THREATLOCKER OVERVIEW

Allowlisting

The approach of allowlisting with ThreatLocker® focuses on permitting essential business software while blocking all other applications. This ensures smooth business operations without the risk of unauthorized or malicious software infiltrating the devices in the organization.

Moreover, it strengthens security by proactively blocking unknown applications while allowing trusted software to function. Regular updates and monitoring are critical to maintaining a secure environment.

Historic Examples of Phishing Attacks

UHS Hospitals

UHS Hospitals encountered a significant disruption as a result of a ransomware attack. UHS Hospitals, a healthcare network encompassing 400 medical facilities in both the United States and the United Kingdom, fell victim to the ransomware Ryuk ransomware variant. The infiltration of Ryuk into the hospital's computer systems is suspected to have occurred through a phishing attack. Subsequently, the malware remained dormant until nighttime, when it initiated the process of encrypting critical files.

Ireland HSE

The Health Service Executive (HSE) of Ireland, the country's publicly funded healthcare system, suffered a security breach when a malicious Microsoft Excel file, delivered via a phishing email, introduced the Conti ransomware. In the aftermath of this breach, the attackers issued a demand for a sum of 19 million dollars in exchange for the decryption of the compromised servers, leading to a temporary IT system shutdown to prevent further infection. The HSE incurred costs of $120 million for system recovery and future security enhancements.

RINGFENCING™

Reduce the chance of a cyberattack by limiting what applications can do, whether it’s interacting with another application, your files, data, or the Internet.

Enabling this feature grants control over the actions that your permitted software can take. When enabled for a software program, its interactions with other applications, data, registry, or the internet will be logged and displayed in the Unified Audit. Necessary exceptions can be identified and implemented to restrict unnecessary behavior while preserving intended functionality.

Historic Examples of Apps Being Weaponized

SolarWinds

The SolarWinds breach was a supply chain attack, internally compromised due to an intern who had used the same password for seven years. Hackers may have brute forced the password to gain access. Another supporting factor to compromise was because of a misconfigured GitHub repository which was made accessible - and was leaking FTP credentials of the company’s download website in clear text. This allowed hackers to use these credentials to upload compromised/malicious updates to SolarWinds download sites. The compromised version of SolarWinds Orion plug-in was used to execute dubious commands, transfer files, disable system services, and gather information about the machine. By misleading vendors into thinking that it was an uncompromised version, they were able to target multiple organizations simultaneously gathering sensitive information from a wide range of machines by means outside of what the software would normally do.

3CX

3CX was also compromised by a supply chain attack. Hackers managed to hijack the 3CX Electron Windows app, and used it to download malicious software from a unrelated GitHub repository. It is believed that they were able to compromise 3CX by using another supply chain attack from a company, called X Trader which experienced a similar compromise. This false update allegedly was written in a way that forced the malicious content to wait a certain amount of time before actually doing anything, increasing the distribution of the update, then attacking all infected platforms at once. Both examples related involved compromised software, but also had access to more than it needed, and could change the intent of how it performed as a result.

REPORT SUMMARY

Devices running ThreatLocker® vs. not running ThreatLocker® **206 out of 42,000**. To capture a complete picture of the environment, all devices should run the ThreatLocker® Agent.

Devices NOT Running ThreatLocker®

0.47%

Devices in Secured mode

When devices are not secured, users are able to execute any software or code that is not known to be bad by an antivirus. This allows shadow IT operations, ransomware and other cyber attacks occur, and the weaponization of built-in tools like PowerShell. It is recommended after a learning period and review, all devices are secured.

0/206

Unused Software

There is no value in permitting unused software within the environment. We recommend restrictively allowing only the essential applications for everyday business operations. By doing so, you can substantially reduce your vulnerability to attacks.

9,986 policies unused out of 17,432 Total

No Default Deny Network Policies

Network Access policies are not being utilized on the organization. Activating this product will not only log and monitor all inbound network traffic, but also give the ability to control that traffic based on organizational needs.

0/206

Restricted Storage

Portable storage should be blocked where it is not required. Allowing portable storage could allow data theft from your environment very easily. Allowing unencrypted portable storage could allow data theft from lost devices.

0/206

Computers with restricted storage policies

Ringfenced™ Policies

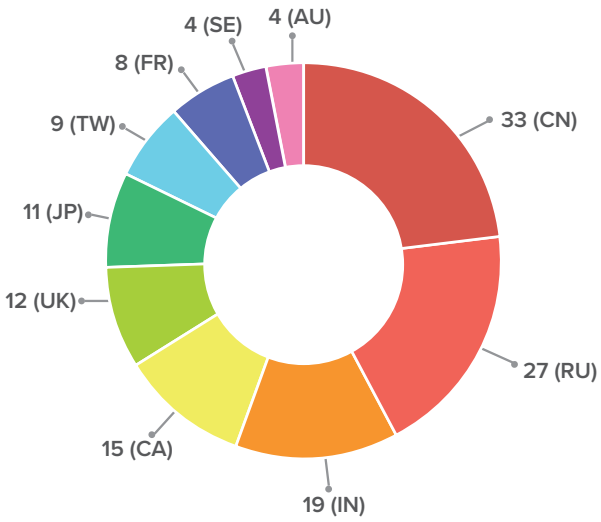
All applications have access to all data, the Internet, and other applications on your computer. Allowing untethered access to your computer from all of the software you run allows vulnerable applications or application back doors to extract data, execute instructions from attackers and expose your organization to cybersecurity attacks.

Recommend action, Ringfence™ applications so they can only access the data they require to perform their function.

64/17,432

APPLICATION REPORT SUMMARY

Foreign Applications by Country of Origin



17,432 TOTAL POLICIES

Average Policy Count: 39

Ideal Policy Count: 22

ThreatLocker® best practices involve removing unused software, as well as limiting functionality with Ringfencing™ to allow programs to only access what they need, and blocking everything else.

AREAS RECOMMENDED FOR REVIEW

Known Vulnerabilities

Devices in the organization still have files present that are vulnerable to the Apache Log4Shell exploit (CVE-2021-44228).

- PaperCut NG
- Apache Log4j
- FortiSOAR
- FortiConverter
- eCatcher

Browser Extensions

There is evidence of 105 browser extensions being utilized in the environment.

- 12, Productivity extensions
- 8, Gaming extensions
- 11, Shopping extensions
- 6, VPN extensions
- 3, ChatGPT Extensions
- 17, Custom Browser Theme Extensions

Gaming and Entertainment

There is evidence of 25 types of Gaming and Entertainment software being used. Some include open-source software, which allows developers from around the world to modify the code.

- Chromium Extension Beyond
- Epic Games
- Candy Crush
- Minecraft

Windows Store Apps

There is evidence of multiple Windows Store Apps being used in your environment. It is important to note that these apps can be developed by various third parties, which may expose them to potential security flaws and vulnerabilities.

- Windows App Microsoft Windows Terminal
- Windows App Candy Crush Saga
- Windows App Splashtop

VPN Tools

There is evidence of more than one VPN tool being used in your environment. They are widely used for enhancing privacy and security. However, they may have the capability to bypass security measures, hindering visibility and exposing sensitive data.

- Nord VPN
- Express VPN
- CyberGhost
- Hotspot Shield
- Azure VPN
- ProtonVPN

Remote Desktop Apps

There is evidence of multiple remote access tools being utilized in your organization. While being commonly used for legitimate purposes, they can also be exploited and used for malicious purposes, making them a security risk if not used or managed properly.

- TeamViewer
- Anydesk
- Splashtop
- UltraVNC
- Bomgar
- ConnectWise Control

APPLICATIONS TO PRIORITIZE & REVIEW

7-Zip

An open-source file compression system. It's been used historically for password cracking and allowing remote code distribution.

(CVE-2018-10115)


Russia

Potential Risks

Permitting software of this nature carries risks such as possible security vulnerabilities, and unauthorized data compression.

Risk Mitigation Strategy

We recommend removing where there's no business need. Otherwise, you can block it from interacting with other software to remove the potential for lateral movement.

Browser Extension Coupert

Mainly used for applying coupon codes and discounts when online shopping. It automatically finds and applies any valid coupons to your checkout.


China

Potential Risks

Permitting software of this nature carries risks such as possible security vulnerabilities, and unauthorized data compression.

Risk Mitigation Strategy

We recommend removing this from your Permitted Applications. This will enable ThreatLocker's Default Deny policy to block its execution, given that your machine is in a secured state. Otherwise, consider implementing an Explicit Deny policy specifically for this application.

PuTTY

Free, open-source terminal emulator and network fil transfer tool used for secure remote connections to servers and devices. It supports SSH, telnet, and serial connections


United Kingdom

Potential Risks

Permitting software of this nature carries risks such as possible security vulnerabilities, and unauthorized data compression.

Risk Mitigation Strategy

We recommend further evaluating the need for this software to run in your environment. If it is required for business use, we recommend limiting access to other software and locking down ports it can use to only 22 (SSH). Additionally, we recommend scheduling the use of this application during business hours.

TightVNC

An open-source remote desktop software that allows you to have complete access over targeted endpoint(s).


Russia

Potential Risks

Permitting software of this nature carries risks such as possible security vulnerabilities, and unauthorized data compression.

Risk Mitigation Strategy

We recommend removing where there's no business need. Otherwise keeping this tool scheduled to only be available during business hour and locking down ports 5800 and 5900 to only be accessible via trusted devices could help prevent unauthorized use of this tool.

Wave Browser

Carries the potential of being classified as a browser hijacker. It can manipulate web browser settings, and often redirects users to unwanted websites.


United States

Potential Risks

Permitting software of this nature carries risks such as possible security vulnerabilities, and unauthorized data compression.

Risk Mitigation Strategy

This is unwanted software that gets installed with other programs. It is a browser that can make unauthorized changes to your devices leaving your endpoints vulnerable. We recommend blocking this application.

Autohotkey

Open-Source software that can create keyboard remappings, and program other peripheral macros to run scripts with the push of a button.


United States
Canada...

Potential Risks

Permitting software of this nature carries risks such as possible security vulnerabilities, and unauthorized data compression.

Risk Mitigation Strategy

We recommend further evaluating the need for this software to run in your environment. If it is required for business use, we recommend limiting access to other software and locking down ports it can use to only 22 (SSH). Additionally, we recommend scheduling the use of this application during business hours.

NETWORK TRAFFIC SUMMARY

We have found machines communicating with the following countries. This information is pulled directly from the policies with ThreatLocker® Network Control and Ringfencing™ settings applied.

ThreatLocker® Network Control includes additional logging information such as Port traffic. Common examples of information that could be valuable to see usage on include:

- Port 3389 (Remote Desktop Protocol)
- Port 135 (Remote Procedure Call Service)
- Ports 139 & 445 (SMB Protocol)

We have found instances of TikTok being used in your Organization. Within the past 30 days, 78 computers have reached out to TikTok. Included in this report is the Government Executive Ban for TikTok on all Government devices.

ThreatLocker® best practices involve Ringfencing™ Applications from reaching out to the Internet. This will prevent unwarranted communication to particular IP's or Domains. Utilize Network Control policies to only allow traffic that's trusted, while denying everything else.

Scan the QR Code to view the official Executive Order.

Inbound Network Traffic

Device 1

The following hostname is accepting incoming connections on the following ports

- Ports: 3389, 445, and 139

Inbound connections coming from:

- China, Russia, Mexico etc.

Device 2

The following hostname is accepting incoming connections on the following ports

- Ports: 3389

Inbound connections coming from:

- France, India, Russia, etc.

Device 3

The following hostname is accepting incoming connections on the following ports

- Ports: 139

Inbound connections coming from:

- Canada, China, Singapore etc.

Device 4

The following hostname is accepting incoming connections on the following ports

- Ports: 139

Inbound connections coming from:

- Germany, United States, Japan etc.

Device 5

The following hostname is accepting incoming connections on the following ports

- Ports: 445 and 139

Inbound connections coming from:

- Ukraine, Estonia, Taiwan etc.

Device 6

The following hostname is accepting incoming connections on the following ports

- Ports: 3389 and 445

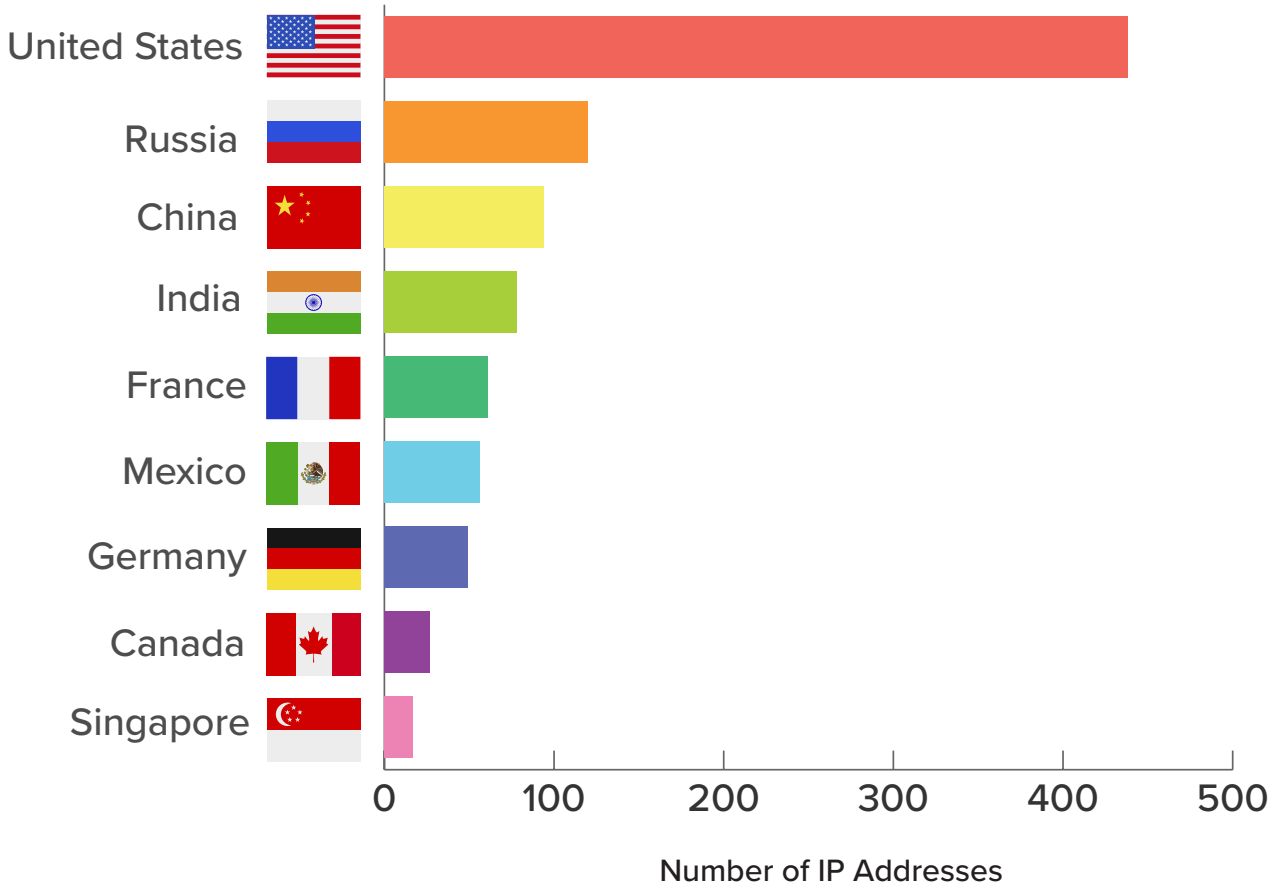
Inbound connections coming from:

- United States, Russia, China etc.

NETWORK TRAFFIC SUMMARY

Outbound Network Traffic

This graph displays the number of IP Addresses that your machines have communicated with across the following countries.



Risks of Allowing Ports 139 & 445

Ports 139 & 445 facilitate the Server Message Block (SMB) Protocol for file and printer sharing across networks. However, enabling access to these ports poses risks like unauthorized access, data theft, malware spread, and potential denial-of-service attacks. To uphold network security, it is advisable to block or limit access to these ports.

APPLICATIONS OVERVIEW

Application Name	Details	Access	Where Code is Compiled	Review Rating
7-Zip	**Description:** An open-source file compression system. It's been used historically for password cracking and allowing remote code distribution. **Potential Risks:** Permitting software of this nature carries risks such as possible security vulnerabilities, and unauthorized data compression. **Risk Mitigation Strategy:** We recommend removing where there's no business need. Otherwise, you can block it from interacting with other software to remove the potential for lateral movement.		Russia	8
Wave Browser	**Description:** Carries the potential of being classified as a browser hijacker. It can manipulate web browser settings, and often redirects users to unwanted websites. **Potential Risks:** Permitting software of this nature carries risks such as possible security vulnerabilities, and unauthorized data compression. **Risk Mitigation Strategy:** This is unwanted software that gets installed with other programs. It is a browser that can make unauthorized changes to your devices leaving your endpoints vulnerable. We recommend blocking this application.		United States	8
TightVNC	**Description:** An open-source remote desktop software that allows you to have complete access over targeted endpoint(s). **Potential Risks:** Permitting software of this nature carries risks such as possible security vulnerabilities, and unauthorized data compression. **Risk Mitigation Strategy:** We recommend removing where there's no business need. Otherwise keeping this tool scheduled to only be available during business hour and locking down ports 5800 and 5900 to only be accessible via trusted devices could help prevent unauthorized use of this tool.		Russia	7
Autohotkey	**Description:** Open-Source software that can create keyboard remappings, and program other peripheral macros to run scripts with the push of a button. **Potential Risks:** Permitting software of this nature carries risks such as possible security vulnerabilities, and unauthorized data compression. **Risk Mitigation Strategy:** We recommend removing this from your Permitted Applications. This will enable ThreatLocker's Default Deny policy to block its execution, given that your machine is in a secured state. Otherwise, consider implementing an Explicit Deny policy specifically for this application.		United States, Canada	7

*Review Rating is based on a scale from 0 to 10, with the higher the rating on the scale, the more attention needed to review the application in question.

 Applications

 File

 Internet

 Registry