Contribution ID: **3** Type: **not specified**

Veil of Silence: Unraveling the Ransom Screen Lock

In this session, we will embark on a journey through the evolution of Ransom Screen Lockers, examining their design, mechanics, and the methods used by cybercriminals to hold users'screens hostage. The session will provide a deep dive into the mechanisms that power these locker programs, detailing the progression from simple lock screens to more complex, effective versions that can bypass security defenses and demand ransom for unlocking systems.

Through a blend of theoretical knowledge and hands-on practical experience, participants will learn how these threats operate and how they have evolved over time. We will also showcase live demonstrations of common techniques used by ransomware, providing attendees with a better understanding of the tools and methods behind these digital attacks. The session will explore real-world case studies to help participants recognize how these locker mechanisms manifest and how they can mitigate their impact.

Key topics we will focus on include:

1. -Understanding the Ransomware Locker Mechanism: A comprehensive look at how screen lockers operate, from initial infection to ransom display, and the technical details behind these attacks.
2. -The Evolution of Ransomware Locker Mechanisms: An exploration of how ransomware lockers have progressed over time, from early screen-locking techniques to the complex, multi-layered strategies employed by today's cybercriminals.
3. -Static and Dynamic Analysis of Ransom Locker Mechanisms: Theoretical insights and practical demonstrations on how to analyze ransomware using both static and dynamic approaches, helping you understand how these threats work in both dormant and active states.
4. -Dissecting the Techniques to Decrypt a Locked Machine: How experts reverse-engineer and break the encryption mechanisms behind ransomware, as well as how to safely recover systems without paying the ransom.
5. -Decrypting and Unlocking the Infected Machine Without Paying the Code: Techniques for circumventing ransom demands by decrypting and unlocking infected systems using available decryption tools, forensic analysis, and manual techniques.
6. -Reverse Engineering of C-Based Screen Lockers to Find a Key: A hands-on breakdown of reverse engineering screen lockers written in C, and how to identify encryption keys or other vulnerabilities to unlock the system without paying the ransom.

Why Attend:
This session is ideal for professionals interested in cybersecurity and malware analysis who wish to gain practical, real-world insights into the ever-evolving landscape of ransomware. Whether you are new to the subject or have some experience, this session will equip you with the knowledge to understand and address the growing threat of Ransom Screen Lockers. You'll leave with a solid grasp of how these threats work, along with strategies to protect your syste

Length

45 minutes

Optional: Speaker / convener biography

Diyar Saadi Ali is a formidable force in the realm of cybersecurity, renowned for their expertise in cybercrime investigations and their role as a certified SOC and malware analyst. With a laser-focused mission to decode and combat digital threats, Diyar approaches the complex world of cybersecurity with precision and unwavering dedication. At the core of their professional journey lies real-time security event monitoring—a task Diyar executes with exceptional vigilance and expertise. As a respected MITRE ATT&CK Contributor, they have made invaluable contributions to the global cybersecurity community, sharing insights and strategies that help organizations bolster their defenses against evolving cyber threats. Diyar's impact is further amplified by their role as the discoverer and owner of critical Common Vulnerabilities and Exposures (CVEs), including CVE-2024-25400 and CVE-2024-25399. These achievements underscore their commitment to identifying and addressing systemic vulnerabilities that could otherwise threaten digital ecosystems. Currently, Diyar is making waves on the international stage as a speaker at prestigious cybersecurity events such as Arab Cyber Security in Cairo, DeepSec in Vienna, and SulyCon in Sulaymaniyah, Iraq. They've also actively participated in GISEC in the UAE, showcasing their commitment to staying at the forefront of industry trends and challenges. With a wealth of experience, an impressive track record of contributions, and a dedication to advancing cybersecurity knowledge, Diyar Saadi Ali continues to inspire and lead in the ever-evolving digital landscape.

Speaker Activities :

1-Speaker Linkedin : https://www.linkedin.com/in/diyarsaadi/
2-Speaker Blog : https://malfav.github.io/malwrdatabase/
3-Speaker Blog : https://malfav.gitbook.io/home
4-Speaker Article : https://memoryforensic.com/inside-cridex-memory-analysis-case-study/
5-Speaker Article : https://hadess.io/memory-forensics-a-comprehensive-technical-guide/

Primary author: SAADI, Diyar (Spectroblock)

Track Classification: Talks and presentations