Panda Adaptive Defense 360

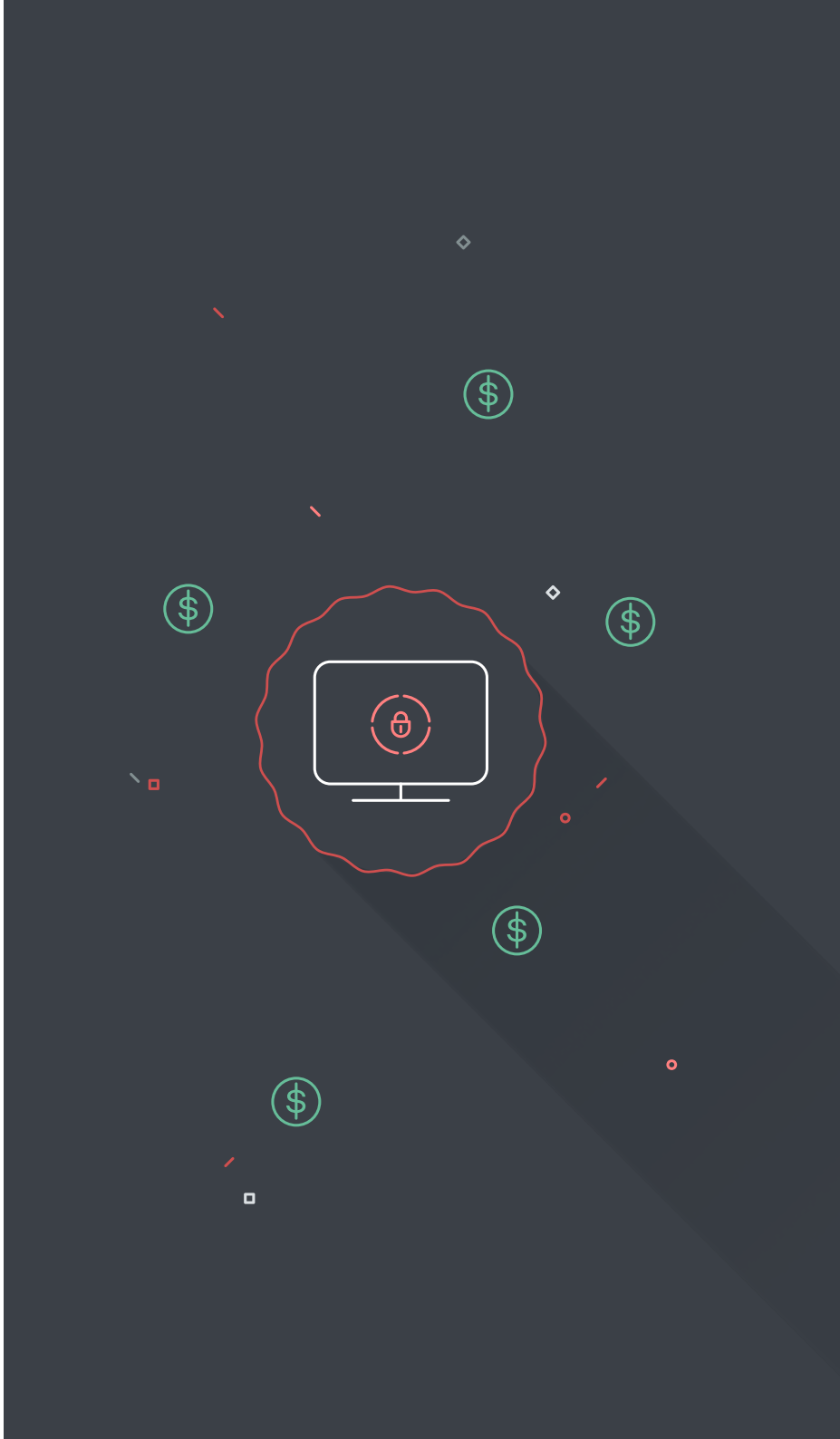
Limitless Visibility, Absolute Control

NO KIDNAPPING, NO RAN$OM

panda

pandasecurity.com/business/adaptive-defense/

Table of Contents



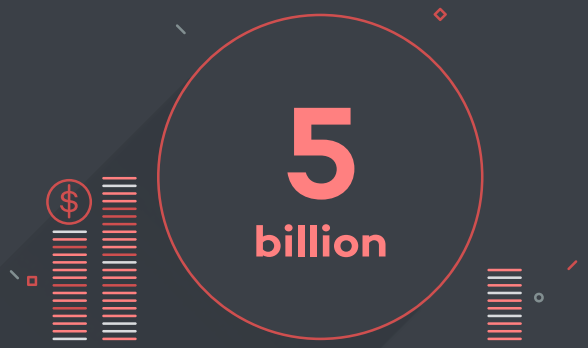
panda

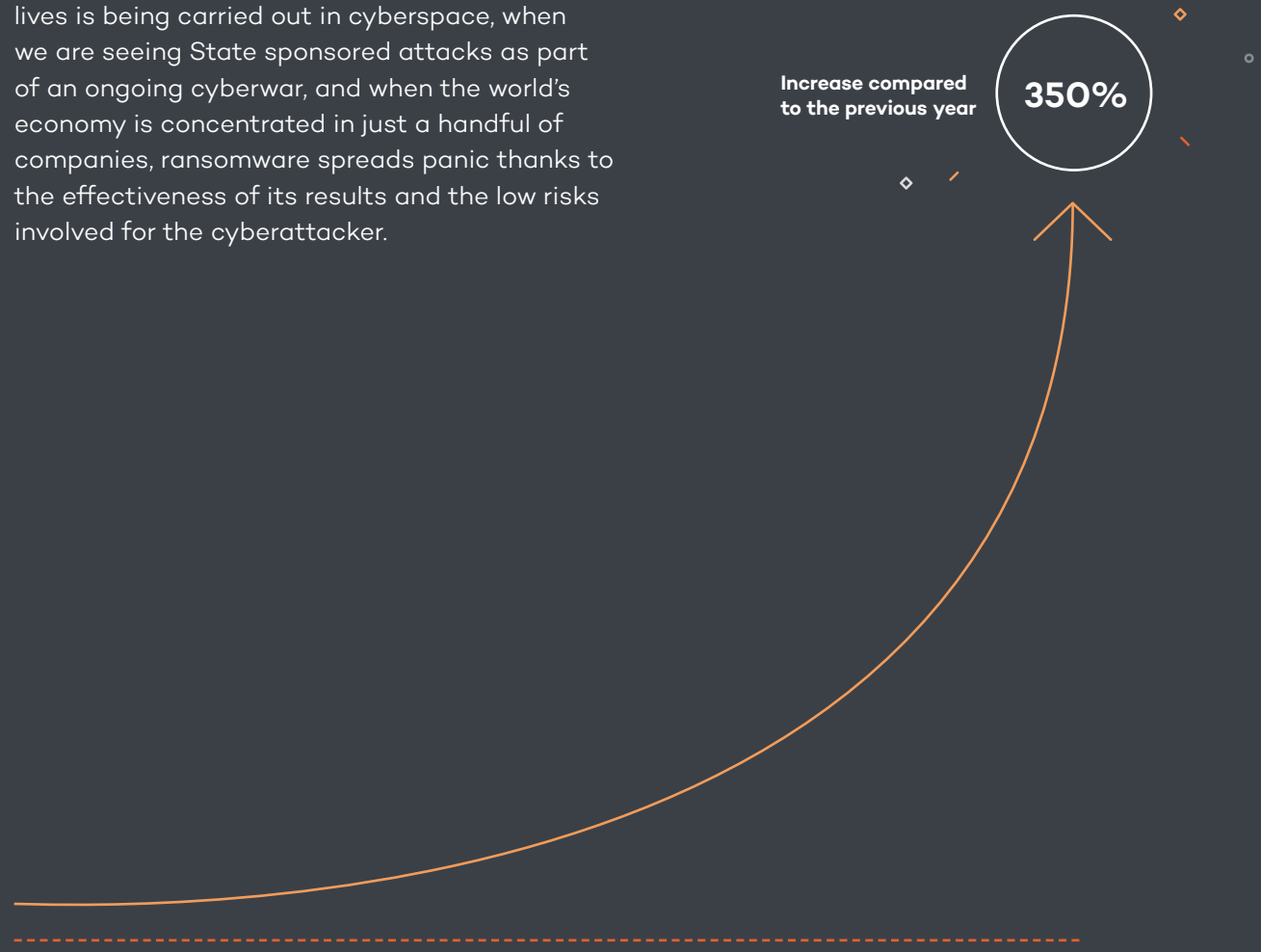
1. Introduction

Ransomware is still one of the most lucrative weapons in a cybercriminal's arsenal. This kind of cybercrime encrypts the files on a computer, and blocks access to them until the required ransom is received, generally in the form of bitcoin, an untraceable **virtual cryptocurrency**.

The total cost of this Trojan in 2017 was around **$5 billion**, a **350% increase compared to the previous year**, making it not only the most sophisticated type of cyberattack, but also the one with the highest impact.

At a moment when more and more of our daily lives is being carried out in cyberspace, when we are seeing State sponsored attacks as part of an ongoing cyberwar, and when the world's economy is concentrated in just a handful of companies, ransomware spreads panic thanks to the effectiveness of its results and the low risks involved for the cyberattacker.

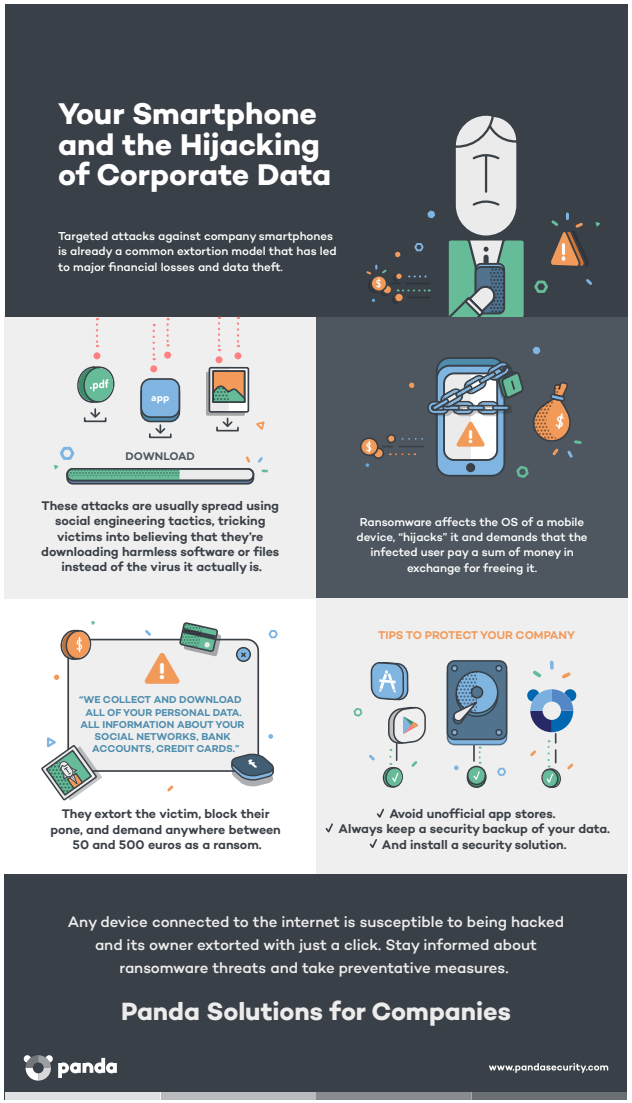




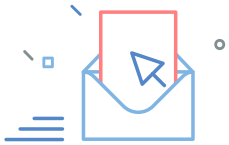
2. The paradigm of digital transformation

With over 258,000 new threats detected by PandaLabs every day, the so-called digital transformation implies major new challenges. Cybercrime is now a more active threat than ever. Cyberattacks and financial fraud that use technologies have reached a degree of sophistication hitherto unimaginable. Online, where it's easy to become anonymous, people's trust can be gained with social engineering, making us lower our guard, and laying bare our privacy.

Along with these new online habits, we also acquire new platforms like **Android**, the most widely used operating system in the world. Android's popularity also makes it the main attack vector to infect and spread **ransomware, such as** Charger, that is able to hold the data on any smartphone to ransom.



In the same vein, it is expected that by 2020, there will be a total of 50 billion devices connected to the Internet, generating 40 trillion GB every ten minutes. **On the Internet of Things (IoT)**, security has become a critical aspect. Having more handheld devices that can connect to the Internet means that hackers can use new methods: would you consider infecting other people to get out of paying the ransom yourself? This is the morbid propagation method used by Popcorn Time.

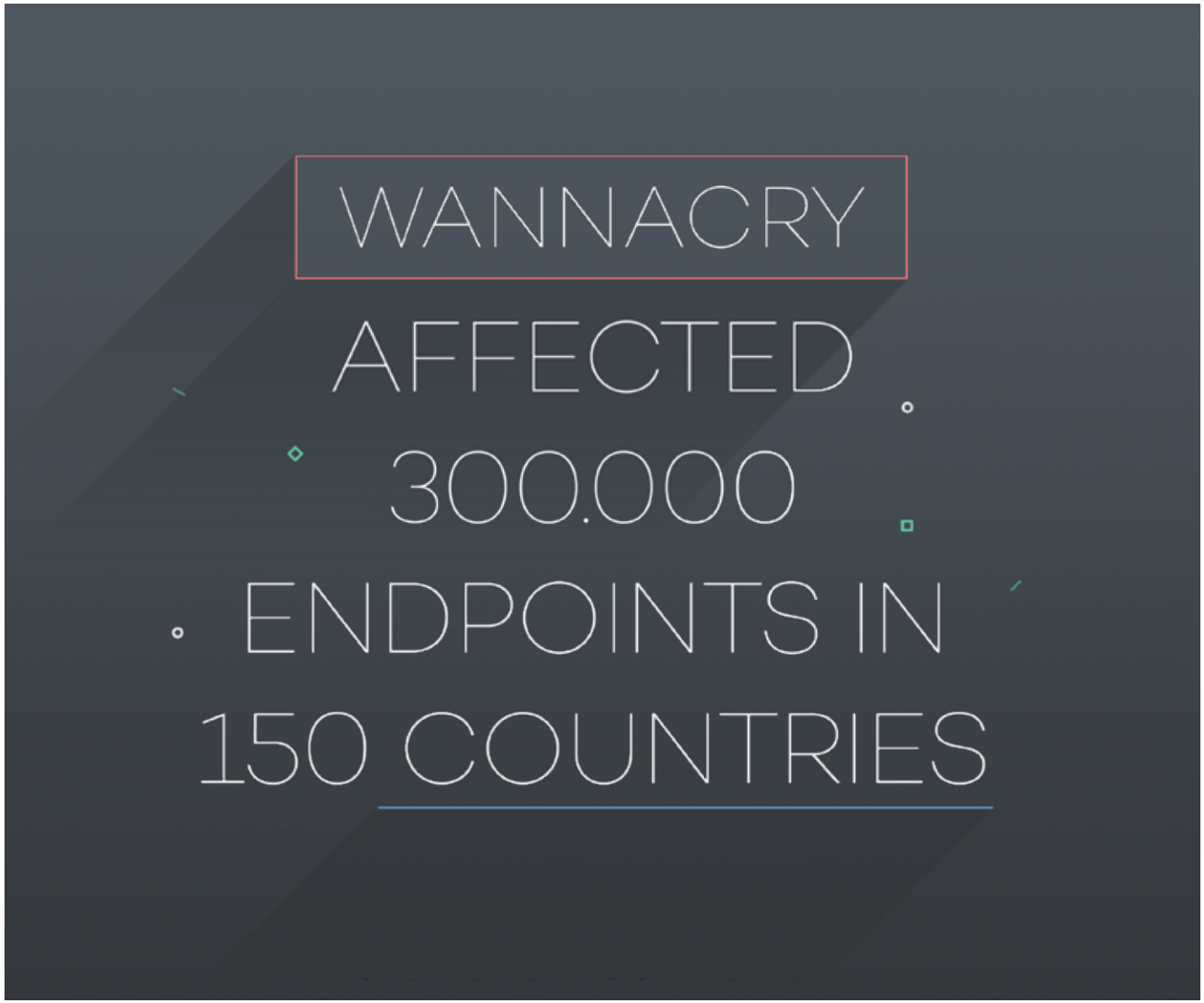


This proliferation of mobile devices has unleashed a whole array of new techniques that allow hackers to carry out attacks in advanced technological spaces. This is what happened in an Austrian hotel, where cybercriminals attacked the hotel, locking the room doors and disabling the software used to program the key cards.

3. State sponsored attacks

There is some suspicion that the two largest attacks in history (WannaCry and Goldeneye/NotPetya) could have been carried out with the backing of governments (North Korea in the case of WannaCry, and Russia in the case of Goldeneye/NotPetya). Both attacks used ransomware, and had a high capacity of self-replication, as was also seen in the case of Bad Rabbit, which shared many similarities with the ransomware NotPetya.

As the ransomware was a network worm, any computer infected with WannaCry ended up with its documents held to ransom, and also contributed to its rapid expansion to over 300,000 computers, making use of an old vulnerability in Microsoft Windows to spread, and infect the very core of organizations and businesses.



4.Businesses in the spotlight

Ransomware is a problem affecting an ever higher number of companies, and one that only really comes to light when one of the attacks goes viral, as was the case last year with WannaCry.

Today, 18% of the market capitalization of listed companies in the US is the sum of just 5 companies: Apple, Google, Amazon, Microsoft and Facebook.

Bearing in mind that the aim of ransomware is economic gain and that, while it isn't possible to make off with the money using physical means, there are ways to transfer it from one person to another using new weapons, cybercriminals have no qualms about using trickery to get their hands on the money via:

Cyber-theft

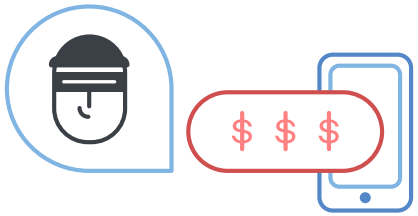
- Cyber-theft, such as the one Equifax fell victim to, making it the center of the largest breach of sensitive private information in history. The breach was made possible by a vulnerability that had previously been exploited by ransomware, opening the doors to the cyberattackers

Extortion

- Extortion, as a way of getting something, especially money, using force or threats. We have three clear illustrations of this in WannaCry, NotPetya and Bad Rabbit.

Sabotage

- Or sabotage of civilian or military facilities. For example, in August 2012, Shamoon infected more than 30,000 systems belonging to Saudi Arabia's state owned national oil and gas company, Aramcio, paralyzing its exports for two weeks. The same software was used again several years later to carry out a series of cyberattacks, this time including a new module containing ransomware.



As well as the aforementioned crimes, in the last few months we've seen several new strategies to get ransomware onto corporate networks, such as the use and abuse of legitimate Windows tools, like PowerShell, to infect computers with **Cerber**. This was the goal of **Crysis/Dharma**. In this case, the server executed the Remote Desktop Protocol (RDP), and the attackers used a brute force attack to guess login details and gain remote access. The trend of installing malware using RDP has reached a point of such sophistication that the ransomware itself has its own interface that allows criminals to select the folders whose content is to be encrypted, pick the network computers, self-delete, find email addresses to contact victims, and so on. This is that we saw with the ransomware **WYSIWYE**, discovered by PandaLabs.

There are also families of ransomware that add functions in order to cause more damage; tricks like working offline, or spreading more quickly are used by the dreaded **Locky**.

With this information, now more than ever it's beginning to feel like companies should have **insurance policies** that can cover, at least partially, the costs of these cyberattacks. It is a rapidly expanding sector and, in fact, most cyber-insurance policies that are taken out to offset ransomware are virtually made to measure, taking into account the main risks faced by the company.

5. The price of attacks

We've seen how the democratization of cyberattacks has been made easier by several variables, such as the professionalization of attackers, the evolution of technology, and the ease with which data can be accessed. Although something that has doubtless helped to popularize this kind of threat is the profitability to be gained from carrying them out. Cyberweapons that can be used by attackers to get a juicy reward are sold at budget-friendly prices.

Fuente: Recorded Future.

Ransomware attacks are still on the up, and the number will continue to rise as long as victims keep paying the ransoms. Nevertheless, there are always some concrete measures we can take to avoid these attacks:

Ensure that employees' user accounts are protected with strong passwords, and that they don't have administrator permissions.

Don't open emails from unknown senders or emails that ask you to open them: the best thing to do is to delete them straight away, and under no circumstances reply to them.

Don't trust shortened links or attachments, even if they're from trusted contacts.

Create backups regularly to avoid losing data.

Draw up and implement an auditing plan (carried out by internal auditing teams, or specialized third parties), both for the organization's systems and for its policies, in order to be able to detect possible vulnerabilities.

Invest resources in improving training and staff awareness of IT security, especially when it comes to this type of threat.

The importance of multilevel security: In view of current threats like ransomware, basic protection is not enough. To ensure maximum protection, it is highly recommended to use complex, robust multiplatform tools like Panda Adaptive Defense 360.

Panda Adaptive Defense 360

Limitless Visibility, Absolute Control

More info at:

pandasecurity.com/business/adaptive-defense/

Let`s talk:

000 00 00 00

panda