**Computer worms**

**Introduction**

Computer worms have been with us for a moment now. They continue to evolve with time and become more sophisticated and hard to detect. Worms do not attract much attention compared to other cyber threats but they still pose real threats (Beede & Han, 2012). The most well-known worm happened in 2004 and was known as MyDoom and it caused an estimated $38 billion. Worms spread through unpatched security loopholes in the operating systems, email attachments and websites that are worm infested. Other means of infections include use of external devices, IM networks and peer-to-peer file sharing or torrents. Worms only need to gain access to a computer unlike viruses that need to inject a working application with malicious code.

Worms do not do immediate damage like viruses. They are less harmless and normally slow down computers. Their main threat is seen in that they come with a malicious payload. This is a code that is made to make the computer prone to other forms of malware. This mostly makes a computer lose sensitive information like passwords or creating leeways of some other forms of online attacks (Sha, Striegel & Song, 2017).

One of the categories of worms is email worms. These are worms that hide in email attachments. IM worms is the second classification and these are worms that spread through instant messaging (IM) networks like the Messenger, Skype or WhatsApp. The other category is bot worms and these ones are made to categorically transform a computer into a ‘bot’. The last category is the file-sharing worms and these spread by copying themselves into a shared folder that users can then go and download

Some of the ways to tell that a computer has a worm is that a computer starts working slower than before and will often crash. Worms in this case slow down the processing power of a computer. A computer system will also run out of storage space since worms eat a lot of space of a computer’s hard drive by continuously replicating themselves (Salomon, 2010). Computers also happen to have strange activities like files continually appearing and disappearing. There is need to regularly check whether a computer has worms even if they are working perfectly

**What to do when computer is infected by a worm**

Worms have no remedy. Some of the steps to take when a computer is infected include disconnecting one’s device from the internet. This stops the worm from spreading any further. One can also use an anti-malware program and also by scanning devices for worms and other forms of malware and also switch on real-time anti-virus protection to keep malwares at bay. In extreme cases of infection, the best way of handling infection is by reinstalling the operating system.

There is need to regularly update the OS and the apps of computers and enable the firewalls of the computers. One should also avoid opening suspicious websites and email and use reliable cyber security software.

**Actual Examples**

The WannaCry ransomware attack happened in May 2017. It targeted computers that were running through the Microsoft Windows Operating System by encrypting data and asking for ransom payments in Bitcoins (Ehrenfeld & SpringerLink, 2017). It affected computers that had not installed Microsoft security update from March of 2017 and those that operated through unsupported versions of Microsoft Windows like Windows XP or Windows Server 2003. These computers were under attack as they had security patches since the last released security updates for Windows XP happened in 2014 and for Windows Server 2003 in July 2015. The attack affected about 200,000 computers in 150 countries and it brought damages amounting to billions of dollars. The most affected countries were Taiwan, Ukraine, Russia and India. The largest agency to suffer from the attack was the National Health Service hospitals in Scotland and England where up to 70000 devices were infected (Ehrenfeld & SpringerLink, 2017). The worm was eventually discovered to have originated from North Korea or agencies working for them.

**Summary**

A company needs to carry out enough assessment of trusts. An assessment that was done after the Wanna Cry attack by National Health Service hospitals in Scotland and England Digital found that out of the 236 trusts, 88 of them did not pass the obligatory cyber security principles (Ehrenfeld & SpringerLink, 2017). NHS trusts had not acted on crucial alerts from NHS digital and a caveat from Department of Health was ignored. Also ignored was a memo from the Cabinet Office for institutions to migrate away from old and susceptible software.

There is need for institutions to manage their computer firewalls and dedicate enough time and resources for fighting ransom ware. There is also need to focus on doing regular cyber security improvements and have a response plan. With a response plan, institutions are able to ensure that crucial cyber security updates get to be done (Ehrenfeld & SpringerLink, 2017). As one observer noted, this attack could have been barred by just following rudimentary IT security practices. It was also established that most institutional executives took cyber security as among their high risks and gave this a priority. The problem came with a lack of planning at the local level. The Department of Health in England had a solid developed plan only that it was not communicated to the NHS trusts.

Investigations established that the Wannacry ransom ware penetrated systems through a vulnerable and outdated Windows XP operating system which was not being supported by Microsoft since 2014 (Barker, 2020). This means that majority of computers do not receive the latest patches which could help in preventing widespread infections. Thus IT infrastructure needs to be up to date at all times. There is need to have a mechanism for how to handle such an attack. Something like a ‘cyber handbook’ to describe the approach and actions to be taken when an attack of such a nature happens. This handbook would state the entity that is responsible for coordinating the system response. The book could stipulate the cyber response activities in depth, including most important, the mechanisms of communication.

There is also a lack of on-site cyber assessments. There is need to have capital investment on areas like addressing weaknesses in infrastructure to secure weaknesses like for instance upgrading firewalls, enhancing network resilience and segmenting so that the risk can be lowered. There also lacks a mechanism for improving device security by having device replacements and automations of patch management. Anti-virus protection also needs to be done often. The WannaCry attack could have been prevented if there was enough funding for supporting organizations that had self-assessed as being non-compliant so that they can strengthen their hardware and software across the system.

There is need for enough investment in the cyber sector and mostly, in the local infrastructure and the national systems to help enhance monitoring and response. Institutions need to commit local revenue funding to support versions of software needed to deal with cyber

security. There is need for a mechanism for registering technical compliance and passing on technical information to help in preventive activities. The other thing that lacks is the presence of an information governance toolkit. This spelts out the data security standards which define the data and cyber security programs. The governance toolkit helps enhance the prevailing data security services which go a long way into preventing the escalation of the ransom ware. An adequate audit of systems and processes needs to be regularly carried out. Institutions need to work with other institutions to ensure that the necessary information is offered that could help in preventing advancement of a cyber-attack. With the presence of ‘Good Practice Guides’ that are under regular monitoring and evaluation, an attack like that of WannaCry nature can easily be stopped.

The presence of a Digital Data Security helpline that operates throughout the day and night makes it possible to have a call team that is supported by a data security expert where one can call if they notice a mishap (Bell,2020).

The digitization programs in place should support cyber security. A mechanism of ensuring that suppliers make the information systems secure should be in place. The providers should be involved in the implementation of data security standards and there should be plans of removing and isolating any unsupported software. To prevent such an incident again, there needs to be leadership governing the entire process (Bell, 2020). The importance of cyber security needs to be communicated especially to staff. There is need to have a set of annual statements of requirements to the various boards and expectations set for every board that they should have a data security lead.

**References**

Barker, J. (2020). Confident Cyber Security: How to Get Started in Cyber Security and

Futureproof Your Career.

Beede, R., & Han, R. Y. (2012). *A Framework for Benevolent Computer Worms*. (Masters Abstracts International, 50-6.)

Bell, G. J. (2020). The organizational resilience handbook: A practical guide to achieving

greater resilience.

### Dasgupta, P., Collins, J. B., & Mittu, R. (2021). *Adversary-aware learning techniques and trends in cybersecurity*. (Springer Nature eBook.)

Ehrenfeld, J. M., & SpringerLink (Online service). (2017). WannaCry, Cybersecurity and Health Information Technology: A Time to Act. (Journal of medical systems.)

Maglaras, L., & In Kantzavelou, I. (2022). *Cybersecurity issues in emerging technologies*.

### Parisi, A. (2019). *Hands-on artificial intelligence for cybersecurity: Implement smart AI systems for preventing cyber attacks and detecting threats and network anomalies*.

### Sha, K., Striegel, A., & Song, M. (2017). *Security, privacy and reliability in computer communications and networks*.

### Salomon, D. (2010). *Elements of computer security*. New York: Springer.

Wilson, D. (2021). *Cybersecurity*.

### Xiao, P. (2019). *Practical Java programming for IoT, AI, and Blockchain*.