Honey Credentials for Attack Response in Ransomware Attacks

Kent Yamada  
*NYU Tandon School of Engineering*

*Cyberfellows, Information Security and Privacy, Fall 2021*New York, NY  
ky2303@nyu.edu

*Abstract*— In this paper I propose the use of honey credentials on networked machines and IoT devices to detect network attacks in the account discovery/lateral movement phase [MITRE ATT&CK [TA0007](https://attack.mitre.org/tactics/TA0007/), [TA0008](https://attack.mitre.org/tactics/TA0008/)]. After an initial foothold is established in a target network, the most likely next step is a lateral movement or elevation of privileges. Honey credentials can be an effective canary-like system for warning network defenders against compromised devices early in the attack chain. [Results will be added here after experiment]

Keywords—honey credentials, honey pot, MITRE ATT&CK, ransomware, lateral movement, privilege escalation

# Introduction

Recent ransomware variants such as Ryuk and Conti change with each new attack, leveraging different initial vectors of intrusion, but once initial access is gained attackers utilize similar lateral movement and privilege escalation techniques. A recently leaked ransomware playbook, translated and published by Cisco Talos [8] shows how PowerShell (which includes tools like PSinject and ProxyShell), Mimikatz, LSASS.exe dumps, and other methods have been used by the Conti ransomware group to steal credentials.

# Related Research

Researchers and security industry vendors have extensively studied, developed, and use honey pots in network implementations with honey credentials usually being treated as a subset of this defense tactic. For example, Rapid7 includes honey folder and honey credential modules in their InsightIDR security product [9]. However, since most companies and organizations handle user and password controls internally, not much research or open-source material on honey credentials is available. This paper focuses on using honey credentials in catching lateral movement in the attack chain. Related studies exist in finance and healthcare fields, but this specific use does not appear to be thoroughly researched.

Herley and Florencio [1] propose the use of thousands to millions of honeypot credentials to protect bank accounts and observe attacker’s behaviors when trying to cash out using compromised accounts. However, since this was written in 2008, their focus was on thwarting brute-force attackers using password spraying techniques to compromise many user accounts at once.

Sibi Chakkaravarthy, et al. [2] experiment using a testbed network of Raspberry Pi’s, honeyfolders and a novel Intrusion Detection Honeypot (IDH) to detect 1000 samples of ransomware. Although only one part of the IDH, the proposed idea of a honey folder is used to detect suspicious file activity and may indicate lateral movement, a similar concept proposed in this paper.

Similarly, S. Sheen and A. Yadav [3] use a large malware sample set (16243) along with a set of benign executables (3620) to identify malware. They first search for API calls within samples then run the set through a classification model to determine if the sample is malicious or benign. Their experiment was able to produce a best performance of 0.9653 true positive classification of malware executables.

# Threat Modeling

Assuming the goal of an attack is financial gain, ransomware has been a main attack vector and events have been rising in recent years. Depending on the size of the institution, the attack surface that leads to financial loss for an organization can be large and difficult to model, however creating models can help identify weak points and risk in the system. A threat model exercise was done to identify potential risks to a hypothetical hospital or healthcare organization. The STRIDE model was used to identify attack vectors for a successful ransomware attack and an attack tree was created to map potential risks to hospital IT assets that are vulnerable to these vectors. Lower-level footholds and intrusions are based on industry and vendor reports [10][11]. Higher level technical details for threat model are based on the Cybersecurity and Infrastructure Security Agency’s 2020 report on ransomware in the healthcare and public health sector [12].

An attack tree visually sorts the threats to a system to gain a better understanding of the system itself. The threats from the previous section are decomposed and mapped to nodes in this attack tree to show potential threats to a hospitals IT system. The root of the tree is the main goal of an attacker in this scenario – financial gain through payment. Categories from the STRIDE model are in parentheses in the corresponding nodes. The attack tree can be found in Appendix A: ransomware attack tree for hospital/healthcare organization or [google drive link].

1. STRIDE Model

|  |  |
| --- | --- |
| **Threat Category** | **Potential threats and vulnerabilities** |
| Spoofing | * Send emails to employees pretending to be a partner organization to trick employees into to opening a malicious link or document. * Send emails to employees pretending to be someone in management or in a higher role to trick employees into to opening a malicious link or document. * Pretend to be an employee to gain physical access to the site and IT infrastructure (servers, routers/switches, clients, ethernet drops). * Pretend to be an employee and reset password through IT department portals or helpdesk using information gathered online. * Pretend to be IT department employee and get passwords from other employees. * Pretend to be auditors/contractors/visitors to gain physical access to site and IT infrastructure (servers, routers/switches, clients, ethernet drops). * Set up a rogue wireless access point and spoof the hospital wifi to crack network passwords and steal packets and/or credentials. |
| Tampering | * Set up a rogue wireless access point and spoof the hospital wifi to inject packets into legitimate communications. * Perform man-in-the-middle attacks on hospital wifi to steal data and/or credentials. * Perform man-in-the-middle attack on a virtual private network set up for remote work to steal data or credentials. * Intercept supply chain(s) and install malicious firmware or persistent backdoors in employee workstations, health IoT devices, point of sale devices, HVAC devices. |
| Repudiation | * Steal management or IT mail account private keys and sign phishing/malware emails. |
| Information disclosure | * Exploit public-facing servers to expose employee and/or patient data. * Scan for misconfigured and/or legacy web servers to find software versions and/or open ports to exploit. * Scan for misconfigured and/or legacy medical devices to gain a foothold in hospital network. |
| Denial of service | * DDoS attack the hospital electronic health records (EHR) system. * DDoS attack the IoT devices (remote patient monitoring, patient cameras, point of sale devices, HVAC devices). * DDoS attack the cloud service hosting hospital systems. |
| Elevation of privilege | * Move laterally from IoT devices/employee workstations to more valuable machines. * Once targets are compromised, use privilege escalation tools to elevate to root/system/admin users to gain full system control. * Exploit remote workers’ VPN to gain access to hospital network. * Bribe insider for system access. |

# Hypothesis

Placing honey credentials is a reliable method to alert defense teams to an initial breach and update firewalls before a large-scale attack can occur.

# Results

# Conclusion

##### Acknowledgment

##### References

1. C. Herley and D. Florˆencio, “Protecting Financial Institutions from Brute-Force Attacks,” Proceedings of The Ifip Tc 11 23rd International Information Security Conference, 2008, pp 681-685, doi: 10.1007/978-0-387-09699-5\_45
2. S. Sibi Chakkaravarthy, D. Sangeetha, M. V. Cruz, V. Vaidehi and B. Raman, "Design of Intrusion Detection Honeypot Using Social Leopard Algorithm to Detect IoT Ransomware Attacks," in IEEE Access, vol. 8, pp. 169944-169956, 2020, doi: 10.1109/ACCESS.2020.3023764.
3. S. Sheen and A. Yadav, "Ransomware detection by mining API call usage," 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2018, pp. 983-987, doi: 10.1109/ICACCI.2018.8554938.
4. K. K. Gagneja, "Knowing the ransomware and building defense against it - specific to healthcare institutes," 2017 Third International Conference on Mobile and Secure Services (MobiSecServ), 2017, pp. 1-5, doi: 10.1109/MOBISECSERV.2017.7886569.
5. H. T. Yew, M. F. Ng, S. Z. Ping, S. K. Chung, A. Chekima and J. A. Dargham, "IoT Based Real-Time Remote Patient Monitoring System," 2020 16th IEEE International Colloquium on Signal Processing & Its Applications (CSPA), 2020, pp. 176-179, doi: 10.1109/CSPA48992.2020.9068699.
6. R. Ranchal et al., "Disrupting Healthcare Silos: Addressing Data Volume, Velocity and Variety With a Cloud-Native Healthcare Data Ingestion Service," in IEEE Journal of Biomedical and Health Informatics, vol. 24, no. 11, pp. 3182-3188, Nov. 2020, doi: 10.1109/JBHI.2020.3001518.
7. A. A. Hady, A. Ghubaish, T. Salman, D. Unal and R. Jain, "Intrusion Detection System for Healthcare Systems Using Medical and Network Data: A Comparison Study," in IEEE Access, vol. 8, pp. 106576-106584, 2020, doi: 10.1109/ACCESS.2020.3000421.

##### Other Resources

1. https://blog.talosintelligence.com/2021/09/Conti-leak-translation.html
2. https://docs.rapid7.com/insightidr/deception-technology
3. https://blog.malwarebytes.com/business-2/2020/10/healthcare-security-death-by-ransomware/
4. https://www.himss.org/resources/cybersecurity-healthcare
5. https://us-cert.cisa.gov/ncas/alerts/aa20-302a

# Appendix A

Ransomware Attack Tree for a Hospital

# Diagram Description automatically generated

Figure 1: Attack threat model for a hospital. For a higher resolution view of the tree, please see: [[Google Drive Link]](https://drive.google.com/file/d/1yZkMfiQxh3LXFfZ6QDPZGRaJH1yZ9k8J/view?usp=sharing)