Ransomware Attacks Information Sheet

Recent cyberattacks using known Windows vulnerabilities and ransomware spread rapidly around the world and affected hundreds of thousands of machines. The massive attack affected personal and business computers, including critical infrastructure in several countries. Unprepared organizations can experience significant losses and disruptions, but strong fundamental security practices can prevent your organization from being victimized.

NCUA reminds credit unions to verify they have implemented and tested appropriate practices and actions that can prevent them from becoming victims of the “WannaCry” campaign or similar ransomware campaigns.

BACKGROUND

Ransomware is one of the fastest-growing types of attacks on business and personal computers. The recent WannaCry attack paired ransomware with a known Windows vulnerability, one of several vulnerabilities recently revealed by a group of hackers.

Microsoft issued security patches for the publically disclosed vulnerabilities for all supported Microsoft products and is urging customers to ensure their computers are patched and are running supported software. In addition, Microsoft also took the unprecedented step of issuing some patches for three operating systems that it no longer officially supports: Windows XP, Windows 8, and Windows Server 2003.

Although the impact in the United States has, so far, been limited, NCUA believes this avenue of attack will continue to be exploited by hackers and cybercriminals. NCUA urges institutions to validate that they have appropriately secured networks and technology assets to prevent damage or disruption to operations.

MITIGATION

The United States Computer Emergency Readiness Team, or US-CERT, has issued guidance on preventing ransomware attacks. Appropriate basic security practices can help stop most attacks. In addition to guidance provided by US-CERT, consider the following:

- Verify all of your networks and endpoints are patched and updated regularly. Consider automatically updating systems where possible.

- Replace equipment running older unsupported operating systems. For those rare cases where immediate decommissioning of legacy systems is impossible, isolate those systems from core networks and sensitive and critical systems and data.

- Verify the vulnerable protocol or file—Microsoft Server Message Book 1.0 (SMBv1)—is disabled or removed from your system.

- Verify that your vendors and third-party service providers connected to your networks or holding your data have implemented appropriate security practices.

- Ensure you have complete and tested current backups of all critical systems and data.
RECOMMENDED STEPS FOR REMEDIATION

• Contact law enforcement. NCUA strongly encourages credit unions to contact law enforcement upon discovery of an intrusion to report the incident and request assistance.

• Implement your security incident response and business continuity plan. Organizations should ensure they have trusted, secure backups so their response is not disruptive to the organization.

REFERENCES and RESOURCES


