AKAMAI BLOG POST

Locked Out and Held for Ransom: A City's Battle Against Cybercrime

May 15, 2025

The story you are about to read is true; the names have been withheld to protect the innocent.

It's a gloomy, chilly day in early February. An HVAC vendor needs to check the system at one of their prominent customers: the city. Firing up his VPN client, the vendor quickly realizes something is amiss and the VPN won't connect. Grumbling to himself about the inconvenience, he calls the city help desk for assistance with the access connection

Probably another authentication issue, he muses. The city help desk engineer immediately springs into action, eager to get the issue resolved for the vendor. She logs into the server, and to her horror, sees directories and file extensions changing in real time, right before her eyes. A ransomware attack is in process.

Caught in time to limit damage

The city in this case was somewhat fortunate. The security team caught the attack just after it had started, so they were able to isolate the affected network segment to limit the damage.

Although the department in which the attack started had to go back to (in their words) “old-fashioned” work — with no tech — the rest of the departments were able to escape largely unscathed. Nonetheless, recovery took weeks, with downtime that made the mission-critical services the department provides to the community unavailable

Compromised vendor access credentials can be lucrative

How did the attacker gain access to the city network? Forensic analysis showed that the attacker was able to use a compromised vendor account (remember the HVAC guy?) to use the city’s VPN to access an HVAC system endpoint. Once connected, the hackers were able to harvest privileged credentials to gain escalated permissions and use the victim computer to move laterally throughout the network.

Sadly, this is a common occurrence. Data breaches and ransomware attacks often start with compromised vendor access credentials. Hacking vendors can be a lucrative proposition for ransomware groups, as they can potentially access credentials for multiple targets by compromising a single organization.

Traditional threats remain in play

While this access method seems to be pretty common as of late, it’s not the only way in. Traditionally, the top two infection vectors for ransomware threats are phishing emails and Remote Desktop Protocol attacks.

Phishing Attacks

Phishing is still super effective, as technology has made phishing emails increasingly harder to spot. Even seasoned professionals can be tricked by some of these well-crafted authentic-looking messages. Gone are the days of poorly worded Nigerian prince scams.

Remote Desktop Protocol Attacks

For some reason, a few organizations haven't figured out that having Remote Desktop Protocol connections open to the internet is a really bad idea. Attackers will find these very quickly, and brute force their way onto the system — and once they do, a ransom note is sure to follow.

The threat actors can also make their way in using the tried-and-true methods like social engineering, credential theft, and leaving compromised USB drives laying around.

The evolution of ransomware

Ransomware has dramatically evolved over the past decade, shifting from simple file-locking malware (better known as cryptolockers) to sophisticated attacks designed to maximize impact and profits. In the old days, ransomware attackers would encrypt a victim's files on a single system, demanding payment in exchange for decryption keys.

This evolved into compromising entire networks, including backup and recovery systems, to limit a victim's ability to recover. Over time, organizations began enhancing their cybersecurity posture, including more robust backups, which significantly reduced the impact of encryption-based attacks.

Double extortion ransomware

What was a poor miscreant to do? There was too much money left on the table to pack up their cards and go home. Instead, cybercriminals adapted by incorporating new ransomware solutions, giving rise to the era of a new type of ransomware called "double extortion."

Double extortion ransomware is a unique ransomware infection that involves two distinct threats: encrypting critical data and the exfiltration of the encrypted files, with the threat to leak sensitive information publicly if the ransom isn't paid.

This tactic dramatically increased pressure on victims because it transformed ransomware attacks from a primarily operational concern into a serious data breach risk with potential legal, regulatory, and reputational implications.

This was the case for our friends who work for the city. Before launching the encryption phase of the attack, the ransomware group exfiltrated several GB of data, and threatened to leak this data on the dark web should their demands not be met.

To pay, or not to pay

This is when things get tricky. Every level of law enforcement — from local authorities to the FBI, CISA, and others — will advise you not to pay the ransom demand. You'll get the same advice from essentially every security professional, including those at operating system vendors like Microsoft, and antivirus/anti-malware vendors.

The reason for this guidance is simple: As long as organizations continue to pay, cybercriminals will continue to launch cyberattacks. Once the payment is made (using Bitcoin or other cryptocurrency), there is no guarantee the decryption key will be provided, no guarantee the decryptor will even work, and no guarantee that you won't be targeted again.

Quite the opposite, in fact, as the attacker most likely still has a footprint in your environment — and since you have paid once, there's a good chance you will pay again.

The costs to rebuild and restore could exceed the ransom price

Multiple security organizations report that around 78% of organizations that pay a ransom demand are targeted again. So, just don't pay the ransom, right? In practice it's not quite that simple. Depending on the severity of the attack, an organization might not be able to recover without paying.

If the attacker can access the backups, they will surely be encrypted (the attack will start with the backups). Without backups the infrastructure cannot be restored. Even if viable backups exist, many organizations struggle with the cost and time of rebuilding everything from scratch.

In larger organizations, the costs to rebuild and restore their environments could far outweigh the ransom price tag. In these cases, they can't afford NOT to pay.

Additionally, the time factor cannot be overlooked. Restoration can take weeks or even months, meanwhile the mission-critical services that the organization's constituents rely upon are not available. The pressure to get these services restored can be immense.

The exposure of sensitive information could be even more damaging

The restoration process is only half of the story. As discussed above, most ransomware gangs are now using double extortion malware. They steal all the data first, then encrypt it.

Organizations are then faced with the threat of having sensitive information exposed for all to see. The result would be brand damage to the organization, loss of trust, and potential fines or other penalties. A victim might be hit with fines for failure to comply with privacy laws, then also have to supply credit monitoring to personnel whose information was stolen in the breach.

Catastrophic results

Add these costs to what the victim has already paid for restoration, and the result can be a financial nightmare. In some cases, the results are catastrophic and the organization simply cannot recover from the attack.

In 2022, Lincoln College in Illinois was forced to permanently close because of a ransomware attack. Already under financial distress due to the COVID-19 pandemic, the college was unable to pay the ransom, and their lack of preparation and incident response did not allow for remediation.

As a result, it was forced to close its doors after 157 years of operation — a heartbreaking outcome.

A ransom payment is a business decision

Ultimately, a ransom payment becomes a business decision. Some of the factors that weigh into this decision are:

- What are the business impacts for not paying?
- What are the business impacts if exfiltrated data is leaked?
- Are systems recoverable if the ransom is not paid?

The city in our story did not pay their attacker. They were able to negotiate with the ransomware gang and significantly reduce the ransom amount. They were fortunate enough to have had the ability to recover their compromised systems and were not dependent upon the decryption key.

However, they did have to inform a large number of individuals that their information had been compromised, and offer a credit monitoring service to all those affected. That said, the results could have been much worse.

Don’t be a target: Strategies to help

Worried yet? I don’t blame you. The thought of being a victim of ransomware is scary. But it doesn’t have to keep you up at night. Having a plan and doing some preparation in advance can either lessen the severity of a ransomware attack or prevent one altogether.

Here are some strategies you can have in place right away, including:

- Data backups
- DNS firewalls
- Segmentation
- Zero Trust application access

Data backups

The restoration process is only half of the story. As discussed above, most ransomware gangs are now using double extortion malware. They steal all the data first, then encrypt it.

Organizations are then faced with the threat of having sensitive information exposed for all to see. The result would be brand damage to the organization, loss of trust, and potential fines or other penalties. A victim might be hit with fines for failure to comply with privacy laws, then also have to supply credit monitoring to personnel whose information was stolen in the breach.

DNS firewalls

Phishing emails are the most common infection vector for ransomware. Try as you might, you can’t stop folks from clicking on phishing and other malicious links. You can, however, minimize the impact.

When someone clicks a malicious link, or opens a malicious attachment, their system does a DNS lookup for the malicious domain. A DNS firewall can block the resolution of the malicious domain and not allow the link to work. A DNS firewall can block similar connection requests to known malware domains and command and control infrastructure.

Akamai Secure Internet Access is a great choice for a DNS firewall. Akamai’s threat research teams use advanced algorithms to proactively block resolution of malicious domains, and the solution even has zero-day phishing protection.

It gets even better for the state, local, tribal, and territorial (SLTT) governments community. A free version of Secure Internet Access is available for MS-ISAC members via their Malicious Domain Blocking and Reporting (MDBR) service.

For organizations that need even more protection, Secure Internet Access is available in the form of MDBR+ from MS-ISAC, and the CIS CyberMarket has steeply discounted pricing for MS-ISAC members who would like to buy direct from Akamai.

Segmentation

The sad reality is that it’s not a matter of if a data breach is going to occur; it’s when. When a breach does happen, what ability does the threat actor have to move laterally in your environment to spread their malicious software?

Having segmentation in place is the key to controlling lateral movement. Basic segmentation is helpful, but the results can still be devastating.

I mentioned that the city was able to disconnect the affected segment of their network from the rest of the departments. The attacker was still able to launch a devastating ransomware attack. Mission-critical services for the city were offline for an extended period, resulting in major financial costs and brand reputation damage.

Even more effective: Microsegmentation

Traditional segmentation methods use Layer 2 and Layer 3 controls in the form of VLANs, firewall controls, and access control lists. A more effective approach is microsegmentation. Using a software-based approach allows you to control segmentation at the host level, which further contains the blast radius in the case of a compromise.

Akamai Guardicore Segmentation is the leader in this space. Akamai Guardicore Segmentation is a host-based firewall solution that gives you visibility into all the network traffic in your environment, allowing you to see not only “who’s talking to who,” but “what they’re talking about.”

This means that we can see not only which devices are communicating with one another, but also get rich contextual Layer 7 information about the processes that are running on each system.

Such visibility allows you to create policies that only allow the required communications for your network and applications to work the way they need to. Anything that is not specifically allowed is blocked, so, in the case of a breach, the attacker cannot move laterally to other systems and cannot execute processes that enable them to escalate privileges.

This software-based approach can make segmentation projects easier and faster to complete, resulting in enhanced security postures with speedier ROI.

Zero Trust application access

In our story of the American city hit by ransomware, the infection vector was a compromised VPN account. VPNs had their day;, in today’s threat environment, however, organizations need something better.

VPN access grants the user entry to the network — meaning that if the user knows what they’re doing, they can access anything on that network segment, whether or not they are supposed to. As we’ve learned, compromised credentials can lead to disaster.

A better approach would be to replace VPNs with a Zero Trust application access solution. These products provide a single sign-on experience for users, giving them access to just the resources they need to do their job, and nothing else. Users can’t access anything they have not been assigned to use.

Akamai Enterprise Application Access is a great choice for this requirement. Our application-aware proxy service provides a seamless application access experience, no matter where the application origin resides, or where the user is accessing the resources. Enterprise Application Access can also help with those pesky Remote Desktop Protocol sessions that you haven’t gotten around to taking off the internet yet. You can even provision Remote Desktop Protocol and SSH sessions to be accessed via web browser, which is perfect for third-party vendor access.

Ready to get started?

Don't wait for a breach to get your ransomware prevention playbook started. Contact Akamai's public sector team today to:

- Schedule a personalized assessment of your organization’s security posture
- See a live demonstration of our Zero Trust security capabilities in action
- Discuss implementation strategies tailored to your specific security requirements

Contact us to begin enhancing your organization's ransomware readiness posture today.

To learn more, visit akamai.com or contact your Akamai sales team.