

xMatters Cybersecurity – Microsoft SMB & Ransomware

by Robert Hawk

xMatters Privacy-Security- Risk Management Office

Monday 15 May 2017

Data Classification

Copyright 2017 xMatters inc. the contents of this document are the property of xMatters inc. All rights are reserved. Do not copy or distribute this material without permission.

This document is classified as Confidential Material and can only be shared with an established Non-Disclosure Agreement (NDA) between the receiving party and xMatters. Printed copies of this material are considered uncontrolled.

If this document is found in electronic or paper format outside of the offices of xMatters please stop reading at this point and advise xMatters Inc. immediately at:

Telephone: 1 (877) xMatters (962 – 8877)

e-Mail: info@xMatters.com

xMatters Service Delivery does not use Microsoft Windows technology and is not susceptible to the Critical Microsoft SMB Vulnerability or the Ransomware Cyber Attack that may be carried out due to the vulnerability. Client data is stored and processed in datacenters that use non-Microsoft Technology for service delivery. xMatters Corporate IT that uses some Windows technology is patched against this vulnerability.

Introduction

xMatters specializes in tool chain integration and communications over multiple devices that provide voice, Short Message System (SMS) text, electronic mail (email) and xMatters Mobile Application for Smart Devices running Apple iOS and Google Android. xMatters communications management is used for Business Continuity Management (BCM), Information Technology Management (ITM) and general notification. xMatters communications management service is defined as Software as a Service (SaaS) Private Cloud per the National Institute of Standards and Technology (NIST) Special Publications 800-145 – The NIST Definition of Cloud Computing.

Ransomware

Ransomware is a type of malicious software that carries out extortion after the target computer Hard Disk Drive (HDD) or the files on the Hard Disk Drive (HDD) have been encrypted by a cyber attacker. The ransomware then blocks access to data until a ransom is paid and displays a message requesting payment to unlock it.

Microsoft SMB & Ransomware

At this time there is a critical vulnerability in Microsoft Server Messaging Blocks (SMB) that can be exploited to install Ransomware (named: WannaCrypt).

xMatters Cybersecurity

xMatters cybersecurity uses a combination of vulnerability scanning, penetration testing and vulnerability notice from multiple vectors such as United States Computer Emergency Readiness Team (US-CERT), the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD), as well as product manufacturers to understand exposure to risks. Once detected risks are assessed, analyzed and treated.

References:

Microsoft Security Bulletin MS17-010 – Critical

<https://technet.microsoft.com/en-us/library/security/ms17-010.aspx>

Ransom: Win32/WannaCrypt

<https://www.microsoft.com/security/portal/threat/encyclopedia/Entry.aspx?Name=Ransom:Win32/WannaCrypt>

Multiple Ransomware Infections Reported

<https://www.us-cert.gov/ncas/current-activity/2017/05/12/Multiple-Ransomware-Infections-Reported>

Customer Guidance for WannaCrypt attacks

<https://docs.microsoft.com/en-us/msrc/customer-guidance-for-wannacrypt-attacks>

End of Document