panda

2019: A Record-Breaking Year For Ransomware

There Was No Escaping Ransomware In 2019

The First Signs of Trouble

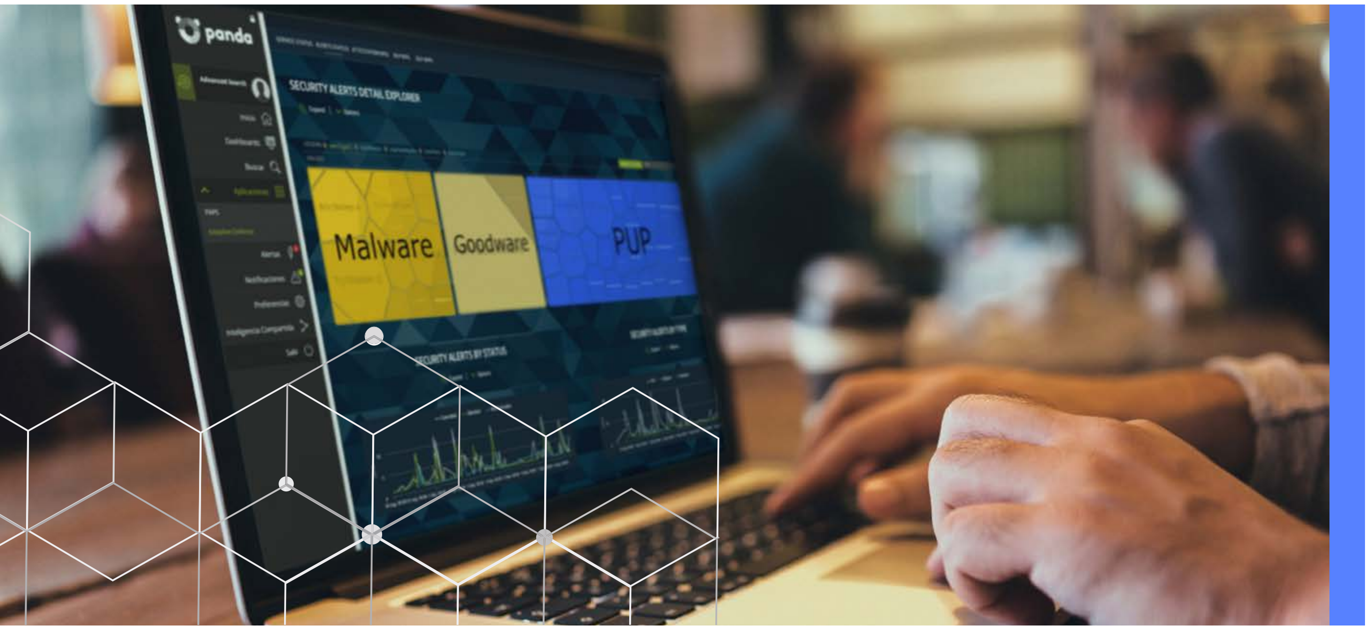
A Focus On US Government Agencies

The Attacks Go Global

The Main Ways Hackers Access A Network

Zero Trust: Your Best Bet For Preventing A Ransomware Attack

There Was No Escaping Ransomware In 2019



2019 has been another record-breaking year for ransomware attacks.

We've seen a variety of attacks more diverse than ever before: from government agencies to international corporations, from the United States to Europe and beyond, it seemed like nothing was safe from ransomware in 2019. The statistics speak for themselves: ransomware attacks have shot up 500% in 2019 since this time last year.

With this increase in attacks in mind, all organizations are exposed to security breaches: from large multinationals, to SMEs, to public organizations. In fact, according to the World Economic Forum, the percentage of organizations that experienced an attack in 2018 was 61%. The 2019 figure is likely to be even higher. This is largely due to the surge of ransomware attacks that we've seen throughout the year.

So what did ransomware in 2019 actually look like? Read on to learn about the biggest attacks of the year, how companies bounced back from them, and how you can stay protected in 2020.

02

RANSOMWARE ATTACKS SHOT UP 500% IN 2019.

The First Signs of Trouble

The earliest indicators that 2019 would be a big year for ransomware came in January. The city of Del Rio, Texas, reported a ransomware attack that affected their systems, and forced them to carry out their administrative tasks manually, with pen and paper. Del Rio's Management Information Services were obliged to disconnect City Hall's computers to keep employees from accessing the system and spreading the infection. According to US media outlets the attack was carried out using an unusual strategy. The ransom note included a phone number to communicate with the attackers and get instructions as to how to pay to recover their files.

It's not just government organizations that were targets for ransomware in 2019. In March, a Norwegian company called Norsk Hydro suffered a devastating attack when a strain of ransomware called LockerGoga got onto its network and forced the closure of 22,000 endpoints in 40 countries. This was a highly targeted attack; according to the BBC, the attackers spent weeks on the company's IT systems, searching for weak points and vulnerabilities before launching the ransomware. So far, the company has spent over $55 million recovering from the attack.

Norwegian company Norsk Hydro has spent over $55 million recovering from the attack.

LockerGoga was most likely delivered via a phishing attack, potentially hidden in Word documents with malicious macros. Some of the characteristics of the ransomware could suggest that encrypting files and demanding a ransom is not the main goal of LockerGoga. In some variants, the malware changes the administrator's password and logs the victim off using logoff.exe, making it much harder to pay the ransom.

03

A Focus On US Government Agencies

While the trend for attacking government agencies began with the incident in Del Rio, it was only a matter of months before similar organizations fell victim.

In March, the city of Jackson County, Georgia unleashed controversy when it paid the $400,000 ransom demanded by cybercriminals after a ransomware attack—probably a variant of Ryuk. The infection closed down almost all of the local government's systems except for its website and its emergency system.

In April, the city of Augusta, Maine, suffered what was described as a highly targeted ransomware attack. The attackers demanded a ransom of at least $100,000. Luckily, the city managed to stop the ransomware, and their systems were almost back to normal the following day.

In May, two cities were attacked in the span of two days. The first was Cartersville, Georgia on the 6th. The following day, the city of Lynn, Massachusetts was hit by a piece of ransomware called "Herpes 1.2", which infected the city's online parking payment system.

The same day as the attack on the city of Lynn, the municipal government of Baltimore announced that the city government had closed most of its servers due to a ransomware attack. The attackers demanded a 3 Bitcoin ransom for each computer, or 13 Bitcoins to free the whole city. The city's systems were out of service for nearly a whole month, and to date, the city has spent $4.6 million on recovering the data on all its computers.

04

The attack on Baltimore was just the start of a ransomware-filled summer in the United States.

05

The strain of ransomware used in these attacks is called RobbinHood. According to Bleeping Computer, the ransomware doesn't get onto computers via spam; rather, it takes advantage of remote desktop protocols (RDP) or other Trojans that can let the attacker gain access. In the last few months, there has been some evidence that the attackers that encrypted the systems in Baltimore are proud of their work: a new variant of RobbinHood includes a ransom note that suggests that the victim google 'Baltimore' to understand the gravity of their situation.

Unfortunately, the attack on Baltimore was just the start of a ransomware-filled summer in the United States. Later in the year, two cities in Florida were attacked in one week, both of which took the controversial decision to pay the ransoms—65 bitcoins (over $650,000) in Rivera Beach, and 42 bitcoins ($450,000€) in Lake City.

One of the most striking incidents came on the morning on August 16: a total of 22 local governments in Texas became victims of a coordinated ransomware attack. Although the Texan authorities didn't reveal what ransomware was used in the attack, they did announce that the 22 attacks came from the same source. The attackers demanded a $2.5 million ransom.

The Attacks Go Global

After a successful summer in the United States, these types of ransomware attacks began spreading to Europe and the rest of the world in the fall. In the middle of September, several city halls and institutions in Spain were affected by ransomware attacks. Additionally, in the Basque Country region of Spain, there were at least four reports of alleged cybersecurity crimes, while the municipal government announced that it had been attacked by a piece of ransomware called Ryuk. This crypto-malware encrypted the files stored on over 50 servers, forcing municipal government employees to carry out their work by hand.

06

The ransomware trend also hit Germany, where a major producer of automation tools was paralyzed for over a week by an incident involving the ransomware BitPaymer.
Outside of Europe, the systems of the city of Johannesburg, South Africa were hijacked by attackers demanding 4 Bitcoins.

Among the latest victims of ransomware are several Spanish companies, whose systems were encrypted at the beginning of November. The team at Panda Labs has reviewed the ransom note received by the affected external clients, and we have seen that these incidents share many characteristics with the ransomware BitPaymer.

PandaLabs explains, "According to our preliminary investigations, which still haven't been confirmed, one of the strongest hypotheses is that the victims could be companies affected by some of the spam campaigns launched in the previous weeks, whose aim is to infect the machines with the malware Emotet. If this is the case, the ransomware will have kept a low profile until now, when its C&C sent it BitPaymer to begin the attack."

The most recent victim is the Mexican oil company Pemex. On November 11, several computers were hijacked, stopping employees from carrying out their work. The IT department advised the employees to disconnect their computers.

> THIS CRYPTO-MALWARE ENCRYPTED THE FILES STORED ON OVER 50 SERVERS, FORCING MUNICIPAL GOVERNMENT EMPLOYEES TO CARRY OUT THEIR WORK BY HAND.

07

The Main Ways Hackers Access A Network

Although this series of attacks have coincided in time and form, in practice they have all used a wide variety of techniques to get onto their victims' systems. The main causes for these ransomware attacks are the following:

In the Norsk Hydro incident, the attackers spent months on the company's system, searching for vulnerabilities that could be used in conjunction with spam to launch the ransomware.

And this isn't an isolated case; in fact, the cause of one in every three security breaches is an unpatched vulnerability. One of the most notorious ransomware attacks in history—WannaCry—exploited a vulnerability to get onto some 300,000 computers worldwide.

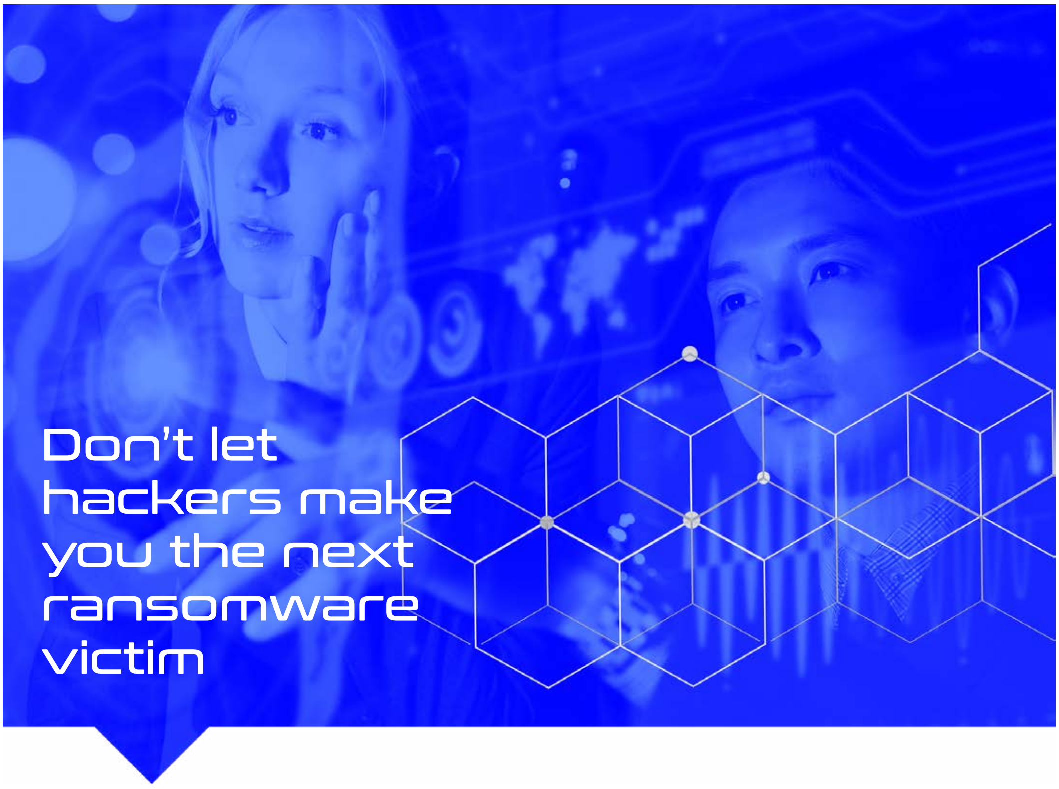
92% of the world's malware gets in via phishing, and ransomware is no exception.

It can be hidden in attachments with macros or links to malicious URLs. One of the theories for how the ransomware made its way into Spanish companies in November is that it got in via a phishing email sent by the botnet Emotet.

08

To carry out the massive attack in Texas, a technique called island hopping was used.

Island hopping is a supply chain attack where cybercriminals infiltrate the networks of smaller companies—marketing or HR companies, for example, that are normally providers for the final target, and use this access to gain entry to larger organizations. In the case of Texas, island hopping was possible because many of the affected municipalities share the same software and IT system provider.



09

Zero Trust:

Your Best Bet For Preventing A Ransomware Attack

The fact remains that ransomware is an ever-present threat, and one that is very hard to contain if you don't have the appropriate protection in place, and don't follow the proper steps. The most important thing is to follow a zero trust approach to security: don't trust anything until you can be sure that it is not malicious.

Panda Adaptive Defense isn't based on signatures or traditional techniques, but on zero trust of all activity on all devices. To achieve this, it proactively monitors all activity on every computer and server in order to classify each process on all of the devices in the organization and define their behavior profiles. If Adaptive Defense detects any suspicious activity, even if the process itself doesn't have a seemingly suspicious profile, it blocks it and analyzes it in order to determine whether or not to allow it to execute. In addition, Adaptive Defense has anti-exploit technology that is able to detect malicious scripts and macros.

99.98% of the decisions are made automatically thanks to artificial intelligence processes based on machine learning and deep learning. The remaining 0.02% of decisions are delegated and scaled to a team of expert threat hunters who determine the nature of the process in question, enriching and perfecting the automatic algorithms at the same time.

In addition, you can further reduce the attack surface with Panda Patch Management. This module searches for and applies patches and updates to operating systems and hundreds of applications so that vulnerabilities don't pose a risk of intrusion.

Don't let hackers make you the next ranomware victim. Join our customers, who have experienced zero breaches in 2019 from ransomware attacks and be breach proof with Panda Adaptive Defense.

Live Demo

Contact Us

More info at:

pandasecurity.com/usa/business

Let's talk:

1-877-263-3881

sales@us.pandasecurity.com

panda