Real-life cybercrime stories from DART, the Microsoft Detection and Response Team

By Microsoft Security Team

Published: 2020-03-09 · Archived: 2026-04-05 16:36:53 UTC

When we published our first blog about the Microsoft Detection and Response Team (DART) in March of 2019, we described our mission as **responding to compromises and helping our customers become cyber-resilient**. In pursuit of this mission we had already been providing onsite reactive incident response and remote proactive investigations to our customers long before our blog. And our response expertise has been leveraged many times by government and commercial entities around the world to help secure their most sensitive, critical environments.

When our team works on the frontlines of cybersecurity, chasing adversaries in many different digital estates on a daily basis, our experiences become valuable lessons on attacker methods as well as security best practices. And because of this, our colleagues and customers have been asking for case studies, reports, and even anecdotes from DART engagements.

Finally, we can respond to these inquiries by publishing our first DART Case Report 001: …And Then There Were Six. Case Report 001 is a story of cybercrime when DART was called in to help identify and evict an attacker, only to discover there were already 5 more adversaries in the same environment. Read the full report for the details.

In the DART Case Reports, you will find unique stories from our team's engagements around the globe; details on the attacker(s) methods, a diagram of how they progressed in the environment, how DART was able to identify and evict them, as well as best practices to avoid similar incidents.

What you *won't* find is any information about our customers, or their defenses, because in our reports we will focus solely on the attacker Tactics, Techniques, and Procedures (TTP) and how to defend against them. Read our first report, reach out to your Microsoft account manager or Premier Support contact if you need more information on DART services—and stay tuned for more DART Case Reports.

DART leverages Microsoft's strategic partnerships with security organizations around the world and with internal Microsoft product groups to provide the most complete and thorough investigation possible.
