HUNTRESS

AKITA

RANSOMWARE PREVENTION GUIDE

A practical guide for spotting the subtle warning signs before the ransom note appears

TABLE OF CONTENTS

```
alert: rat_activity == TRUE
origin: rdp/rmm | svc-backup
defender_state: TAMPERED
```


Stop Ransomware Before it Interrupts Everything — 3

Ransomware is a Business. And it Profits off Your Misfortune. — 4

The Anatomy of a Ransomware Attack — 7

Warning Signs to Watch — 9

Your Ransomware Prevention Toolkit — 11

Stop Ransomware Before the Clock Starts — 17

About Huntress — 18

HUNTRESS

STOP RANSOMWARE BEFORE IT INTERRUPTS EVERYTHING

Ransomware always seems to arrive at the worst possible moment. It hits when your team is slammed, when production is running, when customers are waiting, or when patients need care. Encryption causes the damage, but the interruption is what throws your business sideways.

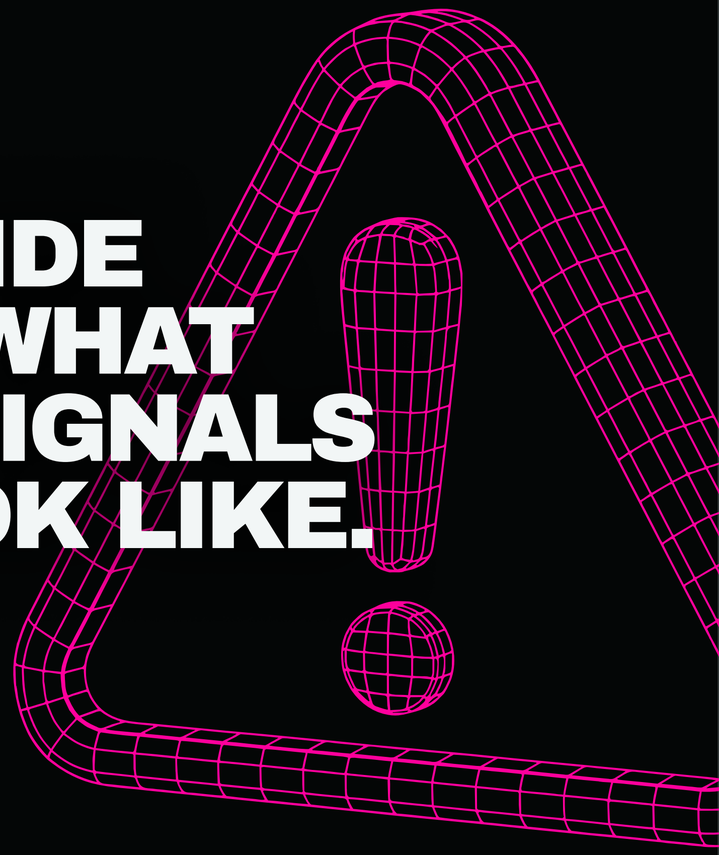
A ransomware attack doesn't start when the ransom note pops up. By that time, attackers have been in your environment for hours, sometimes days, preparing to strike. They mapped your network, silenced your defenses, and exfiltrated your data. The encryption is just the final act.

These attacks can start long before the payload drops, and they can also leave breadcrumbs.

Every stage before deployment—initial access, lateral movement, data theft—create signals defenders can catch. You just need to know what to look for.

THIS GUIDE SHOWS WHAT THOSE SIGNALS CAN LOOK LIKE.

You'll see how modern ransomware operations are structured, and how to strengthen your defenses to catch ransomware before it gets the chance to disrupt your business.



HUNTRESS

RANSOMWARE IS A BUSINESS. AND IT PROFITS OFF YOUR MISFORTUNE.

scan_id: RX-204 | mode: PRE-RANSOM
signals_detected: 07 of 12
ttr_estimate: 20h | window: OPEN
action: harden_access(); log++

Today’s ransomware crews don’t work alone. They run businesses—with R&D departments, affiliate programs, customer support portals, and profit-sharing agreements.

Ransomware-as-a-Service (RaaS) has industrialized cybercrime, making devastating attacks accessible to anyone willing to buy into the model.

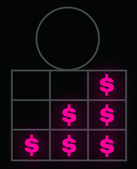
Here are the three specialized roles that usually power modern RaaS supply chain. This division of labor makes ransomware easier to scale and repeat. No single cybercriminal needs to be a master of all trades. They just need to be good at one link in the chain.

INITIAL ACCESS BROKERS

Break into systems and networks, then sell access to operators, affiliates, or other cybercriminals.

RANSOMWARE OPERATORS

Maintain the ransomware “brand.” They often develop the malware, manage the infrastructure, and provide affiliate support.



AFFILIATES

Purchase access from IABs. Conduct the attack using the operator’s tooling. Keep ~70–80% of ransom paid.

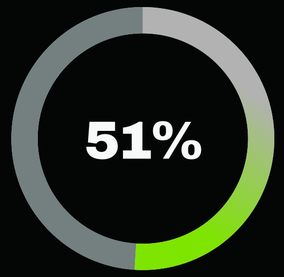
HUNTRESS

FOUR GROUPS. HALF OF ALL ATTACKS

scan_id: RX-204 | mode: PRE-RANSOM
signals_detected: 07 of 12
ttr_estimate: 20h | window: OPEN
action: harden_access(); log++

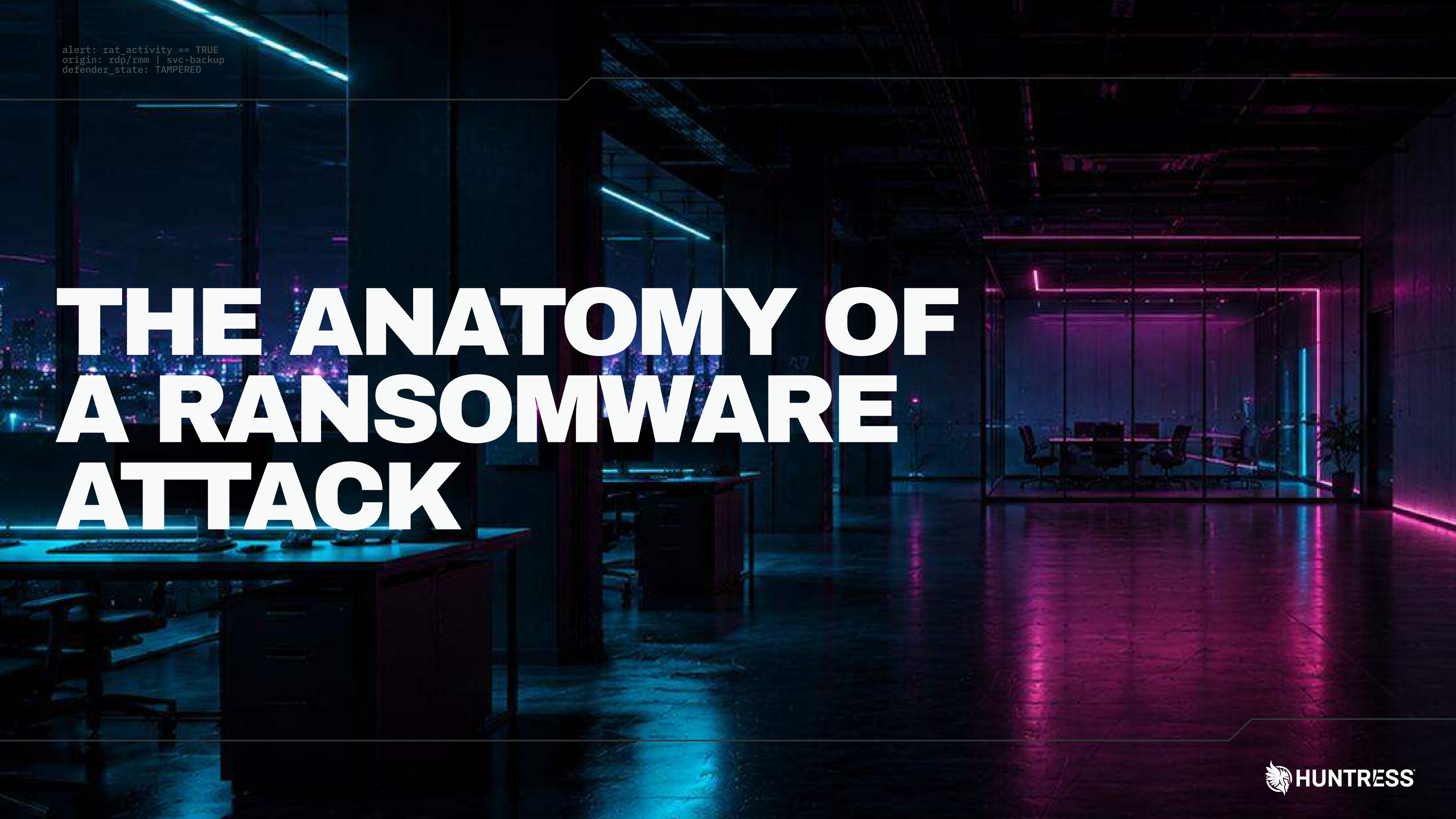
In 2025, four ransomware groups—Akira, Medusa, Qilin, and RansomHub—were responsible for more than half of the ransomware incidents Huntress tracked. Even though they operated independently, these groups often followed a shared pattern: get in, expand control, steal data, and pressure the business through encryption or extortion.

Like any mature business, these groups are just running the same proven process at scale. But that predictability gives defenders a better shot. If attackers are following a process, then defenders have a chance to break it.



of observed ransomware incidents in 2025 were tied to Akira, Medusa, Qilin, and RansomHub[1]

HUNTRESS



THE ANATOMY OF A RANSOMWARE ATTACK

HUNTRESS

scan_id: RX-204 | mode: PRE-RANSOM
signals_detected: 07 of 12
ttr_estimate: 20h | window: OPEN
action: harden_access(); log++

THE ANATOMY OF A RANSOMWARE ATTACK

A ransomware attack usually begins long before files are encrypted. The early stages can look like routine IT activity. Perhaps a remote access tool appears. Maybe a user signs in from a new location. PowerShell runs in the background. Or a VPN login succeeds after hours.

Alone, each event may seem harmless. Taken together, they can reveal an attack taking shape.

ACCESS → CONTROL → LEVERAGE → IMPACT

20HRS
average time-to-ransom in 2025,
up from 17 hours in 2024[1]

ACCESS

1. Find a way in

To find a way in, attackers look for organizations with doors left open. They may use stolen credentials, phishing lures, fake CAPTCHA pages, exposed remote access services such as remote desktop protocol (RDP) or VPNs.

They may also abuse rogue OAuth apps. These apps trick a user into granting access to Microsoft 365 or another cloud service. Once approved, the app or its tokens may let the attacker read mail, access files, or maintain access even after the user changes their password.

CONTROL

2. Turn access into control

Once inside, attackers spend time making sure they can stay in—and stay hidden. Many tools attackers use are also used by legit IT teams. They may install a remote access trojan (RAT), add a remote monitoring and management (RMM) tool, create a scheduled task, or hijack a session token. This is where attacks blend into the background.

LEVERAGE

3. Move toward leverage

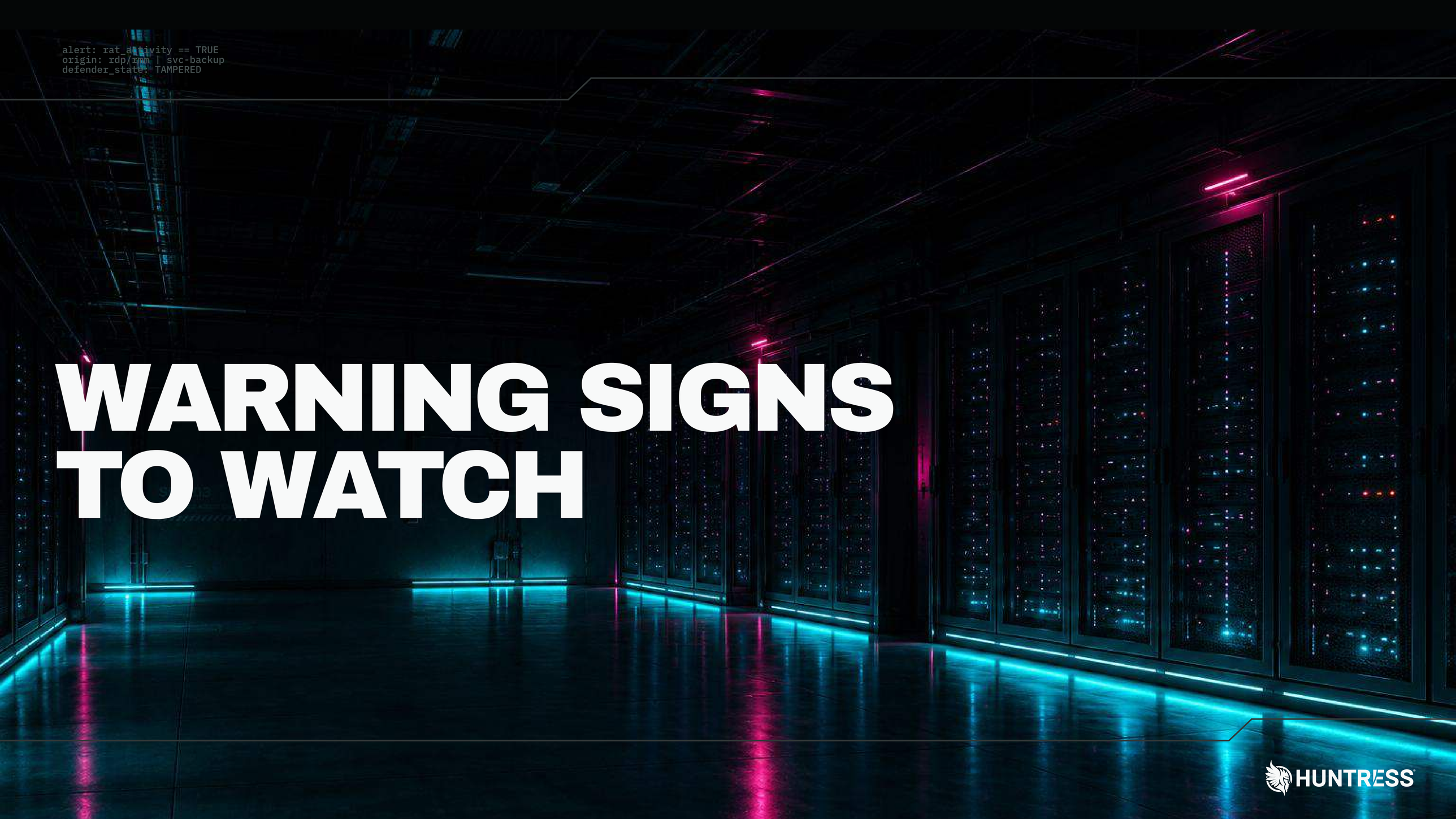
Attackers want a path to impact your business, so they look for the systems and data that create pressure and build their bargaining position. They quietly copy your most sensitive data and move it off your network before anyone notices. This is the step that turns ransomware from a recovery problem into an extortion problem. Even if you could restore your systems from backup, attackers can still threaten to publish what they've taken.

IMPACT

4. Prepare for impact

Before encryption, ransomware crews often weaken defenses and recovery options. Tampering with Microsoft Defender, deleting backups and shadow copies, and clearing logs are all realistic pre-ransomware behaviors. This is the last practical window to stop the interruption before it lands. But by this point, the real damage has already been done, and all that's left is for the ransom note to appear.

HUNTRESS


alert: rat_activity == TRUE
origin: rdp/rmm | svc-backup
defender_state: TAMPERED
WARNING SIGNS
TO WATCH
HUNTRESS

WARNING SIGNS TO WATCH

The ransom note is the obvious part. The warning signs are usually more subtle. Here are some common pre-ransomware signals to look out for.

SUSPICIOUS RMM ACTIVITY

RMM tools provide remote control through software your business may already trust. Monitor when an unexpected RMM tool appears, when an approved tool shows up on the wrong system, or when RMM activity is followed by credential access.

Timing is important, too. RMM activity that appears quickly after access may point to hands-on-keyboard intrusion, while longer delays can suggest staging, handoff, or preparation for a later phase.

CLICKFIX AND FAKE CAPTCHA

ClickFix attacks trick users into copying and running commands that appear to fix a browser or access issue. Fake CAPTCHA lures do something similar by hiding malicious instructions behind a routine "prove you are human" prompt.

The user thinks they're completing a normal step. In reality, they may be launching malware or opening remote access. When follow-on activity occurs hours later rather than immediately, it may suggest the access was handed off or staged for another operator.

IDENTITY ANOMALIES

A valid login can hide bad activity. Watch for sign-ins from unusual locations, unfamiliar VPN providers, disabled multi-factor authentication (MFA), dormant accounts becoming active, new mailbox forwarding rules, risky OAuth consent, or admin actions from users who don't normally perform them.

The signal gets stronger when identity activity lines up with endpoint alerts, mailbox changes, or remote access.

REMOTE ACCESS TROJANS (RATS)

RATs give attackers a hidden way back into the environment. A RAT can let an attacker run commands, move files, observe activity, or reconnect after the first infection is discovered.

277%
year-over-year increase in observed RMM abuse[1]

of identity-based attacks stem from suspicious login activity[1]

of incidents show sketchy identity activity at least 14 days before a ransomware event[1]

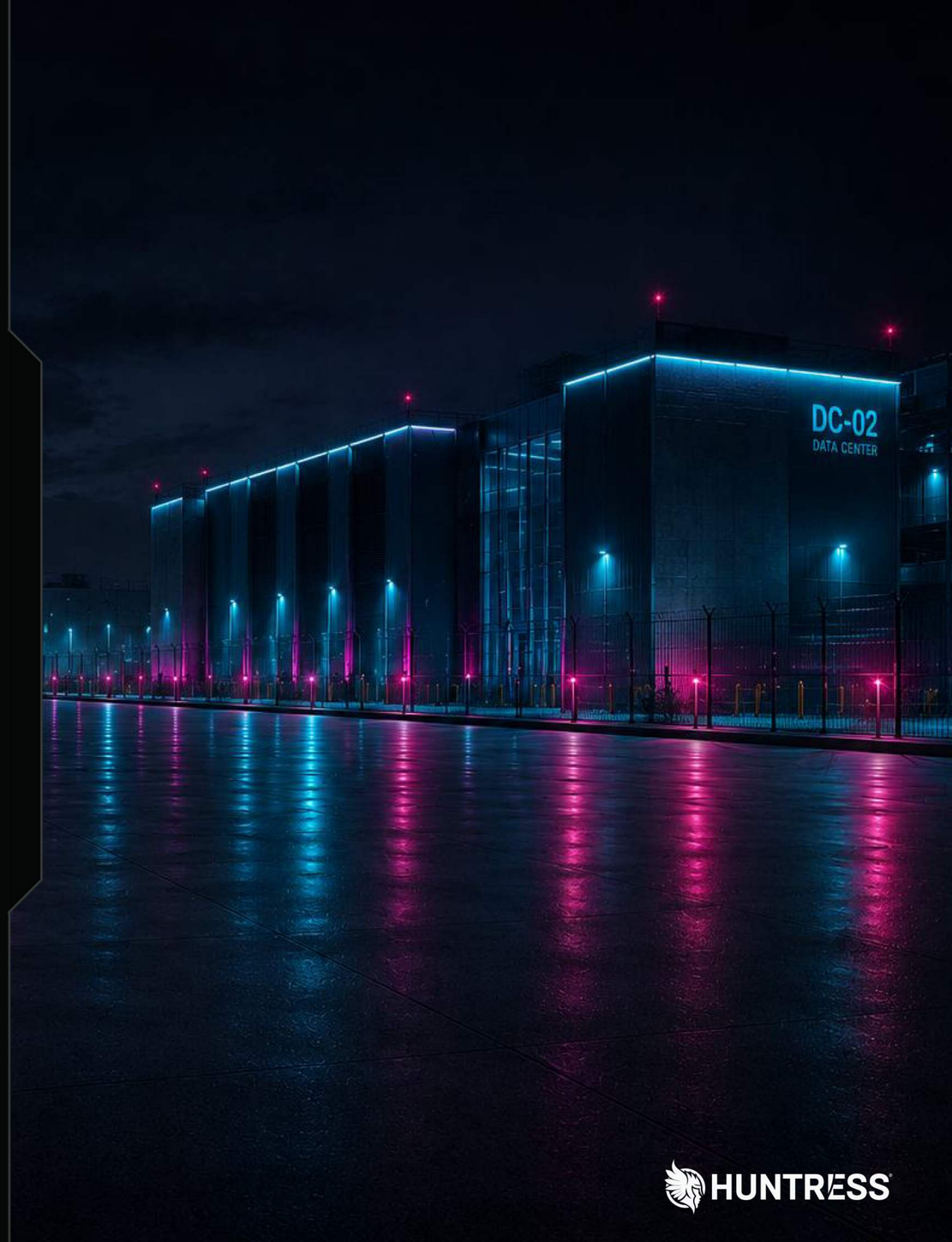
of ransomware incidents see the payload deployed within one hour of a RAT being installed[1]

HUNTRESS

STOP RANSOMWARE BEFORE THE CLOCK STARTS

Once you see a ransom note, it’s too late.
Don’t wait for that to happen to you.

Email: info@akita.co.uk
Visit: akita.co.uk



AKITA

HUNTRESS