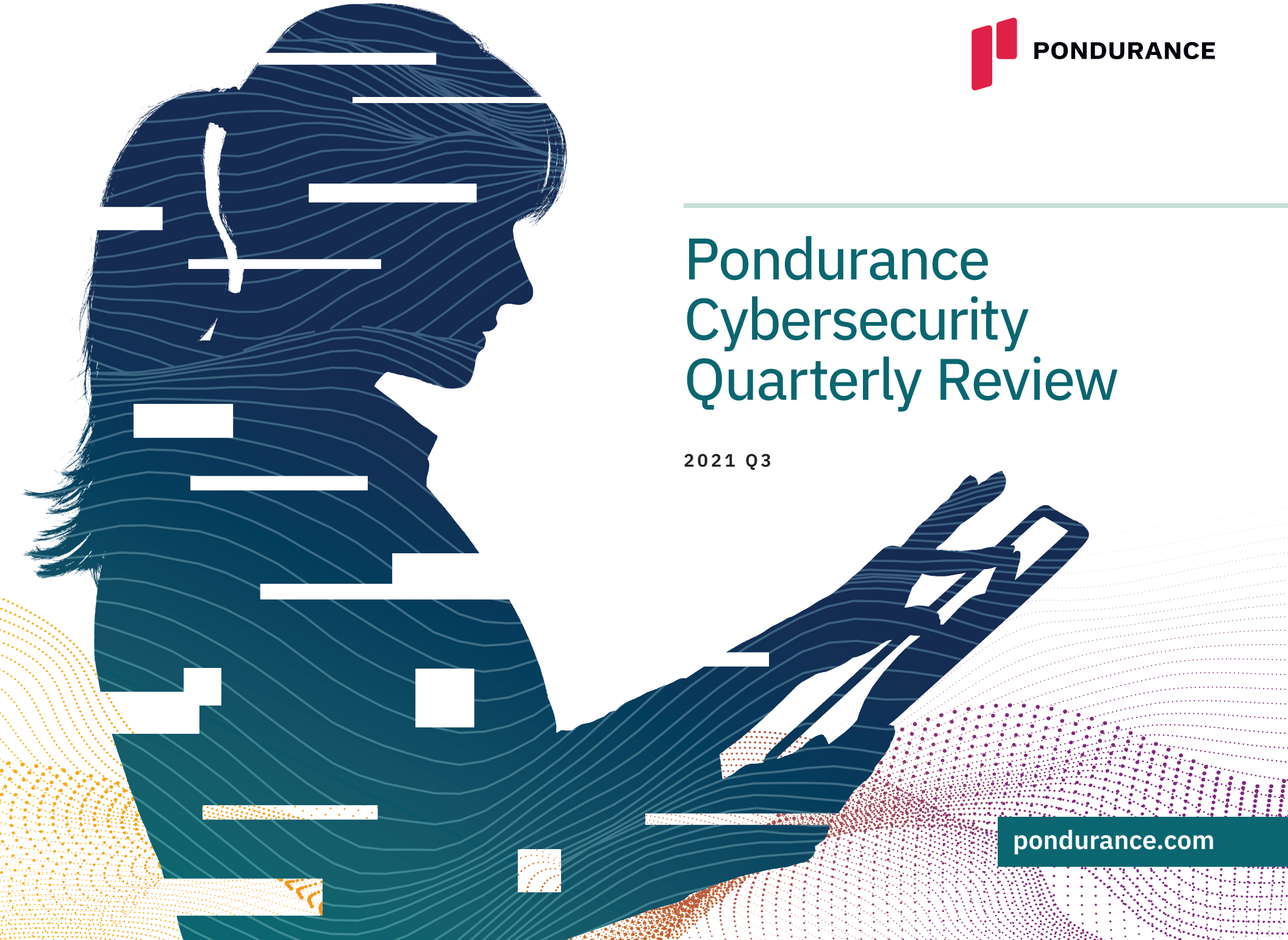


PONDURANCE

Pondurance Cybersecurity Quarterly Review

2021 Q3

pondurance.com

The Pondurance Cybersecurity Quarterly Review: 2021 Q3 shares insights and intelligence collected by Pondurance research teams, providing a glimpse into the growing attack surface and threats that organizations face today.

PONDURANCE

Making a Dent in the Fight Against Cybercrime

The cybersecurity industry is growing quickly with close to $20 billion in venture capital investments coming into the industry this year, yet we still have thousands of organizations experiencing data breaches and ransomware. While we've been adding complexity into our digital ecosystem and attaching more layers to the internet, cybercriminals have gained sophistication and are embracing innovations like cryptocurrency, ransomware-as-a-service and supply chain attacks.

From the Solarwinds supply chain attack to numerous Microsoft Exchange Server exploits and the Colonial Pipeline ransomware attack, cybercriminals have taken full advantage of the disorderly environment caused by COVID-19 and used it as their playground. Is it time for everyone to pull together in the fight against cybercrime?

Listen to the full podcast where Niloofar Razi Howe, Chair of the Board of Directors, and Lyndon Brown, Chief Strategy Officer, at Pondurance examine:

- Today's global threat landscape.
- The power of U.S. government state surveillance and the Civilian Cyber Security Reserve.
- Common cybersecurity pain points for modern businesses.
- Confusion and some clarity with security information and event management (SIEM) versus managed detection and response (MDR) versus extended detection and response (XDR).
- Pondurance's approach to navigating the complex cybersecurity space.

LISTEN HERE

> "There is no silver bullet. It will be a hundred different things we have to do simultaneously to make a dent in the issue, and we need to do more faster."
>
> - Niloofar Razi Howe

> "The attack landscape is drastically increasing, and the average business simply does not have the threat intelligence or the human capital to not only keep the attackers out but also deal with attackers once they gain access."
>
> - Lyndon Brown

Phishing Activity Increases in the Microsoft 365 Tenant

This year, we've seen a notable increase in phishing attacks and many in the Microsoft 365 tenant. Cybercriminals have adopted many different techniques to blend in and make it more difficult for the end user to spot their activity. Microsoft shared that they're seeing new techniques such as:

- Brand impersonation with procedurally generated graphics.
- Text padding with invisible characters.
- Zero-point font obfuscation.
- Victim-specific uniform resource identifier.

We are also seeing:

- **New inbox rules:** Cybercriminals create new inbox rules so that if anyone replies to an email or it bounces, it will go to the trash or a hidden folder in an effort to hide the activity. That way, the end user will not report it. We've also seen bad actors create inbox rules to forward important emails to their controlled domain. This is common for financial terms such as "payments," "statement" and "invoice" as well as for healthcare terms such as "patient data" or "rounds." They then may exfiltrate the data to hold it for ransom.
- **Password spraying:** If a bad actor is able to compromise an employee's credentials, the actor will try to log in to additional accounts based on that password in a brute force style attack.

We recommend using the free tool Have I Been Pwned to gain knowledge into data breaches and know which of your accounts have been affected.

> "Many think that threat actors are not sophisticated, but they are masters of the Office 365 environment and masters of financial fraud."
>
> - Pondurance

PONDURANCE

Pondurance Uncovers Conti Ransomware Group Capitalizing on Microsoft Exchange Vulnerabilities

The Pondurance research team recently uncovered that the Conti ransomware group is now obtaining access to environments stemming from the Hafnium exploits that occurred back in February and March 2021 within Microsoft Exchange. These zero-day vulnerabilities could affect hundreds of thousands of systems.

Our team identified that on-premises Microsoft Exchange servers still had web shells installed that stemmed from the Hafnium vulnerability back in late February and early March 2021. We also identified that the Hafnium exploitation chain resulted in the installation of an unauthorized and abused remote monitoring and management (RMM) agent. The unauthorized RMM tool remained present on the victim machine for approximately four months and granted the ability for remote interaction with the victim machine. In July, the RMM tool was utilized by outside actors to install additional malicious frameworks, including Cobalt Strike. The resulting actions concluded with the installation of Conti ransomware.

Although Microsoft issued patches and diagnostics following the initial February exploit, organizations likely patched these systems without performing due diligence, and systems are still compromised.

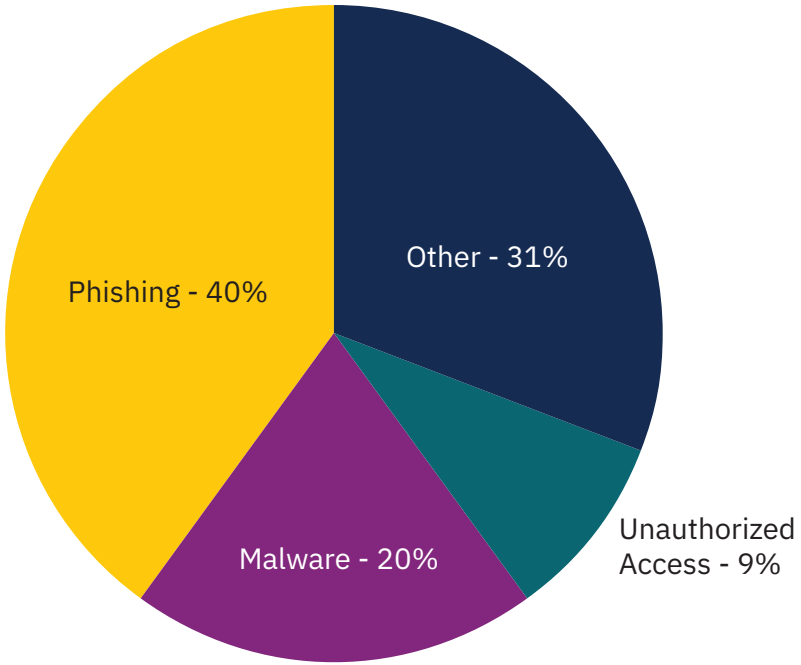
Learn more about this vulnerability including tips on how to reduce the costs associated with incident response recovery in this blog.

READ MORE

Fraud attack glossary

- **Digital forensics** is the use of specialized, investigative techniques and technologies to determine whether a cyber incident occurred on computer systems and provide legally defensible information about the sequence of those events.
- **Incident response** is a methodical process to investigate and mitigate a cybersecurity threat with the goal of minimizing damage and reducing recovery time and costs.
- **Password spraying** is a type of brute force attack where the bad actor tries to gain unauthorized access to an individual account by repeatedly guessing the password in a short period of time.
- **Vulnerability** is a weakness that can be exploited by a threat actor. The attacker uses any means possible to gain unauthorized access or privileged control to an application, network, service, endpoint or server.

Q3 2021 ATTACK VECTORS



PONDURANCE

FEATURED ARTICLE

The Race To Beat Cybercriminals To Open Vulnerabilities

Staying ahead of security vulnerabilities can be difficult, time-consuming and daunting for organizations of all sizes. Every year, thousands of new security vulnerabilities are identified and exploited by bad actors due to the powerful tools they have at their disposal. On the other hand, some organizations, especially those in the healthcare industry, cannot take critical applications and systems offline to patch vulnerabilities in a timely manner, leaving them exposed to ransomware and other types of attacks.

PONDURANCE

Vulnerability management is a key component to provide the highest levels of security within an organization. Taking a risk-based approach to managing cyber risks involves a process that consists of discovering, prioritizing, assessing, remediating and verifying vulnerabilities found in hardware, software, networks, on-site or third parties.

Organizations are allocating as much as $650,000 annually to employ an average of five security analysts dedicated to patching.1 If a team lacks the expertise to scan for vulnerabilities, review the results and patch accordingly, they run the risk of chasing vulnerabilities that are not real vulnerabilities. Ultimately, this could lead to increased false positives and burnout among the group.

PATCH SMARTER NOT HARDER

When implementing a comprehensive **vulnerability management program** (VMP) within your organization, prioritizing and quantifying risk based on the severity can help identify which vulnerabilities to address first. Vulnerability prioritization is unnecessary for a VMP; however, deploying this strategy can improve your organization's productivity because your team will spend less time and resources on vulnerabilities that do not improve security.

Focusing on external and internal vulnerabilities is essential to a comprehensive VMP strategy. External vulnerability scans are performed from outside of your network to find open ports, including cross-site scripting and SQL injections, which bad actors typically leverage to gain unauthorized access to your environment. External scans are ideal when you need to verify the strength of external-facing services.

Internal vulnerability scans are performed inside your network to give you more insight into your environment than an external scan. An internal scan is used to verify that patching has occurred or when you need a detailed report of vulnerabilities within your network — often used for compliance requirements.

COMPLIANCE IS BECOMING A SOLID DRIVER FOR VMPS.

An annual penetration test (pentest) is crucial to an organization's security posture and VMP. A pentest is an authorized simulated cyberattack on your organization's environment, which serves as a way to evaluate your systems' security. Based on the findings, a pentest can provide an enormous amount of information into where your security posture is at its weakest, allowing you to remediate by severity.

Vulnerability management is more than a program; it is a lifecycle that can keep you ahead of threats if appropriately prioritized. You don't have to go at it alone! In fact, having a third party to identify and prioritize vulnerabilities can be objective and eye opening. Learn more about how we can help.

How Pondurance Can Help

Our mission is to ensure that every organization is able to detect and respond to cyberthreats — regardless of size, industry, or current in-house capabilities. We combine our advanced platform with decades of human intelligence to decrease risk to your mission.

CLOSED-LOOP MANAGED DETECTION AND RESPONSE

Recognized by Gartner, Pondurance provides 24/7 U.S.-based SOC services powered by analysts, threat hunters, and incident responders who utilize our advanced cloud-native platform to provide you with continuous cyber-risk reduction. By integrating 360-degree visibility across log, endpoint, and network data and with proactive threat hunting, we reduce the time it takes to respond to emerging cyberthreats.

Pondurance MDR is the proactive security service backed by authentic human intelligence. Technology is not enough to stop cyberthreats. Human attackers must be confronted by human defenders.

INCIDENT RESPONSE

When every minute counts, organizations need specialized cybersecurity experts to help them respond to a compromise, minimize losses, and prevent future incidents.

Pondurance delivers digital forensics and incident response services with an experienced team capable of guiding you and your organization every step of the way. This includes scoping and containing the incident, determining exposure through forensic analysis, and helping to quickly restore your normal operations.

SECURITY CONSULTANCY SERVICES

Our specialized consultancy services will help you assess systems, controls, programs, and teams to uncover and manage vulnerabilities. Our suite of services ranges from penetration testing to red team exercises, along with compliance program assessments for highly regulated industries. We provide security incident response and business continuity planning to put you in the best position to defend against and respond to cyberattacks.

PONDURANCE

500 N. MERIDIAN ST., STE 500
INDIANAPOLIS, IN 46204

About Pondurance

Pondurance delivers world-class **MDR** services to industries facing today's most pressing and dynamic cybersecurity challenges including ransomware, complex compliance requirements, and digital transformation accelerated by a distributed workforce. By combining our advanced platform with our experienced team of analysts, we continuously hunt, investigate, validate, and contain threats so your own team can focus on what matters most.

Pondurance experts include seasoned security operations analysts, digital forensics and incident response professionals, and compliance and security strategists who provide always-on services to customers seeking broader visibility, faster response and containment, and more unified risk management for their organizations.

Visit **www.pondurance.com** for more information.

Sources:

1. 60% of Breaches in 2019 Involved Unpatched Vulnerabilities, Security Boulevard, Oct. 31, 2019.