Shining a Light in the Dark – How Binary Defense Uncovered an APT Lurking in Shadows of IT

⋮ 9/19/2024

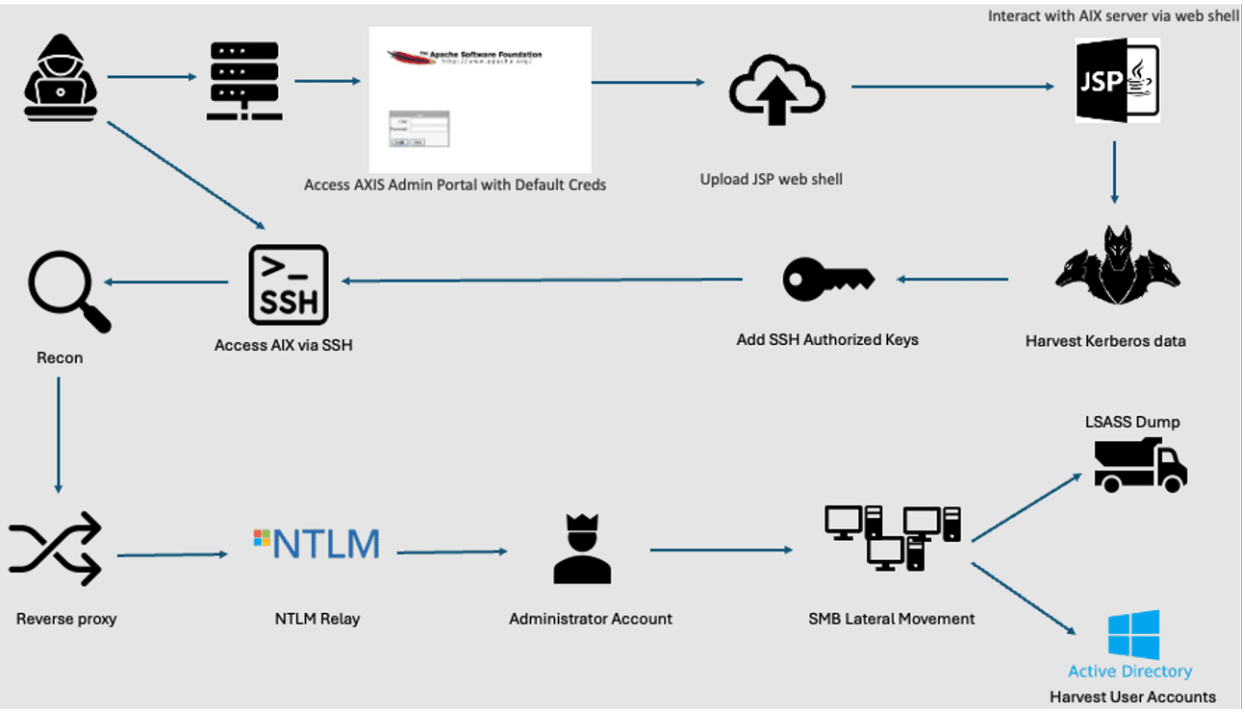
Last Modified: Tuesday October 15, 2024

Written by ARC Labs contributors, John Dwyer, Eric Gonzalez at Binary Defense and Tyler Hudak at TrustedSec

In cybersecurity, the threats we don't see—or don't expect—often pose the greatest danger. Recently, this became all too clear when three unmanaged AIX servers, sitting exposed on the internet, opened the door for a China-Nexus Threat Actor to launch an attack. What may seem like obscure, legacy technology became a launchpad for malicious activity, allowing the attacker to introduce a web shell and pivot deeper into a Windows environment.

This incident highlights the growing risks posed by shadow IT and unmanaged systems, but more importantly, it underscores the critical role that detection and response play in identifying and mitigating threats. Even legacy technologies, like AIX servers, can become high-value targets for attackers. In this blog, we'll explore how the attackers quickly pounced an opportunity to take control of these unmanaged systems and why comprehensive threat detection and response is essential for protecting every corner of your network—no matter how small or seemingly insignificant.

Timeline of the Attacker's Activity



- Attacker access one of the AIX servers using the default credentials for the Apache AXIS Admin portal
- Attacker leverages the upload function of the AXIS admin portal to introduce the AxisInvoker web shell
- Attacker harvests Kerberos data from the AIX server
- Attacker uploads requisite SSH keys and access the AIX server via SSH
- Attacker performs reconnaissance gathering data through LDAP, SMB shares, network information, and search local configuration files for more information about the systems and their configuration
- Attacker attempts to introduce several post-exploitation tools such as Cobalt Strike beacons and different JavaScript-based web shells
- Attacker introduces the FRP reverse proxy tool to establish a direct connection from the attacker-controlled infrastructure to the target network
- Attacker executes various NTLM attacks to perform Active Directory reconnaissance and perform account impersonation attacks for the local Administrator account
- Attacker attempts to harvest credentials through dumping the LSASS process but is detected and removed from the environment.

The Incident

In August 2024, malicious activity was detected on a Windows server. The alert was associated with an attempt to dump the memory of the LSASS process—an indicator of a potential privilege escalation attempt.

Service Name	omKGvRny
Service Image Path	%COMSPEC% /Q /c cMd.exE /Q /c for /f “tokens=1,2 delims= ” ^%A in (‘”tasklist /fi “Imagename eq lsass.exe” | find “lsass””‘) do rundll32.exe C:\windows\System32\comsvcs.dll, #+0000^24 ^%B \Windows\Temp\q4MYcT.lnk full

Through an investigation by Binary Defense and in conjunction with analysis from TrustedSec traced the original alert back to a credential dumping attempt originated from an AIX server which was part of a three AIX server development environment, left publicly accessible with default administrator credentials for the Apache Axis admin portal. The evidence gathered by Binary Defense indicates the attacker had initially compromised the servers in March of 2024 and was able to maintain persistent access to the systems until August when they attempted to move laterally to a portion of the network which was in-scope of the security tools. These types of oversights are often the result of shadow IT practices where systems are deployed without the knowledge or control of the security team and regularly serve as enticing entry points for attackers. The threat actor exploited the default Apache credentials to gain administrative access, upload a web shell, and establish persistent access through SSH keys and a reverse proxy.

A web shell is a malicious script that attackers upload to a web server, allowing them to remotely execute commands, browse files, and control the server as if they were physically present. This tool gave the attacker interactive access to the AIX server, effectively turning it into a launchpad for further attacks. To maintain stealthy communication with the compromised server, the attacker used Fast Reverse Proxy

(FRP), a tool that creates a reverse tunnel back to the attacker's infrastructure, bypassing network defenses and firewalls.

Attack Activity	Details
Upload webshell	/axis2/axis2-admin/upload
Interact with webshell	/axis2/services/AxisInvoker/exec?cmd=
Enable Attacker SSH access	Download of SSH key into /.ssh/authorized_keys
cp /etc/krb5.keytab /opt/<axispath> /axis2-web/krb5.jsp	Collect key tab file
Download /tmp/.1/krb5.ccache	Collect key tab cache
Download /tmp/krb5.keytab	Collect temp key tab
Download /home/<user>/.bash_history	Collect admin bash history
cat /home/<admin>/.sh_history	Collect admin shell history
/tmp/ldapsearch	Active Directory recon
Upload /tmp/frpc & /tmp/ssl/frpc.ini	Stage FRP reverse proxy
/tmp/frpc process execution	Starting reverse proxy process

With this C2 (command-and-control) channel established, the attacker executed NTLM relay attacks, a method where they capture and relay authentication credentials to impersonate a privileged user. This technique allowed the attacker to enumerate Windows users and impersonate a valid Administrator account within the Windows environment, ultimately attempting to dump the LSASS process to harvest credential data.

This incident is a stark reminder that every device on a network, regardless of its purpose or visibility, can be a potential target for attackers.

Unmanaged AIX Servers: Obscurity Does Not Guarantee Security

AIX systems, while not commonly targeted in the same way as Windows or Linux, are by no means immune to attacks. The attackers in this case demonstrated their capability to identify and exploit the vulnerabilities in these systems. By utilizing tools like AXISInvoker webshell and Fast Reverse Proxy (FRP), they effectively turned a relatively obscure system into a beachhead for lateral movement into other systems. This serves as a crucial reminder that security teams must be vigilant about all systems in their network, not just the most obvious targets. It is worth noting that while the attacker was able to navigate the AIX servers and utilize them to maintain access to the environment, they were unable to establish a C2 channel over Cobalt Strike because they repeatedly attempted to use Linux commands such as wget and curl which are not native to AIX.

The Importance of Comprehensive Security Monitoring

The attack was first detected when the China-Nexus threat actor attempted to pivot from the unmanaged AIX servers into the more secure, managed Windows environment, where active security controls were monitoring for suspicious activity. However, the story didn't end there. Even after being thwarted from their initial vector, the attacker made multiple failed attempts to regain access, demonstrating their persistence.

Had the threat actor been able to maintain their foothold within the unmanaged AIX servers, they could have operated undetected for an extended period, potentially causing far more significant damage. Their repeated efforts to infiltrate the system emphasize just how relentless adversaries can be, especially when targeting unmonitored or obscure systems. This incident highlights the critical importance of comprehensive security monitoring across all systems, not just those that are actively managed or considered high-priority. Without visibility into every corner of the network, even seemingly minor, unmanaged systems can become a persistent source of risk.

Final Thoughts

This incident highlights the dangers of unmanaged and shadow IT systems, which can easily become the weak link in an otherwise secure network. It also serves as a reminder that less commonly targeted systems, like AIX, are not immune to attacks. Security teams must maintain visibility and control over all networked devices to prevent similar breaches in the future. The incident also reinforces the importance of regular audits, strong credential management, and the integration of security measures across all environments.

Call to Action

Organizations must take a hard look at their current IT assets and ensure that every system—whether it's perceived as critical or obscure —are included in their security strategy. Every part of your network plays a role in its overall strength, and by giving attention to each system, you're building a more resilient foundation.

As a partner, Binary Defense is here to support our clients security efforts by becoming a extension of their team. We offer full visibility and advanced threat detection across your entire environment, from legacy systems like AIX servers to the latest technologies. Our goal is to help you stay ahead of threats, ensuring that no system, no matter how small, goes unprotected.

We work alongside you to strengthen your security posture, offering managed detection and response, proactive threat hunting, and timely incident response. Together, we can ensure every part of your digital ecosystem is secure, giving you the confidence to focus on what matters most—growing your business. Let's work together to protect your entire network, one step at a time.