Condon
O’Meara
McGinty &
Donnelly LLP
Certified Public Accountants

Established to serve
the unique needs of
not-for-profit organizations

Cybersecurity Threat: ***The “Fog”***

.

With summer drawing to a close, the last thing that nonprofit leaders want to worry about is a new ransomware threat. Yet, that is what has emerged, and is causing headaches to each of the entities it has infiltrated. This new virus has been dubbed “Fog.”

What is Fog Ransomware?

Fog ransomware is a sophisticated form of malicious software that encrypts files, rendering them inaccessible until a ransom is paid. Unlike traditional ransomware, Fog employs advanced techniques to evade detection. It often enters systems through compromised Virtual Private Networks (VPN) credentials, phishing emails, attachments, and compromised websites. Fog has been able to gain access to some Microsoft and Veeam back-ups and delete them as well.

The Fog attacks have focused on U.S. educational and recreational organizations and have succeeded by securing access to the entities’ main servers to encrypt files. Once the files have been encrypted, the attackers pass on their ransom note – typically under a filed named “readme.txt” – with instructions for paying the ransom to restore the files.

The Fog attacks have been successful because the ransomware works quickly from initial infiltration to encryption. Additionally, the attackers have shown little interest in leaking sensitive information or removing any information completely. Instead, they look for a fast payday.

Steps for consideration

- Data Backups:
  - Ensure that all critical data is backed up regularly and stored securely offline.
  - Encrypt back-ups
  - Make sure that back-up software is upgraded regularly

- Employee Education and Training:
    - Conduct ongoing cybersecurity training for employees to recognize phishing attempts and avoid clicking on suspicious links or downloading unverified attachments. This is usually the weakest link, and employees must be extremely diligent.
- Implement Strong Access Controls:
    - Use multi-factor authentication (MFA) to add an extra layer of security, just like your bank does! This should be implemented for any Virtual Private Networks (VPN) as well.
- Keep Systems Updated:
    - Regularly update all software, including operating systems and applications, to patch vulnerabilities that Fog ransomware could exploit.
    - Pay particular attention to any expedited updates considered “critical”. When an exploit is discovered in a particular piece of hardware or software, the manufacturer will issue a Common Vulnerabilities and Exposures (CVE) which will include patches. These should be applied as soon as possible.
- Documented “Action Plan” in case of breach.
- Work with your insurance agent to properly identify risk and remediation policies. Review any changes to your network infrastructure with your agent to maintain coverage.
- Scott Perry, from Flagship Networks recommends communicating with your cyber security experts to ensure they are proactively reducing your risks. Confirm that they are using a multifaceted layered approach in their solutions. If one product or service misses an attack, a second or third layer or type of protection should be in place to catch it.

Fog attackers find a way to log-in – usually with legitimate log-in credentials they have stolen – and proceed. So, now is the time to enhance log-in security, educate staff on cyberthreats, and ensure VPNs are not compromised. To say the least, dealing with cybersecurity can be confusing, but employing experts in this area can help reduce the risk of falling victim as well as dealing with ransomware attacks.

Article contributors

Kim McDonough, Director of Operations at COMD

Matthew O’Dell, CPA, Partner at COMD

Brad D. Steele, J.D., is Founder of PCC – and a longtime collaborator with COMD.