PONDURANCE

The Domain Controller... an Achilles Heel

How attackers use domain controller penetration for large-scale compromises.

INTRODUCTION

Pondurance predicts that domain controller compromises will become one of the primary focus areas for improving security for the industry and affect governments, organizations and businesses alike in 2021. Ransomware will lead the headlines in terms of quantity, but exfiltration and weaponization of intellectual property will become a focus area for many technology-based companies and the defense industrial base. As always, personal identifiable information (PII) will be widespread and drive high fines and significant regulatory consequences. Pondurance has spent considerable time analyzing common attack patterns to better reduce compromise, shorten dwell time and prevent damaging compromises. In doing so, we have identified the compelling common factors associated with most large-scale successful breaches, and the biggest business impact is the compromise of the domain controller.

The most common way a controller is initially compromised is through security hygiene issues, such as unpatched systems, open ports, misconfigurations, stolen credentials and bad user behavior. However, we have also recently seen more sophisticated and highly organized attacks to break through even the most protected and advanced environments so this trend will continue. While compromising a domain controller is not the only way, it is a common tactic that attackers use to quickly achieve their intended outcome. A compromised domain controller is by far the most common denominator related to large-scale breaches and sophisticated cyberattacks.

Prioritize the Domain Controller as a Potential Attack Vector

From a business perspective, relatively small investments have been made to create a focused strategy in domain controller security and ongoing monitoring and testing, and those may be some of the best dollars spent in your security program. When prioritizing assets, the domain controller is often overlooked as a critical asset but in most cases, it should be at the top of the list. A number of exploit paths are attributable to the success of a compromise, often blurring the lines between conduit, condition and cause. For instance, abusing business email is still a leading exploit path for getting an attachment onto a user's system.

Additionally, limited security awareness training is another factor, albeit more of a condition that contributes to the propagation of a number of systems and data compromises including unauthorized system access and ransomware. The nature of root cause is also worth examining when considering the capability to broaden system access and ransomware deployment across an enterprise. That's where the compromise of the domain controller comes into play. While completely eliminating unauthorized access and ransomware may not be an immediate reality, despite the hardening of the domain controller, reducing or eliminating the spread within an organization can be the difference between a nuisance and a business-crippling situation.

COMPROMISES TO THE DOMAIN CONTROLLER

Ransomware receives much attention, but the problem is not just ransomware. Many other broad compromises are accomplished through the domain controller. Government, service providers and technology organizations of all sizes are being targeted and attacks on these types of organizations are expected to accelerate in 2021 and beyond.

Classifications of breaches typically fall into four categories:

- **Confidentiality breach** – an unauthorized or accidental disclosure of or access to personal data
- **Integrity breach** – an unauthorized or accidental alteration of personal data
- **Availability breach** – an accidental or loss of access to or destruction of personal data
- **Safety** – a recent addition because an attack can actually impact human life, which has occurred with autonomous vehicles, health care devices and operational technology in general
- **Intellectual property breach**, where critical information or trade secrets or tools can be used nefariously at a much bigger scale

PONDURANCE

The impact to an organization falls into several areas:

- Risk to revenues
- Risk to mission
- Risk reputation
- Risk to regulatory risk, compliance and legal exposure
- Risk to national security

EXFILTRATION AND ACCESS

According to various published research findings, the average dwell time lasts between three and nine months. Dwell time is the amount of time during which an attack goes undetected. Historically, the longer the dwell time, the more negatively impacted the target becomes, often due to the number of systems impacted and the amount of data exfiltration. For more sophisticated compromises typically involving nation states, the actor can often be in the environment for a year.

COMPROMISES TO THE DOMAIN CONTROLLER

- Credit card information (payment card industry-regulated data)
- Consumer and customer information (personal identifiable information)
- Employee information (including health care information and personal identifiable information)
- User credentials and domain controller access
- Business email access
- Automated clearing house and wire fraud
- Intellectual property

MANUFACTURING, TECHNOLOGY AND SOFTWARE

Companies that design physical products or Internet of Things (IoT), industrial IoT and operational technology (OT) access and control

- Code and intellectual property exfiltration that can be weaponized
- Consumer and customer information (personal identifiable information)
- Weaknesses and vulnerabilities in products or services
- Key personnel

RETAIL

- Product and service pricing and planning information
- Employee information

HEALTHCARE

The value of stolen health care records continue to increase in value on the dark web and black market.

- Health care records
- Insurance information and insurance fraud
- Access to health care devices

GOVERNMENT AND DEFENSE INDUSTRIAL BASE

The objectives of state-affiliated or government-sponsored actors align with either the political, commercial or military interests of their country of origin and often are well funded.

Actors are attempting to gain access to information about their targets or access to their targets through trusted relationships with the third-party company, such as contractors, government system integrators and software and devices manufactured for networking, IT or cyber security. Often, sensitive information held by a third party may not be as well protected as it is at the government-entity level, but more and more regulatory attempts are being put in place through the Defense Acquisition Federal Regulation Supplement and cyber security Maturity Model Certification requirements. For both direct government entities and contractors, targets include:

- Defense intellectual property
- Employee and contractor background checks and clearance levels
- Command and control of critical assets
- World secrets

POWER AND UTILITIES

As approximately 10,000 power and utility plants in the U.S. and the distribution infrastructure become more IT based and automated, there is increasing specialized targeting of these facilities.

- OT and IT infrastructure
- Design and engineering information
- Connectivity to other parties

PONDURANCE

THIRD-PARTY HOP

Finding the weakest link includes the bad actors looking at third-party vendors, connection, etc.

- Compromise for any of the aforementioned methods apply but instead actors go through a third-party relationship by leveraging the technology or engineering to gain access to third parties.
- Another common exploit path is the use of shared local or domain administrator credentials across domain-joined devices and, in many cases within the same organization, nondomain devices.

IMPERSONATION

From phishing and business email hijacking to stolen credentials and social engineering, impersonation is a classic way to gain access, get information or have someone take action on behalf of the bad actor.

WEAPONIZED IPS

While not as common in the headlines, denial of service and distributed denial of service continue to be major issues for many businesses, especially those where online availability ties directly to revenue such as gaming, entertainment and hospitality services. Compromise of a large number of systems is needed and often executed with significant dwell time before system owners, individuals or businesses become aware.

RANSOMWARE

A staggering 100 million ransomware cases have been observed over the last four years alone, and new cases are now expected to occur every 11 seconds, according to some sources. Unlike other compromises, a ransomware compromise may require a direct cost if the ransom is paid, and there also is a cost for incremental cleanup and follow up versus other attacks that have less public and less definable costs measured over a significant period of time. Also, unlike a breach where the damage is done and the only option is cleanup, ransomware carries the heavy business decision burden of whether to pay or not pay.

OWNERSHIP OF YOUR DOMAIN CONTROLLER

The sensitivity and totality of the domain controller is not novel regarding breach or systemic exploitation. In fact, gaining domain administrator or enterprise administrator privileges is often the proverbial crown jewel of the most basic penetration test. Once an actor gains credentials with expansive local administrator privileges, the actor can run through a number of exploits that allow data exfiltration, extended reconnaissance and outright theft in addition to executing a ransomware payload.

In almost all enterprise big-impact, large-scale breaches, a compromised domain controller practically guarantees success. In fact, the actor can also weaken or entirely disable other controls with domain administrator privileges, which makes a defense-in-depth strategy so critical. If an organization places sole reliance on, for instance, an endpoint detection and response (EDR) platform to prevent a ransomware payload and the actor has gained access to the domain controller, the organization may be severely disappointed with the result. A defense-in-depth strategy contemplates ample prevention with dynamic detection controls to provide the most favorable outcomes. A key part of the preventive strategy should address technical and process controls related to the domain controller.

There are many ways for a breach to occur. We've discussed the nature of a broad ransomware infection distributed across the enterprise, but systems can be affected in much smaller numbers with stolen credentials, through email, as a result of unpatched systems, using open ports and so forth, though the outcome is typically limited to a single or few systems. Clearly, the impact of such an event is relative.

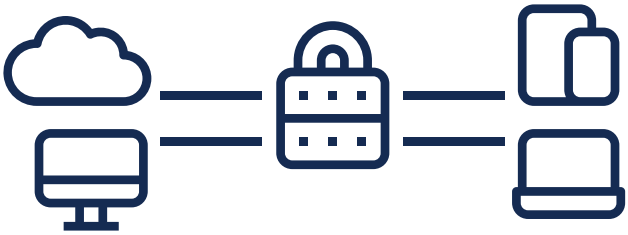
COMMON TECHNIQUES FOR UNAUTHORIZED ACCESS TO DOMAIN CONTROLLERS

Let's explore some of those occurrences. The following methodologies are the most common techniques for accessing domain controllers:

- Compromised user and administrative credentials continue to be a common vector for compromise. This technique takes advantage of human error, allowing user credentials to be captured or malware to be loaded.
- Legitimate credentials via remote desktop protocol (RDP) are common. RDP is a legitimate tool that enables information technology departments to remotely and easily access and manage Windows systems. When proper security is not applied, RDP can give attackers easy network entry or lateral movement routes. RDP exploit programs and services are easy to purchase and use, or the attacker can buy stolen credentials for organizations from

$10 to $100 per credential, depending on the perceived value from the Sodinokibi ransomware-as-a-software (RaaS) operation, also known as REvil and Sodin.

- Sodinkibi RaaS receives a majority of the ransomware. Many have reported that RDP defensive measures have been widely reported and less effective; however, all data supports that RDP is still the most frequently abused protocol when considering lateral movements, network entry and exploitation.



- Altering configurations over SMB to open access over certain protocols is another exploit method, targeting credentials but also using it as an initial entry point. SMB is a critical protocol for an active directory and also serves as a network file sharing protocol. SMB is widely deployed and used by billions of devices in most operating systems, including Windows, Linux, MacOS, iOS and Android. Like RDP, administrators use SMB to access systems, but it is also used system to system for sharing files, data center replication, centralized data management and mobile devices replicating storage for many mobile devices to cloud storage. Backdoor installation over SMB with legitimate credentials can occur based on the above technique and other user-initiated actions (i.e., phishing or clicking a malicious payload such as a file).

For example, if your business is a dental office, a ransomware event may be all it takes to close your doors forever if you are unable to pay the ransom or otherwise recover. To affect large, medium or even small enterprises with a fair number of distributed systems using ransomware, it requires a catalyst to deliver the payload with precision, timing and a level of engineering elegance. Ransomware attackers frequently use a technique to host their payload on a server, where many systems in the network have lateral routes over the Server Message Block (SMB) protocol and typically use a domain controller as a catalyst. From there, the attackers can systematically detonate a ransomware payload to each connecting system. The economy of scale of such an attack is the objective for a skilled attacker looking for a big payout.

- Compromised virtual private network user credentials often make the first step of a compromise much easier. Obviously, multifactor authentication makes this vector much more challenging, if not impossible.
- Exploiting various vulnerable services running on the target domain controller due to lack of patching or from running an unsupported version is a common technique.
- Exploiting other applications running on the domain controller is another method. Why would anyone have other applications running on the domain controller? Sometimes, it's a legitimate need for security or monitoring agents or diagnostic tools. In some situations, however, people put other applications on servers as a temporary solution, and the applications simply never get removed. In a large number of audits, we find unauthorized applications running on domain controllers.

RANSOMWARE EXECUTION

As we mentioned earlier, compromising the domain controller is not the only way to execute ransomware or steal credentials. If, for instance, a user clicks a bad link or exposes his or her credentials and gets malware on the device, the outcome can range from an isolated nuisance to a horrible business-ending scenario, depending on the nature and size of the organization. However, if an attacker parlays an exposed system, ultimately escalating gained privileges to the domain administrator as a pivot to gaining access to the rest of the network, it can be disastrous, no matter your size or your industry and in spite of the technical controls put in place to prevent such an occurrence. To think that the initial set of compromised credentials can come from any system — not just a domain controller as the starting point — can be daunting. That is certainly the desired end state of an experienced penetration tester: Start with simple gains and work toward domain administrator. Since pen testers have proven time and again that this methodology is not difficult, it's easy to imagine a person or group using the same approach, though with complete malfeasance and disregard for any parameters of engagement scope.

One other consideration is domain administration privileges. An attacker need not use malware to systemically encrypt enterprise systems. In fact, Pondurance's Incident Response Team was involved in a case where the attacker leveraged the native BitLocker tool to encrypt the environment, and at that instant, the

systems administrators of the affected organization were unable to undo the deed. They had expected their EDR platform to prevent the issue, and it took some convincing to assure them they were not hit with malware but rather a legitimate tool that is used for the purposes of good. Based on our forensic review, a set of credentials to a single system was leveraged to gain a foothold, upon which the actors escalated privileges to domain administrator. From there, the attackers used their privileges and the conduit of the domain server to roll out BitLocker.

It was fortunate that the master key generated by the attacker was captured by the EDR tool, so while it didn't prevent the attack, the tool demonstrated its merit by logging the key for detective discovery. This is yet another case study to support the development of a defense-in-depth strategy.

PROTECTION OF DOMAIN CONTROLLERS

The domain controller is the heart of any distributed network. Just like the heart of any living creature, it can deliver sustainability with every beat, or it can seize its host with paralysis or even death. Fortunately, prophylactic measures exist that, like with a living heart, can be employed to exercise and strengthen the domain controller, making it more resistant to defeat. In one final analogy to the living heart, despite adequate due diligence, there is no guarantee that the domain controller is impervious to all attacks or can stave off fluke conditions that might otherwise affect its rhythm (e.g., misconfigurations or other errors unrelated to cyberattack). Healthy conditioning is the key, and a little bit of due care can make the difference without having to overengineer or overspend to protect the domain controller. Organizations looking to achieve compliance through configuration hardening (HIPAA, PCI-DSS, CMMC) can do so with real security in mind, not by simply checking a box.

At the highest level, known basic hygiene approaches to protecting domain controllers are the best long-term strategy. The following represent both simple and advanced approaches that organizations should take for protection, all of which can and should be baked into a system hardening program:

- Ensure that multifactor authentication is enabled on compatible protocols, without exception, for all domain level systems to protect against the use of stolen credentials. This simple and relatively inexpensive approach can avoid many stolen credential scenarios.
- Maintain domain controllers with supported release versions and ensure they are patched.
- 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.
- Implement an email defense filtering system, combined with URL/IP outbound blocking capabilities. Malicious emails are privileged vectors for exploit campaigns, while weaponized documents and click-through to malware payload-bearing websites are the main ingredients for almost any spam and phishing attack.
- Similar to RDP, ensure adequate protections are enabled for SMB. SMB is a protocol needed among many applications, so it 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 and prevent malicious traffic from accessing the system or its network.
- Maintain domain controllers with supported release versions and ensure they are patched.
- Ensure the organization has established a defense-in-depth strategy. With a distributed workforce (one that has seen the highest numbers of remote access in all history), approaches that have been used in the past may not be enough. With the advent of software as a service, the cloud and other hybrid models, it's important to revisit logging and monitoring strategies to accommodate these changes.
- Separate the use of local system administration from domain administration. If an endpoint such as a laptop is compromised and an attacker is able to discern local administrator credentials, those credentials will be tested at the domain. If they are the same, an attacker can easily facilitate an attack against the domain controller.
- Monitor your domain controller at a system and application log level, monitor access logs for anomalies such as nondomain IPs and for failed attempts, monitor network traffic at a port and payload level, implement an EDR and schedule more frequent enhanced audits.

- Encrypt endpoints. The use of full disk encryption (FDE) makes a great deal of sense on a number of levels. An organization should not make it easy for a bad actor to foster success. If an industry has reams of regulated data, FDE is assumed as a basic, reasonable control, if not outright mandated. An organization should decrease the attack surface to create a more difficult target to exploit; otherwise, an actor can make easy lateral moves with the goal of escalating privileges. This can be accomplished through the effective use of a data classification program and least privilege and is mostly a continuous approach to hygiene and property prioritizing activities.
- Prepare for the worst-case scenario and have an incident response plan in place.

CONCLUSION

As always, we want to make sure it's understood that there is never absolute assurance where security is concerned, and specifically, there is no single silver bullet that will fully protect an organization from all cyber attacks. And it's not possible to outline a comprehensive cyber defense strategy in a single paper. However, since Pondurance operates on both the red team side (such as during a penetration test) and the blue team side (managed detection and response solutions), we have analyzed varying attack methods and significant amounts of breach data, and the results support the commonality of the domain controller at the heart of nearly every ransomware attack. This paper aims to identify controls and best practices that, when implemented, can reduce the likelihood and the risk of a successful cyber attack against your organization through protection of your domain controller.

In more cases than ever, data exfiltration is a viable threat that makes getting off unscathed a pipedream, despite your ability to recover from something like a ransomware event. As a result, two other interesting things are happening. On one front, there is now a question of legality relevant to paying a ransom. On the second front, which is still evolving and is a key prediction made by us for 2021, your ability to simply and entirely transfer the burden of risk in terms of payment using cyber insurance is not assured. To clarify, the market for cyber liability insurance is not going away. But when you put into context the frequency of occurrence, the exponential increase in ransom demands from a monetary perspective, the use of extortion that may force payment and now the question of legality for ransom payments, there is a reckoning on the horizon.

All of this should provide ample motivation for any organization to reduce the likelihood of a compromise in the first place. It is costly and damaging to any organization that is not actively working to protect itself from it or otherwise is not fully prepared from a defense-in-depth perspective. As the trend for this type of attack increases in frequency and continues to evolve, it is critical that your organization be aware of current attack patterns that lead to an attacker's success and what you can do to reduce your exposure. By following the steps discussed in this paper, you can lower the probability of a successful attack.

ABOUT PONDURANCE

Pondurance delivers world-class Managed Detection and Response services to industries facing today's most pressing and dynamic cyber security 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 team can focus on what matters the 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.