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

MEL CYBER TASK FORCE BULLETIN 18-02

Date: **April 19, 2018**

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

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

Re: **URGENT SECURITY THREATS: Russia & New Ransomware**

Russia-Backed Malicious Activity

The New Jersey Cybersecurity & Communications Integration Cell (NJCCIC) forwarded an urgent advisory this week regarding malicious cyber activity carried out by the Russian Government. The "Technical Alert" was issued via the joint efforts of the US Department of Homeland Security (DHS), Federal Bureau of Investigation (FBI) and United Kingdom's National Cyber Security Centre (NCSC).

Primary Targets: Government and critical infrastructure, plus the internet service providers supporting both of these.

Targeted Devices/Software: Routers and switches

Type of Attack: Spoofing (man-in-the-middle)

Visit https://www.us-cert.gov/ncas/alerts/TA18-106A for full information and how to protect your organization.

New "Bad" Ransomware Strains

Our Cyber insurance partner (XL Catlin) and one of our forensic partners (Kivu Consulting) provided a warning regarding new ransomware. As opposed to the typical ransomware, the following "bad strains" have poor functionality, fatally corrupt large portions of the data, fail to decrypt properly and manned by volatile and unskilled attackers who are unable to troubleshoot decryption issues.

Strain	**Triple M (MMM)**	**Rapid**	**Thanatos**	**Sigma**
Demand	~$16k in Bitcoin	~$14k in Bitcoin	~$200 in Bitcoin	~$400 in Bitcoin
File Extension	None	.rapid	.thanatos	None
Issue	Cannot decrypt	Cannot decrypt	Cannot decrypt	Decryption delay
Other Payload		Destroys email files	Destroys data	

cc: Fund Executive Directors
Fund Professionals
Risk Management Consultants