
HACKED?
THE SURVIVAL GUIDE
TRANSPUTEC

2

The Many Varieties of Cyber Attacks

There are many different types of cyber-attacks and being able to recognise each one can be a difficult task. Despite the numerous varieties of attacks, they all share the aim of stealing an organisation's data for the hacker's own gain. Below we have listed some of the most common cyber-attacks that all organisations should be aware of:

Malware: This is an umbrella term for any software designed for criminals to cause disruption to a computer system. Viruses are one of the most common types of malware and can be used to harm, disrupt or gain unauthorised access to an organisation's data.

Ransomware: Ransomware is a cyber-attack that effectively holds your systems hostage, locking them via a malicious program (malware) until a ransom is paid to the hacker. It's generally installed remotely completely undetected and encrypts either specific files or the whole network.

Trojan: A Trojan is a variety of malware which is implemented into a programme that appears safe at first. What the victim won't realise, is that a harmful code is hidden within, which will allow the hackers to gain access to the system and gather any data available.

Spyware: Another common type of malware is spyware. Spyware can be accidentally installed when software is downloaded over the internet. It allows the hackers to monitor the victim's computer, spying on their activities and therefore learning personal details which can be used for illegal purposes.

Phishing: Phishing is another common scam used against many individuals and businesses. It involves the attacker attempting to deceive the user by directing them to a fake website which may mimic a legitimate one. This is also known as spoofing. The victim will then be asked to put in some form of personal information, usually financial details or a password, which the criminal will then be able to steal.

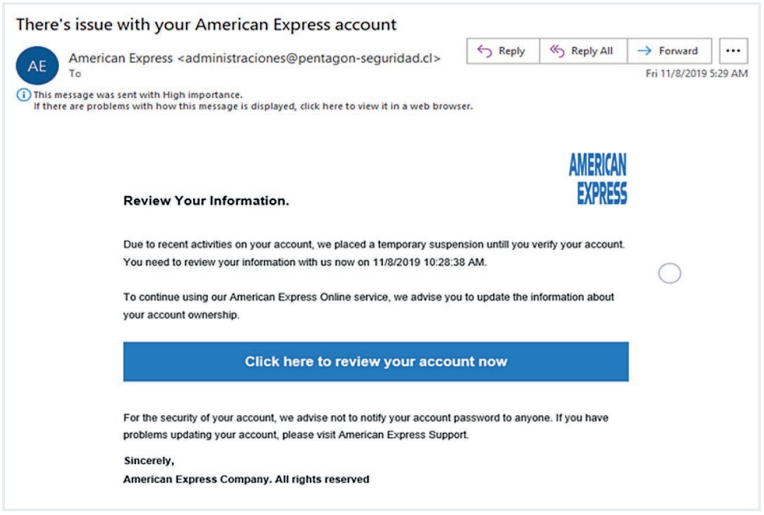
4

What Does a Phishing Scam Look Like?

Phishing attacks have always been a common form of fraud but the frequency of these scams is growing exponentially by the year, as seen in the graph using data from the Internet Crime Complaint Center.

A key reason why phishing attacks are on the rise is that they are consistently successful for hackers. They can tailor phishing scams for each target whilst remaining inconspicuous.

The most common form of phishing is email scams containing a link to a fraudulent website. These are often designed to appear urgent so that the user doesn't spend too much time studying the email or URL. Emails may claim to be from banks, online retailers or any other organisation you are associated with. The example below is a phishing email claiming to be from American Express.



There's issue with your American Express account

AE American Express <administraciones@pentagon-seguridad.cl>
To

Reply | Reply All | Forward | ...

Fri 11/8/2019 5:29 AM

This message was sent with High importance.
If there are problems with how this message is displayed, click here to view it in a web browser.

AMERICAN EXPRESS

Review Your Information.

Due to recent activities on your account, we placed a temporary suspension untill you verify your account. You need to review your information with us now on 11/8/2019 10:28:38 AM.

To continue using our American Express Online service, we advise you to update the information about your account ownership.

Click here to review your account now

For the security of your account, we advise not to notify your account password to anyone. If you have problems updating your account, please visit American Express Support.

Sincerely,
American Express Company. All rights reserved

The phishing email itself is often a means to an end. While the hacker may just use it to steal personal or financial information from the victim, they are also able to use it to install malware onto the victim's computer. This can lead to more complex issues such as ransomware or spyware which will stay on the host computer until they are dealt with.

So how do you spot a phishing email? Firstly, avoid any emails from unknown or unexpected senders and most importantly, do not click any links in emails from which you cannot verify the origin.

If you receive an email from an organisation you recognise, you should check the domain name of the sender's email address. If it does not match the name of the organisation, you should assume the email is a scam. Similarly, some criminals may use a misspelt domain name. They may swap certain letters around or replace the letter "l" with a capital "I". Always check the domain name before you interact with an unexpected email.

How Do Ransomware and Malware Attacks Start?

While phishing attacks on their own are destructive, they can often be used as a method to inflict a ransomware attack on an individual or business. Alternatively, hackers may take advantage of a fundamental flaw in a system, such as an unpatched weakness in an application or a misconfigured security, or other systems.

As previously mentioned, ransomware is a type of cyber-attack where a hacker encrypts files on a computer and demands payment for the data to be released. The really frightening thing about a ransomware attack is not only that the hacker has complete remote control over the system but that, once the malware is infiltrated, it can easily spread to other devices or applications on a connected network. This means that entire companies can be shut down in an instant and the only way to unlock them may be to bow to the demands of a criminal.

A well-known example showing the destructiveness of ransomware was the infamous WannaCry cyberattack in May 2017. In just 24 hours, the ransomware was able to infect more than 230,000 vulnerable Windows computers in more than 150 countries across the world. Although it stopped spreading after only 1 day, the total economic damage was estimated to be between hundreds of millions to as much as US$4 billion.

Ransomware attacks are not necessarily instant. They can be prepared in advance and activated at any time and hackers often lurk inside an organisation's environment for quite an extended period before they announce themselves. They normally use this time to exfiltrate critical and valuable data. Once the hackers have the data, they deploy a program that starts encrypting files on the host system so that the user has no access to their own system. Commonly, ransomware starts with files/folders with the most recent access dates. A notification will then be displayed on the screen where the hacker will list their ransom demands and often a link to a dark web link where contact and further details of their demand can be viewed.

If the victim decides to pay the ransom, the hacker should release the encryption key for the files to be restored. However, there is no guarantee that the hacker still will not use the data they had encrypted for further malicious purposes.

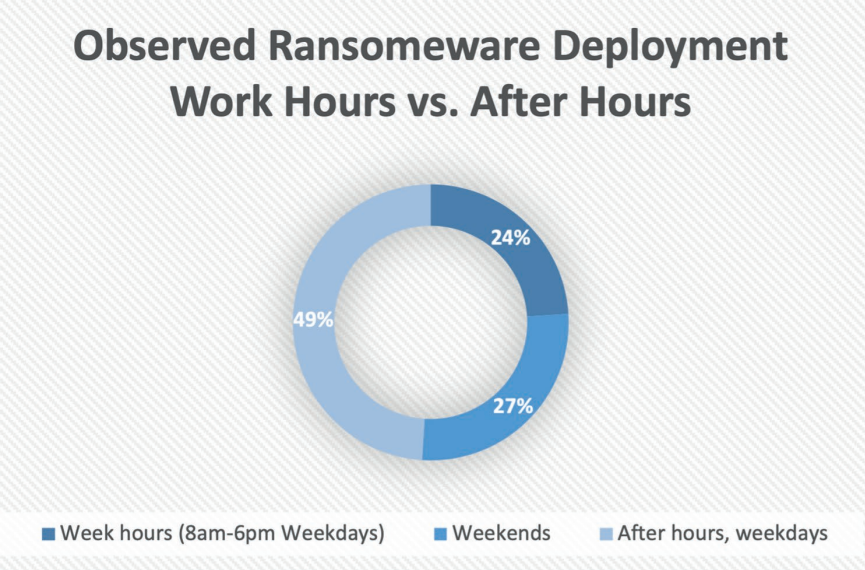
6

How Do Hackers Choose Their Victims?

The most common delivery method of a ransomware attack is via phishing emails.

Targeted attacks: Targeted attacks are used by hackers when they already have some information about their victims. They are normally small-scale attacks and are often individually tailored to selected victims. The phishing email will be from an address the victim relates to or may contain information which deceives the victim into thinking the email is legitimate. When they click the link in the email, the ransomware is deployed onto their device.

When Should You Expect Ransomware?



According to a report published by US cyber-security FireEye, only 24% of ransomware attacks happen during working hours on a weekday. Hackers much prefer to attack on weekends, national holidays or during the night on weekdays. According to research, 49% of ransomware infections occur after working hours on a weekday.

Hackers do this because the encryption of files takes time. If the hacker began encrypting during working hours, it's more likely to be picked up by internal IT teams and reduce the impact of the attack.

Over the past few years, hackers have become smarter at launching their ransomware attacks and have realised the optimal times to cause maximum disruption in an organisation. Microsoft has called these types of incidents "human-operated ransomware attacks." Since 2017, it was reported that human-operated ransomware attacks had gone up 860% worldwide.

Furthermore, cyber-security company Darktrace reported that they had recorded a 30% increase in the average number of attempted ransomware attacks globally over the holiday season from December to January, in every consecutive year from 2018 to 2020 compared to the monthly average.

They also reported a 70% average increase in attempted ransomware attacks in November and December compared to January and February. This number is expected to continue to rise over the coming years as cybersecurity threats grow.

8

Pay or Pray – Should You Pay the Ransom?

A key reason why phishing attacks are on the rise is that they are Should you give in to the hacker's demands and pay the ransom?

It might seem like the only logical option at the time and the best way to get out of the situation as quickly as possible, but there are no guarantees when you are at this point. They might ask for more money and it will only embolden them to continue committing the same crime against other victims. On top of this, this may make your organisation more prone to future attacks. The hackers now know your systems are insecure and that you are willing to pay the ransom. This may only encourage them to attack again and demand an even greater payout.

Despite the risks of paying ransoms, it can still be a viable choice for some organisations. If your organisation absolutely cannot afford downtime, such as important public services, you may have no choice but to pay the ransom to get things back to normal as quickly as possible.

Also, if the hackers have compromised and or exfiltrated critical data that would be extremely damaging to the business if it were leaked, it may be a safer option to consider paying a ransom through negotiation.

Here are some important questions to consider before deciding whether an organisation should pay the ransom:

I. When was the last time the organisation backed up their data? If your organisation has a recent, complete, backup of your data and you can recover systems quickly, paying the ransom may be avoidable.

II. Can the organisation still function? If the data encrypted was not critical to the organisation's operations, they have time to consider other options before paying the ransom.

III. Has the hacker verified they have the data? Sometimes, the hacker's threat may not be genuine and so there is no reason to give in to their demands.

Getting back your data without paying the ransom

While not an easy task, it may be possible for an organisation to overcome the ransomware and retrieve their encrypted data without submitting to the bad actor.

These are some methods that can be attempted to get data back without paying the ransom:

I. Recover the data from a backup: Although this needs to be done before an attack takes place, the most reliable way to restore the data is to retrieve the unencrypted data from a backup. Assuming that the hacker didn't manage to also encrypt the backup files.

II. Find flaws in the implementation of encryption: With enough expertise, it is possible to attack back against encryption. This could be done by identifying architectural flaws in the encryption routine, such as using a repetitive, predictable seed, or misinformation about the strength of cryptographic routines etc.

III. Contact law enforcement: Attempting to extort money using ransomware is of course a crime. Contacting the region's cybersecurity law enforcement may help to track down the criminals and obtain the encryption key to release the stolen data.

10

How & When Do You Report Fraud?

According to the UK's GDPR, you must report data breaches or fraud within 72 hours of knowing the incident occurred. Not only do you have to say this to your supervisor, but you must also report it to the proper authorities; you must release a statement to your clients.

1. Reporting fraud to authorities: Report the theft of personal documents and suspicious credit appraisals to the authorities; they'll give you a crime reference number. You'll then use this crime reference number when you call the CIFAS (UK's Fraud Prevention Service) and ask for protective registration. Once registered, CIFAS members will check to see when anyone (even you!) attempts a financial transaction, such as asking for a loan using your address.

2. Reporting the fraud to the insurance: You'll need to contact your business's insurance company and inform them of the fraud, and they'll provide experts to assist you.

3. Reporting the fraud to the subjects that are affected: The most crucial part is that you articulate what has happened/is happening with your business to the people affected. The list of those affected includes your stakeholders, employees, customers, etc. You must be completely and utterly transparent and truthful while trying to soothe panic.

CIFAS contact info:

The UK's Fraud Prevention Service
6th Floor
Lynton House
7-12 Tavistock Square
London
WC1H 9LT
www.cifas.org.uk

Cloud Computing & Cybersecurity

Advantages and Disadvantages of using data centres:

In today's world 'The Cloud' is a well-known term but if you were asked to explain what it is and how it all works, it may not be quite as easy.

For many, the concept of the Cloud is bizarre and abstract and there are many cloud computing advantages and disadvantages to get your head around, so let's break down what it actually all means and why everyone's talking about it.

Provided your business assesses the risks and configures the platform correctly so you've got eyes on everything, when inevitable threats are identified, you'll be able to locate and mitigate the risks quickly and massively reduce any impact on your business.

Advantages	Disadvantages
Affordable service rates; For businesses looking to invest in Software as a Service (SaaS), you can expect to save on your spending as their standard pay-as-you-go models mean you're not paying for anything you're not using, which results in lower costs and higher returns.	The infrastructure is owned by your cloud service provider and while this is a positive in terms of reducing the need for any internal management, it can also be a concern when your business feels too far removed and with little control. It becomes challenging to verify exactly where your data is physically stored.

<table>
<tr><th>Advantages</th><th>Disadvantages</th></tr>
<tr><td>More than 54% of public users report having captured their cost saving goals.</td><td>Looking after your data is often a shared responsibility, requiring other tools to identify when activity in the cloud seems anomalous and potentially malicious, so you can respond accordingly.</td></tr>
<tr><td>Robust and scalable ecosystem and in both directions. If your needs vary massively throughout the year, your cloud computing spend can reflect the varying demands for more efficiently than on premises solution.</td><td>Usage & Quality are based on internet connectivity at the 's end; several members struggle with quality issues because their mbps is in the lower 25% percentile of users.</td></tr>
<tr><td>Great accessibility and ease of access is such a plus for the modern workforce who, especially post-pandemic, are more spread out and remote in their business operations. Furthermore, you can collaborate not just with your internal team, but customers and other partners, globally.</td><td>The most cited barriers are security and complexity for business transformation.

Legacy infrastructure and/or application sprawl and the lack of cloud skills within the organisation can cause misalignment between IT and the business.

<table>
<tr><th>Just starting</th><th>Moderately</th><th>Heavily</th></tr>
<tr><td>Security (63%)</td><td>Security (65%)</td><td>Security (66%)</td></tr>
<tr><td>Complexity (56%)</td><td>Complexity (58%)</td><td>Complexity (53%)</td></tr>
<tr><td>Sprawl (44%)</td><td>Skills (52%)</td><td>Misalignment (47%)</td></tr>
<tr><td>Skills (41%)</td><td>Sprawl (45%)</td><td>Sprawl (45%)</td></tr>
</table>
</td></tr>
</table>

Advantages	Disadvantages
Always available - 24x7x365 with 99.95% SLA. 92% of UK mobile users own a smartphone. As long as you're connected to the internet via a device, making working on the move entirely feasible.	The main security concerns around cloud-based services are to do with misconfiguration and data breaches. Often many businesses will be unfamiliar with securing this kind of infrastructure so security oversights are very possible, leaving the business vulnerable to attack. Research has shown that 99% of misconfigurations go unnoticed too, proving even more dangerous.
Services are available 24/7 with backups; in case of emergencies or downtime, your business stays running.	Despite a common belief that attacks mostly involve cyber espionage or are state-sponsored, our research found that 42% of security incidents actually come from inside the organisation. With 65% of these internal incidents being identified as accidental or inadvertent, rather than malicious in intent, employees clearly pose a threat to their employer through day-to-day actions such as haphazardly sharing sensitive data across the internal network. The more people who have access to information the greater the risk of a leak.

Tip and Tools – How To Prepare Your Organisation's Defences

Monitor Attack Paths

An attack path is a visual representation of how a hacker could infiltrate your system showing the path of entry and all potential weaknesses that need to be addressed. Why is it important? Businesses can use attack paths to prioritise risks in their overall protection by viewing risks as an interrelated chain. Hackers are always looking at the easiest ways to exploit vulnerabilities, so it would be ideal to a) understand what paths could lead to an attack and b) review and remediate before it becomes a problem. Businesses typically use attack path analysis to model how a potential hacker would hack them. A way to ensure they're secure is to monitor them continuously and remediate them immediately.

Pen Testing

Pen Testing benefits organisations because it can identify and highlight vulnerabilities in their security. It's often called "ethical hacking", and in-house employees or third parties (like Transputec!) perform them. The test mimics strategies and actions of an actual hacker to evaluate the hackability of the company's computer systems, networks, etc. But you may be asking, why do I need to do this? Phishing and ransomware attacks are increasing and trending, putting all internet-based companies at risk. "The greater the crime, the higher the stakes."

Communication Plan

You want to have a plan in an emergency. Time is of the essence, so don't waste it. There's nothing worse than figuring out how to manage a situation such as a cyber-attack right when it happens, so having a plan is ideal. When you have a communication plan, you've carefully outlined what steps and who is needed in the execution to solve the crises. Consider employing a crisis communication team to safeguard your business and your data. Outlining their roles and assigning tasks to specific people can reduce panic and make handling the event of a crisis smoother. An emergency notification system (such as Crises Control) makes communicating with your team simple and efficient. Crises Control allows you to send critical messages to your staff, whether that be updates on the situation or an announcement that an incident has occurred. If the data breach affects people outside your organisation, like suppliers or clients, do not keep them in the dark and assign one trained person to each organisation. Consistent communication won't resolve your data breach but will save your reputation and trust.

Know thy Enemy:

5 Network Security Threats & How to Protect Yourself

I. **Misconfiguration:** These errors and misuse make up 14% of breaches. Misconfiguration occurs when configuring a system or application to be less secure.

II. **Outdated software:** Vulnerability scanners give real-time software inventory in need of updates. Keep your systems patched and updated.

III. **DoS attack:** A properly CDN (configured content delivery network) can protect your website.

IV. **Application bugs:** Penetration testing can detect vulnerabilities.

V. **Attack surface management:** Constantly watch cloud accounts and add new IP addresses as hostnames and targets.

Multi-Layer Protection and Its Advantages

Multi-layered security is an approach in network security that deploys multiple controls to protect the most vulnerable areas. The design uses to mitigate, delay, and prevent threats. Multi-layer covers areas where the most breaches and cyber-attacks occur. Each layer focuses on strengthening specific vulnerable regions or weak spots.

Multiple layers of security ensure if a layer fails because of a loophole, another layer blocks the threat. Some examples are monitoring, patch management, authentication for end users, and device configurations to ensure they run an effective antivirus and host firewall.

An advantage is that the more protection layers you have, the harder it is for hackers to infiltrate your network. Adequate layers should be able to block a hacker's ability to gain entry ultimately. Your team will be able to work at total capacity while your security features work in the background to eliminate any threats. Any emails that entered your system identified as a potential threat will go to quarantine until an authorised user verifies them as not a threat. This process results in less downtime.

Advantages Of Threat Prevention Services

Antivirus, Anti-Spyware, Vulnerability Protection, etc

The advantages of threat protection services include:

Continuous monitoring and real-time visibility,

URL detection and content filtering,

Protection against zero-day malware and vulnerabilities

Threat analyses to prioritise risks effectively and organise responses.

These services enable the organisation to better comprehend the threat landscape and anticipate what the attackers will do next. Keeping up to date with the current cyber-attack trends is crucial because you must take note and prompt action to **protect yourself and our company.**

References

https://darktrace.com/newsroom/darktrace-reports-30-more-ransomware-attacks-targeting-organizations-during-the-holiday-period-e#:~:text=Darktrace%2C%20a%20global%20leader%20in,compared%20to%20the%20monthly%20average

https://www.zdnet.com/article/most-ransomware-attacks-take-place-during-the-night-or-the-weekend/

https://www.rfwireless-world.com/Terminology/Advantages-and-Disadvantages-of-Data-Center.html

https://www.flatworldsolutions.com/IT-services/articles/advantages-disadvantages-data-center-outsourcing.php

https://www.amdhservicesltd.com/the-importance-of-multi-layered-security#:~:text=Each%20layer%20provides%20an%20additional,ability%20to%20gain%20entry%20completely.

https://www.ponemon.org/research/ponemon-library/security/the-economic-value-of-prevention-in-the-cybersecurity-lifecycle.html

https://www.accenture.com/gb-en/insights/cloud/cloud-outcomes-perspective

UK Head Office
Transputec Ltd
Transputec House
19 Heather Park Drive
Wembley, London, HA0 1SS

European Office
Transputec Ltd (Niederlassung Deutschland)
Alt-Heerdt 104
40549 Düsseldorf

Email Us
enquiries@transputec.com
support@transputec.com
europe@transputec.com

Call Us
+44 (0) 20 8584 1400 (Enquiries)
+44 (0) 20 8584 1440 (Support Desk)

TRANSPUTEC