The Computer & Internet Lawyer

Volume 37 ▲ Number 3 ▲ MARCH 2020

Ronald L. Johnston, Arnold & Porter, LLP, Editor-in-Chief

Increased Ransomware Attacks Are Affecting All Industries

By Craig A. Hoffman, David E. Kitchen, Theodore J. Kobus III, and Anthony Valach

Organizations across all industries, including government agencies, are facing a surge of ransomware attacks launched by cybercriminals. New types of ransomware principally causing this surge have the potential to cause significantly more business disruption and difficulty restoring computer data and networks. Attackers are also often demanding steeper amounts and are targeting small and medium-sized companies in addition to the larger organizations that often make headlines. Resources exist, however, to help organizations identify steps they can take to avoid becoming a victim and be better prepared to respond effectively.

Craig A. Hoffman (*cahoffman@bakerlaw.com*), a partner in the Cincinnati office of Baker & Hostetler LLP and a member of the firm's Digital Assets and Data Management Group, advises clients on the regulatory issues that arise from data collection and use. **David E. Kitchen** (*dkitchen@bakerlaw.com*), a partner in the firm's Cleveland office and a member of the firm's Digital Assets and Data Management Group, advises clients through data security incidents involving domestic and international laws and regulations. **Theodore J. Kobus III** (*tkobus@bakerlaw.com*), is a partner in the firm's New York office and chair of its Digital Assets and Data Management Group. **Anthony Valach** (*avalach@bakerlaw.com*), counsel in the firm's Philadelphia office, focuses his practice on privacy and data protection.

Today's Ransomware Threat and Organizational Costs

Organizations affected by ransomware attacks have limited choices:

1. Restore systems from available backups, which is the most efficient and least costly approach, but one that may not be available if backups were deleted or encrypted (increasingly more common with new types of ransomware);

2. Pay the ransom to obtain a decryption tool; or

3. Pursue business without the encrypted data.

Organizations of all sizes are currently facing highly variable ransom demands that often greatly exceed the average amounts paid in prior years. This variability includes both more sophisticated criminal networks who are making demands for hundreds of thousands or even millions of dollars, and newer, less sophisticated

actors who are using the same types of ransomware, but demanding lesser amounts. The financial impact is not limited to the amount of the ransom but includes operational, business interruption, reputational and other costs. Even if a decryption tool is obtained by paying the ransom, there are instances in which not all files can be restored, and it can take an organization several weeks to restore infected systems.

Steps to Protect Against This Threat

While cyber liability insurance provides financial assistance and help connecting to law firms and forensic firms to guide organizations through the response, the following are steps organizations can take now to avoid becoming a victim and be better prepared to respond effectively to ransomware attacks.

- *Avoid being phished*: Most attacks start with an employee falling victim to a phishing email. Through phishing emails, attackers can obtain access to an organization's computer system or steal an employee's access credentials before deploying the ransomware. Train employees to spot suspicious emails and avoid common social engineering tactics. Also look into using an email threat filter.

- *Use strong passwords*: Attackers also exploit organizations with weak password policies. Require the use of strong passwords that must be changed periodically, prohibit reuse of passwords and implement a password management tool for employees.

- *Enable MFA*: The use of multifactor authentication ("MFA"), particularly for remote access to systems and email by employees, can lessen the risk of an attacker accessing your system or email accounts with stolen credentials. MFA creates an additional layer of authentication by requiring the employee to input a unique code before access is granted.

- *Secure remote access to company systems*: In addition to establishing a foothold in the environment through a malicious link or attachment in a phishing email, attackers frequently seek to connect to systems using Remote Desktop Protocol ("RDP") before moving laterally within the system to deploy ransomware. Adopt controls to restrict source IP addresses seeking RDP access. This can be done by requiring the use of a third party to connect to your system remotely or by using a virtual private network ("VPN").

- *Limit use of domain administrator accounts*: Many recent attacks have been preceded by compromise of credentials for a domain administrator account. Such accounts should be limited to select employees who need administrator permissions and, even for such employees, should not be used for normal work functions. Administrators should have separate accounts to use for their non-administrative functions.

- *Maintain good access controls, least privilege*: The greater the access a compromised employee's account has to different parts of an organization's computer system, the more easily ransomware can spread. A basic tenet of good cyber hygiene is to limit an employee's access to the minimum systems and files necessary to do his or her job.

- *Segment the network*: Attackers often move laterally to deploy ransomware to as many systems as possible. By identifying and segmenting critical data stores from systems accessible from the internet, an organization can limit the impact of an attack.

- *Ensure backups*: Organizations that have updated, intact and accessible backups segmented from production systems are in a much better position to respond to and recover from a ransomware attack. Adopt and implement a procedure for the creation, updating, and storage of on-site and off-site backups of all critical files and data. Be sure to include procedures for verifying and testing your backups and for securing them so they are not impacted by the ransomware attack. The right vendor or backup solution can allow for a quick recovery, with minimal operational impact, in the event of a successful ransomware attack.

- *Ensure patch management*: Attackers often exploit software vulnerabilities that could have been remedied by regular and timely deployment of the software developer's updates and patches. Ensure that your organization has a solid plan in place to manage this process.

- *Configure firewalls properly*: Many types of ransomware attempt to move laterally within systems using standard Windows Operating System protocols, including Server Message Block ("SMB"), to communicate between endpoints within a system. Ensure that your Windows firewall policy is configured properly to restrict the scope of permitted communications between common endpoints.

- *Deploy endpoint monitoring*: Endpoint monitoring solutions can detect system anomalies and malware, such as credential harvesting tools, that often precede a ransomware attack. Evaluate your current endpoint monitoring solution and determine whether it should be upgraded to properly protect against the current malware and ransomware threats.

Conclusion

If you suspect that a ransomware attack is underway, contact your insurance carrier immediately. Your carrier can direct you to legal, forensic, and other services available under your policy.