Section 1: Week 4: Analyze Malware and Encryption Options

Nate Bachmeier

TIM-8301: Principals of Cybersecurity

April 26, 2020

North Central University

# Analyze Malware and Encryption Options

When systems become infected with malicious software, it impacts productivity, degrades the customer experience, and introduces risk. These issues typically manifest as background processes stealing resources, mining cryptocurrency, and restrict access to our documents. Mitigating these scenarios requires technological solutions and incident response strategies. Another core set of challenges comes from the application of encryption for protecting privacy, integrity, and ensuring authenticity. Organizations need to be cognizant of risks that arise from incorrect alignment of security objectives and encryption algorithms and protocols.

## Section I: Malware Investigation

## What is malware

Malicious software, or malware, are applications that compromise the confidentiality, integrity, or availability of a system. These programs infect systems via email, file-sharing services, browser vulnerabilities, spoofed resources, and misconfigured services (Lee et al., 2017). It can be challenging to contain the spread through an organization due to homogeneous configurations of the devices. For instance, a branch office will likely run the same software packages on each workstation and share documents through central repositories. The objective of the malware can vary from scenarios such as remote command-and-control, data exfiltration, and denial of service scenarios. One specific attack that is gaining popularity is ransomware, which are applications that encrypt user data and then offer to sell the decryption key (Busdicker & Upendra, 2017). Since malware comes from different vectors with varying objectives, detecting and preventing all scenarios is nearly impossible. Even with protection against all known scenarios, criminal social networks have easy access to exploitation packages and zero-day vulnerabilities across the dark web (Ericsson et al., 2018). Given the availability of exploitation software, organizations need to consider these scenarios as part of their risk management planning. Addressing these unknown unknowns requires defense-in-depth mindsets that expand beyond edge firewalls to include more robust Intrusion Detection and Prevention Systems (IDS/IPS).

## Managing the Incident Lifecycle

The business needs to devise a plan to limit the risk from malware through people, processes, and procedural changes. There are over one million malware strains generated every day, and this creates the need for keeping anti-virus definitions up to date (Kilgallon et al., 2017). When users are aware of the time-sensitive nature of applying new signatures, they are more likely to act. Communicating similar expectations around patch management can reduce the attack surface and decrease the chances of infection. However, enforcing these procedures can be challenging in situations that rely on security governance, like Bring Your Own Device (BYOD) scenarios. An alternative approach by the state of the art systems uses machine learning and sandbox execution instead of signature files (Kilgallon et al., 2017). For instance, an email server could inspect every attached document within a Cuckoo container to determine if the content is malicious. It is also critical that systems have proper backup and restore procedures so that the reinstallation of compromised machines becomes an option.

These challenges create the need for an incident response plan that manages internal investigations. This process begins with identifying what the infected machine has access to from both security policies and users. For example, when malware gets onto Alice's laptop, it can replicate onto her personal Google Drive and corporate Microsoft SharePoint server (Balupari & Singh, 2017). While network administrators can review traffic logs to detect a subset of these scenarios, searching through audit logs is a tedious process that can miss critical entries (Cam, 2017). Applications like Splunk and Amazon CloudTrail improve the experience of searching through oceans of audit logs. However, if the organization hosts the SharePoint site through a third-party, that audit information becomes inaccessible. These sorts of limitations cause the administrators to operate on an incomplete picture.

However, more sophisticated attacks can require external organizations such as digital forensics, security consulting firms, and law enforcement. When attackers installed malware on Target's Point of Sale systems, they were able to steal forty million debit and credit cards (Kreb, 2013). While Target employs numerous engineering professionals, this incident was significant enough to require external domain experts to reassemble subtle details across the entire technology stack. Some nations, like the European Union, have specific reporting requirements for cybercrimes that involve customer data (Kovacs, 2018). These regulations could also require the organization to seek legal experts to navigate international law.

# Section II: Encryption

## What is encryption

The primary goal of encryption technologies is to maintain the integrity, confidentiality, or authenticity of a digital resource (Boneh, 2016). This capability is not limited to sensitive documents and applies to numerous scenarios. For instance, when a blogger uses Pretty Good Privacy (PGP) to sign their public posts, it provides a mechanism to confirm the post is complete and legitimate. DocuSign is another example that relies on encryption for maintaining the integrity of contracts, not necessarily confidentiality. Just as there are different use-case of encryption, there are different technological implementations. Many scenarios, like password management, use one-way hashing to choose deterministically random encodings of credentials. The hashing function is typically computationally complex to calculate, and this prevents attackers from brute-forcing all combinations. Other needs require a mechanism for undoing the hashing to restore the plain-text, such as protecting data in transfer and at rest. A standard implementation of decryption depends on Public and Private Keys, which are large numbers that are prime numbers of each other. These prime numbers are unique and can only be verified or decrypted with the alternative value. As the organization matures, it will often acquire Public Key Infrastructure (PKI) to manage the lifecycle of keys. These lifecycle events occur during distribution, validation, and revocation phases (Buchmann, Karatsiolis, & Wiesmaier, 2013). For instance, when Contoso deploys a new website, they will create a certificate that confirms the identity of the resource. After a few years, the certificate will become compromised or expire. That lifecycle event requires updating the revocation list to contain the deprecated public key and nullify any future use.

## Challenges with Encryption Solutions

While encryption is conceptually a relatively simple concept, there are many hidden challenges across each aspect. For instance, Message Digest Algorithm v5 (MD5) and Cyclic Redundancy Check (CRC32) are sufficiently reliable to detect hardware faults but fragile under malicious attacks. Instead, the Secure Hashing Algorithm (SHA) and Advanced Encryption Standard (AES) has larger key sizes and better protections against birthday attacks. A birthday attack is when two different documents produce the same hash value. Another challenge with one-way hashing comes from rainbow tables, which precompute all combinations and support a reverse-lookup (Alpatskiy et al., 2020). After recovering the plain-text password, attackers will attempt to reuse them in other systems.

Vulnerabilities also exist in the libraries that perform encryption, both in terms of coding and logic errors. In 2017 OpenSSL, the de-facto standard implementation on Linux systems was reported vulnerable to information disclosure (Kyatam, Alhayajneh, & Hayajneh, 2017). Successful exploitation of this issue allows an attacker to read arbitrary memory, such as secrets, within a remote process. Another attack vector into these libraries comes from the participants downgrading the protocol version to use backward compatible code paths that might be less secure (Marshall, 2020). A trade-off exists for administrators where not supporting backward compatibility improves security but can break legacy consumers.

Challenges also originate from the management of the infrastructure that supports encryption and data retention. Such as design limitations in the clients of PKI technologies that do not consult the revocation lists and ignoring certificate errors. Another class of issues comes from the decentralized nature of the Internet, and this creates multiple sources of truth. Businesses are broadly adopting cloud and other storage as a service (StaaS) technologies to improve redundancy and lower costs. As the data leaves the organization, there needs to be considerations around how the data becomes encrypted. Once the data becomes protected, another set of challenges follow around managing the decryption key. If that key is lost, then the backups are useless and critical knowledge is lost.

## Influence of Nations

Protecting data with encryption technologies adds a layer of privacy, and this can come at odds against law enforcement and political values. On the one hand, there are legitimate concerns that data confidentiality can impede stopping terrorist attacks. The Islamic State in Iraq and Syria (ISIS) has notable been very successful at protecting internal communications in part due to adopting encryption technologies (Banks, 2017). Most governments believe they are entitled to the underlying information as part of ensuring their sovereignty (Inkster, 2015). While there are significant advantages from mandating a minimum level of encryption, there are substantial consequences with creating an artificial ceiling (Hunt, 2019). A potential disconnect might exist that politicians do not understand that encryption is math, and it is impossible to ban. Even if government regulation prevents the use of an obfuscation practice, it is unlikely that criminals would follow the law. The net effect then becomes more risk toward legitimate businesses and personal privacy. Despite the risks associated with weakening data protection, different nations are more willing to embrace policies that favor governmental control over the rights of societal and international actors.

## Actionable Suggestions

The National Institute of Standards and Technology (NIST) offers some initial guidelines around encryption best practices. Organizations should consult these recommendations as a starting point, but also recognize that its specific industry might have additional requirements. For instance, medical records and personally identifiable information (PII) could have different expectations than web server transaction logs. The application of these requirements needs to touch every aspect of the value-chain to confirm that digital resources come from legitimate sources and have not changed. When the business provides employees with training and access to the PKI infrastructure through application integrations, it can create a culture than encrypts more content by default. For example, Microsoft Office products support Digital Rights Management (DRM) to restrict copying, editing, and printing scenarios. As these capabilities become a simple button click, there is a higher chance of security-aware employees using it.

# References

Alpatskiy et al. (2020). A new approach in the rainbow tables method for human-like passwords. *IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering* (pp. 2035-2040). St. Petersburg, Russia.

Balupari, R., & Singh, A. (2017, May). Recon and respond to malware threats in the cloud. *ISSA Journal. Vol. 15, Issue 5*, pp. 22-27.

Banks, W. (2017). Cyberespionage and electronic surveillance: beyond the media coverage. *Emory Law Journal. Volume 66, Issue 3*, 513-525.

Boneh, D. (2016, November). *Cryptography by Stanford*. Retrieved from Coursera: https://www.coursera.org/lecture/crypto/

Buchmann, J., Karatsiolis, E., & Wiesmaier, A. (2013). *Introduction to public-key infrastructures.* Goodreads.

Busdicker, M., & Upendra, P. (2017). The role of healthcare technology management in facilitating medical device cybersecurity. *Biomedical Instrumentation and Technology, Vol. 51*, 19-25.

Cam, H. (2017). Online detection and control of malware-infected assets. *Military Communications Conference.* Baltimore, MD.

Ericsson et al. (2018). Community Finding of Malware and Exploit Vendors on Darkweb Marketplaces. *1st International Conference on Data Intelligence and Security.* South Padre Island, TX, USA.

Hunt, T. (2019). Hack to the Future. *NDC Conferences.*

Inkster, N. (2015). *China's cyber power.* Adelphi Series.

Kilgallon et al. (2017). Improving the effectiveness and efficiency of dynamic malware analysis with machine learning. *Resilience Week.* Wilmington, DE, USA.

Kovacs, L. (2018). Cybersecurity policy and strategy in the European Union and NATO. *Revista Academiei Fortelor Terestre. Vol. 23, Issue 1*, 16-24.

Kreb, C. (2013, December 20). *Cards stolen in Target breach flood underground markets*. Retrieved from Krebs On Security: https://krebsonsecurity.com/2013/12/cards-stolen-in-target-breach-flood-underground-markets/

Kyatam, S., Alhayajneh, A., & Hayajneh, T. (2017). Heartbleed attacks implementation and vulnerability. *IEEE Long Island Systems, Applications and Technology Conference Systems.* Farmingdale, NY, USA.

Lee et al. (2017). CloudRPS: a cloud analysis based enhanced ransomware prevention system. *Journal of Supercomputing. Jul2017, Vol. 73, Issue 7, p3065-3084*, 3065-3084.

Marshall, A. (2020, February 18). *Solving the TLS 1.0 problem, 2nd edition*. Retrieved from Microsoft Security Engineering: https://docs.microsoft.com/en-us/security/engineering/solving-tls1-problem