Acronis

Acronis Partner Day at MSP Global 2024

Time to **Go Native.**

Acronis

May I have a (Win)word?

A TRU research story

#CyberFit

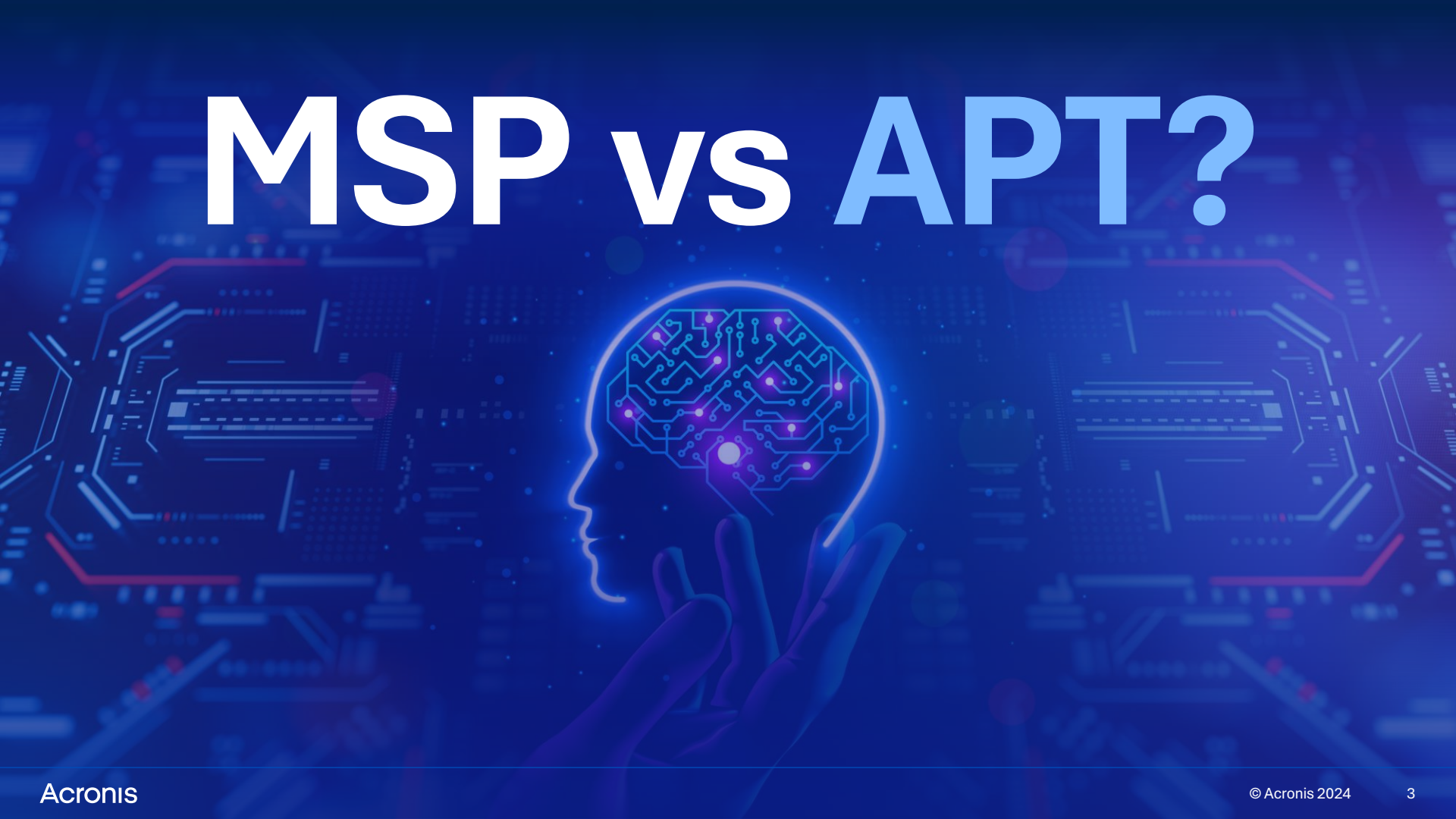
Nick Grebennikoff

Chief Development Officer, Acronis

Robert Neumann

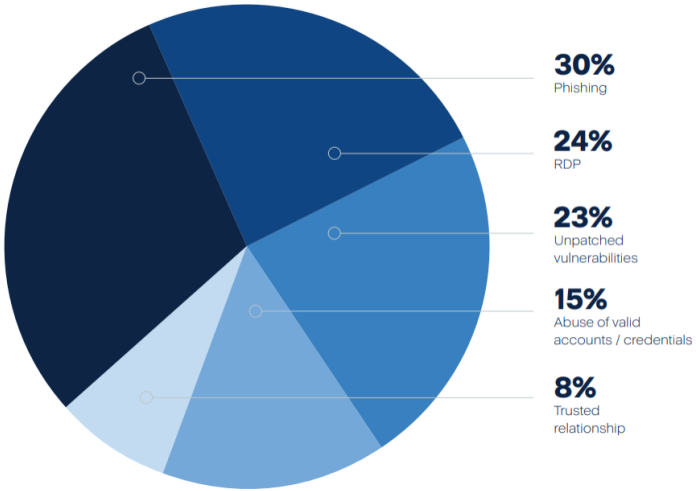
Head of TRU Labs, Acronis

MSP vs APT?

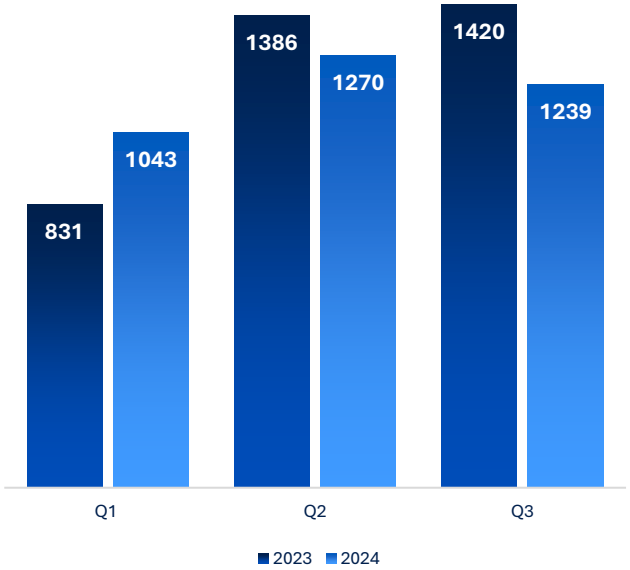


Why Does It Matter?

Initial vector of attacks on MSPs



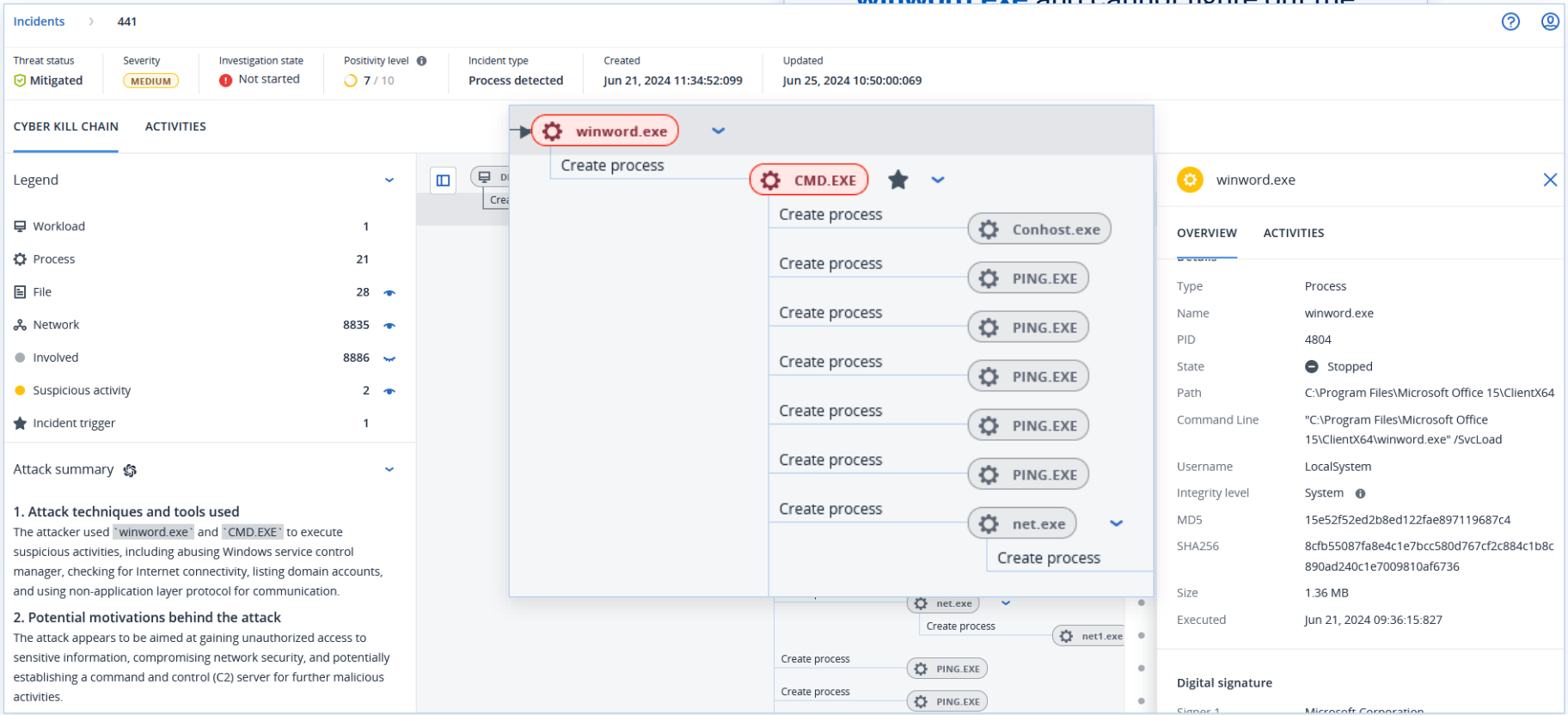
Ransomware victims 2023-2024



How Does Acronis Protect Drones?

How Did It All Begin?

Hi Support, I have an incident triggered from **winword.exe** and cannot figure out the



Is Anything Playing Hide and Seek?

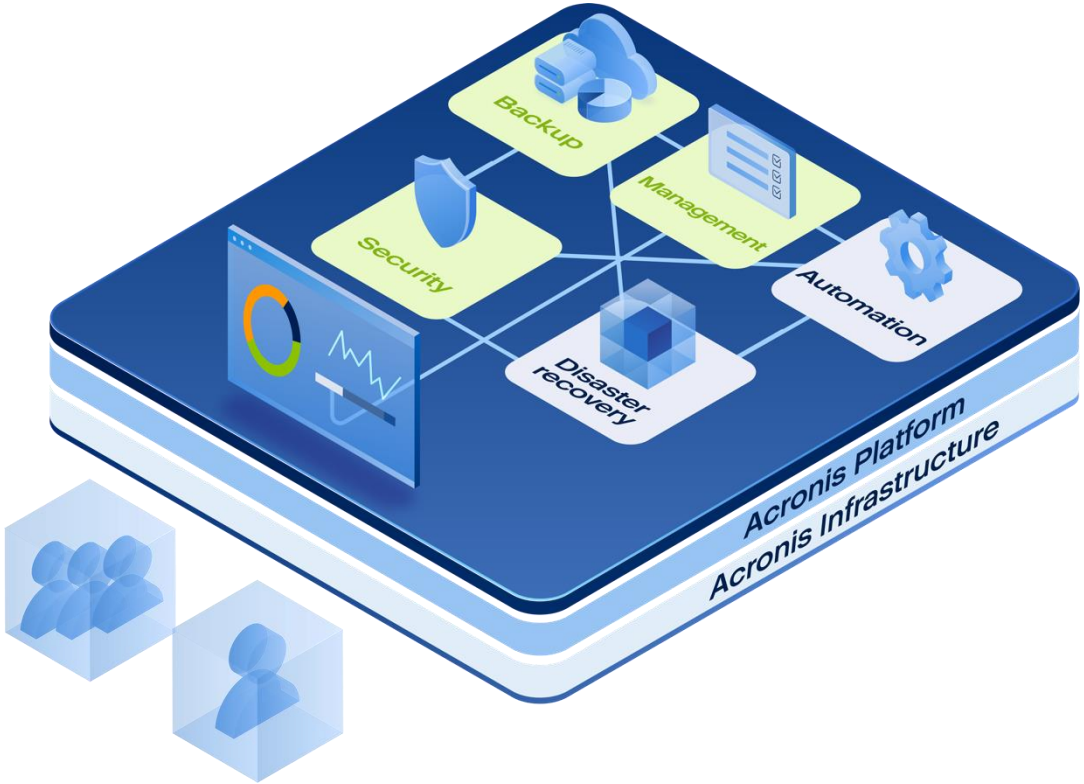
On disk

winword.exe

wwlib.dll
(Loader)

random filename and extension

Deeper Investigation Through a Backup

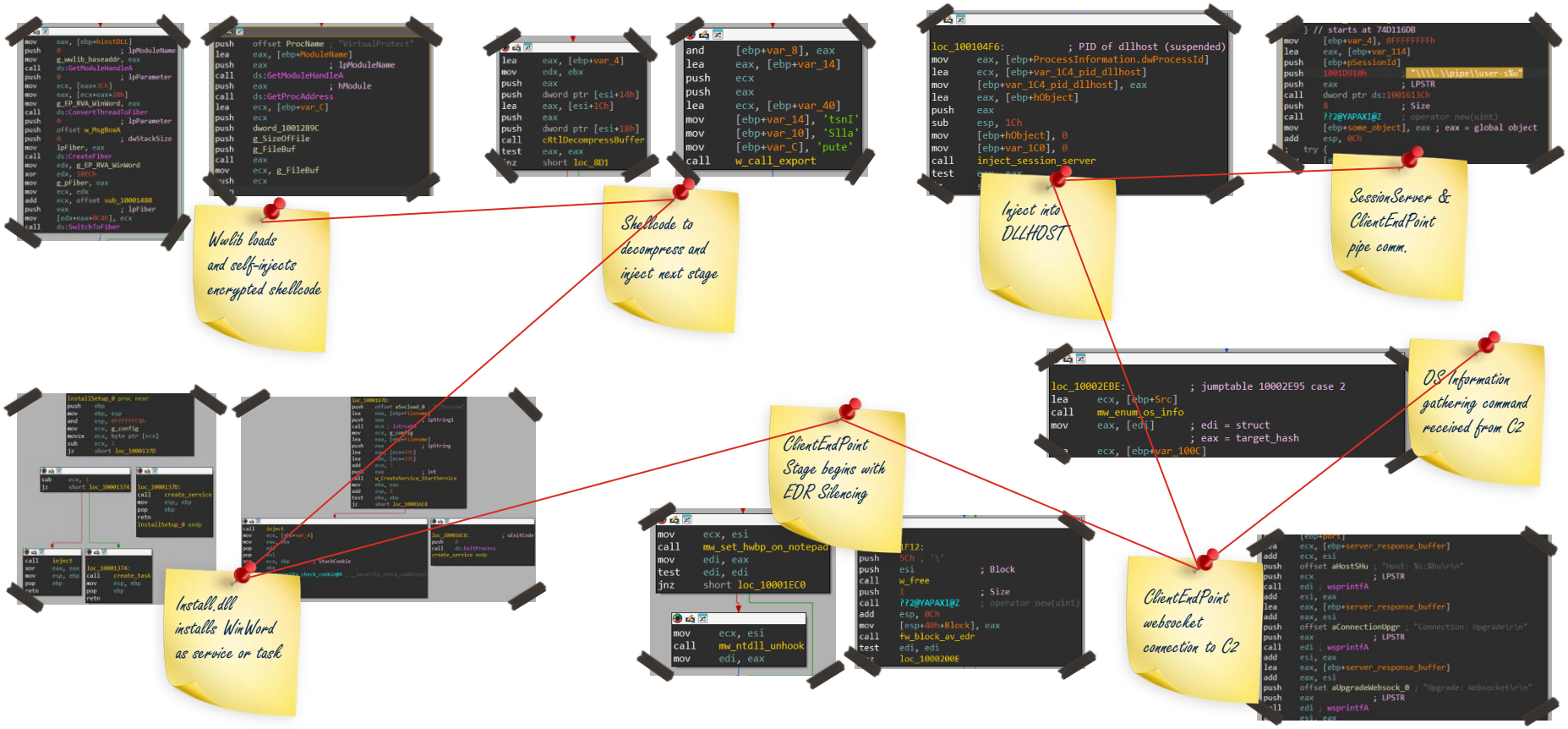


Are Our Customers Safe?

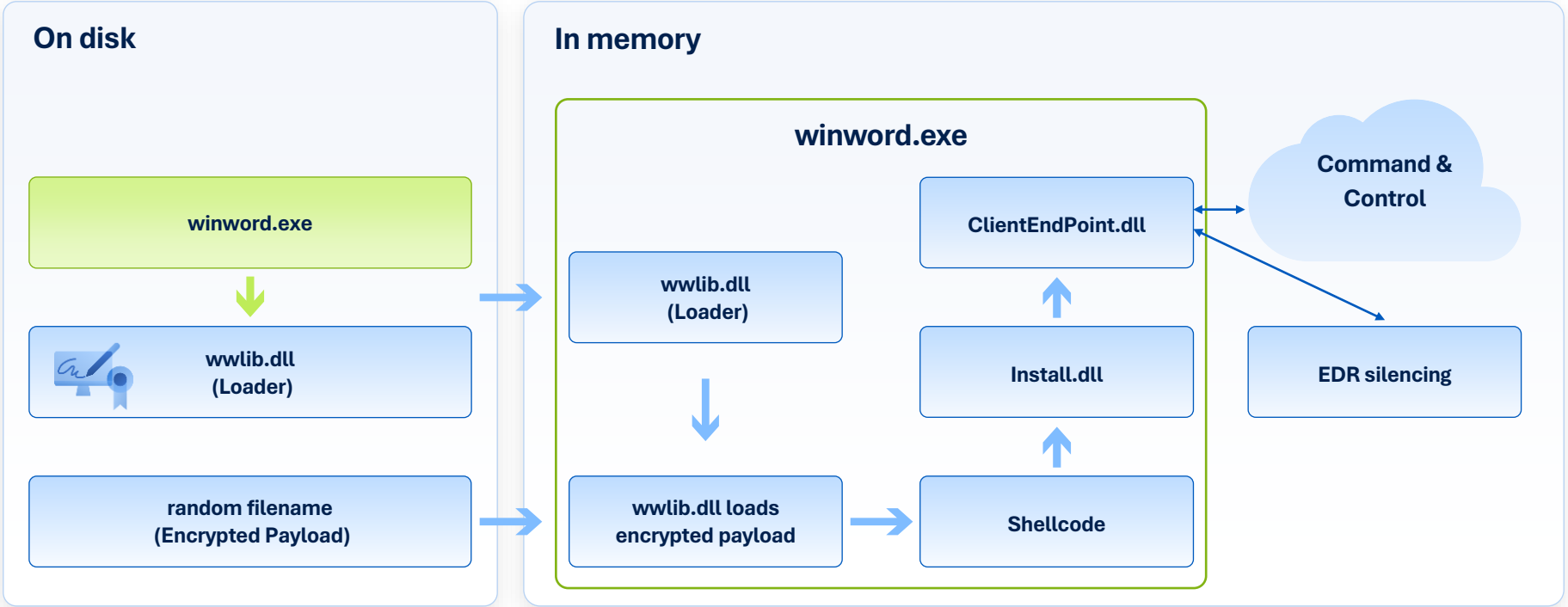
Is It a World-Wide Attack?

All Virtual Roads Lead to Taiwan

What Is the Purpose of It All?



Deep Research Result – A Stealthy Backdoor Discovered



Fingerprinting the Target

Preparing for Future Eavesdropping

Planning to Exfiltrate Data

Summary

Silencing popular EDR products

Exploiting 10+ year old Winword via side-loading

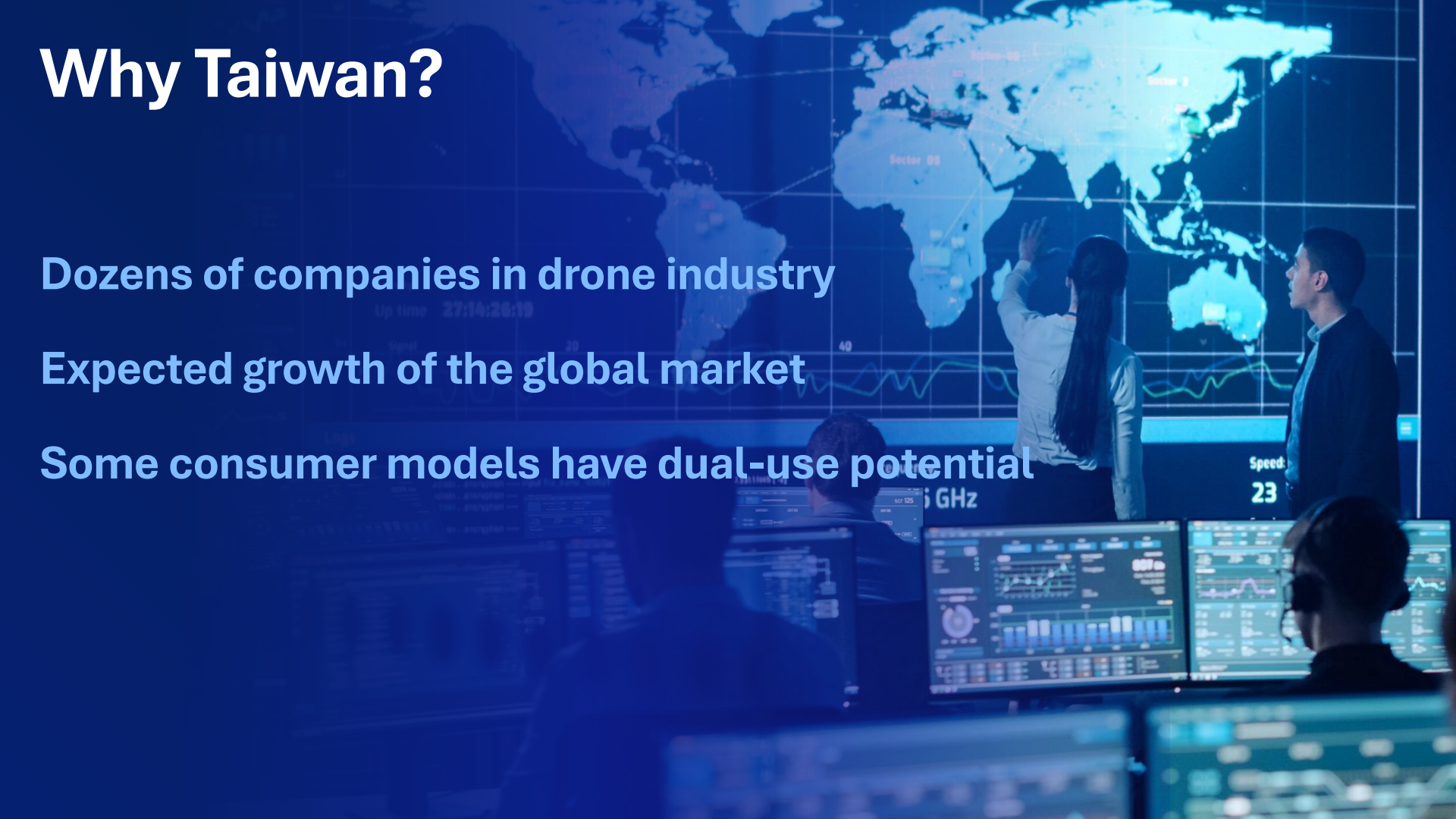
Using a digital signature valid for 3 years

Command and Control is protected by Cloudflare, but located in Taiwan

Stealthy operation with in-memory footprint

Highly sophisticated targeted attack against Taiwanese Aerospace

Why Taiwan?

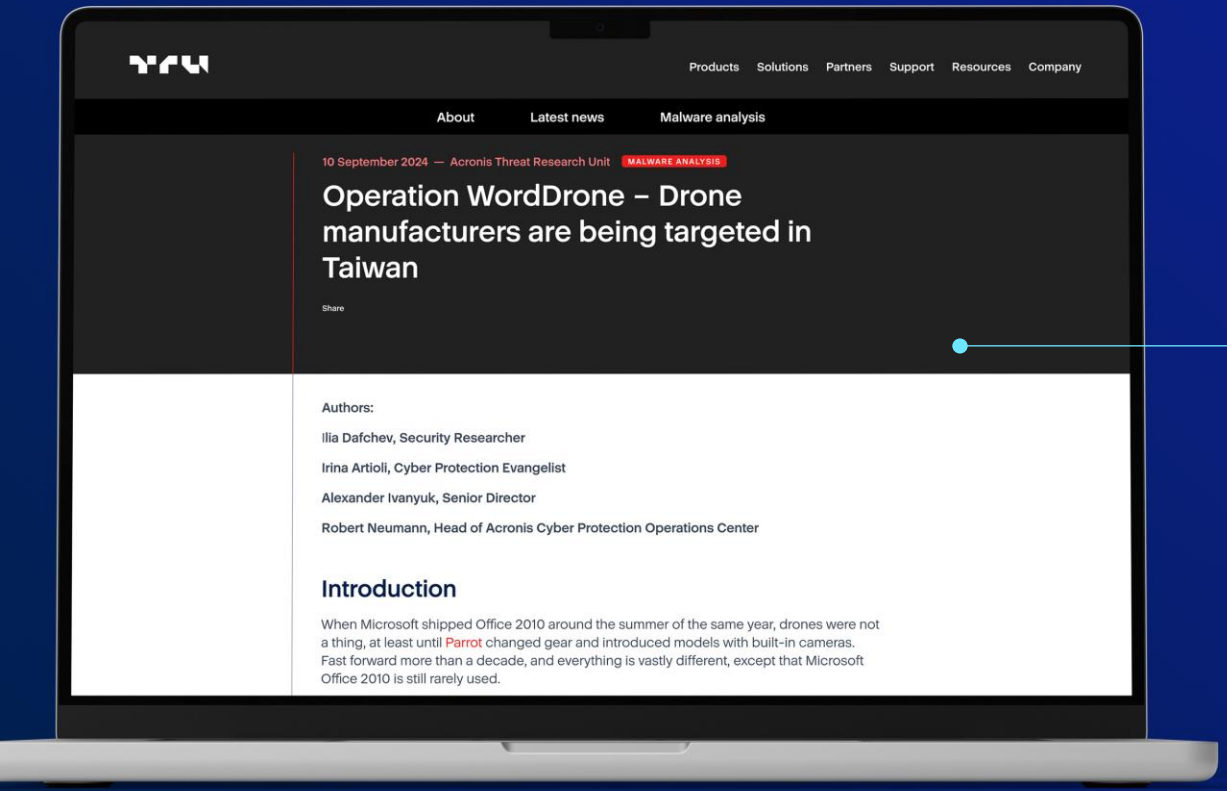


Dozens of companies in drone industry

Expected growth of the global market

Some consumer models have dual-use potential

Media Coverage



Media Coverage

betanews

Operation WordDrone: Taiwan's drone makers hit by sophisticated cyberattack

By Brian Fagioli

DRASTIC
DRONES | ROBOTICS | A.I

Threat Actors Target Taiwanese Drone Manufacturers

BY DRASTIC_ADMIN ON SEPTEMBER 11, 2024 — DRONES, FEATURED STORIES, SECURITY, TECHNOLOGY

The Acronis Threat Research Unit has released new technical details about a threat group targeting Taiwan drone manufacturers who use an outdated version of Microsoft Word.

Dubbed by Acronis as WordDrone, TRU researchers were able to uncover the tools and techniques used in the malware including EDRSilencer and Blindslide. Further, they provide an in-depth analysis of ClientEndPoint.dll, the final stage of the attack carried out in two important steps. Additional analysis of command and control communication, as well as detailed findings of post-exploitation actions, is also included in the findings.

The Hacker News

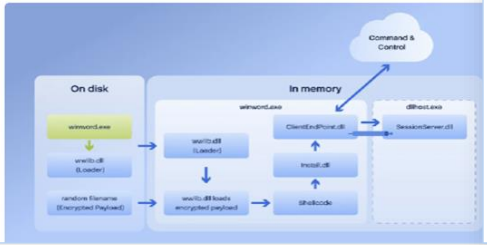
TIDRONE Espionage Group Targets Taiwan Drone Makers in Cyber Campaign

Sep 09, 2024 Ravie Lakshmanan

Update

Cybersecurity firm Acronis has published its own findings into the campaign, which it has dubbed **Operation WordDrone**, stating it observed the attacks between April and July 2024.

The intrusions are also characterized by the use of a technique called **Blindside** to evade detection endpoint detection and response (EDR) software prior to deploying CLNTEND (aka ClientEndPoint



DARKREADING

'Ancient' MSFT Word Bug Anchors Taiwanese Drone- Maker Attacks

Elizabeth Montalbano, Contributing Writer
September 11, 2024

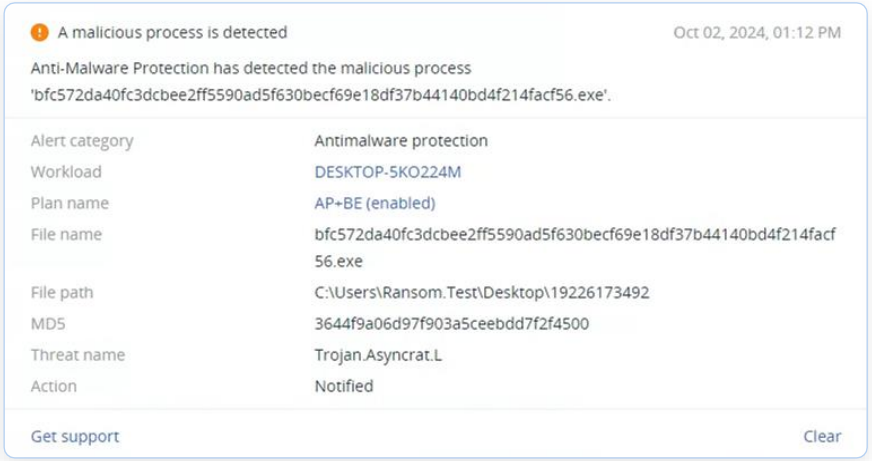
Medium

Why Drone Manufacturers in Taiwan Are Being Cyber-Targeted: A Technologist's Perspective

Dr Mehmet Yildiz (Main) · Follow 425 11
Published in ILLUMINATION · 6 min read · Sep 11, 2024

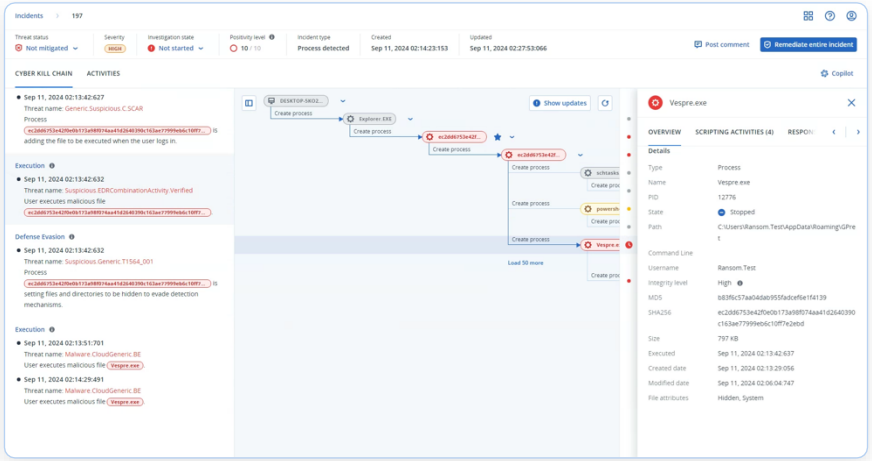
XDR vs APT

Antivirus can detect traditional attacks but lacks context



1. Legacy antivirus cannot reliably block advanced persistent threats
2. Lacks context and proper visualization of complex attack chains
3. Cannot correlate events on the workload or on a wider network

XDR is capable of detecting a lot more and provides visibility and context



1. Capable of blocking traditional malware and advanced persistent threats at the same time.
2. Provides context and appropriate visualization of the entire attack chain
3. XDR can correlate events from multiple sources on the actual workload and on the wider network

Your Trust is Empowering Us!

SE LABS
AAA
SEPTEMBER 2024
ENTERPRISE ADVANCED SECURITY

Acronis

Q&A session

Acronis

Acronis Partner Day at MSP Global 2024

Time to **Go Native.**

Thank you, Ecosystem partners!

MSPGLOBAL | in association with Acronis

Join us in 2025!

Acronis Partner Day at MSP Global

October 20-21 | PortAventura, Spain

Register today:

go.acronis.com/MSPGlobal2025