Aon Risk Solutions
Cyber Solutions

Client Alert: More Cyber Ransomware

Worldwide GoldenEye / Petya variant attack requires continued enterprise vigilance.

On June 27, 2017, a widespread cyber attack referred to by various names, including GoldenEye, Petya, NotPetya, and ExPetr, began impacting computer systems around the world. Similar to the recent WannaCry ransomware attack, victims are each being asked to pay a ransom of USD300 in bitcoin.

According to new research from Lloyd's of London, released on June 28, 2017, organisations could face a much higher bill than they expect, or are prepared for, after falling victim to a cyber-attack like this – especially if aggregated losses impact reinsurance coverage and pricing. Inga Beale, CEO of Lloyd's, said:

"The reputational fallout from a cyber breach is what kills modern businesses. And in a world where the threat from cyber-crime is when, not if, the idea of simply hoping it won't happen to you, isn't tenable. To protect themselves businesses should spend time understanding what specific threats they may be exposed to and speak to experts who can help handle a breach, minimise reputational harm and arrange cyber insurance to ensure that the risks are adequately covered. By reacting swiftly to mitigate the impact of a cyber breach once it has occurred, companies will be able to minimise the immediate costs and their exposure to subsequent slow burn costs."

The Lloyds of London report is apt considering that some of the world's largest companies, including WPP, Rosneft, Merck and AP Moller-Maersk were hit by this latest attack, which also took critical government and bank infrastructure in Ukraine offline, according to the Financial Times.

What Is this Ransomware?

The variant used in this most recent malware is derived from a family of ransomware whose primary function is not to encrypt files, but instead uses a bespoke bootloader to encrypt the Master File Table (MFT). This means that when the victim restarts their computer, the machine will not be able to boot into the Windows operating system. More recent versions include an additional module called Mischa that is responsible for encrypting files in the event that the MFT encryption fails.

The latest research on the ransomware used in yesterday's campaign reveals that although the ransomware does share some code similarities with prior iterations, there are also some significant differences. In particular, prior iterations have a different code base for the initial dropper and do not have the Mischa component that encrypts files.

This new ransomware variant is also designed to spread very quickly through an organisation's network once the initial infection has taken place, utilising multiple methods in order to propagate. Your organisation's files can be permanently encrypted if safeguards are not immediately put in place.

We're here to empower results

Adam Peckman
Global Cyber Risk Consulting Practice Leader
+44 (0)7803 695 386
adam.peckman@aon.co.uk

Spencer Lynch
Managing Director
Stroz Friedberg
+44 (0)20 7061 2304
slynch@strozfriedberg.co.uk

Simon Viney
Vice President Stroz Friedberg
+44 (0)20 7061 2286
sviney@strozfriedberg.co.uk

Vanessa Leemans
Global Cyber Chief Operating Officer
+44 (0)20 7086 4465
vanessa.leemans@aon.co.uk

Renette Pretorius
Global Broking Centre Cyber Team Leader
+44 (0)20 7086 6176
renette.pretorius@aon.co.uk

Shannan Fort
Global Broking Centre Cyber Product Development Leader
+44 (0)20 7086 7135
shannan.fort@aon.com

Kevin Kalinich
Global Cyber Practice Leader
+ 1 312 381 4203
kevin.kalinich@aon.com

aon.co.uk

From an insurance standpoint

Cyber ransom can be included in cyber insurance policies, subject to the following:

- In this case , the ransom demands were for US$300 per machine so only companies with a significant number of machines would incur a ransom loss excess of their policy's deductible.
- Under most policies, the insurer must be notified prior to the extortion payment being made.
- If the extortion payment is within the deductible, the insured must still notify the insurer to comply with both the notice and cooperation clause of the policy.
- Although there is obviously a desire to react swiftly to this type of event, a policy's notice and cooperation clause normally requires the insured to engage the insurer in decisions that could impact insurance coverage. Failure to comply with the provisions of the clause could result in the insurer denying subsequent forensics costs, liability payments, or business interruption loss that result from the same originating cause or source.
- Aside from the amount of any extortion payment, there is potential for financial impact through business interruption, forensics costs, lost productivity and potential third party liability.
- Coverage for cyber extortion is limited to indemnity for the amount paid to the extortionists. Separate coverage is available for business interruption, forensics costs, lost productivity and third party liabilities.
- Many insurers have "failure to patch" exclusions in their policies, which exclude coverage in the event that the vulnerability had been previously identified and not patched.
- Almost all policies exclude coverage for pirated software implementations. One of the possible reasons for the disproportionate impact on computer systems in some countries is the purported high incidence of implementing pirated software in these territories.
- Some cyber policies exclude cyber terrorism and cyber war.
- Some cyber policies require the insured to contact law enforcement to obtain approval to pay the cyber ransom. In some territories, payment of extortion demands is prohibited by law.

In addition to their Cyber policy, impacted companies should also review other insurance policies such as their Property and/or Terrorism & Sabotage policy, Kidnap & Ransom and/or Crime policy; Professional Liability and/or General Liability policy; Director's & Officer's Liability policy.

- Property and/or Terrorism & Sabotage policy: there could potentially be business interruption and forensics coverage under Property and/or Terrorism & Sabotage policies.
- Kidnap & Ransom and/or Crime policy: there could potentially be cyber ransom coverage under Kidnap & Ransom and/or Crime policies.
- Professional Liability and/or General Liability policy: there could potentially be third party liability coverage under professional liability and/or general liability policies.

Despite the urge to move swiftly in response to this crisis, we recommend that policyholders ensure that they understand and comply with the cooperation clause and notice provisions of their policies to ensure they preserve their right to insurance coverage.

From a technical standpoint, CISOs and technical leaders need to know the following:

- It is highly unlikely that files can be recovered by paying the ransom, as the email address victims are being provided has been blocked by the email provider. In addition, some research on the recent attack indicates that the key displayed to users for decrypting files was just random data and would not have worked under any circumstances.
- Blocking the attack vectors used by the ransomware to spread within networks should be a top priority. Steps to mitigate include:
  - Ensure your organisation has applied all current patches addressing the SMB server vulnerabilities (EternalBlue Vulnerability). Physical and virtual patching capabilities are both readily available.
  - If patching is not possible, segregate machines that are not patchable or block access to SMB ports on these machines (TCP/445 and TVP/139 in particular). These ports should also be blocked at the firewall and for any inbound network traffic devices.
  - After the initial infection, this ransomware variant waits for approximately one hour before rebooting to initiate the encryption process. Shutting down infected machines before this time period may prevent files from being encrypted. A LiveCD or external machine can then be used to attempt to recover files.
  - Where possible, disable Windows Management Instrumentation Commandline (WMIC).
  - Ensure local end points do not have administrative privileges and restrict non-critical administrative access until additional mitigating steps have been taken.
- Monitor the on-going analysis of how this ransomware attack initially spread. Some reports have indicated that a software update feature in a specific Ukranian accounting product may have been hacked, and the update feature used to push the ransomware automatically into organisations. If confirmed, this would represent an evolving development in 3rd party vendor risk considerations.
- It is essential to review your back-up systems to ensure they will allow you continued data availability despite the activation of malware on any system (which attempts to lock out users and threatens to destroy data unless the victim pays a ransom).

For ongoing technical updates, please visit **www.strozfriedberg.com/resource-center**

The CISO or technical team and the risk management team should coordinate actions. Understanding your organisation's insurance requirements is critical. Mitigating actions (however well intended) by the technical team in particular could impact the risk manager's ability to recover financial loss through insurance.

Aon recommend the following actions to improve cyber preparedness:

- **Patch Management:** Review the patch management programme, including use of automated patch management tools.
- **Access Management:** Ensure the minimum required access is applied throughout your IT systems, e.g. follow the principle of least privilege in relation to assigning access to business data, avoid users have local administrator access, control how IT administrators access user systems, etc.
- **Back-ups:** Deploy back-up systems that will allow continued data availability despite the activation of malware (which can attempt to lock out users from data and threatens to destroy data unless the victim pays a ransom).
- **Incident Response Planning:** Formation and preparation of an incident response team in advance of an incident to facilitate quicker, more accurate, more coordinated and more comprehensive responses. Critical external team members should include:
  - Legal experts to provide legal and regulatory guidance.
  - Digital Forensics vendors to determine the source of infection and causality, affected data, and expedite system remediation.
  - Claims preparation experts who are familiar with the rapidly evolving insurance policies and business interruption coverages, to support claims preparation and advocacy.
- **Tabletop Simulations / Incident Response Rehearsals:** Companies should conduct tabletop simulations or rehearsals of their Incident Response plans with key decision makers to ensure the plans are appropriate and responsive. Key decisions in this exercise would include whether to pay the ransom, how to comprehensively assess, remediate and recover from any damage done, which (if any) other parties to include in this process, and what actions may need to be taken to comply with applicable law.