



Acronis

Acronis Partner Day at MSP Global 2024

Time to Go Native.

Acronis

May I have a (Win)word? A TRU research story



**Nick
Grebennikoff**

Chief Development Officer,
Acronis



**Robert
Neumann**

Head of TRU Labs,
Acronis

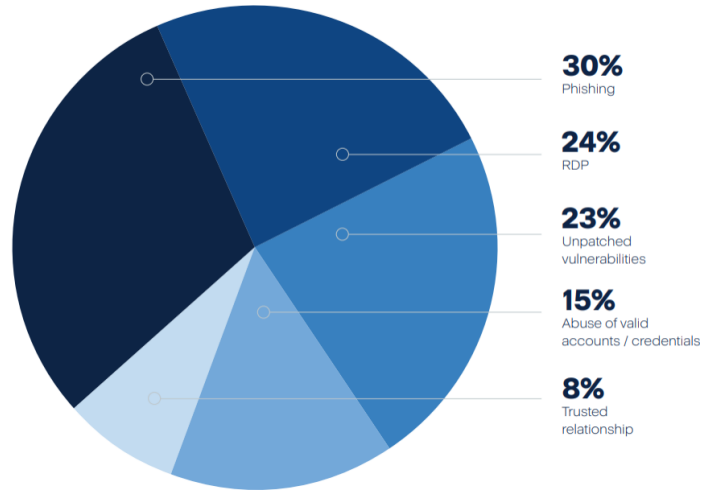
#CyberFit

MSP vs APT?

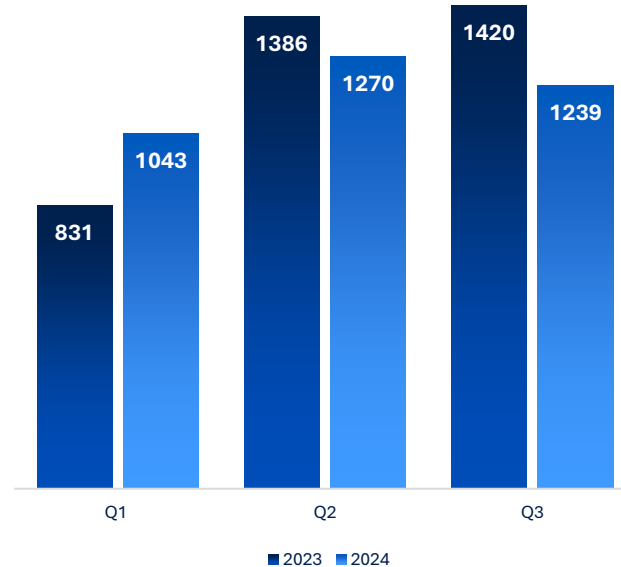


Why Does It Matter?

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

The screenshot displays a security incident response interface. At the top, the incident is identified as 'Incidents' with a count of 441. Key details include: Threat status: Mitigated; Severity: MEDIUM; Investigation state: Not started; Positivity level: 7 / 10; Incident type: Process detected; Created: Jun 21, 2024 11:34:52:099; Updated: Jun 25, 2024 10:50:00:069.

The main section is titled 'CYBER KILL CHAIN' and 'ACTIVITIES'. A legend on the left lists various categories: Workload (1), Process (21), File (28), Network (8835), Involved (8886), Suspicious activity (2), and Incident trigger (1). Below the legend is an 'Attack summary' section with two numbered items:

- 1. Attack techniques and tools used**
The attacker used `'winword.exe'` and `'CMD.EXE'` to execute suspicious activities, including abusing Windows service control manager, checking for Internet connectivity, listing domain accounts, and using non-application layer protocol for communication.
- 2. Potential motivations behind the attack**
The attack appears to be aimed at gaining unauthorized access to sensitive information, compromising network security, and potentially establishing a command and control (C2) server for further malicious activities.

The central part of the interface shows a 'CYBER KILL CHAIN' diagram. A process node for `winword.exe` is highlighted with a red box. A 'Create process' arrow points from `winword.exe` to a node for `CMD.EXE`, which is also highlighted with a red box. From `CMD.EXE`, a series of 'Create process' arrows lead to a chain of processes: `Conhost.exe`, `PING.EXE` (multiple instances), and `net.exe`. The `net.exe` node is also highlighted with a red box.

On the right side, a detailed view for `winword.exe` is shown. It includes an 'OVERVIEW' section with the following details:

- Type: Process
- Name: winword.exe
- PID: 4804
- State: Stopped
- Path: C:\Program Files\Microsoft Office 15\ClientX64
- Command Line: "C:\Program Files\Microsoft Office 15\ClientX64\winword.exe" /SvcLoad
- Username: LocalSystem
- Integrity level: System
- MD5: 15e52f52ed2b8ed122fae897119687c4
- SHA256: 8cfb55087fa8e4c1e7bcc580d767cf2c884c1b8c890ad240c1e7009810af6736
- Size: 1.36 MB
- Executed: Jun 21, 2024 09:36:15:827

Below the overview is a 'Digital signature' section, showing a signature from Microsoft Corporation.

Is Anything Playing Hide and Seek?

On disk

winword.exe

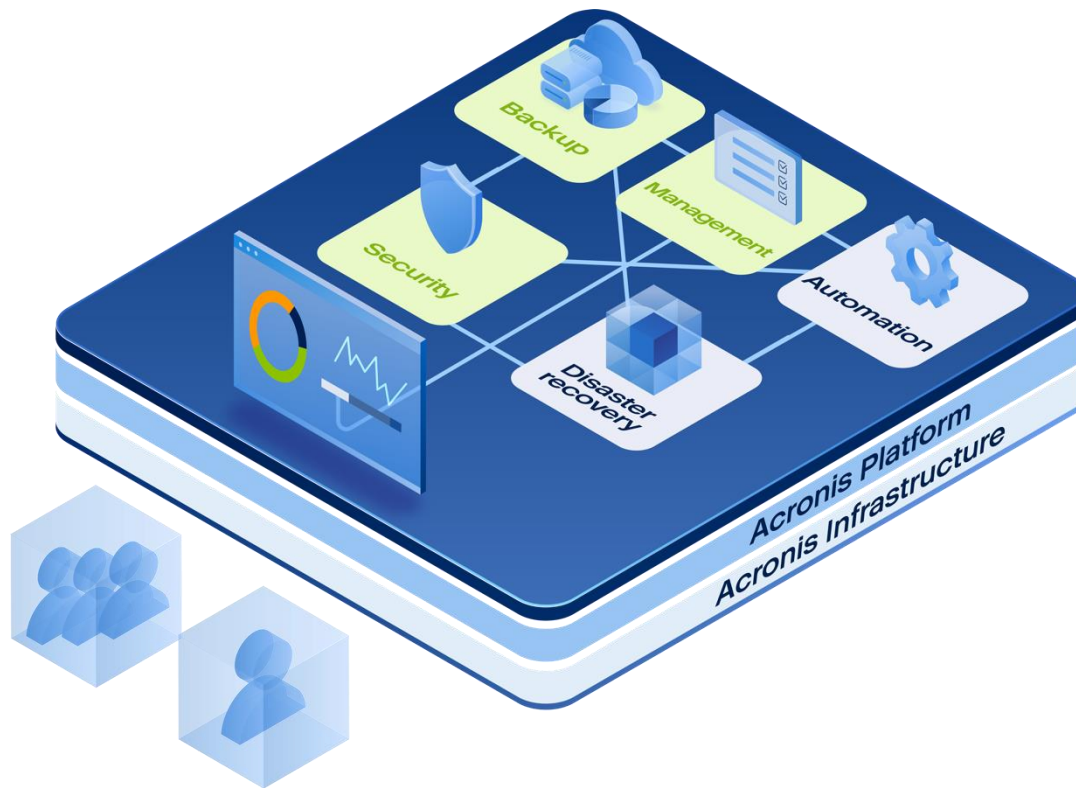


wwlib.dll
(Loader)

random filename and
extension



Deeper Investigation Through a Backup



Are Our Customers Safe?



Is It a World-Wide Attack?

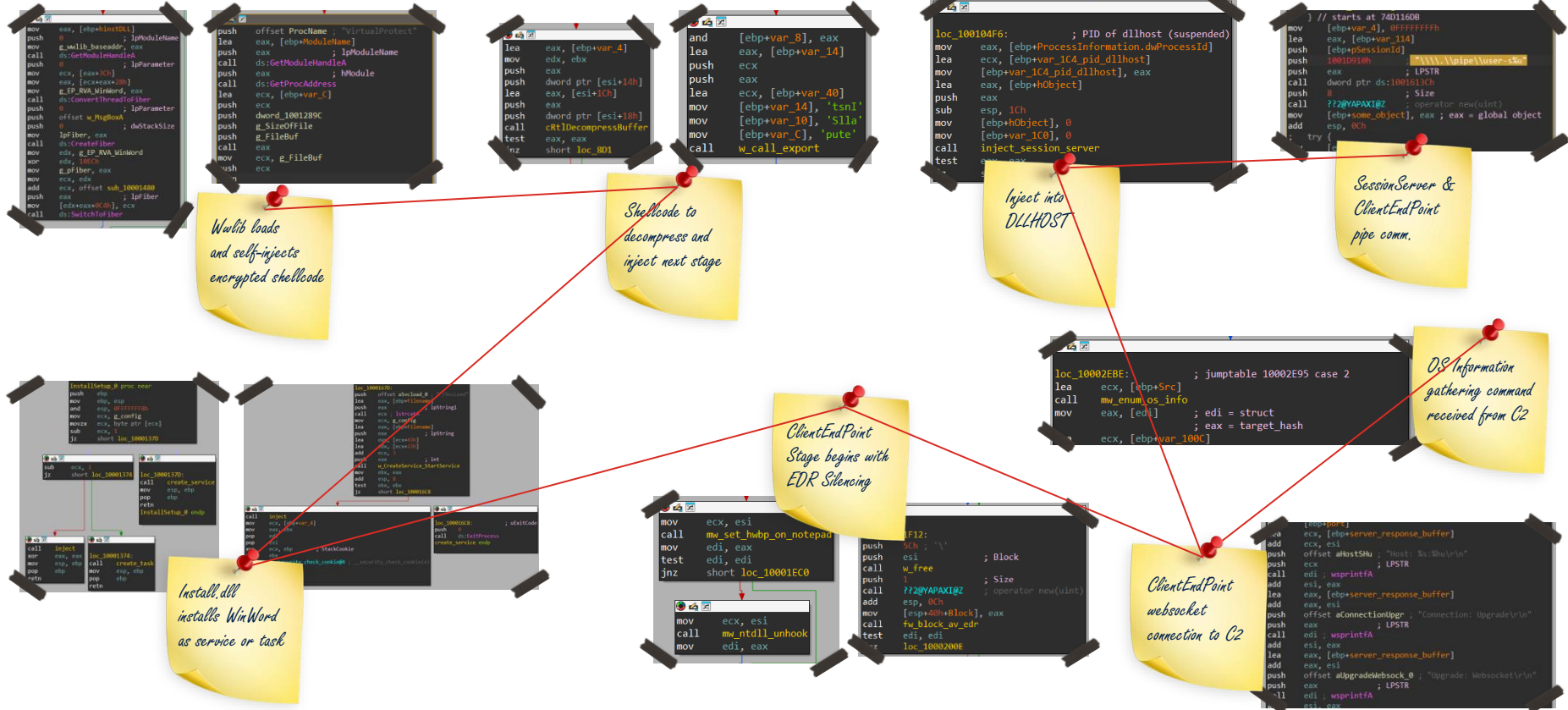




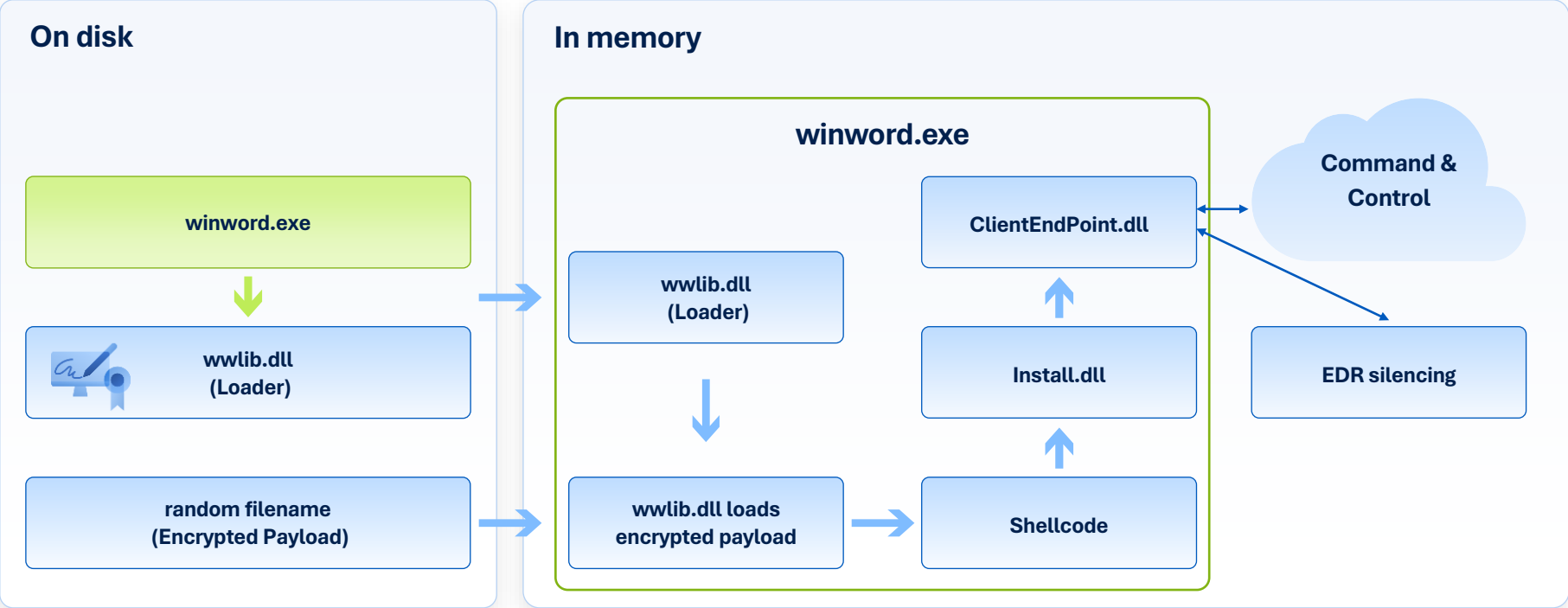
All Virtual Roads Lead to Taiwan



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?

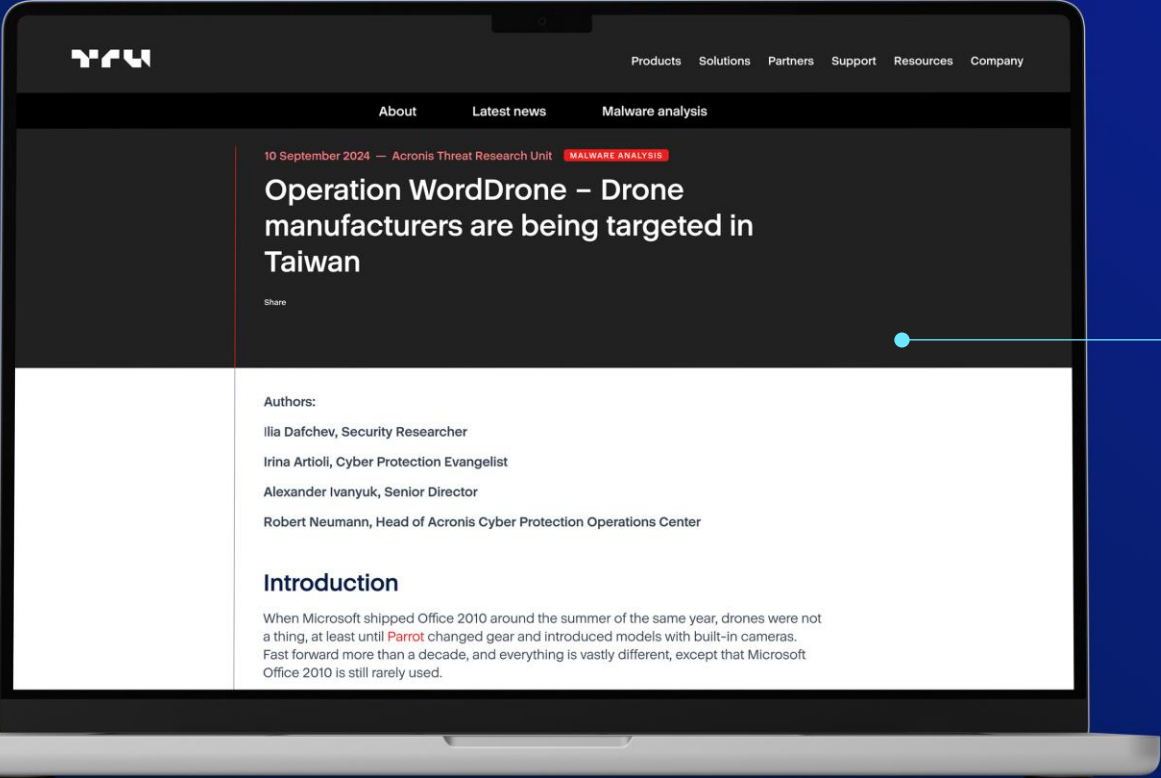
The background image is a blue-tinted photograph of a control room or data center. In the center, a large world map is displayed on a wall, with various data points and lines overlaid. A woman in a white shirt is pointing at the map, and a man in a dark suit is looking at it. In the foreground, several people are seated at desks with multiple computer monitors displaying various data visualizations, including line graphs and bar charts. The overall atmosphere is professional and data-driven.

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 Blindside. 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

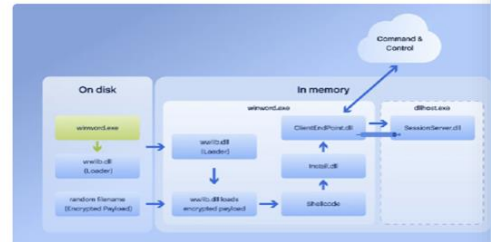
📅 Sep 09, 2024 👤 Ravi Lakshmanan



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 and endpoint detection and response (EDR) software prior to deploying CLINTEND (aka ClientEndPoint.dll).



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

A screenshot of an antivirus alert notification. The alert title is "A malicious process is detected" with a timestamp of "Oct 02, 2024, 01:12 PM". The main text states: "Anti-Malware Protection has detected the malicious process 'bfc572da40fc3dcbee2ff5590ad5f630becf69e18df37b44140bd4f214facf56.exe'." Below this is a table with the following data:

Alert category	Antimalware protection
Workload	DESKTOP-5K0224M
Plan name	AP+BE (enabled)
File name	bfc572da40fc3dcbee2ff5590ad5f630becf69e18df37b44140bd4f214facf56.exe
File path	C:\Users\Ransom.Test\Desktop\19226173492
MD5	3644f9a06d97f903a5ceebdd72f4500
Threat name	Trojan.Asynrcrat.L
Action	Notified

At the bottom left is a "Get support" link and at the bottom right is a "Clear" button.

- 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

A screenshot of an XDR console interface. The top navigation bar shows "Incidents" with a count of 197. Below this is a "CYBER KILL CHAIN" section with a "CYBER KILL CHAIN" tab selected. The main area displays a flowchart of an attack chain. The steps are:

- 1. "Create process" (Generic Suspicious C.SCAR)
- 2. "Execute file" (Generic Suspicious EDRCombinationActivity Verified)
- 3. "Create process" (Trojan.Asynrcrat.L)
- 4. "Execute file" (Trojan.Asynrcrat.L)
- 5. "Create process" (Trojan.Asynrcrat.L)
- 6. "Execute file" (Trojan.Asynrcrat.L)
- 7. "Create process" (Trojan.Asynrcrat.L)
- 8. "Execute file" (Trojan.Asynrcrat.L)
- 9. "Create process" (Trojan.Asynrcrat.L)
- 10. "Execute file" (Trojan.Asynrcrat.L)
- 11. "Create process" (Trojan.Asynrcrat.L)
- 12. "Execute file" (Trojan.Asynrcrat.L)
- 13. "Create process" (Trojan.Asynrcrat.L)
- 14. "Execute file" (Trojan.Asynrcrat.L)
- 15. "Create process" (Trojan.Asynrcrat.L)
- 16. "Execute file" (Trojan.Asynrcrat.L)
- 17. "Create process" (Trojan.Asynrcrat.L)
- 18. "Execute file" (Trojan.Asynrcrat.L)
- 19. "Create process" (Trojan.Asynrcrat.L)
- 20. "Execute file" (Trojan.Asynrcrat.L)
- 21. "Create process" (Trojan.Asynrcrat.L)
- 22. "Execute file" (Trojan.Asynrcrat.L)
- 23. "Create process" (Trojan.Asynrcrat.L)
- 24. "Execute file" (Trojan.Asynrcrat.L)
- 25. "Create process" (Trojan.Asynrcrat.L)
- 26. "Execute file" (Trojan.Asynrcrat.L)
- 27. "Create process" (Trojan.Asynrcrat.L)
- 28. "Execute file" (Trojan.Asynrcrat.L)
- 29. "Create process" (Trojan.Asynrcrat.L)
- 30. "Execute file" (Trojan.Asynrcrat.L)
- 31. "Create process" (Trojan.Asynrcrat.L)
- 32. "Execute file" (Trojan.Asynrcrat.L)
- 33. "Create process" (Trojan.Asynrcrat.L)
- 34. "Execute file" (Trojan.Asynrcrat.L)
- 35. "Create process" (Trojan.Asynrcrat.L)
- 36. "Execute file" (Trojan.Asynrcrat.L)
- 37. "Create process" (Trojan.Asynrcrat.L)
- 38. "Execute file" (Trojan.Asynrcrat.L)
- 39. "Create process" (Trojan.Asynrcrat.L)
- 40. "Execute file" (Trojan.Asynrcrat.L)
- 41. "Create process" (Trojan.Asynrcrat.L)
- 42. "Execute file" (Trojan.Asynrcrat.L)
- 43. "Create process" (Trojan.Asynrcrat.L)
- 44. "Execute file" (Trojan.Asynrcrat.L)
- 45. "Create process" (Trojan.Asynrcrat.L)
- 46. "Execute file" (Trojan.Asynrcrat.L)
- 47. "Create process" (Trojan.Asynrcrat.L)
- 48. "Execute file" (Trojan.Asynrcrat.L)
- 49. "Create process" (Trojan.Asynrcrat.L)
- 50. "Execute file" (Trojan.Asynrcrat.L)
- 51. "Create process" (Trojan.Asynrcrat.L)
- 52. "Execute file" (Trojan.Asynrcrat.L)
- 53. "Create process" (Trojan.Asynrcrat.L)
- 54. "Execute file" (Trojan.Asynrcrat.L)
- 55. "Create process" (Trojan.Asynrcrat.L)
- 56. "Execute file" (Trojan.Asynrcrat.L)
- 57. "Create process" (Trojan.Asynrcrat.L)
- 58. "Execute file" (Trojan.Asynrcrat.L)
- 59. "Create process" (Trojan.Asynrcrat.L)
- 60. "Execute file" (Trojan.Asynrcrat.L)
- 61. "Create process" (Trojan.Asynrcrat.L)
- 62. "Execute file" (Trojan.Asynrcrat.L)
- 63. "Create process" (Trojan.Asynrcrat.L)
- 64. "Execute file" (Trojan.Asynrcrat.L)
- 65. "Create process" (Trojan.Asynrcrat.L)
- 66. "Execute file" (Trojan.Asynrcrat.L)
- 67. "Create process" (Trojan.Asynrcrat.L)
- 68. "Execute file" (Trojan.Asynrcrat.L)
- 69. "Create process" (Trojan.Asynrcrat.L)
- 70. "Execute file" (Trojan.Asynrcrat.L)
- 71. "Create process" (Trojan.Asynrcrat.L)
- 72. "Execute file" (Trojan.Asynrcrat.L)
- 73. "Create process" (Trojan.Asynrcrat.L)
- 74. "Execute file" (Trojan.Asynrcrat.L)
- 75. "Create process" (Trojan.Asynrcrat.L)
- 76. "Execute file" (Trojan.Asynrcrat.L)
- 77. "Create process" (Trojan.Asynrcrat.L)
- 78. "Execute file" (Trojan.Asynrcrat.L)
- 79. "Create process" (Trojan.Asynrcrat.L)
- 80. "Execute file" (Trojan.Asynrcrat.L)
- 81. "Create process" (Trojan.Asynrcrat.L)
- 82. "Execute file" (Trojan.Asynrcrat.L)
- 83. "Create process" (Trojan.Asynrcrat.L)
- 84. "Execute file" (Trojan.Asynrcrat.L)
- 85. "Create process" (Trojan.Asynrcrat.L)
- 86. "Execute file" (Trojan.Asynrcrat.L)
- 87. "Create process" (Trojan.Asynrcrat.L)
- 88. "Execute file" (Trojan.Asynrcrat.L)
- 89. "Create process" (Trojan.Asynrcrat.L)
- 90. "Execute file" (Trojan.Asynrcrat.L)
- 91. "Create process" (Trojan.Asynrcrat.L)
- 92. "Execute file" (Trojan.Asynrcrat.L)
- 93. "Create process" (Trojan.Asynrcrat.L)
- 94. "Execute file" (Trojan.Asynrcrat.L)
- 95. "Create process" (Trojan.Asynrcrat.L)
- 96. "Execute file" (Trojan.Asynrcrat.L)
- 97. "Create process" (Trojan.Asynrcrat.L)
- 98. "Execute file" (Trojan.Asynrcrat.L)
- 99. "Create process" (Trojan.Asynrcrat.L)
- 100. "Execute file" (Trojan.Asynrcrat.L)
- 101. "Create process" (Trojan.Asynrcrat.L)
- 102. "Execute file" (Trojan.Asynrcrat.L)
- 103. "Create process" (Trojan.Asynrcrat.L)
- 104. "Execute file" (Trojan.Asynrcrat.L)
- 105. "Create process" (Trojan.Asynrcrat.L)
- 106. "Execute file" (Trojan.Asynrcrat.L)
- 107. "Create process" (Trojan.Asynrcrat.L)
- 108. "Execute file" (Trojan.Asynrcrat.L)
- 109. "Create process" (Trojan.Asynrcrat.L)
- 110. "Execute file" (Trojan.Asynrcrat.L)
- 111. "Create process" (Trojan.Asynrcrat.L)
- 112. "Execute file" (Trojan.Asynrcrat.L)
- 113. "Create process" (Trojan.Asynrcrat.L)
- 114. "Execute file" (Trojan.Asynrcrat.L)
- 115. "Create process" (Trojan.Asynrcrat.L)
- 116. "Execute file" (Trojan.Asynrcrat.L)
- 117. "Create process" (Trojan.Asynrcrat.L)
- 118. "Execute file" (Trojan.Asynrcrat.L)
- 119. "Create process" (Trojan.Asynrcrat.L)
- 120. "Execute file" (Trojan.Asynrcrat.L)
- 121. "Create process" (Trojan.Asynrcrat.L)
- 122. "Execute file" (Trojan.Asynrcrat.L)
- 123. "Create process" (Trojan.Asynrcrat.L)
- 124. "Execute file" (Trojan.Asynrcrat.L)
- 125. "Create process" (Trojan.Asynrcrat.L)
- 126. "Execute file" (Trojan.Asynrcrat.L)
- 127. "Create process" (Trojan.Asynrcrat.L)
- 128. "Execute file" (Trojan.Asynrcrat.L)
- 129. "Create process" (Trojan.Asynrcrat.L)
- 130. "Execute file" (Trojan.Asynrcrat.L)
- 131. "Create process" (Trojan.Asynrcrat.L)
- 132. "Execute file" (Trojan.Asynrcrat.L)
- 133. "Create process" (Trojan.Asynrcrat.L)
- 134. "Execute file" (Trojan.Asynrcrat.L)
- 135. "Create process" (Trojan.Asynrcrat.L)
- 136. "Execute file" (Trojan.Asynrcrat.L)
- 137. "Create process" (Trojan.Asynrcrat.L)
- 138. "Execute file" (Trojan.Asynrcrat.L)
- 139. "Create process" (Trojan.Asynrcrat.L)
- 140. "Execute file" (Trojan.Asynrcrat.L)
- 141. "Create process" (Trojan.Asynrcrat.L)
- 142. "Execute file" (Trojan.Asynrcrat.L)
- 143. "Create process" (Trojan.Asynrcrat.L)
- 144. "Execute file" (Trojan.Asynrcrat.L)
- 145. "Create process" (Trojan.Asynrcrat.L)
- 146. "Execute file" (Trojan.Asynrcrat.L)
- 147. "Create process" (Trojan.Asynrcrat.L)
- 148. "Execute file" (Trojan.Asynrcrat.L)
- 149. "Create process" (Trojan.Asynrcrat.L)
- 150. "Execute file" (Trojan.Asynrcrat.L)
- 151. "Create process" (Trojan.Asynrcrat.L)
- 152. "Execute file" (Trojan.Asynrcrat.L)
- 153. "Create process" (Trojan.Asynrcrat.L)
- 154. "Execute file" (Trojan.Asynrcrat.L)
- 155. "Create process" (Trojan.Asynrcrat.L)
- 156. "Execute file" (Trojan.Asynrcrat.L)
- 157. "Create process" (Trojan.Asynrcrat.L)
- 158. "Execute file" (Trojan.Asynrcrat.L)
- 159. "Create process" (Trojan.Asynrcrat.L)
- 160. "Execute file" (Trojan.Asynrcrat.L)
- 161. "Create process" (Trojan.Asynrcrat.L)
- 162. "Execute file" (Trojan.Asynrcrat.L)
- 163. "Create process" (Trojan.Asynrcrat.L)
- 164. "Execute file" (Trojan.Asynrcrat.L)
- 165. "Create process" (Trojan.Asynrcrat.L)
- 166. "Execute file" (Trojan.Asynrcrat.L)
- 167. "Create process" (Trojan.Asynrcrat.L)
- 168. "Execute file" (Trojan.Asynrcrat.L)
- 169. "Create process" (Trojan.Asynrcrat.L)
- 170. "Execute file" (Trojan.Asynrcrat.L)
- 171. "Create process" (Trojan.Asynrcrat.L)
- 172. "Execute file" (Trojan.Asynrcrat.L)
- 173. "Create process" (Trojan.Asynrcrat.L)
- 174. "Execute file" (Trojan.Asynrcrat.L)
- 175. "Create process" (Trojan.Asynrcrat.L)
- 176. "Execute file" (Trojan.Asynrcrat.L)
- 177. "Create process" (Trojan.Asynrcrat.L)
- 178. "Execute file" (Trojan.Asynrcrat.L)
- 179. "Create process" (Trojan.Asynrcrat.L)
- 180. "Execute file" (Trojan.Asynrcrat.L)
- 181. "Create process" (Trojan.Asynrcrat.L)
- 182. "Execute file" (Trojan.Asynrcrat.L)
- 183. "Create process" (Trojan.Asynrcrat.L)
- 184. "Execute file" (Trojan.Asynrcrat.L)
- 185. "Create process" (Trojan.Asynrcrat.L)
- 186. "Execute file" (Trojan.Asynrcrat.L)
- 187. "Create process" (Trojan.Asynrcrat.L)
- 188. "Execute file" (Trojan.Asynrcrat.L)
- 189. "Create process" (Trojan.Asynrcrat.L)
- 190. "Execute file" (Trojan.Asynrcrat.L)
- 191. "Create process" (Trojan.Asynrcrat.L)
- 192. "Execute file" (Trojan.Asynrcrat.L)
- 193. "Create process" (Trojan.Asynrcrat.L)
- 194. "Execute file" (Trojan.Asynrcrat.L)
- 195. "Create process" (Trojan.Asynrcrat.L)
- 196. "Execute file" (Trojan.Asynrcrat.L)
- 197. "Create process" (Trojan.Asynrcrat.L)
- 198. "Execute file" (Trojan.Asynrcrat.L)
- 199. "Create process" (Trojan.Asynrcrat.L)
- 200. "Execute file" (Trojan.Asynrcrat.L)

The right sidebar shows details for the "Vespre.exe" process, including its name, PID, state, path, command line, username, integrity level, MD5, SHA256, size, executed date, created date, modified date, and file attributes.

- 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
Threat Research
Unit



Acronis

Q&A session



Acronis

Acronis Partner Day at MSP Global 2024

Time to Go Native.

Thank you, Ecosystem partners!





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

