RESTECH SOLUTIONS

# ResTech Solutions

## Managed IT Services

# Cybersecurity Threats 2021

**In this report, we will explain the realities of cyberattacks on the financial sector.**

# **Size** Doesn't Matter

**In 2020, 28% of breaches involved small business victims, according to the Verizon 2020 Data Breach Investigations Report.**

# WHAT IS **RANSOMWARE**

Ransomware is a type of malware that infects your computer network and other devices. Once infected, your data is locked and encrypted, making it unusable and inaccessible until a ransom payment is received.

While a majority of ransomware encrypts data on the victim's server until the ransom is paid, we have observed an increase in double-extortion methods that take it a step further by copying the stolen data to a cyber criminal's server.

This means, even if a ransom is paid, the victim's data has already been exposed and will likely be exploited or sold illegally on the dark web. Therefore, backing up data is not enough for businesses to mitigate the threat.

It is critical that business leaders begin taking a proactive approach to prevent these attacks from compromising, releasing, and destroying sensitive data.

## HOW DO USERS GET **RANSOMWARE?**

There are a number of ways in which ransomware is spread, including malicious email attachments and URLs. A file can be delivered in a variety of formats including Word documents, Excel spreadsheets, PDFs, zip files, and more. When a user clicks on a malicious link or file, ransomware can immediately deploy or remain dormant for days, weeks, or even months before encrypting a victim's files.

While you may think it's easy to spot a malicious email, cybercrimals are becoming more sophisticated and often conduct extensive research on their target. As a result, ransomware groups are able to deceive users with very credible and believable emails.

If you are interested in learning more about the common ways in which ransomware is spread, please continue reading on page #5.

# In 2021...
# Ransomware is targeting the financial sector

**On July 10th 2020, the SEC issued a warning about a rise in ransomware attacks on U.S. financial firms. This trend is continuing into 2021, therefore institutions need to keep ransomware on their radar. These attacks pose a major threat because organizations are dealing with destructive ransomware designed to cause maximum damage. Additionally, this puts even more pressure on financial services companies because consumer mistrust ultimately leads to users taking their business elsewhere.**

## Squar Milner

Squar Milner is one of the largest accounting firms in the United States offering wealth management, auditing, tax services, CFO advisory, and bankruptcy services. On March 25, 2020, the firm experienced inexplicable technical difficulties which led them to discover a data breach affecting their clients.

The information possibly accessed by the hackers includes full names, addresses, social security numbers, Tax ID numbers, IRS filing information, and state tax submissions. Squar Milner is now covering the costs of 12 months of credit monitoring, dark web monitoring, and identity recovery services for the exposed individuals.

## Advantage and Argus Capital Funding

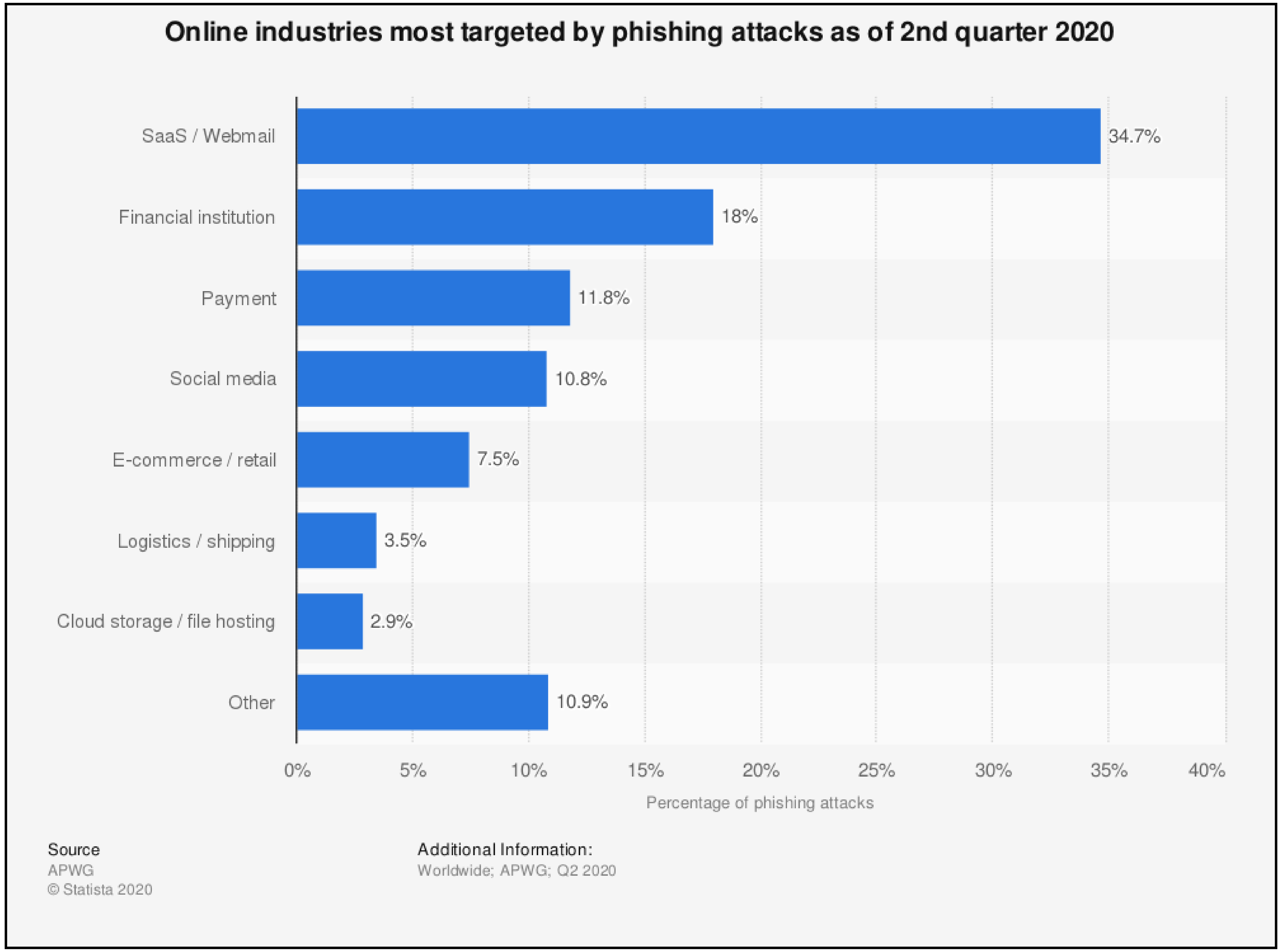
On December 24, 2019, researchers discovered a data breach from Advantage and Argus Capital Funding, a NY-based private equity firm, which included 425GB of 500,000 legal and financial documents, including tax returns and social security information.

The breach was discovered by vpnMentor who claim data including credit reports, bank statements, tax returns and social security information could be accessed without authentication. The database was linked to MCA Wizard, an application developed by Advantage and Argus Capital Funding.

## US, Canadian, Australian Banks Hit By Banking Trojan

On March 30, researchers reported that U.S., Canadian, and Australian banks were being increasingly targeted by Zeus Sphinx, a banking trojan that had been dormant for three years. The attackers target those waiting on government relief payments from Covid-19.

Zeus Sphinx gained notoriety in 2015 for targeting major financial institutions in the UK, and eventually in Brazil, Australia and North America. This version of the malware underwent core changes in its persistence mechanism, injections tactics, and bot configuration.



**Online industries most targeted by phishing attacks as of 2nd quarter 2020**

Source
APWG
© Statista 2020

Additional Information:
Worldwide; APWG; Q2 2020

# Types of Malware

**Malware is a piece of malicious software desgined by cybercriminals to steal your data and carry out other nefarious behaviors. Malware can be spread in many ways, including phishing, malicious URLs, downloads, browser extensions, and more.**

## Ransomware

Ransomware is a type of malware that infects your computer network and other devices. Once infected, your data is locked and encrypted, making it unusable and inaccessible until a ransom payment is received.

## Virus

A Virus is another form of malware that, when executed, replicates itself by modifying other computer programs and inserting its own code.

## Worms

Like viruses, worms replicate in order to spread to other computers over a network. In the process, they cause harm by detroying files and data.

## Trojan

A Trojan is a form of malware that can be used to steal financial information or install ransomware. This is one of the most dangerous forms of malware, as it is often disguised as legitimate software.

## Keylogger

This malware records all of the keystrokes on your keyboard. This sends all of your sensitive information, including credit cards, passwords and other user credientials to a cybercriminal.

## Spyware

Spyware is malicious software designed to enter your device, gather your information, and forward it to a third-party without your consent. This software is used to profit from stolen data.

# The Cost of **Falling Victim**

Ransomware attacks are constantly making news headlines. However, the stories you hear often focus on large enterprise organizations. Today, cybercriminals frequently target small to medium-sized organizations, which are often more vulnerable to these attacks. Additionally, ransomware attacks can destroy a business as a result of the financial burden inflicted from direct and indirect damage. In addition to the ransom payout, you must factor in downtime, reputational damage, data loss, and other repercussions that may follow.

## 2020 **Average**

In 2020, the average ransom demand for SMBs was about $233,817. However, this does not factor in the downtime and damages that follow. The average cost of downtime in 2020 for SMBs was $274,200 which is nearly six times higher than it was in 2018 at $46,800.

## Compromised **Data**

On the dark web, the average cost of banking credentials and credit card details is about $35. Victims who have their banking records compromised are often left grappling with the effects years later.

## Recovery **Time**

As of January 2021, the average numer of days a ransomware incident lasts is now 19 days. This is a result of the time needed to remediate and restore systems after an attack.

# How ThreatLocker **Protects Your Business**

Small to medium-sized businesses are constantly buying into the latest technologies such as next-gen antivirus software and threat detection solutions that use machine learning, artificial intelligence, advanced heuristics, blockchain, and more.

However, none of these solutions protect against the latest cyber threats, including ransomware and other forms of malware. Millions of dollars are spent on cybersecurity annually, yet companies that rely on threat detection are still getting compromised.

Most cybersecurity protections are based on looking for, finding, and stopping threats. The problem is, cybercriminals are getting smarter and entering networks undetected.

End-users are constantly inviting threats through actions such as downloading various applications without ResTech Solutions' approval, clicking on links they shouldn’t, and opening attachments in e-mails.

That’s why a new approach of blocking everything that is not trusted and only allowing those applications that are approved, is a far cleaner and more comprehensive approach to ensuring malware does not end up on your networks.

ThreatLocker combines Application Whitelisting with Ringfencing and Storage Control in ways that make security simple. By combining these three techniques, your applications will not be exploited.

# What is **Application Whitelisting?**

Application Whitelisting is the gold standard in protecting against ransomware, viruses, and other malicious software. The ThreatLocker solution implements a default-deny approach, which means all applications are blocked unless they are on the whitelist.

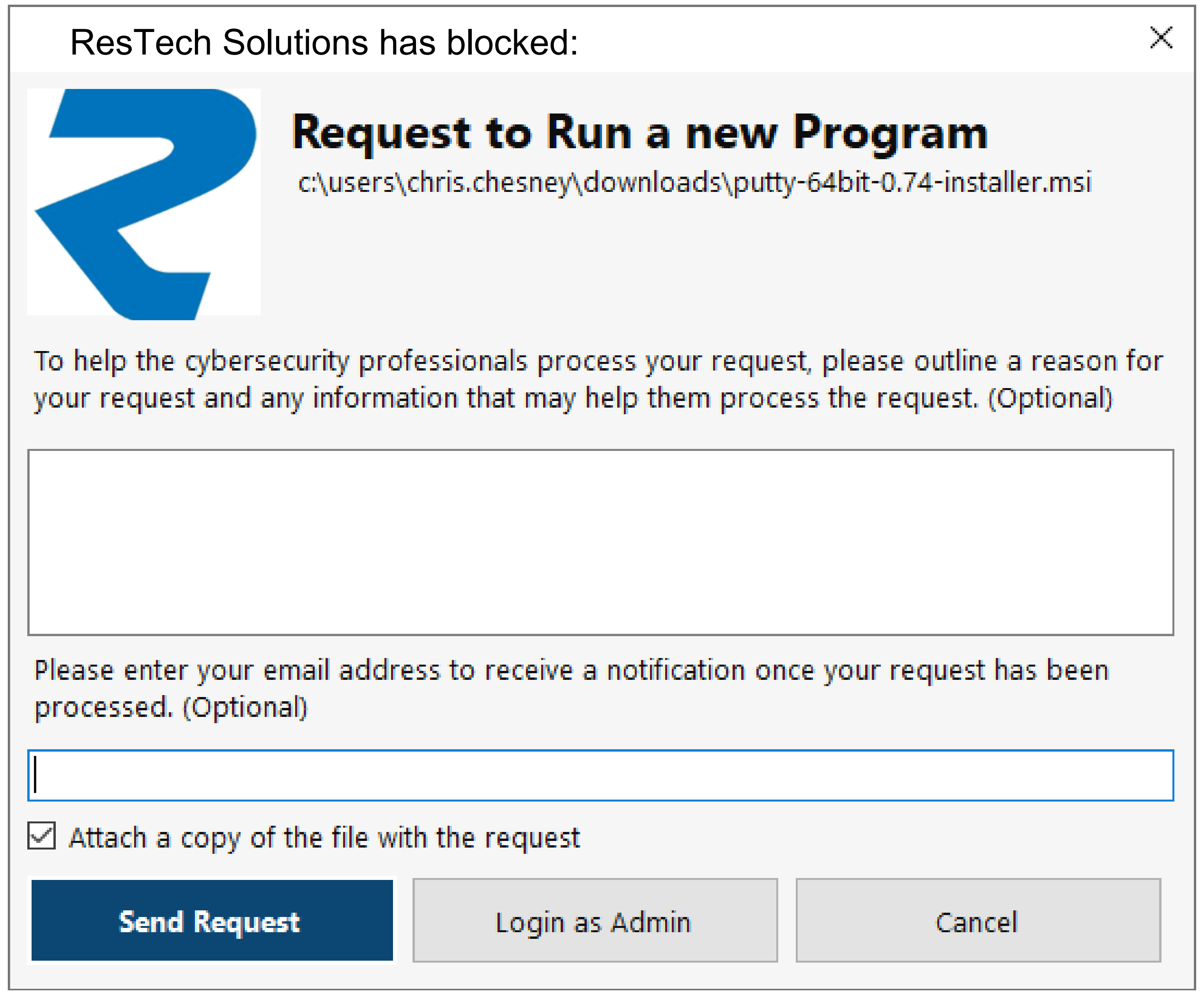
Traditionally, businesses have relied on antivirus to protect their business. The problem is, antivirus software only attempts to block the bad stuff and oftentimes, it fails.

Antivirus relies on existing signatures and known behavior. As a result, it cannot distinguish between malware and a legitimate piece of software like Dropbox.

In the past, application whitelisting was too complex to manage and maintain for non-enterprise businesses. ThreatLocker has addressed this issue head-on, making the solution feasbile for SMBs.

The ThreatLocker solution combines advanced software and service, allowing ResTech Solutions to deploy application whitelisting in a few hours.

The ThreatLocker 24-hour operations center continuously monitors for application and operating system updates, so ResTech Solutions does not have to worry about adding a new file to the application whitelist every time Microsoft, Google, or another vendor releases an update.



ResTech Solutions has blocked:

**Request to Run a new Program**

c:\users\chris.chesney\downloads\putty-64bit-0.74-installer.msi

To help the cybersecurity professionals process your request, please outline a reason for your request and any information that may help them process the request. (Optional)

Please enter your email address to receive a notification once your request has been processed. (Optional)

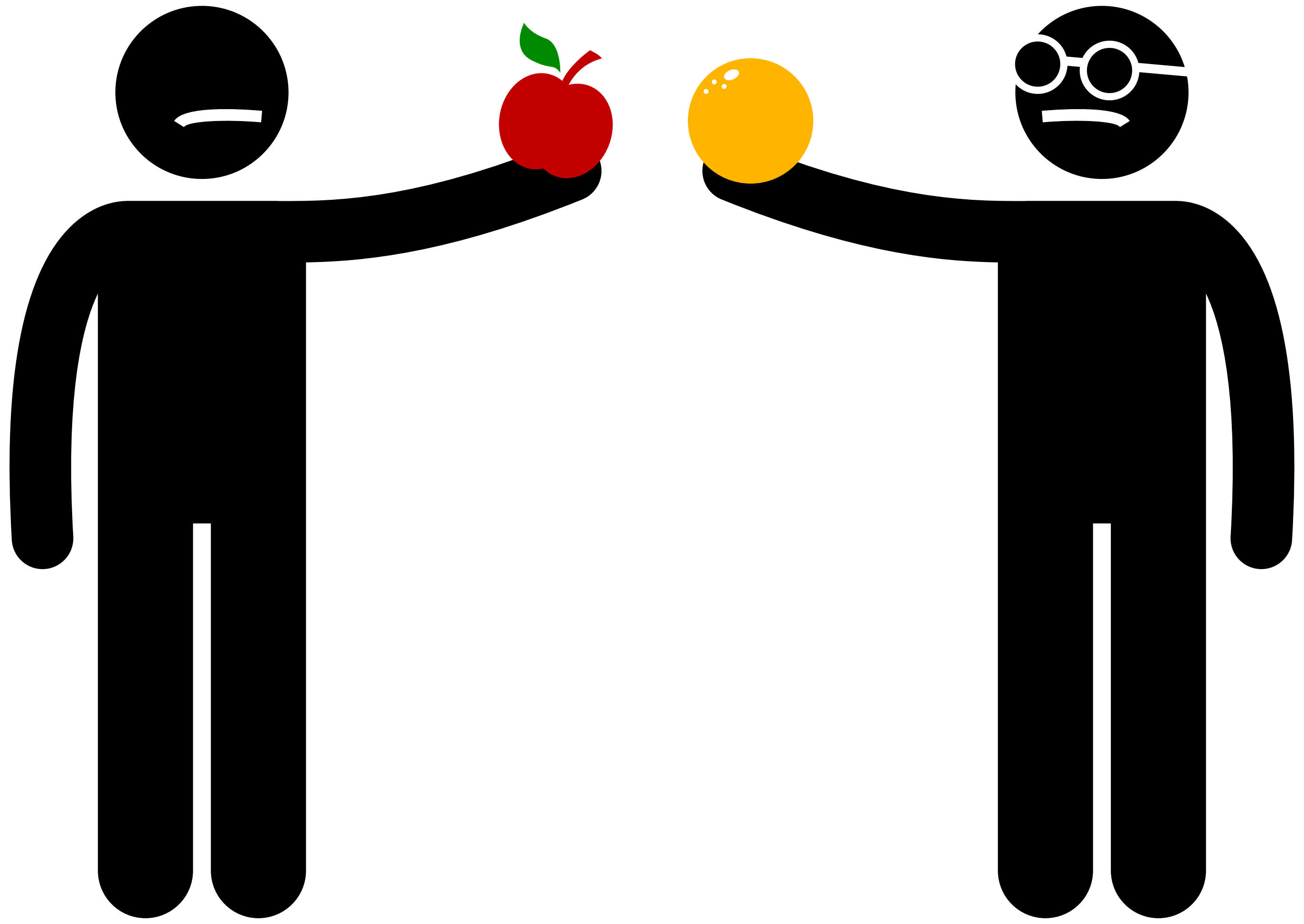
☑ Attach a copy of the file with the request

The approval center allows ResTech Solutions to easily control what is permitted to run on your computer with a 30-second single click approval.

Users have the ability to request permission or ignore notifications for unapproved applications.

# ThreatLocker Vs.
# **Alternative Whitelisting Solutions**

**Whitelisting blocks all untrusted applications, however, it will not stop an attacker from weaponizing tools and applications against you. ThreatLocker's propriety Ringfencing solution goes beyond blocking untrusted applications. Continue reading to learn more.**



# What is **Ringfencing?**

ThreatLocker's proprietary Ringfencing solution enables your IT team to go beyond permitting what software can run and control how applications can behave after they have been opened.

This solution adds controlled, firewall-like boundaries around your applications, stopping them from interacting with other applications, accessing network resources, registry keys, and even your files.

This approach is extremely effective at stopping fileless malware and exploits, and makes sure software does not step out of its lane and steal your data.

For example,  earlier this year, a vulnerability was discovered in Zoom, putting millions of users at risk of a cyber attack.  If you aren't familiar with this tool, it is one of the leading video conferencing software applications on the market, which many have grown accustomed to over the last few months.

By using Ringfencing,  you can stop applications like Zoom from accessing your files and launching other applications that could be used against you - even if it isn't on your whitelist, even it's a trusted application, and even if it's malware.

Whitelisting blocks all untrusted applications, however, it will not stop an attacker from weaponizing tools and applications against you. That's why Ringfencing is critical when blocking these attacks.

We highly recommend you combine Ringfencing with Whitelisting. By combining these techniques, untrusted applications are not going to be permitted, regardless of how the payload is delivered to you.

# Vulnerable Applications are the #1 Cause of Security Breaches

*Verizon Data Breach Investigation Report, 2020

Attacks against web applications are now the fastest-growing category. At ResTech Solutions, protecting your applications from ransomware and other malicious threats is one of our top security concerns.

# What is Storage Control?

It is critical that you configure file shares, USB devices, and other policies to restrict access to files not only at the user level but also at the application level.

With ThreatLocker, you can control device access down to the most granular level, including file type, user or group, application, and serial number - regardless of whether or not the device has been encrypted.

ThreatLocker not only protects you from USB drives, it protects all of your files, including those on your local hard drives and file servers.

# ResTech Solutions
## Your Trusted IT Provider

**At ResTech Solutions, we understand that as technology evolves, so do opportunities to evolve your business. In order to ensure your business evolves and thrives in today’s world, we are always a few steps ahead, making security recommendations to fit your needs and mitigate the latest cyber threats. You can rest easy when you put your IT support needs in our hands.**

RESTECH

SOLUTIONS

- https://restech.solutions
- 713-936-6855
- info@restech.solutions