CyberProof®
A UST Company

Top 10 threats in the age of GenAI

cyberproof.com

Contents

Why Read This Report

Threat prioritization and prediction have become critical components in the fight against cybercrime in the digital age. With the increasing frequency and sophistication of cyberattacks, organizations must be proactive in identifying and mitigating potential threats.

In 2023, advanced technologies such as Machine Learning (ML) and AI are being utilized to analyze vast amounts of data, detect patterns and anomalies, and provide real-time predictions of potential security incidents. This approach not only improves the efficiency of security operations but also helps organizations stay ahead of the rapidly evolving threat landscape.

This report offers a threat hunter's perspective, providing a guide for organizations that are concerned about potential cybersecurity threats and help them prioritize their security efforts and allocate resources effectively to address the most pressing threats. For each of the ten attacks covered in this report, we provide a description of the associated MITRE tactics and techniques. These are followed by actionable threat hunting queries, where relevant.

Some of the key takeaways of this report:

1. **Decrease response time:** As cybersecurity continues to be a critical issue, it is important to identify the top threats that pose the greatest risks to your business. Reporting on these threats can significantly improve the efficiency of security operations, enabling organizations to respond more quickly and effectively to potential threats.

2. **Keep up with attack trends:** AI-enhanced attacks are becoming more widespread and more sophisticated, leading to more dangerous attacks. Ransomware threats continue to be the prevalent threat due to their financial motive, and attackers are constantly looking for ways to increase the attack surface. Supply chain attacks - targeting "Bring your own device" (BYOD) and other kinds of vulnerabilities - are also on the rise.

3. **Be aware of nation-state activity:** Both overt and covert nation-state activity are used to impact potential victims' business activities for their own gains, and as threat actors are evolving, it is important for cybersecurity professionals to stay informed and be prepared. By identifying and addressing these top threats, organizations can better protect themselves from potential cyberattacks.

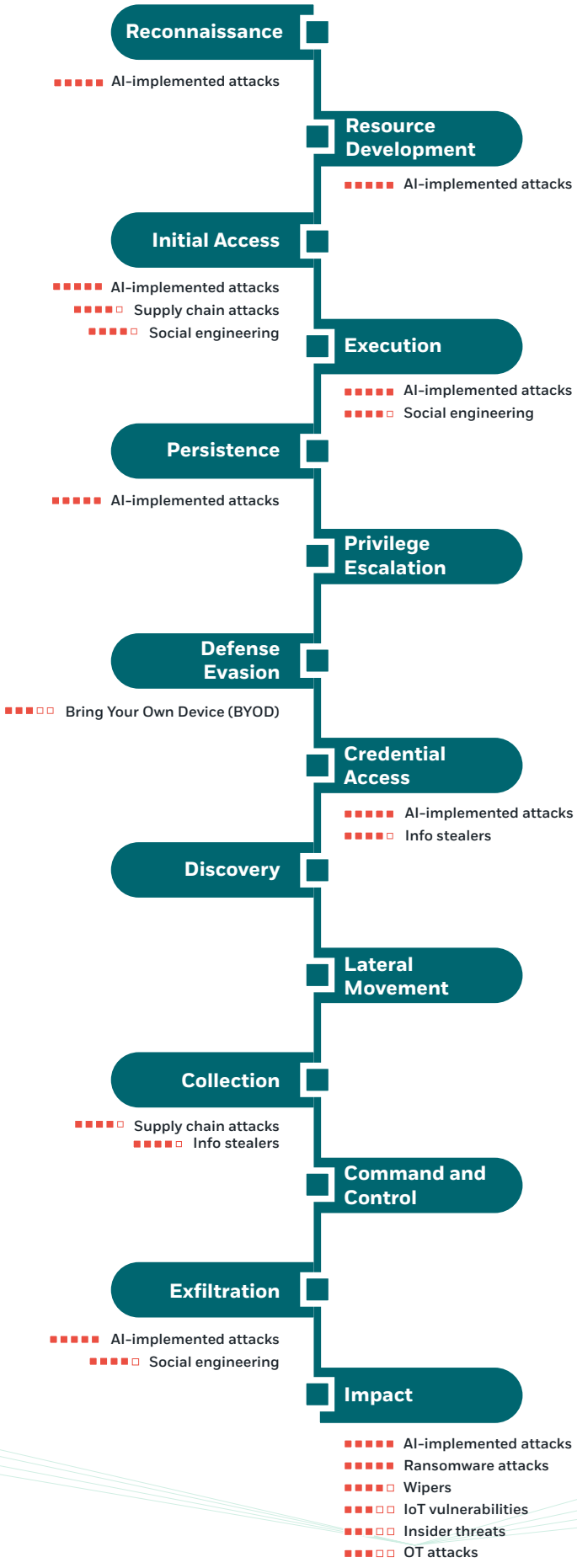
Top ten threats

This report focuses on the top ten threats of today's threat landscape.

The information in this report, alongside scoring rankings, is based on research conducted by CyberProof's dedicated Threat Hunting team. The research identified a combination of persistent past and new threats that have the potential to cause significant future damage.

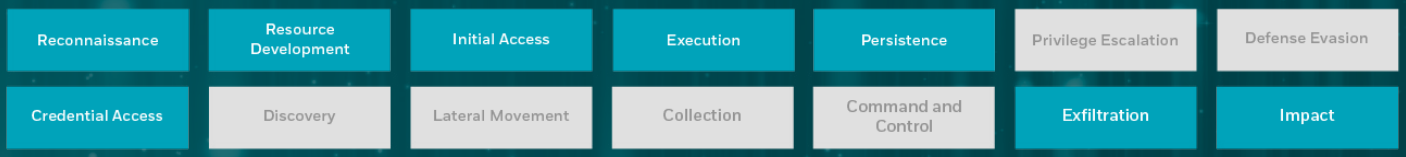
The diagram displayed here indicates which MITRE tactics are used in each of these attacks.

- High priority
- Mid-high priority
- Medium priority
- Mid-low priority
- Low priority



Top threats organized by MITRE tactics

1 AI-implemented attacks



MITRE ATT&CK tactics leveraged in these types of attacks

Artificial Intelligence (AI)-implemented attacks refer to the use of artificial intelligence technologies for malicious purposes, such as cyberattacks, fraud, and disinformation campaigns. These attacks leverage Machine Learning (ML) to automate and scale traditional forms of cybercrime, making them more effective and harder to detect. AI technologies can create malicious code variants and develop new paths for threat actors to infiltrate a network, in addition to elevating 'script kiddie' capabilities to reuse and enhance existing malware to evade detection. This threat remains to be seen, but the possibilities for AI-implemented attacks are certainly increasing.

The following are some possibilities for AI-implemented attacks, organized by MITRE tactic:

Reconnaissance and Initial Access

- **Voice impersonation attacks:** AI-powered voice cloning technology can be used to create realistic impersonations of individuals for phishing scams or social engineering attacks. See Vishing.
- **AI-powered phishing scams:** AI algorithms can be used to automate and scale phishing attacks by generating convincing emails, messages, and webpages that appear to be from trustworthy sources.
- **AI-driven attack surface reconnaissance:** AI algorithms can be used to determine the best way to infiltrate a company. This includes scripts to monitor and initiate an attack on open and unfiltered ports, public-facing applications, or newly added unconfigured cloud instances.

Persistence

- **AI-driven backdoor:** AI algorithms can be used to maintain access to compromised systems by creating stealthy backdoors that are difficult to detect due to their complexity and renewability.
- **AI-driven DGA algorithm:** C2 infrastructures can change the domain using AI algorithms to generate complex and unpredictable DGA domain name patterns that are difficult to block or classify as malicious.

Execution

- **Polymorphic malware:** AI algorithms can be used to create malware that can change static code, causing it to behave dynamically in response to the environment it is running in, making it harder for security tools to detect and block it.
- **Granular malware behavior based on Machine Learning algorithms:** AI algorithms can be used to create malware that can learn from its environment and adapt its behavior to evade detection.

Credential Access

- **AI-driven customized brute force:** AI algorithms can be used to gather intel on a person from online sources and create a customized rainbow table to speed up the process of brute force to the person's accounts.

Exfiltration

- **Decision-making exfiltration techniques based on Machine Learning algorithms:** AI-driven malware can exfiltrate small pieces of data to a temporal C2 server and test which exfiltration path is best to extract data. Once a path is chosen, the rest of the data can be exported through this exfiltration technique without being detected by security products.

Impact

- **Time-based ransomware:** A ransomware could use ML algorithms to identify the most vulnerable times for a security team (such as low activity in the network, slow response times, and shift changes) to quickly encrypt the environment whenever security teams are less alert and prevent them from reacting quickly to the attack.

Our recommendations

The following proactive steps are recommended by our threat hunters to reduce the threat impact:

Awareness of the new threat of AI capabilities

Every Security Operations Center (SOC) should be aware of the threat that AI capabilities pose and prepare for a change in the cyber landscape and workflows.

Training on Social Engineering Techniques

- Run phishing simulations using in-the-wild campaigns, so that employees get into the habit of recognizing and reporting phishing attempts and other suspicious activity.
- Use tools like phishing-resistant Multi Factor Authorization (MFA) and Zero Trust to reduce the risk of account takeover and identity fraud.
- Teach staff to verify the authenticity of financially-related requests, especially if there is a sudden urgency or an unusual request that appears out of the blue.

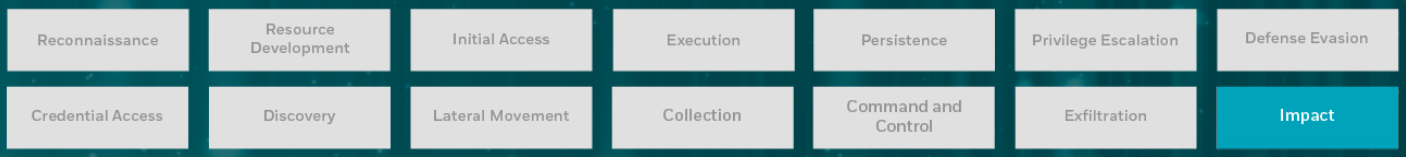
Make perimeters robust

- Patch all internet-accessible devices, applications, and cloud instances regularly so that threat actors or AI-driven scripts cannot discover these loopholes.
- Only work with vendors and partners that are policy-compliant and are transparent about their security policies. Verify they practice Secure Development Lifecycle (SDL) programming.
- Implement access controls to limit the access of individuals and systems to sensitive information and systems.
- Improve the password policy to force users to use different passwords for each system and change them regularly.

AI to fight AI

- Implement AI-based security solutions that can detect and respond to AI-implemented attacks in real-time.
- Develop or use Machine Learning countermeasures and natural language processing (NLP) to detect advanced stealthy threats, such as regular Domain Generation Algorithm (DGA) domains, polymorphic malware, and granular malware behavior.
- Create a baseline of the network traffic to look for anomaly activity, such as unexpected data transfers or incoming connections from unknown sources.

2 Ransomware attacks



MITRE ATT&CK tactics leveraged in these types of attacks

Ransomware is a type of malicious software that encrypts the victim's files and demands a ransom payment in exchange for the decryption key. The threat actors typically use social engineering tactics to trick the victim into downloading and installing the ransomware - for example, by disguising it as a legitimate software update or sending it as an attachment in an email.

Once the ransomware is deployed, it encrypts the victim's files and displays a ransom note on the screen, demanding payment in exchange for the decryption key. Payment is usually demanded in the form of cryptocurrency, such as Bitcoin, and the threat actors may threaten to destroy the encrypted files if the ransom is not paid.

Ransomware attacks can cause significant disruption and financial losses, as victims may be unable to access their critical files and systems until the ransom is paid. Research shows that the average sum of financial losses was $4.5-5 million USD in 2022.

Note that there is more to this threat than just the ransom itself:

- Paying the ransom does not necessarily ensure that the threat actors will provide the decryption key, as some might take payment and abscond without fulfilling their end of the bargain.
- If a company pays the ransom, it may be listed by threat actors as a future target based on past payment history, which could lead to increased attempts by other threat actors to gain access to the company's systems.
- Threat actors could employ extortion tactics by stealing and exfiltrating the company's data, which could have serious consequences such as the public release of sensitive information, intellectual property theft, or violation of data regulation.

Our recommendations

The following proactive steps are recommended by threat hunters to reduce the threat impact:

Backups are essential

It is critical to maintain offline and encrypted backups of data and to regularly test your backup procedure. Backups should be maintained offline or in a separate network, as many ransomware variants attempt to find and delete any accessible backups. Create an effective backup strategy following the 3-2-1 rule:

- Creating at least **three** copies of the data,
- In **two** different storage formats,
- With at least **one** copy located offsite.

Multi-factor authentication

Multi-factor authentication (MFA) should be enforced for connectivity. This can be accomplished either via the integration of a third-party multi-factor authentication technology, for example, a Remote Desktop Gateway (RDG) or Azure Multi-Factor Authentication Server using RADIUS. Only provide remote access via MFA to avoid brute force and password-spraying attacks on Internet-facing services like a Remote Desktop Portal (RDP).

Regularly scan for vulnerabilities

Conduct regular vulnerability scanning to identify and address vulnerabilities – especially those on external-facing devices – to limit the attack surface.

Create detection rules

Implement detection rules and keep them up to date with recent sophisticated ransomware attacks to deploy more detection rules.

Enroll decoys

Bringing in decoys can provide another layer of proactive steps to detect ransomware infections.

Strong passwords prevent a snowball effect

Adopt strong passwords throughout the network. In the presence of a weak password, malicious actors could use a brute force attack to gain access to a system or account. They could then leverage that access to conduct secondary attacks or move laterally throughout the network throughout the network in order to deploy ransomware.

Implement the principle of least privilege

You should consider implementing the principle of least privilege by reviewing levels of control. This will deter ransomware actors from using a compromised account to move through your network. Using the least privileged access helps to limit access and impact sensitive data.

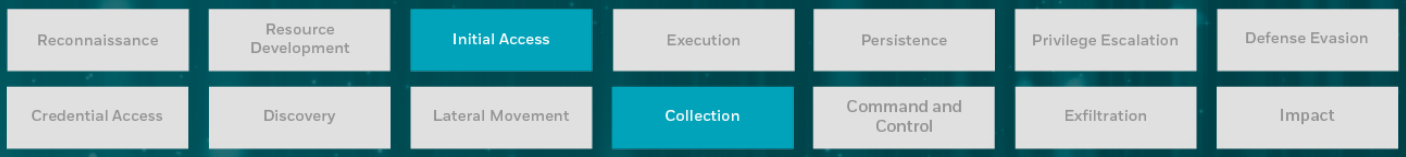
Hunting queries

Hunting queries allow threat hunters to search for and explore specific information related to each threat, enabling a more targeted and efficient retrieval of relevant data.

Hypothesis	Hunting Logics	Defender Query
The Lokibot malware must have AnaMetaphor.dll to operate properly	Hunt for rundll32 execution with the following parameters: AnaMetaphor and Pretor	DeviceProcessEvents | where InitiatingProcessFileName =~ "rundll32.exe" | where FileName == 'cmd.exe' and ProcessCommandLine has_all("rundll32.exe", "AnaMetaphor","Pretor")
Attackers can delete a Shadow copy to prevent backup restoration	Hunt for vssadmin.exe and wmic.exe used to delete shadow copies	DeviceProcessEvents | where ActionType == "ProcessCreated" | where ProcessCommandLine has_all("vssadmin.exe", “delete”, “shadows”") or ProcessCommandLine has_all("wmic.exe”, “shadowcopy”, “delete")

Attackers can terminate the process quickly after starting	Hunt for processes that are quickly executing their payload and terminate	let endTime = now(-3s);
		let startTime = now();
		DeviceProcessEvents
		| where Timestamp between (endTime..startTime)
		| summarize count() by FileName

3 Supply chain attacks



MITRE ATT&CK tactics leveraged in these types of attacks

Supply chain attacks refer to cyberattacks that target the weak links in a supply chain to gain access to the target organization. The attacker enters the target organization by compromising one of its suppliers, contractors, or other third-party partners, and then uses this entry point to move laterally through the target's network.

Supply chain attacks can take many forms, including the compromise of software updates, the injection of malware into hardware components, or the theft of intellectual property and sensitive information. For example, an attacker might compromise the software update process for a widely used software package, such as a software library, to distribute malware to thousands of organizations that use that software.

These types of attacks are becoming more common and sophisticated, as threat actors recognize the potential rewards for compromising a single vendor to gain access to multiple target organizations. To protect against supply chain attacks, organizations should implement security measures to verify the authenticity of software and hardware components and perform thorough risk assessments of their third-party partners.

Recent examples of this threat in the wild include the following:

- **Accellion hack:** A vulnerability in the file transfer software made by Accellion was exploited by a group of hackers, leading to a data breach at several organizations.
- **Codecov supply chain attack:** A malicious actor gained access to Codecov's software supply chain and modified the company's bash uploader script to exfiltrate sensitive information from its clients' continuous integration environments.
- **Okta hack:** A cybersecurity incident occurred in April 2021, when an unauthorized third party accessed a user's credentials for an Okta account. Okta is a cloud-based identity management platform that provides authentication and authorization services for businesses.
- **SolarWinds attack:** This was a highly sophisticated supply chain attack that impacted several government agencies and private sector organizations in the US.

Our recommendations

The following proactive steps are recommended by threat hunters to reduce the threat impact:

Conduct thorough third-party vendor risk assessments

Before granting suppliers access to your network, it is imperative to thoroughly evaluate their security practices. This includes assessing their security risk posture, governance policies, and compliance processes, as well as evaluating their technical security controls. It is important to ensure that their security measures align with your organization's security standards and protocols to mitigate potential risks and vulnerabilities. By doing so, you can enhance your organization's awareness of potential supply chain risks and implement the necessary processes and controls to detect, address, or even prevent supply chain attacks. This heightened visibility can help you better protect your organization and mitigate the risks associated with third-party suppliers.

Build an incident response plan

It is crucial to establish a comprehensive incident response plan well in advance of a potential attack. This plan should include policies, plans, and processes that are tailored to your organization's specific risk profile and that account for all relevant regulatory reporting requirements. By preparing in advance, you can ensure that your organization is equipped to effectively respond to any potential cybersecurity incidents and minimize their impact.

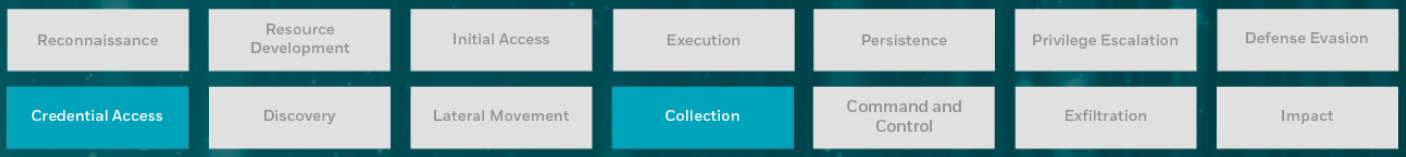
Prevent the internal spread of threats

Once a vendor of yours has been infected, enroll a pre-defined program to block all types of communications between your domain to prevent the malware from spreading to your environment. A suggestion for a Digital Forensics & Incident Response (DFIR) team would be to create a firewall rule to block all kinds of communication with a vendor and disable this rule. Enable the rule once you have an emergency.

Hunting queries

Hypothesis	Hunting Logics	Defender Query
Attackers can use unusual binary file activity to avoid detection	Hunt for process execution of binary files that are not part of the expected system behavior	DeviceProcessEvents | where FileName endswith ".exe" or FileName endswith ".dll" | where FileName != "notepad.exe" and FileName != "calc.exe" | where InitiatingProcessFileName == "cmd.exe" or InitiatingProcessFileName == "powershell.exe" | summarize count() by FileName, InitiatingProcessFileName
Attackers can use signed binaries from temp directories	Hunt for signed binary files that are executing from temporary directories	DeviceProcessEvents | where ProcessVersionInfoCompanyName == "Microsoft Corporation" and FileName endswith ".exe" | where FolderPath startswith "C:\\Users\\" and FolderPath contains "\\Temp" | summarize count() by FileName, FolderPath
Attackers can discover domain trusts to decide future attacking plans	Hunt for attempts to gather information using domain trust	DeviceProcessEvents | where ProcessCommandLine has_all ("dsquery", "-filter","objectClass=trustedDomain") or ProcessCommandLine has_all ("nltest","domain_trusts","trusted_domains") "-filter","objectClass=trustedDomain") or ProcessCommandLine has_all ("nltest","domain_trusts","trusted_domains") "-filter","objectClass=trustedDomain") or ProcessCommandLine has_all ("nltest","domain_trusts","trusted_domains")

4 Info stealers



MITRE ATT&CK tactics leveraged in these types of attacks

Info stealers are malicious software programs designed to steal sensitive information from a computer or network. This information can include passwords, credit card numbers, personal details, and other confidential information. The stolen information is then usually sold on the dark web or used for fraudulent activities. Info stealers can spread through email attachments, malicious websites, and infected software downloads. There are a few types of info stealers, as detailed below:

- **Keyloggers** are software programs or hardware devices that are designed to capture and record every keystroke made on a computer or mobile device. Keyloggers can be used for legitimate purposes, such as monitoring employee activity or for parental controls, but they can also be used for malicious purposes, such as stealing sensitive information like login credentials or credit card numbers.
- **FormGrabbers** are a type of malware designed to steal sensitive information that is entered into online forms. FormGrabbers work by intercepting data that is entered into fields on a web form, such as login credentials, credit card numbers, and other personal or financial information. This data is then transmitted to the attacker, who can use it for malicious purposes such as identity theft, fraud, or other cybercrimes.
- **Browser stealers** are a type of malware built to steal sensitive information from web browsers. This can include login credentials, credit card information, and other personal or financial data. Browser stealers are often delivered through phishing emails or malicious websites and can be designed to target specific browsers or browser versions.
- **Network sniffers**, also known as packet sniffers or network analyzers, are software or hardware tools that capture and analyze network traffic. Network sniffers can intercept and decode network data packets, allowing users to examine network traffic and analyze the data being transmitted.

The latest info stealer examples include the following:

- **RedLine info stealer:** First observed in March 2020, with most recent activity logged in February 2023. The Turla APT group is behind this stealer.
- **Raccoon stealer:** First discovered in April 2019, its most recent activity was in December 2022. Russian APT groups are behind the Racoon stealer.
- **Vidar:** This malware was first discovered in 2018. Its most recent activity was in February 2023. Russian APT groups are behind this info stealer.
- **Taurus:** This malware was first discovered in early 2020, with its most recent activity dating back to August 2022.
- **Stealc info stealer:** This was recently identified as a copycat of the Vidar and Racoon info stealers. Russian APT groups are behind this info stealer.

Our recommendations

The following proactive steps are recommended by our threat hunters to reduce the threat impact:

Employee training

Educate employees to avoid installing unnecessary applications to reduce the attack surface and to be aware of any suspicious email attachments from sources they are not familiar with.

Implement endpoint protection

Use endpoint protection (EDR) to identify this type of malware and implement security controls (DLP) to detect data exfiltration.

Monitor data exfiltration attempts

Hunt for various data exfiltration techniques, such as outbound emails, IRC instant messaging, P2P file sharing, social networks, and steganography.

Build an incident response plan

Make sure to have an incident response plan, including managing your legal team, PR to the press, and business stakeholders in case sensitive data is stolen.

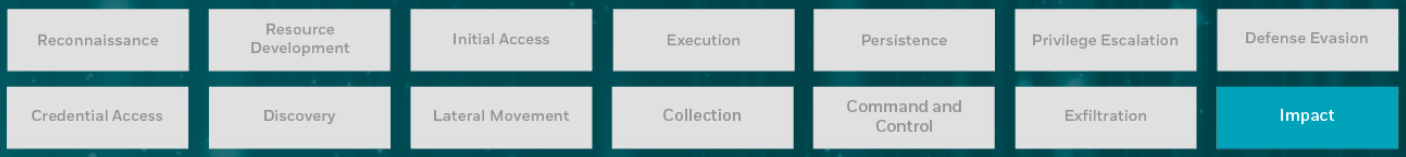
Hunting queries

Hypothesis	Hunting Logics	Defender Query
Attackers can use search for sensitive information to leverage in their attack plans	Hunt for info stealer activities such as the theft of sensitive information such as passwords, credit card numbers, and financial data	let keywords = datatable(keywords:string) ["password", "credit card", "bank", "login", "financial"]; DeviceProcessEvents | where FileName has_any(keywords) or ProcessCommandLine has_any(keywords) | summarize count() by FileName, FolderPath
Attackers can use search for sensitive information to leverage in their attack plans	Hunt for info stealer activities such as theft of sensitive information stored in certain file types	DeviceProcessEvents | where FileName endswith ".txt" or FileName endswith ".csv" or FileName endswith ".doc" or FileName endswith ".xls" | where ProcessCommandLine contains "copy" or ProcessCommandLine contains "download" or ProcessCommandLine contains "upload" | summarize count() by FileName, FolderPath

Attackers can use tunneling using common protocols to exfiltrate information out of the environment	Hunt for outbound connections that use known tunnelling protocols	let knownTunnelProtocols = dynamic(["443", "80", "53", "3389", "137", "138", "45", "22", "20", "21", "3389"]);
		let timeWindow = 1h;
		DeviceNetworkEvents
		| where Timestamp > ago(timeWindow)
		| where RemotePort in (knownTunnelProtocols)
		| summarize dcount(RemoteIP) by Protocol,RemotePort,RemoteUrl, bin(Timestamp, 5m)
		| where dcount_RemoteIP > 3
		"-filter","objectClass=trustedDomain")
		or ProcessCommandLine has_all ("nltest","domain_trusts","trusted_domains")

Attackers can use known protocol to exfiltrate information out of the environment	Hunt for info stealer activities such as theft of sensitive information stored on a device and uploaded to a remote server	DeviceProcessEvents | where ProcessCommandLine contains "ftp." or ProcessCommandLine contains "http://" or ProcessCommandLine contains "https://" | where ActionType == "FileUpload" | summarize count() by DeviceName, FileName

5 Wipers



MITRE ATT&CK tactics leveraged in these types of attacks

Wipers are malware designed to destroy or delete data from a victim's assets. This can be done for a variety of reasons, such as to cover the tracks of other malware or to disrupt the victim's ability to use their asset.

The mechanism that wiper malware employs is overwriting system components, such as the Master Boot Record (MBR) or the Master File Table (MFT).

Several variants of wiper malware were discovered during the Russian invasion of Ukraine in early 2022 on computer systems associated with Ukraine. Named CaddyWiper, HermeticWiper, IsaacWiper, and FoxBlade by researchers, the programs showed little relation to each other, prompting speculation that they were created by different state-sponsored actors in Russia, especially for this occasion. 2022 was named the "year of wipers" due to the large scale of wiper attacks.

Recent examples of this threat in the wild include the following:

- **SwiftSlicer wiper:** According to ESET, this is a wiper written in Go, which was deployed against a Ukrainian organization on January 25th, 2023. It was deployed through Group Policy, which suggests that the threat actors had taken control of the victim's Active Directory environment. A Russian-sponsored APT group is behind SwiftSlicer.
- **CryWiper:** CryWiper was first discovered by Kaspersky this fall, where they say the malware was used in an attack against a Russian organization. CryWiper was first observed in November 2022 and is not related to any wiper families that emerged in 2022. The APT group behind the Cry Wiper is unknown but we can clearly say that it's Ukraine-sponsored, or that the allies of Ukraine are behind the wiper.
- **Azov:** This malware is a wiper instead of ransomware, as was self-announced in October 2022. It is manually written in FASM, unrecoverably overwriting data in blocks of 666 bytes, using multi-threading. Azov was mentioned as the most intriguing wiper of 2022. A Russian-sponsored APT group is behind Azov.
- **Petya:** Petya first emerged in 2016 and quickly gained notoriety for its ability to encrypt entire hard drives, making it particularly destructive. It was recently observed again in September 2022. A Russian-sponsored APT group is behind Petya.

Our recommendations

The following proactive steps are recommended by threat hunters to reduce the threat impact:

Run regular backups

Regularly back up important data. Backing up data is the most effective way to mitigate the impact of disk wipers. Make sure to regularly back up important files to an offsite location or a cloud-based backup service. This ensures that even if a disk wiper attack occurs, you will have a copy of your important data.

Utilize MFA and strong passwords

Use strong passwords and enable Multi-Factor Authentication (MFA) on all accounts, including your operating system and backup systems. This reduces the risk of unauthorized access to your systems and data, which could be used to deploy a disk wiper.

Limit user privileges

Restrict user privileges to minimize the impact of a disk wiper attack. Only grant administrator privileges to trusted users who need them for their job functions. Limiting user privileges reduces the scope of damage that a disk wiper can cause.

Implement network segmentation

Implement network segmentation to limit the spread of a disk wiper to other systems on the network. This involves separating the network into smaller subnetworks or segments, which restricts the ability of a disk wiper to move laterally within the network.

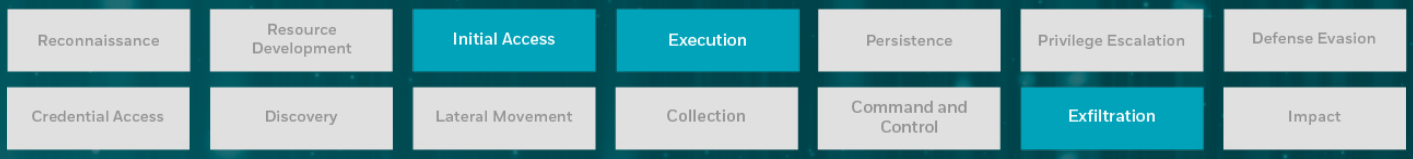
Monitor system logs

Regularly monitor system logs for suspicious activity, such as repeated failed login attempts or unusual file access. This can help identify a disk wiper attack early and allow for a rapid response.

Hunting queries

Hypothesis	Hunting Logics	Defender Query
Attackers can delete critical files or directories on a device	Hunt for deletion of critical files or directories on a device	DeviceProcessEvents | where ProcessCommandLine contains “del /f” or ProcessCommandLine contains “rmdir /s /q” | summarize count() by DeviceName, FileName, ProcessCommandLine
Attackers can delete critical files or the formatting of disks on a device	Hunt for formatting of critical files or directories on a device	DeviceFileEvents | where ActionType ==”FileDeleted” | where InitiatingProcessCommandLine contains “format” or InitiatingProcessCommandLine contains “diskpart” | summarize count() by DeviceName, FileName, InitiatingProcessCommandLine
Attackers can use Cobalt Strike to explore the network by using obscured Base64 encoding and other tricks before deploying the Ryuk payload	Hunt for Cobalt Strike invoked via WMI	DeviceProcessEvents | where Timestamp > ago(7d) | where InitiatingProcessFileName =~ ‘wmiprvse.exe’ | where FileName =~ ‘powershell.exe’ and (ProcessCommandLine hasprefix ‘-e’ or ProcessCommandLine contains ‘frombase64’) | where ProcessCommandLine matches regex ‘[A-Za-z0-9+/]{50,}[=]{0,2}’ | where ProcessCommandLine !has ‘Windows\\CCM\\’ | project DeviceId, Timestamp, InitiatingProcessId, InitiatingProcessFileName, ProcessId, FileName, ProcessCommandLine

6 Social engineering



MITRE ATT&CK tactics leveraged in these types of attacks

Social engineering is a term that refers to tactics that attackers use to manipulate individuals into divulging sensitive information or performing actions that put the organization at risk. There are many different types of social engineering techniques, but some common ones include:

- **Phishing:** This is a tactic where an attacker sends a message, usually through email, that appears to be from a legitimate source (such as a bank or government agency) to trick the recipient into giving away sensitive information or clicking on a link that will install malware.
- **Vishing:** This is a tactic where an attacker uses a phone call - rather than email - to try and trick an individual into giving away sensitive information. Examples of vishing include calls claiming to be from a bank or financial institution, from a government agency, offering a job or a business opportunity, stating to be from a tech support company, or claiming to be from a charity organization.
- **Smishing:** This is a type of social engineering attack that uses SMS text messages to trick individuals into giving away sensitive information or clicking on a link that will install malware. The name "smishing" is a combination of "SMS" and "phishing". For example, baiting is a tactic where an attacker offers a desirable item; pretexting is a tactic where an attacker creates a false identity or scenario; scareware is a tactic where an attacker presents a fake warning; and Quid Pro Quo is a tactic where an attacker offers something of value.

Our recommendations

The following proactive steps are recommended by threat hunters to reduce the threat impact:

Increase threat awareness

We recommend that our customers have employee awareness sessions twice a year.

Protect email accounts

Enable email security products with all additional features such as Spam Filter and Anti-Phishing.

Ensure links are safe

Deploy URL Rewriting to allow redirection to the proxy or a web filtering solution to recheck the link against threat intelligence lists, before allowing a visit.

Extract threats from documents

Deploy Content Disarm & Reconstruction (CDR) to disassemble a document, remove the malicious content, and rebuild the sanitized document to be sent on to the user.

Monitor malicious emails

Deploy Clawback to allow an email to be removed from an Inbox if it is determined to be malicious after it has been delivered.

Analyze suspicious content

Use an email sandbox to upload the email attachments and allow suspicious content to be analyzed within an isolated environment, enabling the detection of malicious functionality without risk to the organization.

Maximize AI technology

The use of AI or Machine Learning (ML) models might be able to classify future content and block malicious content based on patterns and trends in phishing content.

Ship the email logs to the SIEM for detection

Detecting the phishing campaign might assist with reducing the threat level, because the credentials can be reset prior to the attacker taking advantage of the stolen credentials.

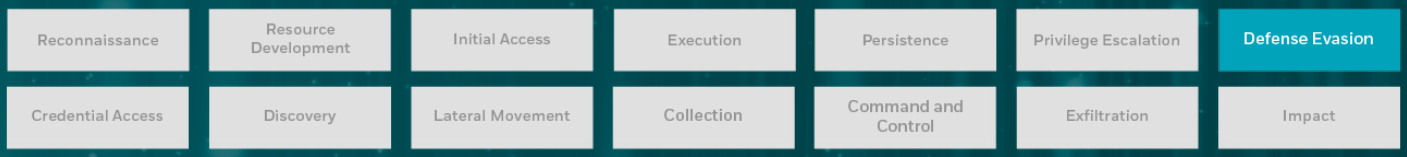
Hunting Queries

Hypothesis	Hunting Logics	Defender Query
Attackers can lure users to click on phishing links in an email	Hunt for URLs redirecting from phishing emails	EmailUrlInfo | where Url matches regex @"s?\:\/\/(?:www\.)?t\.(?:[\w\-\.]+\/+)+(?:r|redirect)\/?\?"

Attackers can redirect users to malicious domains using shorten URL services	Hunt for redirection to shortening URL services	let shortener_domains = dynamic(["bit.ly", "t.co", "ow.ly", "tinyurl.com", "goo.gl", "is.gd", "buff.ly", "adobe.ly", "rebrand.ly", "qr.ae"]);
		let timeWindow = 1d;
		DeviceEvents
		| where Timestamp >= ago(timeWindow)
		| where ActionType == 'BrowserLaunchedToOpenUrl'
		| where RemoteUrl has_any (shortener_domains)
		| summarize Count = count() by RemoteUrl
		| order by Count desc

Attackers can use exploits to extract files from malicious RAR archives	Hunt for files extracting from RAR archives	DeviceProcessEvents | where FileName == "cmd.exe" | where ProcessCommandLine contains @"set path=%ProgramFiles(x86)%\WinRAR;C:\Program Files\WinRAR;" | where ProcessCommandLine contains @"cd /d %~dp0 & rar.exe e -o+ -r -inul*.rar"

7 Bring Your Own Device (BYOD) threats



MITRE ATT&CK tactics leveraged in these types of attacks

BYOD is a policy that allows employees to use their personal devices (such as smartphones, laptops, and tablets) to access company resources, such as email and company data. While BYOD can have many benefits, such as increased productivity and cost savings, it can also pose several security risks.

One of the primary threats of BYOD is that personal devices may not have the same level of security as company-owned devices. This can lead to vulnerabilities in the device that can be exploited by hackers to gain access to sensitive company data. Additionally, personal devices may not have updated software or antivirus protection, leaving them more susceptible to malware attacks.

Another threat of BYOD is the potential for data breaches. Personal devices may store sensitive company data, such as customer information or intellectual property, which could be stolen or compromised if the device is lost or stolen. This can result in significant financial and reputational damage to the organization.

Finally, BYOD can also pose a threat to regulatory compliance. Many industries, such as healthcare or finance, have strict regulations around data privacy and security. If personal devices are used to access or store sensitive information, the organization could be at risk of non-compliance and face significant fines or legal action.

Our recommendations

To mitigate the threats of BYOD, organizations should establish clear policies and guidelines around device usage and security. This could include requirements for antivirus software, regular software updates, and encryption of sensitive data. Additionally, organizations can consider implementing mobile device management (MDM) solutions to help monitor and secure personal devices used for work purposes.

The following proactive steps are recommended by threat hunters to reduce the threat impact:

Manage new device security

Use Network Access Control (NAC) to identify and locate newly added devices to the environment.

Conduct regular vulnerability scans

Regularly scan for vulnerable assets in the environment and update the operating system and other software on these devices.

Implement robust policy

Develop a comprehensive BYOD policy that outlines acceptable use, security requirements, and data management procedures.

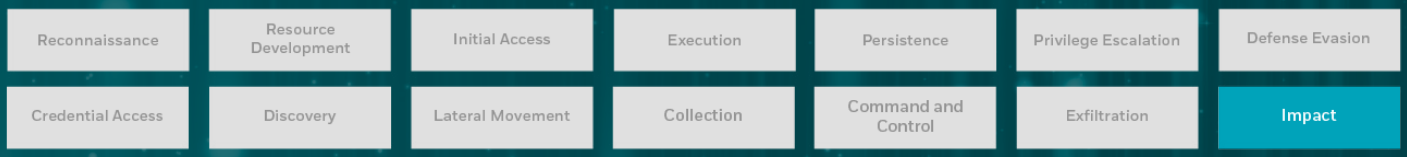
Utilize mobile device security solutions

Organizations should use Mobile Device Management (MDM) solutions to monitor, manage, and secure devices that connect to the network.

Secure and isolate sensitive data

Use containerization to create a secure and isolated environment for sensitive data on personal devices.

8 Internet of Things (IoT) vulnerabilities



MITRE ATT&CK tactics leveraged in these types of attacks

The Internet of Things (IoT) refers to the interconnected network of physical devices, such as smart thermostats and security cameras, for example, that are equipped with sensors, software, and network connectivity, allowing them to collect and exchange data. As the number of IoT devices continues to grow, new vulnerabilities in these devices can have significant impacts.

Some potential impacts of new IoT vulnerabilities include:

- **Data breaches:** If an IoT device is vulnerable to attack, an attacker may be able to access the data being collected and transmitted by the device. This could potentially result in the theft of sensitive information, such as login credentials or financial data.
- **Physical harm:** Some IoT devices, such as connected medical devices or industrial control systems, are used to control or monitor critical infrastructure or processes. If an attacker can exploit a vulnerability in one of these devices, it could potentially result in physical harm to people or damage to equipment.
- **Disruption of service:** An attack on an IoT device could disrupt the normal functioning of the device or the system it is connected to, leading to downtime and reduced productivity.
- **Loss of trust:** If an IoT device is found to be vulnerable to attack, it could damage the reputation of the manufacturer and lead to a loss of trust in their products.
- **Botnet:** A botnet is a network of infected devices that are controlled by an attacker. Botnets can be used to launch cyberattacks, such as distributed denial of service (DDoS) attacks, network flooding, and spreading malware. IoT devices are vulnerable to botnets because many of them have weak security and are easily hackable. For example, outdated software, poorly secured networks, weak passwords, and unsecured communication protocols can all make IoT devices more vulnerable to attack.
- **Covert nation-state activity:** IoT devices can be vulnerable to covert nation-state activity, which refers to the unauthorized gathering of information by a state or other entity. For example, spying on Industrial IoT systems, GPS tracking of IoT devices, remote access to IoT devices, automotive IoT devices, etc.

Our recommendations

The following proactive steps are recommended by threat hunters to reduce the threat impact:

Assess risk

Conduct thorough vendor risk assessments.

Protect data with security controls

Organizations should implement security controls, such as encryption and access controls, to protect the sensitive data that is shared with IoT devices.

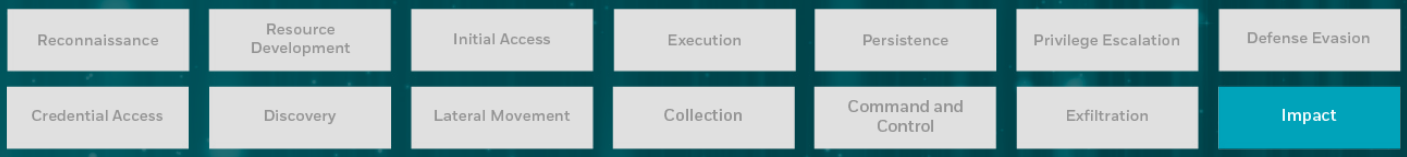
Monitor for signs of attack

Organizations should monitor for unusual activity on their networks - including activity from their IoT devices - to detect any signs of an attack.

Conduct penetration testing exercises

Organizations should conduct regular penetration testing to identify any vulnerabilities in their systems and IoT devices.

9 Insider threats



MITRE ATT&CK tactics leveraged in these types of attacks

Insider threats can come from malicious insiders, such as employees or contractors, who have access to an organization's systems and could intentionally or unintentionally cause harm.

Some examples of insider threats include the following:

- **Malicious insiders:** Individuals who intentionally cause harm to the organization, including stealing sensitive data or sabotaging systems.
- **Negligent insiders:** Individuals who might not intentionally cause harm, but who engage in risky behaviors that put the organization at risk, such as clicking on malicious links or using weak passwords.
- **Human error and non-secured behavior in the cloud:** Individuals who may upload confidential documents to sites like VirusTotal, GitHub, etc.
- **Disgruntled employees:** Individuals who may be unhappy with their job or the organization and take actions that harm the organization, such as leaking sensitive information or sabotaging systems.
- **Contractors or third-party vendors:** Individuals who may have access to the organization's systems or data as part of their work, but don't have the same level of loyalty or commitment to the organization. They could pose a risk if they mishandle sensitive information or if they are targeted by external attackers.

Our recommendations

The following proactive steps are recommended by threat hunters to reduce the threat impact:

Prevent data exfiltration

Organizations should implement data loss prevention (DLP) solutions to detect and prevent the unauthorized exfiltration of sensitive data.

Leverage threat intelligence tools

Use an advanced Cyber Threat Intelligence service to monitor the dark net for stolen or leaked confidential data.

Invest in employee reliability

Organizations should conduct background checks on their employees and contractors to identify any potential security risks.

Be aware of data exfiltration

Hunt for exfiltration of personally identifiable information (PII) data.

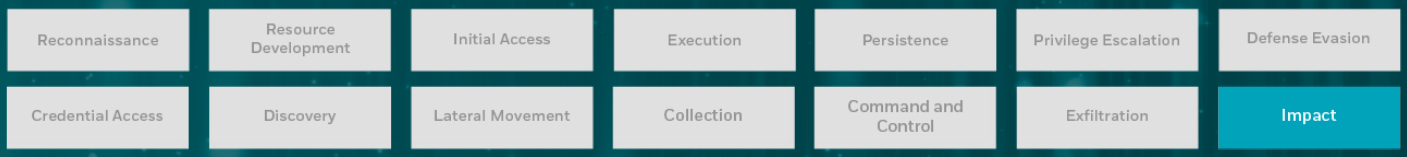
Monitor the public cloud

Monitor all data uploaded to public cloud instances, intentionally or not, such as GitHub.

Hunting queries

Hypothesis	Hunting Logics	Defender Query
Attackers can download confidential information to insecure devices	New USB devices or a smartphone connected to endpoint	DeviceEvents | where ActionType == "PnpDeviceConnected" | extend parsed=parse_json(AdditionalFields) | project Timestamp, DeviceName, DeviceId=tostring(parsed.DeviceId), ClassName=tostring(parsed.ClassName) | where ClassName == "DiskDrive" | summarize UsbFirstSeen=min(Timestamp), UsbLastSeen=max(Timestamp) by DeviceId, DeviceName
Attackers can attempt to access sensitive data	Hunt for users who have accessed sensitive data	DeviceFileEvents | where ActionType == "FileCreated" or ActionType == "FileDeleted" or ActionType == "FileModified" | where FolderPath contains "sensitive_data_folder" // replace with actual folder path | where InitiatingProcessFileName != "svchost.exe" and InitiatingProcessFileName != "System" and InitiatingProcessFileName != "smss.exe" and InitiatingProcessFileName != "lsass.exe" and InitiatingProcessFileName != "csrss.exe" and InitiatingProcessFileName != "wininit.exe" | project Timestamp, DeviceName, RequestAccountName, InitiatingProcessFileName, InitiatingProcessCommandLine, FolderPath, FileName, SHA1, ActionType

10 Operational Technology (OT) attacks



MITRE ATT&CK tactics leveraged in these types of attacks

Operational Technology (OT) security refers to the protection of operational technology systems, devices, and networks used in Industrial Control Systems (ICS). These systems are critical for the operation of industrial processes and are used in the energy, manufacturing, and transportation industries, among others.

OT security is focused on protecting these systems from cyber threats that can cause disruptions, downtime, or even physical damage to industrial processes. This is different from IT security, which focuses on protecting traditional IT systems such as desktops, servers, and databases. An attack on an OT platform can have serious consequences, as OT systems are used to control and monitor critical infrastructure and industrial processes. An attack on an OT platform can potentially result in system downtime, financial loss, environmental and physical damage, or even loss of life.

Some aspects of cybersecurity that are specific to OT systems include:

- **OT/IT convergence:** OT systems are typically designed to operate in isolated environments and are not directly connected to the Internet. In recent years, there has been a trend toward connecting OT systems to the Internet to enable remote monitoring, management, and data analysis. This is often referred to as the Industrial Internet of Things (IIoT) or Industry 4.0.
- **Physical impact:** Unlike traditional IT systems, OT and their components might not be easily replaceable or upgradeable, making it more challenging to address vulnerabilities and prevent cyberattacks. The potential impact of a successful attack on OT systems can be much greater than on traditional IT systems, as it can result in physical damage, safety hazards, and environmental risks.

Our recommendations

The following proactive steps are recommended by threat hunters to reduce the threat impact:

Ensure compliance

Validate that OT systems are working according to compliance setup.

Implement playbooks

Create playbooks for each scenario of system malfunction.

Segment your networks

Implement separate networks for IT and OT systems to reduce the risk of compromise from the IT network to the OT network.

Use encryption

Encrypt sensitive data and communications to protect against unauthorized access or interception.

Prioritization

Organizations should prioritize vulnerabilities based on their criticality and potential impact and consider alternative security measures to mitigate the risks associated with unpatched vulnerabilities.

Conduct regular security assessments

Regularly perform security assessments and penetration testing to identify vulnerabilities and implement remediation.

Implement backup and disaster recovery plans

Have a comprehensive backup and disaster recovery plan in place to ensure the availability of critical systems in the event of a security breach or natural disaster.

Keep up to date with product security updates

Work with OT vendors to understand the security features and capabilities of their products and ensure that they are kept up to date with the latest security patches and firmware updates.

CyberProof®
A UST Company

About CyberProof

CyberProof, a UST company, helps our clients transform their security to a cost-effective, cloud-native technology architecture. Our next-generation Managed Detection & Response (MDR) service is built to support large, complex enterprises by combining expert human and virtual analysts. Our services are enabled by our purpose-built platform, the CyberProof Defense Center – enabling us to be more agile, collaborate better, and deliver powerful analytics. Our integrated security services include Threat Intelligence, Threat Hunting, and Vulnerability Management. Our experts innovate to meet our clients' needs with custom use cases, integrations, and automations.

For more information, visit www.cyberproof.com

Locations
Barcelona | California | London | Singapore | Tel Aviv | Trivandrum