ThreatLocker® E-book

Best Practices for Common Cybersecurity Threats

THREATLOCKER

Contents

3 Introduction

4 Phishing

5 Malware

6 Ransomware

7 Man-in-the-Middle Attacks

8 Password Attack

9 Zero-Day Vulnerability

10 Rootkits

11 Internet of Things Attacks

12 Final Thoughts

Introduction

It has never been as easy for organizations to fall victim to a cyber attack as it has been in the past few years. Threat actors are continuously becoming more creative with their malicious plans of attack, putting everyone at risk at all times.

Criminal cyber activity has become a growing threat for as long as the internet has been around, targeting everyone from select individuals to leading corporations to federal governments. That is why it is essential for everyone, including employees, executives, and small business owners, to understand how to identify and respond to the most common cybersecurity threats on the internet.

In this eBook, you will find a number of cyber threats that are currently active with the full intention of causing irreversible harm to your organization or trying to extort money. Following each featured threat, is a ThreatLocker® solution that provides a proactive defense to stop threats in their tracks before they can disrupt your operations, as well as what each product can do if a cyber attack has already breached your organization's endpoints or network.

CHAPTER 01

Phishing

Phishing is a social engineering attack in which a user is contacted by email, telephone (vishing), or text message (smishing), impersonating reputable companies or individuals. Phishing attacks cause more than 30% of all data breach incidents worldwide and aim to mislead employees into revealing sensitive information such as personally identifiable information (PII), passwords, or even banking and credit card details.

Phishing attacks are often used as vessels for threat actors to get malicious software, code, and scripts onto your device. Through phishing, threat actors may also attempt to access essential accounts, resulting in a loss of trust between clients, reputational damage, and potentially a financial loss. As an extra layer of protection, it is recommended to provide your staff with cybersecurity and phishing awareness training to understand how to identify and react to possible scams or phishing attempts. Multi Factor Authentication (MFA) also provides a crucial layer of protection against these types of attacks.

BEST PRACTICES

- ✓ Provide your staff with cybersecurity and phishing awareness training
- ✓ Implement multi factor authentication as an additional layer of protection

THREATLOCKER® SOLUTION

If a phishing attempt breaches your organization because a user opens a malicious link, ThreatLocker's Ringfencing™ policies can stop applications the link opened, like Google Chrome, from communicating with weaponizable windows components like Command Prompt or PowerShell, rendering them incapable of following through with malicious intentions.

Neal Juern, President and CEO of Juern Technology, had not yet implemented a zero trust security approach until a client's user opened a Word Macro file which launched TrickBot. After over a week of downtime while Juern Technology worked to restore and save files, Juern realized "There are too many threats that anti-virus solutions and EDRs can't stop."

It was after Juern implemented ThreatLocker's solution platform that he found ThreatLocker® has helped his organization not to mostly rely on security awareness because "The end employee who's working on the computer just doesn't have as much control. They can't do as much damage as they used to be able to."

30%

Of all data breaches are caused from phishing attacks.

–The Ultimate List of Cyber Attack Stats (2022), Exploding Topics

CHAPTER 02

Malware

Every day, there are over 500,000 new pieces of Malicious software, or malware, detected. Malware is an umbrella term for viruses, worms, trojans, and other harmful computer programs used by hackers to disrupt a server or computer network. The most frequent cause for malware is phishing, making up 92% of all malware attack origins, which usually occurs when a user opens a malicious link, file, or script. In addition, malware can result from downloading malicious code or instructions from the internet. Malware may be used to leak private information, gain unauthorized access, or deny users access to important files. By implementing an e-mail filtering and protection system to reduce the number of phishing attempts that reach your mailbox, you can better protect your organization from malicious scams and phishing attempts.

92%

Of malware attacks stem from phishing scams.

–2022 Cyber Security Stats, PurpleSec

THREATLOCKER® SOLUTION

ThreatLocker's Allowlisting solution blocks all unapproved software including malware from executing. If your administrative team has not approved an application, code, or scripted set of instructions with ThreatLocker's Allowlisting, the malware will not be allowed to execute and harm your organization.

Allowlisting makes managing and controlling what runs on the endpoints of your organization easy, presenting itself as a strong solution for both enterprises and MSPs. As Joseph Undis, Senior Cloud Engineer at TechCon Consulting, Inc., put it, “ThreatLocker® completely replaces the need for Applocker in an environment, which is something that can really only be properly managed at the enterprise level. The SMB/MSP space needs better-centralized control and automatically updating policies for fewer management hours, and ThreatLocker provides both well.”

BEST PRACTICES

- ✓ Implement an e-mail filtering and protection system to reduce the number of phishing attempts that reach your mailbox

CHAPTER 03

Ransomware

Ransomware is malicious software designed to encrypt files on a device, denying you access and rendering your files and the systems that rely on them unusable. Its code instructs it to explore your system and network and search for all your data and files. When found, the ransomware encrypts them, locking them away behind a wall of elaborate code.

As the name implies, hackers demand that you or your organization pay a ransom to recover your data from its encryption. Upon paying the ransom, you would receive a key to decrypt whatever code is keeping you out of your data. It is not guaranteed that hackers will return access to your data even if you pay.

In the past three years (2019 to 2022) ransomware has grown 466%. Users should be trained to never open an attachment or link from an untrusted source, regularly filter mail content, and organizations should implement a zero trust security posture.

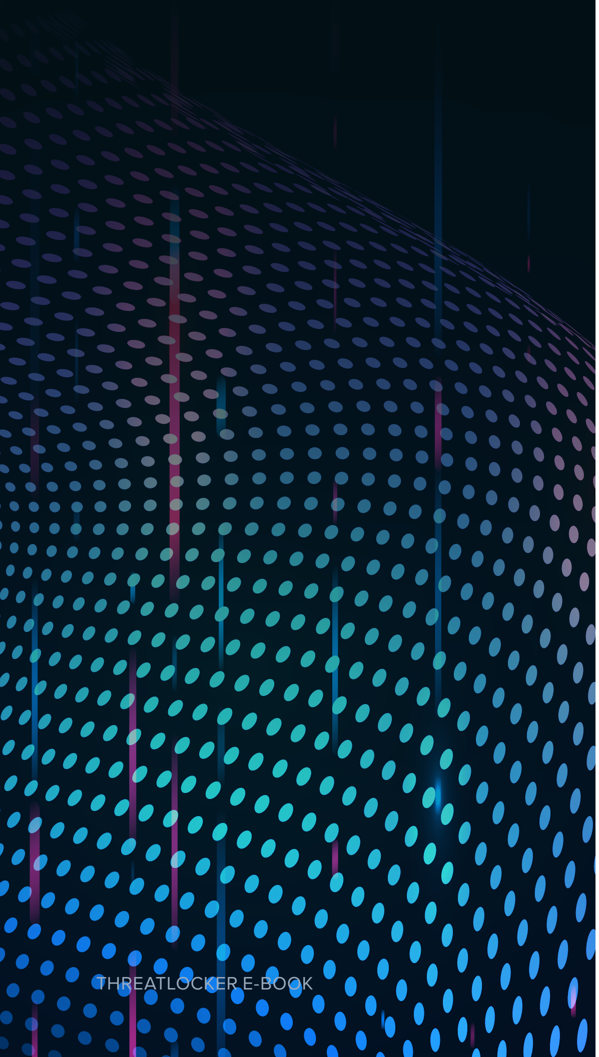
THREATLOCKER® SOLUTION

ThreatLocker's Allowlisting solution blocks all unapproved software including ransomware from executing. This solution stops ransomware from executing and encrypting your data, thus rendering it powerless.

During ThreatLocker’s live demonstration of “what happens when ransomware runs in a zero trust environment,” Zachary Kinder, President of Net-Tech Consulting, LLC, recalled having clients that were hit by ransomware. Kinder stated that upon meeting Danny Jenkins and the ThreatLocker® team, “It was kind of a light bulb moment for us” and “We protect over 1,000 endpoints, and for us, it helps us sleep at night.”

BEST PRACTICES

- ✓ Never open an attachment or link from an untrusted source
- ✓ Regularly filter mail content
- ✓ Implement a zero trust security posture



CHAPTER 04

Man-in-the-Middle Attacks

A man-in-the-middle (MitM) attack occurs when attackers eavesdrop by inserting themselves in the middle of an existing conversation or data transfer, pretending to be the legitimate parties. While this happens, the victims are deceived into sharing essential data, completely unaware of the false party.

MitM attacks allow a cybercriminal to intercept correspondence from different parties while distributing malicious links to unsuspecting, legitimate parties. These wiretapping cyber attacks are, more often than not, challenging to detect. However, you can take preventative measures by educating your employees.

Business email compromise (BEC) attacks, a form of MitM attacks, was the second most common cyber attack in North America in 2021 at 12% of total attacks, and are most commonly associated with successful phishing attacks.

TO AVOID MitM ATTACKS YOU SHOULD

- ✓ Ensure that employees in your organization stay off public networks
- ✓ Implement multi-factor authentication when logging into critical accounts
- ✓ Only use secure (https://) websites
- ✓ Encrypt Emails

> **Business email compromise (BEC) attacks, a form of MitM attacks, was the second most common cyber attack in North America in 2021 at 12% of total attacks.**
>
> -X-Force Threat Intelligence Index 2022, IBM

THREATLOCKER® SOLUTION

ThreatLocker's Network Access Control (NAC) is a zero trust endpoint firewall. NAC gives you total control over all in-bound network traffic, which ultimately helps you protect your devices. Using custom-built policies, ThreatLocker's NAC gives you the ability to allow granular access based on IP addresses, specific keywords, agent authentication, or dynamic ACLs, keeping threat actors out.

Having a zero trust security posture is becoming the standard, and key to preventing outside parties from intercepting internal communications. That being said, implementing and maintaining it is no easy task. ThreatLocker® makes it a point to assist your organization in adopting the standard with ThreatLocker® University, live and recorded product demos, and 24/7 CyberHero support. By joining ThreatLocker®, Dawn Sizer, CEO of 3rd Element Consulting found that making this change is easier than it looks. “Zero Trust isn't easy to architect. ThreatLocker® takes the burden off and does the heavy lifting for you.”

CHAPTER 05

Password Attack

One of the oldest tricks in the book! About 81% of data breaches are due to poor password etiquette, such as reusing the same or similar passwords across multiple sites. A password attack is any method used to gain control of your organization's secure accounts, systems, and networks. The objective is to infiltrate your organization and steal confidential information, spread malicious software, exploit any ads for malicious intents, or personally alter your website or social media accounts to harm your reputation.

THREATLOCKER® SOLUTION

In the event of credentials being compromised, ThreatLocker's Allowlisting will stop any unwanted programs from being run by the compromised user. Additionally, Storage Control allows you to control what applications can access your organization's data by complementing traditional user-based ACLs with application-specific permissions. Between these two solutions, you can reduce the potential for data loss by restricting access to any data your organization hosts

Organizations that host the sensitive data of countless individuals present themselves as huge targets for threat actors. That is why Alex Rupp, Network Engineer at Healthcare Practice IT, states that his favorite ThreatLocker® feature is Storage Control. "Sometimes, one day, a file will disappear." He continues, "With Storage Control, I can just go in, find deletes, and it just makes my life so much easier." Rupp finds that auditing his data and controlling admin rights for non-admin users is much easier with ThreatLocker's solutions platform.

81%

Of data breaches are due to poor password etiquette.

–How Long Does It Take A Hacker to Brute Force a Password? IronTech Security, 2021

BEST WAYS TO PREVENT PASSWORD ATTACKS

- ✓ Use passphrases instead of passwords
- ✓ Implement brute force lockout policies
- ✓ Not allow password hints
- ✓ Use a password manager
- ✓ Enable multi-factor authentication

Zero-Day Vulnerability

Zero-day vulnerabilities arise from regular vulnerabilities, which occur when a flaw in a system or device has weaknesses in its code. It is once the vulnerability has been disclosed as exploited but not yet patched, it becomes a zero-day vulnerability. This vulnerability is usually very targeted and enables hackers to release an exploit code before the developer can create a patch. As time passes, threat actors' tactics and technology advance, accelerating the number of vulnerability exploits, and developers can only release software patches so fast.

> Google's Project Zero reported that as of June 15, 2022, a total of 18 zero-day vulnerabilities were detected and had been disclosed as exploited in-the-wild. A previous report published at the end of 2021, observed that 2021 had seen the highest number of vulnerabilities exploited ever, doubling 2015's 28 exploited vulnerabilities with a record-breaking 58.
>
> -2022 0-Day In-The-Wild, Google Project Zero

HOW TO DIMINISH THE EFFECTS OF VULNERABILITY EXPLOITS

- ✓ Implement threat intelligence
- ✓ Maintain firewalls
- ✓ Restrict user access to only essential files and systems

THREATLOCKER® SOLUTION

Ringfencing™ gives you the power to define how your applications interact with other applications, network resources, registries, and files. Should an application you have permitted to run with Allowlisting become exploited, Ringfencing™ policies can stop the exploited applications from interacting with and weaponizing tools like PowerShell, Command Prompt, and other Windows components.

In a case study conducted with James Cash, Managing Director of Superfast IT, Cash names the Kaseya vulnerability attack as the driving force behind why Superfast IT decided to implement ThreatLocker® into their security stack, calling the incident "a wakeup call for a lot of MSPs."

A big security challenge that Superfast IT faced prior to having ThreatLocker® was supporting around 1,500 machines across their clientbase and knowing what was happening on each machine at any one time. He mentions that Superfast IT has peace of mind now that "ThreatLocker® has given us complete visibility and control over the applications that run on those machines" Cash goes on to add. "One of our business goals is to grow" and "One of the key aspects of that is ensuring the security of our client base, and ThreatLocker® has enabled us to take that security to another level."

CHAPTER 07

Rootkits

A rootkit is a collection of malicious software tools that give unauthorized remote access and control over your computer or systems. Rootkits allow malicious code to hide within your device after trespassing via phishing, drive-by-downloads, baiting, and more. It is observed that rootkits represent 8% of all reported infections in Microsoft's Windows Platform with the Alureon rootkits accounting for more than 50% of those, Cutwail at less than 20%, and Rustock at less than 10%.

The sole purpose of a rootkit is for a threat actor to gain admin-level access to secure technical areas of an organization without being detected. Once in your system, hackers can do numerous malicious activities, including stealing your data, uploading some form of malware, stealing login credentials for other accounts, and more.

Rootkits are hard to detect; however, they can be prevented with Allowlisting, continuous updates, and only downloading files from trusted sources.

> It is observed that rootkits represent **8%** of all reported infections in Microsoft's Windows Platform with the Alureon rootkits accounting for more than **50%** of those, Cutwail at less than **20%** and Rustock at less than **10%.**
>
> -What is a Rootkit?, BullGuard

THREATLOCKER® SOLUTION

Allowlisting and Ringfencing™ will both first step in to stop malware caused by Rootkits, blocking applications from running or communicating with applications they should not. However, in the case where a user with admin-level access to data stores falls victim to a rootkit attack, ThreatLocker's Storage Control provides policy-driven control over storage devices, including local folders, network shares, or external storage such as a USB drive. Storage Control allows you to limit software access to your data, only allowing trusted software access, and preventing unauthorized software from stealing, harming, or encrypting your data store.

The necessity for zero trust security tools like ThreatLocker's Storage Control has grown immensely, proven by the continuous increase of small and large-scale businesses that have experienced viruses and malware attacks like Rootkits. This evolution in the cybersecurity environment is what pushed Pendello's President, Mike Jackson, to invest in ThreatLocker®. "It was the increased concern of malware and the different ways that threat actors were getting into environments, and then ThreatLocker® having that functionality, that initial capability, to provide peace of mind." Jackson further points out that now that he uses ThreatLocker®, things have been much easier. "A lot of times when I tell people about it, it makes me sleep better at night."

CHAPTER 08

Internet of Things Attacks

Internet of Things (IoT) attacks have become exceedingly popular due to the growing number of connected devices on the average network, especially when the world went virtual during the pandemic. In just the first half of 2021 (January to June), about 1.5 Billion breaches of IoT Devices occurred, a massive increase from 2020's 639 Million!

These IoT devices include anything that can connect to the internet. They include computers, phones, smartphones, printers, and more - perhaps even the office refrigerator. IoT attacks attempt to harm your organization by gaining access or complete control over your IoT devices. They may attempt to spread to as many other IoT devices as possible through your organization's network, causing as much damage as possible.

1.5

Billion Breaches

Of IoT Devices occurred in just the first half of 2021 using the telnet remote access protocol.

–IoT Cyberattacks Escalate in 2021, According to Kaspersky, IOT World Today, 2021

THREATLOCKER® SOLUTION

You can prevent IoT attacks by implementing zero trust into your cybersecurity stack. Network Access Control (NAC) allows you to granularly control which devices can connect to your servers and shares. By blocking unauthorized connections you minimize the potential for compromised IoT devices to act as a foothold into your network. Alternatively, Ringfencing™ keeps applications on your IoT devices and endpoints from communicating with internet-connected applications like Chrome, preventing them from sending anything out or downloading anything malicious to your device.

When asked in a case study what his favorite ThreatLocker® feature was, Jason Stone, president of Tech Partners Hawaii, said "the first one that comes to mind for me, because I'm always utilizing Command Line, is Ringfencing™, for a lot of the higher level tools." Stone then goes on to say that he uses it to block administrative rights outside of a normal administrative window like Command Prompt and PowerShell.

CONCLUSION

Final Thoughts

Every day the cybersecurity landscape continues to evolve, and the emergence of new threats doesn't show any sign of slowing down.

ThreatLocker's number one goal is to equip you with solutions that proactively defend your organization against countless cyber threats and provide rapid 24/7 support needed for your dynamic operations. Each solution on the ThreatLocker platform is founded on the basis of operating with a zero trust, default deny strategy. This puts you in command of how your organization facilitates its internal and external cyber defenses and protocols.

THREATLOCKER® SOLUTION

The Zero Trust security solution that offers a unified approach to protecting users, devices, and networks against the exploitation of zero day vulnerabilities. Get unprecedented visibility and control of your cybersecurity, quickly, easily, and cost-effectively. Schedule a free product demonstration and ThreatLocker® will show you how.

Learn more

READY FOR A DEMO?

Visit the ThreatLocker® website for more details.

Contact us

sales@threatlocker.com

+1-833-292-7732

About ThreatLocker®

ThreatLocker® is a leader in endpoint security technologies, providing enterprise-level cybersecurity tools to improve the security of servers and endpoints. ThreatLocker's combined Application Allowlisting, Ringfencing™, Storage Control, Elevation Control, and Endpoint Network Access Control (NAC) solutions are leading the cybersecurity market toward a more secure approach to blocking exploits of known and unknown vulnerabilities.

threatlocker.com

Best_Practices_For_Common_Cybersecurity_Threats_10262022