

Signal & Noise

INCIDENT SPOTLIGHT

Right Vendor, Right Sender, Wrong Keyboard

You work with them every day. Meet on Zoom every month and end every call with, “If you have any questions, just shoot me an email.” And there’s no shortage of communication with your most reliable vendor.

When an email from them lands in your inbox regarding business as usual, there’s not much to question. It’s from the right sender address and not riddled with typos or urgent language. So you open the PDF attachment. It’s not like it’s a link or executable. You even completed MFA while authenticating.

A defense sector client encountered this risk when a seemingly routine email arrived from a vendor’s compromised account. The message carried the credibility of an established business relationship, but attackers were behind it. The response focused on securing the affected account and investigating potential unauthorized activity.

Our vSOC ruled out the usual suspects. Spoofing was out of the question since it came from the vendor’s real Microsoft 365 tenant. No obvious link or zip file in the message’s body. Instead, the payload was embedded in the PDF.

A link that took users to a page that relayed the real Microsoft sign-in.

This technique is better known as Adversary-in-the-Middle (AiTM), which plays middleman between the user and authentication. [Microsoft’s threat intelligence group](#) describes it as follows: “In AiTM phishing, attackers deploy a proxy server between a target user and the website.” In our case, the website was the proxy page linked in the PDF. “Such a setup allows the attacker to steal and intercept the target’s password and the session cookie that proves their ongoing and authenticated session with the website.” We broke down how this works in our [earlier teardown](#).

Fortunately, tokens were revoked within minutes and our SOC found no follow-on activity such as inbox rule creation or business email compromise. An ongoing session could have ended in the client becoming *the next sender*. Malicious actors know that most people don’t think twice when an email comes from a vendor they already work with. We recommend that you navigate to login pages independently rather than following a link.

IN THIS ISSUE

Incident Spotlight	01
Meet the Analyst	02
Awareness Month	02
Eye on the Threatscape	02

THIS WEEK IN CYBER HISTORY

OCT 6 · 2023

[23andMe](#) disclosed that attackers had used recycled passwords to log into about 14,000 customer accounts. Through the DNA Relatives feature, those accounts exposed the ancestry and profile data of roughly 6.9 million people.

CASE AT A GLANCE

What it was
Adversary-in-the-Middle (AiTM) credential phishing

How it arrived
PDF attachment from a trusted vendor’s compromised account

What happened
PDF link to a proxy of the real Microsoft sign-in

Response
Account secured, tokens revoked within minutes

Impact
No inbox rules, no business email compromise

Seen elsewhere
Vendor accounts used to phish their clients

MEET THE ANALYST

**Jason Jenkins**

DIRECTOR OF INCIDENT RESPONSE

Jason has spent more than two decades finding the truth when the facts aren't immediately visible: the United States Air Force, then a law enforcement career spanning patrol, undercover narcotics, and detective work. Investigations are rarely about a single clue.

He brings that investigative mindset to DFIR, having worked every seat from analyst to leadership. When an organization is facing one of its worst days, incident response is about finding the facts, reducing uncertainty, and restoring confidence.



Hackers don't break in. They log in.

JASON JENKINS, DIRECTOR OF INCIDENT RESPONSE · RADICL

CYBERSECURITY AWARENESS MONTH

October is Cybersecurity Awareness Month. [CISA](#) recommends four core steps for everyone. Here's how each one connects to what we see in the vSOC.

01**Avoid and report phishing scams**

Even when it's not obvious, such as emails from a known vendor or with flawless grammar. Better safe than sorry!

02**Use strong passwords**

[CISA](#) recommends your password is at least 16 characters, randomized, and unique to each account.

03**Use MFA and a password manager**

A password manager won't autofill on a lookalike domain. You also don't have to remember your passwords anymore!

04**Update software**

Turn on automatic updates. According to the [Ponemon Institute](#), "60% of data breaches could have been prevented with better patch management."

EYE ON THE THREATSCAPE

01 [Key ShinyHunters hacker detained in Jordan](#)

A suspected ShinyHunters administrator known as "Rey" was reportedly detained in Jordan on September 29 and is helping the FBI identify other members. It's the second arrest tied to the group in two weeks.

02 [PoeLLM malware hides its server address in a poem](#)

PoeLLM has infected more than 3,400 exposed AI and LLM servers to mine cryptocurrency. Its operators change a few words in a poem on GitHub each time they move servers, and the malware decodes the new address.

03 [North Korea drains \\$387M across 11 blockchains overnight](#)

Attackers sat inside crypto exchange Bitget's security appliances for weeks, then at 1:49 a.m. ran a custom tool that emptied its hot and warm wallets.



Your dedicated vSOC & compliance partner. Military-grade managed cybersecurity for the Defense Industrial Base.

radicl.com