KPMG

Forensic Focus

kpmg.ca/forensicfocus

Beware of Ransomware

By Sivan Vaisman, Sr Manager, KPMG Forensic Services, KPMG in Canada and David Colantonio, Sr. Consultant, KPMG Forensic Services, KPMG in Canada

Today's news cycles seem to be full of cyber security incidents and instances of hackers launching attacks on individuals and businesses. These events seem to be happening on almost a daily basis and in certain cases, on an unprecedented scale. Ransomware specifically has been one type of attack that has featured more prominently in the last year. In a report by the cyber security firm Malwarebytes Labs, their analysis showed a 90% increase in ransomware detections by corporate customers and a 93% increase in ransomware detections by consumer customers in 2017 when compared to 2016. Others in the industry have been reported as predicting the global annual cost to victims of ransomware will climb to approximately $11.5 billion, with attacks against businesses predicted to occur every 14 seconds by the end of 2019[1]. As such, it is incredibly important to gain an understanding of ransomware, its risks, and what can be done to protect yourself or your business.

What is it?

Ransomware is a type of malicious software, or malware, which prevents users from accessing files on their computer or network, and demands a ransom payment in order to regain access. Computers are typically infected through means such as malicious email attachments, software updates with exploits, external storage devices, or vulnerabilities on networks. Once infected, the ransomware will lock the files – either through changing the user's login credentials, encrypting files, or preventing a computer from booting up – until the user pays a ransom to the threat actor. Some methods of infection often require participation by the user to deliver the malicious code – they may be prompted to open an attachment or interact with a screen prompt seemingly originating from a trusted source; however, ransomware can also spread on its own without user interaction. One example of this is "malvertising" or the use of online advertising to distribute malware. When browsing websites, users can be directed to criminal servers, which catalogue user and computer information and select malware best suited to attack the user, without the user even clicking on an online ad.

The goal of ransomware threat actors is to obtain payment from the user, often requested in cryptocurrency or some other method of payment that is difficult to trace. Unless an organization or individual maintains regular backups of their most critical and precious data, the only way for the owner of the files to regain access to them is to pay the ransom requested by the individual or group responsible.

[1] Cybersecurity Ventures, *2017 Ransomware Damage Report,* by Steve Morgan, accessed online: https://cybersecurityventures.com/ransomware-damage-report-2017-part-2/

What has it done?

There have been a number of recent examples of ransomware attacks that have had wide-ranging implications:

- Hancock Health, an Indiana-based hospital, was reportedly breached by a ransomware attack in January. The attackers targeted the hospital's email system, electronic health records and internal operating systems, and demanded four Bitcoins – reportedly valued at $55,000 at the time – in return for a decryption key. The hackers gained access to the hospital systems by logging in to the hospital's remote access portal with the credentials of a third-party vendor.
- An Oshawa-based hospital was among a long list of hospitals, companies and government offices, across 100 countries hit with a ransomware attack similar to that suffered by Hancock Health in May 2017.
- The WannaCry ransomware, which spread through the internet, also infected the British National Health Service (which reportedly had to turn away patients and cancel scheduled surgeries as a result). Major corporations like FedEx, Deutsche Bank and Honda, as well as the Russian Interior Ministry were also affected by this ransomware. WannaCry's authors reportedly demanded payment in Bitcoins within seven days before it deleted the files it had encrypted on each computer.
- Bad Rabbit ransomware encrypted files after prompting users to download a file masked as an update to Adobe Flash and reportedly infected parties in Russia and the Ukraine, including the Kiev Metro.

What are the risks and how do you protect yourself?

The effects on institutions can range from the loss of records or productivity due to the inability to access infected machines to the shutdown of large scale infrastructure and service providers. In all cases, investigation and remediation efforts are recommended. Although it is possible to remove ransomware before it fully infects a machine (if detected early enough), it is equally important to direct attention and effort towards preventing such attacks. Some precautionary measures, including:

- Investing and strengthening your cybersecurity infrastructure, specifically:
    - Real-time protection solutions that block processes attempting to make unauthorized changes to data
    - Exploit prevention solutions to stop ransomware from taking advantage of weaknesses in software running on your network
    - Solutions offering examination and detection of web content for ransomware related code
    - Implementing controls over the types of applications allowed to run
- Requiring regular data backups
- Keeping abreast of security news and promptly installing security updates issued by known software vendors
- Educating and raising employee awareness of the risk of ransomware to encourage them to exercise caution when opening e-mail attachments and internet links

What can KPMG offer?

KPMG International member firms have over 450 professionals globally who have managed the response and recovery from some of the largest and highest-profile cyber breaches. Our Cyber Incident Response team can leverage tools to rapidly identify, monitor, and contain malicious or suspicious activity.

Our 24/7 toll-free hotline is available to provide on-demand support from industry professionals.

Cyber Emergency?

Please contact our 24/7 Cyber response hotline

1-844-KPMG-911

1 (844) 576-4911

Sivan Vaisman
Senior Manager
Forensic Services
KPMG in Canada
T: 647-777-5358
E: svaisman@kpmg.ca

David Colantonio
Senior Consultant
Forensic Services
KPMG in Canada
T: 416-777-8990
E: dcolantonio@kpmg.ca

For more information, visit kpmg.ca/forensic or

Contact us

Montréal

Stéphan Drolet
T: 514-840-2202
E: sdrolet@kpmg.ca

Myriam Duguay
T: 514-840-2161
E: myriamduguay@kpmg.ca

Dominic Jaar
T: 514-840--2262
E: djaar@kpmg.ca

Ottawa

Kas Rehman
T: 613-212-3689
E: kasrehman@kpmg.ca

Greater Toronto Area

Peter Armstrong
T: 416-777-8011
E: pearmstrong@kpmg.ca

Colleen Basden
T: 416-777-8403
E: cbasden@kpmg.ca

Enzo Carlucci
T: 416-777-3383
E: ecarlucci@kpmg.ca

Joe Coltson
T: 416-777-8786
E: jcoltson@kpmg.ca

Corey Fotheringham
T: 416-218 7974
E: coreyfotheringham@kpmg.ca

Southwestern Ontario

Karen Grogan
T: 519-747-8223
E: kgrogan@kpmg.ca

Calgary

Paul Ross
T: 403-691-8281
E: pross1@kpmg.ca

Vancouver

Suzanne Schulz
T: 604-691-3475
E: saschulz@kpmg.ca

kpmg.ca/forensic