Trusting Pirated Software

By: Nir Kshetri and Jeffrey Voas

Kshetri, Nir and Voas, J. (2019)."Trusting Pirated Software", IEEE *Computer,* 52(3), 87-90.

Made available courtesy of IEEE: https://doi.org/10.1109/MC.2019.2898719

Abstract:

What is the life span for a fixed version of a software product? Is it a day, a week, a month, a year, or more? There is no single answer. Each product is unique, based on what it does. The point is that all software has a life span for each unique version of itself.

Keywords: ransomware | pirated software | Microsoft Windows | software product | computer crime

Article:

The reason for posing this question lies in software's ultimate capability: malleability. Software can be changed easily, repeatedly, and quickly—and it usually is. For security-sensitive software products, malleability is necessary because vulnerabilities are continuously found, particularly in the early versions. Thus, code updates (patches) that fix vulnerabilities occur often and regularly. Users who do not receive and install the updates are left vulnerable, and those who never had access to the updates because their license to the software was illegitimate are particularly vulnerable.

Because pirated software products are rarely registered to actual users, these users will not get access to security updates from software makers. Therefore, our premise is simple: security-sensitive pirated software is likely a ticking time-bomb if the software has no access to patches.

Because of this issue, cybercriminals are increasingly focusing their attacks on countries with higher software piracy rates. For instance, in 2013, a Symantec report noted that cybercrime was increasing faster in Africa than any other region of the world.[1] Unlicensed software is recognized as a major source of cybervulnerability in developing economies. According to the Software Alliance BSA, malware from pirated software costs US$359 billion annually worldwide.[2]

Consider WannaCry—this ransomware was launched on 12 May 2017 and infected approximately 300,000 computers in 150 countries.[11] The attack cost Internet users thousands of dollars in ransom money and billions in lost productivity.[3] According to F-Secure, large numbers

of computers that were running unlicensed versions of Windows facilitated the spread of WannaCry, which only affected unpatched Windows systems.[4] While WannaCry also victimized Internet users from developed countries, the underlying cause varied among developing and developed countries.

Microsoft had known about the vulnerability in March 2017.[5] The company issued a software fix, which licensed users could download and install. However, many legitimate users did not patch their systems.[6] Users of licensed versions who patched their systems did not experience WannaCry attacks.

COUNTRIES

Table 1 details the impact on several countries that were hit by WannaCry. In China, universities, local governments, and state-run companies were suspected of having networks that were dependent on unlicensed Microsoft Windows products.[12] A senior network engineer for a Beijing-based technology provider noted that most of the WannaCry ransomware victims in China were the users of unlicensed software.[13]

Table 1. The countries affected by WannaCry.

Country	Percentages of unlicensed software installation[9]	Sample effects of WannaCry malware
China	66	By 15 May 2017, roughly 30,000 organizations were attacked. They included more than 4,300 educational institutions as well as government agencies, hospitals, shopping malls, and railway stations.[24]
India	56	By 17 May 2017, roughly 48,000 computers had faced attacks. Most incidents were reported in the West Bengal state,[25] including a state-run power firm.[19] Computers in 18 police units in the Andhra Pradesh state were also affected.[26]
Russia	62	Accounted for 20% of computers infected worldwide by WannaCry one week after the ransomware began.[27] By 15 May 2017, roughly 1,000 interior ministry computers using Microsoft Windows were attacked.[28] Its largest bank, Sberbank, was also attacked.[29]
Ukraine	80	A version of WannaCry attacked government websites and several companies.[30]

Russia also had a disproportionately large share of computers infected. Major victims included the country's interior ministry as well as its banks.

In India, government, diverse private sector industries, and individual consumers were affected. High-profile victims included the Southern Indian Railway, the West Bengal State Electricity Distribution Company Limited, police departments in the Andhra Pradesh and Maharashtra states, and a government-run hospital in the state of Odisha.[14]

In June 2017, the NotPetya malware hit. It started in the Ukraine, which, in the end, wound up being the most impacted by it. NotPetya infected multiple government agencies, energy companies, transportation infrastructures, and banks.[7] Pirated software was arguably one of the main factors that exacerbated the NotPetya attacks on Ukrainian systems.[8]

Next, we consider the computers that were infected by cryptor and cryptomalware.[15] According to the Kaspersky Lab, in the third quarter of 2018, the six countries with the highest cryptor

infection rates were Bangladesh, Uzbekistan, Nepal, Pakistan, India, and China.[16] Among these countries, according to Software Alliance BSA, Bangladesh and Pakistan had unlicensed software installation rates of 84 and 83%, respectively, in 2017.

In the United States, a smaller proportion of computers have become infected by ransomware. Companies in the United States tend to update and patch more regularly because of the threat of legal action.[17]

ENCOURAGING LICENSED SOFTWARE ADOPTION

Increasing vulnerability awareness

One cause of this software piracy problem is a lack of understanding of the link between unlicensed software and cybervulnerabilities. A greater awareness and clearer understanding of the cyberrisks associated with unlicensed software should begin to discourage this practice. For instance, South Africa's proportion of unlicensed software installation in 2017 was 32%—the global average is 37%.[9] In a recent survey, 54% of chief information officers in South Africa cited cyberrisks as the main reason to avoid unlicensed software.[18] Table 2 presents the potential measures that encourage the use of licensed software.

Table 2. The potential measures that encourage the use of licensed software.

Measures	Explanation	Examples
Increasing awareness of the vulnerabilities associated with unlicensed software	Understanding the threats and risks of unlicensed software products should discourage their use	South Africa: the majority of chief information officers consider cybersecurity risks as the number one reason to avoid unlicensed software.
Making licensed software more affordable	Increase incentives for using licensed software	India's negotiation with Microsoft to offer its software at a greatly discounted price.
Legislative and enforcement measures against the use of unlicensed software	Increase the cost of penalties for using unlicensed software	Weak law enforcement measures have led to higher rates of unlicensed software use in China and Latin American countries.
Regulatory measures with indirect effects on the use of unlicensed software	Introducing legislation that users of unlicensed software find difficult and expensive to comply with	The existence of laws requiring mandatory reporting of cyberattacks; this may discourage the use of unlicensed software.

LICENSED SOFTWARE AFFORDABILITY

One reason for using unlicensed software is that the licensed versions may be unaffordable. For example, in India in 2017, the Windows 10 Home Version cost ₹7,999 (roughly US$111.20) and the Pro Version used by institutions cost ₹14,999 (roughly US$208.40).[19] The country's average monthly income that year was US$162.[20] In Russia, Microsoft's Windows 10 operating system cost approximately US$140.92, which was roughly one-fifth of the country's average monthly income. Pirated copies can be downloaded for free at https://tinyurl.com/ydz4hfqu.

However, governments and software vendors may be able to work together to make current versions more affordable. Following the WannaCry attacks, India negotiated with Microsoft to offer Windows at a discounted price to the country's more than 50 million users so that they could upgrade to the Windows 10 operating system.[19]

LEGISLATIVE AND ENFORCEMENT MEASURES

Governments can adopt legislative and enforcement measures against unlicensed products. Intellectual property rights (IPR) infringement is often more a problem of enforcement than of writing laws against infringement.

When businesses violate IPR, proactive law enforcement can be cost-effective. For example, the Chinese government's measures to stop businesses from manufacturing pirated goods have demonstrated success. However, the root cause of piracy lies on the demand side. Software IPR violations may entail violating copyright protections by large, anonymous groups of users. It is difficult to control such violations because it creates congestion in legal systems.[10]

Similar findings have been reported in Latin America. Subject matter experts have been known to use unlicensed versions; however, it is not cost-effective to fight this widespread piracy.[21]

Success with reducing the use of unlicensed software has been achieved in countries that have implemented more effective law enforcement. As mentioned previously, South Africa has among the lowest rates of unlicensed software in use among developing countries. In a recent survey, 43% of South African respondents considered legal issues as the main reason that discouraged them from using unlicensed software.[18] Similarly, the software piracy rate in Egypt has decreased from 61% in 2015 and 59% in 2017 because of the government's enforcement measures that discourage the use of illegal software.[22]

REPORTING MEASURES

Reporting measures, which indirectly affect the use of unlicensed software, can be introduced. For example, the existence of laws requiring mandatory reporting of cyberattacks to regulatory agencies should discourage the use of unlicensed software if it is likely that law enforcement will investigate such attacks. Many organizations in India that were affected by the WannaCry ransomware did not report it to the government. India lacks regulations that require companies experiencing cyberbreaches to report them.[23]

The pervasiveness of unlicensed software can lead to cybervictimization. While most software vendors regularly issue patches that users download and install for protection, a proportion of users cannot take advantage of such resources. Those users will not have up-to-date patched systems.

The lack of law enforcement resources in fighting the use of unlicensed software is another obstacle. Police, prosecutors, and court systems may lack the resources or incentive to deal with this issue in a timely manner.

ACKNOWLEDGMENT

The authors are completely responsible for the content in this article. The opinions expressed are their own.

REFERENCES

1. C. Tredger, *Is Africa heeding the WannaCry wake-up call?*, May 2017, [online] Available: http://www.itwebafrica.com/security/513-africa/237932-is-africa-heeding-the-wannacry-wake-up-call.

2. S. Leesa-Nguansuk, *Local software piracy rate dips to 66%*, June 2018, [online] Available: https://www.bangkokpost.com/tech/local-news/1480229/local-software-piracy-rate-dips-to-66-.

3. N. Kshetri, J. Voas, "Do crypto-currencies fuel ransomware", *IEEE IT Prof.*, vol. 19, no. 5, pp. 11-15, 2017.

4. B. Schnieier, *Patching is failing as a security paradigm*, Nov. 2018, [online] Available: https://motherboard.vice.com/en_us/article/439wbw/patching-is-failing-as-a-security-paradigm.

5. N. Kshetri, *Should spies use secret software vulnerabilities?*, May 2017, [online] Available: https://theconversation.com/should-spies-use-secret-software-vulnerabilities-77770.

6. E. Redmiles, *The Petya ransomware attack shows how many people still don't install software updates*, May 2017, [online] Available: https://theconversation.com/the-petya-ransomware-attack-shows-how-many-people-still-dont-install-software-updates-77667.

7. T. Brewster, "NotPetya ransomware hackers took down Ukraine power grid", *Forbes*, July 2017, [online] Available: https://www.forbes.com/sites/thomasbrewster/2017/07/03/russia-suspect-in-ransomware-attacks-says-ukraine/#1760ea306b89.

8. M. Williams, *Ukraine finally battens down its leaky cyberhatches after attacks*, Aug. 2017, [online] Available: https://www.reuters.com/article/us-cyber-attack-ukraine-idUSKBN1AH35A.

9. *Software management: Security imperative business opportunity*, 2018, [online] Available: https://gss.bsa.org/wp-content/uploads/2018/05/2018_BSA_GSS_Report_en.pdf.

10. N. Kshetri, "'"Institutionalization of intellectual property rights in China"'", *Eur. Manage. J.*, vol. 27, no. 3, pp. 155-164, 2009.

11. "North Korean hackers behind global cyberattack?", *CBS News*, May 2017, [online] Available: https://tinyurl.com/kvewk73.

12. P. Mozur, "China addicted to bootleg software reels from ransomware attack", *NY Times*, May 2017, [online] Available: https://tinyurl.com/k6sy58r.

13. P. Mozur, "China addicted to bootleg software reels from ransomware attack", *NY Times*, May 2017, [online] Available: https://www.nytimes.com/2017/05/15/business/china-ransomware-wannacry-hacking.html.

14. "WannaCry ransomware attack: List of Indian states that have been affected", *The Indian Express*, May 2017, [online] Available: https://tinyurl.com/y7c2tfyp.

15. *Cryptor.*, [online] Available: https://tinyurl.com/ybzlqahk.

16. *WannaCry affected nearly 75000 users in Q3 2018: Kaspersky Labs*, [online] Available: https://tinyurl.com/ycqp4lx3.

17. E. Weise, M. Snider, "How U.S. dodged a bullet in Friday's massive global ransomware attack", *USA Today*, May 2017, [online] Available: https://tinyurl.com/ya5tjwws.

18. *Fewer South Africans using pirated software*, June 2018, [online] Available: https://tinyurl.com/yaqalqak.

19. E. Rocha, *India pushes Microsoft for Windows discount after WannaCry Petya*, July 2017, [online] Available: https://tinyurl.com/yb8pa96m.

20. *GDP per capita (current US\$).*, [online] Available: https://data.worldbank.org/indicator/NY.GDP.PCAP.CD.

21. R. Neff, *Why software piracy persists in Latin America*, June 2012, [online] Available: https://tinyurl.com/y7txx8pm.

22. "Egypt's software piracy drop and legal reforms boost foreign investment", *EABW*, Sept. 2018, [online] Available: https://www.busiweek.com/egypts-software-piracy-drop-and-legal-reforms/.

23. S. Shekhar, "WannaCry ransomware fears: Pirated software makes Indians more vulnerable", *Business Today*, May 2017, [online] Available: https://tinyurl.com/yb773mer.

24. Z. Soo, N. Ng, S. Chen, "Tens of thousands of Chinese firms institutes affected in WannaCry global cyberattack", *South China Morning Post*, May 2017, [online] Available: https://tinyurl.com/ya79qzf6.

25. "India third worst hit nation by ransomware Wannacry; over 40000 computers affected", *Economic Times*, May 2017, [online] Available: https://tinyurl.com/y94pqtdh.

26. "WannaCry ransomware: Andhra police fall prey to global cyber attack", *Hindustan Times*, May 2017, [online] Available: https://tinyurl.com/ybk4e3u9.

27. J. Stubbs, *Exclusive: Wannacry hits Russian postal service exposes wider security shortcomings*, May 2017, [online] Available: https://tinyurl.com/ydz4hfqu.

28. "Ransomware cyber-attack: Who has been hardest hit?", *BBC News*, May 2017, [online] Available: https://tinyurl.com/yasl98sj.

29. "WannaCry ransomware hit some Russian banks", *Fortune*, May 2017, [online] Available: https://tinyurl.com/y7a47qfm.

30. A. Prentice, *Ukraine official says version of WannaCry virus caused cyberattacks*, June 2017, [online] Available: https://tinyurl.com/ya55o68y.