VECTRA
SECURITY THAT THINKS.®

INDUSTRY INSIGHTS

Top Threat Detections Seen Across Healthcare Organizations

Healthcare and Cybersecurity Today

The average number of healthcare data breaches in the US alone is 54 per month—slightly more than two per day, according to the HIPPA Journal's 2021 Healthcare Data Breach Report. But cyberattacks on healthcare institutions span the globe as well, in fact the attack on Ireland's Health Service Executive (HSE) was one of the largest attacks to date in 2021—causing all types of havoc. In many cases, ransomware is a large culprit and one that continues to have lingering impacts long after attacks are reported. Widely known for its economic impacts due to the brash demands criminals make in exchange for encryption keys, these attacks have much different implications when it comes to the healthcare sector—which is precisely why this industry remains a target.

Ransomware attacks that carry through in a healthcare system can mean stolen medical records and data but can also be physically disruptive when they cause delays in patient care. At that point this becomes much less of a technology issue, but rather one that has the potential to diminish the quality of life and care that people need to live. So, as attackers gain skill and expand their reach into new attack surfaces like the cloud—how can healthcare security teams begin to understand attacker behavior and tactics in order to stop them?

> Ransomware attacks that carry through in a healthcare system can mean stolen medical records and data but can also be physically disruptive when they cause delays in patient care.

KEY HIGHLIGHTS

- **Top Threat Detections**: Detections detailing abnormal or unsafe activity in Microsoft Azure AD and Office 365 across healthcare.
- **Suspicious and Risky Activity**: A high level of suspicious Power Automate flow creation could indicate an attacker is configuring a persistence mechanism.
- **Closing the Gap**: Artificial intelligence (AI) provides the vision and visibility required to truly know what's going on in your cloud environment.

While it’s true that the digital transformation has broadened the attack surface, this doesn’t mean ransomware attacks and other forms of cybercrime like account takeovers can’t be stopped. However, it does require a new way of thinking to do so because legacy security tools and endpoint solutions are regularly proven to be bypassed by attackers and that trend has no indication of slowing down. By adjusting our thinking that ransomware attacks can be stopped, but not necessarily prevented—we might just stand a chance. Being able to detect attack behavior that’s already inside a healthcare environment is possible with the right vision and visibility.

> Being able to detect attack behavior that’s already inside a healthcare environment is possible with the right vision and visibility.

The recent Spotlight Report—Vision and Visibility: Top 10 Threat Detections Across Microsoft Azure AD and Office 365 takes a deep look at this exact scenario across all industries, however, the industry insights highlighted below focus on the healthcare sector. These industry insights reveal the top threat detections seen across the Vectra customer base that help ratify attacks for healthcare organizations in Microsoft Azure AD and Office 365. The detection information presented can be put to use along with the right vision and visibility to help keep things on track. A vision for what authorized use should look like and the visibility to monitor and measure deviations from that vision. As the cloud continues to change everything we know about security, the right data along with meaningful AI can help bring clarity to the cloud

Top Threat Detections Across Healthcare

While these insights focus on the top detections spanning across Vectra's healthcare customers, it's important to keep in mind that threat detection and response is easiest when adversaries take actions that are obviously malicious. This makes it critical that modern network defenders understand the intersection that may exist between the types of actions an adversary would need to take to progress towards their objectives and the behaviors routinely taken by authorized users across the enterprise. Many of the detections discussed in this report represent anomalous behavior and not all of these detections are due to malicious activity. Let's see what detections are frequently being trigged in this environment.

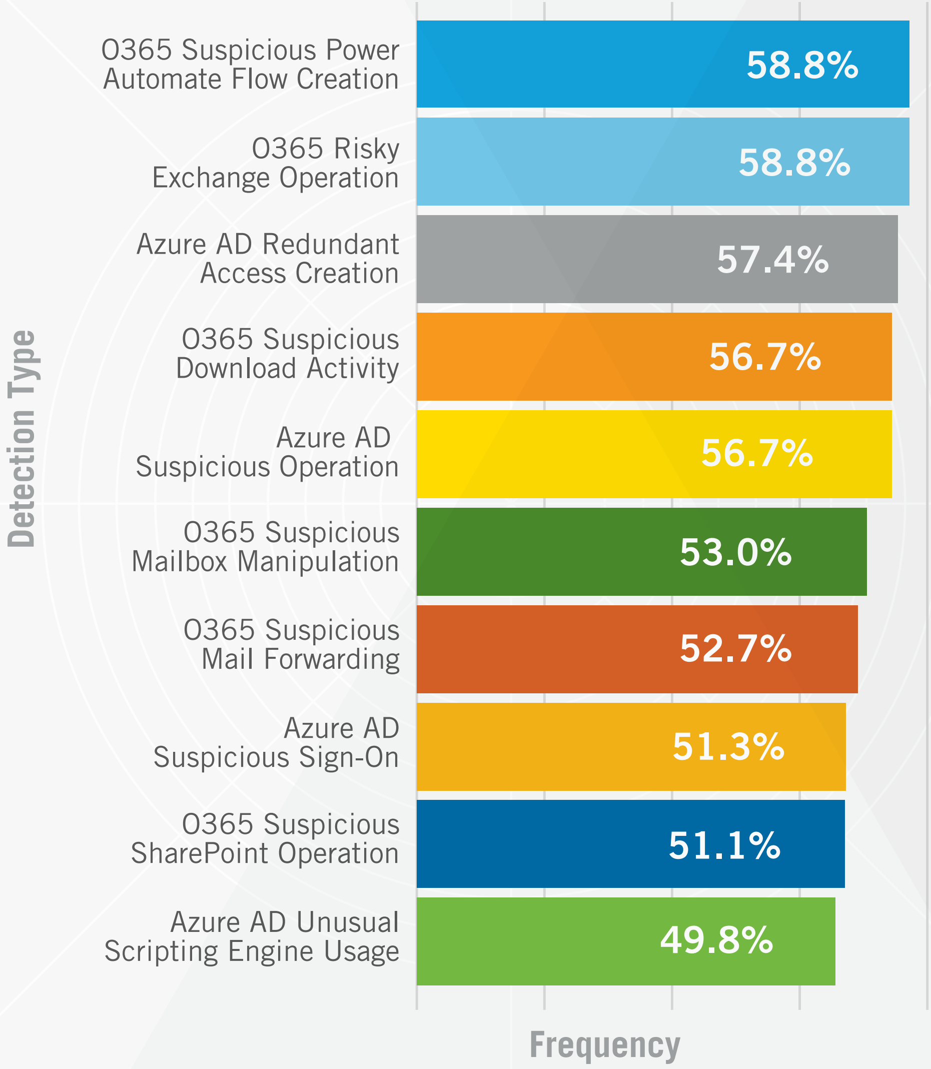
The most frequent detection seen across the healthcare sector was O365 Suspicious Power Automate Flow Creation.

Power Automate Can Create a Power Struggle with Attackers

Result: The healthcare sector experiences a high level of O365 Suspicious Power Automate Flow Creation, O365 Risky Exchange Operation and O365 Redundant Access Creation.

Analysis: The most frequent detection seen across the healthcare sector was O365 Suspicious Power Automate Flow Creation, which could indicate that an attacker is configuring a persistence mechanism. The education sector also saw this detection in its top three, however, it ranked seventh on the overall top 10 detections list across all industries. Power Automate

Healthcare Sector Top 10 Detections



helps automate mundane tasks like saving email attachments to OneDrive, recording form responses in SharePoint and all types of other convenient uses, however, it's on by default in Office 365 and comes standard with hundreds of connectors.

Even with basic, unprivileged Office 365 access, Power Automate is a powerful tool that is appealing to attackers because of the access it would provide for them to live off the land. In March 2020, Microsoft's Response Team actually uncovered threat actors using Power Automate to exfiltrate data at a multinational organization where the attackers went undetected for 213 days. All multinational organizations should rationalize access to Power Automate Flow only for users who require it and closely monitor account manipulation that can lead to elevation of privileges and theft of information.

Power Automate is a powerful tool that is appealing to attackers because of the access it would provide for them to live off the land.

In addition to the O365 Suspicious Power Automate Flow Creation detection, healthcare customers experienced O365 Risky Exchange Operation and O365 Redundant Access Creation detections in their top three as well. O365 Risky Exchange Operation detection can indicate that access is being provided to sensitive information that would be available in email, which can indicate that an attacker is manipulating Exchange to gain access to data to move further into their attack progression. While O365 Redundant Access Creation means that administrative privileges have been assigned to an entity which may indicate redundant access is being created by an attacker to guard against remediation.

O365 Risky Exchange Operation detection can indicate that access is being provided to sensitive information that would be available in email.

Overall, healthcare customers generally exhibited lower relative detection frequencies compared to most other industry verticals. However, the automation of workflows via Power Automate and provisioning of administrative rights to an application, user, or service principal highlight behaviors that attackers have commonly utilized to gain access to email and sensitive information. These are actions present in Office 365 that all customers have, making visibility into account activity a crucial part of managing these attack surfaces.

Knowing “Your” Account Behavior

Regardless of industry, attackers are flocking to the cloud as a target for attacks. Office 365 is an incredibly useful and powerful tool, which is why over 250 million people pay to use it. But when you have that type of user activity, attackers view it as a massive opportunity, and they’ve shown the motivation to target any organization where there’s an opportunity to extort money or steal assets. Microsoft Office 365 and Azure AD are just one part of the large attack surface that organizations need to manage, but as shown here with Power Automate, it’s incredibly convenient to leverage for speeding up processes, but it’s also important to understand the risks and know exactly how tools like this are being used.

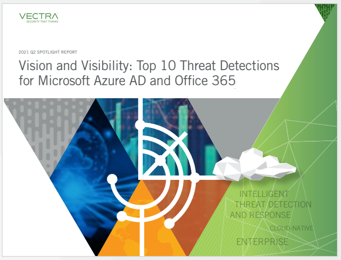
The difference between attacker behavior and privileged account usage can be a blurry line without the ability to collect the right data that is properly aligned with defined vision and visibility. But it’s important to get to a point where you know what authorized use looks like in order to understand the behaviors adversaries are going to take. Meaningful AI can help close the gap in your Office 365 and Azure AD accounts, so you have the right data to detect when something out of the ordinary happens. Are you sure which privileged or unprivileged users are leveraging tools like Power Automate? It probably wouldn’t hurt to know.

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

Email info@vectra.ai   vectra.ai

Version: **071321**

Get the full report



VECTRA
SECURITY THAT THINKS

2021 Q2 SPOTLIGHT REPORT

Vision and Visibility: Top 10 Threat Detections for Microsoft Azure AD and Office 365

INTELLIGENT THREAT DETECTION AND RESPONSE

CLOUD-NATIVE

ENTERPRISE

Cognito® Detect for Office 365 from Vectra® automatically detects and responds to hidden cyberattacker behaviors, accelerates incident investigations, and enables proactive threat hunting.

About Vectra

Vectra® is the leader in threat detection and response—from cloud and data center workloads to user and IoT devices. Its Cognito® platform accelerates threat detection and investigation using AI to enrich network metadata it collects and stores with the right context to detect, hunt and investigate known and unknown threats in real time. Vectra offers four applications on the Cognito platform to address high-priority use cases. Cognito Stream™ sends security-enriched metadata to data lakes and SIEMs. Cognito Recall™ is a cloud-based application to store and investigate threats in enriched metadata. Cognito Detect™ uses AI to reveal and prioritize hidden and unknown attackers at speed. And Cognito Detect for Office365 and Azure AD™ finds and stops attacks in enterprise SaaS applications and the Microsoft 365 ecosystem. For more information, visit vectra.ai.