Asigurarea Calitatii - Quality Assurance, ISSN 1224-5410
Vol. XXIII, Issue 90, April-June 2017
Pages 4-7

WannaCry Ransomware Analysis. 1 day, 150 countries, > 57k infected computers

Cristian PASCARIU, Ionuţ-Daniel BARBU, Ioan C. BACIVAROV
EUROQUALROM - ETTI, University "Politehnica" of Bucharest, Romania
crpascariu@gmail.com

Abstract
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. This paper 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 main focus is on the description of the virus technical details concentrating on the phases of the cyber kill chain. Therefore, the authors perform an analysis of WannaCry ransomware from the delivery, infection, mitigation and detection perspectives. The long-term goal of these efforts is to anticipate threats before turning into incidents and, consequently, decrease the impact. 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.

Keywords: Cybersecurity, WannaCry, Ransomware, encryption, cyber kill chain, defense in depth, social engineering, MS17-010

References:

[1] Pascariu, C., Barbu, I.D. (2015). Ransomware – an Emerging Threat. International Journal of Information Security and Cybercrime, 4(2), 27-32. Retrieve from https://www.ijisc.com.
[2] https://www.us-cert.gov/ncas/alerts/TA17-132A.
[3] https://technet.microsoft.com/en-us/library/security/ms17-010.aspx.
[4] https://blog.malwarebytes.com/cybercrime/2017/05/wanacrypt0r-ransomware-hits-it-big-just-before-the-weekend/.
[5] https://blog.malwarebytes.com/threat-analysis/2017/05/the-worm-that-spreads-wanacrypt0r/.
[6] https://www.washingtonpost.com/business/economy/more-than-150-countries-affected-by-massive-cyberattack-europolsays/2017/05/14/5091465e-3899-11e7-9e48-c4f199710b69_story.html.
[7] https://blog.malwarebytes.com/cybercrime/2017/05/wannadecrypt-your-files/.
[8] https://blog.malwarebytes.com/cybercrime/2017/05/how-did-wannacry-ransomworm-spread/.