Extortion on the Internet : the Rise of Crypto-Ransomware

Jean-Loup Richet

abstract:
This article highlights the transition from traditional ransomware threats (ransomware 1.0) to new and more complex attacks (crypto-ransomware) targeting desktop computers. The article suggests that cybercriminals will capitalize on malicious codes and target emerging and less-secured areas: mobile devices, M2M and the Internet of Things

Keywords:
Crypto-ransomware, Cybercrime, Malware, Internet of Things, M2M.

***

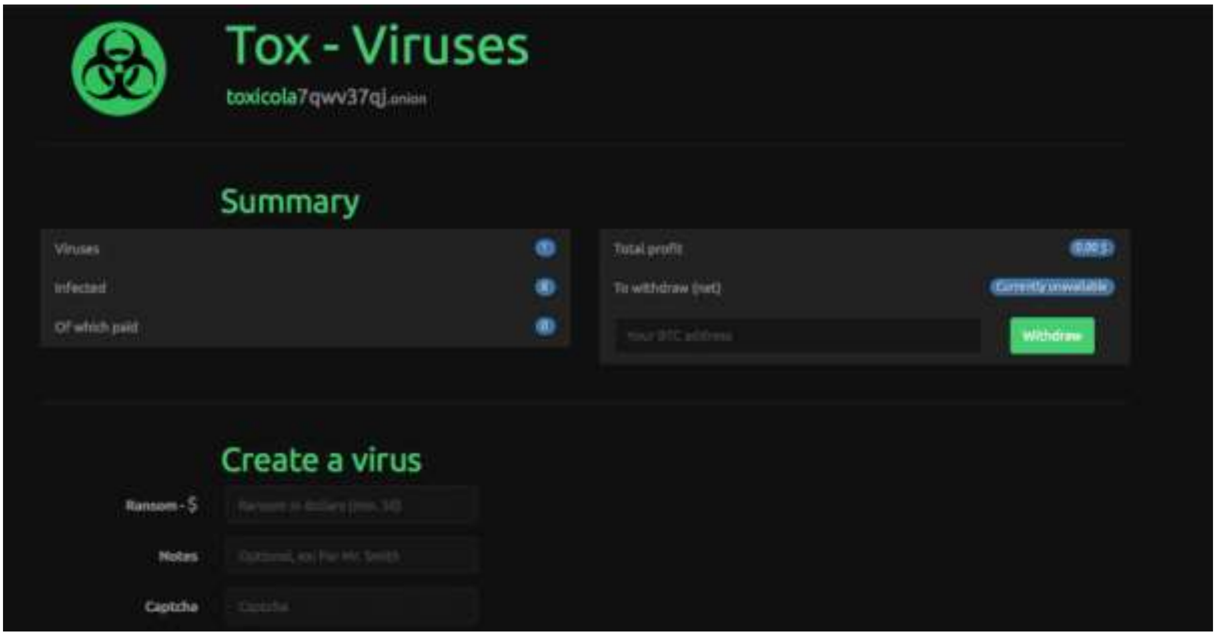
We all know the ransom mechanics: a hacker threatens an online business to flood its website with requests, thus resulting in a Denial of Service—which means the website will become unavailable and the online business will not be able to sell its products. Kshetri (2013) describes the story of an online CD and DVD retailer that "*paid a ransom of US$40,000 to a hacker based in Balakov, Russia* […] *the fund was wired to 10 accounts in Latvia.* [Money] *mules then rewired the money to St. Petersburg and Moscow. Another set of mules brought the money to Balakov. The computer server used to launch the attacks was in Houston*" (p.9).
However, this case involves what we could term as a 'manual,' 'targeted' and 'dedicated' attack and management: the attack is focused on one target, involves a specific threatening action and a relationship with the target (exchange, negotiation, etc.).
What we will discuss today is ransomware and its evolution: malicious software spread en masse and 'industrialized' (Richet, 2013). The hacker just needs to spread the malware, and all the other processes will be automated (fund reception through bitcoin, automated delivery of the decryption key through email, etc.).

There is a lot of 'basic' ransomware on the internet; spread through drive-by downloads, torrent, scams, etc., these common pieces of ransomware aim to scare users. Some are just scams and fear appeals, with no impact on data—for instance, fake antivirus warnings showing annoying pop-ups everywhere with messages like "*you have been infected by a dangerous malware, we are currently protecting your files, but sooner or later they will be deleted by the virus if you don't act. Click here to buy our antivirus and solve all your issues.*" Other ransomware can restrict computer use, preventing access to some programs or files—for instance, fake US government messages, again, through annoying pop-ups, with messages like "*you have downloaded copyright-protected content. We have restricted the use of your computer. Click here to pay your fine*." In 2006-2007, ransomware attack processes were quite straightforward—it simply stored selected files in a compressed archive, then password-protected these archives (Luo & Liao, 2007).

Gazet (2010) studied the wave of ransomwares spread in the summer of 2007, and made the following conclusion: "*Code is most often quite basic, no armoring, no pure jewel of low level assembly or nothing of this kind*. […] *The kind of ransomware we have analyzed for this study is clearly intended for mass propagation and we should not forget that ransomwares' strength comes from the fear they generate into lambda-user mind, not from their technical skills.* […] *The ransomware phenomenon is a reality that has to be monitored but in some ways it is not a mature and complex enough activity that deserves such communication around it. Ransomwares as a mass extortion means is certainly doomed to failure. Their extinction* […] *means that criminals have evolved to something else and other sources of income.*"

However, should we review this conclusion in the light of current trends in the cybercrime underworld?

In their report, Fossi & al. (2015) highlight this emerging issue: ransomware attacks more than doubled in 2014, from 4.1 million in 2013, up to 8.8 million. While describing eHealth security in the context of Australia, Foster and Lejins (2013) outlined the threat of ransomware targeting small Australian health organizations.



Tox - Viruses

toxicola7qwv37qj.onion

Summary

Viruses 1

Infected 0

Of which paid 0

Total profit 0.00 $

To withdraw (net) Currently unavailable

Your BTC address

Create a virus

Ransom - $ Ransom in dollars (min. 50)

Notes Optional, ex: For Mr. Smith

Captcha Captcha

Image description: Crimeware-as-a-service and ransomware: Tox is a ransomware construction kit that allows cybercriminals to create crypto-ransomware in a few clicks.

Moreover, ransomware codes have become more sophisticated and shifted from basic programs to well-designed crypto-ransomware. I define crypto-ransomware as the following: "A crypto-ransomware is a type of malware that encrypts a users' data. Data access is restricted until a ransom is paid to decrypt it." Virlock is a good example of current ransomware sophistication; this crypto-ramsomware locks its victims' screens, encrypts specific files (such as images, documents, musics, executable and so on) but has also self-spreading capabilities. What makes it stand out is the fact that this malware is polymorph (meaning the code changes each times it runs and is different for each infected host).

According to Fossi & al. (2015), crypto-ransomware expanded from 8,274 in 2013 to 373,342 in 2014.

What would be new areas of expansion for crypto-ransomware and their 'basic' counterparts?

My best guess is that cybercriminals will be taking advantage of the security loopholes of smartphones, as well as emerging IT trends such as M2M & the Internet of Things.

The number of mobile malware threats has exploded in 2013, and multiple mutated ransomware appeared in the Android application ecosystem (Apvrille, 2014)—what works on desktop computers could be easily mimicked in a mobile environment (Becher et al., 2011). According to Oberheide and Jahanian (2010), ransomware attacks have already targeted mobile users en masse in China.

As vehicles become increasingly connected in this Internet of Things era, they will also face the threat of ransomware in the years to come. Zhang, Antunes and Aggarwal (2014) highlighted this security challenge: "*ransomware could allow an attacker to remotely disable selected vehicle functions (e.g., lock the doors or the in-car radio, immobilize the engine) in a way that the vehicle owner's car keys can no longer activate them. The attackers can then demand ransom to be paid before reenabling these functions*" (p.14).

To sum up, we are experiencing the transition from traditional ransomware threats (ransomware 1.0) to new and more complex attacks (crypto-ransomware) targeting desktop computers. However, I believe cybercriminals will capitalize on malicious codes and target emerging and less-secured areas: mobile devices, M2M and the Internet of Things.

References:

Apvrille, A. (2014). The evolution of mobile malware. *Computer Fraud & Security*, *2014*(8), 18-20.

Becher, M., Freiling, F. C., Hoffmann, J., Holz, T., Uellenbeck, S., & Wolf, C. (2011). Mobile security catching up? revealing the nuts and bolts of the security of mobile devices. In *Security and Privacy (SP), 2011 IEEE Symposium on* (pp. 96-111). IEEE.

Fossi, M., Egan, G., Haley, K., Johnson, E., Mack, T., Adams, T., & Wood, P. (2011). *Symantec internet security threat report trends for 2015.* Volume XX.

Foster, B., & Lejins, Y. (2013). Ehealth security Australia: The solution lies with frameworks and standards. *Proceedings of the 2nd Australian eHealth Informatics and Security Conference*, 2-4 December 2013, Edith Cowan University, Perth, Western Australia.

Gazet, A. (2010). Comparative analysis of various ransomware virii. *Journal in computer virology*, *6*(1), 77-90.

Kshetri, N. (2013). Cybercrimes in the Former Soviet Union and Central and Eastern Europe: current status and key drivers. *Crime, law and social change*, *60*(1), 39-65.

Luo, X., & Liao, Q. (2007). Awareness education as the key to Ransomware prevention. *Information Systems Security*, *16*(4), 195-202.

Oberheide, J., & Jahanian, F. (2010). When mobile is harder than fixed (and vice versa): demystifying security challenges in mobile environments. In *Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications* (pp. 43-48). ACM.

Richet, J. L. (2013). From Young Hackers to Crackers. *International Journal of Technology and Human Interaction (IJTHI)*, *9*(3), 53-62.

Zhang, T., Antunes, H., & Aggarwal, S. (2014). Defending connected vehicles against malware: Challenges and a solution framework. *IEEE Internet of Things Journal*, *1*(1), 10-21.