
JOANNA.KRETOWICZ@EFORENSICSMAG.COM

ASSOCIATE EDITOR
EWA DUDZIC
EWA.DUDZIC@EFORENSICSMAG.COM

Cover Image
Wiktoria Bukowska

Cover Design
Wiktoria Bukowska

All trademarks, trade names, or logos mentioned or used are the property of their respective owners. The techniques described in our articles may only be used in private, local networks. The editors hold no responsibility for misuse of the presented techniques or consequent data loss.

DIGITAL FORENSICS ANALYSIS IN DEEPFAKE

CHIRATH DE ALWIS

Deepfake is a type of artificial intelligence (AI) that allows for the manipulation or creation of realistic-looking videos or images. It can be used for a variety of purposes, including entertainment, education, and research, but has also been used to commit cybercrimes such as identity theft, fraud, extortion, and spreading false information. Deepfake technology can be difficult to detect, making it a challenge for law enforcement agencies and digital forensics professionals to identify and prosecute crimes committed using it. To conduct a digital forensics investigation involving deepfake, professionals must identify the scope of the investigation, collect and preserve evidence, analyze the evidence, identify the use of deepfake technology, determine the authenticity of the content, and present the findings. Deepfake technology also has the potential to be used as a tool for anti-forensics, which is the practice of attempting to conceal or destroy evidence to hinder a forensic investigation.

What is Deepfake and How Does Deepfake Work?

Deepfake is a type of artificial intelligence (AI) that can be used to manipulate or creation of realistic-looking videos or images. It works by using machine learning algorithms to analyse and replicate the appearance and mannerisms of a person, allowing it to create convincing copies of their appearance or voice. The technology is based on a neural network, which is a computer system designed to mimic the structure and function of the human brain. The neural network is fed a large dataset of images or video clips of the person being copied, along with a set of rules or parameters for how the deepfake should be created. As the neural network processes the data, it learns to recognize patterns and features that define the person's appearance and mannerisms. It then uses this information to create a deepfake version of the person, either by altering an existing video or image, or generating a new one from scratch. Deepfake technology can be used for a variety of purposes, including entertainment, education, and research. However, it has also been used to commit cybercrimes, such as spreading false information, identity theft, and fraud. The technology is becoming increasingly sophisticated and can be difficult to detect, making it a challenge for law enforcement agencies and digital forensics professionals.

How Can Criminals Use Deepfake to Commit Crimes?

Criminals can use deepfake technology to commit a wide range of cybercrimes. Here are some examples of how they can use deepfake to commit crimes:

1. Identity theft: Criminals can use deepfake images to impersonate someone else and gain access to their accounts or steal their personal information. They may also create fake documents, such as driver's licenses or passport, using deepfake technology.

2. Fraud: Criminals can use deepfake videos or images to manipulate people into believing something that is not true. For example, they may create a deepfake video of a CEO making false statements, which could be used to manipulate stock prices or deceive investors.

3. Extortion: Criminals may use deepfake videos or images to blackmail or extort victims by threatening to release embarrassing or damaging content.

4. Spreading false information: Criminals may create deepfake videos or images to spread false or misleading information, such as propaganda or fake news. This can be used to influence public opinion or create chaos and confusion. Deepfake technology can be difficult to detect, making it a challenge for law enforcement agencies and digital forensics professionals to identify and prosecute crimes committed using deepfake. It is important for individuals and organizations to be aware of the risks and take steps to protect themselves from deepfake attacks.

How to conduct digital forensics investigations when criminals use deepfake

Digital forensics investigation is a crucial tool for uncovering evidence of criminal activity or misconduct involving digital devices, such as computers, phones, and servers. When a criminal uses deepfake technology to commit crimes, digital forensics professionals must follow specific steps to conduct an effective investigation. Here are some steps to follow:

1. Identify the scope of the investigation: Determine the type of cybercrime that has been committed, the devices involved, and the potential suspects.

2. Collect and preserve evidence: This involves seizing and securing all relevant digital devices and data, including computers, phones, servers, and cloud storage accounts. It is essential to follow proper forensic procedures to avoid contaminating the evidence.

3. Analyze the evidence: Use forensic tools and techniques to examine the data on the seized devices and identify any anomalies or suspicious activity. This may include analyzing log files, web history, email accounts, and social media accounts.

4. Identify the use of deepfake technology: Look for signs that deepfake technology has been used, such as inconsistencies in the appearance or voice of a person in a video or image. This may require the use of specialized software or consulting with experts in the field.

5. Determine the authenticity of the content: Use forensic techniques, such as analyzing metadata, pixel patterns, and audio frequencies, to determine whether the content has been altered or manipulated.

6. Present the findings: Use the evidence gathered during the investigation to build a case against the perpetrator and present it in court or to law enforcement agencies.

Conducting a digital forensics investigation when a criminal uses deepfake technology can be complex and time-consuming. However, by following these steps, digital forensics professionals can help uncover the truth and bring criminals to justice.

Role of Deepfake in Anti-forensics

Deepfake technology has the potential to be used as a tool for anti-forensics, which is the practice of attempting to conceal or destroy evidence to hinder a forensic investigation. Criminals can use deepfake to create fake or misleading evidence, making it difficult for forensic analysts to determine the authenticity of the content.

For example, a criminal may create a deepfake video of a victim confessing to a crime they did not commit, which could be used to mislead investigators or throw them off the trail. They may also use deepfake to alter or delete log files, emails, or other evidence to cover their tracks.

Anti-forensics techniques can be challenging to detect and counter, especially when they involve sophisticated technologies like deepfake. Digital forensics professionals must be aware of the potential for deepfake to be used as an anti-forensics tool and take steps to identify and overcome it. This may involve using specialized software or consulting with experts in the field to detect and analyze deepfake content. Overall, the use of deepfake technology for anti-forensics purposes highlights the importance of proper forensic techniques and procedures in digital forensics investigations. It is essential for forensic analysts to follow established protocols to ensure the integrity and reliability of the evidence they gather.

About the Author

Chirath De Alwis is an information security professional with more than 8 years' experience in the Information Security domain. He is armed with MSc in IT (specialized in Cybersecurity) (distinction), PgDip in IT (specialized in Cybersecurity), BEng (Hons) Computer networks & Security (first class), AWS-SAA, SC-200, AZ-104, AZ-900, SC-300, SC-900, RCCE, C|EH, C|HFI and Qualys Certified Security Specialist certifications. Currently involved in vulnerability management, incident handling, cyber threat intelligence and digital forensics activities in Sri Lankan cyberspace. Contact: chirathdealwis@gmail.com

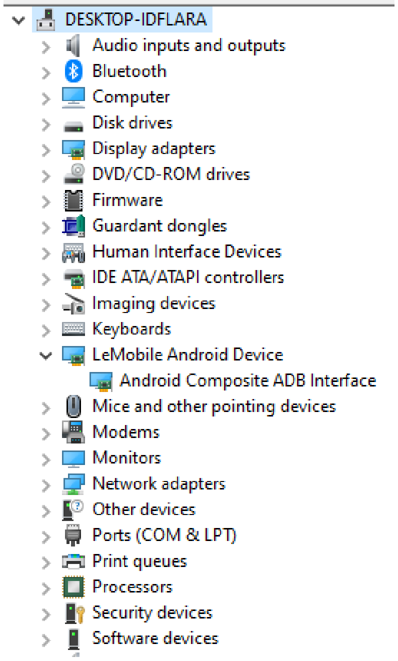
IMAGING AN ANDROID SMARTPHONE LOGICALLY

AMBER SCHROADER

There are a variety of imaging techniques available when you work with smartphones. With most acquisitions, we rely on logical acquisition techniques to get our evidence. As this is a well-known technique, it is always good to review the logical image procesing.

Android devices, when doing logical imaging, can need some coaxing to get them to where they are going to communicate with your forensic workstation. Android has a large variety of devices as well as different versions of Android itself. When you look at the setup steps, they are typical for Android, Android Oxygen, and Android Go.

When working with the Android device, remember if your forensic workstation cannot see it, neither can your tool. One of the tips I find helpful is to keep the Device Manager open when working with an Android. This allows you to see the device from the workstation's perspective and how it is being loaded into the operating system.



```
DESKTOP-IDFLARA
  Audio inputs and outputs
  Bluetooth
  Computer
  Disk drives
  Display adapters
  DVD/CD-ROM drives
  Firmware
  Guardant dongles
  Human Interface Devices
  IDE ATA/ATAPI controllers
  Imaging devices
  Keyboards
  LeMobile Android Device
    Android Composite ADB Interface
  Mice and other pointing devices
  Modems
  Monitors
  Network adapters
  Other devices
  Ports (COM & LPT)
  Print queues
  Processors
  Security devices
  Software devices
```

Figure 1-Windows Device Manager with an Android LeMobile Android Device loaded for processing.

UNUSUAL EMAILS: INVESTIGATING

JEFF MINAKATA

For this article, we will be performing an OSINT investigation on an email that was sent to see what information we can find by verifying parts of the email's content. This is a scenario based on real email investigations. As with any investigation, I do recommend exercising precaution (use a VM, sock puppet accounts, VPN, etc.). In terms of this article, you can assume that the previously mentioned precautions are already being exercised. For this article, we will be using the fictional email: *oddemail@webdomain.com*.

Figure 1. Investigation clipart

Figure 2. E-mail clip art

How to Better Prepare for a Memory Forensics Investigation

Bunde Collins

Memory forensics is an investigative technique that involves finding and extracting raw forensic artifacts from computer RAM (Monnappa, K. A. 2018). The RAM stores valuable information about the runtime status of a system. Hence, acquiring a memory dump is crucial in revealing important information during an investigation exercise. It provides details on the existing network connection, registry hive modifications, process handles, loaded modules as well as kernel drivers, among others. For a long time, the Random Access Memory was overlooked as a bane for forensic artifacts, most forensic analysts focused their investigation solely on the evidence in the hard drive (Johansen, G. 2017).

In recent times, memory forensics has become a valuable investigative technique during digital forensics and incident response. According to Monnappa, K. A. (2018), it can also be used to complement malware analysis by helping to gain proper context into the malware behavior post-infection. In the wave of changing technological disruption, memory forensics has become more challenging as the operating systems, software, and hardware architectures keep evolving. However, there is always room to level up your skills and expertise despite the rapid technological advancement. Importantly, an understanding of the basics of the fundamentals is always a step in the right direction.

This article will provide insights on how to better prepare for memory forensic investigation by touching on memory forensics methodology, customizing a toolkit manager, and reviewing the current challenges in memory forensics.

Methodology for Memory analysis

While preparing for a memory forensics analysis, and in order to uncover potential evidentiary artifact material for an investigation, it is important to follow a methodology. Methodologies may exist in various forms but are always dependent on the incident type.

It is important to follow a memory forensics analysis process, since a secure and proven methodology would ensure collected data or artifacts are valid in the investigation process. Investigation methodologies may vary based on the specific incident.

iPhone Forensics

Kate Libby

Have you ever wondered what happens to all that data you interact with on your iPhone? I mean, where does all that data go or, a better question should be, where did this data come from? Since the early 2000s, few devices have earned the cult following as the iPhone did since its introduction. Ever trending upwards in demand, a few sources suggest that there are as many iPhones in the world as there are leaves on the ground. You should take that assumption with a pinch salt; however, according to one source, there are more than 2.24 billion iPhones in existence - now that is a lot of data being transmitted.

With the increasing popularity of the iPhone, its use in nefarious activities has also increased. This has resulted in the need for security professionals and law enforcement agencies to use the latest forensic techniques to investigate and uncover evidence stored on these devices. On the surface, iPhone forensics is the process of extracting and analyzing data stored on Apple iPhones. This data can include text messages, emails, call logs, and other information stored on the device. As we get into the finer details of these forensic techniques, the path to evidence discovery is often shrouded in complex encryption algorithms and secure cloud storage.

Another problem with the popularity of this device is that it is not just consumers that drive the market share. It is also a favorite device for criminals, as it can be used to store sensitive information and secretly communicate with other personnel within the network. Because of this, the iPhone has become a target for international and domestic law enforcement agencies, who must investigate and uncover evidence stored on these devices. In order to carry out a successful iPhone investigation, these agencies and investigators must have a thorough understanding of the device and the data it contains. This includes understanding the operating system, hardware, file system, and software of the device, as well as the various data types that can be found on it. Since the 90s, Apple has used a Hierarchical File System and other advancements in data handling in order to protect user data, not to mention the ability to use passkeys in a recent iOS update. Combined, all of this makes forensic investigations much more difficult, especially if the current advancements are not tracked properly.

The Basics of iPhone Forensics

The process of iPhone forensics can be complicated and time-consuming, but there are many tools available to help with the analysis. It is important to use the right tool for the job, as each tool is designed to work with specific versions of iOS. In addition, it is important to have a good understanding of the iPhone’s hardware, as this will help in understanding the data stored on the device.

The first step in an iPhone investigation is to acquire the device and perform a physical extraction of the data. This involves connecting the device to a computer or sandbox appliance and using a forensic tool to acquire the data. This can be done by using a USB cable, Firewire cable, or a specialized forensic tool.

Using Neural Networks to Protect Systems Against Phishing Attack Vulnerabilities on iOS Platforms

Rhonda Johnson

With the increasing threat of cyberattacks threatening the security of personal data, innovative methods of detecting malicious user behavior have been a top priority. One of the most pressing security issues today is phishing, which can significantly threaten mobile devices, including those running iOS. However, with the application of neural networks, identifying phishing attempts on iOS operating systems is possible. This article will explore the possibilities provided by applying neural networks.

Phishing is a social engineering technique cybercriminals use to obtain unauthorized access to computer systems and sensitive information, such as passwords, credit card numbers, or social security numbers. Attackers deceive users using legitimate-looking communications such as instant messages, social media, e-mails, or websites that trick the user into providing login credentials and other sensitive personal information. Kaur et al. (2021) note that phishing attacks remain a significant threat to cybersecurity at the individual and organizational level due to the rapidly evolving sophistication of phishing attacks.

Neural networks, on the other hand, are a class of algorithms that work like the human brain's neural structure in that it learns from input data and makes predictions or decisions based on the learning (Zhang et al., 2020). Neural networks have advanced research in several areas, such as natural language processing, speech recognition, and image recognition. However, neural networks can also be used for cybersecurity tasks such as identifying and preventing phishing attacks in iOS operating systems by analyzing the behavior of end users.

Yadav and Reddy (2019) noted that neural networks effectively detect phishing e-mails by analyzing the content, sender, and formatting of suspected e-mails. Content attributes, such as certain words and phrases, URL links or attachments, and how similar the phishing e-mails are to previous e-mails, are used in the neural network training set. With over 95% accuracy in classifying new e-mails as phishing attempts or legitimate, neural networks have shown some promise in phishing detection.

ROOTING ANDROIDS FOR FORENSICS

AMBER SCHROADER

When you look at the different imaging options for Android devices, you cannot ignore the value of getting root. Root-level access allows you more access to the device's data. If you have read the prior article about logical imaging with Android devices in forensics, you probably noted that app access can be very limited. This obstacle is not there when root is acquired. If the time for research and rooting is available, it is highly recommended that it be added to the Android process steps.

Let’s start out by making sure we understand what the root is. The root is the level of access or control of a device. In general, it is the highest permission level on the device, and sometimes it is referred to as the “superuser.” The root is typically reserved as a method to protect the primary file system of the device from damage or malicious access. When looking at the root, there are a lot of different methods out there that can help you through this process. It is important to note that most of the root methods are not designed for digital forensics, but are designed, so consumers can gain greater access to and control of their devices.

Once you understand the root, you might wonder how it can be used in smartphone forensics and still be considered as a forensic method. That is where the implementation and the documentation play a strong role in your investigation.

When using root and looking at the implementation, the best option is to do root process through a forensic tool. That way, the method, and record of what you are doing, become part of the operational steps that should be recorded with every examination. In the following example, you can see what is done with rooting inside the Paraben E3 Forensic Platform using a third-party root. Note that many tools, including the E3 Forensic Platform, also have rooting options that are internal to the tool. However, as the device changes, understanding how to use third-party rooting options can be valuable. A third-party rooting option is done by the community of Android developers, and that community can make swift changes and innovations faster when it comes to rooting than the forensic tool developers.

In the following example, we will use a Samsung Galaxy On5. Rooting this device, we will be using Odin with a Twrp.tar, then acquiring the data using the E3 Forensic Platform.

There are a couple of important procedural notes when rooting the device. This is not a method that can be done if the device is locked, as you must have access to certain settings on the device to have the root be successful. First, you must have the device in USB debugging mode. This mode can be found in the settings area of the device.

The Human Element: an Analysis of the Relationships Between Social Engineering and Ransomware Attacks

Sergio Figueiredo & Fabiana Botton

Over the last twelve years, ransomware attacks have been growing globally. As a result, the cybersecurity community considers them one of the most threatening operational and financial risks to various organizations in different sectors. Although the technical aspects are critical to understanding the threat, we should also consider social engineering skills and techniques to address this problem correctly. To understand how the human element is exploited, this article aims to present an overview of ransomware and social engineering, discussing their relationship and focusing on how the human factor can be used as an agent to exploit becoming an attack vector.

Introduction

In April 2022, Costa Rica's government suffered a cyberattack that significantly affected government agencies, disrupting their services and operations. A couple of months later, another cyberattack hit the country in May, and the healthcare system was the most severely affected. What do those incidents have in common, apart from the victim? They were ransomware attacks.

Although ransomware attacks are nothing new, nowadays, this type of attack has become a global threat, even if some countries are more affected than others, with a threat landscape that is constantly changing. Gaining traction in 2020, the threat actors modified their operating model to allow more criminals, regardless of technical expertise, to be part of the big game, which made highly-advanced malware available to low-skilled mercenaries [1]. Inspired by the gig economy movement, some have a 24/7 customer helpdesk, ethics code, and third-party source-code reviewers.

This modus operandi is called Ransomware-as-a-Service (RaaS) and social engineering plays a significant role in this model. Phishing and its variations are often employed by ransomware groups to attract users to click, run a program, or proceed with malicious operations. Threat actors take advantage of social situations, interests, holidays, and major events to create scams directed at different topics to spread and leverage your attacks. Such happened during the Covid-19 pandemic period or, more recently, with the World Cup in 2022, for example, which drove a massive collective desire for information.

Ransomware Investigation: The New Challenges

Paulo Pereira, PhD

The term ransomware is used to define a type of artifact that encrypts files and folders of an operating system, in most cases Windows, but not exclusively this system. A few years ago, this artifact was delivered as a file only. Today, there is cloud infrastructure and servers for hire on the dark web and deployment is known as “ransomware-as-a-service” (RaaS). As the cloud service enables multiple ransomware deliveries, reuse of code from other ransomware is common. For this reason, it is interesting to analyze the artifact to verify if it belongs to any already detected ransomware family.

Evolution of Attacks

Unit 42’s 2023 report reveals an evolution in ransomware attacks with the expansion of the social engineering blackmail technique that attackers are using to target specific C-Suite team targets and continue with financial extortion.

This is a change in the behavior of the groups of attackers who, previously, negotiated the extortion of the victims until the moment of decrypting the compromised files. However, the trend for the coming years is for these groups to continue with extortion even after the encryption stage of the files and the ransom demand, trying to denigrate the company’s image by exposing the stolen data.

Another aspect is the denial-of-service attack built into ransomware. According to Liska and Gallo (2017, p.16), “ransomware is an umbrella term used to describe a class of malware that serves to digitally extort victims, making them pay a specific price.”

Attacks carried out using ransomware have also evolved in this period. Sobers highlights the average growth of RaaS (Ransomware as a Service) since 2019: “Ransomware-as-a-service, or RaaS, is a subscription that allows affiliates to use ransomware tools already developed to carry out ransomware attacks. It also allows them to extend their reach and the decentralized nature of the attacks makes it difficult for the authorities to end the attack. […] The creators of these tools receive a percentage of each successful ransom payment. As the average ransom demanded by hackers has increased by 33% since the third quarter of 2019 ($11,605), affiliates are earning up to 80% of each payout. (SOBERS, 2021)”.

In this sense, the greater the unpreparedness to respond to an incident of this nature, the greater the impact on business continuity. Morgan (2020, n.p.) estimates that the costs of cybercrime will grow by an estimated 15% per year until 2025, becoming the third economy, behind only the economies of China and the United States; a financial transaction that reaches the annual figure of approximately 10.5 trillion dollars, much higher than the US$ 3 trillion recorded in 2015. According to the author, the costs of cybercrime include:

Sensory-based Deception Attacks to thwart Drone Forensic Investigations

Rhonda Johnson

In this article, sensory-based deception attacks that hinder drone forensic investigations will be discussed. Sensory-based deception attacks on drones are attacks that manipulate a drone's behavior by feeding deceptive sensory information. Sensory-based deception attacks can pose a severe challenge for drone forensic investigations. Drone Forensics is the process of collecting and analyzing digital forensic evidence from drones to determine how they were used, who operated them and what actions were performed using traditional forensic techniques to extract data and any associated systems such as GPS devices, cameras, and communication systems. Mainly, these attacks aim to interfere with the sensory systems of a drone by disrupting the signals that the drone uses to navigate and collect data. Attackers can achieve these objectives through various means, such as using bright flashes of light or loud noises to overload the drone's sensors or creating false signals that mislead the drone's navigation system.

The use of deception sensory attacks in recent years has grown in popularity, as drones are increasingly used in sensitive areas such as military zones and critical infrastructure. Attackers can use these tactics to make it difficult or impossible for investigators to collect forensic evidence, ultimately hindering their ability to identify the source of the attack and bring the responsible parties to justice. Malicious actors, such as hackers, terrorists, or criminals, can exploit drones' vulnerabilities to manipulate their sensors and confuse forensic investigations. The sensors on a drone are responsible for collecting data and transmitting it back to the operator or storage unit. Depending on the drone's purpose, they include GPS, cameras, microphones, accelerometers, gyroscopes, and other specialized sensors.

Here are some ways malicious actors can deceive sensors in a drone to thwart forensic investigative tools:

GPS Spoofing

GPS is an essential sensor in drones, enabling them to navigate and maintain stability in the air. However, GPS signals are vulnerable to spoofing. A hacker can used advanced software tools to create a fake GPS signal to trick the drone's GPS receiver into thinking it's in a different location, which can cause the drone to fly off course, crash, or land some place other than intended, making it difficult to retrieve and analyze. GPS spoofing attacks can be designed to be very targeted, affecting only a single drone, making it even more challenging for investigators to identify the attack.

Ransomware Attacks in the USA: Statistics Data Analysis

Paulo Pereira, PhD

Freak out
And give in
Doesn't matter what you believe in
Stay cool
And be somebody's fool this year
'Cause they know
Who is righteous, what is bold
So I'm told
Who wants honey
As long as there's some money
Who wants that honey?
(Cherub Rock, Smashing Pumpkins)

Attackers' strategies

This article focuses on statistical data published by Wright (2023) to make an analysis of ransomware attacks between January and February 2023 in the United States, highlighting which cities and sectors were affected during this period.

One of the most important factors in the growth of ransomware attacks in the last two years is the adoption of two strategies: affiliation and pay-for-return. Such strategies are being adopted by the groups that create ransomware. Once created, ransomware becomes a commodity that is offered in a relationship that is not limited to buying and selling: it creates an affiliation between the ransomware creators and those who will use the ransomware in attacks. In addition, the scheme of offering payment to these users is made according to the success rate of an attack. A reward for the use of the artifact.

The LockBit Ransomware emerged on the malware scene in September 2019, when it was offered in a RaaS (Ransomware-as-a-Service) scheme. The threat operators looked for affiliates who would carry out the actual ransomware attacks and then split the profits: the affiliates would withdraw about 70-80% of the funds, while the rest would be handed over to the creators of LockBit.

Ransomware's Effect on Critical Infrastructure Security

Greg Kipper

Ransomware is a type of malicious software that encrypts data or systems and demands payment from the victim in exchange for the decryption key or to prevent the public release of stolen data. This type of attack has grown exponentially over the past five years, with a substantial increase in both the frequency and sophistication of attacks. The risk of ransomware attacks on industrial control systems (ICS) is significant and can have severe consequences for critical infrastructure and industrial operations. Industrial control systems are a type of computerized system that is used to monitor and control industrial processes or critical infrastructure. They are designed to manage and automate tasks in industries such as manufacturing, energy, transportation, and water treatment, among others, and are often interconnected and rely on computer networks, software, and hardware components to operate, making them vulnerable to ransomware attacks.

The Five Major Risks

The first risk is operational disruption. Ransomware attacks can disrupt the normal operation of industrial processes by encrypting critical data, systems, or applications. This type of disruption can lead to production downtime, reduced productivity, loss of revenue, and increased costs for organizations that rely on ICS for their operations. The impact can be particularly severe in industries with continuous or time-sensitive processes, where even short periods of downtime can result in significant financial and reputational losses.

There have been several notable examples of ransomware attacks causing operational disruption to industrial control systems (ICS) in recent years. Some of these incidents have resulted in significant financial losses, production downtime, and safety risks. Below are two recent examples:

Colonial Pipeline ransomware attack in 2021

The Colonial Pipeline is a major fuel pipeline operator in the United States. In May 2021, the company fell victim to a ransomware attack that disrupted its operations. The attackers encrypted critical systems, including those used to control the pipeline's operations, and demanded a ransom for the decryption key. As a result, Colonial Pipeline had to shut down its pipeline operations for several days, leading to fuel shortages, price spikes, and significant disruptions to the fuel supply chain in the eastern United States.

THE POPULARITY OF RANSOMWARE ATTACKS: UNDERSTANDING WHY HACKERS USE THEM WITH CASE STUDIES

KALPA KALHARA SAMPATH

Ransomware is a type of malicious software (malware) that encrypts the victim's data, rendering it inaccessible until a ransom is paid to the attacker, usually in cryptocurrency. Ransomware has a long history, with the first known attack dating back to 1989, when the "AIDS Trojan" spread via floppy disk and demanded payment by snail mail. However, it wasn't until the mid-2000s that ransomware became a significant threat, with the emergence of encrypting ransomware, which made it much harder to recover data without paying the ransom. Since then, ransomware attacks have grown in frequency and sophistication, with high-profile attacks on companies, hospitals, and governments, making it one of the most significant cyber threats of our time.

Ransomware attacks typically occur when a user clicks on a malicious link or attachment in an email. Once the ransomware is installed on a computer, it begins encrypting files. The encryption process can take several hours, and during this time, the victim may be unable to access their files. Once the encryption process is complete, the ransomware will display a message demanding a ransom payment. The ransom payment is typically demanded in a cryptocurrency, such as Bitcoin, which makes it difficult to trace.

There are many types of ransomware attacks, but they all share the same basic goal, to encrypt a victim's files and demand a ransom payment in order to decrypt them. Some of the most common types of ransomware attacks include:

- **Crypto ransomware:** This is the most common type of ransomware attack. Crypto ransomware encrypts a victim's files and demands a ransom payment in order to decrypt them. The ransom payment is typically demanded in a cryptocurrency, such as Bitcoin, which makes it difficult to trace.

Examples:- WannaCry, CryptoLocker, Petya, Maze, NotPetya

RANSOMWARE PHISHING ATTACKS

JEFF MINAKATA

Figure 1. Computer virus

Imagine sitting at work or home when you get an alert that you have a new email. It can be from a friend, co-worker, box, family member, etc. As you open your email, you find a link or a PDF file and then…

AI Powered Ransomware Protection

Kate Libby

Problem

Ransomware has become an increasingly common and severe threat to organizations and individuals alike, and even more dangerous is artificial intelligence (AI) powered ransomware attacks. These attacks involve the encryption of data by cyber criminals who demand payment in exchange for a decryption key, often leaving victims with no choice but to pay a ransom to regain access to their own files, and quite often they are not honored, leaving the user unable to retrieve their data at all. While there are many ways to mitigate the risk of ransomware attacks, one promising solution making serious strides is the use of AI automation.

Artificial Intelligence Automation

AI refers to the development of computer systems that can perform tasks that typically require human intelligence, such as learning, reasoning, and problem-solving. These computer systems are designed to mimic human cognitive abilities, including perception, recognition, and decision-making. Some recent and very well-known examples are Open AI's ChatGPT and Microsoft's AI that has been integrated into Bing. If you have used any of these platforms, then you have probably experienced some of the scary capabilities and shortcomings.

AI is already used in a wide range of applications, including image and speech recognition, recommendation systems, autonomous vehicles, fraud detection, and predictive analytics. AI technology continues to advance and is expected to have a significant impact on a variety of industries, including healthcare, finance, education, manufacturing, and transportation, so it's a no brainer to implement this technology into ransomware mitigation and recovery.

AI automation can help prevent ransomware attacks by detecting and responding to them quickly and efficiently, more so than its human counterparts. AI-powered systems can monitor network activity in real-time, detecting unusual or suspicious behavior that may indicate a ransomware attack is underway. This can include unexpected access to files or attempts to modify data in unauthorized ways.

CLOUD STORAGE AND CJIS COMPLIANCE IN THE U.S.

CHRISTOPHER COLLINS

In May of 2023, I published research that focused on the use and applicability of cloud storage for digital evidence titled *"Cloud Storage & Digital Forensic Evidence",* which can be found here: https://revo4n6.com/docs. In this research, I outlined several security standards, with specific compliance and certifications requirements for digital evidence cloud storage. One of the biggest questions posed by industry leaders in the cloud storage and computing realm is how does the Federal Bureau of Investigations' (FBI) Criminal Justice Information Services (CJIS) Security Policy apply to digital evidence being stored in the cloud? Without a clear certification process, this leaves the Cloud Service Provider industry in uncharted territory as to what's required by them. This article will focus on Cloud Storage Provider requirements when hosting digital evidence specific to Criminal Justice Information.

There are numerous security standards and certification levels that cloud service providers (CSP) can obtain such as the Federal Information Processing Standards (FIPS), National Institute of Standards and Technology (NIST), Department of Defense Cloud Computing Security Requirements Guide (DoD SRG), and the Federal Risk and Authorization Management Program (FedRAMP). All of these security standards have some form of compliance certificate or methods of validation that can be readily accessible by a potential client, while CJIS does not.

I began looking into the CJIS Security Policy Version 5.9.2, released 12/07/2022, to really dive into how this policy affects cloud storage, digital evidence, and the burden placed on the client and CSP.

I highlight what information is a concern in the CJIS Security Policy. In the first paragraph of the Executive Summary, it reads *"… the CJIS Security Policy contains information security requirements, guidelines, and agreements reflecting the will of law enforcement and criminal justice agencies for protecting the sources, transmission, storage, and generation of Criminal Justice Information (CJI)."* This means that the CJIS Security Policy is only concerned with what the policy defines as Criminal Justice Information (CJI).

The purpose of the CJIS Security Policy is defined in Section 1.1 of the policy as it provides Criminal Justice Agencies (CJA) and Noncriminal Justice Agencies (NCJA) with a minimum set of security standards to access CJIS systems and data for information protection and security.

ENGAGING SOCIAL ENGINEERING: EXTRACTING INFORMATION THROUGH STRATEGIC INTERACTIONS

D4RKR4BB1T47

*Editorial note: We decided to remove any and all last names from the examples section as to not be drawn into any potential legal disputes. In the place of any last names, you will find "*****"*

Throughout this process, it is important to exercise restraint; failure may result in a backfire of your own method. The method aims to anger or cause great sadness in the target and extract information. Remember, it's not illegal to gaslight or purposefully annoy the threat actor. It is crucial to approach this technique responsibly, ensuring that the methods are employed with good OPSEC and skill.

By employing these aggressive social engineering tactics, you can potentially gather key details about the target's operations, infrastructure, and, potentially, even their associates. However, it is essential to emphasize that this approach should only be utilized within a safe working environment and with thorough understanding of the potential consequences if you fail.

In conclusion, aggressive social engineering through gaslighting and argumentation can be a powerful method for gathering information from individuals engaged in criminal activities. However, it should be noted that your targets most likely are going to use every threat but most fall through. Show no weakness and continue on strong.

Real World Examples (A Treat for you readers)

Sheriff the Colonial Pipeline hacker AKA Alexander: this fool came out of hiding post-lockbit ban (see sickkids(.)ca hack) only to admit to open air with a hired person in breach forums shoutbox he came out of the hiding because of me... this wasn't the worst part, He also went on to admit he was in AVOS, not even a month later? AVOS hits a hospital... what a surprise? He comes out, exposes his currant affiliation and hacks a hospital (This dude is extensively doxed btw) I planned to mention "Springwood Hospital" but this is a rather harsh topic and I'm not trying to traumatize you if you wanna google it, Happened in 2019.

Docker Forensics Secrets within Containers

Kate Libby

Introduction

Docker has revolutionized software deployment by enabling the isolation of applications within containers. While this technology offers numerous benefits, such as keeping code out of production environments, it also presents new challenges in terms of security and forensics, especially in the aftermath of a ransomware or cyber-attack. On the surface, Docker forensics refers to the process of investigating Docker containers to uncover evidence and gain insights into potential security breaches or malicious activities. However, it is more complex than that.

The goal of this article is to explore the key concepts, challenges, and techniques involved in Docker forensics, highlighting its importance in modern-day digital investigations and some of the tools involved.

Understanding Docker Containers

Docker containers provide a lightweight, portable, and isolated environment for running applications. Each container encapsulates the application, its dependencies, and the underlying operating system, making it self-contained and easy to replicate. Containerization also allows developers to study how a piece of software, or a quality update, could affect the application that is currently in production. However, these characteristics also make containers an attractive target for attackers or a potential hiding place for bad actors planning malicious activities. Docker forensics involves understanding the internal workings of containers, their file systems, network configurations, and runtime artifacts to uncover valuable evidence during an investigation. These forensic activities do have some uphill challenges that exist naturally within the docker ecosystem.

Challenges in Docker Forensics

Docker forensics presents unique challenges compared to traditional digital forensics. Firstly, the temporary nature of containers poses a significant hurdle. Containers can be created, modified, and destroyed rapidly, potentially leading to the loss of critical evidence, which is often the case. Secondly, the layered architecture of Docker images adds complexity to the forensic process, as each layer may introduce additional artifacts or hidden data, such as slack space or the lack of.

Safeguarding Remote Video Identification: A Look at Drone Cybersecurity

Rhonda Johnson

Unmanned aerial vehicles (UAVs), commonly known as drones, have revolutionized various industries, and one of their critical applications is remote video identification. This technology enables real-time monitoring of distant locations, providing invaluable assistance in fields such as law enforcement, disaster response, and infrastructure inspection. However, as the use of drones for remote video identification grows, the importance of drone cybersecurity becomes increasingly paramount. We examine drone cybersecurity in the context of remote video identification in this article, supported by recent news items and statistics.

The Significance of Remote Video Identification

Remote video identification allows for the identification of objects, individuals, and incidents from a distance using drones equipped with high-resolution cameras. Its applications are far-reaching, such as tracking criminal activities, monitoring remote areas, and conducting search-and-rescue operations. For instance, in law enforcement, it aids in the identification of suspects and helps protect officers by minimizing direct engagement. Moreover, during public health crises like pandemics, drones can monitor public spaces, ensuring adherence to safety protocols while preserving privacy. The potential benefits are immense, but they come with cybersecurity challenges.

Understanding Drone Cybersecurity

Drone cybersecurity involves safeguarding drones, their communication systems, and the data they collect from unauthorized access and cyber threats. As drones increasingly connect to the internet and operate within IoT networks, the risk of cyberattacks rises. Attackers can exploit vulnerabilities in communication channels, data storage, and authentication protocols to hijack drones, intercept sensitive data, and compromise operations. Ensuring robust drone cybersecurity is vital to prevent the misuse of surveillance data and protect against malicious intent.

Remote Video Identification

Kate Libby

In today's digital age, remote video identification has emerged as a powerful solution for verifying the identity of individuals without requiring their physical presence.

This technology has applications in various industries, such as government, finance, healthcare, telecom, and intelligence services, just to name a few, revolutionizing processes, such as account onboarding, passport identification, remote transactions, and customer support. The technology combines document verification, face recognition, and liveness detection techniques. Remote video identification offers enhanced security and efficiency, especially in the aspect of remote or security work activities.

In this article, we will explore the technologies and methods used in remote video identification and examine their impact on different sectors.

Document Verification and Analysis (Scenario)

Remote video identification typically begins with document verification. Users are required to present official identification documents, such as passports, driver's licenses, or ID cards. Advanced Optical Character Recognition (OCR) technology is employed to extract information from these documents.

OCR algorithms analyze document images, extract data from specific fields, and verify its authenticity by comparing it against known templates or databases of accepted documents.

Furthermore, machine learning algorithms are used to detect any signs of tampering or forgery (sciencedirect.com, n.d.), such as a missing watermark, ensuring the integrity of the identification process.

There are numerous organizations offering remote video verification services, some with apps and some without them. In this article, we will be looking at a few of the companies that offer this service. We will start with Jumio.

Jumio offers a variety of services that companies can take advantage of based on the needs of their organization. Whether it’s ID verification or ongoing monitoring, Jumio has it covered with their patented app. (justia.com, n.d.)

ENISA Video Remote Identification Guidelines

Paulo Pereira, PhD

This article presents the topics debated in *Remote Video Identification: Attacks and Foresight Workshop* held by ENISA (European Union Agency for Cybersecurity) on last 10 May 2023 and in the report *Remote Identity Proofing: Attacks & Countermeasures*, published in 2022. In recent years, the expansion of video cameras scattered throughout the streets of cities and inside buildings has had a great growth. Certainly, with this demand, the exposure of information recorded in these videos became the target of cyber attackers interested in gathering such information to blackmail people and companies and sell possible secrets contained in the images.

Key Takeaways

The resulting report of the Workshop[1] shows four important pillars that need immediate implementation, among the main discussions on security against unauthorized access to videos:

Remote Identity Proofing Attacks:

- Multiple remote identity proofing allowed by the same SB,
- Need of a harmonized regulatory framework regarding remote identity proofing testing and certification,
- Challenges to sectorial enforcement and supervision include the absence of legislation at national level and a skills gap,
- Innovative identification methods may be available in 2 years.

National implementations:

- Deepfakes are a major concern,
- AI perceived as a game changer, injection attacks introduce persistent threats to biometrics systems and are on the rise due to scalability,
- eIDAS 2.0 to provide high levels of assurance.

Good Practices for Remote Identity proofing:

- A dynamic approach, rather than static, is needed for auditing purposes,

[1] Source: https://www.enisa.europa.eu/events/remoteidentity_workshop_amsterdam2023/remote-id-workshop-amsterdam-briefing.pdf

Breaking Weak Implementations of VPN Encryption and the Role of Entropy Levels

Kate Libby

In the modern era, having the ability to work remotely, maintaining solid data security and privacy are paramount. Virtual Private Networks (VPNs) have become essential tools for safeguarding sensitive online communications. VPNs provide a secure and encrypted tunnel between a user's device and a remote server, ensuring that data remains confidential and protected from potential threats. However, not all VPNs and implementations are created equal. Weak implementations of VPN encryption can expose vulnerabilities that malicious actors can exploit, compromising the very security they are intended to provide. In this article, we delve into the intricacies of breaking weak implementations of VPN encryption and explore the pivotal role that entropy levels play in bolstering cryptographic strength.

To commence our exploration of breaking VPN encryption implementation, we initiated our own in-house VPN system utilizing the well-regarded OpenVPN framework. Our approach involved steering clear of any commercial or enterprise-level VPN setups in production environments, to avoid any potential risks or service disruptions. Our actions aimed to maintain caution while being confident that, given the vulnerabilities in commercial systems and weak implementations, we could attain results that are remarkably similar.

While more significant efforts have been channeled into reversing through proxies as opposed to VPNs, it was our experiment with proxies that paved the way for our investigation using a custom-created VPN within a controlled laboratory environment.

The primary objective of our experimentation, considering that we are not cryptography experts by profession, revolved around identifying and capitalizing on vulnerabilities within the implementation itself. While ample computational power such as quantum could potentially be harnessed to exploit weaknesses inherent to a more robust algorithm, our specific focus for this examination was on exploiting vulnerabilities arising from the implementation aspect. Below are some screenshots from the disassembly of the Ovpn file.

Unraveling Digital Mysteries: How AI Copilots can Revolutionize Digital Forensic Investigations

Hans Henseler

In hindsight, 2021 was a significant inflection point in the world of artificial intelligence, characterized by remarkable developments in deep learning, manifesting in models such as DALL·E, CLIP and in models that were surpassing GPT-3 in size and ability. These advancements hinted at a future not limited to machines performing computational tasks but also emulating intricate human-like activities. However, it was November 2022, with the emergence of ChatGPT, that the world glimpsed a truly transformative tool, suggesting potential applications even in niches like digital forensics [1,2].

Yet, the digital forensics community, by and large, has yet to fully embrace or debate the profound implications of these advancements. Every case in digital forensics presents its own universe of data, sourced from confiscated devices, cloud accounts, and other digital touchpoints. Parsing through this enormity, especially with looming backlogs in forensic labs and the aspirations to involve detectives without specialized forensic training, demands a radical rethinking of our tools and approaches.

Instead of merely focusing on the limitations or potential pitfalls of Large Language Models (LLMs), we ought to explore their promise. Retrieval-Augmented Generation (RAG) is one such promising frontier. By coupling real-time data retrieval with the robust capabilities of generative models, RAG offers a compelling case for the next evolutionary step in digital forensics. This article emphasizes not just the challenges but also the transformative potential of AI for forensic experts and investigative detectives alike.

Understanding the gaps in LLMs

GPT-4 and ChatGPT are heralded for their unparalleled capacity to understand and generate content with a human touch. However, as much as these tools have revolutionized the AI landscape, they aren't without shortcomings. Central to their limitations is their fixed knowledge base; after their training phase, they cannot easily update or expand their knowledge, e.g., on seized data.

AI-Driven Analysis in Digital Forensics: Uncovering Patterns from Pixels

Greg Kipper

Digital forensics has become a crucial discipline in solving cybercrimes and uncovering digital evidence in today's ever-evolving landscape of technology and crime. As the volume and complexity of digital data continues to grow, traditional investigative methods are being challenged. However, artificial intelligence (AI) has emerged as a game-changing force that is transforming the field of digital forensics. In this article, we will delve into the world of AI-driven analysis and explore how it is reshaping the way investigators approach digital evidence and solve complex cases.

The Data Deluge Dilemma

The digital age has brought about an overwhelming amount of data, with each byte potentially holding valuable insights. From emails and documents to images and metadata, the digital realm is a treasure trove of evidence waiting to be discovered. However, the sheer volume of data has created a dilemma for digital forensic investigators. Traditional manual methods of analysis are often time-consuming and may not yield comprehensive results.

Unleashing the Power of AI

AI has the potential to play a significant role in identifying patterns in digital forensics using a number of techniques. The first is automated log analysis, where these systems can identify potential security incidents and other threats that may go unnoticed by human investigators. The next is pattern recognition algorithms, which can analyze massive amounts of data to detect patterns and trends that humans might miss. The third technique is cognitive-data analytics, which can help investigators look through criminal records, identify potential suspects, and observe commonalities in communication, dates, times, and location. The fourth is using machine learning models, which can uncover hidden evidence in digital data by utilizing their pattern detection and recognition capabilities. Lastly, unstructured data analysis is the ability to process and understand unstructured data, such as documents, emails, notes, etc.

AUTOPSY 4.21 VERSION

PAULO PEREIRA, PHD

Introduction

This article shows you how to start a case with the new version 4.21.0 of Autopsy, one of the pioneering tools responsible for the digital change in forensic investigation in recent years. The article itself does not claim to be a complete guide for a person to use Autopsy. For this, there are several sources on the web. However, an introduction is made on how to start a case in Autopsy, using an image called SUSPECT_LAPTOP, which was used in Belkasoft training and for which I received permission to use.

Version 4.21.0

Version 4.21.0 of Autopsy brings important changes over version 4.20.0. According to the repository of the tool, there are the following changes:

Table 1: Autopsy New Features

New Features	List of Updates
Library Updates:	• Update Java to version 17 • Update aLeapp/iLeapp executables. • Update JNA Version • Update SQLite library version • Updated 3rd party libraries that have known CVEs
Ingest Module Updates:	• Recent Activity checks for malicious Chrome extensions from list provided by https://github.com/randomaccess3/detections • Keyword Search module now can search without needing to index text into Solr. • New Cyber Triage Malware Scanner module that uses Reversing Labs (requires license). https://www.cybertriage.com/autopsy-malware-module/
Add Data Source Updates:	• Timestamps for logical files can be added. Issue https://github.com/sleuthkit/autopsy/issues/5852, https://github.com/sleuthkit/autopsy/issues/1788 • List of logical files/folders can be edited before they are added. Issue https://github.com/sleuthkit/autopsy/issues/7347

DIGITAL FORENSIC ANALYSIS USING AUTOPSY 4.21.0

PAULO PEREIRA, DIFIR

Introduction

This article shows a forensic analysis using Autopsy 4.21.0. The *SUSPECT.EO1* file is a disk image case study and is evidence used in Belkasoft's *X* training and CTF challenge. The article is not intended to be a complete analysis of this image because this image has a lot of detail and has an investigative complexity that would require more than one article. In this way, some parts will be analyzed with the intention of showing the use of Autopsy.

Operating System Details

Forensic analysts often ask, “Where do we start?” This question does not have one correct answer; for example, start here or start with this evidence. Often, the analyst's expertise defines where an investigation begins. Starting with the operating system (Figure 1) can be a decision that helps the analyst in identifying the name of domain accounts, structure of accounts registered in the system and the specific artifacts that were intended for the compromise of that system.

Digital Forensic Lab Management Made Easy with Monolith

Christopher Collins

There are multiple areas to focus on when managing a digital forensic laboratory.

Some of the important items to track are physical evidence like mobile devices or hard drives. However, how do we keep on track with other devices or evidence? In a forensics laboratory, for instance, there is hardware, software and other equipment that needs to be tracked.

Some laboratories use spreadsheets, or inventory management systems, but these methods are seldom cohesive in relation to documenting evidence and building reports.

A company called Monolith Forensics created a solution for this called Monolith. Monolith is a lab management software for digital forensics labs and teams that provide this cohesive environment.

Who is behind Monolith Forensics?

I had the opportunity to speak with Matt Danner, the Founder of Monolith Forensics.

Matt has a diverse history in digital forensics starting as a Special Investigator of the Texas Workforce Commission and the Texas State Auditor's Office. While working for the State of Texas, Matt was given the opportunity to take digital forensics training and start supporting investigations with forensic collection and examination of data. Matt eventually moved into the private sector and began managing digital forensics labs and teams. This experience with lab management made it clear to Matt that we needed better tools to manage a lab. The laboratories Matt worked with handled digital forensic cases from Civil Litigation, E-Discovery, and consulting with the Travis County Sheriff's Office on Criminal Investigations.

Just before running Monolith Forensics full-time, Matt was a senior consultant for Palo Alto Networks where he continued to work in DFIR roles and even worked on major projects involving reverse engineering of mobile applications. Matt uses this experience as a former investigator and digital forensics practitioner when creating or considering features for Monolith. One quality Matt portrays is that he strives to make sure the product is right for the customer, not to just make another sale.

When asked what sparked the creation of Monolith, Matt explained that he wanted to expand his knowledge and was looking for a good challenge. When Matt looked for a total lab management solution, there were none on the market that checked all the boxes as a "total solution".

FORENSICATING THREATS IN THE CLOUD

CHRIS DOMAN & MATT GEORGY

As organizations have shifted to the cloud, it's not surprising that threat actors have followed. Below we run through some of the most prominent attacks in the cloud today, and how to perform cloud forensics and incident response to resolve them.

TeamTNT, the cloud and containers

TeamTNT is a cybercriminal group that targets cloud and container environments, using various techniques to compromise and exploit them. TeamTNT has been active since at least April 2020, and has evolved its tactics and tools over time. Some of the methods used by TeamTNT include:

- Scanning for exposed Docker APIs and Kubernetes clusters, and deploying malicious containers that run cryptojacking malware or backdoors:

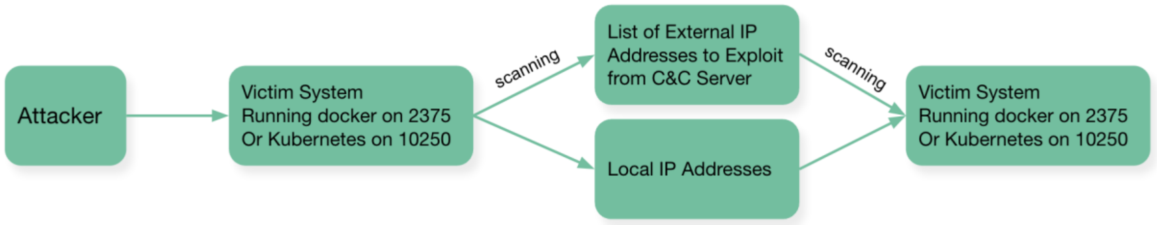


Figure 1: How TeamTNT compromises systems over exposed Docker and Kubernetes APIs

- Stealing cloud credentials from compromised instances, and using them to access other cloud resources or services:

History of Ransomware

Chirath De Alwis, Nipuni Sathsarani, Sandali lavanya liyanaarachchi, Wathmi Sureshika, Ahamed Nuski

Ransomware is malware that locks your computer or prevents you from accessing your data using key encryption until you pay a ransom. That ransom in demand is usually paid in Bitcoin. Data based extortion has been around since about 2005, but the development of ransom encryption software and Bitcoins have greatly facilitated the scheme [1].

The early days of ransomware can be traced back to the late 1980s and early 1990s when cyber-criminals began using simple tactics to lock users' computers and demand payment in exchange for unlocking them. One of the earliest known instances of ransomware was the AIDS Trojan, which emerged in 1989 and was distributed via floppy disks. The AIDS Trojan targeted AIDS researchers and locked users' computers while claiming to be a software program that could provide information about the disease. Another early example was the PC Cyborg ransomware, which was first detected in 1989 and spread via infected floppy disks. The PC Cyborg ransomware encrypted users' filenames and demanded a $189 ransom to restore access to the files. These early examples of ransomware set the stage for the more sophisticated and widespread attacks that would emerge in the coming decades. [2]

In early 2006, ransomware was starting to gain traction, and more attackers started to try their hand. Trojan.Cryzip appeared in March 2006. It copied data files to password-protected archive files and deleted the originals. The code for the malware included the password, so recovering it was straightforward. Trojan.Archiveus also came on the scene in 2006. It operated much like Trojan.Cryzip, except instead of asking for a ransom, it required victims to buy medication from specific online pharmacies and submit the order ID to get the password [3].

As the internet became more widespread and sophisticated, so did the tactics of cybercriminals. One of the key evolutions in the history of ransomware was the shift from simple locking mechanisms to the use of encryption algorithms to hold data hostage. This type of ransomware is known as encryption-based ransomware, and it is much more difficult to crack than earlier forms of ransomware. One of the turning points in the rise of encryption-based ransomware was the CryptoLocker attack of 2013. CryptoLocker was a particularly virulent form of ransomware that spread through email attachments and encrypted users' files with a 2048-bit RSA key. The attackers demanded a ransom in exchange for the decryption key, and victims who refused to pay risked losing their data forever. [4]

A study by Kaspersky found that for 2014-2015, ransomware attacks increased by 17.7 percent but crypto ransomware attacks increased by 448 percent [5].

The success of the CryptoLocker attack and the large sums of money earned by the attackers inspired other cybercriminals to adopt encryption-based ransomware as a favored tactic. In the years that followed, ransomware attacks became increasingly sophisticated and targeted, with attackers using a variety of tactics to evade detection and increase their profits.

How AI And ML Can Be Used To Counter Ransomware

Kavindu Anjana Gunasekara, Buddhi Nayani Perera, Shameen Samarawickrema, Pubudu Priyanga Liyanage, Chirath De Alwis

Ransomware is a type of malware that encrypts a victim's files or data and demands a ransom payment in exchange for the decryption key. Ransomware attacks have become increasingly prevalent in recent years, causing significant financial damage to individuals and organizations worldwide. As a result, security researchers are turning to advanced technologies, such as artificial intelligence (AI) and machine learning (ML), to counter this growing threat. In this article, we will explore in detail how AI and ML can be used to counter ransomware.

Before that, let's dig into some of the more popular ransomware in the world.

Year	Ransomware	Attack Type
2016	Ransom32	Offered as a service (RaaS). After system infiltration it encrypts stored data [1].
	7ev3n	Targets the Windows OS and spreads via spam emails containing malicious attachments, as well as file sharing networks [2].
	CryptXXX	Encrypts files stored on local and mounted drives using RSA4096 – an asymmetric encryption algorithm [3].
2017	Spora	Uses a combination of RSA and AES encryption to lock victim files [4].
	Dyn-A-Crypt	Encrypts files and steals data from the local machine [5].
	Samas	An aggressive hybrid attack that attempts to infect all machines on an organization's network [6].
2018	Ransomcloud	Block data or the use of applications that are in the Cloud and then demand a ransom to let organizations recover access [7].
	GrandCrab	Part of RaaS. This is the first ransomware that demands cryptocurrency which makes it hard to trace [8].
	SamSam	Leave ransom notes on encrypted computers [9].
2019	LockerGoga	Locks you out of your device using login credentials that the threat actor somehow got hold of, and/or encrypts your files, then forces you to pay a ransom to get them back [10].
	vxCrypter	Encrypt files with ".crypter" extension [11].

MODERN DETECTION MECHANISMS FOR COUNTERING RANSOMWARE

K.I. SRIMAL, IROMIKA UDAYAPPRIYA, M.P. NADUN CHATHURANGA, J.L. KAVINDA AKALANKA, CHIRATH DE ALWIS

Ransomware is malicious software that blocks access to a victim's computer or data and demands a ransom to restore the system [1]. Attackers gain access through phishing emails or system vulnerabilities, install the ransomware, and encrypt the victim's data. Ransomware attacks can have serious consequences, including data loss, business interruption, financial costs, and reputational damage. Ransoms can range from a few hundred dollars to millions, often paid in cryptocurrency for anonymity. Paying the ransom doesn't guarantee access will be restored, and attackers may demand further payment. The most common types Crypto Ransomware or Encryptors, Lockers, Scareware, Doxware or Leakware, RaaS (Ransomware as a Service) [2]. Prevention methods are regular data backups, software updates, and detection mechanisms for ransomware attacks.

What is Ransomware Detection?

Ransomware detection is the process of identifying and alerting users to the presence of ransomware on their computer systems or networks. It involves the use of security software and tools that can detect suspicious activities and behaviors that are characteristic of ransomware.

Effective ransomware detection is essential for early detection and response to ransomware attacks, allowing organizations to take action to isolate and remove infected systems and prevent the spread of the ransomware to other parts of the network. After that, regular backups of critical data can help minimize the impact of a ransomware attack.

Need FOR Early Detection

Early detection is very important when dealing with a cyber-attack. The need for ransomware early detection is very clear, as these attacks can cause significant financial and representational damage to organizations and individuals. The cost of ransom payments can be significant, and the damage caused by lost data, downtime, and business disruption can be extensive. The impact of ransomware attacks can also extend beyond the immediate financial costs, as organizations may suffer reputational organizations may suffer damage to their reputation if they are unable to recover from an attack quickly.

TAKE YOUR SEAT NOW!

THIS COURSE IS AIMED AT PRESENTING AN ELEMENTARY YET COMPREHENSIVE PICTURE OF THE FIELD OF DIGITAL AUDIO FORENSICS