Bloomberg Law

White Collar Crime Report™

HACKING

Four Perkins Coie LLP attorneys discuss the recent global ransonware attack, which hit all types of industries, including FedEx, hospitals in Britain's National Health Service, and automakers Renault and Nissan. The authors provide a road map for companies to follow to help mitigate the risks of being attacked, and also what to do if your company becomes a victim.

Global Ransomware Attack: How to Avoid Being a Victim and Steps to Take If You Were Attacked




BY SELENA J. LINDE, T. MARKUS FUNK, TODD M. HINNEN AND JONATHAN G. HARDIN

In the past two weeks, computer systems around the world were impacted by the largest cyber-extortion attack in history. According to news reports, the ''ransomware'' attack hit more than 250,000 victims in 150 countries since it began Friday, May 12, and the numbers continue to climb. Companies and organizations in all types of industries were affected, including FedEx, hospitals in Britain's National Health Service, automakers Renault and Nissan, Russia's Interior Ministry and Central Bank, Germany's national railway service, and universities and gas stations in China. In the intervening days, intelligence and security experts have identified hackers linked to North Korea as potential suspects.

The Attack Originates With The NSA and Winds Its Way Across the Globe

In this historic case, the ransomware used in this historic attack is known as ''WanaCryptor 2.0,'' or ''WannaCry.'' The attack draws upon the leaked vulnerabilities and hacking tools the U.S. National Security Agency reportedly used as part of its surveillance arsenal. Microsoft released updates in March 2017 that were designed to address the issue, but many computers remained vulnerable, because either system administrators failed to apply the patch or their organizations use outdated software.

While the attack swept quickly across Asia and Europe, its momentum fortunately slowed before it caused

 ISSN 1559-3185

significant damage in the United States. First, an analyst called ''MalwareTech'' discovered and implemented a temporary ''kill switch'' that bought more time for systems not already infected by the ransomware to be patched. Second, Microsoft released a rare emergency patch to better protect Windows XP devices, even though it officially stopped supporting XP in 2014.

The Attack Was Bad . . . But Could Have Been Much Worse

Unfortunately, the kill switch and security patch are not permanent fixes. In fact, there are already reports of more powerful versions of ransomware being released. And the first wave of WannaCry could have been an even more significant threat if hackers had actually extracted and threatened to expose confidential corporate data, rather than merely encrypting data without extracting it.

Further, in responding to this attack, analysts discovered that another global cyberattack known as ''Adylkuzz'' began nearly two weeks before WannaCry and was exploiting the same vulnerability. The Adylkuzz attack is not ransomware, but is a virus that reduces the speed of computer systems by stealing processing power to generate a digital currency. Some experts believe that Adylkuzz could be larger in scale than WannaCry and that the WannaCry episode might even have limited Adylkuzz's spread. Regardless, it is clear we are entering a new era of global cybersecurity threats.

The punchline here is that companies and organizations need to be prepared. To that end, this article analyzes:

- How ransomware works
- How to protect your company from victimization
- Immediate steps to take if and when you are attacked

How Ransomware Works

Ransomware is a type of malware most frequently transmitted by email. The malware, once ''in,'' encrypts all of the files on a computer using a key only the attacker has, and prevents the user from accessing any data unless a ransom is paid. The ransom, moreover, is time-sensitive and usually requested in the digital currency bitcoin, with the amount increasing as time elapses. If the ransom is not paid before the final deadline, the data is deleted and could be lost forever. Here, by way of illustration, is a screenshot of the WannaCry ransom demand:

Infection of ''Patient Zero'' Machine. Generally, ransomware attacks are triggered by clicking on links or attachments to fraudulent emails. There is a high chance this attack was transmitted in this manner.

Spread of Malware to Other Machines. Kevin Beaumont, a security architect, says that the malware spreads to unpatched machines through corporate VPNs, ininadequately secured Wi-Fi networks and other intranets.

Activation of Ransomware on Infected Machines. Once machines are infected, the malware is activated and data is encrypted. The desktop background changes, and a window appears with instructions to recover the data. A timer is displayed, which incentivizes victims to pay quickly to avoid scheduled increases-.Consider putting in call-out box

How to Protect Your Company From Becoming a Victim

We recommend that companies take the following actions:

Install all Updates. As noted above, Microsoft released a security update in March and additional security patches in recent days. The company released a statement on May 12, 2017: ''Those who are running Microsoft's free antivirus software or have Windows Update enabled are protected. Given the potential impact to customers and their businesses, Microsoft released updates for Windows XP, Windows 8, and Windows Server 2003.''

Unfortunately, many companies and organizations still use old operating systems and other software that developers no longer support. Such arcane software should be replaced immediately.

Ensure IT Policies and Procedures Are Best-in-Class.

- Use daily automatic file backup and offsite storage. Automatic data backups to offsite storage areas ensure that, if devices are infected, minimal loss will occur.
- Ensure that your IT department updates spam filters and firewalls daily.
- Have a system in place for automatically updating security patches within an hour of receipt.
- Disable macros, auto-play and file-sharing in employee email settings.

Properly Train Employees. As the U.S. Department of Homeland Security stated on May 12, 2017: ''Individual users are often the first line of defense against this and other threats, and we encourage all Americans to update your operating systems and implement vigorous cybersecurity practices at home, work, and school.''

- IBM estimates that ransomware is present in 40 percent of spam emails.
- A study done by Nuix showed that 84 percent of hackers utilize social engineering while carrying out their attacks. Ransomware is most commonly spread

  WCR ISSN 1559-3185

through attachments in emails (pdf, doc, etc.). Education of company personnel goes a long way toward preventing breaches.

- Do not click on unfamiliar links.

- Continually review security policies with all employees, and train employees on how to recognize and prevent phishing.

How to React If Attacked

- **Isolate the Malware**

You may be able to prevent the malware from spreading to other systems by isolating the malware. Disable connections between infected computers and resources and other parts of your network immediately.

- **Assess Backup Resources**

Determine when your last uninfected backup occurred. If you have strong backup practices, meaning that you back up frequently and your backups are not directly connected to your network, you may risk only losing a day's work as a result of the ransomware attack.

- **Initiate Your Incident Response Plan**

Now is the time to use the Incident Response Plan you had the foresight to adopt. Get the right decision-makers on the field, bring in outside counsel, follow your escalation plan, consult your outside vendors, activate your crisis communications , consult with outside counsel and work the problem until it is resolved.

- **Contact the Authorities—But Maintain Realistic Expectations**

Ideally, you will have an established relationship with your local FBI or Secret Service Cyber Unit. That said, no matter how familiar your company (or counsel) are with these agencies and their personnel, understand that in the event of a widespread attack the FBI may be inundated with victim complaints. Law enforcement most likely will not have the technical resources to resolve the ransom demand, but reporting demonstrates a proactive response.

Ransomware may trigger many different types of coverage. A company should immediately review its entire insurance portfolio when attacked and promptly notify all potentially relevant insurance companies.

If you have not identified a law enforcement point of contact in your Incident Response Plan, contact your local FBI Field Office directly (www.fbi.gov/contact-us/field provides a list of office by geographic location) or file an online complaint with the FBI's Internet Crime Complaint Center (IC3) at www.IC3.gov. Regardless of the option you chose, be prepared to provide the following information:

1. Date of infection.

2. Ransomware variant (identified on the ransom page or by the encrypted file extension).

3. Victim company information (industry type, business size, etc.).

4. How the infection occurred (link in e-mail, browsing the internet, etc.).

5. Requested ransom amount.

6. Actor's bitcoin wallet address (may be listed on the ransom page).

7. Ransom amount paid (if any).

8. Overall losses associated with a ransomware infection (including the ransom amount).

9. Victim impact statement (how the attack disrupted the business, shook company morale, etc.).

Review All Potentially Relevant Sources of Insurance And Provide Prompt Notice

Ransomware may trigger many different types of coverage. A company should immediately review its entire insurance portfolio when attacked and promptly notify all potentially relevant insurance companies. Below are the insurance steps that should be taken immediately.

Assess Potential Coverage While cyber insurance policies are the first obvious insurance policies to review, do not overlook the possibility of coverage in your company's crime, property policies, directors' and officers' policies, errors and omissions policies or bundled liability policies. All of these policies may contain coverage that could be applicable to a ransomware attack.

For example, the following types of coverages may be found under multiple types of policies:

- **Specific Ransomware Coverage**: Commonly called ''Cyber Extortion Coverage,'' this coverage pays ransomware demands and expenses in addition to other extortion schemes, such as threats to conduct a denial-of-service attack or unauthorized public disclosure of stolen personal or company information. This coverage often includes reimbursement of expenses incurred in obtaining the ransom currency on short notice (bitcoin, foreign currency, etc.) and applicable legal expenses.

- **Forensic Investigations Coverage**: Ransomware demands may be diversions. Companies are still determining the extent of the breaches that occurred at the end of last week. Often ransomware is only the beginning, and the hackers place additional malware on the computer system at the same time. Systems need to be swept and forensic investigations are needed to determine whether data was compromised or stolen.

- **Breach Response Coverage:** Almost all U.S. states have breach notification laws. Since the ransomware attack may have compromised your data, if notification is required by law, breach response coverage will pay for these costs along with the cost of obtaining privacy counsel.

- **Regulatory Coverage**: If the ransomware attack also included a breach of sensitive data, regulatory in-

vestigations may be warranted. Regulatory coverage often includes the costs of counsel needed to respond, as well as potential coverage for fines and penalties imposed against the policyholder.

■ **Data Restoration Coverage**: Found in multiple types of policies, this is first-party coverage companies can use if they need to recreate lost data, decrypt data or reinstall data from backup servers.

■ **Business Interruption Coverage**: Given ransomware amounts are often low, business interruption costs regularly account for the greatest losses to the policyholder. Ransomware events result in a loss of income while the policyholder is unable to access its computer system. This downtime may be extremely costly, especially for healthcare, retail and e-commerce organizations. Business interruption coverage will pay for the loss of income and/or extra expenses needed to help restore the system, after the application of an hourly waiting period, a self-insured retention or both.

Further, depending on whether your company's clients were affected, there may also be a case to be made for coverage under certain errors and omissions policies. Do not be discouraged when policy exclusions may initially appear to preclude coverage. The caselaw in this area is still in its infancy, and many policies contain ambiguous language that should ultimately be construed in favor of coverage. If you are unsure of whether coverage exists, you should reach out to experienced coverage counsel.

Notify Your Insurers Once you have reviewed your policies, provide prompt notice of claims, and determine whether to provide notice of circumstances under other policies. Your notice letters must conform to the requirements of the language in the particular insurance policy.

Further, depending on the nature of the known facts at the time of discovery, you should consider entering into nondisclosure agreements with your broker and insurance carriers that are specific to the attack. Companies should not wait until investigations are complete to provide notice. Instead, inform your insurance companies that you are still investigating and determining the facts, and update them as the investigations proceed.

Watch Your Words What you say to whom and how you say it, even in the initial notice letter, may make the difference between a covered and an uncovered claim. Be careful in the initial stages when characterizing your claims or discussing coverage with your insurance companies, your brokers or any outside consultants.

There are a number of issues that can significantly affect the existence or amount of an insurance recovery. For example, the coverage a claim falls under within a single policy may not be obvious initially. It may require a legal judgment that should not be made until the policyholder understands how the decision affects the amount and scope of the insurance coverage it may collect.

This could involve layers of analysis, including the law on the definition of fraud in all potentially relevant jurisdictions, the relevant deductibles, limits and sublimits under the policies and how the investigation into the attack is developing. Outside coverage counsel can work with risk managers and in-house legal counsel to ensure that a policyholder meets its reporting obligations without compromising potential coverage. Policyholders should avoid being bullied into making premature calls.

Select an Insurance Spokesperson To maintain a single cohesive message with insurers and your broker, you should identify one point of contact in your company who will communicate with the insurance companies and broker, along with outside counsel, throughout the life of the claim. This is usually the risk manager or in-house counsel. In addition to carefully watching what is said to your insurance companies, this individual should also be careful when discussing coverage issues with brokers or any outside consultants. In many jurisdictions, communications with a broker or outside consultants are not subject to any privilege. Thus, any unprotected communications may be discoverable if a coverage dispute ultimately arises.

Carefully Manage Forensic Consultants' Scope of Work Your forensic consultant's scope of work should be limited to determining how the attack occurred, restoring the computer system and files, and, if applicable, how your company's computer system was breached. If the fraud is a covered claim, these forensic costs are usually covered expenses under your insurance policy. Be careful, however, not to expand the scope of work into a full analysis of your company's policies, procedures and security controls. The forensic reports will be discoverable in any future coverage litigation. Any expansion in the scope of work, beyond the specific details of the current fraud could lead to ultimate findings by your forensic consultants that the insurance carriers may use to attempt to deny your claim or rescind your coverage.

Demand Your Insurers Fulfill Their Coverage Obligations Policyholders must demand that their insurance companies meet all contractual obligations. They should not accept any denial as final. Instead, a denial is often the beginning of the dance with an insurance carrier.

If policyholders eventually need to file suit or to arbitrate against their insurer, they should review the policies, and determine what steps need to be taken. Some policies contain mandatory waiting periods and mediation or arbitration prior to bringing a coverage suit. Policies also may contain suit limitation clauses that limit the policyholders' time to bring a suit or notice arbitration.

Since ransomware is fairly new and pervasive, policyholders should determine early which potentially relevant jurisdictions may apply and whether those jurisdictions have competing caselaw. If there is competing caselaw, the insurance company may ''jump'' the policyholder and file a declaratory judgment action in the less favorable jurisdiction. If you determine that you may have competing caselaw, you should consider filing a declaratory judgment action against your insurance carrier to preserve the forum of your choice.

Ransomware Prevention And Recovery Are Possible

Despite its simplicity, this type of scam can cripple companies. It isn't the price of the ransom but the distruption to businesses that could will put losses in the hundreds of millions of dollars. Companies can avoid falling victim to ransomware and other cyber attacks by regularly installing security updates, properly training personell, and taking some relatively simple steps such

  WCR ISSN 1559-3185

Selena Linde is a nationally recognized partner in Perkins Coie's Insurance Recovery Practice. She can be reached at slinde@perkinscoie.com.

Markus Funk, who served with the US Attorney's Office in Chicago and the US State Department in Kosovo, is the Firmwide Chair of Perkins Coie's White Collar & Investigations Practice. Markus can be reached at mfunk@perkinscoie.com.

Todd Hinnen, who served as the Acting Assistant Attorney General for National Security at the U.S. Department of Justice, is a partner in Perkins Coie's Privacy & Security Practice. Todd can be reached at thinnen@perkinscoie.com.

Jonathan Hardin is a counsel in Perkins Coie's Insurance Recovery Practice. Jon can be reached at jhardin@perkinscoie.com.

This article was adapted from a May 15, 2017, Perkins Coie Update ''Ransomware: How To Avoid It and What To Do If You Have Been Hit.''

as those discussed above. If your company does become a victim, contact experienced counsel to help guide your team as it through findsing and fixes the vulnerabilities in your system, protectsing the company's reputational and other interests, and maximizesing any insurance available to offset your lossesJust want to avoid saying that counsel will find the vulnerability for them. A technical vendor will likely do that, but they want us to hire that vendor for them.