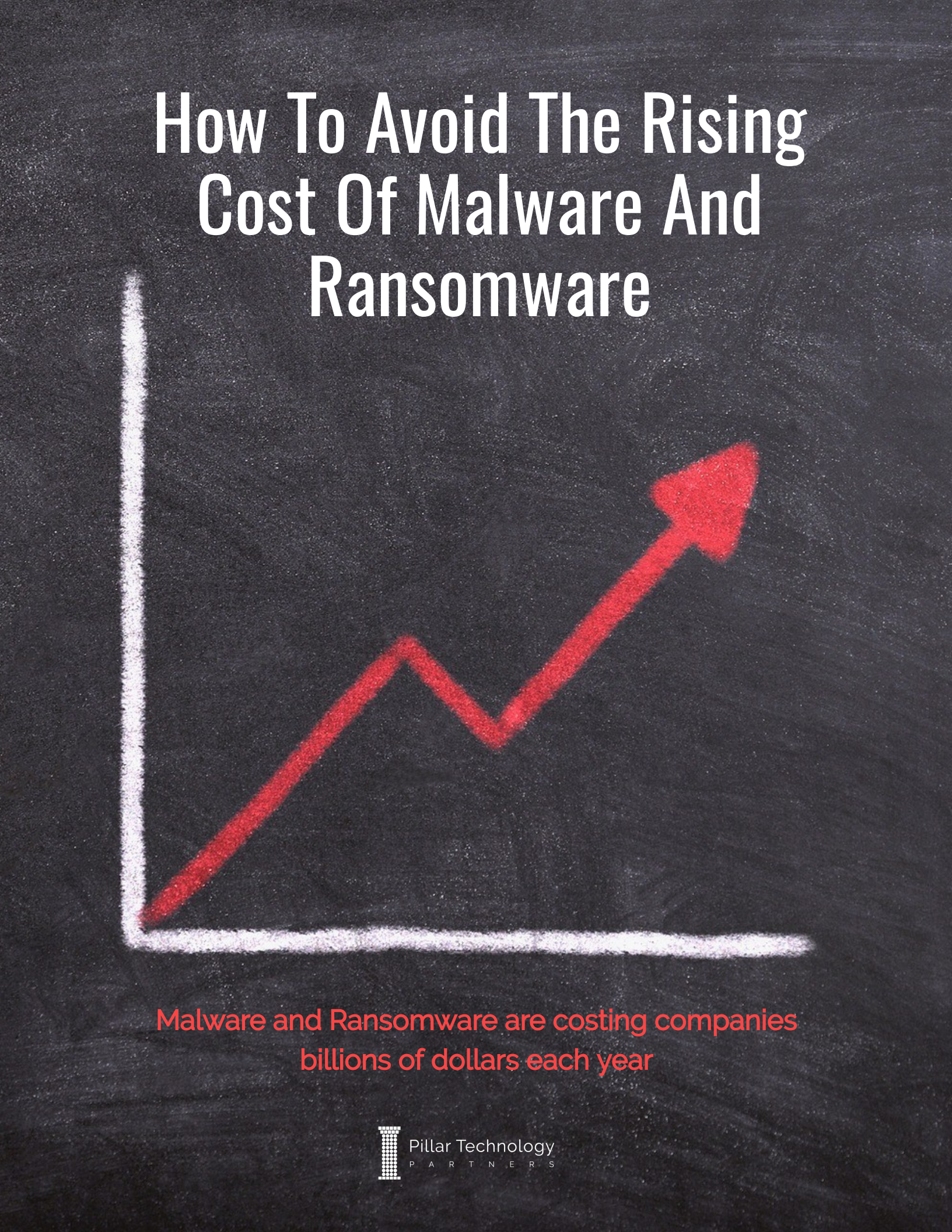
How To Avoid The Rising Cost Of Malware And Ransomware



Malware and Ransomware are costing companies billions of dollars each year

Pillar Technology
PARTNERS

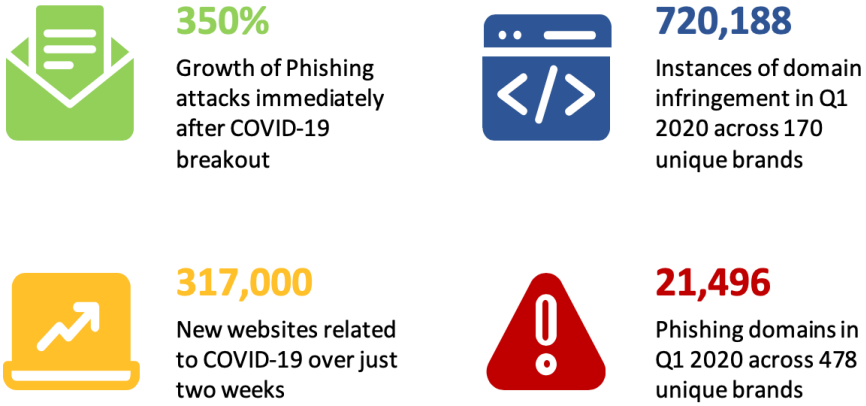
The Realities of Malware & Ransomware

Currently, the largest and potentially most impactful cyber threat is malware and ransomware. Persistent attacks from both nation state organizations as well as criminal organizations have been on the rise the past few months, and these attacks are wreaking havoc on many organizations worldwide.

Just this week, Honda manufacturing was paralyzed by a ransomware attack and was forced to suspended production of automobiles and motorcycles at several manufacturing plants around the globe. As reported by The Telegraph, Honda has been infected by EKANS malware which was designed specifically to shut down the computer systems that run heavy machinery in factories. Honda stated, "Teams from IT globally and across the NA Region are working continuously to contain this attack and restore normal business operation as quickly as possible, however many business processes that rely on information systems are impacted."

During this time of COVID, we have seen a significant increase in attacks on hospitals, health care providers and aid groups, but unfortunately, they are not the only ones being attacked. In these times where business operations are somewhat fractured and shifted to working from home, the threat surface for attacks has increased exponentially, yet most organization have not been able to retool or increase monitoring resources to meet increased threats.

A recent report from RiskIQ reports:



RiskIQ Analysis of an Attack Surface: Five Ways Hackers Are Targeting Organizations

Malware is heavily dependent upon human error. Nearly 90% of successful attacks are the result of email phishing campaigns. Effective security awareness training and a comprehensive InfoSec communications program are required to minimize these attacks. Provide employees with examples of current phishing schemes, so they know what to look for and never take the bait, clicking on a link or downloading a file they cannot confirm is legitimate. Employees should receive regular communications regarding current, known phishing campaigns and cyber threats and know who to call when questions arise. Employees need to be on alert and understand the implications of becoming a victim - compromising corporate assets and risking financial and brand loss for the organization. Having open lines of communication with employees and establishing a culture of "Healthy Paranoia" is key.

When attempting to prevent malware and ransomware breaches it is important to understand the fundamentals of how they work and how systems are infected.

- Viruses are most commonly downloaded by employees via phishing emails. Once downloaded a virus is active when a file is opened or edited. Similar to a biological virus, computer viruses spread as more files are opened.
- Worms are considered especially dangerous because they do not necessarily require a click, but rather can take advantage of existing weaknesses in software. Any software vulnerability will remain until the software is updated. Worms can also be distributed through email or even IM messages. Once the worm has found its way in, it can delete files, replicate and eat up hard drive space and bandwidth, steal data or even install a back door to give hackers access to your system and its settings.
- Trojans are similar to worms but requires running a program. As the name suggests phishing schemes with trojans often appear as non-threatening or even helpful. Unlike a worm, once the end-user runs a trojan script it is very difficult to stop and results in great destruction to an entire network of connected devices.
- Ransomware is most commonly distributed via phishing or spear phishing emails. The important distinction here is the function of the malware after you are compromised. Once a device is infected, ransomware encrypts your data and the bad actor then requests payment for return of data. If properly prepared you can recover your data from a secure backup. If not, you can attempt to solve the encryption which requires significant computing resources or special software and typically is not successful unless you engage highly specialized experts that have deep experience in cryptography.

- Spyware/Adware are often considered less dangerous to users' software, but still can be very compromising at an enterprise-level if you have confidential information on your device. Spyware and adware infect using similar methods, typically when someone clicks on an ad or link. Once on a computer, they have the ability to log keystrokes or view your screen allowing for bad actors to get passwords or information required to implement a more overarching and nefarious plan.
- Fileless Malware often takes advantage of tools which already exist on a user's workstation but may not have been properly secured. This could be operating system tools, such as Microsoft Powershell. These tools execute in memory which allows the attack to execute scripts on the computer and take control of services without being detected by traditional, signature-based anti-malware ☆ solutions. These attacks are generally activated when a user clicks on a link in a phishing email.

But don't be dismayed. Practicing good cyber hygiene, combined with cyber tools which are configured properly will significantly reduce risk of becoming a victim to malware or ransomware attacks.

Identifying & avoiding an attack

Good hygiene and security awareness training are vital to preventing attacks. Good hygiene involves making sure that operating systems and applications are patched and current, practicing good information security behaviors like not clicking links and effective password management.

Good security training and awareness programs teach and reinforce the risk level of phishing attacks and employees' ongoing role in prevention. Simple one-time-only training exercises fall short of the reinforcement required to build a culture of "Healthy Paranoia". When your employees understand how they are targeted, learn how to recognize phishing attacks and have a clearly defined process for how to handle phishing attacks, the risk of becoming a victim decreases substantially. Remember, nearly 90% of successful attacks are the result of email phishing campaigns.

In addition to practicing good hygiene and implementing consistent training programs, Anti-virus / Anti-malware tools are a critical component. Traditional AV tools counted on signature matching to identify an attack. While this is still a valid approach for "known" threats, many of today's threats are "zero-day" attacks which are new variants or new attack methods and have no signature. Fileless malware can also bypass these because they operate in memory only and look like a normal request. To combat these types of threats, it is important to implement next-generation tools that can address these gaps.

When building a successful security architecture, it is necessary to create a **"Defense-in-depth"** architecture that utilizes a combination of tools to address the threats at different stages of the attack. Starting on the outside of your network you can implement tools like *Mimecast's Email Security with Targeted Threat Protection*. This will eliminate many of the threats before they reach your users by filtering malicious emails. Advanced tools like *Area1's anti-phishing tool* leverages Artificial intelligence to identify and block phishing attacks that are targeting your users. Another tool that can be deployed in your architecture is *FileWall by ODIX*. This tool is a Content Disarmament and Reconstruction tool that identifies malicious files and removes the harmful components. Endpoints present a unique challenge because they are where the user works and are many times the most vulnerable. Deploying tools like *Sophos Intecept X Advanced* which utilizes a combination of signature and Artificial Intelligence to identify and stop these types of attacks on both existing and new attacks. In addition to these types of tools in your "*Defense-in-Depth*" architecture, engaging an effective MDR Vendor (Managed Detection and Response) like *RampartMDR*, who can be your first line of defense when something occurs and proactively block attacks.

Recovering from an attack

Even with a great "Defense-in-Depth" architecture and an effective training program it is still possible to be attacked. If an attack happens it is vital that you react quickly and efficiently. The first step is to isolate the infected machine. This will minimize the attack's spread. If it has infected multiple workstations, then you should isolate all involved up to and including blocking inbound and outbound Internet access.

Once you have successfully isolated the attack, the next step is investigation.

- What happened?
- How did it happen?
- What type of attack was it?
- What is the damage?
- Was there a resulting data breach?

At this point you may need to engage external forensics assistance, law enforcement and your cyber insurance carrier. You should clearly document the steps taken and develop a timeline of the attack. This will be helpful after the attack when you conduct a "lessons learned" session. Remediation of the attack's damage can be the longest part of the response efforts. It may involve rebuilding of workstations and servers, restoring of data and notifying external parties of a breach.

If you have been attacked by ransomware. The FBI and the US Secret Service both recommend you should NOT pay the ransom. Paying the ransom does not guarantee that the criminal will unencrypt your files. They may raise the fee, and they could attack you again because you paid.

There are really 3 methods to recovery from a ransomware attack:

1. The first method is to restore from your backup (if it was not involved in the attack). An effective backup strategy could be the difference between a complete loss and a quick recovery. You should always back up files using the 3-2-1 rule. This will avoid data loss in case of a ransomware attack and make recovery possible. It involves creating three backups in two different formats and storing one copy offsite.
2. The second method is to engage our Ransomware Response team. Pillar Technology Partners works with our partner, ***Unit221B***. This team has deep expertise and experience in cryptography and ransomware. They can attempt to decrypt your files and remove the ransomware threat.
3. The final method is the least attractive, requires the most effort and still does not restore normal operations. This involves rebuilding all of the affected workstations and servers and recreating the data, (where possible).

As you can see, when dealing with malware and ransomware *"An ounce of prevention is worth a pound of cure". If you are trying to solve any of these issues and would like to discuss how Pillar Technology Partners and our partners can help you, please contact us.*