Rising Threat: NoPac Vulnerability as a Gateway for Ransomware Deployment

The NoPac vulnerability, encompassing two critical Active Directory vulnerabilities, CVE-2021-42278 and CVE-2021-42287, is seeing a sharp uptick in exploitation by advanced threat actors. Originally patched by Microsoft in late 2021, NoPac has recently been weaponized by ransomware groups like BlackBasta and now Qilin, leveraging its capability to bypass domain protections and escalate privileges with shocking speed and ease.

Understanding the NoPac Vulnerability

NoPac combines two key AD vulnerabilities:

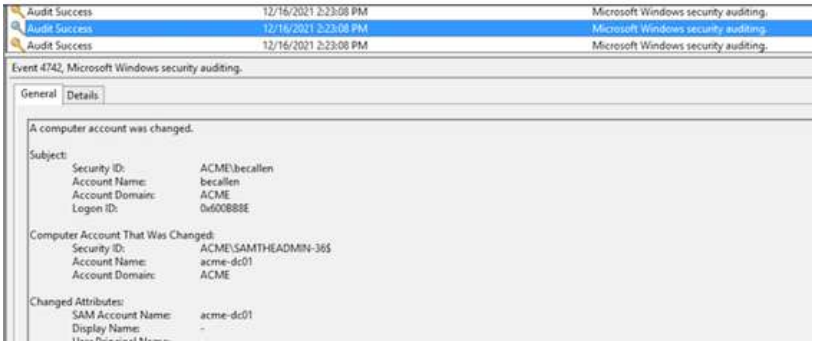
- **CVE-2021-42278:** This allows attackers to spoof computer account names by exploiting weaknesses in the sAMAccountName attribute.
- **CVE-2021-42287:** This enables privilege escalation by exploiting flaws in Kerberos ticket handling, allowing attackers to impersonate domain controllers.

When chained, these vulnerabilities permit an attacker to impersonate a domain controller and escalate privileges from a regular domain user to a domain administrator within seconds. As highlighted by CrowdStrike, this attack vector is particularly dangerous due to its low complexity and critical impact.

Exploitation Process

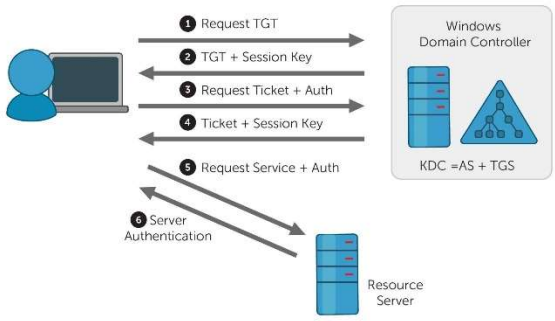
The NoPac attack follows these steps:

1. **Create a New Machine Account**: Threat actors exploit default permissions allowing any authenticated user to add up to 10 machine accounts in Active Directory.
2. **Spoof a Domain Controller**: By renaming the `sAMAccountName` to that of a domain controller (sans the trailing `$`), attackers bypass validation mechanisms.



SecureWorks Blog

3. **Request a Ticket-Granting Ticket (TGT)**: Using the spoofed account, the attacker requests Kerberos authentication.
4. **Revert Account Changes**: The attacker renames the `sAMAccountName` back to its original value, confusing the Key Distribution Center (KDC).
5. **Obtain Domain Admin Privileges**: The attacker leverages the TGT to request service tickets (TGS) with elevated privileges, enabling full domain access.



PaloAlto Networks Blog

This attack can be executed in as little as 16 seconds, as shown by researchers from Secureworks, leaving organizations exposed to significant damage, including total domain compromise.

NoPac in Ransomware Campaigns

Ransomware groups like **Qilin** and **BlackBasta** have adopted NoPac as a precursor to ransomware deployment. By obtaining domain administrator privileges, these actors can:

- **Disable Security Tools**: Preventing detection and mitigation efforts.
- **Exfiltrate Sensitive Data**: Preparing for double extortion schemes.
- **Deploy Ransomware Network-Wide**: Achieving widespread encryption of systems.

NoPac has become a preferred vector for ransomware operators due to its stealth, speed, and effectiveness, as highlighted in the Red Piranha Threat Intelligence Report.

Indicators of Compromise:

Exploitation of NoPac generates specific Windows event logs:

- **4741**: Machine account creation
- **4742**: SPNs cleared or renamed
- **4781**: sAMAccountName changes
- **4768**: TGT requests with spoofed sAMAccountName
- **4769**: TGS requests with mismatched account names

Organizations should monitor these events for anomalous activity.

Mitigation Strategies

To defend against NoPac exploitation, organizations should:

1. **Apply Microsoft Patches**: Ensure all domain controllers are updated with patches released in November 2021 and subsequent updates. CISA emphasizes that even one unpatched domain controller can leave the entire network vulnerable.
2. **Restrict Account Creation Privileges**: Limit machine account creation permissions to reduce the attack surface.
3. **Implement Multi-Factor Authentication**: Enforce MFA for all externally accessible accounts to prevent unauthorized access.

4. **Enable Advanced Threat Detection**:
    - Utilize tools like SentinelOne, CrowdStrike Falcon or Palo Alto Cortex XDR to detect and block NoPac exploits.
    - Use behavioral analytics to identify anomalous activity in Active Directory.
5. **Conduct Regular Audits**: Manually review sAMAccountName changes and machine account creations.
6. **Implement Zero Trust Policies**: Restrict lateral movement and ensure proper network segmentation.

Conclusion

The NoPac exploit highlights how vulnerabilities in identity management are becoming key tools for ransomware operators. Groups like Qilin and BlackBasta are actively exploiting these flaws, making it essential for organizations to prioritize securing their Active Directory environments.

Staying ahead of these threats requires immediate action: patching systems, watching for indicators of compromise, and implementing advanced tools to detect and block exploitation. These steps can significantly reduce the risk of falling victim to a devastating attack.

NoPac serves as a wake-up call for businesses to take a proactive approach to cybersecurity. Identity security isn't just another checkbox—it's the frontline defense against increasingly sophisticated ransomware campaigns.

References

- CrowdStrike: NoPac Exploit
- Palo Alto Networks: Detecting NoPac Vulnerabilities
- CISA: Cybersecurity Advisory
- Secureworks: NoPac Exploitation
- NVD: CVE-2021-42278 and CVE-2021-42287
- Red Piranha: Threat Intelligence Report
- ManageEngine: Windows Event ID 4768

Who is Waintraub Cyber Solutions?

Waintraub Cyber Solutions Waintraub Cyber Solutions was incorporated in 2020 to provide top-tier cybersecurity services tailored to protect and defend businesses from evolving cyber threats. Our team of experienced professionals ensures rapid incident response and proactive threat management, offering flexible, scalable services for businesses of all sizes.

Cybersecurity Service Offerings

Waintraub Cyber Solutions offers a comprehensive range of cybersecurity services, designed to help your business prepare for and respond to cyber threats. Our service offerings are divided into two categories: Pre-Incident and Post-Incident Services.

Our services include:

- **Pre-Incident Planning & Gap Assessments**: Preparing your organization to withstand cyber risks.

- **Threat Intelligence & SOC/XDR Monitoring**: Continuous protection and insights to fortify your defenses.
- **Security Awareness Training**: Empowering teams to recognize and mitigate cyber threats.
- **Incident Response & Ransomware Negotiations**: Rapid containment and recovery to minimize downtime and data loss.

At Waintraub Cyber Solutions, we partner with businesses across industries to deliver peace of mind in the face of uncertainty. Whether you're looking to bolster your defenses or need expert guidance during a crisis, we're here to help. Visit us at waintraubcyber.com to learn more.