LABSCON

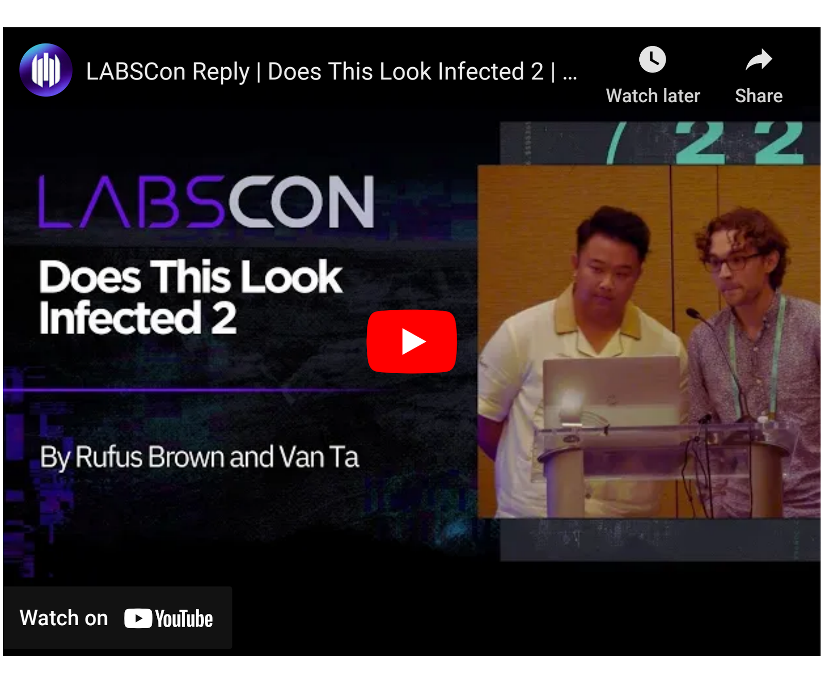
LABScon Replay | Does This Look Infected 2 (APT41)

LABSCON / MAY 18, 2023

In March of 2022, Mandiant released new research detailing APT41's persistent campaign leveraging novel exploits, malware, and techniques to compromise U.S. State Government networks. APT41 continued to demonstrate their tempo by exploiting a zero-day in an animal health management application before quickly shifting to operationalize the then fresh Log4j vulnerability.

At the time, APT41's goals were unclear. The "Double Dragon's" name is derived from APT41's well documented dual espionage and cybercrime operation. Were they hitting U.S. State Governments to support greater intelligence collection initiatives, or for financial gain?

Mandiant researchers Van Ta and Rufus Brown take us on a journey of discovery into the mysteries of a long tail, persistent compromise of U.S. Government networks and offer a unique insight into one of the world's most sophisticated threat actors.



Does This Look Infected 2

Transcript

00:00:05 **Van Ta**
All right. Thank you, everyone. Thank you for attending. We also wanted to extend a thank you to the lab's organizers for a great inaugural event so far. So let's give them a round of applause before we get started. So my name is Van Ta. This is my colleague Rufus Brown, and we're both part of Mandiant's Advanced Practices Team. We're really excited to be here today to expand on a story that we began telling in March of this year. And so, without further ado, this is Does This Look Infected? First. I must disclaim you.

00:00:43 **Van Ta**
All right. So in March of this year, we published research on a persistent, months long APT41 campaign to gain access to state government networks. Between May 2021 to February of 2022, APT41 compromised

SentinelOne

1.00x

00:00:00 00:21:34

About the Presenters

Van Ta is a Principal Threat Analyst on Mandiant's Advanced Practices Team, where he leads historical research into the most impactful adversaries facing Mandiant's customers. His research on various named threat actors FIN11, FIN12, FIN13, and APT41, has been referenced by both private and public organizations.

Rufus Brown is a Senior Threat Analyst on Mandiant's Advanced Practices Team specializing in attribution and malware tradecraft. His joint research into APT41 was covered by national media outlets.

About LABScon

This presentation was featured live at LABScon 2022, an immersive 3-day conference bringing together the world's top cybersecurity minds, hosted by SentinelOne's research arm, SentinelLabs.

Want to join us for LABScon 2023? The Call for Papers is now open!

APT41 LABSCON

LABSCON

LABScon brings together the world's top cybersecurity minds to share cutting-edge research and push the envelope of threat landscape understanding.