PONDURANCE



3 Techniques for Stopping Domain Controller Attacks

pondurance.com



Introduction

Through our Managed Detection and Response (MDR) and Incident Response engagements, we have seen an increase in attacks targeting domain controllers (DC). In this eBook, we will take a look at three common techniques for gaining unauthorized access to domain controllers, as well as the foundational hygiene tips you can take to protect your domain controller.

3 Common Attack Methods & Prevention Techniques

HERE ARE COMMON TECHNIQUES WE OBSERVE ATTACKERS USING TO IMPROPERLY ACCESS DOMAIN CONTROLLERS AND THE BEST WAYS TO PREVENT THESE ATTACKS:



Compromised User and Administrative Credentials

Attack Method: Gaining user credentials for an endpoint, administrative credentials, or a virtual private network makes the first step of a domain controller compromise much easier.

Prevention: To prevent a bad actor from seizing credentials, ensure that multifactor authentication is enabled on compatible protocols for all domain level systems.



Legitimate Credentials via Remote Desktop Protocol (RDP)

Attack Method: RDP is a legitimate tool that enables IT departments to remotely and easily access and manage Windows systems. RDP exploit programs and services are easy to purchase and use. RDP is the most frequently abused protocol when considering lateral movements, network entry, and exploitation.

Prevention: If you must enable RDP, ensure that there are compensating controls associated with it such as registered origin IP addresses, destination-only access, and individual credentials with multifactor authentication added.



Altering Configurations Over Server Message Block (SMB)

Attack Method: SMB is a critical protocol for active directory and also serves as a network file sharing protocol. Backdoor installation over SMB with legitimate credentials can occur as well as other user-initiated actions like phishing or clicking a malicious payload file.

Prevention: SMB requires protection from attacks where a server or device might be tricked into contacting a malicious server running inside a trusted network or to a perceived trusted remote server outside the network perimeter. Segmentation, traffic monitoring, enhanced authentication, and firewall best practices can enhance security, preventing malicious traffic from accessing the system or its network.

For more information on attack methods and approaches to protecting your domain controller, read our The Domain Controller...An Achilles Heel white paper.

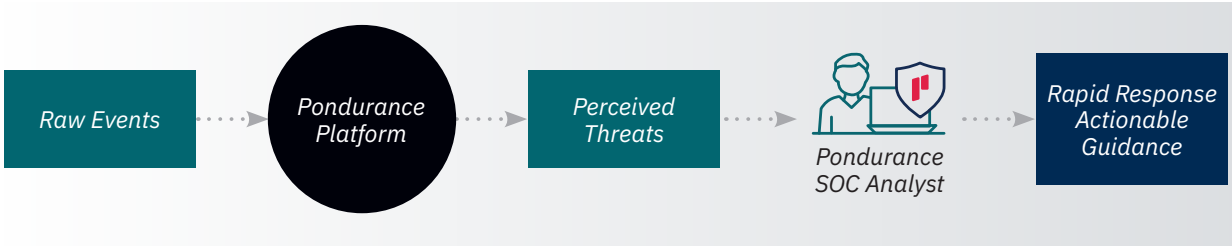
How Pondurance Can Help

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.

MANAGED DETECTION AND RESPONSE

Recognized by Gartner, Pondurance provides 24/7 U.S.-based security operations center (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

Conclusion

As domain controller attacks continue to increase in frequency and evolve, it is critical that your organization be aware of current attack patterns that lead to an attacker's success and know what steps to take to reduce exposure. By following prevention steps and developing a plan, you can lower the probability of a successful cyberattack through your domain controller.

Want to dive deeper into attacks on domain controllers?

Read our white paper: The Domain Controller...An Achilles Heel.

Or contact us to discuss!



PONDURANCE

PONDURANCE

Copyright © 2021 Pondurance

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.



pondurance.com

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