NUS | Engineering
National University of Singapore

# **Cybersecurity Risks** from Non-Genuine Software

## The Link between Pirated Software Sources and Cybercrime Attacks in Asia Pacific

Microsoft

Study commissioned by
Microsoft Operations Pte Ltd, Singapore

# FOREWORD

Security is an ever-growing concern and the number of security breaches and their impact has increased with time, despite efforts to improve cyber defenses.

One of our key motivators behind this research was to investigate how malware infects computers, particularly in the context of Asia Pacific. Pirated software is still prevalent in the region and we wanted to characterize the link between software piracy and cyber risks. A total of eight countries were involved in this study – Malaysia, Indonesia, Thailand, Vietnam, Sri Lanka, Bangladesh, South Korea, and Philippines.

The means through which people acquire pirated software has changed over time, with downloads from peer-to-peer networks such as BitTorrent becoming increasingly popular. We found that the downloading and installation of pirated software is fraught with malware exposure at every step. It is evident that cybercriminals are increasingly using this medium to infect computers, steal information, create botnets etc.

That said, traditional methods of acquiring pirated software, such as buying counterfeit CDs and DVDs as well as preloading them in new computers by unscrupulous sellers, remain prevalent in this region. And we found that these non-genuine software frequently come with malware bundled with them. This shows that malware spreading through pirated software is still one of the common means of infection and more awareness among the users is needed.

This report also highlights multiple risks associated with pirated software that users are usually unaware of, or may not fully appreciate the severe consequences. In addition to the significant possibility of installing malware, getting a pirated software to work usually requires disabling many of the security-related features that puts the computer at serious risks. In many cases, a false sense of security may also come from the use of pirated anti-virus software, which, in reality, do not offer much of a protection and may include malware of their own.

Lastly, we wanted to use this opportunity to share best practices that organizations and individuals can adhere to better protect themselves and their data. At the end of the day, the most effective way for users to stay safe is to use genuine operating system and anti-virus software, which are updated and patched regularly.

**Associate Professor Biplab Sikdar**
Department of Electrical & Computer Engineering
National University of Singapore (NUS) Faculty of Engineering

# INTRODUCING THE NUS RESEARCH TEAM

### Associate Professor Biplab Sikdar

Department of Electrical & Computer Engineering

National University of Singapore, Faculty of Engineering

### Rahul Singh Chauhan

*Qualification:*
B.Tech in Mechanical Engineering from National Institute of Technology, Kurukshetra.

*Pursuing:*
M.Tech in Software Engineering from NUS.

### Siddharth Deshmukh

*Qualification:*
B.Tech in Electronics and Communication Engineering from Uttar Pradesh Technical University, India.

*Pursuing:*
M.Tech in Software Engineering from NUS.

### Ramkumar Rajendran

*Qualification:*
B.Tech in Electrical and Electronics Engineering from Amrita Vishwa Vidyapeetham University, India.

*Pursuing:*
M.Sc in Electrical Engineering (Computer Engineering Specialization) from NUS.

### Ritesh Khurana

*Qualification:*
B.Tech in Electronics and Communication Engineering, from the National Institute of Technology, Kurukshetra, India.

*Pursuing:*
M.Sc in Electrical Engineering from NUS.

# CONTENTS


Introduction ---------- 5

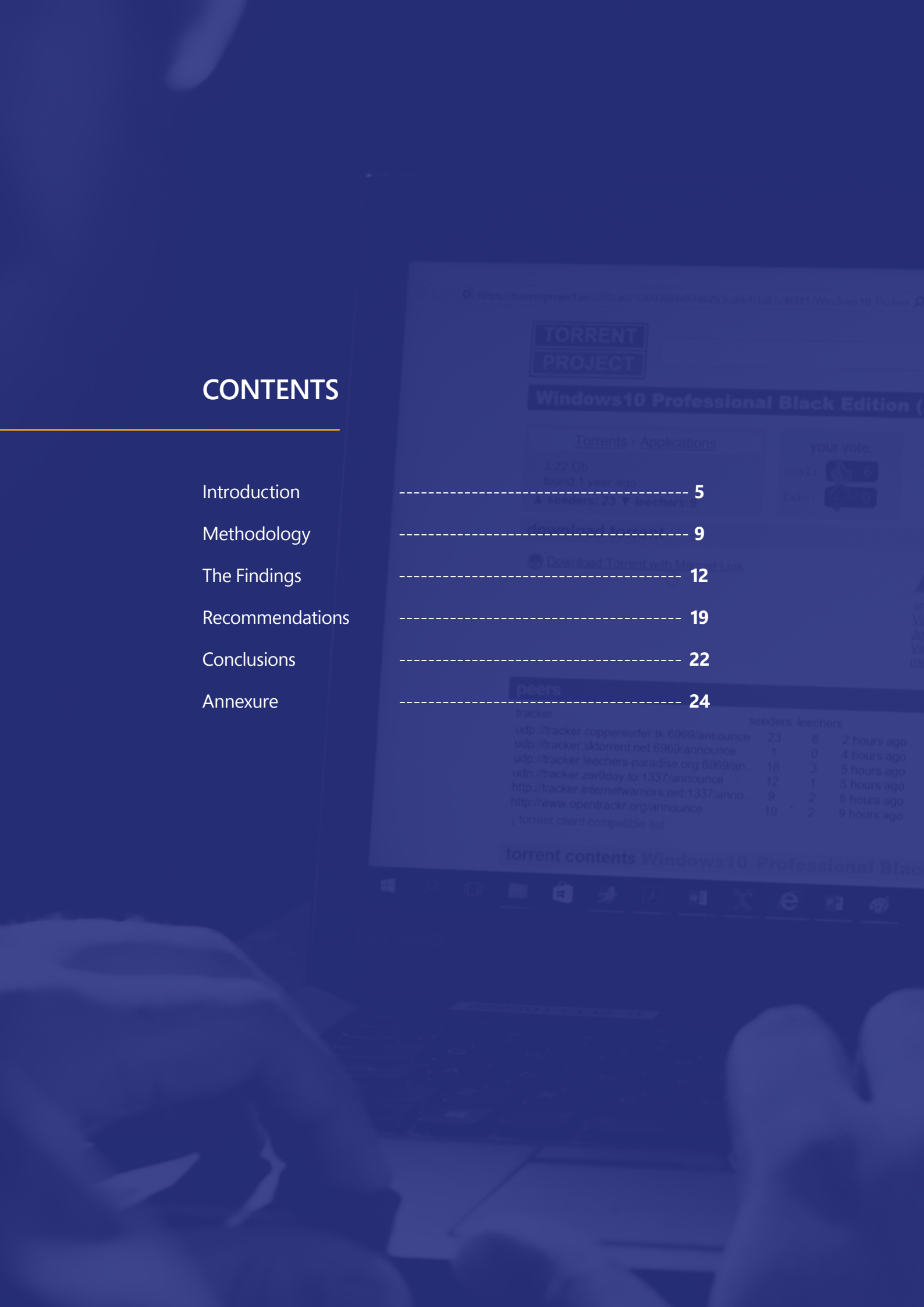
Methodology ---------- 9

The Findings ---------- 12

Recommendations ---------- 19

Conclusions ---------- 22

Annexure ---------- 24

# 1. INTRODUCTION

**a.** **Rise of Digital Transformation:** Digital information and computing technologies have permeated our daily lives. Starting from the prevalence of social media and networking affecting personal lives, computer based technologies have had a significant impact in the way we shop, access government services, connect with people, and interact with entertainment content.

Digital technologies are also starting to transform our economies and industries. The advent of machine learning and artificial intelligence (A.I) to interpret and make decisions based on advancements in the areas of big-data analytics and cloud computing, coupled with the rise of the Internet of Things (IoT) to facilitate the collection and dissemination of data, are some of the key driving forces of this transformation.

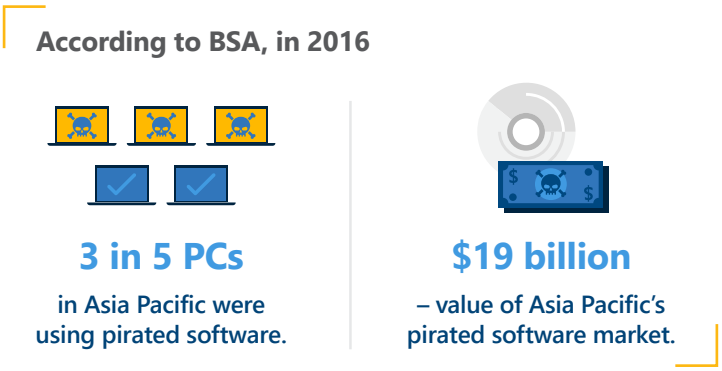
The digital transformation of our personal, social, and work environments has led to an increasing dependence on communication and computing technologies. We rely on the ready access to data and cloud-based services for many of our personal and business needs. These technologies provide convenience and efficiency and are a welcome opportunity.

*Digital transformation is changing the way we work, play and interact with each other.*

However, they also come with a wide range of cybersecurity issues. The improper use or use of untrusted information technologies can lead to serious cybersecurity risks and challenges for both organizations and governments but also small businesses and individuals.

Inadequate cyber-defenses such as improperly configured (or absent) firewalls and anti-virus software, use of unpatched software, lack of awareness on strong passwords and phishing attacks, lack of appropriate information technology policies and their implementation (e.g. on encryption, multi-factor authentication) etc. are some of the risk factors.

Additionally, in many parts of the world, the use of pirated/counterfeit/non-genuine software is a serious contributor to the growth of cyber-risks and is responsible for extensive economic harm and productivity losses. It is also causing a rise in cybercrime attacks and related losses.




Software piracy is an acknowledged global problem whose impact on industries, governments, small businesses and individual users goes far beyond economic issues. According to recent studies, the global piracy rate for personal computer (PC) software was around 39% in 2016, and the commercial value of the market for pirated software was $52.2 billion [1].

While pirated software is fairly prevalent among individual users, the rate of unlicensed use in banking, insurance, and securities industries is 25%, despite the latter having a stricter enforcement of regulations. While the economic implications of software piracy in terms of harm to intellectual property, revenue losses, lost jobs and taxes receive significant attention in the media and academia, another significant impact of pirated software comes in the form of an assortment of cybercrime risks.

Pirated software are increasingly becoming associated with the spread of various forms of malware (malicious software) such as worms, viruses, trojans, spyware, adware, droppers, to name a few. It is known that the malware are configured by cyber criminals to take advantage of various vulnerabilities in the host computer or a set of systems, to use or compromise sensitive/private information, steal money or disrupt, and can be executed and controlled remotely and covertly.

**b.** **Malware Infections through Pirated Software:** Malware in pirated software may originate from various sources. In certain cases the malware comes pre-installed or embedded in with the pirated operating system or application software at the point of sale.

Alternatively, some of the pirated software may require the user to visit certain websites to download activation keys or software bits, where such malicious websites install/drop malware onto the computer.

A third mechanism for the transfer of malware through pirated software comes from writable CDs (compact disks) and DVDs copied with pirated software. They may be purchased from online market places or brick-and-mortar stores. In many cases, these unauthorized CDs and DVDs come bundled with additional unwanted software and malware, which also gets installed along with the main application.

Finally, computers may also get infected with malware when visiting websites or peer-to-peer (P2P) services that offer pirated software downloads. Many of the pirated software also tamper with the systems, user accounts and security settings that are recommended by the vendors of the original software. We will discuss some of those examples in this study. Overall, such computers with pirated software become highly prone to easy malware infections.

*Pirated CD and DVD samples that the NUS researchers acquired for this study.*

c. **Impact of Malware Infections:** The primary impact/risks associated with malware are time, money and loss of confidential/private data of the users. A common impact of using pirated software is the loss of time and productivity due to the behavior and actions of the malware. Examples of malware-inflicted loss of time include slowing of computers, inundation with pop-up advertisements, corrupted files, increased need for cleanups and reinstallations etc.

Many of the malware forms are targeted at stealing financial information and specialize in stealing credit card, identity and banking information. Such malware facilitate illegal financial transactions and their impact can be directly evaluated in economic terms. Malware such as key-loggers may also steal username and passwords for email, online accounts, and social networking websites and then use those accounts to send information promoting scams, websites selling dubious products, digital piracy, pornography, etc.

While the impact of such malware is difficult to quantify in exact economic terms, it is well-established that rise of cybercrime attacks can cause enormous personal, reputation, economic and business losses, including risks to national security of the governments.

**d. Objectives of this Study:** The objective of this report is to present the results and the analysis of our research study to quantify the relationship between software piracy and malware infections.

One of the primary goals of our study was to check what malware infections come with new personal computers (PCs) which are installed with pirated software at the point of sale/shops, directly in the hands of the users – a common practice around the world, particularly in the developing countries.

The study aims to demonstrate and highlight the fact that such new PCs are increasingly coming pre-infected with malware before they have been used by the users and even before the PCs connect to the Internet or external storage devices. These trends reflects how malware is maliciously embedded in the uncontrolled and unauthorized sources of pirated software, that isoften controlled by cybercriminals and organized criminal syndicates.

The second objective of the study was to investigate pirated software, that can be bought from brick-andmortar shops or downloaded from the Internet, for presence of malware.

The overall objectives of the study are

(i) Provide evidence of the presence of malware in computer hardware procured through public distribution chains, pirated software CDs and DVDs, and pirated software downloaded from the Internet.

(ii) Highlight the cybersecurity risks and cybercrime threats posed by such malware and the effects they may have on consumers, small businesses & organizations.

The study is based on an in-depth analysis of 458 samples from 8 countries in Asia-Pacific. These samples consists of, a combination of PCs installed with pirated software, software CDs/DVDs copied with pirated software, and online downloaded copies of pirated software. Each of these software samples and PC "samples" were thoroughly investigated for the presence of malware infections and signs of tampering with the software, user and security settings.

**Based on this analysis, the major findings of our study are:**

**(i) 55% of the total samples were infected with malware, of which over 90% infections were in the PC samples.**

**(ii) Main strains of malware found were trojans, viruses, adware, etc.**

**(iii) In addition to the malware in the PCs & CDs/DVDs, significant threats existed in the form of malware that is encountered in the websites that offer links to pirated software.**

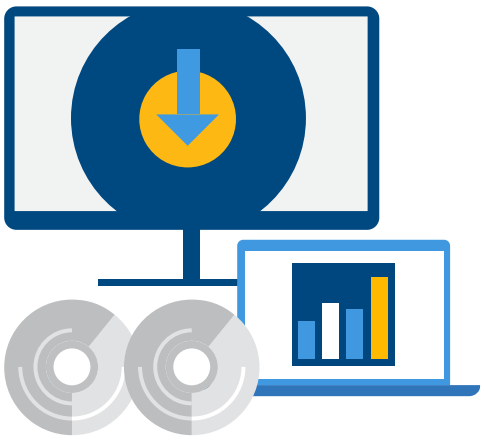
# 2. METHODOLOGY

This section described the methodology followed during this study. The overall methodology consists of three steps. The first step is the procurement of personal computers, physical media such as CDs and DVDs, and the online software downloads that serve as the samples for our study. The subsequent steps are related to the investigation of the samples for the presence of pirated software and malware. The details of the individual steps of the methodology are presented below.

a. **Sample procurement:** The sample procurement step involves the purchase of computers and software for analysis from across the markets in Asia-Pacific (Malaysia, Indonesia, Thailand, Vietnam, Sri Lanka, Bangladesh, South Korea, and Philippines). Towards this end, a total of 90 samples of personal computers and laptops from these 8 countries from south east Asia were procured.

Additionally, 165 CDs and DVDs containing software were also acquired. These samples were purchased from the target countries on a random basis, from PC and software vendors. These vendors could be standalone shops in street markets, or located in IT market hubs (for example, an open market full of shops located in the same zone doing similar business), or PC shops in specialized IT malls. The shops visited for this study included multi-brand, single brand, PC assemblers and IT retail chain stores.

**Our team conducted a similar study in 2014 [2]. The previous study mainly focused on laptops and desktop PCs with pirated software. In the current reboot of the study, our choice of samples reflects the growing trend where software is increasingly being acquired through online downloads. In addition to laptops and desktops with pirated software, this study also considers CDs and DVDs, as well as pirated software available online, for example from peer-to-peer networks.**



The purchases were done by independent investigators who would act on a pretext of a "normal walk-in customer" such as student, young professional, home maker, small business owner, etc. The objective was to target everyday PC distribution and sales business model which interacts with walk-in customers, and where piracy, by way of hard-disk loading, happens the most. This option is usually offered as an incentive to drive the PC sales.

It is important to note that the test purchasers did not specifically ask for computers with pirated software. The test purchasers usually discuss the PC brand options, features, configurations, pricing, deals/discounts etc. Our empirical observation suggests that through this discussion and negotiations, free installation of software is generally offered and agreed by the shop sales person as an added incentive to make the sale.

In addition to the "physical" samples consisting of hard drives from computers and CDs/DVDs, 203 software samples were downloaded from the Internet. These samples were available online as torrents and were downloaded using the BitTorrent peer-to-peer software.

Online search engines (e.g. torrentz2.eu) that specialze in torrent files were used to serch for downloadable software. While a wide range of software is available for downloads, our samples were restricted to well known software titles, including operating systems, design, productivity tools, anti-virus engines etc.

**b.** **Sample imaging:** The first technical step in our methology consisted of creating a software image of the hard disk from each of the samples. The image is usually created by making a sector-by-sector copy of the contents of the hard disk. The primary reason for creating an image is to allow easy analysis of the sample without the risk of contamination or modification of the original sample.

To achieve this objective, the actual malware analysis on the sample is done on a copy of this image. Consequently, the impact of any inadvertant action by the anti-virus engines or any breakout is limited to the copy of the image. Images were also created for the software downloaded from the Internet as well as those from CDs and DVDs. In the case of CDs and DVDs, the primary motivation for creating the images was to speed up the malware detection (since the speeds of the CD/DVD drives limits the scanning rates).

The images were created using software tools that create VHD (Virtual Hard Disk) versions of physical disks and these images conform to Microsoft's Virtual Machine disk format. These VHD based disk images can be directly used in various virtual machine (VM) environments that are needed for the system investigation and behavior analysis steps of the methodology. For the purposes of this study, virtual machines were used. All partitions of the hard disks were selected when creating the images.

**Avoiding Sample Contamination:**

In a large-scale malware study, sample contamination is always a concern. Care should be taken so that malware from a sample does not spread to others. Also, the integrity of the sample between scans by different anti-virus engines is necessary. In our study, these objectives were achieved by creating their software images and conducting all malware analysis on these samples.

*Hard disks from brand new PCs that are preloaded with pirated software.*

c. **Malware detection:** The malware detection step consists of scanning each of the sample images with anti-virus software. For this study, the following seven anti-virus engines were used: AVG, BitDefender, Ikarus, Kaspersky, McAfee, Norton, and Windows Defender. For scans on a given sample, for each anti-virus engine, a separate copy of the software image of the sample was used. This was done to ensure that each anti-virus engine scans the same (and original) image of the sample and any inadvertent modification of the sample that may be made by an anti-virus engine during a scan does not impact the results of subsequent scans.

For each scan, the following basic rules were applied:

1. Before each scan, the latest definitions and updates for the anti-virus engine were downloaded.
2. The settings for the anti-virus engine were set to scan all files and directories.
3. The options for automatically removing malware was turned off. At the end of each scan, the malware samples are copied and saved for further investigation.
4. The output of the scan including the details of the malware identified, their locations etc. is recorded.

At the end of the scans from the seven anti-virus engines for each sample, the results were collated and the number of unique malware in each sample was counted.

**Variation in Capabilities of Anti-virus Software:**

**Most organizations and individuals rely on a single anti-virus software to protect their assets. Our study shows that this is largely ineffective and there are many malware samples that are detected by one anti-virus software but missed by others. Thus, we used 7 different anti-malware software to thoroughly examine the samples.**

# 3. THE FINDINGS:

This section presents the details of the results of the study, as follows:

**a. PCs, and CDs/DVDs with pirated software:** Our study found an overwhelming majority of the new computers with pirated software (92%), that were analyzed, were infected with malware. This result is particularly important considering that the samples were brand new computers that were previously unused.

The presence of malware in these computers should be of particular concern to consumers, who naturally expect new computers to be risk-free.

Additionally, our study found that of the 165 CD and DVD samples that were investigated, 100 samples contained malware, resulting in an infection rate of 61%.

The bulk of the malware found in these samples were trojans, droppers, and adware. These malware (more details are provided subsequently in this section) expose the users to a wide range of security and performance issues. Some of the malware such as adware may cause disruptions and performance issues due to pop-up advertisements and unwanted processes running on the computer. Of greater concern are Trojans, key-loggers, and backdoors that can download additional malicious software on the infected computer, delete and encrypt files, and allow hackers to gain remote access of the computer.

**92%** Brand new, unused software were infected with malware

**61%** Pirated DVDs & CDs were infected with malware

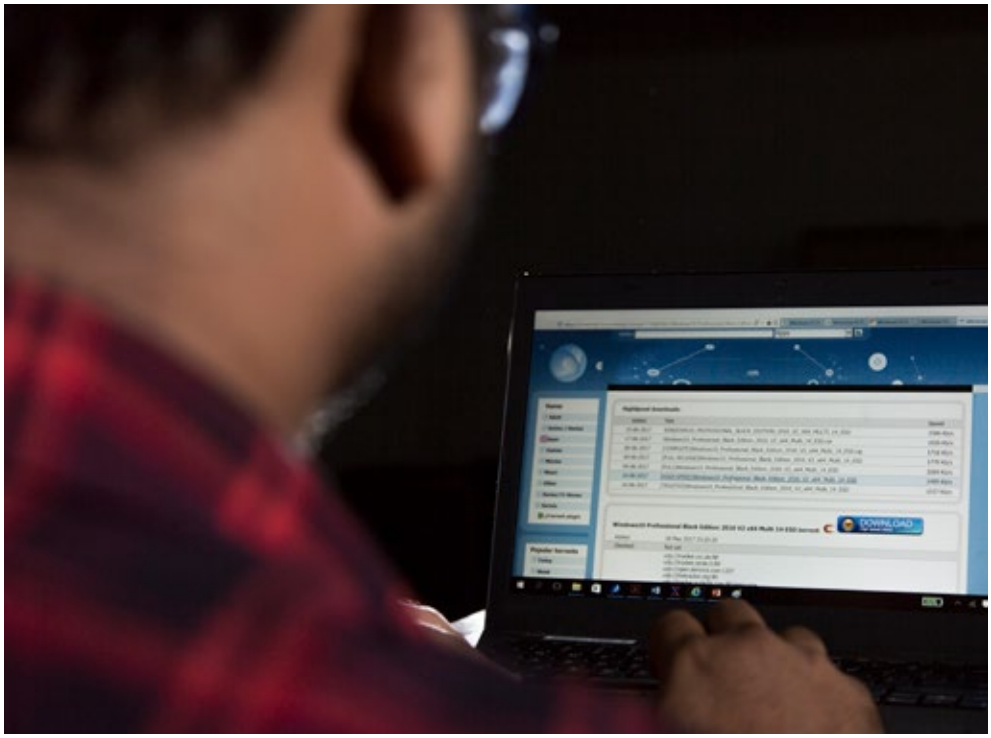
**5** Average no. of malware strains on an infected CD or DVD

**38** No. of malware strains found on some DVDs

**Malware patterns in CD/DVDs:** The bulk of the malware present in the CD and DVD samples were Trojans and Droppers. Once the software in these CDs and DVDs are installed, the infected computers will likely see a rise in infections and anomalous behavior as additional malware is automatically downloaded. Infected CDs typically had multiple strains of malware, and on an average, each infected CD/DVD has 4.9 instances of malware. We also observed large instances of malware in some cases, with 38 pieces of malware in just one DVD.

**b.** **Downloaded pirated software:** Among the 203 samples of software downloaded from the Internet, our study not only found malware presence in several samples, we also encountered various security risks and malicious threats to the users who were made to visit such websites. We were able to establish that the web links to these pirated software were posing several risks since they made attempts to infect the computer through malicious advertisements and software downloads which were able to bypass anti-virus software checks.

It was reported that in 2015, almost a third of torrent websites served malware to their visitors and around 12 million users were infected (per month) by visiting these websites[3]. Our own investigations support these reports and found that visiting websites with links to torrent files lead to malware drops, pop-up ads, and misleading links aimed at tricking visitors. Additional details of malware risks associated with downloading pirated software are highlighted in our analysis later in this report.



*A NUS researcher accessing a torrent website and analyzing the cyber risks encountered.*

The common pirated software downloaded include the Microsoft family of operating systems, Microsoft Office suite of software, document and image handling software by Adobe, file compression software such as WinRAR, and other popular software such as CorelDRAW and AutoCAD. Perhaps more interestingly, we observed a number of cases where malware was bundled with anti-virus software that was being distributed in the DVDs and CDs. Using such compromised security software not only infects the computer to begin with, it also does lulls the users into a sense of complacency and keeps the computer open for further exploitation.

## Several categories of software were downloaded for analysis. Here are the infection rates for different categories of pirated software.

**Productivity software: 42%**

**Operating systems and system software: 29%**

**Games and apps: 19%**

**Anti-virus software: 17%**

**a.** **Types of Malware:** The results presented above give a quantitative view of the results of the study. Further analysis into the nature of the malware infecting the samples highlights the common modes used by cyber criminals to steal the personal and financial information of the computer's owners.

Additionally, our results show some of the common methods used by these cyber criminals to get users, through pirated software, to compromise their computers. Our observations are described below.

**i.** **Trojans:** The most common family of malware encountered in our study was Trojans. Trojans are a class of malware that typically distinguish themselves as legitimate software are often employed by cyber criminals to gain access to computers.

While Trojans typically depend on some form of social engineering to trick users into loading and executing them [4], bundling them with pirated software makes it easier for cyber criminals to compromise and control computers.

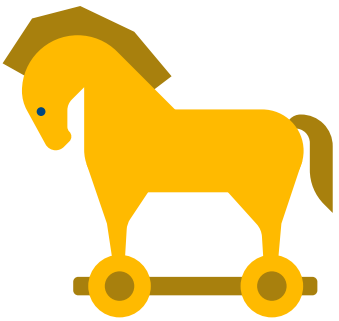
Once a Trojan is active in an infected computer, they can allow the cyber-criminals to spy on the users and steal the private data. Additionally, Trojan can open backdoors to allow remote access and control of the computer, modify and delete data, and degrade the performance of the computer.

Some of the common Trojan strains that were seen in the samples include Downloader, Floxlib, Wpakill, Pioneer, Turkojan, FakeGina, and WrongInf.

### Trojan Win32:Skeeyah.A!rfn

This Trojan was frequently found in our samples and its main purpose is to create a backdoor for the attacker to gain remote access on the compromised computer.

The malware modifies the registry and firewall settings, and may disable anti-virus programs. and is designed to steal sensitive data from the infected computer. Once the malware installs a backdoor, the attacker can gain access to private information stored on the computer, send spam, and launch '*denial of service*' attacks.



ii. **Viruses and worms:** The study also found a large range of worms, viruses and other forms of infectious software in the samples. Unlike Trojans that are not able to self-replicate, computer worms can replicate without human intervention and have the capability to spread more rapidly.

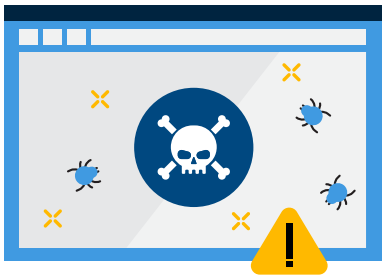
Worms and viruses may execute malicious code that deletes files with certain extensions and/or beginning with specific strings, terminate security-related programs and services such as firewalls and anti-virus software, send spam messages, and contact remote hosts to download additional malware.

Common worms and viruses encountered in our study included Virut, Nuqel, Jenxcus, Sality, and Xorer.

### worm VBS/Jenxcus

This malware allows cyber criminals to gain remote access to the infected computer. Once installed, the worm can create a backdoor for the hacker to command the infected computer.

Additionally, the malware can record the usernames and passwords that the computer's owner uses on various websites and send all this information to cyber criminals. The malware can also delete or update files on the infected computer, execute any commands that the cyber criminals want, open websites, and download files to the computer.



iii. **Other malware:** In addition to worms and viruses, the samples also contained malware that may be classified as adware, hacktools, and droppers.

Adware are software that automatically download and display advertising material on the infected computer. Adware may also redirect search requests made on the infected computer to advertising websites and collect private user information (e.g. the types of websites visited) in order to enable customized advertisements to be downloaded.

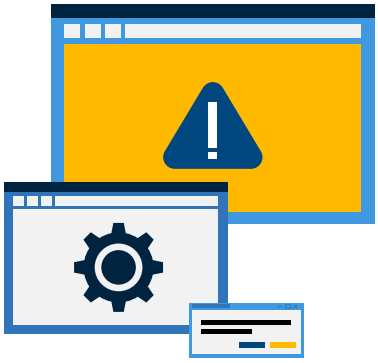
Hacktools are programs used by cyber criminals to gain access to the infected computer and are used for a number of malicious activities. Such activities include logging the keystrokes on the computer, stealing and cracking passwords, sending spam emails, and acting as port and vulnerability scanners.

Some of the adware found in our samples include yabector, Adon, OpenCandy, SwBundler, and Amonetize.

### adware Amonetize

Amonetize is an adware that often comes bundled with software installers (e.g. in .RAR and .ZIP files) and is dropped on the computer during the installation process. This adware has the ability to ability to change computer settings, installing toolbars in browsers, display advertising banners, pop-up advertisements, in-text advertisements, and browser popups that recommend fake software updates.

While Amonetize may sometimes have legitimate uses, it is mainly used for malicious purposes including generating advertising revenue, browser hijacking, and manipulating page ranks in search engines.



**High-risk malware examples found in online samples**

1) **Trojan/Omaneat:**
Collects username and passwords, targets banking details and social media.

2) **Trojan/ChePro:**
This Trojan is designed to steal user account data relating to online banking systems, e-payment systems and plastic card systems.

3) **Trojan/Skeeyah:**
It installs a keylogger on the infected computer to record information about browsing history, online searches, banking operations and various online accounts such as social media or emails and their passwords.

4) **Malware/Artemis:**
Artemis is a malware that affects the work of web browsers by changing the homepage, redirecting search engine queries to advertisement pages, and creating pop-up windows.

**b.** **Infection Patterns:** As defense mechanisms against cyber-threats evolve, developers of malware have also adapted to these changes to continue with their quest for compromising and exploiting vulnerable computers for financial gains.

*NUS researchers scanning pirated software samples for malware infections.*

While traditional methods of procuring pirated software through brick-and-mortar shops or roadside kiosks is still popular in many parts of the world and South-east Asia, increasingly, such software is being downloaded through websites and peer-to-peer networks. Consequently, malware developers have targeted the distribution of malware through the forums used for the online distribution of pirated software.

Also, our study shows that malware developers exploit both technological and human factors so as to increase the chances of infecting computers. Our observations on the methods used by malware developers and the trends in infections from pirated software are as follows:

i. **Bundling of malware with popular software:** Our study revealed that the malware are typically bundled with popular software, in order to increase the likelihood of infecting computers. For example, many CDs/ DVDs with pirated software include a bouquet of software. Among these, software commonly used by users of personal computers were more likely to contain malware.

ii. **Rising Dangers of Online Software Piracy:**

A wide variety of pirated software are available in peer-to-peer networks, and torrent based applications (e.g. BitTorrent) are usually used for accessing content on these networks. The ease of downloading software using torrents and the false sense of anonymity on peer-to-peer networks may seem enticing. However, there are a many security risks associated with pirated software. In our attempts to download and install pirated software on our computer, we frequently experienced the following from the tested websites:

1. **Multiple Popups With Suspicious Ads:** Contacting the website hosting the torrent file opened multiple popup windows with advertisements. Many of the advertisements have links to malware, and frequently show objectionable content such as pornography.

   Prevalence: **100%**

2. **Misleading Links and Automated Downloads:** Torrent hosting websites have multiple misleading links (e.g. "Download"), which lead to further popups, signups for marketing emails etc. Frequently, these links also lead to malware that is downloaded once the link is clicked.

   Prevalence: **100%**

3. **Deactivation of Anti-Malware Software:** Malware bundled with the pirated software deactivated the anti-malware software running on the computer. Once the anti-malware engine is blocked, the downloaded malware installs itself on the computer and may download and install additional malware.

   Prevalence: **24%**

4. **Changing Browser Settings/Installing Toolbars:** During installation, the user is prompted to change default settings on browsers and install add on toolbars. These changes to the browser settings lead to new home pages, changes in the default search engine, and unwanted toolbars.

   Prevalence: **18%**

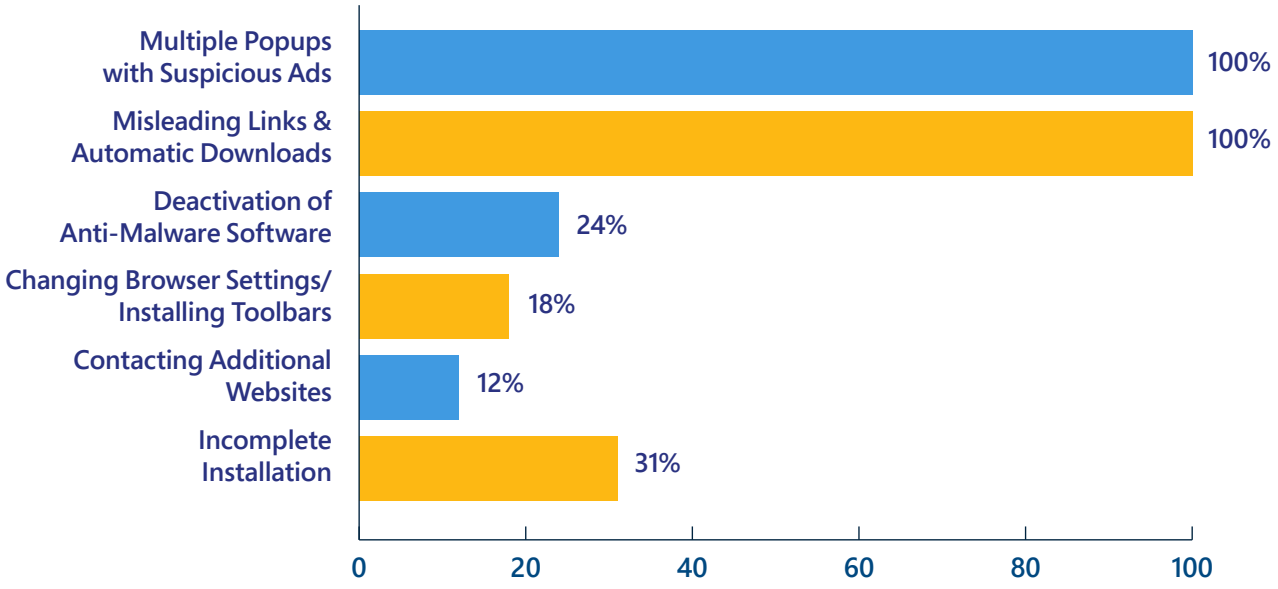
5. **Contacting Additional Website:** The user is required to contact additional websites to complete the installation. Often, these visits are portrayed as steps required to obtain the license keys or "cracks" needed to activate the pirated software. These websites result in popups and try to drop additional software.

   Prevalence: **12%**

6. **Incomplete Installation:** Many of the downloaded software do not complete installation, suggesting other motives behind their presence on torrent hosting websites. Such misleading torrents are used to increase the traffic to the torrent hosting sites and subject the visitor to malware and/or advertisements. Additionally, while the download may not contain the software that it claims to contain, they may contain malware that is installed instead.

   Prevalence: **31%**

**Dangerous Activities Encountered when Downloading Pirated Software**




In many countries, access to torrent hosting websites is restricted by court orders (primarily due to their links to copyrighted material). Proxy websites are typically used by residents of these countries to access the torrent websites. Many of these proxies add their own content to the websites downloaded by their users, including malware and software related to click-fraud.

iii. **Increasing the risk of infections:** Our study also observed that malware is often packed with files that are auto -executed on startup/setup files for software, or files that are executed in order to activate the software. This ensures that malicious software is more likely to be executed on the infected computer.

In addition, since software activation usually requires Internet access, Trojans and Droppers use this opportunity to download addition malicious software on the computer. In our samples, malware was frequently bundled with the auto-run software for CDs and DVDs, as well as the activators for software such as Microsoft Windows, media players, Microsoft's office suite of software, and SOLIDWORKS. The malware bundled with software activators includes all classes such as Trojans, backdoors, and adware.

# 4. RECOMMENDATIONS:

Knowing the threats, disruptions and losses malware infections bring to all computing environments through pirated software, the study has endeavored to bring together a set of fundamental IT/Cyber hygiene recommendations and best practices towards building a stronger IT security and online safety ecosystem. While most of the fundamental IT/Cyber hygiene recommendations are common in nature, they have been divided into the following three broad categories of users:

**a. Consumers & Small Businesses:**

1. The first rule of online safety and defense should be to refrain from procuring and accessing pirated software. The losses and harm from cybercrime can be devastating.

2. Access software vendors' websites to learn about software products, genuine downloads, their security benefits, how to distinguish between genuine vs pirated software, including how to report piracy if you have been a victim.

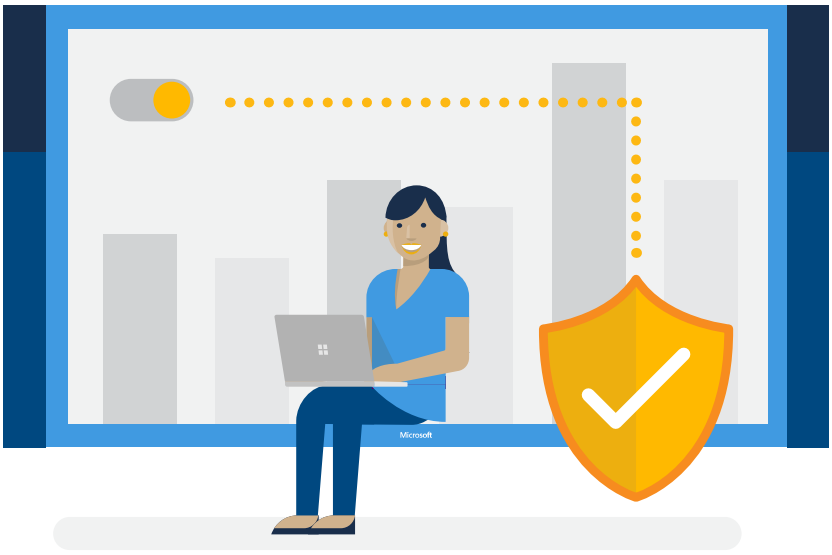
3. Always insist on genuine software from your IT Vendor and opt for computers which come pre-installed with genuine software by hardware manufacturers.

4. When purchasing computers, always demand an invoice which clearly calls out the software title & version which has been installed on the machine.

5. Keep your products current with latest product updates and security patches, which are always free in nature, coupled with having a strong Anti-Virus software.

6. It is advisable to avoid using very old software which have reached their end of life and are no longer supported by the software vendors for updates & security patches.

7. Get educated, trained & follow good and safe internet/IT practices and do not visit untrusted websites, download and file sharing portals, for the risk of being infected.



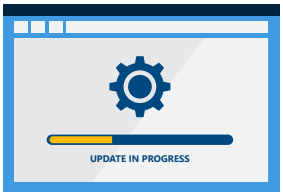
**b. Enterprises & Governments:**

1. **Information Technology (IT) management:** IT management policies in organization play an important role in safeguarding its data and computational resources. The first step in this direction is to have policies and frameworks for situational awareness of an organization's IT environment. Best practices on software asset management practices (e.g. ISO/IEC 19770-1) include audits of software installations and their versions, hardware specifications, user lists and their privilege levels, and network-mapping to localize network devices and end hosts.

In addition to the software and hardware assets, audit and management of data is also important, with main tasks being data classification (e.g. critical versus general), data location, and access control.

Finally, an important part of the IT policy is the guidelines for procurement of hardware and software. Policies should only allow the procurement of genuine software and these policies should be strictly enforced. All software must be validated during installation to ensure that they are genuine. Only trusted sources such as authorized outlets and manufacturer's websites should be used for software procurement.

2. **Software Patching and Updates:** Malware attain their objectives by exploiting vulnerabilities in the software of a computer. As vulnerabilities are reported or become known, software manufacturers release updates and patches to fix them. Thus both organizations and individual users should ensure that their software is regularly updated and all security patches are applied immediately on release.




The recent WannaCry outbreak is a case in point. Computers that were up-to-date with their patches were immune to this attack. It is recommended that all older and unsupported versions of software be retired immediately on the availability of modern and secure versions. Finally, preference should be given to software that have threat-detection capabilities embedded in them.

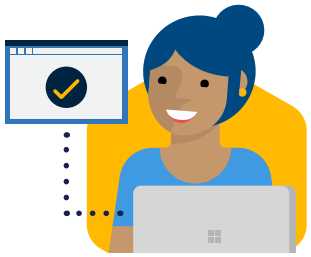
**WannaCry and Pirated Software:** China and Russia were two of the countries most affected by the WannaCry ransomware and security experts have pointed to the widespread use of pirated software in these countries as a primary factor [5]. While a patch that fixed the vulnerability exploited by WannaCry was released in March 2017, computers running unlicensed versions of Windows did not install it. Consequently, a significant fraction of WannaCry victims were users of pirated software and those who did not update their software with the security patches.

3. **Threat Detection and Monitoring:** All computing devices in an organization or with a private user should be protected with a robust and reputed anti-malware solution. The anti-malware definitions should be updated every day to ensure up-to-date protection against malware.

For anti-malware engines that allow the user to customize the scanning, the recommended search settings are to scan for all types of malware (including adware and suspicious files), scan archived files, executable files and files with no extension, and scan system memory. Detected malware should be removed or quarantined immediately.

Firewalls should be used continuously by both organizations and individuals. It is advisable to use location specific firewall settings and err on the side of caution when in public networks. All unsolicited incoming connections should be blocked and specific exceptions may be created for trusted applications. No exceptions should be created for either outgoing or incoming traffic that use port numbers known to be used by malware.

4. **Awareness and Capacity Building:** To protect against malware and the wide variety of exploits they use to infect and propagate, training employees on safe cyber practices and educate them on the importance of using trusted software platforms is extremely important.



Similarly, individuals should also stay vigilant against cyber-crime and follow safe cyber practices. Employees in an organization as well as individuals should keep abreast of current threats and scam employed by cyber-criminals. Browser protection and safe browsing practices should be emphasized at the workplace and at home. Websites offering adult content, illegal downloads, and pirated software are more likely to be contaminated with malware. Safe browsing practices also include avoiding pop-ups, checking links for redirections before clicking on them, not responding to spam, etc.

Organizations should make regular efforts at educating employees about online safety and ensuring that the IT and safety teams are exposed to the state-of-the-art attack and defense mechanisms.

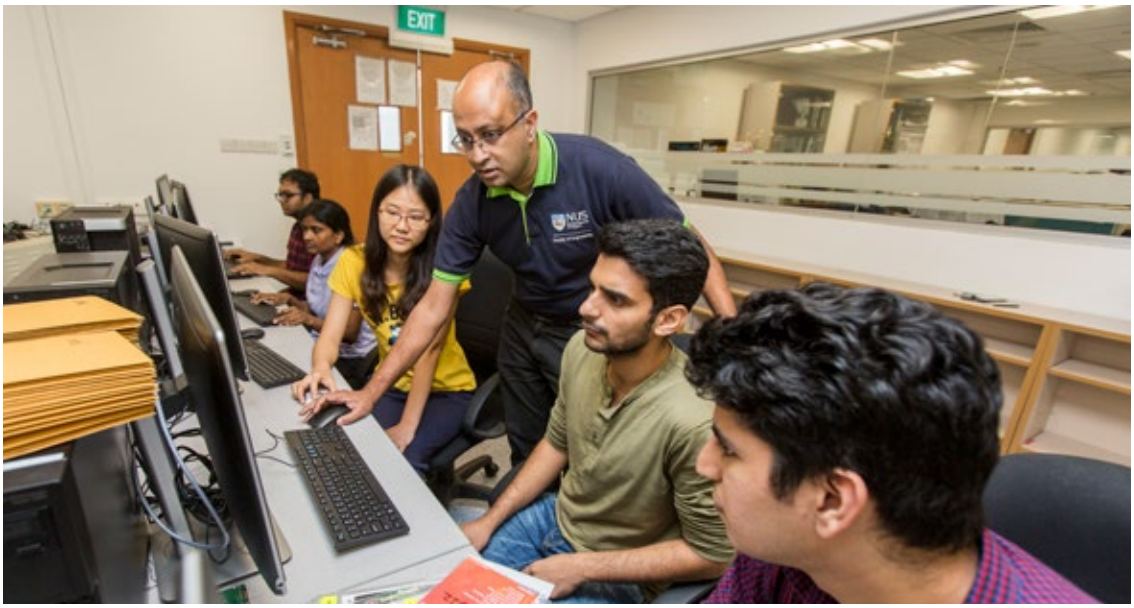
5. **Access and Identity Management:** Providing secure and authenticated access to an organization's computing and data resources is a core component of its cyber-security readiness.


With basic identity management systems that rely on username and passwords, policies that ensure the use of strong passwords and regular changes are necessary. It is recommended that such basic policies be augmented with multi-factor authentication mechanisms to achieve greater levels of trust.

Finally, data encryption can form the final line of defense against unauthorized access to data, even in the case where conventional perimeter-based defenses such as firewalls and anti-virus programs are breached.

Additional protection against the risk of data leaks can be achieved by storing individual data elements in separate locations which reduces the likelihood of attackers gaining enough information to commit any significant damage.

# 5. CONCLUSIONS




*Associate Professor Biplab discussing the results of the malware analysis with his team.*

Consumers & businesses often turn to pirated software for a wide range of reasons. These reasons may be economic, ignorance of ethical and legal issues, motivated by ideological issues or simply a lack of respect for intellectual property rights in software.

However, the users of pirated software ignore an extremely important associated risk: security. As demonstrated by this study, pirated software frequently comes with embedded malware and it also increases the malware infections with new strains. These malicious software include the entire range of malware such as trojans, worms, viruses, ransomware, backdoors, spyware, droppers, injectors, adware, etc, and with time, their strains are multiplying as well as becoming more sophisticated, dangerous and highly targeted.

As the study reflects, the threat of malware looms high on all sources of pirated software – PCs installed with pirated software, CDs and DVDs copied with pirated software, as well as pirated software downloaded from the Internet.

However, it is the online downloads which are turning out to be more dangerous and malicious to expose consumers and small businesses to a high degree of cyber-attacks and resulting in debilitating personal and financial losses. The online access not only brings the scale for cybercriminals to attack anybody, anywhere, anytime, the cybercriminals/ hackers are also able to hide their identities and camouflage their criminal activities, making them capable of undertaking more malicious attacks, without being investigated and prosecuted.

Overall, the most effective defense against the risks associated with pirated software for consumers & small businesses is education on safer online practices, genuine hardware buying policies, and user awareness around serious security risks from piracy, coupled with using only current and up-to-date genuine software, a robust anti-virus software and a regular IT health checks to monitor threats.

# 6. REFERENCES

[1] BSA global software survey, Seizing Opportunity Through License Compliance, May 2016.

[2] J. F. Gantz et al. The Link between Pirated Software and Cybersecurity Breaches: How Malware in Pirated Software Is Costing the World Billions, March 2014.

[3] Charlie Osborne, Torrent websites infect 12 million users a month with malware, December 2015.

[4] Kaspersky, What is a Trojan Virus?

[5] M. Moon, "Pirated Windows led to WannaCry's spread in China and Russia, May 2015.

# ANNEXURE

## WALKTHROUGH OF A TORRENT DOWNLOAD

**Pirated software of all types are easily available for download through peer-to-peer networks. In this appendix, we present the details of our experience with the download of one specific software sample (Microsoft Office). This experience highlights the wide range of security threats associated with downloading malware from online sources.**

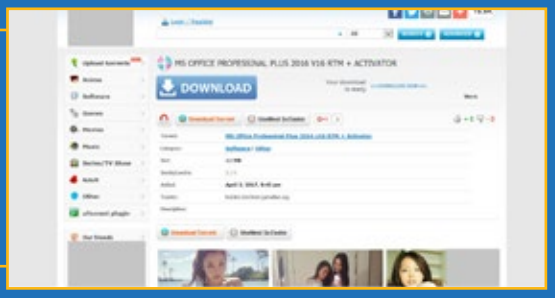
The steps associated with the download process and the malware encountered are as follow:

**1**

Our first step in the download of pirated software through peer-to-peer networks was to search for torrent files related to the desired software. We used the website torrentz2.eu as our search engine. Clicking on the search box led to a pop-up window advertising a "get rich quick" scheme.


**2**

Of the various sites listed in the search results, we chose torlock.com. Opening the link to torrent.cd opened a page with a link to the torrent as well as advertisements. The page also opened a pop-up window to a site that is known to drop malware.




**3**

The website also included misleading links marked "Fast download" and "Safe download". Clicking on these links directs the user to another page, where another link labeled "Download now" needs to be clicked to proceed further. This link takes the user to a signup page for usenet.nl which asks for credit card information. This website is well known for scamming its users, not providing the promised services, and sending fraudulent bills.

**4**

Once the torrent file was downloaded, it was used to download the desired pirated software using BitTorrent.

**5**

The downloaded software came infected with malware which automatically turned off the anti-malware engine running on the computer as well as Windows defender.

**6**

Scanning the downloaded software with anti-malware engines revealed the presence of multiple strains of Trojans.

**7**

The software failed to install, citing missing files as the reason. **This suggests that the torrent and the associated files were planted in the torrent hosting sites by cyber criminals** whose intention is to exploit popular software titles to spread malware.

NUS | Engineering
National University of Singapore

Microsoft

Study commissioned by
Microsoft Operations Pte Ltd, Singapore