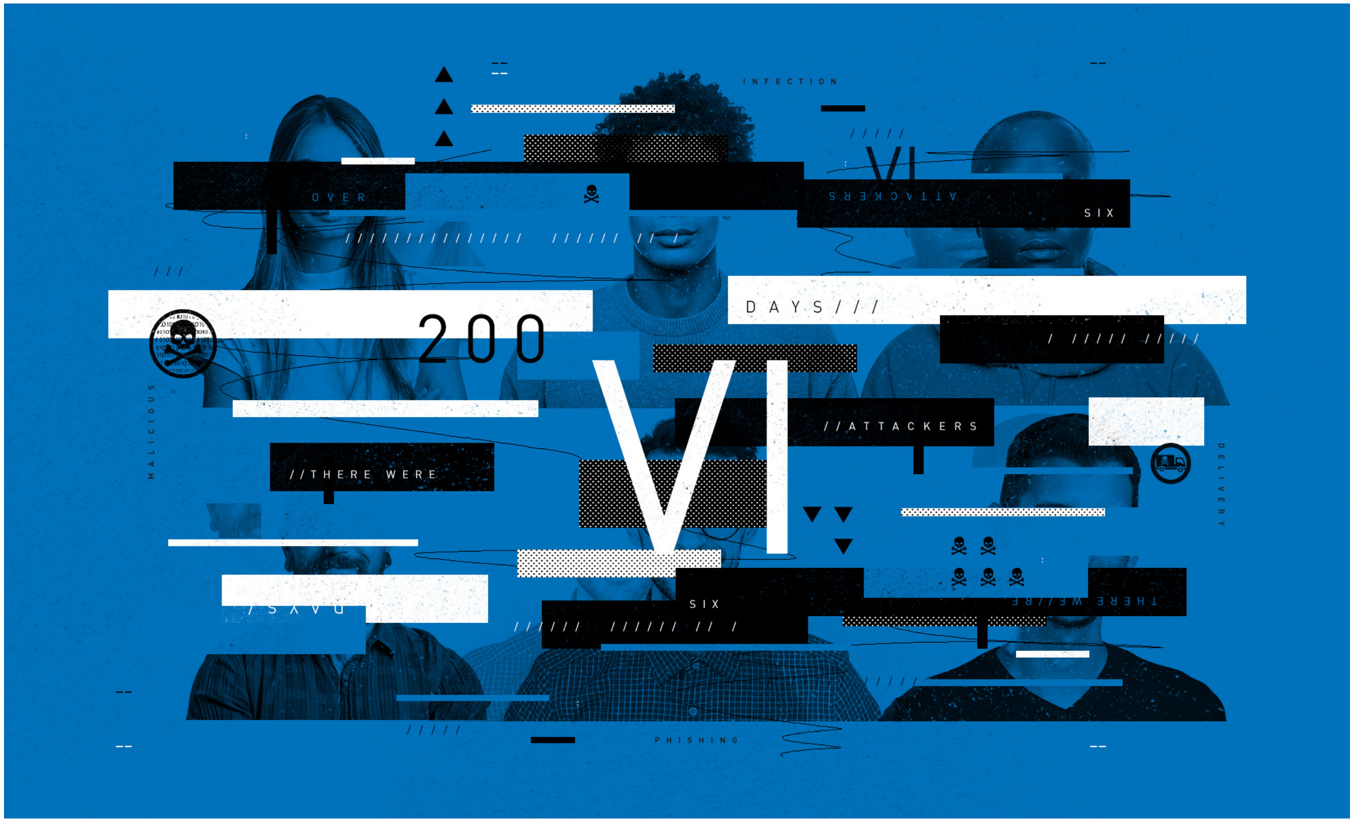
MICROSOFT DETECTION AND RESPONSE TEAM
INCIDENT RESPONSE CASE REPORT // 001

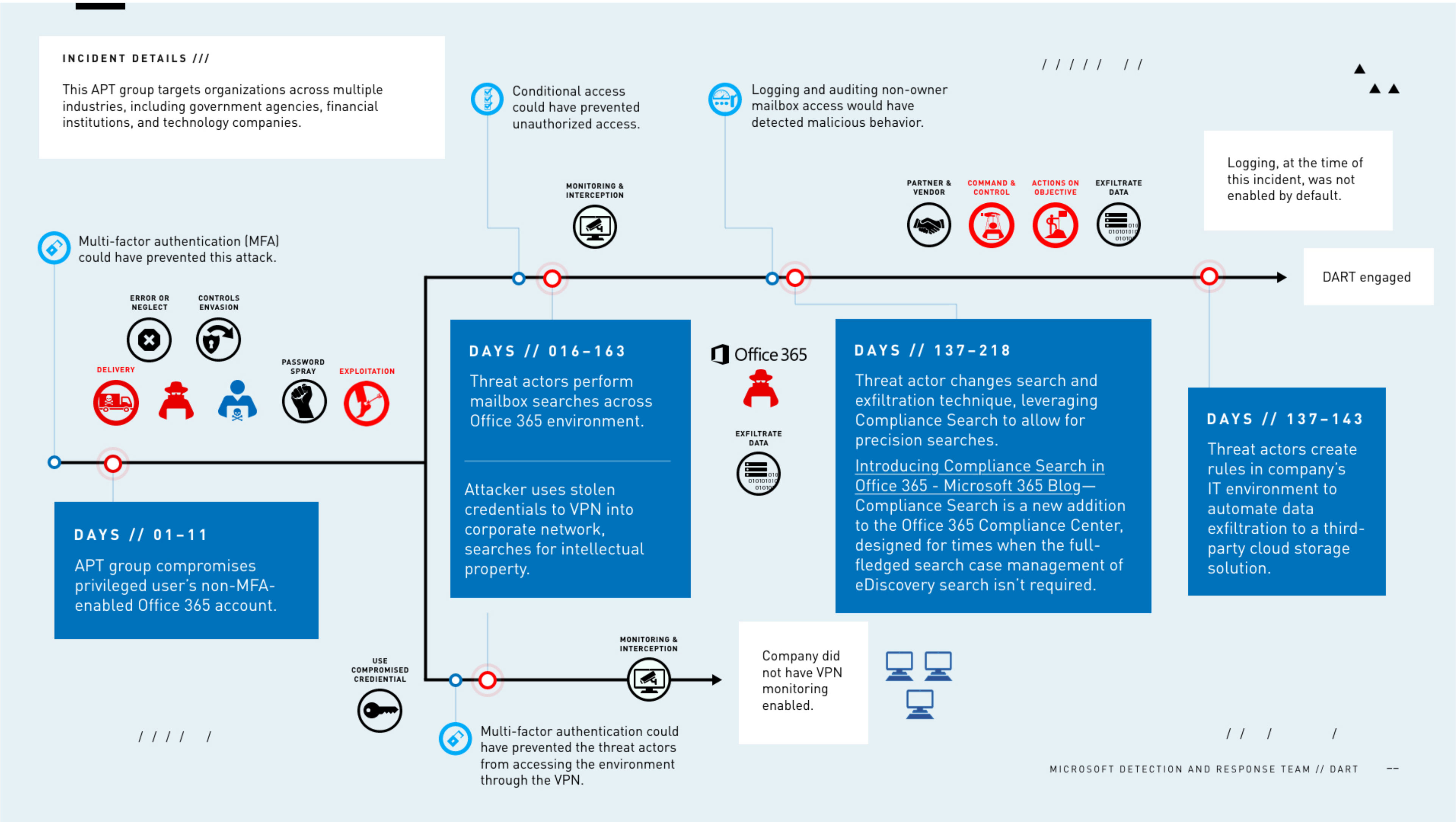
...AND THEN THERE WERE SIX

A STORY OF CYBERESPIONAGE INCIDENT RESPONSE BY DART THAT UNCOVERED FIVE ADDITIONAL THREAT ACTORS IN ONE ENVIRONMENT



Incident Response Case Report 001 is the first of our new series focusing on stories from the cybersecurity frontlines by the Microsoft Detection and Response Team (DART).

If the idea of a malicious attacker's presence in your environment is uncomfortable, imagine discovering six threat actors all at the same time! Recently, Microsoft's Detection and Response Team (DART) was engaged by a large, multinational company that faced a sophisticated, state-sponsored advanced persistent threat (an APT is a malicious actor who gains unauthorized access to a network and remains undetected for an extended period). The APT infiltrated the company's networks after stealing administrator credentials and gaining access, then used sophisticated techniques to systematically access and transfer data as well as sensitive emails. Despite multiple attempts by the company to remove the malicious actor, it remained in the network for 240 days. DART was brought onsite to help the company gain back control and investigate, discovering five additional threat actors in the company's network.



INCIDENT DETAILS ///

This APT group targets organizations across multiple industries, including government agencies, financial institutions, and technology companies.

Multi-factor authentication (MFA) could have prevented this attack.

DAYS // 01-11

APT group compromises privileged user's non-MFA-enabled Office 365 account.

Conditional access could have prevented unauthorized access.

DAYS // 016-163

Threat actors perform mailbox searches across Office 365 environment.

Attacker uses stolen credentials to VPN into corporate network, searches for intellectual property.

Logging and auditing non-owner mailbox access would have detected malicious behavior.

DAYS // 137-218

Threat actor changes search and exfiltration technique, leveraging Compliance Search to allow for precision searches.

Introducing Compliance Search in Office 365 - Microsoft 365 Blog—Compliance Search is a new addition to the Office 365 Compliance Center, designed for times when the full-fledged search case management of eDiscovery search isn't required.

DAYS // 137-143

Threat actors create rules in company's IT environment to automate data exfiltration to a third-party cloud storage solution.

Logging, at the time of this incident, was not enabled by default.

DART engaged

Company did not have VPN monitoring enabled.

Multi-factor authentication could have prevented the threat actors from accessing the environment through the VPN.

MICROSOFT DETECTION AND RESPONSE TEAM // DART

HOW DID IT BEGIN?

The attacker leveraged a password spray attack to gain the company's Office 365 administrator credentials. Password spray is a technique in which a volume of common passwords are attempted in the hope that one will provide access to an account. Admin credentials are often targeted for the access they give to the company's IT environment.

With access to the network, the attacker entrenched itself in the company's environment. It used the stolen credentials to conduct multiple mailbox searches for other credentials that were, unfortunately, often shared via emails without digital rights management between the company and its customers. DART noted that the attacker specifically searched for these emails in certain regions and market segments, which provided clues about the attacker's motivations. The team advised the company that this attack was most likely a case of cyberespionage as the attacker was looking for specific information—in this case IP in certain markets.

In an uncommon move, the attacker used the customer's existing systems, including eDiscovery, the Compliance Search feature, and Microsoft Flow, to automate stealing its search results. By "living off the land" and easing its workload, the attacker found ways to turn on existing features that the customer had implemented but was not actively using or had not turned on. These systems had not been configured to gather logs from high-value systems or to detect unauthorized use of them. The attacker spotted this and took advantage of it.

This activity finally ended on day 243 when the DART investigation began.

DART also identified five additional, distinct attacker campaigns persisting in the environment that were unrelated to the initial incident.

HOW DID DART RESPOND?

During the first month, the company attempted to remediate the compromised Office 365 account. When the attack persisted, the company engaged an incident response vendor to perform an investigation. This investigation lasted more than seven months and revealed a possible compromise of sensitive information—pertaining to the victim and the victim's customers—stored in Office 365 mailboxes. 243 days after the initial compromise, DART was then brought in to work alongside the incident response vendor and the company's in-house teams.

DART quickly identified targeted mailbox searches and compromised accounts, as well as attacker command-and-control channels. DART also identified five additional, distinct attacker campaigns persisting in the environment that were unrelated to the initial incident. They discovered these attackers had entered the environment even earlier to establish access channels (i.e., back doors) for later use as needed.

Rapid detection was possible during the investigation because DART applied their expertise with the Microsoft security stack and solutions to assess the products, their configurations, and the security state. Comprehensive assessment of all Microsoft operating systems was conducted to ensure that no other APT actors were present. A plan was formulated to regain control of the customer's environment, harden assets to prevent future intrusion, and enable monitoring and detection in the event of future attempts to compromise the company's network.

WHAT COULD HAVE BEEN DONE?

The company could not see the APT group's attack coming because they did not have the recommended auditing and logging set up. This was a big factor in the adversaries' ability to exploit attack opportunities in the company's environment.

What can be done then to minimize exposure to similar attacks?

01

Best practices such as multi-factor authentication (MFA), conditional access, and enabling logging cannot be optional. These measures must be deployed as part of routine deployment plans. https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted

02

Legacy protocols always need to be addressed. Even combining legacy authorizations with MFA and Conditional Access can be risky, as these protections can be bypassed via legacy authentication. The only safe option is disallowing legacy authentication altogether. https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/block-legacy-authentication

03

Training of first responders against the latest attack scenarios within the current infrastructure is critical in defending against these types of attacks.

04

Proper aggregation of all the logging sources from company resources, such as through a SIEM solution, assists in identifying attacks and anomalous behavior.

05

Legitimate tools and software continue to be leveraged in a malicious manner, which means that existing security tools must be configured to gather logs from high-value systems. This change allows unauthorized activation or use of these systems to be noticed and investigated as soon as possible.

Microsoft offers a variety of solutions as well as benchmarks for security configurations. DART currently offers Security and Crisis Response Exercises for organizations to train their in-house teams on incident response scenarios. Microsoft has also partnered with the Center for Internet Security (CIS) to develop benchmarks to provide prescriptive guidance for establishing secure baseline configurations for Microsoft 365 and Azure.

Stay tuned for more DART Case Reports from the incident-response frontlines...

MICROSOFT DETECTION AND
RESPONSE TEAM // DART

THIS DOCUMENT IS FOR INFORMATIONAL PURPOSES ONLY. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.