DTEX
WORKFORCE CYBER INTELLIGENCE & SECURITY

ENERGY ORGANIZATION
CASE STUDY

PROTECTING TRUSTED INSIDERS

How DTEX helped a large energy organization identify, understand and mitigate a targeted phishing attack

Introduction

Though DTEX is not a traditional network firewall or malware solution, our Workforce Cyber Intelligence Platform is typically working alongside these kinds of perimeter solutions as part of a layered defense system. And in the case of a security incident or attack, we are often called upon to fill in the gaps or provide insights that other applications cannot.

Phishing: An Insider Vulnerability

The enterprise security threat landscape is more complex than ever, with new risks and attack methods emerging faster than we can keep up with them. If there's one established attack vector that shows no signs of slowing down, however, it's phishing; a recent industry report notes it to be responsible for more than 90 percent of incidents and breaches driven by social engineering, with 66 percent of malware reportedly installed via malicious email attachments.

As phishing attacks have become more sophisticated, they're increasingly focused on exploiting a key, but often overlooked, vulnerability: the users inside of your network. It is user behavior - the opening, the clicking, the downloading - that serves as the enabler, allowing malicious actors to gain entry to your network and find the valuable personal or company information they're seeking.

Recently, a slew of invoice-themed malicious phishing emails was found to have penetrated a customer network - past a tried-and-true network defense system and straight into employee inboxes. A proxy service eventually detected and flagged that users had visited malicious URLs, but there was limited visibility into where and how the attackers entered the network, the number of users affected, and the extent of the potential damage. That's where DTEX, and our Workforce Cyber Intelligence, comes in.

INCIDENT FACTS

INDUSTRY

Energy

COMPANY SIZE

3,000 employees

SPOTLIGHT CHALLENGE

A phishing attack, which occured due to the failure of perimeter security

DTEX'S ROLE

Providing critical insights and answering important questions enabling the security team to fully understand the origin and trajectory of the attack, and pinpoint affected users and endpoints

DTEX Findings

Increasingly sophisticated attack methods are outsmarting tried-and-true network defense systems and penetrating even the strongest of perimeter solutions.

The success or failure of phishing attacks largely hinges on an attacker's ability to feign legitimacy and camouflage their malicious intent. In addition to more polished and well-designed email messages, malicious actors are leveraging new obfuscation mechanisms that allow them to successfully evade the firewalls, gateways and perimeter solutions acting as your first line of defense.

While it is concerning that basic network defense mechanisms failed to spot and block the phishing emails used in this particular attack, as they were found to be fairly textbook in nature, DTEX did uncover evidence of these advanced techniques commonly leveraged to avoid detection and successfully infiltrate employee inboxes.

One such technique was the use of polymorphism, including dynamic email subject lines, URLs, document names, and executed payloads. In the face of these unique and constantly changing elements, security approaches that rely on known, specific or consistent patterns to identify potential threats - such as traditional signature-based detection - are futile. It's reported that nearly 94 percent of malware and potentially unwanted application executables identified last year were seen only once.

Additionally, the links contained within the phishing emails were found to be addresses of actual company sites that had been compromised and used as transient locations to host malicious documents. Because the URL names presented themselves as legitimate, they were not blacklisted or blocked by antivirus or firewall solutions, or recognized as dangerous by most affected users.

Malicious actors are studying and exploiting the routine, yet unpredictable, nature of user behavior.

We've seen a demonstrated understanding among malicious actors that user behavior is often unpredictable and widely varied - and can be used to their advantage. They know that all it takes is one vulnerable recipient to establish an initial foothold and compromise your entire network. An increased focus on user behavior profiling allows attackers to both better understand routine user activities, and find inconsistencies that represent potential gaps in a network.

The invoice-themed emails used in this particular attack represent a fairly standard and highly successful phishing tactic, with actors preying on what are typically mundane day-to-day activities for today's employees: email communication, document review, and administrative task management. And leveraging a series of activities that are almost second nature to today's employees - open email, download attachment, proceed to edit file - ultimately allowed malicious processes to ensue and endpoints to be compromised.

INCIDENT TIMELINE

DAY 1 - DELIVERY

Invoice-themed phishing emails bypass gateway security and penetrate network, reaching employee inboxes

EXPLOITATION

Users interact with the phishing emails:

- Some open the email, take no further action
- Some open the email, then forward or reply
- **Some open the email, follow instructions to visit malicious URL and download the file**

INFECTION

Users who visited malicious URL follow prompts, granting read/write/macro permissions and enabling malicious processes to run

Endpoint infected

DETECTION

Web security gateway flags malicious URLs

Security team runs endpoint scan to detect malicious payloads or malicious executables; scan comes back clean

DAY 3 - SOURCE OF URLS IDENTIFIED

DTEX identifies source of malicious URL(s); retraces user behavior to develop attack timeline and pinpoint affected users and potentially compromised endpoints

The stages of user behavior in this incident were noted to be particularly varied and wildly diverse, and it's important to acknowledge that all users shared an equal part in the risk posed. Those who opened emails, and subsequently accessed links and downloaded files, posed an obvious direct threat to the company network. But others are not without blame: forwarding, replying to, or neglecting to report suspicious emails all represent actions that bring a risk of secondary compromise.

Elementary "Smash-and-Grabs" have evolved into targeted "low-and-slow" attacks - and traditional security approaches are struggling to match pace.

Once this customer received notification of malicious URLs being visited and a potential attack underway, a scan for potentially affected endpoints came up clean - despite no remedial action being taken. This is not uncommon: as threats evolve faster than anti-malware solutions can keep pace with, it's become nearly impossible for every single piece of malicious code to be recognized and stopped. In fact, it's recorded that legacy antivirus solutions missed nearly half of the malware delivered in Q2 of this year alone.

While traditional defense systems are equipped to monitor north-south traffic, or spot key events such as initial infiltration or data exfiltration, few are capable of detecting an attack in the middle phase - the 'dwell time' that malicious actors use for surveillance, data collection, and peer-to-peer propagation. Leveraging lateral movement, actors use this period to expand their foothold and amplify the of their attack with the ability to move throughout the network undetected (for up to 99 days, on average.)

It's only the security approaches that look beyond known threat patterns and attributes, and work to develop a contextual understanding of potential threats continually and in real time, that can find and stop the dangers associated with lateral movement. As this customer recognized, with the ability to retrace steps of user behavior, it becomes possible - and far less overwhelming - to find and secure all compromised endpoints instead of pursuing manual, time-consuming remediation efforts or relying on the strategy of 'hoping for the best.'

No perimeter solution in impenetrable.
The user is the first and last line of defense.

AFTER A PHISHING ATTACK, DTEX PROVIDES CRITICAL ANSWERS:

» Which users opened the malicious email?

» Which users clicked on the malicious link or downloaded the attachment? What about forwarding or responding to the email?

» When did the malicious email enter the organization?

» Which endpoints are potentially compromised?

Conclusion and Recommendations

First and foremost, a review of the technical blocks implemented to mitigate these types of attacks is strongly advised. DTEX recommends a comprehensive investigation is conducted, including a forensic study of compromised endpoints, to gain the complete and thorough understanding critical to successfully defending against similar threats in the future.

As evidenced by vast inconsistencies in user behavior, there's a critical opportunity here to conduct additional user education focused on how to spot, and flag, potential phishing-related activity. No amount of filtering or firewalling will stop every single malicious email or file from entering your network, so it's imperative to invest in comprehensive training and processes related to identifying, and responsibly handling, phishing-related threats.

At the same time, as touched on earlier, this incident underscores the importance of having real-time visibility into user behavior. As organizations come to the stark realization that it's impossible to close every loophole, we're see the focus quickly shift from prevention to threat detection and response. But with more and more malware bypassing perimeter defenses and slipping through undetected, there's a critical need to swiftly find and stop threats before they have a chance to infiltrate. This becomes possible only with comprehensive visibility and a contextual understanding of user behavior, proven critical in this particular case for both uncovering gaps in user understanding and identifying all potentially compromised endpoints.

If there's a single conclusion to be drawn here, it's that no perimeter solution is impenetrable. It is the user that stands as the last line of defense, with their actions determining if a potential threat becomes a disruptive and devastating attack. Protecting your enterprise - including your network, critical business systems, and incredibly valuable data - starts and ends with seeing, knowing, and deeply understanding your users and their uniquely human behaviors.

As organizations come to the stark realization that it's impossible to close every loophole, we're see the focus quickly shift from prevention to threat detection and response.

DTEX

WORKFORCE CYBER INTELLIGENCE & SECURITY

REQUEST A DEMO

Contact us today to schedule a demonstration at demo@dtexsystems.com

ABOUT DTEX SYSTEMS

DTEX Systems helps hundreds of organizations worldwide better understand their workforce, protect their data and make human-centric operational investments. Its Workforce Cyber Intelligence & Security platform brings together next-generation DLP, UEBA, digital forensics, user activity monitoring and insider threat management in one scalable, cloud-native platform. Through its patented and privacy-compliant meta-data collection and analytics engine, the DTEX platform surfaces abnormal behavioral "indicators of intent" to mitigate risk of data and IP loss, enabling SOC enrichment with human sensors and empowering enterprises to make smarter business decisions quickly.

To learn more about DTEX Systems, please visit www.dtexsystems.com.