PONDURANCE

Stop the Spread of Ransomware at the Root

99% of ransomware spreads through your domain controller.

INTRODUCTION

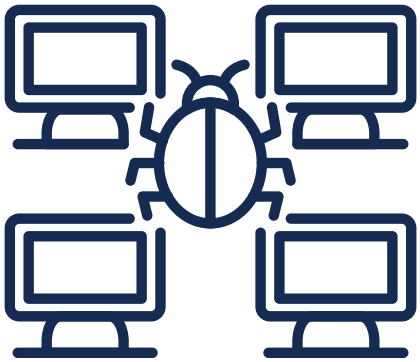
A staggering 100 million ransomware cases have been observed over the last four years alone, and new cases are now expected to occur every 11 seconds, according to some sources. The inherent competitive nature among humans clearly has a dark side, and we can see that playing out as new threat actors race to execute their attacks and compromise their victims. In fact, the level of competition among bad actors is shaping timing and outcome toward a first-in, first-out mentality, and all industries are fair game.

Pondurance has spent considerable time analyzing common attack patterns to better reduce compromise, shorten dwell time and prevent damaging ransomware outcomes. In doing so, we have found that a compelling common factor associated with the vast majority of cases is the compromise of the domain controller. While compromising a domain controller is not the only way, it is a common method attackers use to quickly impact a Microsoft Windows active directory domain.

A compromised domain controller is by far the most common denominator related to large-scale ransomware events. It is the Achilles' Heel worth protecting with extra diligence, as once an attacker controls it, it's game over.

From a business perspective, relatively small investments have been made to create focused strategies addressing domain controller security and ongoing monitoring and testing, and those may be some of the best dollars spent in your security program. However, a number of exploit paths are attributable to the success of ransomware, 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, lack of or 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 ransomware.

Another factor worth examining when considering the capability to broaden a ransomware attack across an enterprise is the nature of the root cause. That's where the compromise of the domain controller comes into play. While completely eliminating 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. An additional exploit path common in ransomware cases involves the use of shared local or domain administrator credentials across domain-joined devices and, in many cases within the same organization, nondomain devices.



It's not just ransomware. Many other broad compromises are accomplished through the domain controller. Government, service providers and organizations of all sizes are targeted, and this trend will continue to accelerate in 2021 and beyond.

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 ransomware. 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 scanning,

penetration test, and application testing) and the blue team side (log monitoring, network monitoring, Managed Detection and Response [MDR], and hunt 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 ransomware attack against your organization by reducing the risk of widespread ransomware through protection of your domain controller.

HOW RANSOMWARE ATTACKS SUCCEED

The sensitivity and totality of the domain controller is not novel regarding breach or systemic exploitation, and we're not trying to overstate the obvious in terms of its importance. In fact, gaining domain administrator or enterprise administrator privileges is often the proverbial crown jewel of the most basic penetration test. After all, 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 ransomware cases, it was a compromised domain controller that 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 will likely 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.

Ransomware can get into your environment in many ways. 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. For example, if your business is a dental office, a ransomware event may be all it takes to close the 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.

HOW DOMAIN CONTROLLERS ARE COMPROMISED

Let's explore some of the common methodologies 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-service (RaaS) operation, also known as REvil or Sodin. 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).

- 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.

HOW RANSOMWARE EXECUTES

As we mentioned earlier, compromising the domain controller is not the only way to execute ransomware. If, for instance, a user clicks a bad link or exposes his or her credentials and gets ransomware on the device, the outcome can range from an isolated nuisance to a business extinction 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 operating similarly with nefarious intent and disregard for any parameters of engagement scope. One other consideration is domain administrator privileges. An attacker need not use malware to systemically encrypt enterprise systems. In fact, Pondurance 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 developing a defense-in-depth strategy.

HOW TO PROTECT DOMAIN CONTROLLERS

The domain controller is the heart of any distributed network. 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 cyber attack). 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. 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.
- 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.
- 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. 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.

- 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. This is mostly a continuous approach to hygiene and property prioritizing activities.

CONCLUSION

Ransomware can become an extinction event. It has been weaponized with near perfection over time in its ability to render system downtime with little or no physical damage but has a high potential for collateral damage. At least one death very recently has even been directly attributed to a ransomware outbreak at Germany's University Hospital of Düsseldorf, leading a patient to be diverted and causing the person to perish in transit.

The evolution of ransomware techniques has proven to be the epitome of evil. Whereas some companies have recovered data without paying a ransom, others have been compelled to pay more than seven figures in a single instance. It should be noted, however, that the ability to recover your data may no longer be enough to stave off the effects of a ransomware attack. Bad actors want to get paid for their efforts, which has shifted their techniques from simply holding your data for ransom to outright extortion unless you pay their demands.

All of this should provide ample motivation for any organization to reduce the likelihood of a ransomware occurrence in the first place. It is costly and damaging to any organization that is not actively working to protect itself 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, your organization should be aware of current attack patterns that can 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 ransomware attack.

For more information on how to protect your domain controller from a cyber attack, read our whitepaper: The Domain Controller...An Achilles Heel

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 Pondurance.com for more information.