Catching APT3 with cyber deception

Three case studies

Cymmetria

Contents

Executive summary

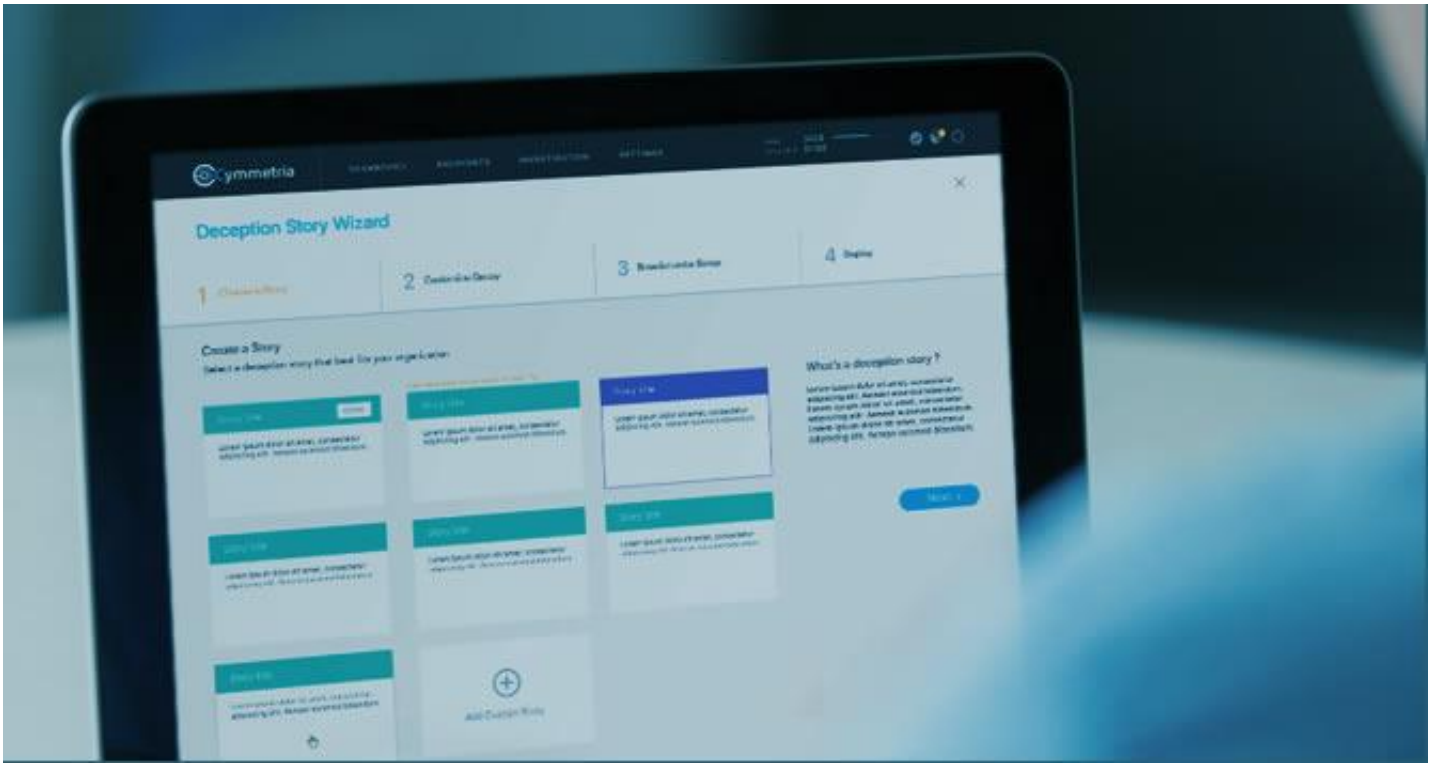
In this document we will discuss successful captures of APT3 (a.k.a. pirpi), which we have encountered multiple times during our work with customers. We will briefly examine three case studies that show how cyber deception (and specifically, MazeRunner) was used to detect and mitigate this type of APT, and will dive deeper into one of the case studies to more closely examine how this works.

The first case study takes place in a European government organization's network. The organization was warned by a third party of a breach in their network. While the organization was initiating its investigation, MazeRunner alerted to the threat actor's presence within a week of being deployed.

Our second case study has taken place several times at multiple customers. In these cases, a simplistic technique (network scanning) was used by the threat actor, and MazeRunner alerted on the threat actor's activity.

Our third case study, which we discuss in more detail, takes place in the network of a defense contractor, where MazeRunner caught APT3 "on the rebound" as it was returning to the network after being mitigated during incident response. In this case, MazeRunner was deployed to assist with stealth incident response using cyber deception. After remediation, MazeRunner remained deployed and we were able to assure the defense contractor that the threat actor was inactive. One month later, MazeRunner caught APT3 when it returned to activity from a previously unmonitored part of the network.

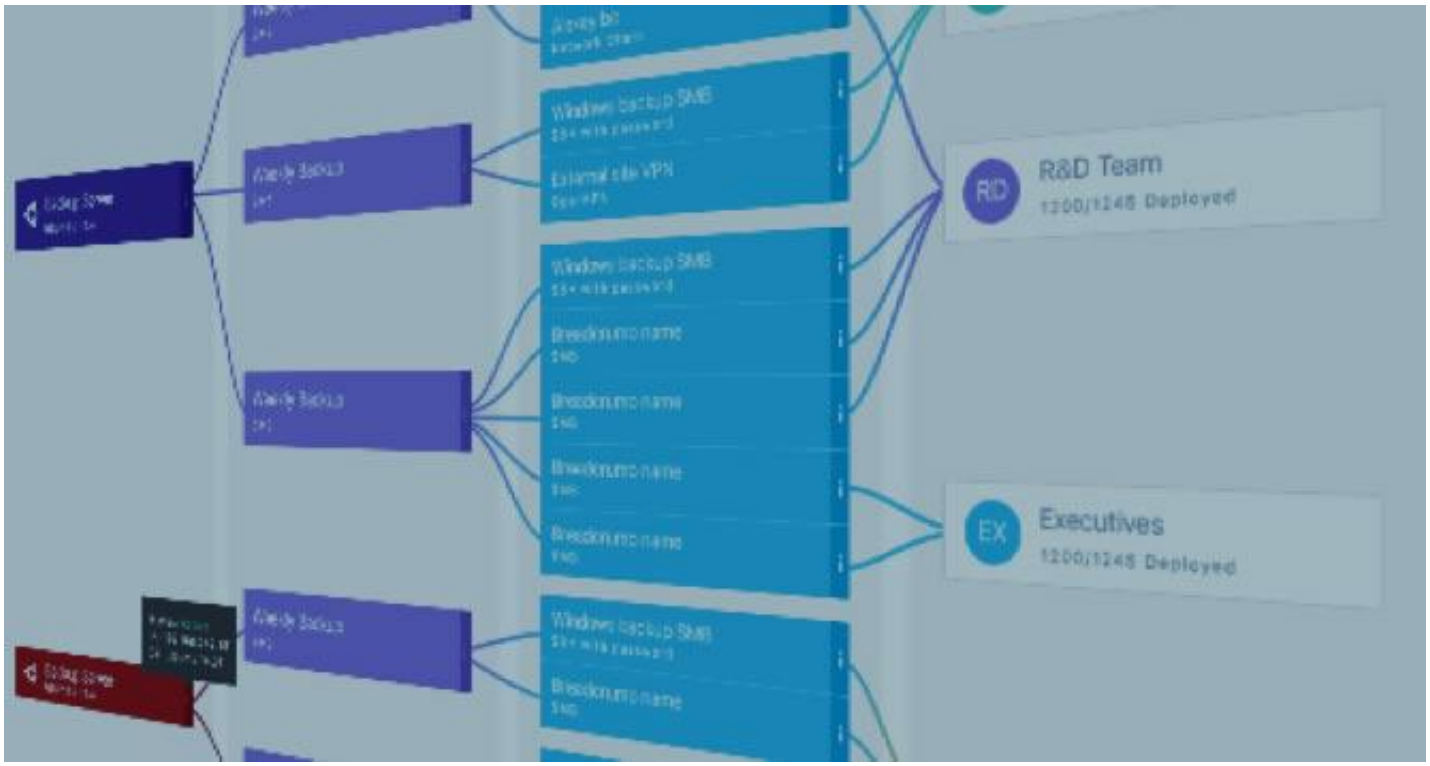
Unlike our Patchwork APT report or our work with CrowdStrike on Rocket Kitten, these case studies do not cover a new APT group; they describe the cyber deception tools, techniques, and processes used by Cymmetria's cyber deception product, MazeRunner, to catch the threat actors.



Case study 1

AT THE EUROPEAN GOVERNMENT ORGANIZATION

A European government organization received warning (from an outside agency) that APT3 had had access to its network for some time. While the organization was initiating its investigation, MazeRunner was installed and, within a week, detected the threat actor's location in the network, as well as their toolset. MazeRunner provided the organization with IoCs (compromised hosts) to get the incident response process started, as well as the malware sample that MazeRunner caught the attacker running on one of its decoys. This led to the discovery of a compromised Citrix server, among other compromised assets. Cymmetria assisted the organization in using MazeRunner alongside its endpoint solution, to streamline the remediation process as IoCs were discovered.



Case study 2

SEEN SEVERAL TIMES AT MULTIPLE CUSTOMERS

MazeRunner has detected network scanning activity, which proved to be simplistic network scanning, on multiple occasions at different customer sites. On these occasions, the threat actor was easily identified as APT3 due to the IoCs of the first- and second-stage toolsets used by the threat actor.

Case study 3

AT THE DEFENSE CONTRACTOR

Cymmetria was invited to participate in live incident response after an APT was discovered at a customer site. The thinking was that, with deception, the threat actor could be detected more quickly, and stealthily.

If a threat actor is entrenched on a network, planting a new remote site, new backup server, or perhaps a new VPN service for them to find might "wake them up"; this allows us to force the threat actor to tip their hand, without tipping ours with a noisy incident response process. Essentially, we are able to collect Indicators of Compromise (IoCs), and the threat actor's tools, techniques, and procedures (TTPs), as well as their second stage toolset.

Following the stealth incident response, MazeRunner remained deployed. We were able to assure the defense contractor that the threat actor was inactive, and MazeRunner later caught the threat actor when it returned to the network after lying dormant in an unmonitored part of the network.

THE INVESTIGATION

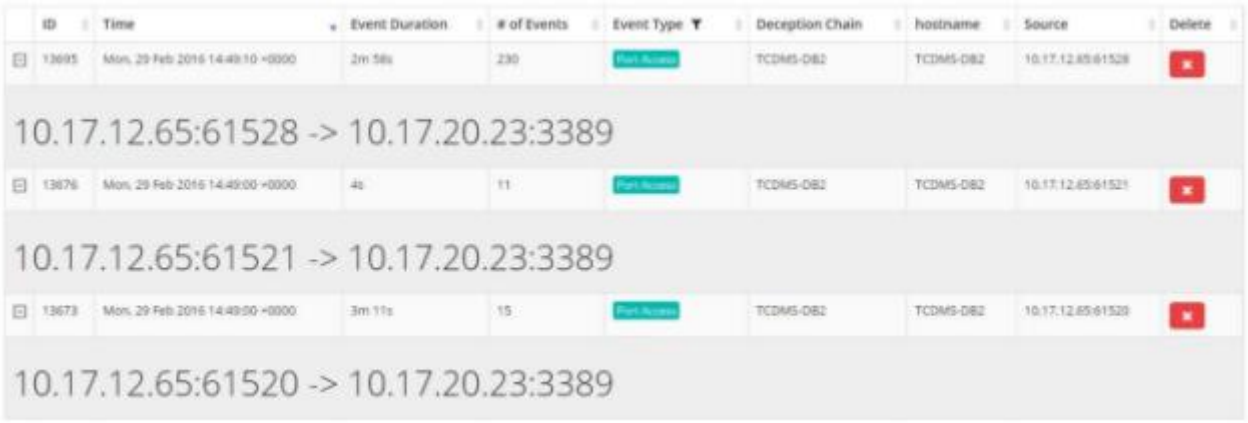
The defense contractor was alerted by threat intelligence to possible Chinese threat actor activity on its network. The intelligence received was a low-quality IoC (on how investigators could find a specific file dropped by the threat actor, when it had an exception—which occurred in only a small percentage of the cases). With this limited intelligence, the defense contractor was only able to discover 12 compromised machines, from which it was able to extract only the first stage malware (identified as APT3 and attributed to the Chinese).

The defense contractor further discovered an exfiltration module of the malware, which targeted Lotus Notes, in a different area of the network.

INCIDENT RESPONSE AND CYBER DECEPTION

The incident response was carried out in three stages. First, the defense contractor's responders worked alone. Then, Cymmetria was brought in and we installed MazeRunner to deploy cyber deception in the network. Lastly, a well respected third-party incident response firm was brought in to verify the original incident response team's efforts.

As far as cyber deception goes, our goal was to attempt to "wake up the dragon" —to create interesting network elements that would tempt a threat actor, even if the threat actor had already been in the environment for a while. We gave the decoys names that were reflective of what the defense contractor believed to be the threat actor's intelligence requirements. Incident response and remediation were completed and MazeRunner remained deployed in the network.



Connections from 10.17.12.65 to a decoy on 10.17.20.23, on the RDP (Remote Desktop Protocol). These indicate that 10.17.12.65 is an infected endpoint.

ASSURANCE OF INACTIVITY

Since we knew the threat actor's TTPs, we were able to monitor the environment for lateral movement, and assure the defense contractor to a high degree that the threat actor was in fact inactive.

ON THE REBOUND

One month after remediation, we received an RDP connection attempt alert from one of our MazeRunner decoys. This led the defense contractor to investigate the machine behind the source IP, at which time they observed new and significant malicious traffic. The defense contractor realized that this was a previously unknown, compromised machine in a part of the network they weren't aware had been breached.

OTHER INCIDENT RESPONSE ACTIVITIES

Other incident response activities we assisted with included examining and retrieving stolen data, discovering the attacker's exfiltration site, discovering the extent of the damage caused, and more.

In summary

Cyber deception detects threat actors in short order, reducing the cost of detection. Further, it can assist by stealthily performing incident response in order to avoid tipping your hand, as well as provide assurance that the threat actor has indeed been remediated (or has returned) following an incident.

Cyber deception has been successful in catching multiple advanced threats. While it can be deployed with a simple goal in mind (such as lateral movement detection) at low effort and maturity requirements, it can also be deployed and scaled for advanced use cases, from Responder.py/Pass-the-Hash detection, to attacker profiling and personalized threat intelligence.

For more information about MazeRunner, or for a product demonstration, please contact Cymmetria at info@cymmetria.com.