forsyte
I.T. SOLUTIONS

How a Georgia School District

PUT AN END TO "TRUSTED" PHISHING ATTACKS

A Fulton County Schools Case Study

Executive Summary

After Fulton County Schools (Fulton) encountered a "trusted" phishing attack that resulted in the theft of 46 employee payroll accounts and the loss of more than $75,000, the district knew it needed to take steps to prevent and to respond to future attacks. With the help of Forsyte IT Solutions (Forsyte), Fulton implemented Phish Hunter, a comprehensive solution that leverages multiple Microsoft cloud technologies in an orchestrated fashion to fight against attack scenarios and combat compromised accounts by means of automatic protection and automatic remediation. Since implementing Phish Hunter, Fulton has incurred no additional losses from phishing and multiple attacks have been thwarted.

Organizational Overview

Founded in 1871, the Fulton County School System is one of the oldest and largest school districts in Georgia. With a focus on student achievement and a commitment to continual improvement, Fulton has earned a reputation as a premier school system. This long history of excellence is evidenced by the many state and national honors bestowed on Fulton's schools, staff and students.

Fulton County Schools
Where Students Come First

Industry

Education

Students

95,600+

Employees

12,000+

Contact: 844-587-4535 | info@forsyteit.com | www.forsyteit.com

Phishing Prevention Solutions

- Phish Hunter
- Phish Hunter Managed Services

Benefits

- 98% faster time to discover and respond to an attack.
- 90% reduction in the number of successful phishing attacks.
- More than 100,000 email accounts are better protected.
- Access to critical threat protection data increased by 90%.

"Our previous solution to phishing attacks relied on receiving an alert from a user. By the time we heard about a compromise, the damage was already done. Since we've engaged Forsyte, we now receive actionable alerts and reports regarding phishing, spam and malware. Coupled with Forsyte's Managed Services, we have the tools and the manpower in place to take advantage of the full security capabilities offered by Microsoft 365. Our experience with Forsyte has been excellent."

— Derek Johnson, Director of Information Technology Security, Fulton County Schools

Schools Under Siege

Phishing is rapidly becoming the most significant security threat today. Phishing uses well-crafted emails made to convince the recipient of their legitimacy. Countless individuals and organizations have unwittingly wired money, sent tax information, and emailed credentials to criminals who were impersonating their boss, colleague, or a trusted customer. These attacks are compelling and cannot be stopped with legacy email security solutions.

The phishing attack on Fulton was just one of many experienced by educational institutions across the U.S. over the past several years. Email phishing scams have become more prevalent due to the widespread adoption of Single Sign On (SSO), which exposes multiple applications to attack once a single credential has been stolen, and an increasingly mobile workforce, which increases the difficulty in finding compromised accounts.

In the case of Fulton, attackers utilized a series of tailored spear phishing emails that impersonated a "trusted" user's email account. The objective of these spear phishing emails was to use social engineering to trick employees into entering their credentials (in this case, username and password) into an attacker-controlled website that was designed to mimic a frequently used Fulton web portal. Once the attackers had the employee's network credentials, it was relatively easy to gain access to the employee's payroll portal and then to reroute electronic payment to an account of their choosing.

After several employees reported that they had not received their paycheck via the standard direct deposit process, Fulton realized that a theft had occurred. Although Fulton had been subject to pervious phishing attacks, this was the first attack that resulted in a payroll breach and a financial loss for the district. Fulton's leadership team knew it had to take the necessary steps to protect the district's employees and data from future attacks.

Harnessing the Full Value of Microsoft 365

Prior to the phishing attack, Fulton did not have an integrated security solution in place. The district had purchased Microsoft 365, a combination of solutions including Office 365, Windows 10 and Enterprise Mobility + Security; however, the district had not fully implemented the security features included in their license. Fulton's technical team lead by Derek Johnson, Director of Information Technology Security, made the decision to engage the expertise of Forsyte to help determine the best course of action moving forward.

Fulton had worked with Forsyte on several prior projects including the deployment of Microsoft Identity Manger (MIM). Forsyte is a Microsoft Gold Partner that specializes in Identity Management, Threat Protection, and Information Protection. In the months leading up to the attack at Fulton, Forsyte had been coincidentally working with the Microsoft One Commercial Partner Security Team and Steve Faehl, Microsoft's Security Strategy Lead for the Public Sector, on the first generation of a phishing detection and remediation solution for clients. Steve was keenly aware of the impact phishing was having on his clients and decided to engage Forsyte to help build out a security solution that would address this expanding threat.

After several months of development, Phish Hunter (as the solution was named) was ready for action. Phish Hunter is not an "official" Microsoft product, but rather a solution set that leverages multiple Microsoft 365 technologies in an orchestrated fashion to fight against attack scenarios and combat compromised accounts by means of automatic protection and automatic remediation. The solution utilizes a combination of Advanced Threat Protection (ATP), Cloud App Security (CAS), Azure Automation, Machine Learning (ML) and Power BI to provide clients with a one-of-a-kind, comprehensive approach to predict and combat compromised accounts.

Fortifying Fulton's Defenses

Forsyte met with the Fulton team and introduced them to the capabilities of Phish Hunter. Confident in their relationship with Microsoft and Forsyte, Fulton made the decision to immediately deploy Phish Hunter. In the days, weeks and months post deployment, Fulton has thwarted multiple attacks, prevented any additional losses from compromised accounts, and has been able to take a proactive posture to detect and stop phishing from having an impact on their district. With the success of Phish Hunter, the Fulton team was able to see the full security capabilities of Microsoft 365 in action and have become major proponents of the offering, encouraging other school districts to take advantage of these tools and technology.

A Highly Scalable Solution

With the success of the Fulton deployment under their belt, Microsoft and Forsyte recognized that Phish Hunter had the potential to help any Microsoft customer that has purchased Microsoft 365. In an effort to maximize the value of Phish Hunter, the technical team at Forsyte has invested resources to further enhance the base Phish Hunter solution, including a series of Power BI Dashboards and reports that provide better line of sight to critical, actionable data; user experience improvements that facilitate system administration and on-going system maintenance; and additional forensic policies that drive the detection and remediation engine of Cloud App security.

In addition, Forsyte worked with Fulton to develop and launch a Phish Hunter Managed Services

offering. Because attackers are constantly changing their tactics for infiltrating a victim's network, solutions like Phish Hunter need to evolve and require care and feeding. Forsyte's Managed Services are designed to provide clients with continuous product updates as well as provide clients with a series of system monitoring and advisory services. For large clients like Fulton, Forsyte provides auxiliary capacity to their internal team to help Fulton maximize the benefits of Phish Hunter on an on-going basis. This includes actively monitoring Fulton's Phish Hunter environment and working with the Fulton team on a daily, weekly, monthly basis to ensure that Fulton's defenses are fully fortified.

As stated by Derek Johnson, "we didn't have the manpower in place to monitor and take advantage of the full capabilities offered by these tools. We (Fulton) want to move forward with Forsyte and take a more proactive approach — stopping these attacks when Phish Hunter identifies them. By utilizing Forsyte's Managed Services, we now have the capacity to do just that."

References

"Payday Scam Reported at Fulton County Schools." *Atlanta Journal-Constitution*, 3 Oct. 2017, Vanessa McCray, www.ajc.com/news/local-education/payday-scam-reported-fulton-county-schools/SJRK8IMkhfakuNUa9zRHiI/

"Deconstructing the DOJ Iranian Hacking Indictment." *Dark Reading,* 29, Mar. 2018, Cameron Ero, www.darkreading.com/attacks-breaches/deconstructing-the-doj-iranian-hacking-indictment/a/d-id/1331403?_mc

Get Started

Many large organizations have dozens of different security vendors inside their networks. Every different product will have separate management systems, often with limited connectivity to work alongside others… thus slowing down response and remediation times. This results in the ironic situation of having more security devices in your network which results in making it less secure. The team at Forsyte will help you regain viability and control over your security management imperatives. Whether your assets are deployed in the cloud, on-premises or a across a hybrid environment, Forsyte will ensure that you have the best solutions and configuration to manage your identity, devices, applications, data, and infrastructure.

Microsoft Partner

Microsoft

Gold Cloud Platform
Gold Cloud Productivity
Gold Windows and Devices
Gold Enterprise Mobility Management
Silver Messaging

Contact: 844-587-4535 | info@forsyteit.com | www.forsyteit.com