KPMG

The rise of ransomware

As this growing cyber threat gains currency worldwide, organizations need new mitigation strategies to protect themselves

Introduction

According to the National Security alliance, ransomware has become one of the world's biggest cybersecurity threats today.[1] While on the surface, ransomware may seem like a simple attack, it actually involves complex and diverse strategies that hinder recovery.

More specifically, ransomware attacks involve the use of an executable to encrypt an organization's sensitive files, after which the files are held hostage until a ransom is paid. If the target of the attack refuses to pay the ransom, then attackers often threaten to delete the data or release it to the public. However, it should be noted that deleting the data deprives attackers of the leverage needed to extort payments from their targets.

Cyberattackers use different network penetration strategies to gain access to data, including phishing, stealing Remote Desktop Protocol credentials, using brute force, and exploiting software vulnerabilities. No matter how threat actors gain access to an organization's sensitive data, ransomware attacks often result in heavy financial loss and irreparable damage to their reputation.

History of ransomware

The first known occurrence of ransomware was in 1989. It was called AIDS Trojan, also known as PC Cyborg, and was developed by Dr. Joseph Popp, who distributed floppy disks at an AIDS research conference that contained the ransomware.[2] Researchers brought the floppy disk home and installed it. A program on the floppy disk counted the number of times the machine rebooted. Once the machine has rebooted 90 times, the user's filenames were encrypted and a message would show up demanding $189 to be paid to an address in Panama. While the attack worked, not many paid the ransom, and eventually, a decryptor was developed to restore the files. Some victims even wiped and rebuilt their machines, which resulted in the loss of years of AIDS research.

After the first occurrence of ransomware, there were no further occurrences until 2004, when the internet became much more popular and affordable.[3] More users were on the internet and became unsuspecting of the attack. Ransomware attacks didn't change much as they follow the basic steps like AIDS Trojan.

[1] Source: National Security Alliance, Cybersecurity for Business Section, "The Top Cybersecurity Trends for 2022" (October 13, 2021).
[2, 3] Source: Actualtech Media Ransomware Web site, what is ransomware section, "The History of Ransomware" (November 2021)
[4] Source: Associated Press, "Costa Rica, 'under assault' is a troubling test case on ransomware attacks" (June 17, 2022)0

Latest trends in ransomware attacks

Although there were few ransomware attacks between the first known occurrence in 1989 and 2004, the number of individuals on the internet today made this type of attack a much more viable option:

- ***More coordinated attacks:*** Ransomware perpetrators have evolved from single entities to groups of attackers. There are even groups that sell ransomware attack capabilities as a service. Groups that provide such services include the Hive Ransomware Group, which attacked Costa Rica's government services in 2022.[4]
- ***Increase in social engineering methods:*** There is an upward trend in the social engineering aspect of ransomware attacks, which involves sending a well-constructed phishing email to a victim, thereby gaining access to their confidential and sensitive data. Fortunately, some organizations are prepared with backup strategies that help them avoid paying the ransom.
- ***More modern means of ransom payment:*** As the nature of attacks and the strategies have evolved, so have the means of receiving the ransom payment. Such methods today include paying through digital currencies like Bitcoin, which are difficult to track back to the perpetrators.

Expansion of attacks surfaces from businesses to governments

Although businesses have long been an attractive target for ransomware due to their financial coffers, the current geopolitical situation has expanded attackers' purview to include governments as well.

Businesses: Businesses are enticing targets due to not only their financial resources, but also the vast amount of sensitive information they hold. Ransomware can show up in any industry, but it is more prevalent in sectors that rely heavily on data for their operations, such as finance, healthcare, and utilities.

That said, the impact on business operations differs from industry to industry:

- For example, in healthcare, if a patient's health record or protected health information data is released or locked by an intruder, then it can bring the medical operations of a given hospital or a clinic to a standstill, thus jeopardizing patient well-being.

By contrast, a ransomware attack on a technology company could impact not only the targeted company but also many companies that use their technology, thus effecting a massive halt of service and damage to the company's brand. Attacks on the fuel industry could lead to cessation of services if hackers gain access to internal systems through a leaked credential. Ultimately, attacks on the gas industry have driven an increase in gas prices. Attacks on food-based companies can cause disruptions in the supply chain, driving an increase in the price of supplies.

Governments: All around the world, ransomware can disrupt important national services managed and operated by the government. National leaders were so concerned with this growing trend that the Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation, National Security Agency (NSA), and International Partners issued a joint Cybersecurity Advisory that outlined the growing international threat posed by ransomware in 2021.[1] Separately, CISA and NSA have published important information and guidelines that governments can refer to and implement to protect themselves from a major ransomware incident.

Some recent government-focused ransomware attacks include:

- In 2021, a local U.S. county government system was attacked by ransomware called PayOrGrief. The attack blocked access to servers and disrupted services such as COVID-19 vaccination appointments. Furthermore, the attackers exfiltrated over two gigabytes of sensitive information.[2] In 2021, 14 of the 16 U.S. critical infrastructure sectors were involved in a ransomware incident.[3]
- Similarly, both the Australian and United Kingdom's Cyber Security Centers saw ransomware attacks on their infrastructures.[4]
- Given current geopolitical tensions, governments have become targets of attacks from foreign adversaries. Government leaders are hard at work devising policies and practices that can help shut down these types of organized attacks, which can transform into national security threats.[5]

The nature of ransomware attacks on cloud

Although cloud technology offers organizations flexibility (e.g., by moving their information technology infrastructure to a complete or hybrid cloud environment), the change in how data is stored, processed, and transferred can open up a wider cyberattack surface. For example, cloud applications such as virtual machine software, cloud application programming interfaces (APIs), data-backup processes, and storage services can be used as entry points to the entire infrastructure of an organization.

One strategy attackers often use is targeting local on-premises devices. Once they gain control of those devices, they can move laterally to the cloud to access more information. Additionally, according to Google, they can use denial-of-service attacks to distract organizations from discovering that their data is locked up for ransom.[6]

While some of the ransomware attacks today are sophisticated and complex, they can evolve and combat emerging security technology. In 2016, a security group from Turkey published the source code for the Hidden Tear ransomware on GitHub.[7] The security group wanted to show the masses how ransomware works and how to protect yourself from it. Instead, people with malicious intent took it and quickly made improvements and deployed their attacks. Today, according to ransomware.org, variants of ransomware attacks can be traced to the Hidden Tear source code, but with each passing year, the impact continues to diminish.[8]

Protective mechanisms against ransomware

While some groups have sought to publish guidelines for how organizations can protect themselves from ransomware attacks, there have been incidents of threat actors using this guidance to improve their attack methods. Today, however, there are a various of newer approaches that organizations should take into consideration, including the ransomware recovery vault, Google Cloud-specific tools, and tools like the KPMG ShardSecure-based methodology.

[1] Source: National Security Alliance, "CISA, FBI, NSA and International Partners Issue Advisory on Ransomware Trends from 2021" (February 9, 2022)
[2] Source: Internet Crime Complaint Center (IC3), Federal Bureau of Investigation PIN Number 20220330, "Ransomware Attacks Straining Local US Governments and Public Services" (March 30, 2022)
[3, 4] Source: Cybersecurity & Infrastructure Security Agency, "2021 Trends Show Increased Globalized Threat of Ransomware" (February 9, 2022)
[5] Source: Office of the Director of National Intelligence, "2022 Annual Threat Assessment of the U.S. Intelligence Community" (March 8, 2022)
[6] Phil Venables, "best practices to protect your organization against ransomware threats," Google, (May 21, 2021)
[7, 8] Source: Actualtech Media Ransomware Web site, what is ransomware section, "The History of Ransomware" (November 2021)

The ransomware recovery vault

Organizations are constantly trying to build and integrate technology that offers businesses continuity and resilience. The ransomware recovery vault is a comprehensive technology that provides efficient protection against ransomware and destructive malware. The solution is an air-gapped environment with data integrity checking, data immutability, and other robust mechanisms to ensure no harm is caused to valuable backup copies even during a ransomware incident.

The cost to implement and integrate a recovery vault solution in the cloud is less steep than in an on-premises environment. Further, from an implementation standpoint, cloud implementation of a cyber recovery vault is more viable as it can utilize the features offered by cloud services to deliver an efficient and resilient infrastructure.

Ransomware prevention on Google Cloud

Google Cloud comes with a host of security features that can be leveraged to enhance the security of the solution architecture. Organizations can utilize these controls to take the ransomware recovery vault solution to the next level, i.e., cloud-based, cost-optimized, and with robust security for backup data. Google Cloud's tools for data protection, such as encryption, immutability, integrity checking, and a custom sandbox environment, can help an organization plan its ransomware recovery strategy based entirely in the cloud. While scaling, organizations can continuously improve data security and services.

Finally, a Google Cloud–enabled implementation can help organizations manage compliance and regulatory requirements successfully. With Google Cloud's multiregion availability, clients can easily store their backup with the Google Cloud–a supported region they decide is best for complying with critical statutory and regulatory requirements. This will help eliminate any additional costs that organizations may otherwise have to absorb while setting up a ransomware recovery vault on the premises.

KPMG's approach to ransomware recovery

Most ransomware attacks focus on accessing an organization's data layer, thereby causing disrupt the business. In such circumstances, an organization under attack could be forced to pay out the ransom simply to resume its day-to-day operations. To help ensure business resiliency, KPMG Cyber Security services, in conjunction with ShardSecure, can help organizations neutralize the effect of cloud-based ransomware on data (see Figure 2) and protect and empower organizations to refuse to pay a ransom to safeguard their data and resume business operations.

How does microsharding work?

Microsharding involves a three-step process (refer to Figure 1 diagram):

1. Shred – Unstructured and structured data are shredded into four-byte microshards, which are too small to contain sensitive data.
2. Mix – Microshards and poison data are mixed across multiple containers.
3. Distribute – Containers are distributed to multiple, customer-owned storage locations of their choosing.

Organizations can choose the storage layer for the microshards, which could be a hybrid-cloud deployment or a single-cloud deployment. The technology microshards data and poisons it to make it impossible for an intruder to reassemble the data. ShardSecure stores the microsharded data in a distributed fashion among multiple storage locations. If an intruder gains access to one of the containers, then there would be no impact on the business since the original data can still be rebuilt using the self-healing capability of the product, which ensures data resiliency. The following diagram illustrates a high-level overview of the microsharding process performed by ShardSecure.

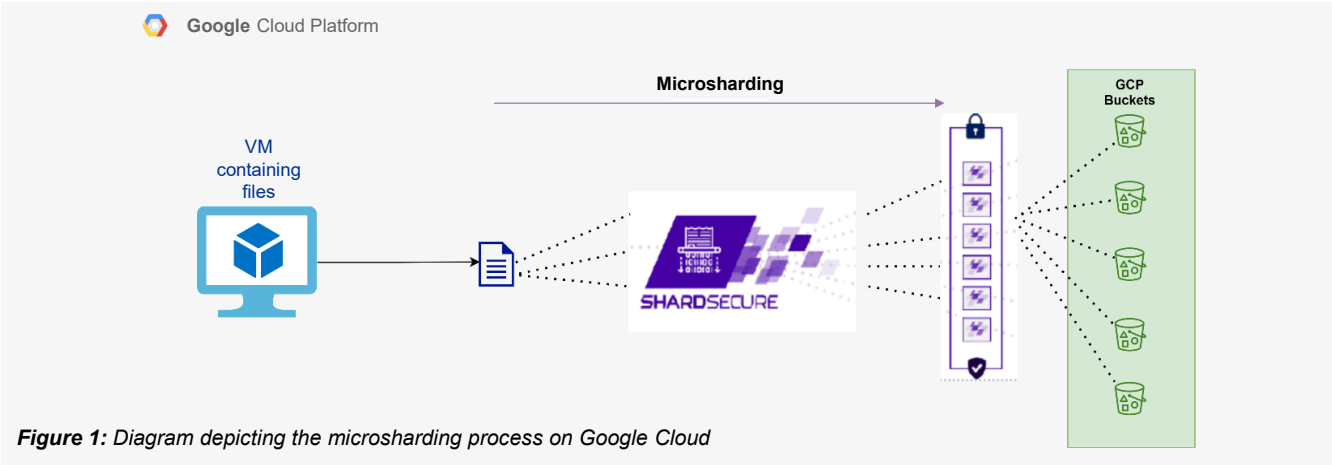

Figure 1: *Diagram depicting the microsharding process on Google Cloud*

Neutralize the effect of cloud-based ransomware attacks on data

Figure 2 depicts a scenario where ransomware gains access to an organization's environment and encrypts the data files (microshards) in a storage location. In other environments, this might bring the business operation to a standstill. Since ShardSecure underpins the data with RAID-like technology, the original data can be recovered without issue. This help ensure business resiliency through data availability even during a catastrophic situation like a ransomware attack.

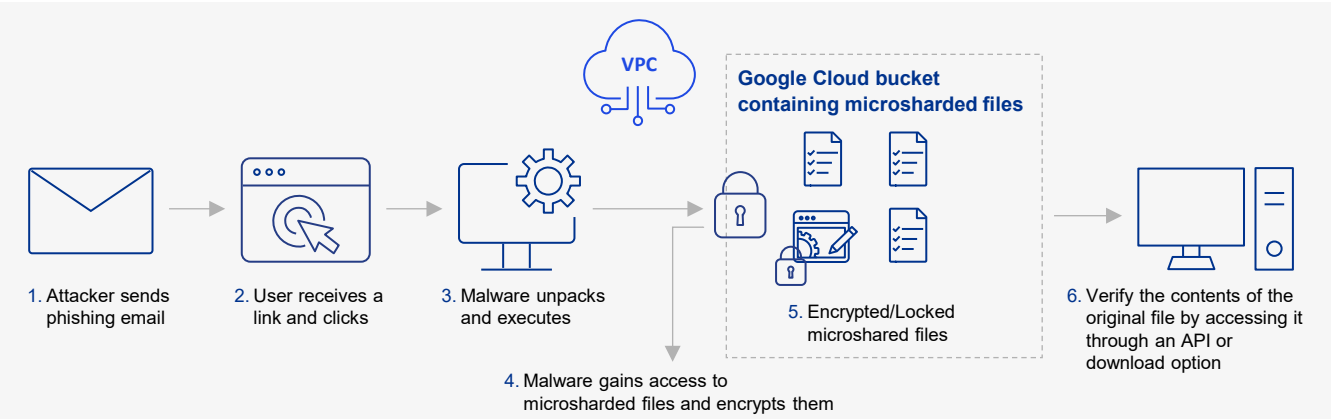

Figure 2: *Neutralizing effect of ransomware attack on data*

What are the first steps your organization should take?

Building and implementing a solution that offers ransomware protection and data recovery is imperative for every organization. Businesses are using and storing more data than ever and the need to protect the data is growing every day. Further, as more and more data are stored, it is much more efficient to implement an automated process to provide protection. Utilizing Google Cloud's tools, KPMG can help clients build a roadmap to advancing their data security workstream. In addition, ShardSecure is integrated into the KPMG cyber offering, providing an additional layer of security and the means of recovering missing data. With the combination of Google Cloud and ShardSecure, KPMG helps enable corporations and institutions to build a robust data security architecture while providing advanced controls and processes to attain the desired security level.

Authors

Sailesh Gadia
Partner – Advisory
KPMG LLP
+1 612 357 2484
sgadia@kpmg.com

Shashank Mishra
Senior Associate – Advisory
Cloud Data Security Architect
KPMG LLP
+1 214 840 2000
Shashankmishra4@KPMG.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us: **kpmg.com**