CUSTOMER CASE STUDY: ARMED™ POWERED BY UDT

CLIENT – INDUSTRY VERTICAL
Logistics Industry – Large client, with many distributed offices.

CUSTOMER SUCCESS STORY
One of United Data Technologies (UDT) clients, a large Logistics industry business, experienced a significant information technology and operational security issue resulting from what was identified to be a targeted phishing campaign.

A wire fraud scheme, aimed at a user within the finance department of the Logistics company, caused the event, resulting in the user transferring several hundreds of thousands of dollars to the cybercriminals that launched the attack. This Logistics company is large, so at first, the attack went un-noticed, despite the fact that it had at the time an already robust Microsoft cyber-defense architecture.

UDT is a Microsoft Gold-competency Partner and supports a number of needs surrounding cybersecurity, and offers other IT business solutions, for this client. When the cybersecurity incident was identified, UDT initiated its unique ARMED™ Powered by UDT Governance-as-a-Service (SaaS) solution to interact with, and augment, the Logistics client’s Microsoft services. ARMED further isolate the issue and provided a very detailed detection, cleansing, and, going forward, hardening of critical systems through a unique combination of professional services and a SaaS “single pane of glass,” which consolidates Microsoft Security and other related protection and remediation services. In the case, the application was of UDT’s ARMED platforms for Microsoft Office 365 ATP, and Microsoft Windows Defender ATP.

• Deal Size: Approximately 250 servers migrated to MS Azure services
• Vertical/Region: Logistics Industry (National/Worldwide)

CO-SELL OPPORTUNITY
United Data Technologies (UDT) is a Microsoft Gold-competency Partner. ARMED™ Powered by UDT is a unique solution to the company – representing UDT’s intellectual property – that is designed specifically to work with, and add significant additional layers of detection, isolation, remediation and process design, for Microsoft Security solutions. ARMED combines unique, patent-pending professional services and technology that supports, enhances and adds to Microsoft Advanced Threat Protection (ATP) for Microsoft Azure (Azure ATP), Microsoft Office 365 (365 ATP), and Microsoft Windows Defender (Windows Defender ATP). UDT can bundle the ARMED Governance-as-a-Service professional services and SaaS platform with the Microsoft tools, or provide it as an addition/supplement to these platforms based on previous subscriptions.
PROOF POINTS – ARMED POWERED BY UDT FOR MICROSOFT OFFICE 365 ATP AND MICROSOFT WINDOWS DEFENDER ATP

1. UDT’s Logistics industry client’s security incident initially identified as potentially malicious in Microsoft Office 365 ATP:
   - Office 365 ATP recognized it as spoofing from what would have been perceived as authorized vendor to the finance department. (Office 365 ATP and Windows Defender ATP detected a small misspelling of the vendor’s name in the potentially malicious email.)

2. The user payload on the email had a “backdoor” – for the recipient – for an invoice (an .exe file).

3. Once accidentally initiated – via presumed download of the false invoice – the user began to experience slowness on the internal system.

4. The identified vulnerability was connected to all of the Logistics industry client’s systems attached to credit cards and other financial information.

5. UDT was engaged to investigate the issue. UDT activated ARMED for Microsoft Office 365 ATP and Windows Defender ATP to:
   - Analyze Office 365 ATP, wherein UDT’s ARMED platform identified that the security incident spread to eight (8) users in the accounting department.
   - Search on .exe files /payloads, execute detection and remediation on six (6) of the eight (8) user systems, and infections on systems in the company’s network. UDT’s ARMED professional services and technology extended the Microsoft Security platform to search and detect which directories and systems were affected, including what outbound activity may have been coming from those identified systems.

6. With ARMED, UDT’s team was able to discern that if undetected, the phishing email and attachments may have created a large hole in the Logistic industry client’s network, with six (6) to eight (8) systems causing outbound communication to a malicious network:
   - As the client is large, they may have missed this security vulnerability for a long time without UDT’s ARMED Governance-as-a-Service solution.
   - Detailed by the findings through ARMED, the security incident was a two-tier/two-phase attack with the following potential results if not quickly addressed:
     - The email demanded a mid-six-figure dollar amount in ransomware.
     - Then, as above, it used phishing to install a back door into the company’s systems, wherein the cybercriminals could have, if the incident were not detected and remediated, siphoned off information from the company, including sensitive financial information, for 180 days.

7. If publicized, the incident could have created a huge credibility loss with the company’s customers. UDT, with ARMED, was able to detect, protect and remediate the issues in a timely-enough fashion to avoid this unfavorable outcome.

ABOUT UNITED DATA TECHNOLOGIES, INC.

United Data Technologies is a technology enabler that helps clients in major industries evaluate, architect, provide, secure, and manage technology on the go, in the rack and in the cloud. UDT provides flexible and interoperable services, including mobility, cloud, collaboration, data, cyber security and software and IT as a service. The company also provides technical, professional and managed services. Accomplish more with UDT: www.udtonline.com