smallworld

Before Ransomware Strikes

Understand the key stages of a ransomware attack and learn effective strategies to protect yourself before it's too late.

In partnership with HUNTRESS

The Bomb in the Machine

It's morning. You're still waking up, coffee in hand, ready to start the day. You open your laptop, but instead of seeing your usual inbox, you're greeted by a chilling message:

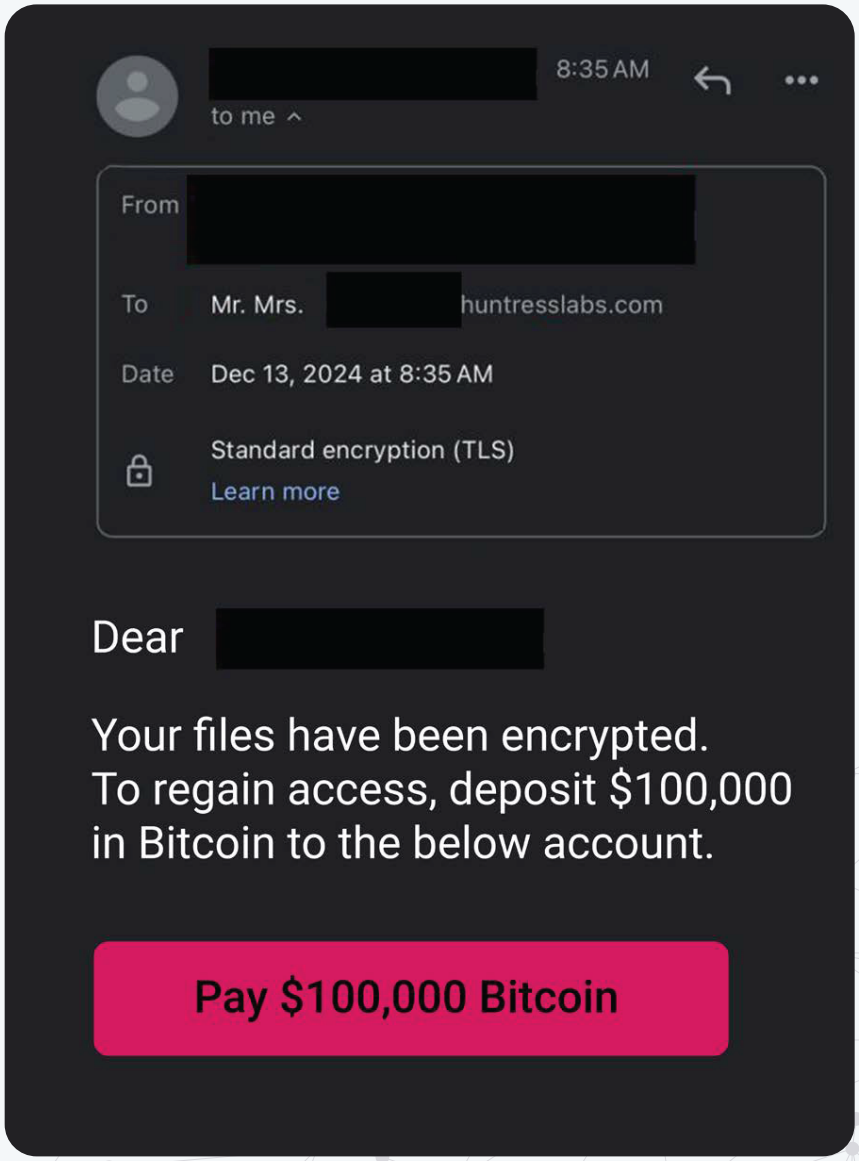
> Your files have been encrypted. To regain access, send $100,000 in Bitcoin.

You're wide awake now. Your heart pounds, and panic sets in. It's ransomware. The scary thing is, though this is your first exposure to it, malicious hackers may have been snooping around your systems for hours, possibly days, waiting for this exact moment.

Ransomware has become one of the most devastating threats today. It's a multi-billion-dollar terror targeting businesses and individuals across the globe. It's a silent digital bomb that can destroy your data, reputation, and sense of security in an instant.

Something businesses must now understand is ransomware attacks aren't randomised chaos. They're calculated, deliberate, and unfold in stages. But if you know what to look for, you can spot the warning signs and stop detonation before it's too late.

In this eBook, we'll uncover the red flags that signal a ransomware attack in progress. By identifying these threats early, you'll be able to strengthen your defences and protect everything you've worked so hard to build.



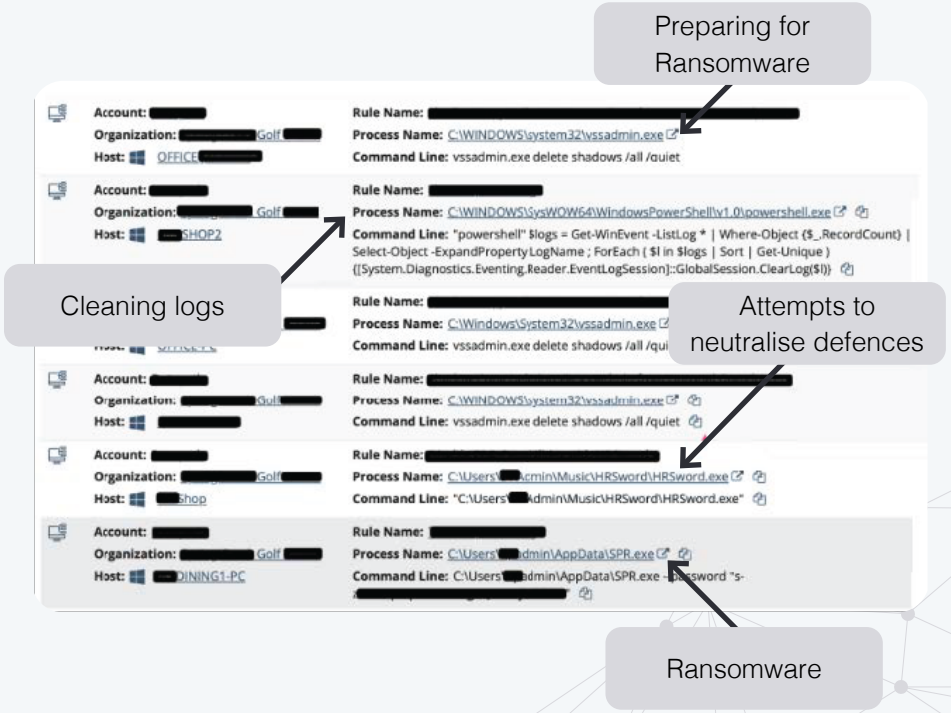
smallworld | In partnership with HUNTRESS

What Is Ransomware?

Imagine being locked out of your own system—your files, work, and memories all held hostage by malicious hackers. That's ransomware. This nasty malware encrypts your data and demands payment, often in cryptocurrency, in exchange for a "decryption key."

But, as we should all know by now, trusting criminals is never a good idea. Paying their ransom doesn't guarantee you'll get your data back. Some hackers just take the money and run. Others might give your files back, only to come back later and extort you again. And some take it further by stealing your data and threatening to leak it unless you pay a hefty sum.

The point is you can't rely on hackers to play fair. The best move is to focus on prevention and avoid these situations altogether.



smallworld | In partnership with HUNTRESS

Average Activity Before Ransomware Takes Hold

Ransomware is tricky because hackers can do a lot before actually deploying it. In 2024, Huntress' threat analysts kept a close eye on hacker groups, tracking what they did in the 48 hours leading up to ransomware attacks. They typically carried out about 18 steps beforehand. These included gathering info, escalating privileges, moving laterally, running scripts, downloading extra tools, and uploading files.

What hackers do depends a lot on what they're after. If the goal is extortion or espionage, they usually take a more complex approach, moving through systems, gathering sensitive info, and stealing data. In fact, with extortion becoming more popular, Huntress found that over 70% of incidents involved data exfiltration right up to the point of deploying ransomware.

But if they're just after a quick payout, they go for a simpler, faster "smash and grab" approach, taking fewer actions and focusing on speed over complexity.

Hackers undertake all kinds of actions to prepare for an attack, but there are four main stages you should know about. Let's break them down.

181

Average number of actions taken before triggering ransomware[1]

71%

Of incidents observed by Huntress in 2024 saw data exfiltration as the top action taken before ransomware dropped[1]

2,131

Pre-ransomware notifications sent by the Cybersecurity Infrastructure and Security Agency (CISA) in 2024 (as of Nov. of same year)[2]

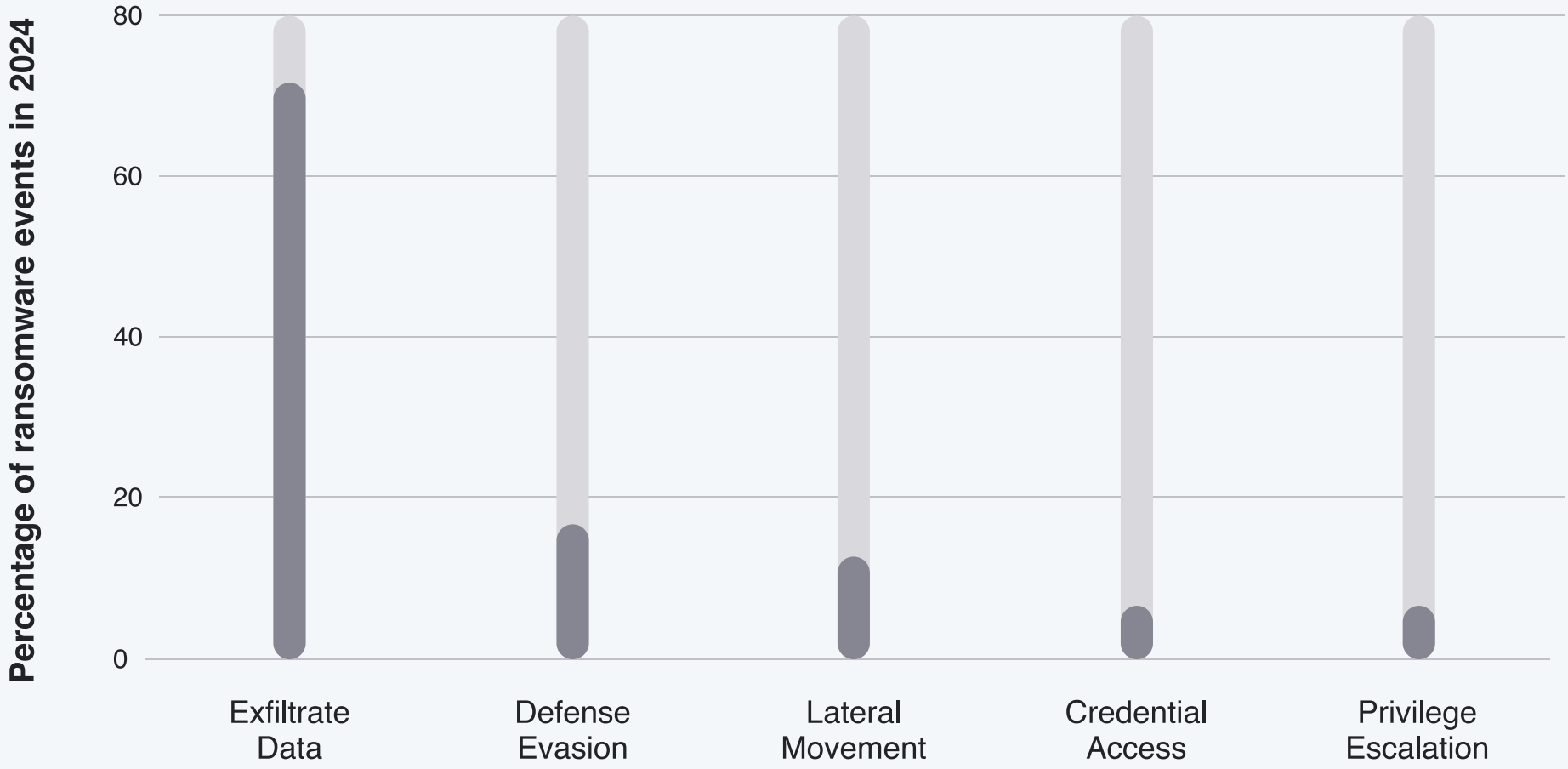
2x

Number of pre-ransomware notifications CISA sent in 2024 over 2023[1]

[1] Huntress, 2025 Cyber Threat Report, Feb. 2025
[2] Matt Kapko, CISA's Pre-Ransomware Alerts Nearly Doubled in 2024, Cybersecurity Dive, December 17, 2024

smallworld | In partnership with HUNTRESS

Activity Immediately Prior to Ransomware vs. Activity



The Four Main Stages Leading Up to a Ransomware Attack

Hackers might do many things before deploying ransomware, but knowing the main stages of their process is key to stopping them effectively. Let's break down their primary steps to better understand how to counter them with confidence.

STEP 1
Targeting Victims

→

STEP 2
Gaining Initial Access

→

STEP 3
Maintaining Access

→

STEP 4
Deploying the Payload

STEP 1
Targeting Victims

→

STEP 2
Gaining Initial Access

→

STEP 3
Maintaining Access

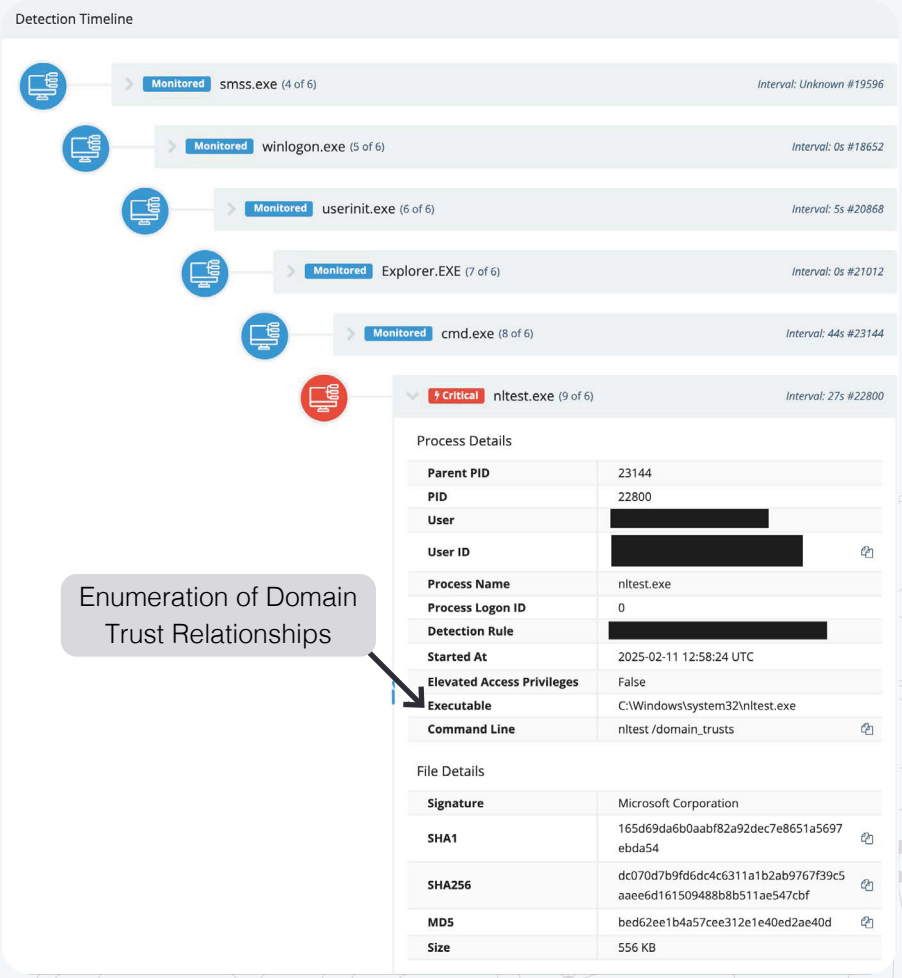
→

STEP 4
Deploying the Payload

Targeting Victims

For malicious hackers, this is the reconnaissance phase, where they start looking for their next target. They're basically "scoping out the joint."

This step is crucial because it sets the stage for everything that follows. If they can't find a target that's both vulnerable and worth their time, the attack won't go anywhere.



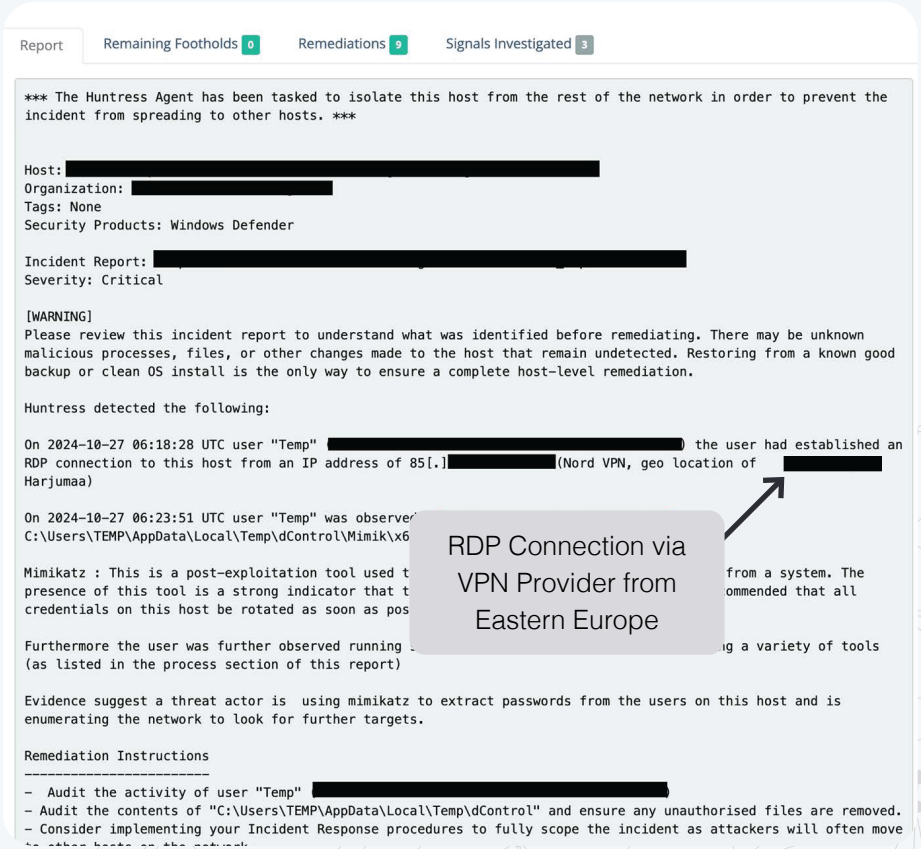
smallworld | In partnership with HUNTRESS

Gaining Initial Access

Once attackers choose their target, the next move is gaining access and hunting for the data they plan to encrypt. There are two popular methods for this:

1 Targeted Tactics

Hackers often zero in on publicly accessible systems, using stolen or purchased credentials to break in. If the systems are tucked behind access controls, they up their game, stealing credentials from high-level users to bypass restrictions and slip through the cracks.



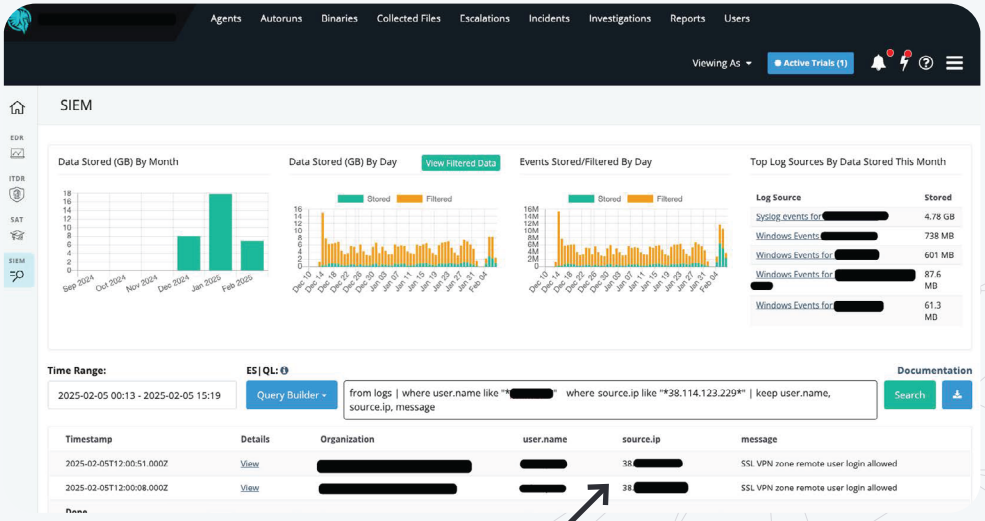
smallworld | In partnership with HUNTRESS

Gaining Initial Access

Once attackers choose their target, the next move is gaining access and hunting for the data they plan to encrypt. There are two popular methods for this:

2 “Scattershot” Tactics

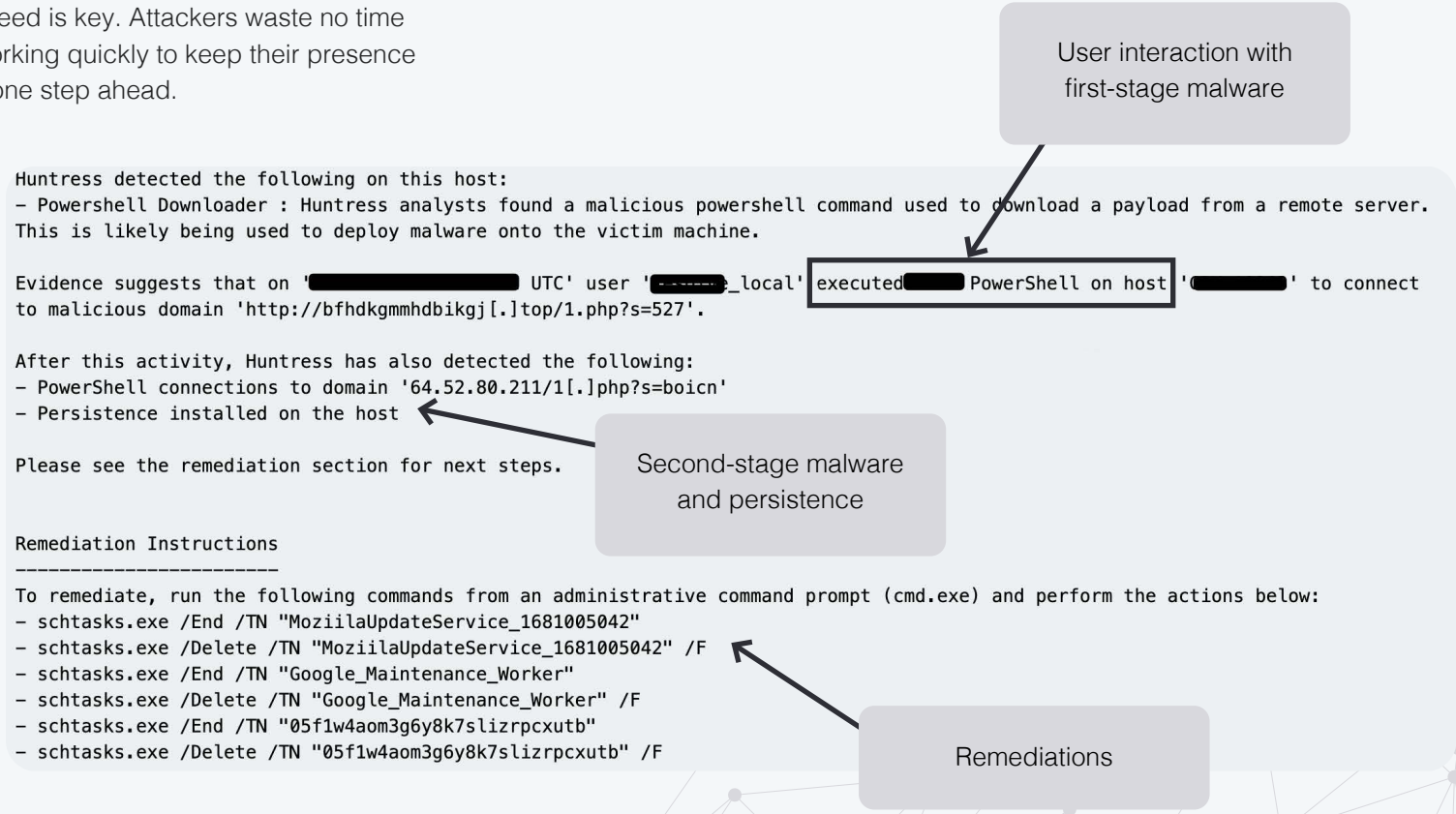
These can involve anything from phishing emails stuffed with malicious links to phone scams from fake IT support. Hackers prey on inherent human trust and lapses in judgment to trick someone into clicking something shady or revealing sensitive info.



Huntress SIEM search to identify anamolous VPN auth

Gaining Initial Access

No matter the strategy, speed is key. Attackers waste no time securing their foothold, working quickly to keep their presence under the radar and stay one step ahead.

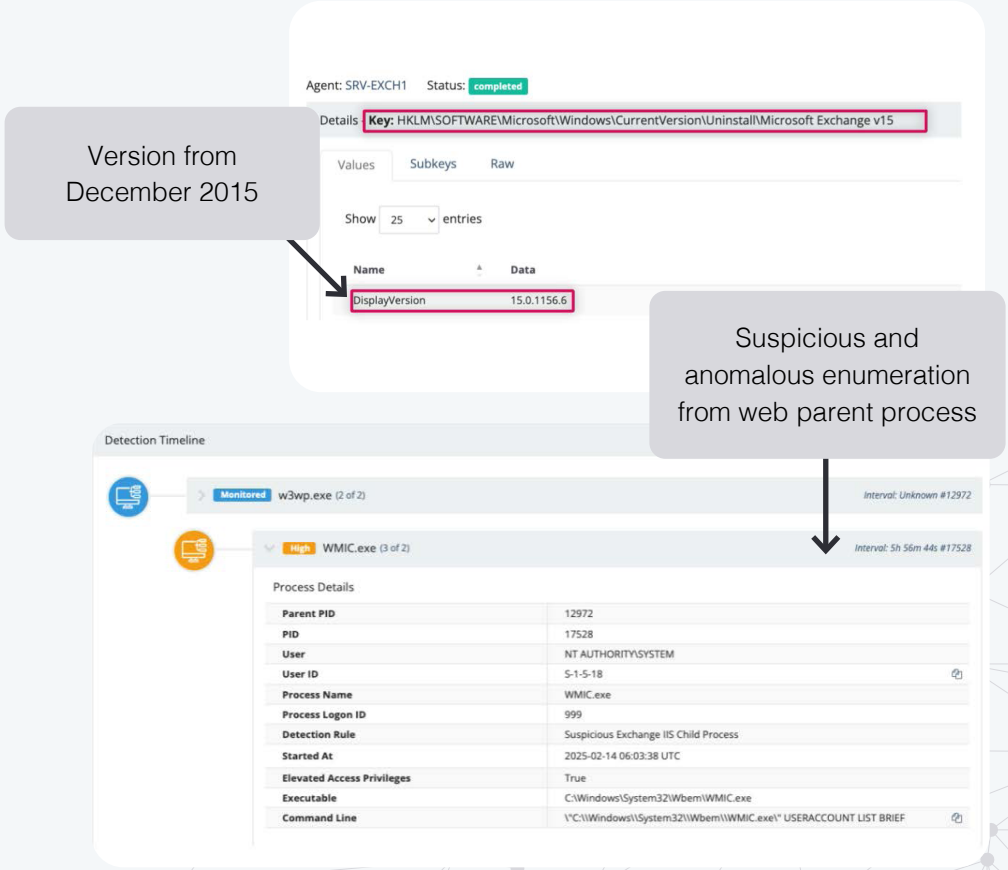


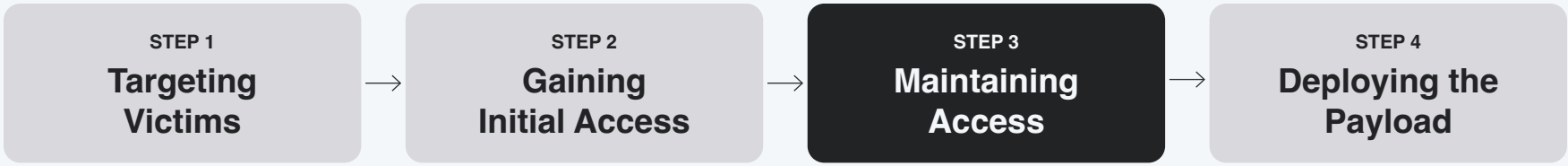

```
Huntress detected the following on this host:
- Powershell Downloader : Huntress analysts found a malicious powershell command used to download a payload from a remote server.
This is likely being used to deploy malware onto the victim machine.

Evidence suggests that on '[redacted] UTC' user '[redacted]_local' executed[redacted] PowerShell on host '[redacted]' to connect
to malicious domain 'http://bfhdkgmmhdbikgj[.]top/1.php?s=527'.

After this activity, Huntress has also detected the following:
- PowerShell connections to domain '64.52.80.211/1[.]php?s=boicn'
- Persistence installed on the host

Please see the remediation section for next steps.


Remediation Instructions
------------------------
To remediate, run the following commands from an administrative command prompt (cmd.exe) and perform the actions below:
- schtasks.exe /End /TN "MoziilaUpdateService_1681005042"
- schtasks.exe /Delete /TN "MoziilaUpdateService_1681005042" /F
- schtasks.exe /End /TN "Google_Maintenance_Worker"
- schtasks.exe /Delete /TN "Google_Maintenance_Worker" /F
- schtasks.exe /End /TN "05f1w4aom3g6y8k7slizrpcxutb"
- schtasks.exe /Delete /TN "05f1w4aom3g6y8k7slizrpcxutb" /F
```

Maintaining Access

Once attackers get into a network, they move like ninjas—quiet, calculated, and in no rush. Acting too fast would be like setting off an alarm, making it easy for detection tools to catch them. Instead, they play the long game.

Their first move is establishing persistence. They make sure they have backup ways to stay in, like through sneaky back doors, fake admin accounts, or tools like RMM (remote monitoring and management) or RDP (remote desktop protocol).





Maintaining Access

So, even if their original entry point gets blocked (like a stolen password being reset), they've already set things up to slip back in without anyone noticing.

What makes this even worse is how well hackers can use legit tools and mimic normal network activity. Their movements blend right into the background, making detection more like searching for a needle in a haystack.

17

Average time (in hours) for an attacker to move from initial access to ransomware deployment in 2024[3]

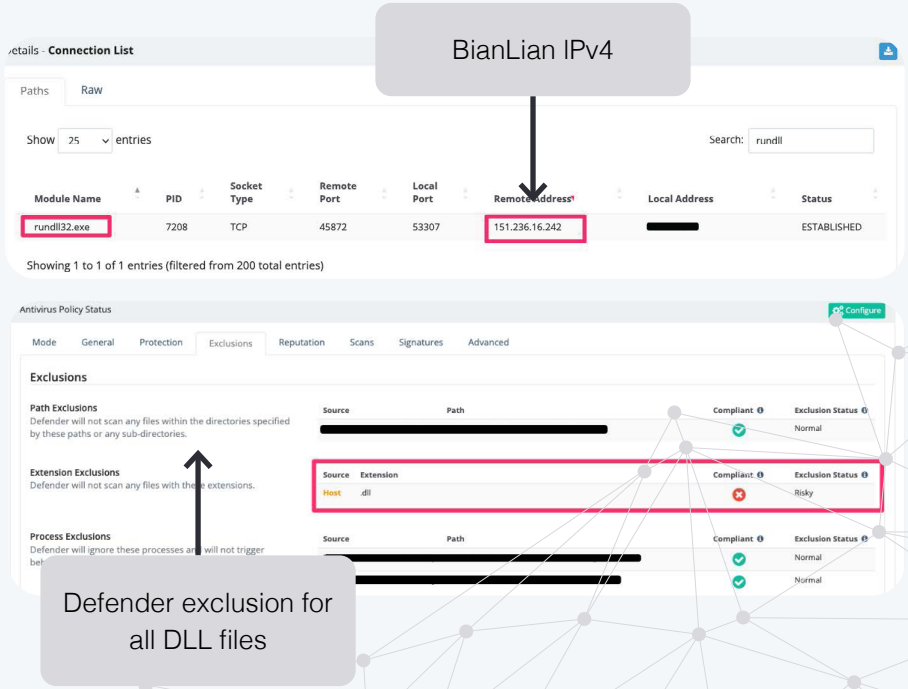
[3] Huntress, 2025 Cyber Threat Report, Feb. 2025

Deploying the Payload

If a ransomware attack was chess, this is when all the pieces fall into place for a decisive checkmate. It's the dreaded moment when attackers spread ransomware to as many machines as possible.

Here, hackers might use malicious tools or even hijack legitimate software to accomplish their goals. Their main targets are data servers, local email systems, and domain controllers—or really anything that'll cause the most disruption for your operation.

By now, they've set everything up. They've scouted the network, figured out the perfect time to launch their attack, and maybe even kept an eye on staff activity to spot the best opportunities.

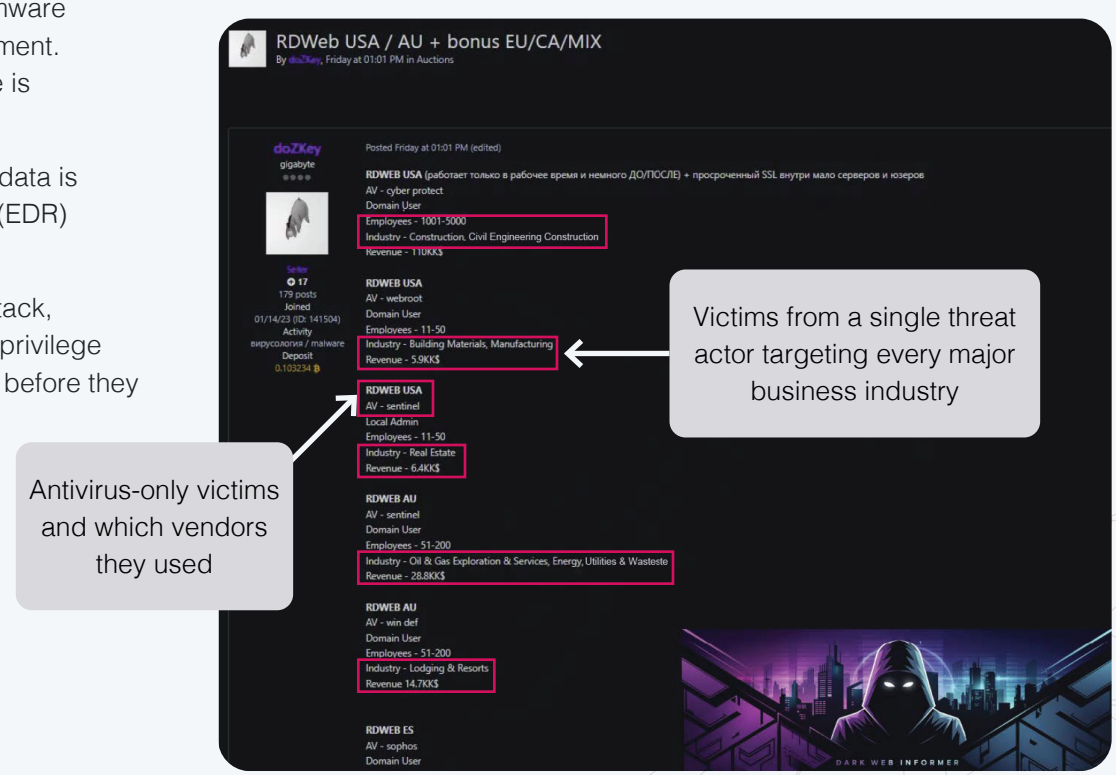


Antivirus (AV) Isn't Enough

Many assume AV solutions are enough to block ransomware, but they're not. Traditional AV tools basically just detect ransomware payloads—the part that locks your data and demands payment. The problem is, if the payload goes unnoticed, the damage is already done.

The real solution is stopping ransomware long before your data is encrypted. That's where endpoint detection and response (EDR) comes in.

EDR detects suspicious activity in the early stages of an attack, spotting warning signs like initial access, persistence, and privilege escalation. By catching these red flags, EDR stops attacks before they cause harm, keeping your systems safe.



smallworld | In partnership with HUNTRESS

How do you solve for this?

Ransomware attacks might involve complex moves from hackers, but protecting yourself and your organisation doesn't have to be difficult. It really comes down to staying informed, staying alert, and using strong security measures. Here's how you can keep the bad guys out:

Educate Your Team

Your team is your first defence against cyber threats, so help them remain alert. Teach them how to avoid clicking on suspicious links or replying to messages from unknown sources. Adopt a monthly security awareness training program. And be sure to review your company's incident response policies. Taking these simple steps will help you stop potential attacks before they happen.

Implement "Zero Trust" Practices

Adopting a zero trust approach gives your security an extra boost. It makes sure any new software or network changes go through strict approval before going live. This helps block attackers from slipping into hidden connections, keeping your systems safe and secure.

Stay Up-to-Date on Threats

Cyber threats always evolve quickly. Subscribe to cyber security bulletins, or better yet, partner with reliable cyber security platforms that do it all for you.

Adopt Fully Managed Solutions

Hackers don't sleep, but you certainly should. That's why it's so important to have cyber security that's fully managed by a 24/7 Security Operations Centre (SOC). These experts can catch ransomware attacks the moment they spot the precursors of an attack. By pairing a human-led SOC with the solutions below, you can keep your organisation better protected:

Endpoint Detection and Response (EDR)

An EDR backed by real cyber security experts can pinpoint activity indicative of ransomware and then isolate compromised devices and neutralise threats before they can do any damage.

Identity Threat Detection and Response (ITDR)

Ransomware attacks often begin with stolen credentials. An ITDR fully managed by a people-powered SOC helps stop attacks by preventing login hijacks, session theft, and other sneaky attempts to break in.

Stay Up-to-Date on Threats

SIEM monitors logs, user behaviour, and unusual activity around the clock. It not only detects, blocks, and contains potential ransomware threats, but also provides critical insights to speed up recovery and meet compliance standards.

Security Awareness Training (SAT)

An engaging SAT program developed by real experts— preferably paired with phishing simulations—can teach your employees to outsmart potential ransomware attacks by building sharper instincts and smarter habits.

With the right tools and expertise in place, you can rest easy knowing your organisation is prepared to fend off even the most relentless cyber threats.

Defuse Ransomware

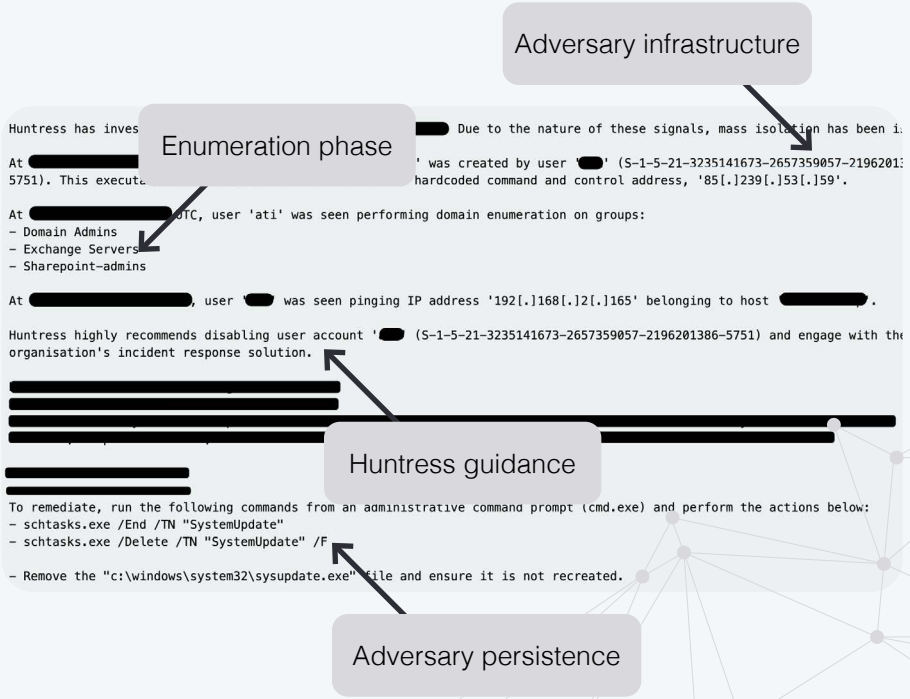
In the Introduction, we presented a stark scenario: waking up to a ransomware note, your data locked, and your business held hostage. For many, however, this is no longer a hypothetical. It's very real, like a ticking time bomb ready to go off. But now, equipped with the right knowledge, you're no longer a passive target, waiting for detonation.

As cyber attacks grow more sophisticated, ransomware is becoming increasingly destructive. However, with layered defences and proactive strategies, you can neutralise the threat before it takes hold.

That's where we come in.

Hackers are getting smarter-it's not a matter of just having an antivirus to protect your organisation. They're finding new ways to avoid detection and breach environments. To stay protected, organisations must be able to determine weaknesses in their infrastructure, detect when there's a potential breach, and so much more.

By partnering with Huntress, we are able to provide enterprise-grade protection for a fraction of the cost. This means you don't need to stress about cyber security because you have a 24/7 team of experts watching your back.



smallworld | In partnership with HUNTRESS

Stop Ransomware Before It Stops Your Business

Once you've been hit, it's too late. Don't wait. Protect your business and get ahead of ransomware now.

Contact Us

Website	smallworldit.com
Email	hello@smallworldit.com
Phone Number	03303338175

smallworld

In partnership with HUNTRESS