WannaCry

Francesca Fraioli[1] and Marco Lupia[2]

[1] *fraioli.1696638@studenti.uniroma1.it*
[2] *lupia.1694700@studenti.uniroma1.it*

Abstract— On 12 May 2017, a massive ransomware attack occurred across a wide range of sectors, including health care, government, telecommunications and gas. To date, WannaCry has spread to over 300,000 systems in over 150 countries. The countries that appear to be the most affected are Russia and China, probably because of the high percentage of legacy software, with significant impacts elsewhere, notably to the UK National Health Service. The spread of the ransomware reportedly slowed in the two days following the launch of the attack, in part due to the discovery of a "kill switch" in its code. However, there are reports of new variants of the malware which do not have this kill switch. Data on new variants is unconfirmed and limited at the moment, and EY wil publish updates as more information becomes available.

Keywords— WannaCry, Ransomware

INTRODUCTION

In computers and computer networks an attack is any attempt to expose, alter, disable, destroy, steal or gain unauthorized access to or make unauthorized use of an asset. A cyberattack is any type of offensive maneuver that targets computer information systems, infrastructures, computer networks, or personal computer devices. Cyberattacks use malicious code to alter computer code, logic or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and identity theft.

An attacker is a person or process that attempts to access data, functions or other restricted areas of the system without authorization, potentially with malicious intent.
In recent years, the scale, the sophistication and the robustness of cyberattacks has increased rapidly. It may steal, alter, or destroy a specified target by hacking into a susceptible system. So the legal experts are seeking to limit them.
Each cyberattack is ranking by some definitions. For example: depending on context, Cyberattacks can be part of *Cyberwarfare* (any virtual conflict initiated as a politically motivated attack on an enemy's computer and information systems) or *Cyberterrorism* (a premeditated attack against a computer system, computer data, programs and other information with the aim of violence against clandestine agents and subnational groups. The main aim is to cause harm and destruction).
The attack can be: active or passive. *Active attack* attempts to alter system resources or affect their operation, instead *passive attack* attempts to learn or make use of information from the system but does not affect system resources.
Each attack can be perpetrated by an insider or from outside the organization. The *inside attack* is initiated by an entity that is authorized to access system resources but uses them in a wrong way. The *outside attack* is initiated from outside the perimeter, by an unauthorized or illegitimate user of the system.
Between the most catastrophic cyberattacks we were interested to Trojan ransomware WannaCry.

WANNACRY

Wannacry was a ransomware attack that first appeared on Friday, May 12. The main interface is shown in Figure 1. Symantec saw a dramatic upsurge in the number of attempts to exploit the Windows vulnerabilities used by WannaCry from approximately 8:00 GMT onward.

Ransomware Ransomware is a subset of malware in which the data on a victim's computer is locked, typically by encryption, and payment is demanded before the ransomed data is decrypted and access is returned to the victim, as shown in Figure 2.

Unlike other viruses however, WannaCry propagates through the network and infects computers like a worm, which means that their users do not have to activate the infected file or link for the software to continue spreading [Symantec (2017)].

Overview More than 200,000 computers across 150 countries have been affected by a large-scale cyberattack in the past few days. The malicious software was first spotted in

Fig. 1: Wannacry interface

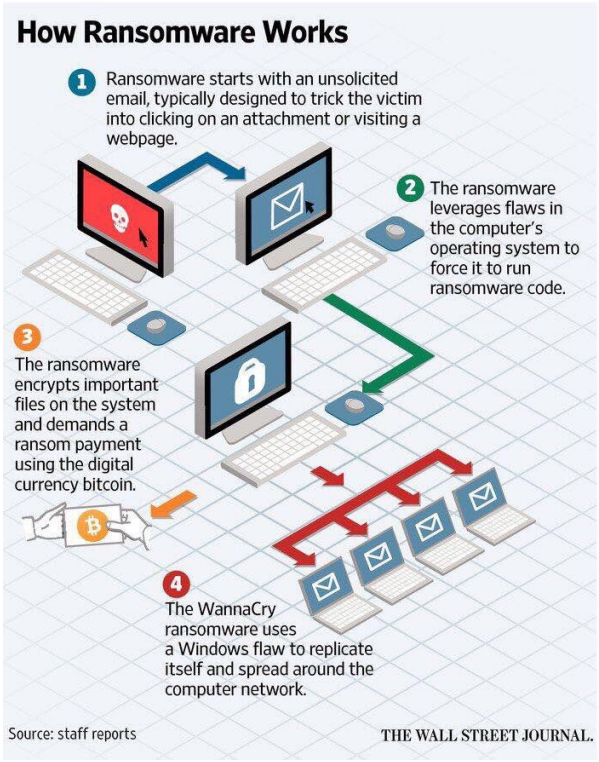


Fig. 2: Ransomware infographics

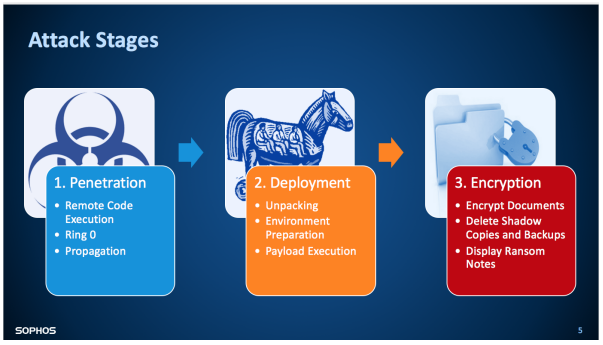


Fig. 3: Attack stages

Russia but rapidly spread across the globe in what might turn out to be an attack of unprecedented scale. The attackers took advantage of a known flaw in Windows XP, the operating system that is still used by millions of PC users and machines across the globe. Microsoft officially stopped providing security support for XP in 2014 but issued an emergency patch in response to the latest attacks.

The investigation revealed a three-stage attack, as shown in Figure 3, starting with remote code execution and the malware gaining advanced user privileges. From there, the payload was unpacked and executed. Once computers were hijacked, it encrypted documents and displayed ransom notes. [Sophos (2017)]

Computer security firm Trend Micro [micro (2018)] surveyed over 300 IT decision makers in the UK in September 2016 and found that 44 % of businesses have been affected by ransomware over the last two years. The same survey found 79 new types of ransomware in the first nine months of that year. This compared to just 29 in the whole of 2015.

In around 20 % of the cases, £1,000 was requested, with an overall average of £540. Some large organisations faced demands of as much as £1m. But for many companies, this is the tip of the iceberg as it can be costly for a company in terms of reputation as customers could start seeing them as untrustworthy.

Perhaps the most frightening statistic that Trend Micro found was that in one in five cases, even when the company paid the ransom, they were unable to recover their important files – indicating that the ransomware service is not quite as robust as it should be.

Working principles WannaCry is a type of ransomware, or extortive malware, that encrypts files, disks and locks computers. The malware demands a ransom of $300-$600 to be paid to one of three bitcoin accounts within three days in return for decrypting the files. WannaCry spreads via SMB, the Server Message Block protocol operating over ports 445 and 139, typically used by Windows machines to communicate with file systems over a network. Once successfully installed, this ransomware scans for and propogates to other at-risk devices. WannaCry checks to see if backdoors (like DoublePulsar) are already on previously infected machines. Both DoublePulsar and the *EternalBlue* exploit the SMB vulnerability that was made public by the Shadows Brokers hacking group in April.

WannaCry utilizes the exploit Eternal Blue, created by NSA and released by Shadow Brokers (full details in Appendix IV) on 14 April 2017. Of note, the malware also checks for existing backdoors via Double Pulsar, also released by Shadow Brokers, in order to help propogate through client networks. It should also be stated that the kill switch will not pause the attack if an organization is routing through a proxy for internet access. [EY (2017)]

WannaCry is a dangerous combination of two malicious software components:

- A worm that has the ability to spread itself within networks without user interaction
- A ransomware variant that encrypts user files and then asks for money in order to decrypt the files.

The attacks works in the following way:

1. Attacker uses a malicious email as initial attack

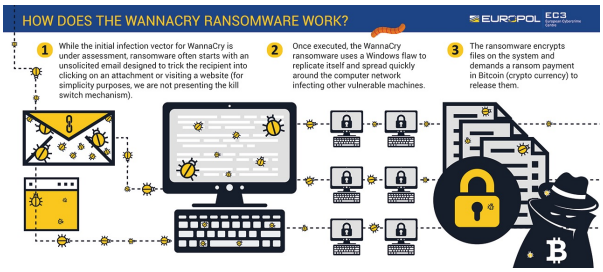


Fig. 4: Wannacry attack steps

vector

2. WannaCry encrypts files in the victim's machine using AES-128 cypher, deletes shadow copies. It then displays a ransom note requesting $300 or $600 in bitcoin

3. `TOR.exe` is used by `wannadecryptor.exe`, initiating connections to tor nodes in order to connect back to the attacker (therefore making this extremely difficult, if not impossible, to track)

4. IP address of the infected machine is checked; then IP addresses of the same subnet are scanned for additional vulnerable machines and connected to via port 445 TCP

5. When a machine is successfully connected, data containing the exploit payload is transferred

[Europol (2017)]

Figure 5 explains in details how the attack works.

Spread Upwards of 250,000 infections have been reported in various news articles and social media posts. [McBride (2017)]

In the four day period between May 12th and May 15th, the WannaCry ransomware was observed on over 160,000 unique IP addresses.

After only 4 days from the outbreak, almost every country in the world was infected, as shown in Figure 6.

The top 10 targeted countries, according to our data, are (in order): Russia, Ukraine, Taiwan, India, Brazil, Thailand, Romania, Philippines, Armenia, and Pakistan. Most of the cities on the northern hemisphere were hit. Various countries are impacted at different periods, with China, Russia, the United States, France, UK, Brazil, and Peru having notable periods of a high number of infections compared to other countries. After the malware has infected a specific machine, it scans for other vulnerable systems both external and internal to the network. Strong concentrations of infections within countries often occur due to the worm making headway by infecting a large number of machines behind a set of IP addresses. [Dahlberg (2017)]

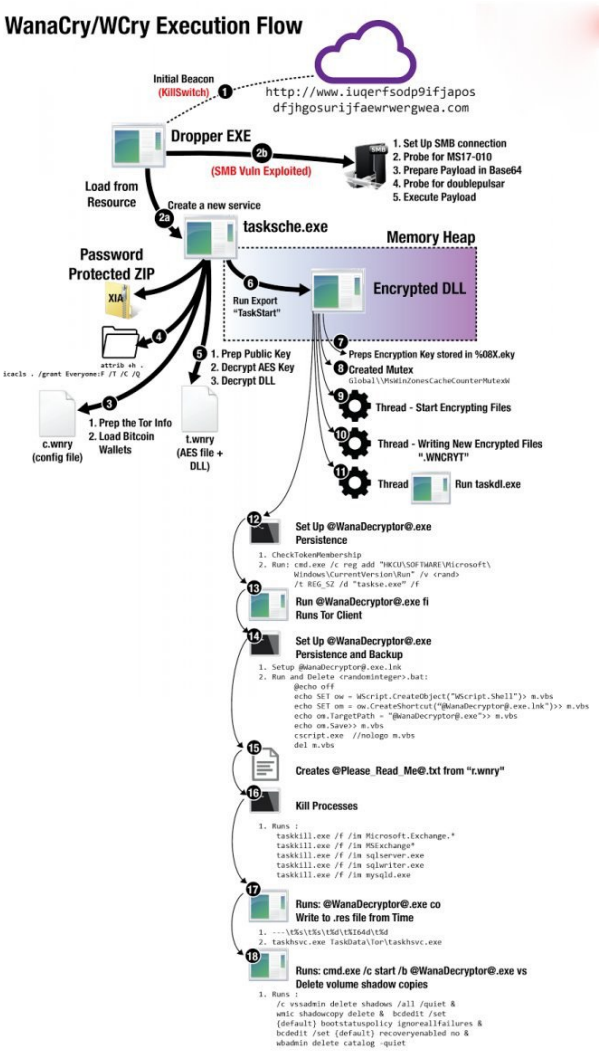


Fig. 5: Exectuion flow

Fig. 7: infected computers at 11 p.m.

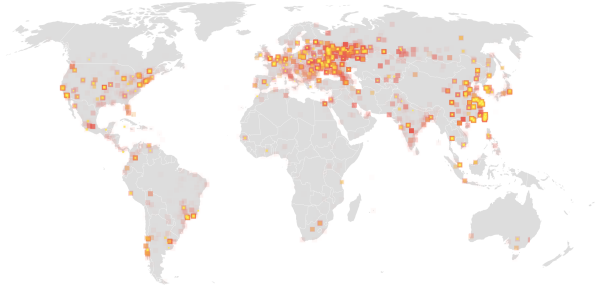


Fig. 8: infected computers at 6 p.m.

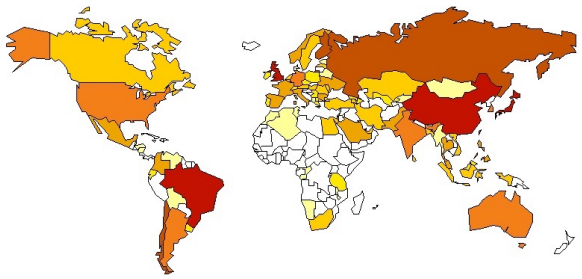


Fig. 6: Infected Countries

Industries The trends for the overall industry breakdown remain relatively consistent, as shown in Figure 9. The utilities industry moves from 5th to 3rd place for large companies affected by WannaCry. Large companies, like Telefonica and the Deutsche Bahn were affected by the attack, but even worse, hospitals around the world were also affected. Hospitals often lack budget to keep their systems up-to-date and were therefore hit hard on Friday, which greatly affected patient care [Kroustek (2017)]

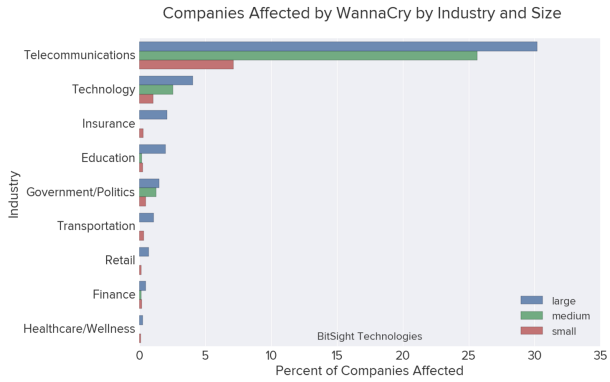


Fig. 9: Affected industries

Platforms Data from Kaspersky has shown the the majority of infections affected Windows 7 platforms, and some of our research also point in this direction. When we looked at the set of IP addresses affected by WannaCry, we extracted the operating systems that are typically used on the machines behind those IP addresses. The graphic in Figure 10 shows our data representing the composition of networks affected by WannaCry. There is still ongoing research regarding why Windows 7 is the most popular operating system among victims. It is known that the worm had difficulty infecting Windows XP machines and spreading as it often caused the machine to crash when it attempted to exploit the vulnerabilities. Microsoft has also designed a more seamless automatic update experience for Windows 10 that would have allowed for the MS17-010 patch to be installed on a much larger population of Windows 10 machines compared to older operating systems.

Kill switch Probably one of the most interesting parts of WannaCry is the kill switch. While this may not be the first time such a mechanism was found in a piece of malware (e.g. Necurs), its intent is undeniably curious. It might have been

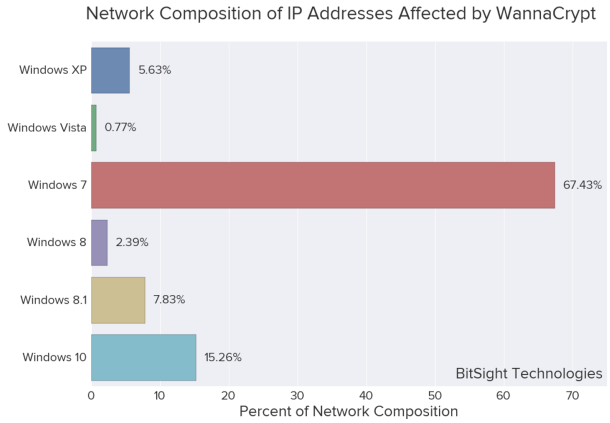


Fig. 10: Infected Operating Systems

for the attacker to control the worm, for the attacker to uncover when it was discovered by checking when it got sinkholed, or simply a sandbox evasion gone wrong. Whatever the reason, it played a huge part in halting the infection.

A researcher known on Twitter as MalwareTech, discovered a kill switch, which stopped the most prevalent variant of WannaCry from spreading any further.

The kill switch worked like this: If WannaCry made a request to a specific domain and if a response was received, showing the domain is live, the malware would just exit and stop spreading. Before the kill switch was activated, the domain wasn't registered and WannaCry therefore spread uncontrollably. The kill switch only stopped one variant of WannaCry from spreading, but won't do anyone whose PC was already infected any good. [Kroustek (2017)]

Money The ransom demanded by WannaCry is between $300 and $600 and the demand increases over time. The threat the ransomware makes, claiming it will delete the encrypted files if the ransom isn't paid within seven days, is fake.

Figure 11 shows how many organizations paid ransom requests.

Fig. 11: Payments statistics

The Bitcoin payment addresses used by the group behind the attack received more than 260 payment transactions, making the total money sent 41 BTC or approximately $70,000.

Losses usually go well beyond the amount of the ransom, and may even include the loss of human lives, as with the major disruption of the hospital system in the UK. Other negative consequences to businesses include:

- temporary or permanent loss of sensitive or proprietary information;

- financial losses from the disruption to business operations;
- financial losses incurred to restore the systems and files;
- potential harm to reputation.

Ransomware can also disrupt digital commerce, either in direct or on indirect ways. In 2016, the Magento e-commerce platform, used for backend management, was infected with ransomware. Files were encrypted and a ransom in the range of $140 to $415 was asked for decryption. Indirectly, ransomware impacts consumer trust, causing chilling effects on e-commerce. [P (2017)]

As the chart in Figure 12 illustrates, the $300 ransom asked of users affected by the WannaCry attack is low compared to other attacks in recent years. The average ransom across all attacks known to security software provider Symantec in 2016 was $1,007. [Richter (2017)]

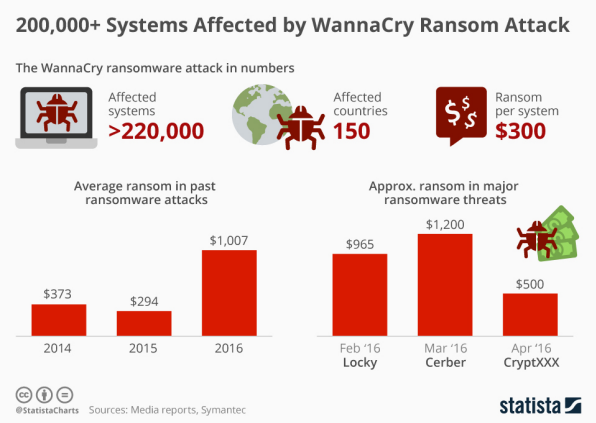


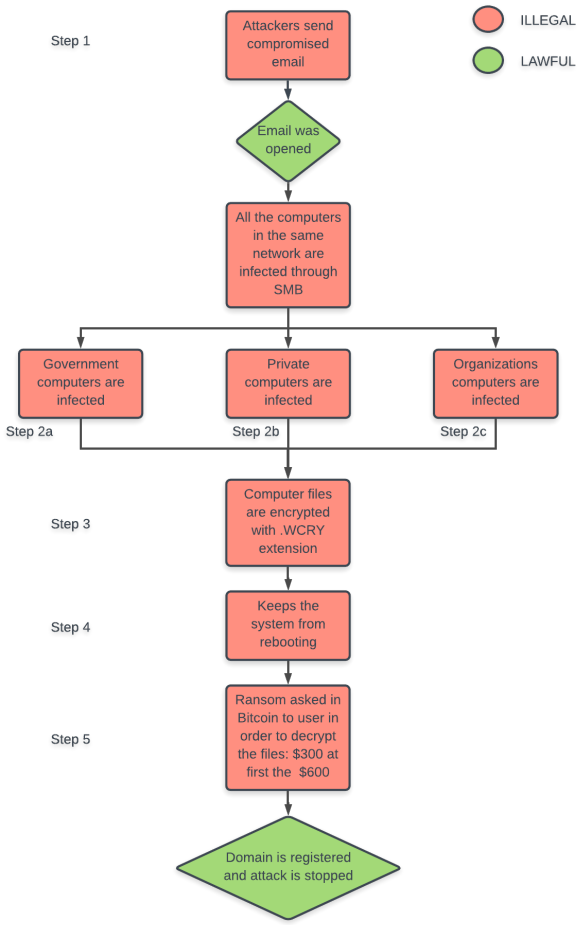
Fig. 12: Statista infographics

Authors After the initial dust settled, various security researchers began working to try to figure out the origins of WannaCry. Symantec had a provocative take: they believed that the code might have a North Korean origin. They laid out the evidence in a blog post [Sysmatec (2017)], where they discussed a little-known fact: that WannaCry had actually been circulating for months before it exploded across the internet on May 12, 2017. This earlier version of the malware, dubbed Ransom. Wannacry, used stolen credentials to launch targeted attacks, and there were "substantial commonalities in the tools, techniques and infrastructure used by the attackers" between this version of WannaCry and those used by the Lazarus Group.

The Lazarus Group in turn is a hacking group that has been tied to North Korea. Beginning their run in 2009 with crude DDoS attacks on South Korean government computers, they've become increasingly sophisticated, hacking Sony and pulling off bank heists.

On the other hand, without an explicit claim of responsibility, it's impossible to know for sure that either the initial wave of WannaCry attacks or the later EternalBlue-driven explosion was directed by North Korea, since malware code is copied liberally by various groups. [Fruhlinger (2017)]

Graphic representation



Penal evaluation

The illegal steps of the previous graphic are reported below, together with the correspondig law:

- **Attackers send compromised email:**

  Art. 640 ter ICC: *IT fraud*

- **All the computers in the same network are infected through SMB:**

  Art. 615 ter: *access or abusive stay*

- **Violated entities: Government computers are infected; Private computers are infected; Organizations computers are infected:**

  Art. 635 ter ICC: *damage to data, information, programs of the state or of the p.a. or otherwise of public utility*

- **Computer files are encrypted with .WCRY extension:**

  Art. 635 bis: *damage to data, information, programs*

- **Keeps the system from rebooting**

  Art. 615 quinquies ICC: *Distribution of equipment, devices or computer programs aimed at damaging or interrupting an IT or telematic system*

- **Ransom asked in Bitcoin to user in order to decrypt the files: $300 at first the $600:**

  Art. 640 ter: *IT fraud*

VIOLATED NORMS

Art. 640 ter ICC: *IT fraud* Anyone who, by altering in any way the functioning of a computer or telecommunications system or intervening without any right in any way on data, information or programs contained in a computer or telematic system or pertinent to it, procures to himself or others an illicit profit with other people's damage, is punished with imprisonment from six months to three years and with a fine from fifty-one euro to one thousand and two euros. The penalty is imprisonment from one to five years and a fine from 309 euros to 1549 euros if one of the circumstances provided for by number 1) of the second paragraph of article 640 occurs, or if the fact is committed with abuse of the status of system operator. The penalty is imprisonment from two to six years and a fine from 600 euro to 3,000 euro if the fact is committed with theft or improper use of the digital identity to the detriment of one or more subjects. The crime is punishable upon complaint by the injured party, unless any of the circumstances referred to in the second and third paragraphs or any of the circumstances provided for in Article 61, first paragraph, number 5 occur, limited to having taken advantage of personal circumstances, including in reference to age, and number 7.

- **Fact**: attackers send compromised emails, once the email was opened the malware is spread.
- **Typical fact**: Anyone with tricks or deceit, inducing someone into error, gives himself or others an unjust profit with other people's damage.
- **Subject**: Anyone, the conspirators.
- **Action**: sending compromised email.
- **Event**: the victim receives a compromised email.
- **Causality**: the principle of causality is validated: without the action of conspirators, the victim would never have received the compromised email.
- **Suitas**: conspirators know they are sending compromising emails.
- **Intent**: conspirators want to send compromising emails to access employee computers.
- **Aggravating or extenuating circumstances**: there are no aggravating or extenuating circumstances.
- **Causes of justification**: there are no causes of justification.

Art. 615 ter: *access or abusive stay* Anyone who illegally introduces himself into a computer or telecommunications system protected by security measures or keeps himself against the express or tacit will of those who have the right to exclude him, is punished with imprisonment for up to three years. The penalty is imprisonment from one to five years:

1. if the fact is committed by a public official or a person in charge of a public service, with abuse of powers or with the violation of the duties inherent to the function or service, or by those who also illegally exercise the profession of private investigator, or with abuse of the quality of system operator;
2. if the offender uses violence against things or people to commit the act, or if he is clearly armed;
3. if the fact leads to the destruction or damage to the system or the total or partial interruption of its operation, or to the destruction or damage to the data, information or programs contained therein.

If the facts referred to in the first and second paragraphs concern computer or telecommunications systems of military interest or relating to public order or public security or health or civil protection or otherwise of public interest, the penalty is, respectively, imprisonment by one to five years and three to eight years. In the case provided for in the first paragraph, the crime is punishable upon complaint by the injured party; in other cases, the procedure is official.

- **Fact**: After that a victim opened the compromised email then his computer was infected and all the computers in the same network are infected through SMB.
- **Typical fact**: Anyone introduces himself into a computer or telecommunications system protected by security measures or keeps himself against the express or tacit will of those who have the right to exclude him.
- **Subject**: Anyone, the conspirators.
- **Action**: intrusion in victim's computer.
- **Event**: the access to private computers
- **Causality**: the principle of causality is validated: without the action of conspirators, the victim would never have received the compromised email and even all the other computers in the same network, would never have been infected.
- **Suitas**: conspirators know they are illegally accessing information.
- **Intent**: conspirators want to access and compromise information in order to ask for a ransom.
- **Aggravating or extenuating circumstances**: there are no aggravating or extenuating circumstances.
- **Causes of justification**: there are no causes of justification.

Art. 635 ter ICC: *damage to data, information, programs of the state or of the p.a. or otherwise of public utility* Unless the fact constitutes a more serious offense, anyone commits a fact aimed at destroying, deteriorating, canceling, altering or suppressing information, data or computer programs used by the State or other public body or relevant to them, or in any case of public utility, is punished with imprisonment from one to four years. If the fact leads to the destruction,

deterioration, cancellation, alteration or suppression of information, data or computer programs, the penalty is imprisonment from three to eight years. If the fact is committed with violence to the person or with threat or abuse of the quality of system operator, the penalty is increased.

- **Fact**: Private, Government, Health Services and Companies computers are infected.
- **Typical fact**: Anyone who destroys, deteriorates, cancels, alters or suppresses information, data or computer programs of others used by the State or other public body or relevant to them, or in any case of public utility.
- **Subject**: Anyone, the conspirators.
- **Action**: intrusion in public, government and organizations computers.
- **Event**: the access to public computers
- **Causality**: the principle of causality is validated: without the action of conspirators, a random public office would never have received the compromised email and even all the other computers, in the same network, would never have been infected.
- **Suitas**: conspirators know they are illegally accessing information.
- **Intent**: conspirators want to access and compromise information in order to ask for a ransom.
- **Aggravating or extenuating circumstances**: the attackers willingly compromised computer of public utility such as hospitals and police stations putting the lives of patients at risk.
- **Causes of justification**: there are no causes of justification.

Art. 635 bis: ***damage to data, information, programs*** Unless the fact constitutes a more serious offense, anyone who destroys, deteriorates, cancels, alters or suppresses information, data or computer programs of others is punished, upon complaint by the injured party, with imprisonment from six months to three years. If the fact is committed with violence to the person or with threat or abuse of the status of operator of the system, the penalty is imprisonment from one to four years.

- **Fact**: Files of the infected computers are encrypted with .WCRY extension.
- **Typical fact**: Anyone who destroys, deteriorates, cancels, alters or suppresses information, data or computer programs of others.
- **Subject**: Anyone, the conspirators.
- **Action**: damaging data in computers through malicious software.
- **Event**: the alteration of data in computers.
- **Causality**: the principle of causality is validated: without the action of conspirators, the victims would never have their data compromised.
- **Suitas**: conspirators know they are illegally manipulating data and information.
- **Intent**: conspirators want to access and compromise information in order to ask for a ransom.
- **Aggravating or extenuating circumstances**: there are no aggravating or extenuating circumstances.
- **Causes of justification**: there are no causes of justification.

Art. 615 quinquies ICC: ***Distribution of equipment, devices or computer programs aimed at damaging or interrupting an IT or telematic system*** Anyone, for the purpose of unlawfully damaging an information or computer system, the information, data or programs contained therein or relevant to it or to favor the interruption, total or partial, or the alteration of its operation, obtains, produces , reproduces, imports, disseminates, communicates, delivers or, in any case, makes available to other equipment, devices or computer programs, is punished with imprisonment up to two years and a fine of up to 10,329.

- **Fact**: The malware keeps the system from rebooting.
- **Typical fact**: Anyone, for the purpose of unlawfully damaging an information or computer system, the information, data or programs contained therein or relevant to it or to favor the interruption, total or partial, or the alteration of its operation.
- **Subject**: Anyone, the conspirators.
- **Action**: damaging computer system to favor the interruption, total or partial, or the alteration of its operation.
- **Event**: the alteration computers.
- **Causality**: the principle of causality is validated: without the action of conspirators, the victims would never have received the compromised email and the computer wouldn't have been damaged.
- **Suitas**: conspirators know they are illegally damage computers.
- **Intent**: conspirators want to interrupt computer system.
- **Aggravating or extenuating circumstances**: there are no aggravating or extenuating circumstances.
- **Causes of justification**: there are no causes of justification.

Art. 640 ter ICC: *IT fraud* Anyone who, by altering in any way the functioning of a computer or telecommunications system or intervening without any right in any way on data, information or programs contained in a computer or telematic system or pertinent to it, procures to himself or others an illicit profit with other people's damage, is punished with imprisonment from six months to three years and with a fine from fifty-one euro to one thousand and two euros. The penalty is imprisonment from one to five years and a fine from 309 euros to 1549 euros if one of the circumstances provided for by number 1) of the second paragraph of article 640 occurs, or if the fact is committed with abuse of the status of system operator. The penalty is imprisonment from two to six years and a fine from 600 euro to 3,000 euro if the fact is committed with theft or improper use of the digital identity to the detriment of one or more subjects. The crime is punishable upon complaint by the injured party, unless any of the circumstances referred to in the second and third paragraphs or any of the circumstances provided for in Article 61, first paragraph, number 5 occur, limited to having taken advantage of personal circumstances, including in reference to age, and number 7.

- **Fact**: After the computer gets enctypted, the attackers demand a ransom between $300 and $600 in order to get the decryption key to make the files usable again. It clearly produces illegal profit with other people's damage.
- **Typical fact**: Anyone obtains, produces, reproduces, imports, disseminates, communicates, delivers or, in any case, makes available to other equipment, devices or computer programs.
- **Subject**: Anyone, the conspirators.
- **Action**: encrypting user data and asking a random
- **Event**: user data are encrypted and a ransom must be paid in order to get them back.
- **Causality**: the principle of causality is validated: without the action of conspirators, the victim would never have their files compromised and their money taken.
- **Suitas**: conspirators know they are compromising user data and illegally profiting from their damage.
- **Intent**: conspirators want profit from people's damage
- **Aggravating or extenuating circumstances**: there are no aggravating or extenuating circumstances.
- **Causes of justification**: there are no causes of justification.

In depth legal analysis

Immediately following WannaCry ransomware cyberattacks, the United Kingdom's National Cyber Security Centre (NCSC) speculated that the hacker group *Lazarus* believed to have ties to the North Korean government—launched the operation.

A variety of companies, including FEDEX, Renault, Telefonica and Deutsche Bahn, were affected. Hardest hit, however, was England's National Health Service (NHS England). According to a National Audit Office report [Office (2018)], 603 primary care facilities were impacted. Many NHS staff could not access their files and therefore were unable to retrieve or update patient records, while thousands of pieces of medical equipment were locked. Countless medical appointments, and even surgical procedures, had to be cancelled. Many patients needing immediate care were diverted to providers unaffected by the ransomware attacks.

The Legal Character of the Operation Assuming that the ransomware attacks were attributable to North Korea, the question is whether the operation breached any international law obligations North Korea owed another State, such that it constituted an "internationally wrongful act." In cases involving States, the international law rules most likely to be violated are the prohibition on the use of force, the prohibition on intervention into other States' internal or external affairs, the obligation to respect the sovereignty of other States, and the obligation to exercise due diligence.

There is general agreement that destructive operations or those that are injurious cross the use of force threshold, and thus constitute a violation of Article 2(4) of the UN Charter and customary international law stating that .*All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."* . The WannaCry operation did not appear to reach this level.

Whether non-destructive and non-injurious cyber operations can qualify as uses of force is unsettled. Hostile cyber operations of a significant scope and scale that disrupt the provision of healthcare could reasonably be viewed as a use of force. By contrast, we believe it unlikely that States will treat non-destructive cyber operations directed against or affecting private firms as uses of force absent at least a major disruption of the national economy.

Although a number of the WannaCry attacks could arguably be treated as uses of force, the same is not true with respect to the prohibition on intervention into other States' internal or external affairs. Intervention has two elements. First, the act must relate to the target State's domaine réservé (field of activity that is not committed to international law regulation). Certain WannaCry attacks did so, particularly those affecting law enforcement. However, the operation arguably did not satisfy the second criterion, that the act be coercive. A coercive cyber operation is one that causes a State to engage in conduct in which it would otherwise not engage, or refrain from conduct in which it would otherwise engage. WannaCry was disruptive, but not coercive in this sense.

The WannaCry attacks might, however, be considered a violation of the sovereignty of certain affected States. There is a debate over whether respect for another State's sovereignty is a primary rule that imposes a legal obligation or is instead merely a legal principle from which primary rules, such as the prohibitions on intervention and the use of force derive.

Whatever the correct answer, a violation occurs whenever a cyber operation either causes damage to cyber infrastructure in another State or interferes with an inherently governmental act, the paradigmatic example being the conduct of elections. "Damage" includes a permanent loss of functionality or one that requires physical repair of the damaged infrastructure, such as replacement of the hard drive.

That does not appear to have occurred this time. Instead, the WannaCry effects fall into a grey zone in which the threshold for violation remains unsettled. We are of the view that the operation did in some respects violate the sovereignty of a number of States, particularly in light of the significant disruption of functions, which we would count as "damage," necessary for the delivery of medical care. Moreover, the operation interfered with an inherently governmental function—law enforcement.

A final possible internationally wrongful act is North Korea's failure to abide by its due diligence obligation, which obliges States to put an end to ongoing cyber operations from their territory that have "serious adverse consequences" for other States' rights. Thus, if North Korea is not legally responsible as described below for the Lazarus Group's hostile cyber operations, it might nevertheless have been in breach of its due diligence obligation if it knew of the operation and failed to act to end it. It must be cautioned that a number of States are assessing the contours of this obligation in the cyber context and thus it remains somewhat controversial.

The Attribution Issue Pursuant to the law of State responsibility, an internationally wrongful act not only requires a breach of an obligation owed by one State to another, but also attribution of the underlying act to the former. This begs the question of whether the WannaCry operation may be attributed to North Korea as a matter of law. North Korea, for its part, denies any link with the operation.

Little definitive evidence has been released supporting the conclusion that North Korea, through the Lazarus Group, was behind the WannaCry attack, although an internal assessment by the National Security Agency concluded that "cyber actors," suspected of being "sponsored by" North Korea's Reconnaissance General Bureau, were responsible for developing the WannaCry ransomware.

As confirmed by Article 8 of the International Law Commission's Articles on State Responsibility, *"the conduct of a . . . group of persons shall be considered an act of a State under international law if the . . . group . . . is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct."* The terms "instructions," "direction," and "control" are legally abstruse. Nevertheless, in an oversimplification, the State should either have charged the group with conducting the cyber operation in question or it must exercise "effective control" over the group such that it is acting on the State's behalf.

Thus, attribution is a two-step process. First, it must be shown that the Lazarus Group conducted the operation. Second, the relationship between the group and North Korea must be established at the level of instructions, direction, or control. Unfortunately, it is difficult to tease loose these two analytical strands from the limited material available, for public accounts tend to conflate them.

In this regard, several high-profile cyber-attacks have been attributed to the Lazarus Group, including the 2014 attack on Sony Pictures and the 2016 attack against Bangladesh Bank. In the former case, the FBI determined that the North Korean government was responsible. Its conclusion was based, in part, on "similarities in specific lines of code, encryption algorithms, data deletion methods, and compromised networks" that "North Korean actors previously developed," "significant overlap between the infrastructure used in [the Sony] attack and other cyber activity the U.S. government has previously linked directly to North Korea," and "similarities" in "the tools used" to an earlier cyber-attack against South Korean banks and media outlets. As to the latter, Kaspersky's forensic analysis "strongly link[ed]" the malware used to Lazarus' malware arsenal, while Symantec found a "rare piece of code" that was also found in the Sony attack.

Similarly, at the Dec. 19 White House press briefing that the U.S. assessment attributing the WannaCry attack to North Korea was based on "technical links to previously identified North Korean cyber tools, tradecraft, [and] operational infrastructure." These included routines used by "intermediaries" carrying out attacks "on behalf of the North Korean government in the past." Symantec also conducted a forensic analysis of the WannaCry operation and found "strong links" to the Lazarus Group based on similarities to malware used in previous attacks. Exercising caution, though, Symantec stated that "the WannaCry attacks do not bear the hallmarks of a nation-state campaign but are more typical of a cybercrime campaign."

It would seem that a strong consensus has developed that the Lazarus Group conducted the WannaCry attacks and that the group has ties to the North Korean government. But whether those ties are sufficient to meet the Article 8 threshold cannot be established from open sources. Nor can the more demanding other bases for attribution of non-State actor cyber operations—that the group is a de facto State organ (Article 4) or exercises elements of governmental control (Article 5)—be established.

Finally, the 2015 report of the UN Group of Governmental Experts, a body composed of representatives from 20 countries including the P5, suggested that "accusations of organizing and implementing wrongful acts brought against States should be substantiated." It must be emphasized, however, that the statement was hortatory; although doing so may be prudent in avoiding political or other tensions, insufficient State practice and opinio juris (in great part because cyber capabilities are in most cases highly classified) exist to conclude that there is an established basis under international law for such an obligation.

Response Options In terms of active defense, there are three core options beyond simple retorsion (actions that are unfriendly, but lawful, such as a counter-cyber operation that does not breach any legal obligation to the target State).

First, an "injured" State may take "countermeasures," actions that would be unlawful but for the fact that they are in response to another State's unlawful cyber operation and designed to terminate it or compel the "responsible State" to make reparations. As the WannaCry attacks have ended, countermeasures are now only available to compel North Ko-

rea to make reparations, such as a "guarantee" in the form of breaking up the Lazarus Group or providing compensation to injured States.

Second, a State may act based upon the plea of necessity (Article 25 of the Articles on State Responsibility) to end a harmful cyber operation that poses a "grave and imminent peril" to an "essential interest" of the State, even if the response might otherwise violate an international law obligation to a State that is not responsible for the operation. The precise meaning of "essential interest" is ambiguous, but it certainly would include the population's health, as with WannaCry's effects in England. A particular benefit of the plea is that attribution to a State is not a precondition for acting. However, like countermeasures, the plea is only available to put an end to the harmful cyber operations, and accordingly would no longer be available in this case.

Finally, a State may act in response to a cyber operation that qualifies as an "armed attack" pursuant to the customary international law right of self-defense, which is also codified in Article 51 of the U.N. Charter. As with the use of force, the armed attack threshold is unsettled in the cyber context, although the prevailing view is that, consistent with the judgement of the International Court of Justice in Nicaragua, an armed attack is a particularly grave use of force (the U.S., by contrast, maintains that the use of force and armed attack thresholds are identical). We believe it is unlikely that States would characterize the consequences of the WannaCry attack as rising to the armed attack level, thereby justifying a response at the use of force level. And, as with the aforementioned responses, the fact that the attacks have definitively ended would mean a response on the basis of self-defense would run afoul of its "immediacy" criterion.

Conclusion

Two years ago, a powerful ransomware began spreading across the world. WannaCry spread like wildfire, encrypting hundreds of thousands of computers in more than 150 countries in a matter of hours. It was the first time that ransomware, a malware that encrypts a user's files and demands cryptocurrency in ransom to unlock them, had spread across the world in what looked like a coordinated cyberattack.

Hospitals across the U.K. declared a major incident after they were knocked offline by the malware. Government systems, railway networks and private companies were also hit.

In just a few hours, the ransomware had caused billions of dollars in damages. Bitcoin wallets associated with the ransomware were filling up by victims to get their files back.

Two years on, the threat posed by the leaked NSA tools remains a concern. As many as 1.7 million internet-connected endpoints are still vulnerable to the exploits, according to the latest data.

WannaCry caused panic. Systems were down, data was lost and money had to be spent. It was a wake-up call that society needed to do better at basic cybersecurity.

Bibliography

[1] Dahlberg, D. (2017). *Assessing the Global Impact of WannaCry Ransomware*. https://www.bitsight.com/blog/assessing-the-global-impact-of-wannacry-ransomware.

[2] Europol (2017). *WANNACRY RANSOMWARE*. https://www.europol.europa.eu/wannacry-ransomware.

[3] EY (2017). *WannaCry ransomware attack*. https://www.ey.com/Publication/vwLUAssets/ey-wannacry-ransomware-attack/$File/ey-wannacry-ransomware-attack.pdf.

[4] Fruhlinger, J. (2017). *What is WannaCry ransomware, how does it infect, and who was responsible?* https://www.csoonline.com/article/3227906/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html.

[5] Kroustek, J. (2017). *Avast update on WannaCry: who was affected, who was targeted, how to remove it, and more.* https://blog.avast.com/wannacry-update-the-worst-ransomware-outbreak-in-history.

[6] McBride, A. (2017). *The Hours of WannaCry*. https://umbrella.cisco.com/blog/2017/05/16/the-hours-of-wannacry/.

[7] micro, T. (2018). *Ransomware: The Truth Behind the Headlines*. https://www.trendmicro.co.uk/media/misc/ransomware-the-truth-behind-the-headlines.pdf.

[8] Office, N. A. (2018). *Investigation: WannaCry cyber attack and the NHS*. https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf.

[9] P, S. (2017). *WannaCry: The ransomware cyber attack explained*. https://dig.watch/trends/wannacry.

[10] Richter, F. (2017). *200,000+ Systems Affected by WannaCry Ransom Attack*. https://www.statista.com/chart/9399/wannacry-cyber-attack-in-numbers/.

[11] Sophos (2017). *WannaCry: how the attack happened*. https://news.sophos.com/en-us/2017/05/19/wannacry-how-the-attack-happened/.

[12] Symantec (2017). *What you need to know about the WannaCry Ransomware*. https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack.

[13] Sysmatec (2017). *WannaCry: Ransomware attacks show strong links to Lazarus group*. https://www.symantec.com/connect/blogs/wannacry-ransomware-attacks-show-strong-links-lazarus-group.