SPONSORED
FEATURE

onapsis

Why Attackers Are Turning Their Attention Toward ERP Applications

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

https://bit.ly/2rsNg96

Business-critical SAP and Oracle applications (also known as enterprise resource planning [ERP] applications) run the economy by managing the critical data and processes of large global organizations. Because of the processes these applications support, the enterprise "crown jewels" are stored here.

This is the foundation for a risky *status quo*. The fact that these applications are so critical, combined with additional attributes such as complexity, proprietary protocols and components, and extensive customizations and integrations, make them difficult to update. Moreover, these applications have a massive attack surface and, historically, have been a blind spot in most organizations, leaving them exposed to insider and outsider threats. Attackers have been targeting these applications for several years, but the attacks are now becoming more common and more complex, pushing this topic to the forefront of many boardroom conversations.

Cyberattackers, who typically aim to compromise organizations by targeting more traditional platforms and technologies (such as Microsoft Windows), are now realizing that business-critical applications are extremely high-risk applications. These platforms support business processes that can be abused to compromise a target organization, steal proprietary information, shut down systems, and affect revenue and reputation.

Juan Pablo Perez-Etchegoyen
Is chief technology officer at Onapsis where he leads the research and development team that keeps Onapsis on the cutting-edge of the business-critical application security market. He is responsible for the design, research and development of Onapsis's innovative software solutions and helps manage the development of new products as well as the SAP cybersecurity research that has garnered critical acclaim for the Onapsis Research Labs. He is regularly invited to speak and host trainings at global industry conferences including Blackhat, HackInTheBox, Troopers, and SAP TechEd/DCODE.

On 25 July 2018, Onapsis and Digital Shadows released a report[1] that highlights how different types of internal and external cyberattackers are directly targeting ERP applications. There has been evidence of SAP and Oracle applications being the target of cyberattacks since 2012; however, the report highlights the evolving sophistication of these attacks and the growing frequency with which they are being deployed. Furthermore, the report provides examples of more than 20 campaigns incorporating these ERP applications as a key attack vector in the plan.

> “COMPROMISING AN ERP APPLICATION REQUIRES A VERY SPECIFIC SKILL SET THAT ATTACKERS ARE INCREASINGLY DEVELOPING.”

There are several interesting angles that attackers are incorporating while targeting ERP applications:

- **Non-advanced persistent threats (APTs)**—Many of the threat detection capabilities that span different cybersecurity vendors try to detect the most sophisticated and advanced threats. In the ERP world, unfortunately, organizations historically cannot properly implement security, meaning that the same vulnerabilities that were applicable three, five or even 10 years ago are still exposed in these environments. What is worse, attackers are beginning to understand that.
- **Catching up with the technology gap**—ERP applications are not only complex on their own, but they are built on top of a diverse set of components (mostly closed source and proprietary) that talk to

each other. Compromising an ERP application requires a very specific skill set that attackers are increasingly developing. Examples of this are detailed in step-by-step guides on how to hack SAP applications posted on very select cybercriminal forums and requests for SAP exploits on underground forums.

- **A very beneficial patching window**—Everyone is probably familiar with the Equifax breach, where attackers abused a vulnerability that was patched by Apache and weaponized quickly after the patch was released. In the ERP world, it sometimes takes organizations months or even years to apply security patches, leaving these systems exposed longer as the list of vulnerabilities grows bigger.
- **Abusing the business processes**—ERP applications are not just complex technology, they are the foundation of most business processes for organizations. They contain sensitive finance, human resources (HR), supply, customer and personally identifiable information (PII) data that are at risk of being exploited. An example of this is attackers changing the bank account information of vendors and employees so attackers can receive considerable payments that go undetected by the organization.

As part of the research performed by Onapsis and Digital Shadows, a discovery of Internet-facing ERP components was performed, resulting in more than 17,000 Internet-facing ERP components being identified. Not only are the sheer number of Internet-facing results eye-opening, but there are other remarkable findings, including:

- **Thousands of nonproductive systems**—While it is sometimes necessary, exposing a productive ERP application to the Internet is a risky move. Organizations need to have a process to properly assess and manage the risk to these applications and perform regular audits. However, there should be no reason for exposing nonproductive environments to the Internet as these environments are typically less protected and, in some way, connected to productive applications, rendering them insecure.
- **Insecurely exposed applications**—More than 10,000 ERP components were detected as Internet-facing and unnecessarily open for anyone to connect with, a situation that considerably increases the attack surface.
- **Old and no longer maintained components**—A considerable number of applications were detected as old versions that could be exposed to a continuously increasing number of vulnerabilities.

Internet-facing applications are not the only ERP applications organizations need to secure, as attackers are also targeting internal applications. This is shown by the update of a well-known banking Trojan aimed at capturing SAPgui data, which could include user credentials, screenshots and other critical data.

Threat actors are targeting ERP applications, and organizations should stay vigilant to prevent a breach to their business-critical data and processes. Furthermore, if an organization is running ERP applications in the cloud or is undergoing a cloud migration project, the Cloud Security Alliance (CSA) ERP Working Group provides documents to help address some of those associated challenges.

Endnotes

1 Onapsis and Digital Shadows, "ERP Applications Under Fire: How Cyberattackers Target the Crown Jewels," USA, 2017, *https://www.onapsis.com/research/reports/erp-security-threat-report?utm_source=article&utm_medium=isaca&utm_campaign=erp_under_fire_threat_report*