KPMG

What's next

**Ransomware attacks—
Do you know how to respond to and
prevent one before it happens?**

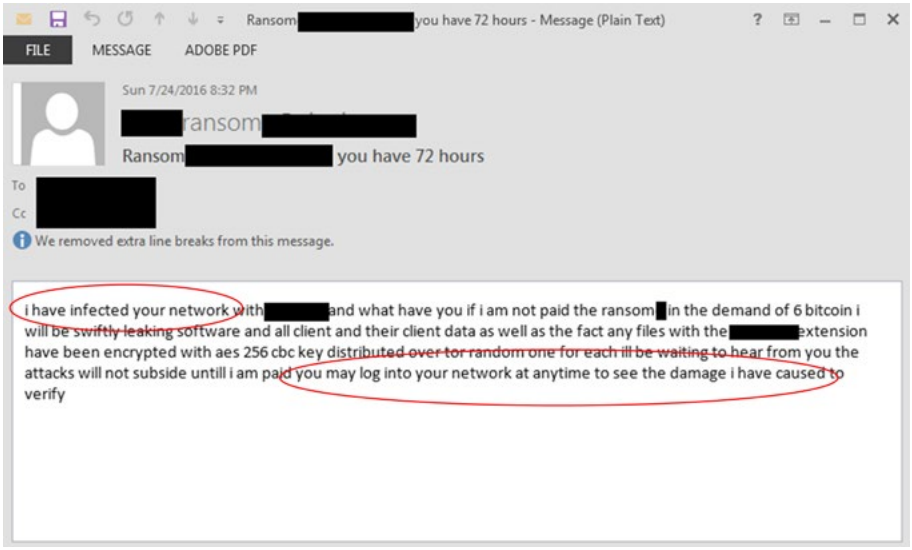
2018

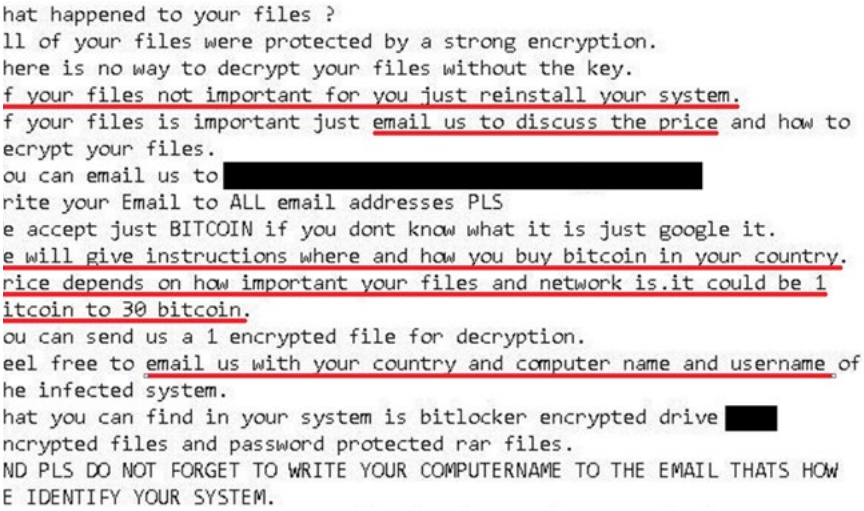
kpmg.com

The workday begins like any other—until you open your first e-mail message and discover a demand for money in exchange for access to your own data, which is now encrypted and in the possession of a ransomware attacker.

Would you know what to do if you received a message like those illustrated here, which depict actual messages received by our clients? Do you know if you have the appropriate policies and procedures in place for responding to an attack—or, better yet, the safeguards for preventing an attack in the first place?

Examples of actual ransomware demands (with identifying information redacted)





Source: KPMG LLP, 2018.

Understanding ransomware

Ransomware resembles other cyberattacks in terms of how it enters a network and propagates, but the threats it poses for businesses and individuals are often magnified.

In addition to loss of revenue, a ransomware attack prompts legal challenges and, in some cases, even national security concerns, along with the need to decide whether to pay the ransom to restore access to business systems and data. With recent attacks having crippled operations in cities and businesses worldwide, leaders of both public and private organizations are increasingly focused on identifying and addressing their own potential vulnerabilities.

For leading organizations worldwide, investing in cyber security has become a means of creating competitive advantage and driving business innovation and growth. Determining how to respond to ransomware in the context of a larger cyber security program will help companies address the specific threats they may face, ward off an attack and, if necessary, recover from one. A plan to protect the organization against ransomware should be a critical component of a broad, holistic cyber strategy that is aligned with the organization's business and governance objectives.

Scope of the problem

When ransomware shuts down operations or makes back-office software inaccessible, the immediate loss of revenue can be significant. When attackers also obtain customer data, legal issues quickly transcend technical concerns. A data breach (e.g., exfiltrated data) means attackers are able to demand a faster response and larger payment.

The trend of ransomware delivery from virus to worm to warfare has increased the concern among observant corporate boards, who are evaluating their international exposure in a new light. Although ransomware attackers could be company insiders or amateur outsiders, evidence increasingly shows they could also be sophisticated agents of a foreign entity or government. For example, after extensive investigation and with the support of numerous allies, the United States publicly attributed the massive WannaCry cyberattack in May 2017 to North Korea.[1] Foreign entities are especially effective in targeting and exploiting specific organizational weaknesses that tend to escape notice or seem insignificant.

High success rates have prompted increased investment by organized cyber criminals in "ransomware as a service" (RAAS), which allows less sophisticated attackers to outsource negotiations and payment facilitation in exchange for a way into an organization. Antivirus vendors noticed the trend early on and have done a good job of deploying signatures quickly, but ransomware attackers have found that commonly installed tools such as WinZip, BitLocker, 7Zip, and WinRar are just as effective at making data inaccessible.

[1] https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/

Preventing and responding to ransomware attacks

A mature and well-implemented security and controls program can help prevent many of the more common threats. With robust monitoring and control, a company can identify and repair vulnerable aspects of its environment to help prevent future attacks. Management and their executive boards must consider in what circumstances they would pay, or not pay, a ransom and then establish processes for decision making.

Preparation begins with a security assessment to quickly identify gaps and weaknesses. Tools to prevent the most prolific e-mail-based threats include properly configured spam-filtering, antivirus software, and employee training. When not accompanied by offline storage, real-time backup solutions do not provide adequate protection and only further increase the destructive impact of ransomware. Offline backup solutions are needed to supplement real-time backup solutions.

A policy guided by legal and business factors to formulate a response will significantly reduce stress and allow for a more informed response. Incident response policy, programs, and plans can significantly reduce the impact to the business and potentially diminish the success of the long-term legal challenges that can follow an attack. Combining successful monitoring and incident response will aid in quickly identifying the scope of the threat, which will further support remediation and eradication efforts.

Ransomware victims can be held legally responsible for their attacks

A ransomware attack is a red flag that points to a larger problem with the organization's overall cyber security protection program—namely, the likelihood that its business systems and data are vulnerable to other threats (e.g., remote access, phishing, or other illegal activity) for which it could be held legally responsible.

For example, in certain jurisdictions, a breach due to ransomware could be interpreted as a data disclosure event that in turn triggers a legal or reporting requirement. Or, if the attack results in the disclosure of personally protected information, the business could be liable for the release of private information. Thus, ransomware is not just a viral problem but a governance one.

How KPMG can help

When a company is the victim of ransomware, its leaders need an adviser who understands the larger legal and regulatory issues that could be at play—the governance considerations, not just the IT concerns. In the wake of an attack, you cannot afford to treat ransomware as merely a technical issue.

KPMG understands the broad legal, jurisdictional, and security implications a company faces in the wake of ransomware attacks. Having helped many companies deal with ransomware, we can help you understand and evaluate your response. For example, we never recommend paying the ransom: meeting the demands of an attacker that could be a terrorist or other illegal entity may not stop the attacks and could even increase them (the logic being that if you pay once, you will again). What is more, paying an attacker exacerbates the problem of ransomware in general, and it could result in legal or regulatory problems for you specifically. Nonetheless, we understand the business and stakeholder issues involved with recovering your assets quickly and can assist you in deciding on your next steps.

Those next steps should include determining how to guard against ransomware within the context of a holistic cyber security program. KPMG can help you develop and implement a cyber strategy that will allow you to innovate, transform, and differentiate your business—all while protecting your most critical assets. We have a deeply experienced, dedicated team with a broad understanding of cyber issues, encompassing strategy, governance, transformation, and response. We can help you respond to a single attack as well as prepare strategically with an overall program to safeguard your business assets.

KPMG

Contact us

Ed Goings
Principal
Cyber Security Services
E: egoings@kpmg.com

Steven Morrison
Director
Cyber Security Services
E: sjmorrison@kpmg.com

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

kpmg.com/socialmedia