CISO MAG

beyond cybersecurity

Volume 5 | Issue 09 | September 2021

60

Computer Forensics in the Cloud

Karim El Chenawi
CISO
John Doe Invest

COVER STORY

76

Cloud Forensics in Today's World

SURVEY REPORT

CLOUD FORENSICS

An Evolving Investigative Realm in Cybersecurity

EC-Council

codered
FROM EC-COUNCIL

Elevate your team's skill set and performance with in-demand tech skills fit for your organizational needs. Our intensive Micro Degrees are designed by leading experts and integrated with world-class iLabs for an enriched learning experience.

What do We offer?

- Master your specialized degree in just 3 months
- Practice live with virtual simulated labs
- World-class simulated labs
- Proctored exam
- Intense 200+ hours of online learning
- Official certification from EC Council

codered
FROM EC-COUNCIL

Programs We Offer

Explore our impactful Micro Degrees tailored to your enterprise needs. Access the latest resources to help your team achieve scalable results and transition to specialized roles with industry-leading certification.

PHP Security MicroDegree

Cross-train your team in advanced PHP Security with hands-on experience in building a secured web application from the ground up.

USPs

- **Learn to write secure PHP code**
- **Unlimited access to quizzes**
- **40+ hours of premium videos**
- **Exclusive workshops**

Enroll Now to Certify Your Team

Python Security MicroDegree

Provide your team with access to the latest resources and in-demand curated online content in Python Security designed to fit your organiza- tion's needs.

USPs

- **Innovative learning in python programming**
- **50+ best-in-class simulated lab access**
- **34 hours of premium video content**
- **Insights from industry experts**

Enroll Now to Certify Your Team

Upskill your talent pools with in-demand skills facilitated by virtual simulated labs & resources with CodeRed.

Get Started Now

EC-Council
WAHS
Web Application Hacking & Security

WEB APPLICATION HACKING AND SECURITY

100% Hands-On | Lab-Based

From the team that brought you the Certified Ethical Hacker

Become A Certified Web Application Associate | Professional | Expert

CERTIFIED

WHY Is It Important?

Application security is one of the fastest growing cybersecurity skill[1]

If you are tasked with implementing, managing, or protecting web applications, then this course is for you. If you are a cyber or tech professional who is interested in learning or recommending mitigation methods to a myriad of web security issues and want a pure hands-on program, then this is the course you have been waiting for.

Get Certified Today

[1] https://www.forbes.com/sites/louiscolumbus/2020/11/01/what-are-the-fastest-growing-cybersecurity-skills-in-2021/

HOW You Will Learn?

Unlike many Capture-the-Flag challenges and Vulnerable Virtual Machines, Web Application Hacking and Security provides the challenger with the ability to follow an instructor as they make their way through the challenges. The instructor will present alternatives, do scans, upload malicious payloads, and crack passwords from their home computer just like you. – But don't rely on the walkthrough; challenge yourself and see how far you can get. Play some of the walkthroughs, then pause and try some more.

Beginner Intermediate Proficient Expert

Break The C</>DE

REGISTER NOW

WHAT You Will Learn?

- Advanced Web Application Penetration Testing
- Advanced SQL Injection (SQLi)
- Reflected, Stored and DOM-based
- Cross Site Scripting (XSS)
- Cross Site Request Forgery (CSRF) – GET and POST Methods
- Server-Side Request Forgery (SSRF)
- Security Misconfigurations
- Directory Browsing/Bruteforcing
- CMS Vulnerability Scanning
- Network Scanning
- Auth Bypass
- Web App Enumeration
- Dictionary Attack
- Insecure Direct Object Reference Prevention (IDOR)
- Broken Access Control
- Local File Inclusion (LFI)
- Remote File Inclusion (RFI)
- Arbitrary File Download
- Arbitrary File Upload
- Using Components with Known Vulnerabilities
- Command Injection
- Remote Code Execution
- File Tampering
- Privilege Escalation
- Log Poisoning
- Weak SSL Ciphers
- Cookie Modification
- Source Code Analysis
- HTTP Header modification
- Session Fixation
- Clickjacking

Level up your skill

CISO MAG
beyond cybersecurity

Volume 5 | Issue 09
September 2021

President & CEO
Jay Bavisi

Editorial

Editor-in-Chief
Brian Pereira*
brian.p@eccouncil.org

Editorial Consultant
Minu Sirsalewala
minu.sirsalewala.ctr@eccouncil.org

Sub Editor
Pooja Tikekar
pooja.v@eccouncil.org

Sr. Feature Writer
Rudra Srinivas
rudra.s@eccouncil.org

Management

Senior Vice President
Karan Henrik
karan.henrik@eccouncil.org

General Manager - Marketing
Seema Bhatia
seema.b@eccouncil.org

Senior Director
Raj Kumar Vishwakarma
rajkumar@eccouncil.org

Head - Research & Content
Jyoti Punjabi
jyoti.punjabi@eccouncil.org

Publishing Sales Manager
Taruna Bose
taruna.b@eccouncil.org

Manager - Digital Marketing
Rajashakher Intha
rajashakher.i@eccouncil.org

Asst. Manager Visualizer cum Graphic Designer
Jeevana Rao Jinaga
jeevana.r@eccouncil.org

Manager – Marketing and Operations
Munazza Khan
munazza.k@eccouncil.org

Image credits: Shutterstock & Freepik
Illustrations, Survey Design, Cover & Layouts by: Jeevana Rao Jinaga

* Responsible for selection of news under PRB Act. Printed & Published by Brian Pereira, E-Commerce Consultants Pvt. Ltd.,

CLOUD IS NEW TERRITORY FOR FORENSICS

Brian Pereira
Editor-in-Chief

Volumes have been written extolling the virtues and benefits of cloud computing. The cloud enables organizations to scale up rapidly and to be more agile. There are cost-savings and efficiencies too, which can be leveraged through various cloud models.

Today, it is common practice for an organization to adopt a hybrid, multi-cloud approach. That makes cloud security more challenging. If an organization experiences an attack or data breach, it will have to trace the source of the attack, what the damage was, the extent and impact of the attack.

That's where Cloud Forensics comes in.

When infrastructure is virtualized and hosted by multiple clouds with servers in different jurisdictions, it poses a tremendous challenge to cloud forensics specialists. In fact, doing forensics on the cloud is complicated and differs vastly from traditional computer forensics. With computer forensics, investigators had to find the *media* that had the data or digital evidence. With the cloud, this evidence could be anywhere.

The cloud offers various architectures, service models, processes, and continuously changing paradigms. So, it is challenging for investigators to gain access to data and resources required for forensics – to obtain the "artifacts," as they call it. That includes registry keys, files, timestamps, and event logs. This is digital evidence that can be used in a court of law for criminal litigation.

We wanted to determine what are the biggest challenges posed to cloud forensics today. For this, **EC-Council's Cyber Research** team undertook a survey titled *"Cloud Forensics in Today's World."* The report on page 76 uncovers some interesting findings from their investigation:

- Both multi-tenancy-related privacy *issues and distributed data location were considered equally challenging by* ***one-fourth*** *of the respondents.*
- ***More than half*** *of the respondents believe the hybrid cloud deployment model presents the most challenges towards cloud forensics.*
- ***Nearly 40%*** *of the respondents say that a lack of channels for international communication contributes significantly to the legal challenges faced by cloud forensics.*
- *There is a growing demand that the SLA should mention when and what data to collect, its purpose and legal liabilities.*
- *FaaS (Forensics as a Service) is the most anticipated trend towards improving the cloud forensics domain.*

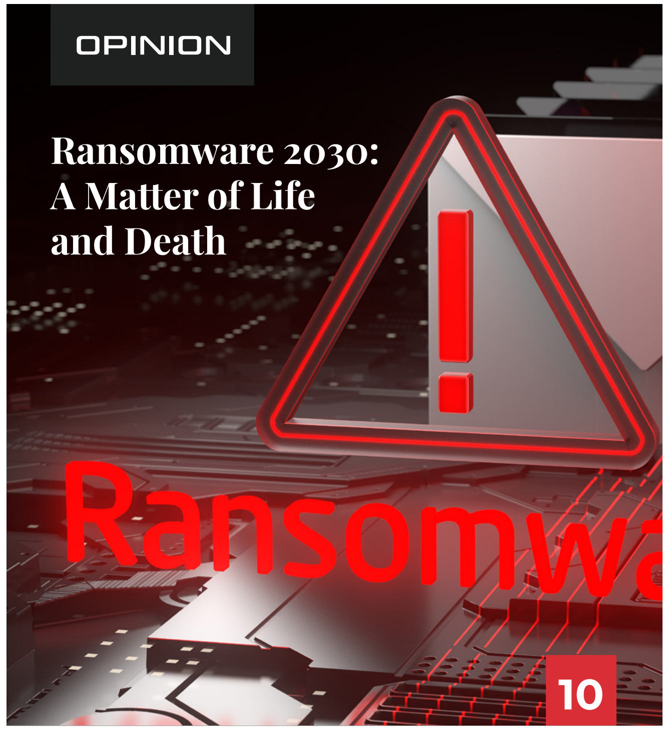
Since the cloud is now a shared responsibility, some have suggested that cloud service providers offer Forensics as a Service. Yes, FaaS is being offered by third parties today. But more CSPs need to offer it.

In the cover story on page 60, **Karim El Chenawi, CISO at John Doe Invest**, writes that the shared responsibility model for cloud computing puts the onus of cloud security on both the cloud service provider and the client. And that increases the attack surface for threat actors to exploit. So there is a need for a trustworthy cloud forensic process that overcomes the existing challenges associated with cloud computing and provides clear and actionable data towards security enforcement and incident handling. He suggests that the complete cloud forensic process should be classified into incident identification, data collection, and analysis and examination phases.

We hope you enjoy the stories that our team curated and produced for this issue.

INDEX

Contents



Ransomware 2030: A Matter of Life and Death

Dick Wilkinson
Chief Technology Officer
New Mexico Judicial Information Division

On an early morning in the year 2030, a remote surgery bay is powering up and getting prepped for the patient. The patient is in Dallas, Texas, and the doctor is in Baltimore, Maryland. The FDA approved remote surgical procedures for most routine surgeries, and the field of remote outpatient surgery became common, back in 2025. Now more than 100,000 remote surgeries are performed in the U.S. each year. The patient is a 50-year-old man having a benign tumor removed from his liver. The doctor specializes in remote tumor removal and has done this procedure more than 100 times. What could possibly go wrong with all that experience and approved safety procedures in place?

The surgery begins with no concerns, and the patient is doing well. The procedure is scheduled to last for about two hours, and over an hour has gone by. The doctor in Baltimore readies his blade to remove the tumor, and his controls become unresponsive. Nothing in his heads-up display gives him any indication of an error, and his blade does not respond to his command. The onsite nurse with the patient notices an alert coming from the robotic arm but can't tell what is wrong. The doctor tries again but fails to get a response from the machinery.

The service provider for the hospital's remote medicine department gets an alert on their security control panel. The connection has somehow been rerouted to a cloned server, and it is clear that a man-in-the-middle attack is taking place on the hospital's robotic control servers. The hospital's CISO receives an email with a ransom note at the same time as the alarms begin to cascade across various IT systems. The hospital's redundant robot control servers have been encrypted, and the clock is now ticking.

The patient lies on the table with full life support and an open abdomen while the doctor in Baltimore is completely helpless to recover the situation. The man's life is now in the hands of the hospi
makers and not a
ransom note was s
worth of cryptocur
cease. The crimi
they knew the
the speed of r
ransom in l
hospital i
alarms c
were r
Shak