VECTRA
SECURITY THAT THINKS

E BOOK

Stopping Ransomware: Dispatches from the Frontlines

Summary

No organization wants to discover a ransomware attack unfolding in their environment, but if you can quickly identify the signals — you'll have the best chance possible to stop it. So how do we do that? Well, that's what we're here to discuss along with real examples of how our top customers are working alongside the Vectra Sidekick team to respond to early-stage ransomOps attacks in order to stop disastrous business disruption before ransomware gets deployed.

This ebook dives into everything from why detecting attacker activity and recon known as ransomOps is critical to stopping ransomware and many of the steps security professionals are taking to successfully slam the door on today's ransomware tactics. We'll share how customers utilizing Vectra Sidekick Services are able to detect active attacks almost immediately as well as some of the challenges, observations and recommendations that every organization should know.

One thing is for sure, the difference between success and failure when it comes to stopping ransomware comes down to response speed and quick action — let's stop some ransomware!

Vectra Sidekick MDR Service

Vectra Sidekick MDR is a 24/7/365 eyes-on-glass service that proactively investigates malicious activity surfaced by Vectra Detect.

SideKick MDR acts as a security team multiplier by deploying experienced security analysts to help you fully utilize Vectra's AI to see threats early and stop breaches. With Sidekick MDR layered on top of the Vectra platform, you get:

- A boost to your security team with access to experienced security analysts who help expel sophisticated adversaries and ransomware actors.
- Expertise, context, and clarity regarding the early telltale signs of an attack, threat or ransomware surfaced by Vectra Detect with analysts to proactively assist in rapid response.
- 24/7/365 proactive monitoring so you know when a priority threat or ransomware detection requires immediate action and response.
- Customization of your Vectra deployment tailored to your unique environment, business objectives and industry risks. This includes customizing controls, providing expert recommendations, environment trends and metrics and accelerating investigations.

First and Foremost, Ransomware is a Business

As distasteful as it may be, ransomware gangs and their affiliates are running a business, and just like any other business — they exist to make money. They have an ROI mindset and just happen to be cashing in on the ability to reach systems and data that they can steal as quickly as possible, while charging you a hefty sum for the return of your own property.

This mindset drives many of the observations discussed throughout this ebook, while understanding the motivation that drives attackers is a key piece to any security strategy. When you know what drives attackers and can clearly identify the systems and data in an environment that would cause disruption if compromised — your organization will be in a good position to make it as difficult as possible for an attack to unfold.

Let's see why tabletops can help bring this into focus, and how red teams can give an objective evaluation of current readiness.

Start with the Basics

Of course, the best outcome is to keep the ransomware gangs from ever gaining access to your environment. And while prevention is never foolproof, the ROI mindset can work to your advantage. In fact, you can dramatically reduce your risk by getting the basics of authentication hygiene and patching right.

This is because initial access by attackers most commonly occurs via an unpatched and DMZ-exposed vulnerability, an account without MFA or similar low-hanging fruit. Basically, if organizations miss some of the basic prevention methods — there's no need for attackers to use sophisticated and time-consuming tactics to gain access.

> The best outcome is to keep the ransomware gangs from ever gaining access to your environment.

The good news is that by enabling MFA (multi-factor authentication) on your VPN, IDP and other points of entry, you'll make life more difficult for attackers who may just decide to knock on someone else's door instead. The same goes for patch management — making sure patch practices span across your DMZ will help in turning away attacks. While no prevention strategy is foolproof, sensible investments in prevention will make it harder for attackers to get in.

Be Ready to Respond at Speed…Day or Night

Dialing in the basics will improve, but not eliminate, risk. There are a lot of reasons for this, but the truth is that it only takes one mistake in account setup, one missed patch, one user clicking on a link they shouldn't…or one new 0-day in your VPN of choice (funded by the gobs of money pouring into the ransomware ecosystem) to break through. We've seen it all.

And when a ransomware actor gets into your environment — expect that they will move FAST. We have certainly responded to attacks that progressed slowly over several days, however; it's not uncommon for the majority of an attack to occur in a single, after-hours evening. Remember, time is money for attackers with an ROI mindset. Whether giving defenders the least amount of time to respond or just playing the numbers game, we generally see few signs of attackers trying to stay below the radar. In fact, the global dwell time for ransomware attacks has dropped significantly over the last few years.

The good news for defenders is that speed makes the attack obvious with the right detection technology. As is the case with Vectra, we've seen critical hosts within two minutes of initial access. However, due to the speed of the attack progression, this also makes it crucial to be prepared to respond quickly and decisively in order to stop the threat prior to ransomware deployment.

Unfortunately, this ability to respond at speed isn't limited to business hours. We've observed early-stage reconnaissance and lateral movement occurring at all hours, seemingly whenever the ransomware actor had some time. Sometimes it will be in the middle of the day, other times at night, on a weekend or even during a holiday. However, based on our observations, the final push to exfiltration and encryption is more likely to be in the middle of the night or on a weekend or holiday — when incident response capabilities are at their weakest.

Practically speaking, this means 24x7 monitoring is a must.

Have a Game Plan for Response

The first step in responding to a ransomware threat is to detect the adversary in your environment. It's equally critical to know what you'll do in various scenarios to stop the attack. How far are you willing to go? In one of our engagements, the attacker made it as far as the domain admin on the domain controller where the security team in play had to make a split-second decision to fully disconnect their systems from the internet in order to buy time for response. Fortunately, it worked for them.

As close as that team was to a ransomware attack unfolding, this scenario isn't all that uncommon. It could be worth asking — if your organization were in the same situation, what would you do? Would this level of disruption be acceptable to the business? Would you be able to effectively respond without connectivity for your remote security staff? Are there other response options that you would have to buy?

We've seen rapid, decisive action under pressure be a key ingredient in successful response. Knowing and practicing your game plan before you need it could make all the difference.

To Stop Ransomware, Don't Look for the Ransomware

Modern ransomware attacks (really ransomOps), don't deploy the ransomware binary until the very end of the attack. This means that if you see the ransomware itself, you'll most likely be too late.

This is a common misconception because to stop these attacks in progress, you'll need to detect and respond to the steps that come BEFORE ransomware is deployed. The reality is that that you'll almost certainly be operating without full knowledge of the adversary or their end game. In many cases, you'll see a rapidly-progressing attack, and potentially some telltale signs in tooling or C2 infrastructure that allow you to make an educated guess about what's happening.

Here, your response plans will need to focus on a more general class of intrusion and attack progression, then, understanding that the endgame is just a probability and not a certainty.

Accounts and Admin Tools are Key

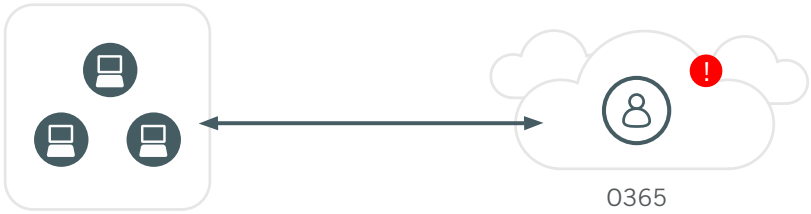
We've observed exploits used to gain initial access, and occasionally for lateral movement. But, as with most modern attacks, the focus is on credentials — admin and service accounts. In combination with admin protocols, these are the favored tactics for virtually all ransomware affiliates.

The intent, as in many attacks, is to get to domain admin on the domain controller to launch the final phase of the attack. From this vantage point, it's easy to get access to the most valuable data. It's also possible to deploy ransomware blazingly fast, using admin tools including GPO.

Due to the focus on credentials, it's absolutely key to carefully monitor the use of all privileged accounts as we've seen this reliably be one of the most valuable attack detection signals.

Common Themes

Vectra analysts compiled user, process and security challenges that were common across different customer engagements.



Initial Access:

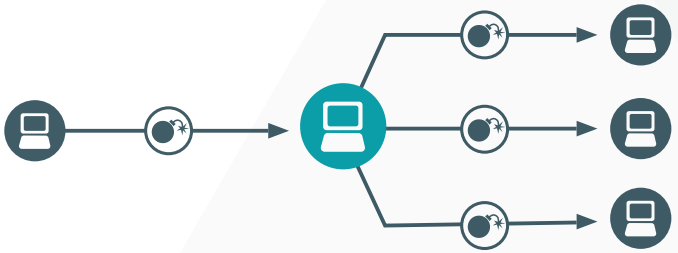
- Attackers continue to scan for vulnerabilities on publicly available, internet facing services and systems.
- Servers running RDP, FTP or VPN are popular targets, providing initial access into enterprises and cloud.
- Lack of MFA is a gap commonly targeted.
- Attack progression in some cases took hours from initial entry, and in other cases took days or even weeks. There is time for security teams to detect and respond early, but it does require 24x7 vigilance.

C2:

- Cobalt Strike seems to be the current favorite tool.
- Popular remote access tools, irrespective of if they were sanctioned or unsanctioned, were also used to control systems. In one case, we detected Cisco AnyConnect software used to control machines on the inside, by a human on the outside.

Recon and Lateral Movement

- In most cases scanning was aggressive, and included network mapping, rDNS queries, and share enumeration. The rapid scanning generally made the attacks visible within minutes of initial access.
- Credential-related recon, including LDAP queries and RPC calls to map credential locations, were also common.
- Lateral movement in the early stages included common exploits. Later stages relied mainly on credentials and admin protocols.



Exfiltration

- Free fileshare sites were commonly used to upload reconnaissance information for analysis. These included Mega Upload (mega.com) and temp.sh.

Recommendations

Our teams work closely with security teams daily, responding to critical alerts generated by the Vectra AI-driven threat detection and response solutions. When we initially engage with customers, it is not obvious if a threat is ransomware. As alerts grow in severity, we're able to gain additional clarity and context about the attack and determine if it is in fact ransomware. We have found an array of security tools and security practices that make it harder for adversaries to carry out successful ransomware campaigns and ultimately stop them with certainty. This includes.

Prevention

- Regularly assess your external security posture and implement high-priority fixes. Focus especially on remote access infrastructure and commonly-vulnerable services like RDP and FTP, which have proven popular targets.
- Enable MFA wherever possible on any identity providers or remote access infrastructure.
- In general, strong preventative controls, rules and policies make it harder to escalate privileges even post-access, which buys more time for response.
- A special area of focus is on privileged accounts. While operationally challenging, the more that can be done to focus use through jump servers and privileged account management systems, the harder the escalation path will be.

Detection

- There is time to stop the attack after the ransomware actor has gained access and before data is exfiltrated or ransomware is deployed.
- Invest in threat detection and response across your network, identity infrastructure, cloud and endpoint to maximize the odds of early detection.

Investigation and Response

- Ransomware attacks can progress fast, any time of the day or night. Ensuring that you are monitoring critical alerts 24x7x365 is key, whether by augmenting internal teams or leveraging managed detection and response (MDR) or MSSP offerings.
- Integrating telemetry from network, endpoint, and cloud logs provides the best context, clarity, and enrichment in investigating threats and arriving at a definite root cause.
- Looking back for increased scanning activity of your DMZ prior to the initial access, in combination with OSINT, may provide an early assessment of the likely threat actor and provide more clarity in response.

For more information contact us at info@vectra.ai.

Email info@vectra.ai vectra.ai