Ransomware - an Emerging Threat

Cristian PASCARIU, Ionuț-Daniel BARBU
EUROQUALROM, University POLITEHNICA of Bucharest, Romania
proteus_web5@yahoo.com, barbu.ionutdaniel@gmail.com

Abstract
One of the most representative threats predicted for 2016 is Ransomware. This type of malware operates by restricting access to the data on an information system. The access is further regained after ransom is being paid by the affected entity to the malicious actors operating the ransomware. This article presents an overview of the threat and also both new and historical issues and functionalities. Furthermore it focuses on how ransomware works.

Index terms: ransomware, cryptoviral, RaaS, Hidden Tear, encryption, Tor

References:

[1]. Team Register. (2015, November 13). Ransomware-as-a-service surfaces, wants 10 percent profit cut [Online]. Available: http://www.theregister.co.uk/2015/11/13/ ransomwareasaservice_surfaces_wants_10_percent_profit_cut/
[2]. Utku Sen. (2015, August 16). Hidden Tear [Online]. Available: https://github.com/ utkusen/hidden-tear
[3]. Pierluigi Paganini. (2015, August 18). Hidden Tear Ransomware is now open Source and available on GitHub [Online]. Available: http://securityaffairs.co/wordpress/39419/ cyber-crime/ransomware-open-source.html
[4]. Talos Group. (2015, April 27). Threat Spotlight: TeslaCrypt – Decrypt It Yourself [Online]. Available: http://blogs.cisco.com/security/talos/teslacrypt
[5]. Fedor Sinitsyn. (2014, July 24). A new generation of Ransomware [Online]. Available: https://securelist.com/analysis/publications/64608/a-new-generation-of-ransomware/
[6]. Lucian Constantin. (2015, April 24). With Ransomware on the rise, cryptographers take it personally [Online]. Available: http://www.pcworld.com/article/2914692/ with-ransomware-on-the-rise-cryptographers-take-it-personally.html
[7]. KeriLynn Engel. (2015, May 25). The Relentless Rise of Ransomware (and How to Beat It) [Online]. Available: http://www.whoishostingthis.com/blog/2015/05/ 25/ransomware/
[8]. Ian Barker. (2015, June). Ransomware sees 165 percent increase in 2015 [Online]. Available: http://betanews.com/2015/06/09/ransomware-sees-165-percent-increase-in-2015/
[9]. FBI. (2015, January 20). Ransomware on the Rise [Online]. Available: https://www.fbi.gov/news/stories/2015/january/ransomware-on-the-rise
[10]. Alex Drozhzhin. (2015, July 14). TeslaCrypt 2.0 ransomware: stronger and more dangerous [Online]. Available: https://blog.kaspersky.com/teslacrypt-20-ransomware/ 9314/
[11]. Chip McSweeney. (2015, September 29). TESLACRYPT REVISED [Online]. Available: https://labs.opendns.com/2015/09/29/teslacrypt-revisited/

[12]. Richard Hummel. (2015, September 16). TeslaCrypt 2.0: Cyber Crime Malware Behavior, Capabilities and Communications [Online]. Available: http://www.isightpartners.com/2015/09/teslacrypt-2-0-cyber-crime-malware-behavior-capabilities-and-communications/

[13]. Trendmicro Team. Ransomware [Online]. Available: http://www.trendmicro.com/vinfo/us/security/definition/Ransomware

[14]. Kevin Savage, Peter Coogan, Hon Lau (2015, August 6). The evolution of ransomware [Online]. Available: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf

[15]. Roland Dela Paz (2015, November 25). FAKBEN Team Ransomware Uses Open Source "Hidden Tear" Code [Online]. Available: https://blog. fortinet.com/post/fakben-team-ransomware-uses-open-source-hidden-tear-code

[16]. Wikipedia. CryptoLocker [Online]. Available: https://en.wikipedia.org/wiki/CryptoLocker