MUNICIPAL EXCESS LIABILITY JOINT INSURANCE FUND
9 Campus Drive, Suite 216
Parsippany, NJ 07054
Telephone (201) 881-7632

MEL CYBER TASK FORCE BULLETIN 19-01

Date: **January 9, 2019**

To: **Fund Commissioners & IT Managers of Member Joint Insurance Funds**

From: **Underwriting Manager, Conner Strong & Buckelew**

Re: **URGENT SECURITY THREAT: New Ransomware – Ryuk**

The MEL saw a number of cyber claims at the very end of 2018. While the holiday season is a very popular time of year for cyber criminals, the number of claims was unusually high. As the incidents are being dissected, the MEL is noticing most of the claims containing a new strain of ransomware, called Ryuk. The New Jersey Cyber Communications and Integration Cell (NJCCIC) reported in late August the Ryuk strain was first detected in early August of 2018 by Check Point Research, a leading cyber threat intelligence company. According to Check Point's report, the Ryuk strain seemed to be related to other existing ransomware, indicating the same creator. The NJCCIC update indicates Ryuk is very advanced, killing many processes and embedding itself deep into the system, in addition to deleting backup files, making it difficult to successfully overcome.

The criminals appear to have learned that designing such advanced malicious software with a high success rate would pay off, as the ransoms demanded have been over $100k in each incident……and that is in bitcoin, of course (15 BTC – 50 BTC). In addition, the ransom escalates each day by 0.5 BTC.

Ryuk seems to enter via email phishing campaigns, weak Remote Desktop Protocol (RDP) passwords, and stolen credentials. Once the system is infiltrated, the attacker patiently waits and escalates their privileges until become an administrator on the system.

The MEL Cyber Risk Management Program offers key security recommendations which would help against these attacks, such as patching, requiring regularly updated passwords, good backup practices and cyber hygiene training. In addition, sources, such as Sophos and KnowBe4, recommend controlling RDP access, utilizing VPNs, initiating two-factor authentication, automatic lockout after a few password attempts and highly restrict administrative privileges.

In the recent news, Ryuk Ransomware was reported at the Chicago Tribune, Recipe Unlimited (Canadian Restaurant chain) and DataResolutions.net (a cloud hosting provider).

Following is a link to Check Point's initial publication on Ryuk:
https://research.checkpoint.com/ryuk-ransomware-targeted-campaign-break/

cc: Fund Executive Directors
Fund Professionals
Risk Management Consultants