HORIZON3.ai

~~TRUST BUT~~ VERIFY

Education

WHITE PAPER

# An Offensive Approach to Defeat Human-Operated Ransomware in Education

 @Horizon3ai info@horizon3.ai www.horizon3.ai

*An Offensive Approach to Defeat Human-Operated Ransomware in Education*

# Time for a Shift in Thinking About Ransom-Based Attacks

If you're a security professional defending an educational institution, you know how difficult it is to secure your IT environment. This fact is well known to the cybersecurity community – and attackers. Education is all about elevating the minds of your student body, and this goal demands an open, information-sharing environment that adapts to constant change.

Safeguarding the various network environments from both internal and external attackers creates a balancing act you must walk daily. Too much security can thwart your institution's main goal. Too little security puts your entire organization at risk. But there is a way to address both sides of the issue that results in a more secure environment without affecting your institution's main objectives.

This whitepaper is designed to help inform you of the current state of cybersecurity in education and highlight how human-operated ransomware works. We discuss what's not working in the context of defending yourself against these attacks and delve into a better approach to vastly improving the security of your IT infrastructure – without adding more layers of defensive security technologies to it.

After reading this whitepaper, you should have a much better understanding of what is needed to defeat human-operated ransomware and how the Horizon3.ai NodeZero™ platform can help you achieve that goal.

# Current State of The Ransomware Affair

Since you're reading this whitepaper, we're sure ransomware attacks must be one of your top concerns. Who wouldn't be overly concerned after what happened at the University of Michigan in August 2023?

According to the Vice President of Communications, Public Affairs, the University of Michigan experienced an internet outage that began on Sunday, August 27. The outage lasted three days and disrupted over 50,000 students, faculty, and staff members across their three campuses just as the fall semester was starting.

The University said they detected suspicious activity on the campus computer network on August 23 and took quick action to contain the incident, including disconnecting the campus networks from the internet. They believed that an attacker stole personal information relating to students and applicants, alumni and donors, employees, and contractors.

So, was this a human-operated ransomware attack that severely affected the university and their campuses?

The university has not confirmed if it was – or was not, but many industry experts suspect that it had to be the result of a human-operated ransomware attack. Very few organizations would purposely cut their internet lifelines to the outside world the week classes were set to begin because they "suspected a data breach". As we can see here, human-operated ransomware has elevated to a whole new level.

## World-Wide Counter Ransomware Initiative (CRI)

On October 31, 2023, news of a global counter ransomware initiative was making headlines. The third annual summit convening 48 countries, the European Union, and Interpol met in Washington, DC to reaffirm their joint commitment to building their collective resilience to ransomware. As shown in the Joint Statement, **"This year's CRI gathering is focused on developing capabilities to disrupt attackers and the infrastructure they use to conduct their attacks, improving cybersecurity through sharing information, and fighting back against ransomware actors."**

If there is any sign of the challenges around ransomware, this must be it. People at the highest levels of government, combined with local, national, and international law enforcement all see ransomware attacks as a huge problem.

# The Rise of Human-Operated Ransom-Based Attacks

When people hear news of an attack that involves a ransom, they normally think "malware" since the name ransomware ends in the "ware" term. However, there is a considerable misunderstanding in general about how ransom-based attacks work. Therefore, it makes sense to highlight the differences between ransomware (malware) and human-operated, ransom-based attacks.

In the early days of ransomware attacks (circa 2013-2018), most were opportunistic in nature – targeting a single device. While ransomware primarily existed in small circles during that period of time, the business model didn't grow at scale until the introduction of CryptoLocker in 2013. This accelerated the growth in this opportunistic, single-device way of monetizing cybercrime. These ransomware attacks are usually automated, they spread like a virus, they normally involve phishing then malware delivery, and they require malware remediation.

Then in 2019, human-operated ransom-based attacks began to surface. These attacks do not target a single device; they target an entire enterprise. Attackers vastly expanded their extortion scope to enterprise-scale attacks and began targeting all data and systems while monetizing largescale business interruption and exposure of confidential information. A new seed was planted in the threat-actor community that grew into the current super-sized extortion model.

## Human-based ransom attacks are extremely targeted and focused

**In human-operated ransom-based attacks, the tactics, techniques, and procedures (TTPs) are particularly clear. Often using open-source intelligence (OSINT), attackers first target employees via email phishing attempts or browser exploits for the sole purpose of gaining someone's user credentials. Remember: They are not targeting an individual computer. They are targeting an entire enterprise, and stolen credentials are key to attackers gaining an initial foothold.**

**Once an attacker has someone's legitimate credentials, regardless of the level of privileges that user has, attackers use those credentials to remain persistent in an environment without you even knowing they are there. Then attackers move laterally, and elevate their privileges through password spray techniques, credential dumps, known vulnerabilities, and risky software defaults with the sole purpose of landing and expanding in order to gain administrative access to your entire enterprise.**

**Once administrative access is obtained (think domain admin), attackers find your data, exfiltrate and/or encrypt your data, prove they have access or control of your data (usually via an email), sabotage your backup/recovery processes, and demand payment to get your data back. If you do not pay their initial ransom demands, they effectively take your entire enterprise offline by crashing your systems (since they now have admin access) and/or they make it impossible to recover your data on your own accord. This is big game hunting that can generate extremely high payouts, and this is why governments all over the world are genuinely concerned with the rapid spread of this attack vector. These are very targeted attacks.**

# Lessons From Defensive Warfare for the Modern Cyber Warrior

Too often in the fight against cybercrime, most organizations, including those in education, believe that throwing more security technology – in addition to more budget – at the security problems they face will either solve them or make them go away. And as time has shown repeatedly, this type of approach is not working.

Anyone who studies civilizations of antiquity will quickly discover how the earliest cities defended themselves from their enemies. Wartime in those days often pitted mobile armies attacking stationary targets. Cities built walls, then added layers of walls including towers, walkways, parapets, ramparts, moats, obstacles, and so on to deter their enemies.

Although all of these fortifications worked at some level when they were initially built, advancement in warfare like gunpowder, cannon fire, and eventually aerial bombardments made this entire method of defense worthless. What history proves is that no matter how well a position is defended, attackers always discover ways of defeating a purely defensive approach.

When drawing a parallel to today's cyber terrain, organizations are repeating history by purchasing and deploying layers of purely defensive-based technologies with the hope of defeating today's attackers. However, every time a new defensive measure becomes the must-have technology, attackers hone their TTPs and eventually find a way around every defensive mechanism known to humanity.

Although deploying the most modern defenses is necessary, attackers eventually find a "chink in the armor" and the organization gets breached. Then more budget is requested, more technology is purchased and deployed, and the false sense of security perpetuates. This never-ending approach simply cannot solve all of the security challenges organizations, including educational facilities, face.

# A Mindset Shift is Required: Use Offense to Inform Defense

How do modern militaries discover their greatest weaknesses? They go on the offensive and attack themselves by running various red team/blue team exercises so they can learn where they are most vulnerable. In other words, militaries use offense to inform defense, but the issue most organizations face is that they are not doing the same. Instead, they're depending on layers of defenses to cover every possible weakness and attack scenario they can think of.

The challenge here is that the same defenses organizations deploy are nothing new to attackers. In fact, most modern attackers have years of cybersecurity experience. They are skillful software developers, they are experts at exploiting weaknesses, and they know the defensive approaches organizations take. And when it comes to the layers of defenses you likely have in place, none of them can tell you where your greatest weaknesses are lying in wait, ready to be exploited.

So, what is the answer to all of this? It's time to go on the offensive, find your truly exploitable vulnerabilities, and fix them – before attackers discover them and use them against you.

**The most common weaknesses we see daily in networks just like yours include:**

- Vulnerable services
- Weak authentication
- Data leakage
- Data exposure
- Exposed credentials
- Weak network segmentation
- Gaps in your security controls
- Misconfigure network devices, servers, and applications

For those interested in learning more about becoming a certified penetration tester, here is a list of penetration testing certification programs available.

Certified Ethical Hacker (CEH)

Licensed Penetration Tester Master (LPT) Certification

Offensive Security Certified Professional (OSCP)

GIAC Penetration Tester (GPEN) Certification

GIAC Exploit Researcher and Advanced Penetration Tester (GXPN) Certification

CompTIA PenTest+

# Think Like an Adversary Instead of a Victim

It's time for security teams to think like an adversary instead of a victim since there is no other way to completely defend yourself from today's highly advanced and skillful attackers. You must use the same TTPs they use, and you must attack yourself as often as you possibly can to uncover the unknowns in your networks.

The reason for this is simple. If you cannot find that hidden chink in your armor, that crack in your layered walls of defense, that blind spot you didn't even know existed, you will never be able to adequately defend yourself against a purposeful attacker with nothing but time on their side – and money on their mind.

But here lies another challenge most organizations face: There are not enough highly skilled penetration testers available to continuously help them find their exploitable weaknesses. Therefore, security teams must either work to become proficient in ethical hacking techniques, or they must look for solutions that can exactly mimic what attackers are doing – using the same TTPs they use.

# Where Best to Spend: Offense or Defense?

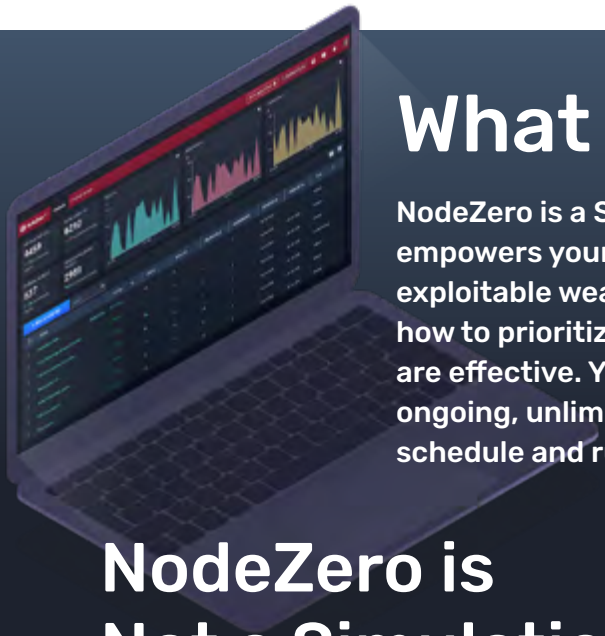
Performing a single penetration test, executed by a highly skilled pentesting expert, is not inexpensive. In fact, a single pentest offered by a manual pentesting firm can exceed tens of thousands of dollars for a single test. And if you want them to test every single endpoint in your entire educational facility (which is often not possible due to so many BYOD endpoints connected to your networks), it will take months if not longer to complete. By the time that pentester is finished, your network environments have already changed, especially since education environments are in a constant state of flux as new students arrive and others leave.

So, where is the best place to spend your limited security budget? Do you purchase a single penetration test that doesn't necessarily make you more secure, or do you purchase more defensive security technologies in the "hope" they will make you more secure? This quandary is nothing new to organizations of all sizes. Also, how do you go about proving that you remediated the exploitable vulnerabilities a pentester may have uncovered or missed because they only took a snapshot that's now outdated? Our founders faced the very same problem before they established Horizon3.ai.

# Enter NodeZero™

Prior to the formation of Horizon3.ai, our founders worked together in the United States Special Operations Command (USSOCOM) where they realized they needed to access the security of their own IT infrastructure, since they supported the combat readiness of US armed forces. They hired third-party penetration testers to test their environments, and the pentesters found security issues. The USSOCOM personnel went on to remediate the discovered security issues, yet they had to wait months if not longer to have the same pentesters return to validate that their issues were resolved.

Our founders knew there had to be a better way, and as a result, Snehal Antani and Anthony Pillitiere (from USSOCOM) joined forces, started Horizon3.ai, and named their technology NodeZero. The name of the solution seemed fitting because a single exploitable node in a network could be the "ground zero" of a complete network takeover.



## What exactly is NodeZero?

**NodeZero is a SaaS-based autonomous penetration testing platform that empowers your organization to reduce your security risk by helping you find the exploitable weaknesses in your network, giving you detailed guidance about how to prioritize and fix them, and helping you quickly verify that your fixes are effective. You can continuously improve your security effectiveness with ongoing, unlimited, and orchestrated deployments of NodeZero, and you can schedule and run as many pentests as you want against any of your networks.**

## NodeZero is Not a Simulation – It's an Actual Attack

NodeZero is designed to safely attack any infrastructure using the same TTPs that attackers use. NodeZero is not a breach and attack simulation (BAS) tool since there is nothing "simulated" about it. Instead, NodeZero is designed to move autonomously throughout your networks, discover your greatest weaknesses, and prove it can exploit them without doing any harm to your environment.

**For example, here are two real-world attack paths NodeZero discovered in two of our customers' networks. Both organizations are in education, and both attack paths could have resulted in data theft, leading to a successful human-operated ransom-based attack.**

**Note:** An attack path is a visual representation of the path an attacker could take to discover and exploit multiple weaknesses in an environment that could lead to often-disastrous results.

## Attack Path Example 1: Result = Ransomware Exposure

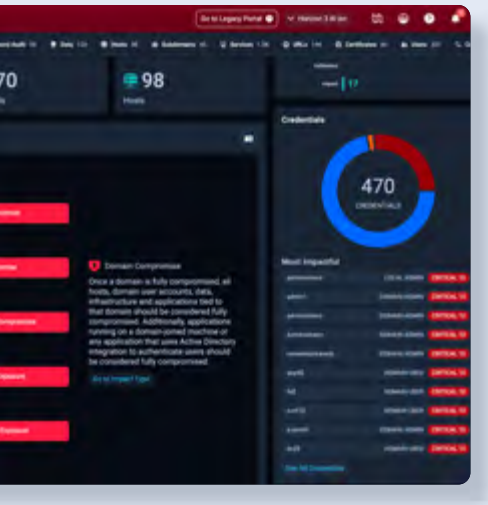
In less than 2 minutes, NodeZero identified a ransomware exposure risk in a read/write file share that exposed 221 files due to Weak NFS Export Permissions. This autonomous pentest was run in a K-12 school system that supported more than 40 local schools.

In this example, NodeZero was launched from a host in an internal network on Nov. 10, 2023. NodeZero quickly discovered an anonymous credential on an RPCBIND service and then discovered a file share on an NFS service. NodeZero leveraaged an NFS Export Permissions weakness that affected the NFS service. From there, NodeZero enumerated 221 files in a file share on the NFS service using the anonymous credential it discovered.

## Attack Path Example 2: Result = Ransomware Exposure

In a little over 10 hours, and through using a password spray technique, NodeZero was able to move laterally, find, and enumerate 8,556 files containing what appeared to be social security numbers that were at risk of ransomware exposure. This autonomous pentest was performed in a university environment.

In this example, NodeZero was launched from a host in an internal network on Oct. 25, 2023. NodeZero discovered 5,687 verified usernames and discovered a cleartext password for a certain user while accessing the SMB service on a Domain Controller. Next, NodeZero leveraged a password spray weakness affecting the credential for that certain user. Using that credential, NodeZero discovered a file share and enumerated 8,556 files contained within it.




# Using NodeZero Identifies Your Ground Zero

There is little doubt that you have a “ground zero” hiding in your networks, and the chances that attackers will find it are so high, it’s almost guaranteed. So, what can you do now to find that one truly exploitable vulnerability, that one cleartext password, or that one misconfiguration oversight before attackers do? The answer is simple. With NodeZero, you can safely hack yourself as often as you like. Our customers use NodeZero during anytime of the day or night, against systems in production, and are completely amazed by what NodeZero is able to find in their networks.

## More About NodeZero

NodeZero shows you the actual attack paths in your environment for every weakness it discovers, revealing and detailing each step an attacker could take to penetrate your defenses. It uncovers blind spots in your security posture that go beyond known CVEs and patchable vulnerabilities, such as easily compromised credentials, exposed data, misconfigurations, poor security controls, and weak policies. Weaknesses are prioritized based on their impact on your organization so you know exactly what you should fix first. NodeZero also provides detailed guidance to support your remediation. Here are a few additional benefits provided by NodeZero:

• **Autonomous Operations:** The NodeZero platform offers a growing list of operations to help you assess and validate your security posture: internal pentesting, external pentesting, AD password audit, and N-day testing.

• **Breadth of Coverage:** NodeZero can be used to assess on-premises infrastructures, external attack surfaces, cloud infrastructures, identity and access management infrastructures, data infrastructures, and more.

• **Autonomously Chains Attack Vectors:** NodeZero pivots through your network, chaining weaknesses together just as an attacker would and then safely exploits them.

• **Prioritizes:** NodeZero shows you what weaknesses are truly exploitable in your network, and which have the most critical impacts to your organization so you can prioritize your remediation efforts. It also identifies systemic issues that allow you to remediate many weaknesses with a single change, such as a policy fix.

• **Requires No Agents or Special Hardware:** NodeZero is a true self-service SaaS offering that is safe to run in production. It has no hardware or software for you to maintain, and it requires no persistent or credentialed agents.

• **Continuous, Unlimited, and Orchestrated Deployments:** NodeZero will empower your daily security standup, helping you continuously improve your effectiveness. You can schedule and run as many pentests as you want against your largest networks and run multiple pentests at the same time.

# Conclusion

The goal of this whitepaper was to demonstrate how you and your institution can take an offensive approach to defeat human-operated ransom-based attacks. Horizon3.ai has hundreds of customers in education, government, healthcare, finance, manufacturing, and other industries who are using NodeZero to do just that. And speaking with our customers, they continue to be amazed by what NodeZero is able to find in their environments.

Our customers acknowledge they are using NodeZero on nearly a daily basis to discover their truly exploitable weaknesses, and they are fixing them before falling victim to a litany of possible attack vectors. This purely offensive approach allows you to preemptively defeat human-operated ransom-based attacks while enabling you to experience significant ROI. We suggest you test-drive NodeZero yourself to see what it discovers in your environments – before attackers do.

- **To test drive NodeZero in your own education environment, sign up for a free trial.**

**https://www.horizon3.ai/trial**

- **To learn how NodeZero can help secure your education business, schedule a demo today.**

**https://www.horizon3.ai/demo**