Investigative Analysis and Technical Overview of Ransomware Based Attacks. Case Study: WannaCry

Cristian PASCARIU, Ionuţ-Daniel BARBU, Ioan C. BACIVAROV
EUROQUALROM - ETTI, University "Politehnica" of Bucharest, Romania
crpascariu@gmail.com, barbu.ionutdaniel@gmail.com,
bacivaro@euroqual.pub.ro

Abstract

This research represents the starting point of a process of reducing the attack surface in the case of ransomware attacks. The most recent cybersecurity alert - from May 2017- was a global one, and has, once again, drawn attention to the global importance of this issue and the need to take effective actions to counter cyber-attacks.

The main aim of this article is to describe the virus technical details, concentrating on the phases of the cyber kill chain. This research is intended to present this type of malware on the rise that affects users in both enterprise and personal space as well by encrypting user developed content and restricting access until ransom is paid.

The authors perform an analysis of WannaCry ransomware from the delivery, infection, mitigation and detection perspectives. This research represents the starting point of a process of reducing the attack surface in the case of ransomware attacks.

Needless to say, the first layer worth addressing is represented by the weakest chain in the information security link, the end user. With the advent of complex techniques, tactics and procedures used by the adversaries, Information Technology Professionals focus their efforts on defending environments from advanced persistent threats and highly sophisticated attacks. WannaCry ransomware came in as a caveat in this context, a way of reminding the industry that efforts should be divided into addressing the various layers of the defense in depth model.

Index terms: Security, Cybersecurity, Social engineering, Encryption, Ransomware, MS17-010, WannaCry, Defense in depth

References:

[1]. C. Pascariu, I.D. Barbu, (2015). Ransomware – an Emerging Threat. International Journal of Information Security and Cybercrime, 4(2), 27-32. Retrieved from https://www.ijisc.com.

[2]. US-CERT. Indicators Associated With WannaCry Ransomware [Online]. Available: https://www.us-cert.gov/ncas/alerts/TA17-132A.

[3]. Microsoft Security Bulletin MS17-010 [Online]. Available: https://technet.microsoft.com/en-us/library/security/ms17-010.aspx.

[4]. WanaCrypt0r ransomware hits it big just before the weekend [Online]. Available: https://blog.malwarebytes.com/cybercrime/2017/05/wanacrypt0r-ransomware-hits-it-big-just-before-the-weekend/.

[5]. The worm that spreads WanaCrypt0r [Online]. Available: https://blog.malwarebytes.com/threat-analysis/2017/05/the-worm-that-spreads-wanacrypt0r/.

[6]. More than 150 countries affected by massive cyberattack, Europol says [Online]. Available: https://www.washingtonpost.com/business/economy/more-than-150-countries-affected-by-massive-cyberattack-europol-says/2017/05/14/5091465e-3899-11e7-9e48-c4f199710b69_story.html.

[7]. WannaDecrypt your files? The WannaCry solution, for some [Online]. Available: https://blog.malwarebytes.com/cybercrime/2017/05/wannadecrypt-your-files/.

[8]. How did the WannaCry ransomworm spread? [Online]. Available: https://blog.malwarebytes.com/cybercrime/2017/05/how-did-wannacry-ransomworm-spread/.

[9]. Player 3 Has Entered the Game: Say Hello to 'WannaCry' [Online]. Available: http://blog.talosintelligence.com/2017/05/wannacry.html.