

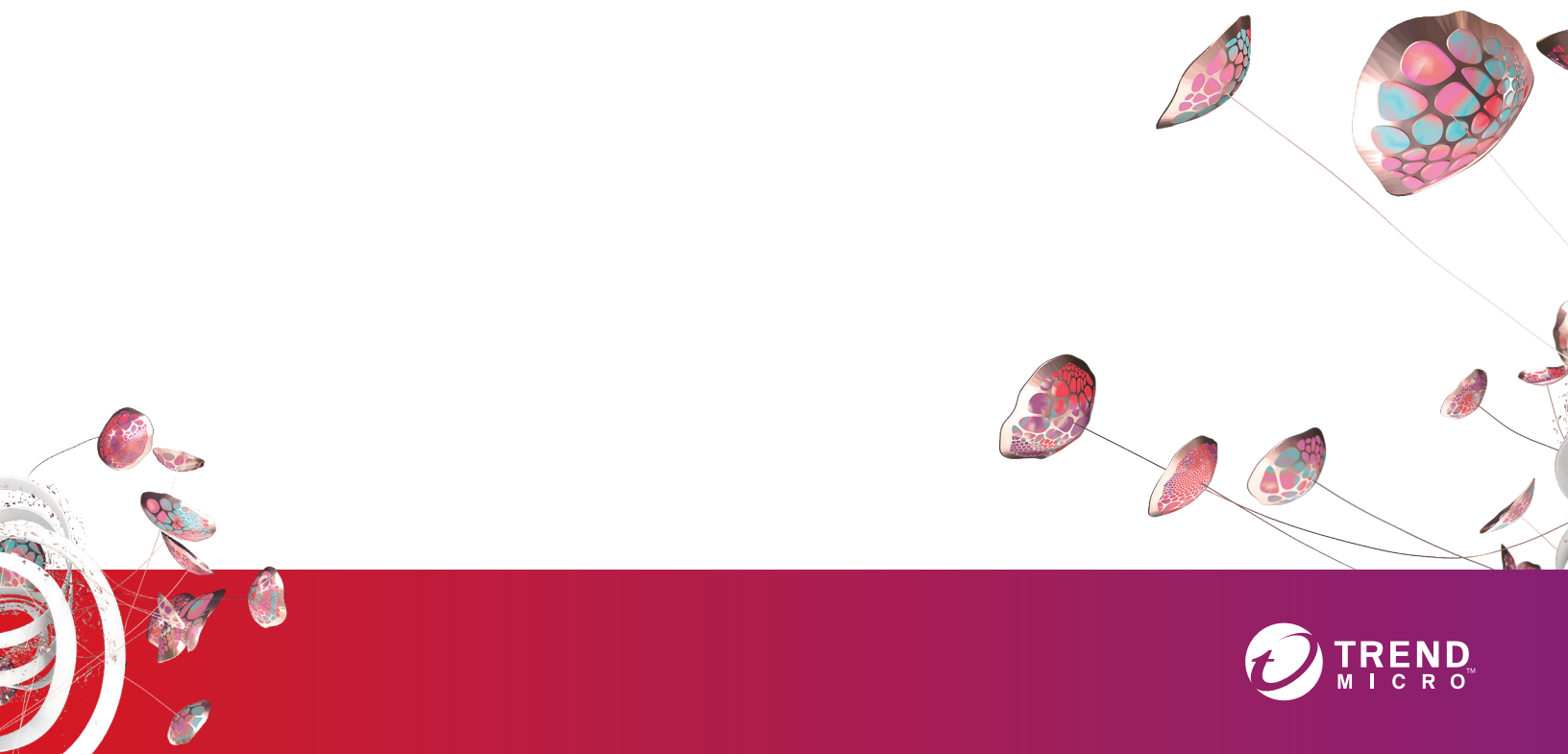
# Securing Your Clients From Modern Ransomware

Fight back as a team



# Contents

- 3** Traditional vs. Modern Ransomware
- 4** Four Stages of Modern Ransomware Attacks
  - 1. Initial access
  - 2. Network reconnaissance and lateral movement
  - 3. Data exfiltration
  - 4. Ransomware deployment
- 9** Disrupt Modern Ransomware
- 10** Ransomware Best Practice Checklist
- 11** Resources



# Traditional Ransomware vs. Modern Ransomware

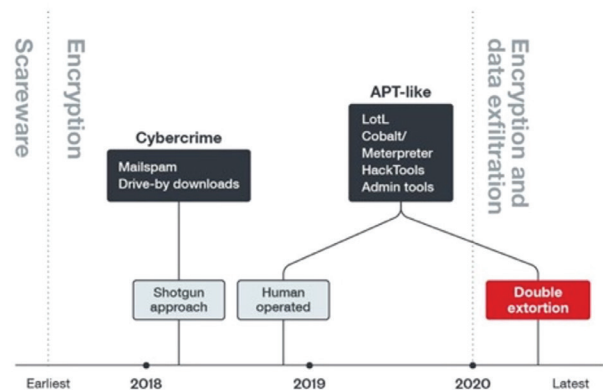
Ransomware is an old but persistently evolving threat that remains a top cybersecurity risk.

Many new ransomware families emerged in 2016, and in 2017 WannaCry wreaked havoc across the globe. In response organizations strengthened their defenses and ransomware notoriety diminished from a hazard to a nuisance.

However, the trend only signified a major turning point for the introduction of modern ransomware.

Ryuk was among the first documented ransomware to operate as modern ransomware. It used Trickbot to propagate using common admin tools for lateral movement. By 2019, ransomware attacks took on a more targeted approach, which has become the norm in the new decade.

Since, we have tracked this continued increase of high-profile attacks including Solarwinds, Colonial Pipeline and Kaseya. Leading to the increased need for SecOps to mandate security across the organization to defend against modern ransomware attacks.



## Traditional Ransomware - Shotgun Approach

**Target:** Single device

**Delivery:** Spam or drive-by downloads

**Impact:** Monetize data of victim

**Disruption:** Localized

**Defense:** Malware prevention and remediation



## Modern Ransomware - Targeted APT-Like Approach

**Target:** Enterprise-wide

**Delivery:** Human operated scripts and malware

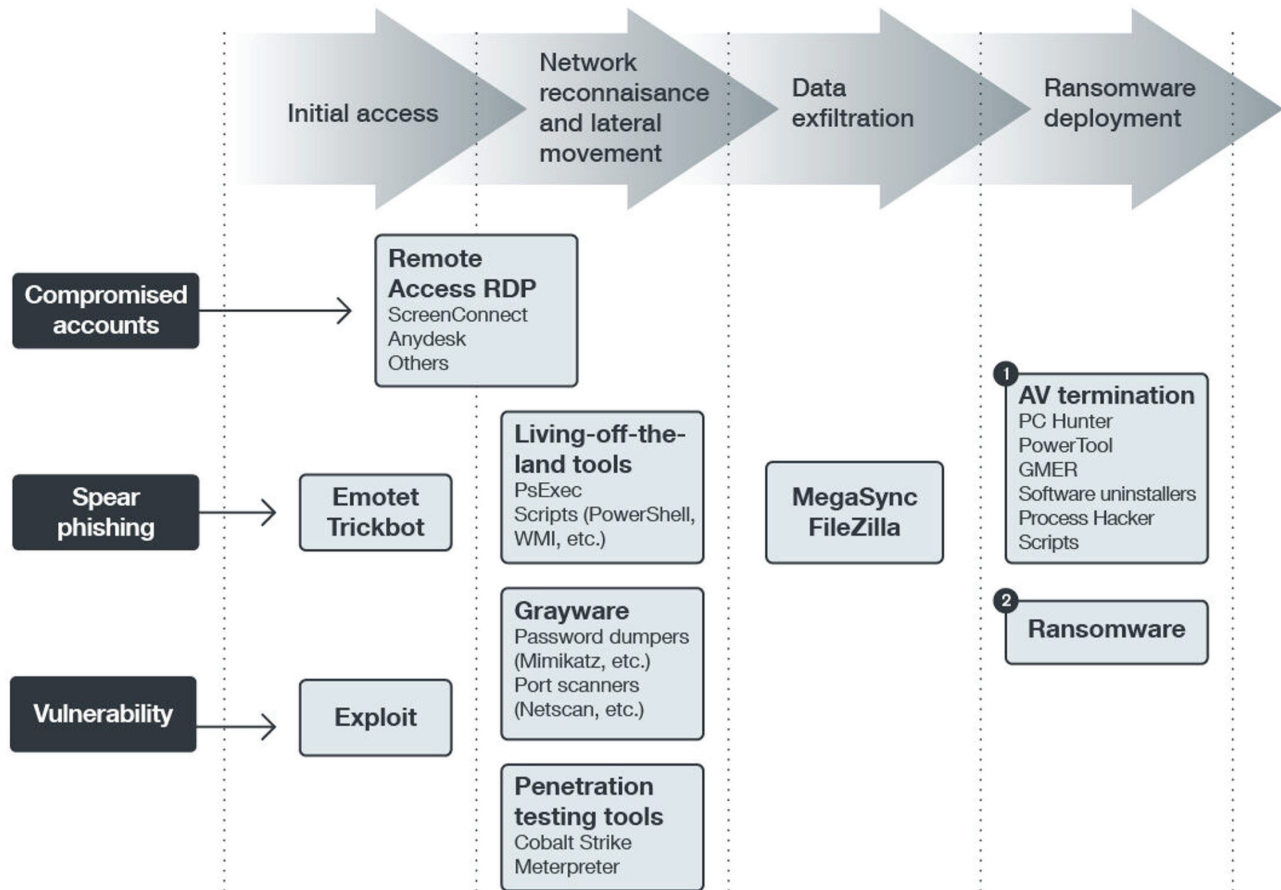
**Impact:** Encryption and data exfiltration

**Disruption:** Enterprise-wide

**Defense:** Layered threat prevention, detection, and response

# Four stages of modern ransomware attacks

To better understand the typical modern ransomware attack process, we break down the stages and components used in today's campaigns.



- 1. Initial access:** Phishing emails, vulnerabilities, or compromised accounts are used to penetrate a system's defense to initiate the attack.
- 2. Network reconnaissance and lateral movement:** Hacking, open-source, and pen-testing tools are used to gain deeper access across the enterprise, building an inventory of the network to spread laterally.
- 3. Data exfiltration:** Before encrypting data, the attacker steals important data that can be used as leverage against the victim. This part is essential for double extortion.
- 4. Ransomware deployment:** With data stolen, running processes, and services are taken down to ensure effective ransomware deployment. Attackers also remove their footprints by deleting event logs. After the files have been encrypted, the operators declare their demands via a ransom note.

# 1. Initial Access

Proactively defending your endpoints and email, and hybrid cloud environments against the very first stage of a ransomware attack is critical.

Trend Micro solutions incorporate a blend of protection techniques to keep the attackers out.



## **Phishing Prevention**

Phishing emails are the most common way ransomware can get into your organization, and Trend Micro™ Cloud App Security is the most effective layer to stop these attacks. Combined with threat intelligence, machine learning, exploit detection, and sandboxing to stop threats before they reach your users.



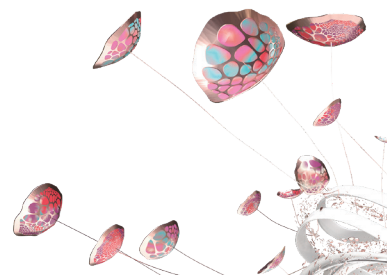
## **Vulnerability Protection**

Virtual patching across endpoints automatically shields systems from new threats and vulnerabilities, minimizing disruptions and ensuring your critical applications and sensitive enterprise data stay protected.



## **Compromised Account**

Increasing the visibility of user behavior is critical in identifying early indicators of a ransomware attack. Trend Micro™ Worry-Free™ XDR allows you to quickly investigate suspicious activities related to users and devices and determine how to mitigate the risks found in your environment.



## 2. Network Reconnaissance and Lateral Movement

Closely monitoring your client's email, users, and endpoint environments to spot abnormal behavior is critical when it comes to this stage of the attack.



### **Network reconnaissance**

Gaining visibility across your client's environment is critical in identifying stealthy/living off-the-land techniques that typically involve the attacker staying longer in the network and systematically enumerating the network.

Trend Micro, assisted with telemetry across endpoints and email, provides critical visibility of attackers that identify early-warning noteworthy events that could lead to a ransomware attack.



### **Lateral Movement**

Lateral movement is a key tactic that allows ransomware attackers to avoid detection by embedding themselves amongst regular traffic deep into the network.

If the threat actors are still living in your network and moving laterally, data correlation across the environment is crucial in connecting the dots and weeding out the attacker before their final steps.



# 3. Data Exfiltration

As is common practice with modern ransomware, critical files are exfiltrated prior to the ransomware being launched for double extortion. This is the riskiest step so far in the ransomware execution process, as data exfiltration is more likely to be noticed by the victim organization's security team. It is the last step before the ransomware is dropped, and the attack often speeds up at this point to complete the process before it is stopped.



## Data Protection

Data loss prevention (DLP) can quickly and easily gain visibility and control of your sensitive data and prevent data loss via your endpoints, SaaS applications, messaging, cloud storage, and web gateways.



## Application Monitoring and Control

Limiting and monitoring the activity of common tools used for data exfiltration can assist in lowering the risk of data leaving your network.

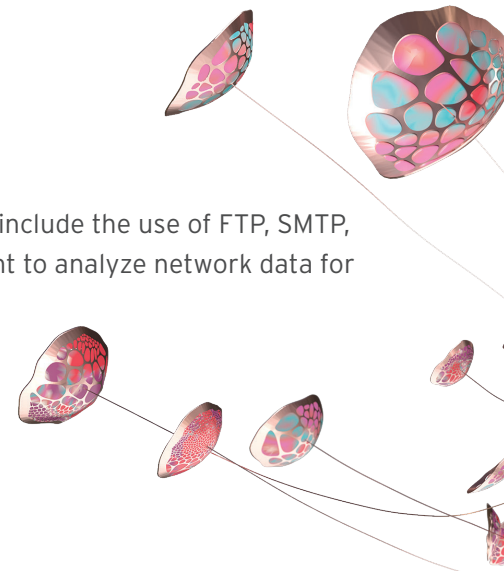
In recent attacks, we have seen the following tools being used:

- Rclone and Mega client: Tools used for exfiltrating files to cloud storage
- 7-Zip: A utility used for archiving files in preparation for exfiltration
- PuTTY: An alternative application used for network file transfer



## Network Monitoring

Adversaries looking to steal data by exfiltration include the use of FTP, SMTP, HTTP/S, DNS, and SMB. Therefore, it is important to analyze network data for anomalies for rapid investigation.



# 4. Ransomware Deployment

Attackers at this stage are now looking to deploy the ransomware. They will first try to disable security defenses, running processes, and services to ensure deployment.

After the files have been encrypted, the operators declare their demands via a ransom note.



## Disabling Security Services

Trend Micro tamper protection control help to ensure critical security services cannot be disabled. Protecting prevention and detection capabilities is imperative when human operators are looking to carry out a modern ransomware attack



## Deployment Detection

Endpoints and workload actively record all system events and behaviors of ransomware deployment, allowing threat investigators to understand the entry, spread, and depth of attacks. Worry-Free XDR can easily generate a root cause analysis of the attack, allowing you to get a complete picture of the incident.



## Ransomware Execution Protection

Trend Micro leverages machine learning for pre-execution and runtime analysis with specific models for different types of files, so you can be assured that, even before you click, we've checked all files to ensure that it exhibits no malicious intent.

Expert rules detect malicious ransomware behavior, blocking threats in milliseconds and killing off encryption processes.

Built-in ransomware rollback automatically create copies of files being encrypted. This offers users an added chance of recovering files that may have been encrypted by a ransomware process.

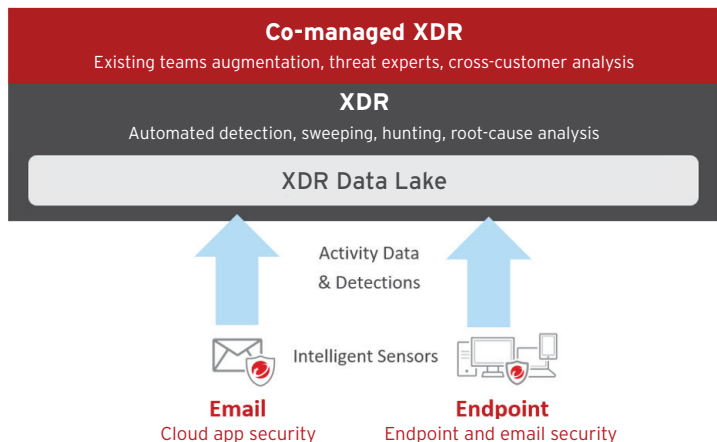


# Disrupt Modern Ransomware.

## A threat operations center to prevent, detect, and respond to ransomware

MSPs can leverage Worry-Free XDR, which collects and correlates data across your customers endpoints and email, to provide better context and enable investigation in one place.

This, in turn, allows teams to respond to similar threats faster and detect advanced and targeted threats earlier in the attack lifecycle, across customer environments.



## Add co-managed detection and response services and receive:

- > 24/7 threat expert monitoring
- > Cross-customer analysis
- > Incident response
- > Monthly case activity summary report

## Disrupt Modern Ransomware with Trend Micro

TREND MICRO MODERN RANSOMWARE DISRUPTION TECHNOLOGIES		Initial Access <i>Compromised accounts - spear phishing vulnerabilities</i>	Network Reconnaissance and Lateral Movement <i>Living-off-the-land tools - Grayware penetration testing tools</i>	Initial Access <i>File upload</i>	Ransomware Deployment <i>Security tool termination ransomware execution</i>
Prevent	Phishing Protection Machine Learning Behavior Analysis Vulnerability Protection	Trend Micro™ Cloud App Security - Email Trend Micro Worry-Free XDR Trend Micro™ Phish Insight™ - Phishing Simulation	Trend Micro Worry-Free XDR	Trend Micro Worry-Free Services	Trend Micro Worry-Free Services
Detect	High Confidence Detection Intrusion Detection Activity Monitoring User Behavior	Cloud App Security - Email Trend Micro Worry-Free Services	Trend Micro Worry-Free XDR	Trend Micro Worry-Free Services	Trend Micro Worry-Free Services
Respond	Infection Identification Hunting and Sweeping Forensic Investigation Mitigation	Trend Micro Cloud App Security - Email Trend Micro Worry-Free XDR	Trend Micro Cloud App Security - Email Trend Micro Worry-Free XDR & Co-Managed XDR	Trend Micro Cloud App Security - Email Trend Micro Worry-Free XDR & Co-Managed XDR	Trend Micro Worry-Free XDR & Co-Managed XDR

Technology control mapping to help you prevent, detect, and respond against ransomware.

# Ransomware Best Practice Checklist

## Audit and inventory

- › Take an inventory of assets and data.
- › Identify authorized and unauthorized devices and software.
- › Audit logs of events and incidents.

## Configure and monitor

- › Deliberately manage hardware and cloud service configurations.
- › Only grant admin privileges and access when necessary to an employee's role.
- › Monitor the use of network ports, protocols, and services.
- › Implement security configurations on network infrastructure devices such as firewalls and routers.
- › Monitor configurations for cloud security posture management.

## Patch and update

- › Perform regular vulnerability assessments.
- › Conduct patching or virtual patching for operating systems and applications.
- › Update software and applications to their latest versions.

## Protect and recover

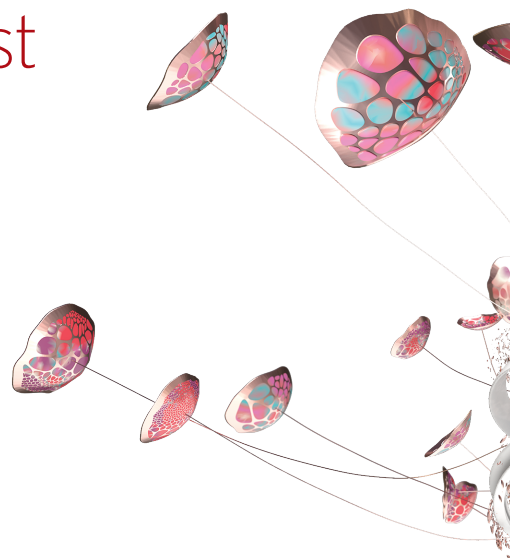
- › Enforce data protection, backup, and recovery measures.
- › Implement multifactor authentication.

## Secure and defend

- › Perform sandbox analysis to examine and block malicious emails.
- › Employ the latest version of security solutions to all layers of the system, including email, endpoint, web, and network.
- › Spot early signs of an attack such as the presence of suspicious tools in the system.
- › Enable advanced detection technologies such as those powered with AI and machine learning.

## Train and test

- › Perform security skills assessment and training regularly.
- › Conduct red-team exercises and penetration tests.



# Resources

## Modern Ransomware's Double Extortion Tactics and How to Protect Enterprises Against Them

Cybersecurity is also evolving constantly and always finds new ways to defend against these persistent threats.

To learn more about modern ransomware, read our [full report](#).



## Trend Micro Worry-Free XDR Trial

[Access within your Trend Micro™ Remote Manager console](#)

## Trend Micro™ Cloud App Security

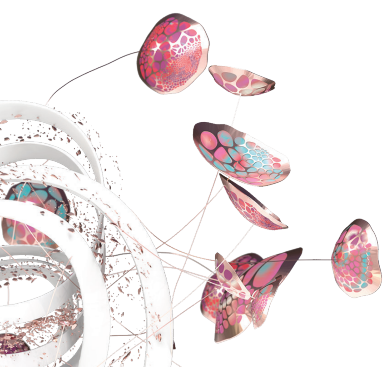
[Access within your Trend Micro™ Remote Manager console](#)

## XDR Customer Value Report

[Included with your Worry-Free XDR Trial](#)

## Trend Micro™ Phish Insight - Phishing

[www.phishinsight.com](http://www.phishinsight.com)



## About Trend Micro

Trend Micro, a global cybersecurity leader, helps make the world safe for exchanging digital information. Fueled by decades of security expertise, global threat research, and continuous innovation, our unified cybersecurity platform protects hundreds of thousands of organizations and millions of individuals across clouds, networks, devices, and endpoints. [TrendMicro.com](https://www.trendmicro.com)