APRIL 2016

CYBERSECURITY BULLETIN

Borden Ladner Gervais

GOVERNMENT GUIDANCE FOR PREVENTING AND RESPONDING TO RANSOMWARE ATTACKS

Ransomware attacks are a significant and increasing threat to organizations of all kinds. Government agencies have recently issued guidance for preventing and responding to ransomware attacks. Organizations should consider that guidance and take appropriate steps to prevent, and prepare to respond to, ransomware attacks.

RANSOMWARE

Ransomware is malicious software that prevents access to or use of an infected information technology device or system (an "IT Resource") or related data, and demands (typically through an on-screen warning or other form of ransom note) that a ransom be paid (often in virtual currency or other forms of untraceable payment) by a specified deadline to obtain a key to restore the infected IT Resource or data. There are two basic kinds of ransomware: "locker" ransomware (which prevents use of an IT Resource by locking the user interface) and "crypto" ransomware (which encrypts specific files or data so they cannot be used without the required decryption key).

Ransomware is often installed on an IT Resource through fraudulent techniques, such as a deceptive email with a malicious attachment or link (known as "phishing" or "spear-phishing"), surreptitious downloading from an infected website (known as "drive-by downloading") or an infected message on a social media site. Sophisticated ransomware can spread throughout a computer network (including to data stored in cloud services) before the ransomware activates, and can install other kinds of malware on the network.

A ransomware attack can cause significant financial loss and other harm to the victim organization, including: (1) temporary or permanent loss of use of IT Resources and data; (2) business disruption loss and resulting liability to customers and business partners; (3) costs to restore infected IT Resources and data, if possible, and to otherwise respond to the ransomware attack; and (4) harm to the organization's reputation and relations with customers and business partners.

While most hackers profit by using or selling stolen data, ransomware criminals profit by demanding ransom payments from organizations and individuals whose IT Resources and data are affected by the ransomware. The primary result of a ransomware attack is business disruption and loss of use of data to the victim organization, rather than harm resulting from unauthorized disclosure of data, but some ransomware attacks can result in hackers obtaining access to data.

Paying a ransom is risky because the payment encourages ransomware criminals and does not guarantee that required restoration codes will be provided or that the ransomware and other malware will be removed from the infected IT Resource. Nevertheless, ransomware victims often chose to accept those risks and pay the ransom to avoid the cost, delay and other adverse consequences of relying on alternative remedies (e.g. attempting to restore infected IT Resources and data) if any are available. For those reasons, the number and sophistication of ransomware attacks have increased over recent years and are predicted to continue to do so.

GOVERNMENT GUIDANCE

On March 31 and April 1, 2016, the Canadian Cyber Incident Response Centre ("CCIRC") and the United States Department of Homeland Security Computer Emergency Readiness Team ("CERT") collaboratively issued related *Alerts* (CIRC AL16-005 and CERT TA16-091A) that recommend various measures to protect against ransomware attacks: technological measures (data back-ups, application whitelisting, up-to-date operating systems and application software, up-to-date anti-virus and anti-malware software and user restrictions based on the "least privilege" principle) and user education and training.

The *Alerts* discourage ransomware victims from paying a ransom. The CCIRC *Alert* warns: "Paying the ransom does not guarantee the encrypted files will be released; it only guarantees that the malicious actors receive the victim's money, and in some cases, their banking information as well. In addition, decrypting files does not mean the malware infection itself has been removed". In contrast to that advice, a member of the FBI's CYBER and Counterintelligence Program reportedly acknowledged in October 2015 that the FBI often advises ransomware victims to pay the ransom.

In March 2016, the Alberta Privacy Commissioner issued an *Advisory for Ransomware* to provide recommendations for preventing ransomware attacks. The *Advisory* recommends that organizations ensure that they have an incident response plan that deals with ransomware, and that they educate users about the plan. The *Advisory* reminds that if a ransomware attack results in unauthorized disclosure of personal information in the organization's custody or control, then the organization might have a statutory breach reporting obligation under the Alberta *Personal Information Protection Act*. Breach reporting obligations were recently added to the Canadian federal *Personal Information Protection and Electronic Documents Act*, but those provisions are not yet in force.

COMMENT

Organizations should prepare to respond to a ransomware attack by establishing and testing a detailed incident response plan that will enable the organization to make important technical, business and legal decisions in a timely manner. Those decisions may include the following:

- **Payment:** Should the organization pay the ransom? An organization that is not capable of successfully defending against a ransomware attack may have no choice but to pay the ransom and hope that the ransomware criminal provides the required key to restore infected IT Resources and data. Even if an organization is theoretically capable of successfully defending against a ransomware attack, there might be compelling pragmatic reasons to pay the ransom.
- **Reporting:** Should the organization report the ransomware attack? An organization may be under a legal obligation (under statute, generally applicable common or civil law or contract) to report a ransomware attack to law enforcement, regulators (including privacy commissioners), insurers, affected individuals (e.g. customers) and organizations (e.g. business partners) and other interested persons (e.g. shareholders and investors). In addition, there might be important business reasons to give notice of a ransomware attack to certain stakeholders even if there is no legal obligation to do so.
- **Remedies:** Does the organization have insurance coverage for the ransomware attack, and what are the applicable insurance policy requirements? Should the organization seek remedies for its costs and other financial losses against culpable persons (e.g. if the ransomware infection was caused by carelessness of a service provider)?

Organizations should obtain appropriate technical and legal advice when preparing a cyber incident response plan and when responding to a ransomware attack. ■

AUTHOR

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

BORDEN LADNER GERVAIS LLP
LAWYERS | PATENT & TRADEMARK AGENTS

Calgary
Centennial Place, East Tower
1900, 520 – 3rd Ave S W, Calgary, AB, Canada T2P 0R3
T 403.232.9500 | F 403.266.1395

Montréal
1000 De La Gauchetière St W, Suite 900
Montréal, QC, Canada H3B 5H4
T 514.879.1212 | F 514.954.1905

Ottawa
World Exchange Plaza, 100 Queen St, Suite 1300
Ottawa, ON, Canada K1P 1J9
T 613.237.5160 | F 613.230.8842 (Legal)
F 613.787.3558 (IP) | ipinfo@blg.com (IP)

Toronto
Scotia Plaza, 40 King St W, Toronto, ON, Canada M5H 3Y4
T 416.367.6000 | F 416.367.6749

Vancouver
1200 Waterfront Centre, 200 Burrard St, P.O. Box 48600
Vancouver, BC, Canada V7X 1T2
T 604.687.5744 | F 604.687.1415

blg.com