HORNETSECURITY

INFOPAPER

CYBERCRIMINALS IN THE PRE-CHRISTMAS SEASON - 5 TIPS ON HOW TO BEST PROTECT YOUR BUSINESS

The year is coming to an end: it is getting colder, it is getting darker and the earliest shoppers are already thinking about what to give their loved ones for Christmas. Online retailers and local stores are getting ready for the annual, high-turnover pre-Christmas rush.

It all starts with the discount battle on the last November weekend with **Black Friday and Cyber Monday**. Ideally, this period is also good for enterprises to promote appropriate offers for their customers, in order to draw the good deal hunters out. But this period is not only profitable for enterprises— **cybercriminals would also like to cash in and claim a tidy Christmas bonus for themselves.**

What types of attacks are most frequently used by cyber criminals? What makes the attacks so dangerous? And how does the Corona pandemic change the pre-Christmas business? We'll explain all this and more in the following Infopaper plus give you **5 tips on how to best protect your business.**

Content

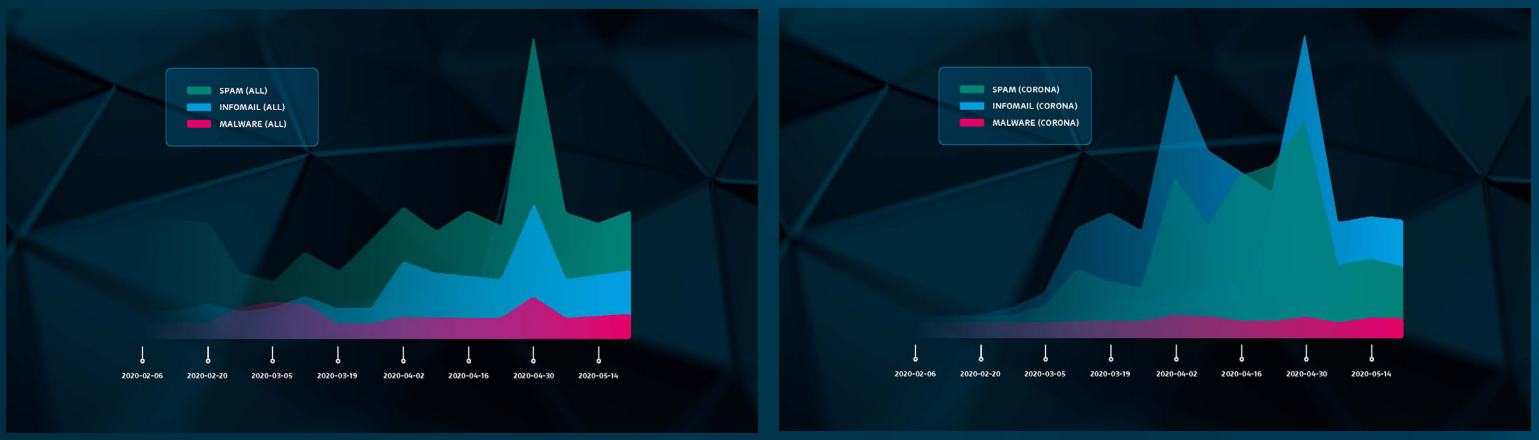
Caution: Cybercriminals in the Christmas spirit...or not?

Cybercriminal gangs leverage current events and hot media topics for their attacks. This should have become clear to everyone since the advent of the Corona virus:

Increased hacker attacks on medical facilities, attacks on research laboratories as well as phishing attacks that referred to fake corona tests or discount campaigns for mouth and nose masks have already adorned the headlines.

The Hornetsecurity Security Lab has recorded a corresponding increase in cyber attacks via e-mail since February 2020, as shown in the following chart:

FIG. 1: Increase in spam, infomail and malware before and during Corona



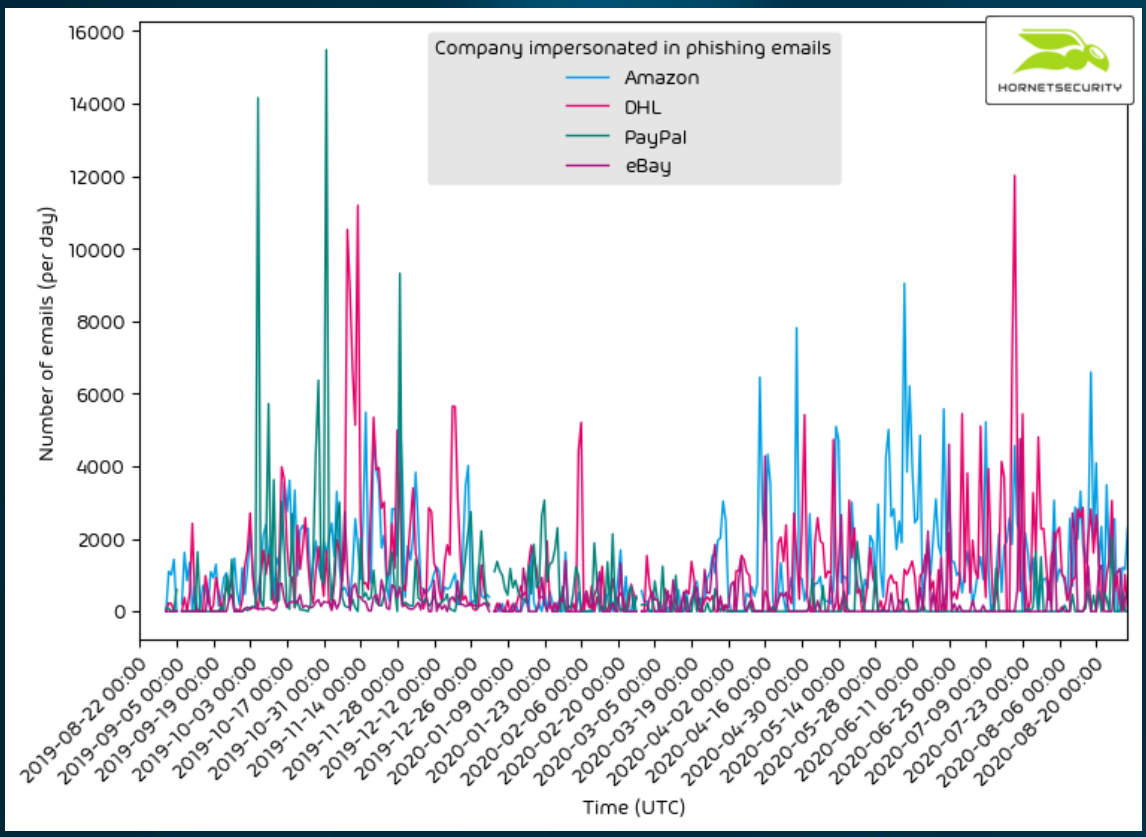
Although the Corona pandemic is far from over, another event is already on the horizon, which has been used again and again in recent years as **a trigger for cyber attacks: The pre-Christmas business around Black Friday and Cyber Monday.**

But what does the consumer demand actually look like in times of Corona? Are Black Friday and Cyber Monday still important for getting bargains? The answer is yes.

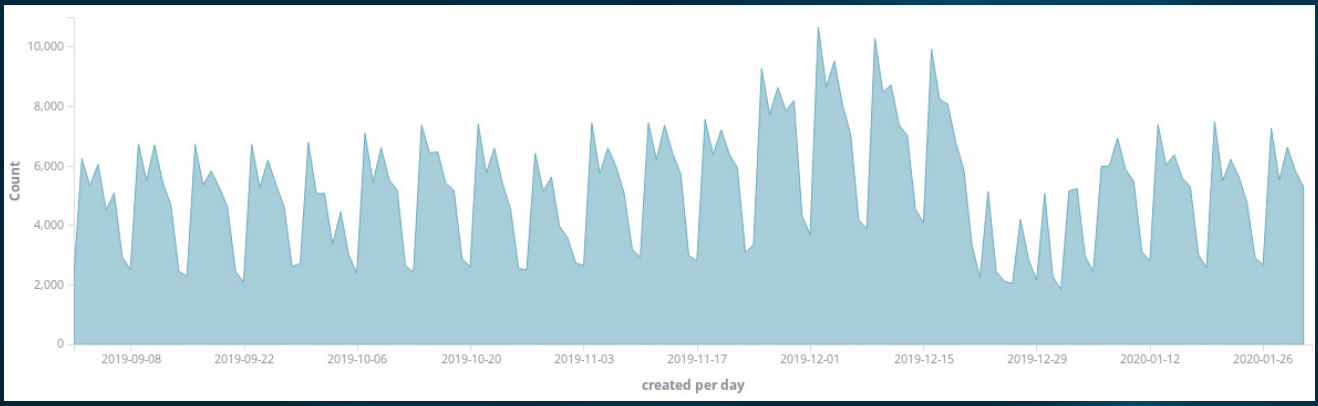
In the middle of the year, Google started a worldwide survey among its users to find out how the Corona Pandemic is changing purchasing behavior. **75% of the users surveyed actually plan to increase their online Christmas shopping this year.** Where in recent years, some consumers still preferred to shop locally in stores, everything is increasingly shifting to the Internet. As a result, Internet store providers expect demand to rise this year, but they also expect increased competitive pressure—especially if brick-and-mortar retail also proves competitive in online business—and the focus is on price in particular. As a result of reduced working hours and increased unemployment worldwide, online providers are entering a price war and consumers are going bargain hunting.

All of this means more opportunities for cybercriminals to attack.

Last year, Hornetsecurity's Security Lab observed an **increase in phishing campaigns from November to mid-December.** The fake e-mails often lure with tempting offers during the pre-Christmas period and high-consumption days like Black Friday and Cyber Monday.



The online giant Amazon, in particular, has to pay for its popularity by being targeted by the criminal activities of hackers time and again. **From the end of last November onwards, an increasing number of phishing e-mails were sent on behalf of Amazon.**
This is shown by the following observation of Hornetsecurity Security Labs from last year:



But not only phishing attacks are expected to increase these days, online retailers in particular must prepare for an **increase in DDoS attacks**. With a flood of server requests, hackers are forcing the providers' systems to their knees, which means that many sales opportunities are lost. But that's not all:

For two years now, Emotet has been back with Christmas greetings at the end of the year.

It is therefore not unlikely that **an increased number of ransomware attacks on companies can be expected this December as well.**

Following is a comprehensive insight into the threat situation resulting from DDoS, phishing and ransomware attacks—including 5 helpful tips to help you protect yourself against the increasing professionalism of these types of attacks.

„Server down." How DDoS attacks bring online merchants to their knees

For the digital business world, they represent one of the greatest threats of all:
DDoS attacks.

They can **cause enormous economic damage to the companies** affected and, not least, have an enormous impact on their image.

DDoS is an abbreviation for 'Distributed Denial of Service' attacks. In contrast to a DoS attack, several previously hijacked systems are used to act against the target system. **The attack consists of sending an excessive number of requests to a server, so that the target system is overloaded** and cannot respond to further requests.

Target systems are, for example, a mail server or web server of a company.

Especially in the pre-Christmas period, such a failure —even if only for a short time—is catastrophic.

All services that depend on the server are no longer or only partially available. The customer base spills over to the competition, and the internet store provider spends the Christmas season with repair work.

Victims of DDoS attacks have been mostly small stores, but even large well-known online retailers such as Amazon and Otto are not immune to such attacks.

DDoS attacks pose an increased risk, especially during special events. The BSI (German federal office for security in IT) was able to determine in its status report that **such attacks are increasingly launched during the pre-Christmas period and on Black Friday and Cyber Monday.**

The professional business with DDoS attacks

In addition to the increasing professionalism of phishing attacks, DDoS attacks are also developing continuously.
These include, for example, **technically advanced attacks that use increasingly sophisticated strategies instead of high-bandwidth ones**. In the past year, the BSI recorded an increase in reports of actively controlled attacks in which attackers reacted to the security defenses of the target server, thereby significantly intensifying the attack.

In the second half of 2019, analysts also noted **the use of so-called carpet bombing**. In this attack strategy, attackers bypass the classic protective measures at the network border so they are below the detection thresholds (in Gbit/s) and are therefore not recognized by the system. To do this, the hackers direct their attack against a large number of IP addresses within the network.

Companies are thus confronted with new, professional DDoS strategies, whereby even classic protection solutions reach their limits. Dynamic countermeasures are required to fend off such advanced attacks.

That pays off: How hackers profit with ransomware attacks

Ransomware, also known as an encryption and blackmail Trojan, is a malicious program which ensures that files are blocked for the user and only released again after payment of a ransom.
The main gateway is business-relevant e-mail communication. Ransomware is usually reloaded by other malware hidden behind attachments or URLS. If the user opens the malicious file or link, the first hurdle is overcome, and the ransomware reaches the computer. As soon as the malware becomes active, the encryption of the files begins.
Individual files on one system or even several systems within a company network can be encrypted. In order to regain access to the files, the victim has to pay a ransom. But there is no guarantee that the files will actually be returned after payment.

The damage to companies in a successful ransomware attack is enormous. In 2018, for example, attackers could capture 8 billion dollars in the USA alone. In 2019, this figure will rise to almost 24 billion dollars.

The damage caused to the companies affected is usually far greater than any ransom money paid. This results in considerable additional costs for cleaning up and restoring systems. For many companies, a successful ransomware attack also involves a loss of reputation.

Particularly in the high turnover pre-Christmas period, an increased number of attacks with ransomware is to be expected.
In order to keep the business running, there is a greater chance companies will pay a ransom –
and this fact is mercilessly exploited by cybercriminals.

New strategies for ransomware attacks

The mere encryption of files now seems to be far from enough for cybercriminals. Since 2019, a new strategy has been observed among cybercriminal gangs.

For example, **the actors behind the Maze Ransomware threatened to publish stolen files if the ransom payment of the affected company failed to materialize.** This scam gives ransomware attacks a new dimension of danger. **The affected company is thus under even greater pressure to protect the sensitive data from being published.** Internet store providers, for example, store not only personal data of their customers, such as name and address, but also often sensitive payment information, which is highly vulnerable. If this data were to be published, it would result in a huge loss of reputation and sales.

Rip-off Alert: Phishing attacks on Christmas mission

As mentioned at the beginning, phishing e-mails are a common and simple, but still very effective, type of attack. **Attackers use phishing to gain access to sensitive and personal data.**
To do this, the attackers exploit a weakness that is difficult to control: the human being.

They usually appeal to qualities such as helpfulness, fear, sense of urgency or respect for authority, and thus try to manipulate their victims.
In doing so, they **increasingly orient themselves toward current events such as discount campaigns on Black Friday.** Here, a particularly watchful eye is needed when processing e-mails, especially during this year's pre-Christmas business, where more discount campaigns are expected.

Professionalization of phishing mails

The Nigerian prince has long outlived his usefulness: **Phishing attacks are becoming increasingly professional** and are therefore difficult to distinguish from originals.
Grammatical and orthographical deficiencies are rarely found; instead, phishing e-mails are often written in grammatically correct language. Even the use of HTTPS protocols do not make it easier to unmask phishing attacks: In its IT Security 2020 status report, the BSI explains that **cybercriminals are increasingly using HTTPS links in phishing messages.**
While in November 2019, the share was still 44%, December saw a 20% increase with its pre-Christmas business. The first half of 2020 also saw increased use of HTTPS protocols in an average of 75% of phishing emails.

What do I have to consider as a company?

Basically, the security of the internal company infrastructure must be maintained throughout the year. Of course, this is not always a high priority, because IT security is not part of the core business of most companies.

This is precisely when **fully managed services are exactly the right solution.**
In view of the threat situation described above, we recommend the following five protective measures:

- **Protection from spam and malware:** An initial security barrier is created when e-mail communication is protected from spam and malware attacks.
- **Protection against phishing:** A special focus should also be placed on phishing attacks. Particular attention should be paid to links embedded in messages. URL scanning is used to examine links in e-mails and open them in a secure environment. As soon as the link is classified as suspicious by the system, the user receives a notification.
- **Protection against DDoS attacks:** Appropriate security solutions should be able to block the momentum of requests at an early stage. With regard to the use of Carpet Bombing, a fail-safe system should be implemented in case of an emergency, which can step in without interruption in the event of a server failure.
- **Protection against ransomware attacks:** Classic anti-virus filters reach their limits with sophisticated attack tactics. Appropriate security solutions should use at least one sandbox to open suspicious attachments in a secure environment and with a corresponding time delay. It is not uncommon for the malicious functions of ransomware to be activated at a later time. Some providers, such as Hornetsecurity, also offer intelligent detection mechanisms that are able to unmask targeted attacks on particularly vulnerable persons and to react to certain content patterns that indicate malicious intent.

HORNETSECURITY

As a responsible online store operator, you should also be concerned about protecting your customers:

- ☑ Give your customers information about current phishing campaigns.
- ☑ Set up a hotline for any suspicious cases your customers may report.
- ☑ Give your customers information on how to distinguish your messages from phishing messages.

As a cloud-based e-mail security provider, Hornetsecurity has holistic e-mail security services in its portfolio. With Advanced Threat Protection you can secure your e-mail traffic against phishing, ransomware and targeted attacks. You use Microsoft 365? In seconds, the 365 Total Protection Suite integrates seamlessly with your Microsoft 365 and provides 21 features to protect you holistically against cyber attacks via email.

www.hornetsecurity.com