How to Stop Ransomware Attacks

Learn how ransomware works, how three simple steps can stop most attacks, and why legacy security tools just aren't enough

by James Nelson, Vice President of Information Security, Illumio and Ron Isaacson, Field CTO, Illumio

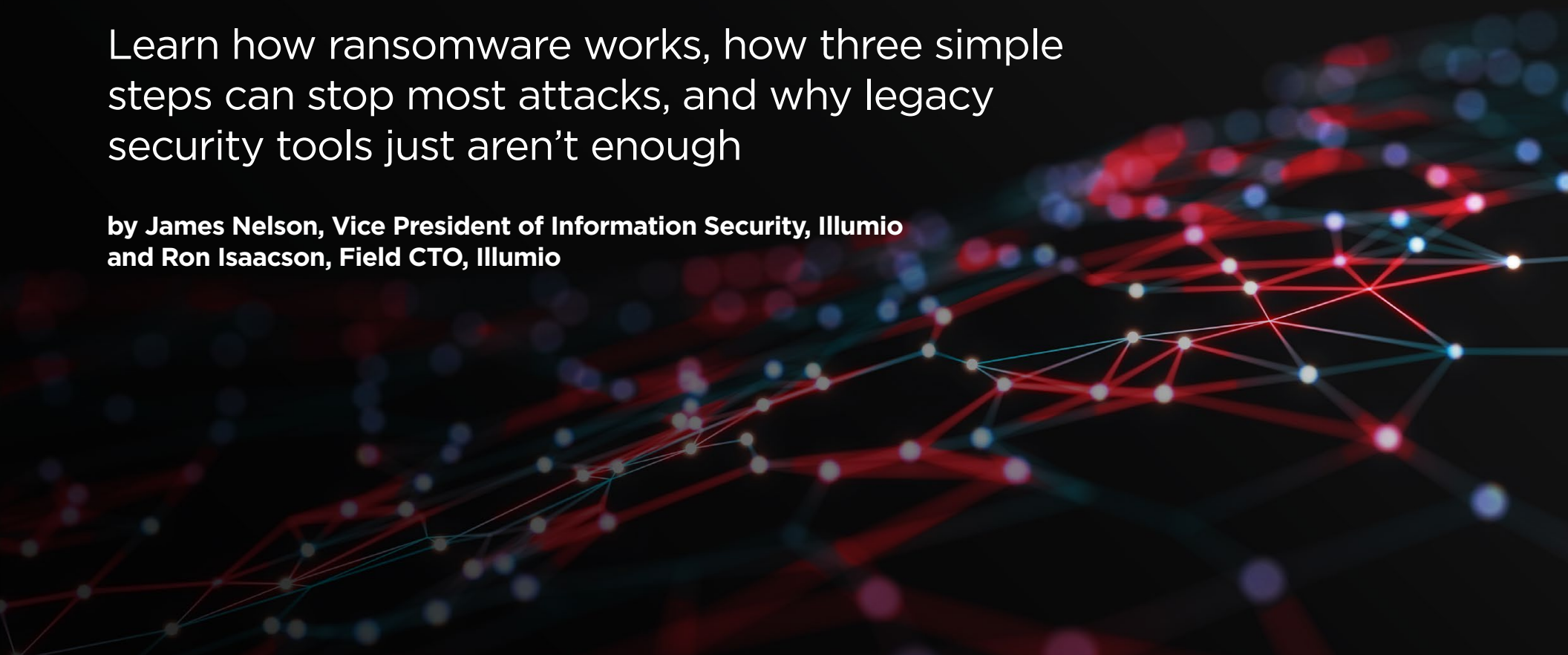# Table of Contents

illumio

Why Ransomware Is Today's Biggest Security Threat

Protecting your critical assets is harder than ever.

Your infrastructure is evolving and becoming increasingly digital, you have dissolved your traditional security perimeter, and you are forced to innovate your operations and environment quickly — even if doing so creates new security risks.

Ransomware takes advantage of these trends. It's designed to infiltrate, spread and compromise assets within modern digital environments. By doing so, ransomware has become the biggest security threat you face today — and it's only growing.

- Since 2016, more than 4,000 ransomware attacks have occurred every day.[1]

- The average ransom request has increased from $5,000 in 2018 to $200,000 in 2020.[2]

- The largest ransom so far is $40 million. It was paid by an insurance company in 2021.[3]

- The largest total damage caused by a ransomware attack was $300 million.[4]

These numbers make one point clear — traditional security architectures are failing to stop the new ransomware threat. Prevention is no longer enough, breaches are now inevitable, and conventional detection and response protocols can't keep up with the speed and scale of today's attacks.

To stop ransomware, you need a new security architecture — and we wrote this ebook to give you just that. To do so, we will:

- Detail the attack pattern that most ransomware follows and provide a three-step framework that counters this pattern to stop ransomware.

- Explain why legacy security tools are failing — and show you how Illumio addresses these problems.

- Break down three recent real-world examples of ransomware and show how organizations could have stopped them with a few small actions.

1. https://www.justice.gov/criminal-ccips/file/872771/download

2. https://www.nsi.org/2021/02/15/employee-cyber-security-awareness-ransomware-wave/

3. https://www.businessinsider.com/cna-financial-hackers-40-million-ransom-cyberattack-2021-5

4. https://www.zdnet.com/article/maersk-forced-to-reinstall-4000-servers-45000-pcs-due-to-notpetya-attack/

illumio

Understanding Ransomware:
How to Stop Most Attacks

You can't stop what you don't understand. In this first section, we'll break down the common attack pattern that most ransomware follows. From there, we'll provide three simple steps you can follow to counter this attack pattern and stop ransomware attacks.

The Most Common Ransomware Attack Pattern

Ransomware variants go by many names. But beneath the surface, most ransomware follows a standard attack pattern built around three common components:

1. It hides in the network and goes undetected for months before striking.

2. It exploits common pathways for initial intrusion and lateral movement.

3. It has to perform multiple actions across multiple stages to achieve its goals.

Let's look at each component of this attack pattern in greater depth.

Component 1: Attacks Go Undetected for Months

Most ransomware attacks are detected only after they've locked down systems, threatened a data dump, and demanded a ransom. Before that moment, they spend as much time as possible silently building their foothold to increase their leverage.

To do so, most ransomware:

- **Exploits assets that organizations don't know they have.** Most attacks initially breach an unknown "invisible" device, application or workload with an open connection to the Internet and other assets on the network.

- **Travels pathways that organizations don't know are open.** Most attacks move through noncompliant data flows, excess application communications, and other commonly open and unnecessary sources of security risk.

- **Leaves hard-to-follow trails of risk data.** Most attacks compromise multiple systems that span multiple functions, making it difficult for admins to correlate the attack's activity and realize it all adds up to a single incident.

Component 2: Attacks Exploit Common Pathways

Most ransomware attacks take the easy route into and through their targets. Recent research finds that more than 80% of ransomware attacks succeed with fundamental tactics such as exploiting software vulnerabilities, misconfigurations or user errors.[5]

To do so, most ransomware:

Targets a small set of high-risk pathways. Most attacks exploit applications such as Remote Desktop Protocol (RDP) and Server Message Block (SMB), which are widely used, often misconfigured, usually span the entire environment, and which attackers can easily map to find the straightest line to their objectives.

Automatically scans the Internet for open ports. Most attacks are opportunistic, not targeted — attackers use scripts and crawlers to broadly search the web for exploitable assets and then just breach whatever entry points they find.

Spreads very quickly once it lands. Most attacks can ride these pathways to compromise every system in an open environment within just a few minutes, and force organizations to shut down their network to stop an in-progress attack.

5. https://www.zdnet.com/article/ransomware-these-are-the-two-most-common-ways-hackers-get-inside-your-network/

illumio

Component 3: Attacks Are Multistage

Most ransomware attacks start by breaching a low-value asset that can be easily compromised. They must complete many more stages of action before they can compromise a valuable asset, build real leverage, and ensure a ransom payment.

To do so, most ransomware:

- **Targets high-value assets as the end goal.** Most attacks gain little value from their initial entry point. Instead, they compromise a low-value asset in their initial breach, then gradually work their way to compromise higher-value assets in the network.

- **Connects to the Internet to advance its attack.** Attackers usually need to pull down tools from an external server to take the next steps in their attack, and they always need to actually exfiltrate (i.e., steal) the sensitive data they access.

- **Causes most of its damage through lateral movement.** To build leverage and ensure their ransom is paid, attackers must move beyond their initial intrusion point to compromise as many systems and as much data as possible.

Most ransomware attacks take advantage of an organization's poor visibility, poor policy controls and poor segmentation. Once you understand this, the new security architecture that can stop this threat comes into focus.

How to Stop This Attack Pattern With Three Simple Steps

Stopping most ransomware is simpler than you think. Take the above attack pattern and counter each of its components following these three steps:

1. Develop comprehensive visibility of communications flows across your entire environment.
2. Block common ransomware pathways to limit intrusions, mitigate in-progress attacks, and build overall resilience to ransomware.
3. Segment your environment to isolate high-value assets.

Let's look at each in greater depth.

Step 1: Develop Comprehensive Flow Visibility

With the right visibility, ransomware attacks will have nowhere to hide. You will gain access to the data you need to either detect attackers when they first breach your environment, or early enough to eliminate them before they build a harmful foothold.

To do so, you must:

- **Develop real-time visibility into all assets and communications.** When you know what assets you have in your network and how they are communicating, you can rapidly identify and address unessential or anomalous data flows.

- **Identify the unnecessary security risks in your environment.** Build a real-time map of your environment. That way, you can understand which of your workloads, applications and endpoints need to be open and which can be closed.

- **Centralize and correlate multiple sources of risk data.** Create a unified view of communication flows that your NetworkOps, SecurityOps, DevOps and DevSecOps teams can work from. This will reduce internal friction while helping your teams identify complex incidents.

Step 2: Develop Ransomware-Blocking Capabilities

To prevent most ransomware attacks — and to limit the potential damage from any incident you do suffer — you must eliminate the low-hanging fruit in your environment.

- **Restrict and monitor high-risk pathways.** Close as many high-risk pathways as possible, and then establish real-time monitoring over those pathways that must be left open.

- **Maintain good IT hygiene.** Specifically, close ports that don't need to be open. This will decrease your attack surface and lower your chances of being found and exploited by an attacker's automated scans.

- **Create a reactive emergency containment switch.** Establish a set of restrictive security policies that can be launched in seconds to lock down as much network communication as possible to stop an in-progress incident.

illumio

Step 3: Isolate Critical Assets

Finally, you must limit an attack's ability to spread from one system to the next. This will prevent attackers from compromising your critical assets, frustrate them at each stage, and force them to take bolder (and therefore easier to detect) actions to try to progress their attack.

To do so, you must:

- **Isolate and protect high-value assets.** Create barriers around individual applications ("ring-fencing") to separate them from each other and to prevent high-value assets from being compromised during an incident.

- **Close outbound connections to unknown, untrusted IPs.** Create an "allowlist" of the IP addresses your assets must connect with. Then block the rest, especially IPs commonly used in incidents, such as MegaUpload.

- **Develop post-intrusion security to contain in-progress attacks.** Build security that, after a breach, will contain attacks, stop them from spreading past their intrusion point, and limit the assets and data they can compromise.

To stop most ransomware, focus on building your visibility, policy controls and segmentation. By doing so, you will create a new security architecture that can counter most ransomware's every move.

Most Ransomware Attacks	How to Stop Them
Go Undetected for Months • Exploit assets that organizations don't know they have. • Travel pathways that organizations don't know are open. • Leave hard-to-follow trails of risk data.	**Develop Visibility Into Communication Flows** • Develop real-time visibility into all assets and communications. • Identify (and fix) the unnecessary security risks in your environment. • Centralize and correlate multiple sources of risk data.
Exploit Common Pathways • Target a small set of high-risk pathways. • Automatically scan the Internet for open ports. • Spread quickly once they land.	**Block Common Pathways** • Restrict and monitor high-risk pathways. • Maintain good IT hygiene. • Create a reactive emergency containment switch.
Need Multiple Stages to Achieve Goals • Target high-value assets as their end goal. • Connect to the Internet to advance their attack. • Cause most of their damage through lateral spread.	**Protect Critical Resources** • Isolate high-value assets. • Close outbound connections to unknown, untrusted IPs. • Develop post-intrusion security to contain in-progress attacks.

illumio

A New Approach for a Growing Threat

Establishing a security architecture to stop ransomware may be a challenge for organizations that rely on legacy security tools. In this section, we'll explore why these tools fail to create strong visibility, policy controls and segmentation. Then we'll outline how to easily build this new architecture and stop ransomware with Illumio.

Why Legacy Tools Fail to Stop Ransomware

Historically, organizations secured their networks with manual firewall and segmentation tools. Because these tools were created decades ago, they were designed to secure an older technology environment. Also, they often fail to create a modern security architecture that defends today's large, distributed and dynamic networks.

Why Legacy Tools Fail to Deliver Real-Time Visibility

Legacy IT visibility and observability tools were not designed to create an accurate picture of the complex maze of communications going into and out of applications. And it's precisely this maze that most ransomware exploits.

Most legacy tools:

- **Can't map many asset connections and communications.** They can't see and understand devices, applications and workloads, and typically they do not collect data on their inbound and outbound communications.

- **Don't identify necessary or unnecessary risk.** Because legacy tools were not built to capture risk data, they often leave internal teams in the dark. Organizations with legacy tools typically don't know which risks they carry, which risks they could eliminate, or which risks must remain open.

- **Leave risk data scattered and create internal silos.** Legacy tools separate monitoring from policy creation, forcing teams to waste time trying to correlate data across systems and departments.

Why Legacy Tools Fail to Block Ransomware

Legacy firewall management tools force you to follow manual processes. Because these processes cannot manage security policies at scale, they often create large attack surfaces filled with easy-to-exploit pathways.

Most legacy tools:

- **Don't identify high-risk pathways.** They cannot create a centralized view of commonly exploited pathways or lingering technical debt, and they don't identify which assets are actively communicating to high-risk services.

- **Struggle to maintain hygiene.** Legacy tools do not help to prioritize preventive action. Also, they require significant amounts of manual, prerequisite actions to make even small policy changes that reduce the network's attack surface.

- **Cannot quickly shut down environments.** These tools have no way to rapidly close compromised ports and network connections without either impacting other important security policies or harming business operations.

Why Legacy Tools Fail to Isolate Critical Assets

Legacy segmentation tools typically require multiyear journeys to create and enforce enterprise-wide policies. What's more, the policies they do create are often fragile, cannot handle changes in the environment, and require constant, costly maintenance.

Most legacy tools:

- **Require high levels of effort to close and manage ports and vectors.** They do not provide scalable, policy-based workflows, making it impossible to efficiently manage firewalls for complex enterprise networks.

- **Drop policy enforcement as IP addresses change.** While they attach security policies to a device's IP address, in today's dynamic environments a device's IP address can rapidly change and detach its security policies.

- **Are physical in-line solutions.** Legacy tools use their own firewalls, which

illumio

can fail, lower defenses or harm operations. Also, they have to physically move cables or change virtual infrastructure every time they establish or tweak a boundary.

Legacy security tools cannot provide the visibility, policy control or segmentation that organizations need to stop most ransomware attacks.

Fortunately, we built Illumio to address each of these problems.

How Illumio Works Where Legacy Tools Fail

Illumio is a modern workload and endpoint security solution. It provides streamlined, scalable policy management, making it easy to build a new security architecture that stops most ransomware attacks.

Illumio Delivers Comprehensive Visibility

Illumio gives you actionable insights in minutes by automatically mapping all communications among assets, including clouds, containers, data centers and endpoints. And it does this without touching or changing your network.

With Illumio, you will:

- **Build full real-time network visibility in as little as an hour.** You will automatically map the internal communications and outbound Internet connections for each of your devices, applications and workloads.
- **Lower operational risk by identifying unnecessary connections.** You'll build a clear picture of your vulnerable systems, noncompliant data flows, and excessive communications. You'll gain a better understanding of what's open and why.
- **Create a unified view of your application communications for your teams and your SIEM/SOAR tools.** You will create tight collaboration, offering customized views for Network Ops, Security Ops, DevOps and DevSecOps and feeding real-time data to your SIEM or SOAR.

Illumio Blocks Ransomware

Illumio immediately shrinks your attack surface by automating workflows — like policy discovery, authoring, distribution and enforcement — that block network communications on any high-risk port in your entire global network.

With Illumio, you will:

- **Pinpoint your critical sources of ransomware risk.** You'll see all of your commonly exploited pathways, lingering technical debt, and data flows that are out of compliance with your existing security policies.
- **Proactively close and monitor high-risk pathways.** You will close every highly connected, peer-to-peer, or commonly exploited port in your environment that can be closed. And you'll monitor those ports that must remain open.
- **Create a reactive containment switch to stop in-progress incidents.** You will develop a one-click solution that can precisely block communications down to the workload level, isolating and protecting unaffected systems during an incident.

> Illumio gives you actionable insights in minutes by automatically mapping all communications among assets, including clouds, containers, data centers and endpoints. And it does this without touching or changing your network.

illumio

Illumio Isolates Critical Assets

Illumio gives you an end-to-end Zero Trust segmentation solution. It allows only necessary communications, eliminates east-west paths that allow lateral movement, and enforces and maintains policy within large, rapidly changing environments.

With Illumio, you will:

- **Easily segment assets, environments, users and groups.** You will segment your environment in minutes through data-driven policy design, automatic policy creation, and scalable enforcement using your existing infrastructure.

- **Enforce policies dynamically to consistently secure evolving applications and networks.** You will write simple rules — for example, ordering systems can talk only to payment systems — and policies will automatically update as systems change.

- **Operate at the host level.** You will manage existing host-based firewalls that fail safe, scale easily, and can be managed from a single console. And you'll do all this without moving cables or changing your virtual infrastructure.

Illumio stops ransomware in ways that legacy security tools simply cannot. With Illumio, you will reduce your attack surface, limit the blast radius of a successful breach, and protect your most sensitive data, applications and assets.

Stopping Ransomware With Legacy Tools	Stopping Ransomware With Illumio
Visibility With Legacy Tools • Can't map many asset connections and communications. • Can't identify necessary or unnecessary risk. • Leaves risk data scattered and create internal silos.	**Visibility With Illumio** • Builds full real-time network visibility in as little as an hour. • Lowers operational risk by identifying unnecessary connections. • Creates a unified view of your communication flows for your teams.
Blocking With Legacy Tools • Can't identify high-risk pathways. • Struggles to maintain enforcement policies. • Cannot quickly shut down environments.	**Blocking With Illumio** • Pinpoints your critical sources of ransomware risk. • Proactively closes and monitors high-risk pathways. • Creates a reactive containment switch to stop in-progress incidents.
Segmentation With Legacy Tools • Requires high levels of effort to close and manage ports and vectors. • Drops policy enforcement as IP addresses change. • Uses physical in-line solutions.	**Segmentation With Illumio** • Easily segments assets, environments, users, and groups. • Enforces policies dynamically alongside evolving networks. • Operates at the host level.

illumio

How Illumio Stops Ransomware:
Three Recent Examples

Ransomware makes headlines almost every day. But as Gartner notes, at least 90% of these incidents are preventable.[6] To substantiate this point, and to show how effectively the new security architecture can stop ransomware, we will break down three recent examples of high-impact incidents. For each, we'll show:

- What the attack is.
- How it works.
- How to stop it.
- How Illumio can help.

How Illumio Can Stop Ransomware That Exploits RDP

Nearly a million attacks against Microsoft Remote Desktop Protocol (RDP) servers are launched every day, and these attacks are often cited as "the most common target for many ransomware operators".[7, 8]

What It Is

This attack pattern exploits RDP servers that are exposed to the Internet. RDP runs on every Windows server, and it connects many services and users across the network. Because RDP is so ubiquitous and so connected, it has become the most common starting place for ransomware attacks, and it's a big source of risk for most organizations.

How It Works

RDP lets a user log into a remote computer, commonly on port 3389. An attacker will first scan its target organization (or the Internet) for a Windows server with a public IP address and an open port 3389.

Often, the target organization doesn't even know its Windows servers are exposed to the Internet. And once the attacker finds one or more servers to exploit, it will typically be able to compromise those servers through one of two tactics:

It will exploit known vulnerabilities or Zero Day threats found within Microsoft's security model. These vulnerabilities have included flaws that allow attackers to use RDP to bypass two-factor authentication, methods that let hackers execute malware directly through an RDP connection, and small bugs like BlueKeep that have exposed a million machines at a time.[9, 10, 11]

2. It will perform a brute force attack, such as trying to find an admin account with a weak, popular password. To avoid detection and increase the chance of success, these attacks are now moving slower, with criminals trying only a few combinations per hour over the course of days or weeks.[12]

Once the attacker compromises a single server, it can perform a simple pattern to compromise other assets and data. With reconnaissance, it can find additional exploitable assets in the network. It can then move laterally to those assets and expand its foothold. Then it can perform additional reconnaissance to find new exploitable assets from its new position. This cycle can be repeated until the attacker has built a large enough footprint — and compromised enough high-value assets and data — to lock up systems, threaten a data dump, and credibly demand a large ransom.

6. https://www.gartner.com/smarterwithgartner/5-must-read-ransomware-and-cybersecurity-articles

7. https://threatpost.com/millions-brute-force-attacks-rdp/155324/

8. https://www.group-ib.com/resources/threat-research/ransomware-2021.html

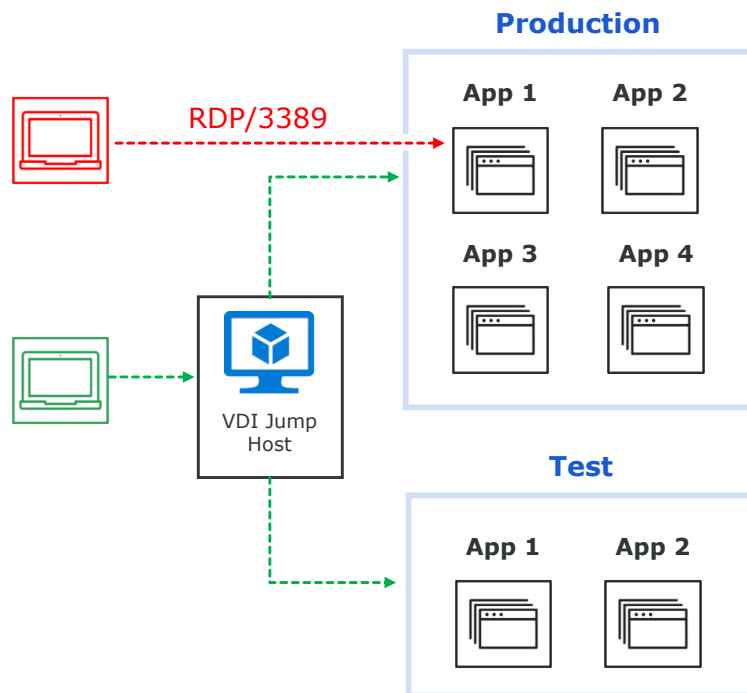9. https://www.bleepingcomputer.com/news/security/remote-desktop-zero-day-bug-allows-attackers-to-hijack-sessions/

10. https://www.securitynewspaper.com/2020/04/23/zero-day-for-any-windows-how-to-exploit-microsofts-remote-desktop-protocol-rdp-using-dll-side-loading-no-patch-available/

11. https://threatpost.com/one-million-devices-open-to-wormable-microsoft-bluekeep-flaw/145113/

12. https://www.zdnet.com/article/microsoft-rdp-brute-force-attacks-last-2-3-days-on-average/

illumio

How to Stop It

Organizations can stop this attack by simply knowing where they have RDP servers exposed to the Internet, identifying which of their RDP connections are unnecessary, and then restricting those connections as much as possible. Specifically, they should block port 3389. Doing this will reduce the organization's attack surface, lower its intrusion points, and limit the potential for lateral spread via RDP connections.

How Illumio Can Help

With Illumio, you can stop ransomware attacks that exploit RDP by:

- Mapping all RDP servers and connections
- Identifying both essential and nonessential connections
- Rapidly deploying policy to restrict communications at scale

How Illumio Can Stop Ransomware Used by the Clop Gang

Early in 2021, the Clop ransomware gang claimed to have completed a successful breach, stealing files from the prominent law firm Jones Day. The Clop gang then demanded a ransom and threatened to publish those files on the dark web if their terms were not met.[13]

What It Is

This incident demonstrates the evolving nature of ransomware and how to stop it. In the past, a ransomware gang would compromise an organization, encrypt its data, and demand a ransom for the encryption key. If the target organization had good data backups, it could simply restore those backups to mitigate the attack.

But now, ransomware gangs like Clop are exfiltrating data and threatening to release it if their demands are not met. This new pattern cuts to the heart of organizational risk — especially when the target organization loses both its own sensitive data as well as its clients' sensitive data, as was the case for Jones Day.

How It Works

This attack pattern exploits Active Directory (AD) misconfigurations and compromises AD accounts with domain privilege access. With this access, the attacker can perform a wide range of actions, including:[14]

- Executing remote commands — like WMI and PowerShell scripts — through remote control malicious code on both the compromised asset and other systems connected to it through AD.

- Ensuring persistence by creating new accounts, creating or modifying system processes, and automatically executing commands or initializing scripts on a compromised asset's boot or logon. These policies can be simultaneously distributed to every asset connected through AD.

13. https://www.wsj.com/articles/hacker-claims-to-have-stolen-files-belonging-to-prominent-law-firm-jones-day-11613514532
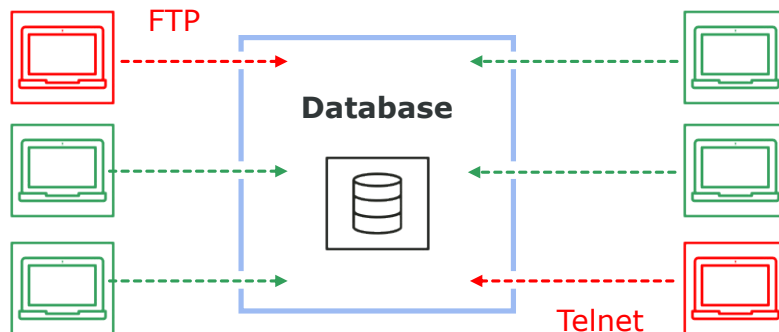
14. boho.or.kr/filedownload.do?attach_file_seq=2808&attach_file_id=EpF2808.pdf

To perform these and other related actions, the attack must connect back to the Internet to pull down additional tools needed to progress the attack, and to actually exfiltrate the data that it accesses and compromises.

Finally, it's important to note that Jones Day denied it was breached. Instead, it said the breach had affected a file-sharing company that it used. This highlights the ransomware vulnerabilities opened by software supply chains (more on this later).

How to Stop It

Organizations can stop this attack by removing domain privilege access from AD accounts that don't need it, and by restricting other common pathways this attack pattern might exploit (including WinRM, NetBIOS and SMB).

How Illumio Can Help

With Illumio, you can stop ransomware used by the Clop gang by:

• Mapping all AD instances and connections

• Identifying essential inbound/outbound connections

• Rapidly deploying policy to restrict communications at scale

How Illumio Can Stop Ransomware Used by the REvil Gang

In April 2021, the REvil ransomware gang compromised Quanta Computer, a company that assembles devices for Apple. When Quanta declined to pay the ransom, REvil asked Apple to pay the ransom instead, and it also threatened to release Apple's sensitive IP — such as laptop diagrams — that the gang had acquired by hacking Quanta.[15]

What It Is

This incident highlights the main security challenges created by today's complex supply chains. First, it shows that a gang might target your company to reach one of the organizations you serve. Second, it shows that even if you have your own security in line, your data is only as safe as your least-secure partner.

How It Works

The attack pattern used by REvil exploited a vulnerability in Oracle WebLogic software. With this particular vulnerability, an attacker can force a vulnerable server to download and execute the malware without any user action. More specifically, it:[16]

• Made an HTTP connection to an unpatched WebLogic server, then forced it to download the "Sodinokibi" ransomware variant. The attackers used a PowerShell command to download a file named "radm.exe" from malicious IP addresses, and then forced the server to save the file locally and execute it.

• From there, the attack attempted to encrypt data in the user's directory, and to hamper data recovery by deleting "shadow copies" of the encrypted data that Windows automatically creates.
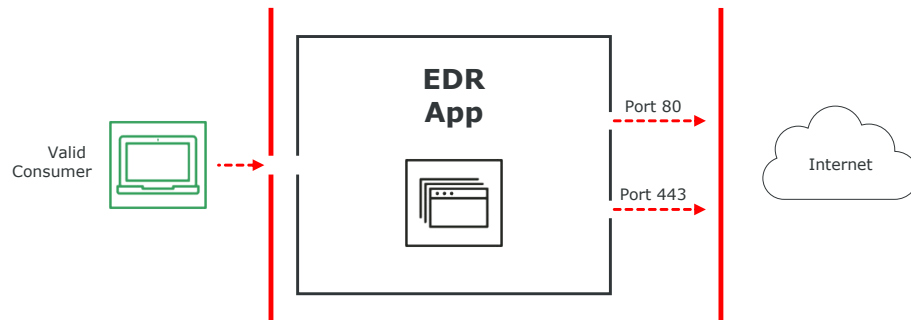
15. https://www.economist.com/business/2021/04/29/a-ransomware-attack-on-apple-shows-the-future-of-cybercrime

16. https://blog.talosintelligence.com/2019/04/sodinokibi-ransomware-exploits-weblogic.html

illumio

While there are a few unique elements to this variant, ultimately this is a broadly applicable attack pattern that can exploit any vulnerable, outward-facing software or service. Variations on this pattern were used in other high-profile incidents, including the Microsoft Exchange and SolarWinds breaches.

How to Stop It

Organizations can stop this attack — and similar patterns — by first understanding that ransomware can be delivered through "trusted" channels, including legitimate third-party software. At the very least, organizations must segment their Commercial Off the Shelf (COTS) solutions to protect the rest of their environment from vulnerabilities — especially security solutions such as EPP, EDR and XDR.
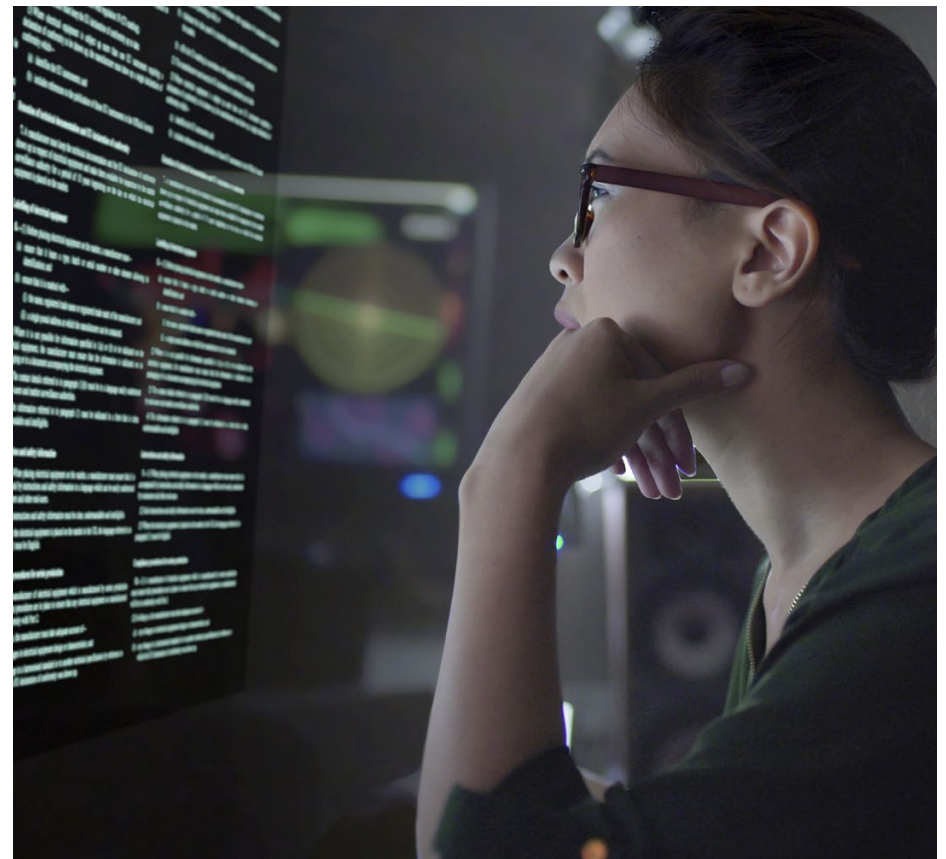

In addition, organizations must identify and restrict nonessential outbound connections to stop this attack pattern's progression. To do this, they must block untrusted Internet-facing connections (including on ports 80/tcp and 443/tcp), except to authorized destination IPs.

How Illumio Can Help

With Illumio, you can stop ransomware attacks used by the REvil gang by:

- Mapping essential and nonessential outbound connections
- Rapidly deploying policy to restrict communications at scale
- Monitoring outbound connections that can't be closed

illumio

Real-World Results: Better Visibility, Better Control, Better Security

Illumio is used by many of the world's largest and most innovative organizations to stop ransomware. With Illumio, they gain visibility of their communication flows and a clear understanding of their riskiest pathways, with full segmentation control down to the application level.

Illumio currently protects assets for:

- More than 10% of the Fortune 100
- 6 of the 10 largest global banks
- 5 of the leading insurance companies
- 3 of the 5 largest enterprise SaaS companies

Our customers also use Illumio to build fundamentally stronger security postures that defend against a wide range of attacks.

- An e-commerce site used Illumio to secure 11,000 systems in 3 months — and successfully pass a critical audit.
- A leading SaaS platform uses Illumio to secure 40,000 systems under full DevOps automation, including policy and enforcement.
- A large custodial bank uses Illumio to isolate $1 trillion per day of financial transactions under federal regulatory scrutiny.

Here's What Customers Say About Illumio

"With Illumio, we know exactly what is talking to what. No one wants to be the company that gets breached. But if that happens, we have peace of mind that the breach will be contained."

**Nathan Powell,
IT Operations Manager, Investa**

"Given the complexity of a highly fragmented network, Illumio provides unparalleled and practical traffic transparency. This allows us to manage all traffic and to quickly discover misconfigurations and malicious activity."

**Thomas Vavra,
Manager of Communication Networks, Mondi**

"Gaining live visibility into flows between workloads down to the paths of protocols provided immediate value. Illumio's simple yet powerful graphical map gave us visibility that we never had before."

**Mikael Karlsson,
Head of IT Infrastructure,
AFA Försäkring**

illumio

Stop Your Biggest Security Threats, Today and Tomorrow

Illumio stops most ransomware attacks by countering common attack patterns.

- **Creates visibility** into all appplication communications for all teams. It also provides an actionable picture of enterprise-scale environments.

- **Blocks and contains ransomware** by proactively closing high-risk pathways and reactively shuttering environments in seconds during incidents.

- **Isolates critical assets** and builds scalable, persistent Zero Trust segmentation across modern diverse, dynamic and distributed environments.

And by doing so, Illumio stops more than just ransomware. Illumio also creates a fundamentally mature and effective security posture that can stop a wide range of common attack patterns. Illumio prepares you for today's biggest cybersecurity threats — whatever they may be.

Learn How Illumio Helps Stop Ransomware

Contact us today to speak with our security experts and arrange your demo of the Illumio product suite.

illumio