RANSOMWARE IN A PANDEMIC

A PERFECT STORM

On Device Data Privacy

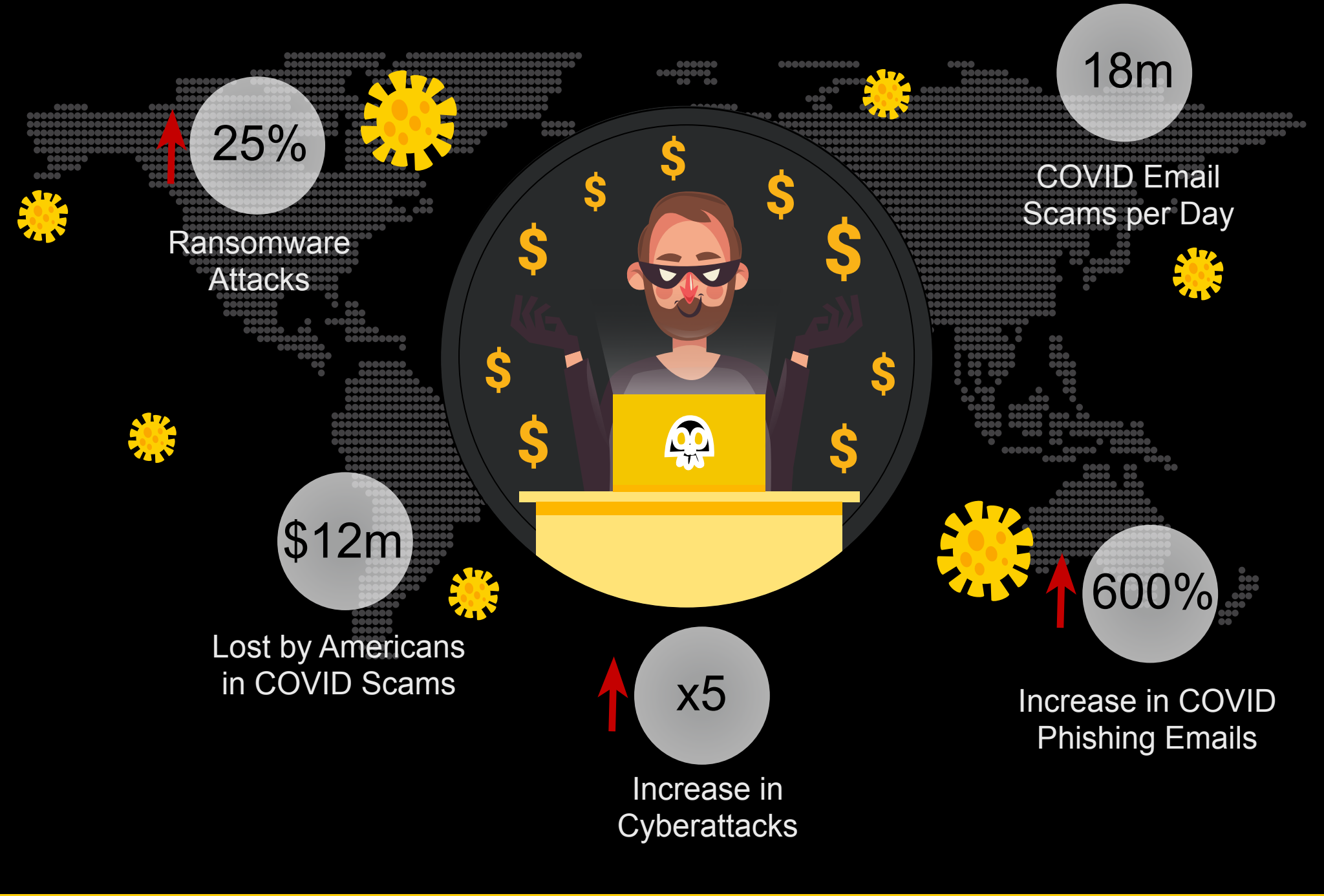
Prevent the unauthorized collection and transmission of user data on and off your network.

On Device Data Security

Ensure compliance with global privacy and data protection regulations.

Insider Threat Prevention

Protect your intellectual property and the risks associated with industrial espionage from inside your organization.



CONTENTS

Ransomware's Next Wave

COVID-19 has provided cybercriminals with a unique opportunity to take advantage of remote workers lack of preparedness and lack of security to make a lot of money.

The way we work forever changed with the onset of Coronavirus. As companies everywhere closed their doors and pivoted to a remote model with little time to prepare, the disruption of the newly dispersed workforce was creating the perfect storm for cybercriminals. Evident by the barrage of ransomware attacks thus far in 2020, and the vast number of malicious campaigns exploiting Covid-19.

Over the past several months cybercriminal rings have found success with Covid-19 themed attacks. Victims have been lured with everything from phishing emails containing Fake News around vaccines, malware hidden in free downloads for video conferencing software and malicious advertisements for commodities in short supply such as hand sanitizer. All inevitably designed to infect an organization with ransomware.

The current pandemic and rise in cyberattacks generally has seen concerns around ransomware pushed to the forefront for those responsible for an organizations data privacy and security, with recent studies showing that 96% of companies now consider ransomware to be a critical threat to their business.

Ransomware Doesn't Discriminate

Much like Covid-19, ransomware doesn't discriminate, and for cybercriminals everyone is a target. Whilst government, healthcare and educational institutions regularly hit the headlines following ransomware attacks, all organizations, regardless of sector or size must assume that they will at some point become a victim of a cyberattack.

The Rise of Remote Work

Global organizations are now being run by individuals from home offices, something which hasn't gone unnoticed by cybercriminals. Some companies of course had foundations in place to support this 'new normal' and others pivoted as quickly as possible, but most were unprepared for the momentous shift that 2020 unexpectedly brought. As with any major changes, there is inevitably some level of disruption and a period of adjustment. Office based workers scrambled to download virtual meeting apps and programs, companies hastily implemented security strategies, and all the while remote employees became targets for cybercriminals.

Ransomware Facts

Every 11s

Organizations Attacked

187m

Attacks 2019

$42k

Average Ransomware Demand

75%

Have Up-To-Date Protection

Gone Phishing

As Pandemic scams flourished cybercriminals took advantage of increased public anxiety and got creative with phishing campaigns.

Email was once the preferred way to infect victims with ransomware, but in recent years attackers moved on to other methods such as insecure public facing portals, remote ports and other vulnerabilities. However, researchers have noted a significant rise in the number of ransomware attacks once again being delivered by phishing emails during the current pandemic. Since March of this year attackers have been taking advantage of public anxiety and luring victims to click on messages promising important information about Covid-19, and while employees in their native office settings might not have been so quick to click, this level of heightened anxiety combined with the new way of working has created new ransomware opportunities for attackers.

The Weakest Link

Most cyberattacks involve some human interaction, particularly with social engineering attacks. Employees no longer have the layers of security around them that they once had when they worked in an office environment, meaning organizations must trust and rely on their employees to be extra vigilant with cybersecurity protocol. Although phishing campaigns typically contain grammatical and spelling errors, many are seen to be increasingly sophisticated and capable of deceiving even the savviest of individuals. These non-technical attacks can prey on particular individuals and dupe them into breaking standard security practice. Once successful, hackers are able to gain authorized access to confidential information. Once the damage has been done and the data has been exfiltrated, the fallout can be enough to stop a business in its tracks.

The Risks of Return to Work

Just as individuals and organizations have become accustomed to remote work, the easing of lockdown restrictions means that companies are preparing for the return of many employees. From a security perspective this should be seen as a benefit, but the reality is that organizations should be prepared for a resurgence in cyberattacks and ransomware as it's not just the remote worker returning that needs to be considered. There is a strong chance that employees have spent the past few months working from a compromised endpoint, whether corporate owned or in a BYOD scenario.

With many employees oblivious to the malware that potentially lies dormant on their device, the attackers are waiting for the right opportunity to connect to the server and wreak havoc on the organization. It's not uncommon for attackers to spend weeks or even months lurking around the network with the intention of accessing important emails from C-Level staff and sensitive company data in order to pressurize the victim even further.

Reputation is Everything

Ransomware attacks have significantly more consequences than the cost of remediation, assessment and regulatory reporting. Perhaps the most significant of all is the loss of business through reputational damage that can take years to repair.

Information technologies services giant Cognizant provides a sobering example of what can happen. The company who is one of the largest IT Managed Service Providers in the world, saw their revenues decline from $509 million to $360 million in less than one quarter after the attack, even while industry revenues were still soaring.

It certainly doesn't help that this company was in the industry of advising other companies about how to protect themselves. More recently, a subsidiary of DXC Technology, a large global MSP provider, announced that they also suffered a ransomware attack that took services offline for several hours.

Ransomware is increasingly targeting MSPs and IT service providers who often find themselves caught off guard while using traditional cybersecurity solutions that focus on the fortress approach, building moats, walls and sentries around their assets.

If attackers holding an organizations data to hostage isn't bad enough, double extortion attacks are rising in popularity. Thought to be initially adopted by the cybercriminal ring behind the Maze ransomware in 2019, they are now being used as a means to extort even more money from the victim and draw more widespread attention to the incident. A recent example is the US law firm known for representing celebrity clients. The attack made global news when private celebrity data was deliberately leaked on the Dark Web. Ransomware groups are doubling down of their blackmailing efforts and if the ransom isn't paid, organizations may find their trade secrets in the hands of competitors or their sensitive data posted online for all to see. With many private sector ransomware attacks going under the radar, this tactic will undoubtably cause concern for organizations intent on staying out of the headlines. Organizations perceived to have the most to lose from leaked data are considered most likely to pay and therefore targeted more frequently.

Data Privacy Regulations

Data privacy and protection regulations are also rising. This year we've seen new regulations come into force in Dubai, Singapore, New Zealand, South Africa and Brazil. Organizations cannot afford to ignore cyberthreats that inevitably lead to ransomware and data breaches. The implications rising from cyberattacks, especially double extortion attacks, are about much more than just data recovery. Regulatory fines, legal costs, reputational damage and loss of proprietary information can have disastrous consequences.

Prevention as a Form of Defense

Intrusion detection systems such as Firewalls and Anti-Virus solutions that remove known infections are not enough to prevent attackers from infiltrating the network, and VPN's do not prevent attacks.

Companies relying on VPN's should be aware of their limitations. Firstly, they assume that users actually turn on the VPN on their device, which is often not the case as recent reports suggest that only 46% of users actually do.

It's also important to note that VPN's don't actually prevent an attack on a device, and are still prone to the same vulnerabilities as a normal device. They can still download malware, become infected by ransomware and be subject to a data breach. From a security perspective, VPN's have become a new attack vector for cybercriminals, with several reports suggesting that hackers have been targeting VPN's from major vendors to infiltrate and plant backdoors into corporations all over the world.

More Products ≠ More Security

With the average IT department trying to manage over 57 different security tools it is not surprising that this often causes more problems than it solves. It suggests that many organizations feel that more products equate to more security, when in fact it only serves to increase complexity, management, overhead and most notably 'alert fatigue'. With so many systems working to secure multiple devices throughout an organization, IT professionals are forced to deal with an overwhelming number of security alerts. A 2019 research report found that 70% of security professionals investigate more than ten alerts every day, with 78% saying it takes more than 10 minutes to investigate each one. This becomes a major issue when organizations do not have the resources to adequality focus on the incident reporting, making such reactive approaches largely ineffective.

By taking a preventative approach to the problem, IT professionals can receive alerts that do more then tell you a problem has been identified but proactively take action to fix it. BlackFog Privacy for example, alerts IT departments that a threat was identified and blocked, enabling the IT professional to review detailed analytics of impact assessment across their entire organization.

Hackers Will Always Find a Way In

A hacker who is intent on infiltrating a device or network will eventually find a way in. The challenge is preventing an attack in the first place and ensuring attackers or insider threats cannot remove data from the device, eliminating data breaches all together.

Preventing cyberattacks and data breaches can be effectively managed using a multi-layered approach involving a combination of defensive and preventative techniques. Monitoring data exfiltration provides a unique approach to data security, unauthorized data profiling and data collection. Tools that monitor the flow of outbound traffic and stop attacks in real-time will ensure that no unauthorized data falls into the wrong hands.

This new approach together with the right tools, will help CISO's and their security teams out manoeuvre cybercriminals and malicious insider threats. Preventing them from becoming the next statistic and a data breach headline.

BLACKFOG™

Privacy. Security. Prevention.

Threat Prevention

Data Privacy

Data Security

Aragon Research

2020 HOT VENDOR