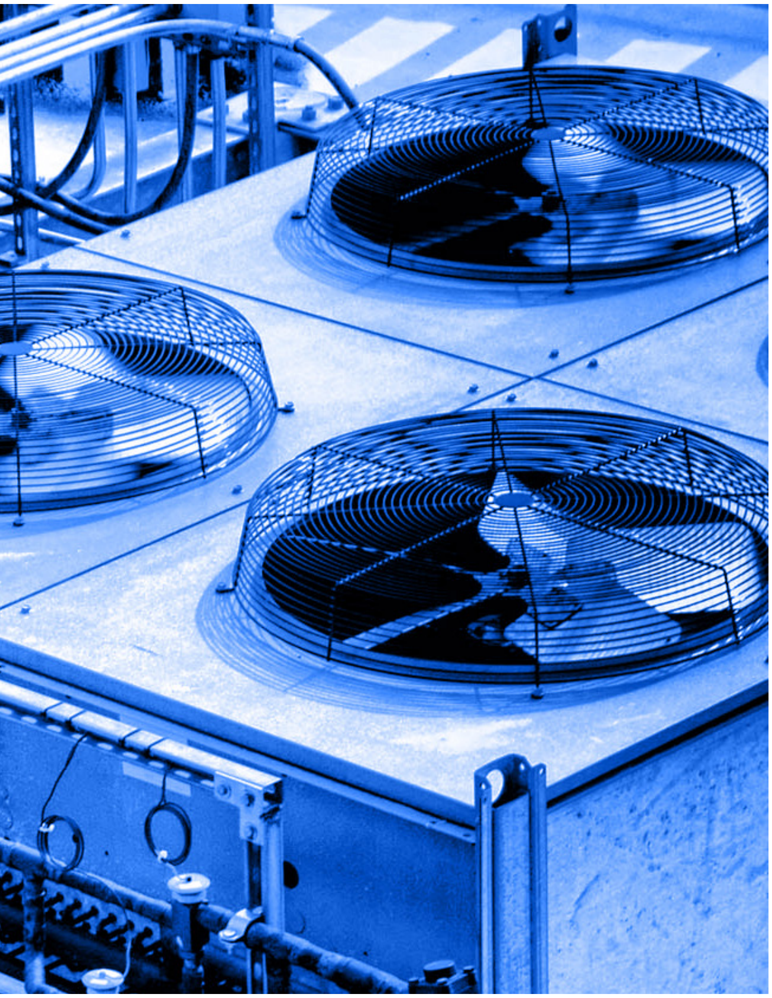
> *Users enjoy the product, and we feel much more comfortable knowing that our network is more protected*

Tyler Wisenburg, IT director
Key Mechanical

SECRET
DOUBLE
OCTOPUS

About Key Mechanical

Founded in 1956, Key Mechanical is a HVAC and refrigeration contractor serving the West Coast, USA. The Company specializes in the design, construction and service of HVAC/refrigeration systems for commercial applications for some of the most demanding retail environment including clients such as Costco, Whole Foods, Target Express, and others.



SECRET
DOUBLE
OCTOPUS

At a glance

Customer Problem

- Key Mechanical, a leading provider of HVAC and refrigeration systems for commercial applications, fell victim to a successful phishing attack on one of their Office 365 accounts. Using the stolen credential, the attacker crafted a fraudulent message to a client, asking to transfer money to a mule account. The incident was a sobering reminder for how vulnerable passwords can put Key Mechanical and its customers at risk.

Solution

- Key Mechanical deployed the Octopus Authenticator to replace vulnerable passwords and allow its employees to logon to their workstation and company network, their Office 365 account, and any other Active Directory joined resource, whether connected or offline.

Business Outcome

- By removing passwords and other forms of authentication that need to be keyed in by the user, phishing is no longer a risk. With Secret Double Octopus, authentication occurs out of band, via secured channels. User experience is also improved, as users simply swipe their authenticator in response to a secure push notification.

Customer problem

Key Mechanical, a leading provider of HVAC and refrigeration systems for commercial applications, fell victim to a successful phishing attack on one of its Office 365 accounts. An unsuspecting employee gave up their Office 365 credentials to a phishing website, which allowed the attacker to access his Outlook account. And because Key Mechanical synchronizes passwords between Office 365 and its Active Directory (AD), the attacker had access to all AD connected resources as well.

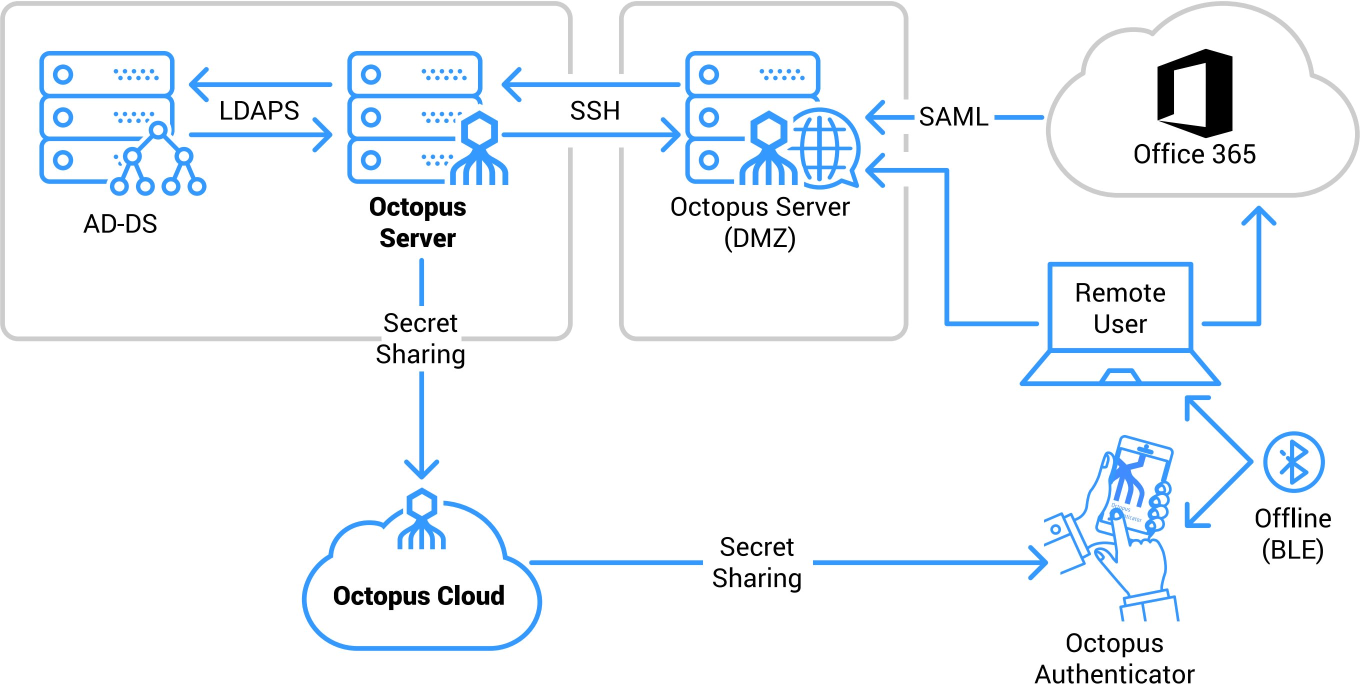
Using the stolen credential, the attacker crafted a fraudulent message to a Key Mechanical client, which was in midst of setting up payment for a large construction project. The message sent to the client looked almost identical to what they would have normally received from Key Mechanical. Thanks to vigilance exhibited by the customer and Key Mechanical, the change in payee account was noticed, and the attack was thwarted.

The incident was a sobering reminder for how vulnerable passwords can put Key Mechanical and its customers at risk.

Solution chosen

Key Mechanical deployed a high-assurance, password-free authentication solution from Secret Double Octopus to replace its vulnerable passwords. All Key Mechanical employees now use the Octopus Authenticator on their mobile device instead of passwords to logon to their workstation and company network, their Office 365 account, and any other Active Directory joined resource, whether connected or offline.

When presented with the login screen/page, users are sent a secured push notification to their registered mobile device to approve the connection request, instead of keying in a password. When offline, users can still use the authenticator on their mobile device via a secured local BLE (Bluetooth Low Energy) connection.



User UI on Office 365 >> Backend SAML exchange + push notification to mobile app

Business outcomes

Deploying the Octopus Authenticator resulted in better protection for the company and its customers. By removing passwords, and other forms of authentication that need to be keyed in by the user, phishing is no longer a risk. With Secret Double Octopus, authentication occurs via out of band, secured channels.

User experience is also improved. The Octopus Authenticator provides better user experience when compared to stringent password policies or use of traditional multi-factor authentication solutions (e.g. OTPs). To authenticate, user simply swipes the authenticator on their mobile device in response to a secure push notification.

Why Secret Double Octopus

To address the phishing risks they were exposed to, Key Mechanical considered different phishing prevention solutions, including user education, email and web filters, and traditional multi-factor authentication solutions.

But instead of trying to detect and block the phishing attack, Key Mechanical decided to go after the root cause – the passwords themselves. By removing vulnerable passwords from the equation, and moving to a high-assurance authenticator that uses secure out-of-band communication channels, phishing is no longer a problem, as there are no credentials that can be phished.

With many of its most vulnerable users working out of the office, and with spotty access to the internet, Secret Double Octopus's ability to work both online and off was a critical consideration in Key Mechanical's decision to buy Secret Double Octopus.

Another important consideration was the tight integration with Active Directory, which meant that all corporate resources could benefit from the added security provided by Secret Double Octopus.

Finally, Key Mechanical valued the fact that Secret Double Octopus actually improved the security of Active Directory itself. Unlike other solutions that are completely decoupled from- and work in parallel to- AD, Secret Double Octopus actively manages Active Directory to make it more resilient to attack.

"Users enjoy the product, and we feel much more comfortable knowing that our network is more protected", Tyler Wisenburg, IT director, Key Mechanical.

About Secret Double Octopus

Secret Double Octopus is the global leader in next generation workforce authentication solutions. Its industry-leading Octopus platform offers mid-market to Fortune 100 enterprises the ability to progressively move to a higher security, more frictionless authentication – from MFA to end-to-end, unified passwordless authentication. From leveraging existing MFA authenticators to supporting legacy on premise applications, no other desktop MFA and enterprise passwordless platform offers as much robustness and flexibility as the Octopus solution. The company has been designated a Gartner "**Cool Vendor**" and more recently named "**Best-in-Class**" passwordless solution by AITE Group in 2021.
Learn more at doubleoctopus.com.

For sales inquiries, please email sales@doubleoctopus.com

US HQ
1600 El Camino Real,
Suite 280, Menlo Park, CA
94025 USA

International HQ
97 Rokach Blvd
Tel Aviv 6902068,
Israel

SECRET
DOUBLE
OCTOPUS