CASE STUDY

DETECTING A JAVA BACKDOOR WITH DTEX

INCIDENT FACTS

Industry: Finance

Company Size: 10,000+ Users

Threat: Targeted phishing attack to deliver a java backdoor

Time-to-Resolution: Detected in real time, resolved in 24 hours

Introduction

When organizations have true visibility into how users interact with data enterprise-wide, they illuminate blind spots that help them fill in the gaps across their entire security posture.

This recent incident at a Dtex customer is perfect proof. This customer – a large financial services company with more than 10,000 employees – was the victim of a java backdoor attack that targeted a senior member of the company.

Despite the fact that they had several AV, EDR, and email security tools deployed, this attack still managed to slip through the cracks and land on the computer of a high-ranking employee. Because the malware utilized commonplace admin commands, other solutions did not alert on it. Dtex, however, was the only tool that contextualized this activity within the user's full story – and therefore was the only one to pinpoint the threat, while building a full audit trail.

Had it not been for Dtex's visibility and alerting, the attack would have gone completely undetected, potentially leading to data theft, sabotage, lateral movement within the organization, or worse.

What's more, without Dtex's audit trail and organization-wide visibility, the SOC team would not have understood exactly how this malware got onto the machine, nor would they have been able to confirm that no other users were affected.

Ultimately, Dtex's detection and forensic capabilities enabled a complete time to resolution of under 24 hours.

INCIDENT TIMELINE

Hour 0:
Targeted phishing email received by a C-level executive. Email was shipping-themed, and the user was in fact expecting a package.

ProofPoint scanned the email but found no suspicious links.

User opens email, clicks on malicious link and is pointed to a compromised Turkish website that downloads malware.

Within 2 hours:
Dtex alerted on unusual and potentially malicious application behavior: the application attempting to conceal files related to its execution. EDR did not alert.

SOC analyst reviewed the alert & escalated to Dtex investigators.

Within 3 hours:
Dtex produced report identifying that this was a targeted high-risk attack requiring immediate action.

Within 8 hours:
ProofPoint, long after the fact, triggered an alert retroactively identifying the link in the email as malicious.

Within 24 hours:
SOC team took possession of the affected laptop, reformatted it, and took it off the network.

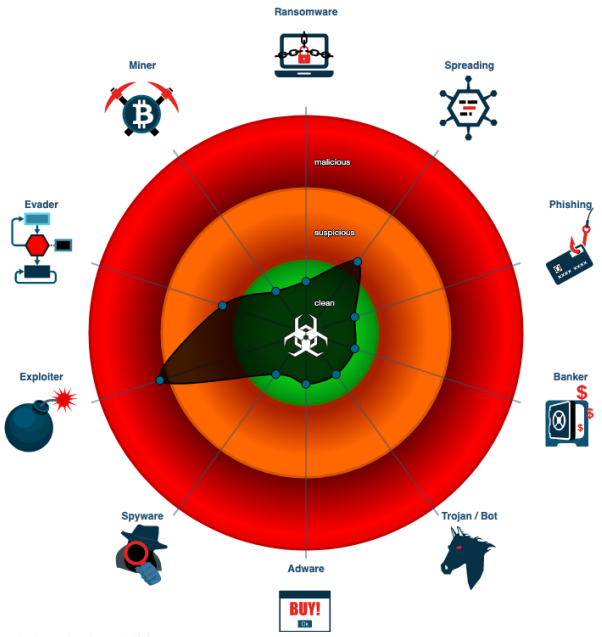
With Dtex, they were able to definitively confirm that no other users were affected and no further lateral movement took place.

The Threat

In early August, Dtex customer received a series of alerts relating to potential lateral movement and malware behavior on a single user's device. Analysis of these alerts and the surrounding activity identified a remote access trojan (RAT Java backdoor operating on the user's device.

This backdoor bypassed security measures to provide easy access to the device to an unknown, malicious third party – enabling user information and data to be stolen, or for other malware to be distributed onto the endpoint.

Worse, the affected laptop belonged to a C-level executive, significantly increasing the risk level of this threat had it remained undetected.



Classification of the malware from JoeSandbox.com

Detection

When the user opened the email and clicked the link, the device was pointed to a malicious domain and downloaded a .jar file named "ShipmentLabel". Unbeknownst to the user, this malicious executable then rendered itself hidden by creating a new temporary folder on the desktop and them moving all associated malware files to this new location.

It also created a new path in the registry directory, setting up a persistent foothold on the machine, and took a number of actions to enumerate the environment.

Though this organization had Cylance Endpoint Detection and Response, anti-virus solutions, and ProofPoint installed, none of these alerted on this malware. ProofPoint had even scanned all of the links in the original USPS-themed phishing email that launched the malware – and raised no suspicion, as the underlying domain was a legitimate website.

These tools did not alert because the malware utilized typical admin commands – activities that were commonplace with, for example, an IT or administrative user. On their own, outside of context, these individual actions did not raise alarm.

Dtex, however, was the only solution that looked at the context of the scenario and took into account the fact that these activities were wildly suspicious for this specific user. Therefore, it alerted on this potential malware activity immediately.

Mitigation and Investigation

After the initial malware was identified, the customer's security team conducted searches of those indicators of compromise across the rest of the user environment, in order to establish if any other users had interacted with similarly-themed emails or anomalous instances of Java-related activities.

With Dtex, these searches were conducted organization-wide i n minutes, answering questions such as:

- Was anyone else impacted?
- Has anyone else visited that malicious domain?
- Did the user forward the email to other members of staff?

The company immediately decided to wipe and decommission the device. They could also quickly confirm that this phishing email was a targeted attack to this particular user that did not affect any other users, nor did it spread laterally throughout the organization.

Without Dtex, not only would the customer have never have found this major threat, but they also would have lacked the visibility and audit trail to conduct a quick and thorough investigation.

Conclusion

In the end, this story exemplifies a universal truth that affects the entire industry: no single security tool is perfect, and achieving full visibility into the blind spots is key. When it comes to malware, AV signatures and IOCs are important building blocks, but do not always provide the full story on their own.

In this case, simple heuristics related to hiding directories/files and the execution of administrative commands quickly pointed the security team in the right direction, highlighting activity that even malware-focused tools didn't catch.

This is the importance of visibility into user behavior, with statistical contrast against the rest of the user population. Organizations cannot detect – or analyze – what they cannot see.

With Dtex, organizations get scalable, comprehensive user visibility enterprise-wide that will see threats that inevitably slip through the cracks. Ultimately, this is what enabled this customer to quickly find the threat, investigate it, contain it, and adjust their future education and security goals to prevent it from ever happening in the future.