Kaspersky Industrial Cybersecurity Conference 2024

# OT Cybersecurity: statistics and how to treat it

A Practical Approach to the Industrial Threat Landscape

kaspersky

Kaspersky Industrial Cybersecurity Conference 2024

# Vladimir Dashchenko

Principal Security Researcher
Kaspersky ICS CERT

kaspersky

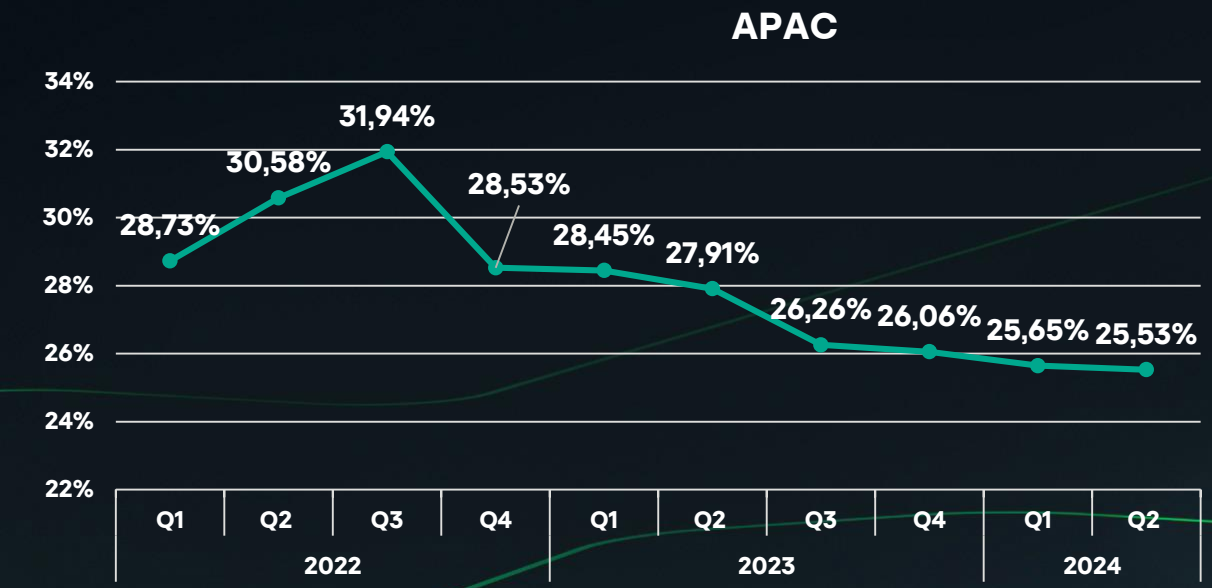
> I keep my eyes wide open. Because trouble is out there....

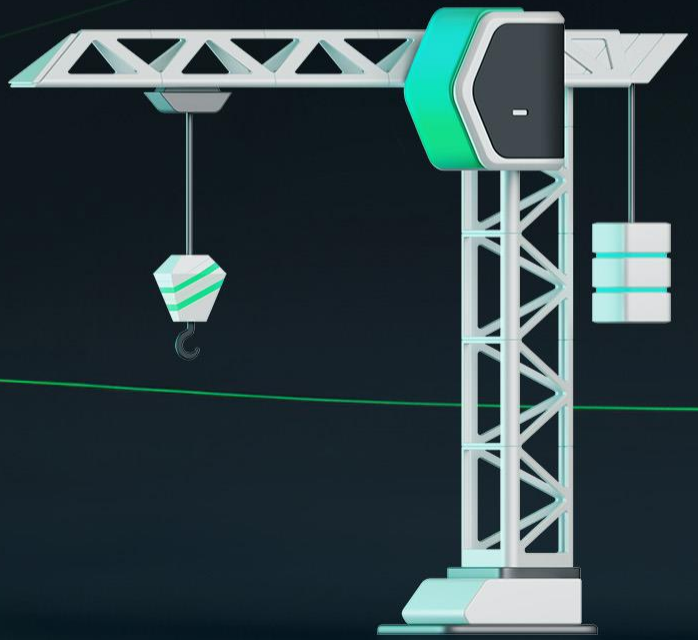
LaDainian Tomlinson

We have

- 160 countries
- 10 major industries
- 4 threat sources
- 10 threat types

Not that we needed all that for the **ICS Threat landscape**, but once you get into a serious statistics, the tendency is to push it as far as you can

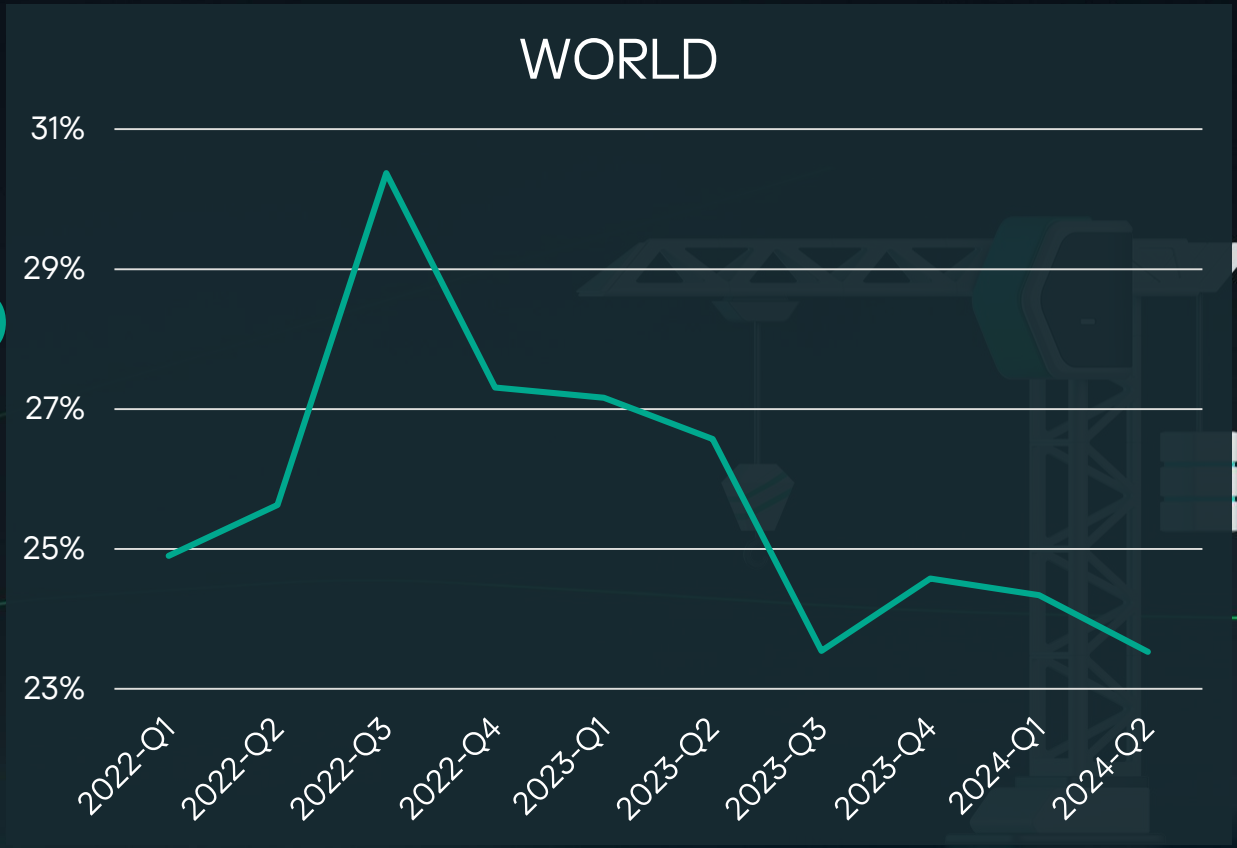

APAC
34%
32%
30%
28%
26%
24%
22%
28,73%
30,58%
31,94%
28,53%
28,45%
27,91%
26,26%
26,06%
25,65%
25,53%
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
Q1
Q2
2022
2023
2024



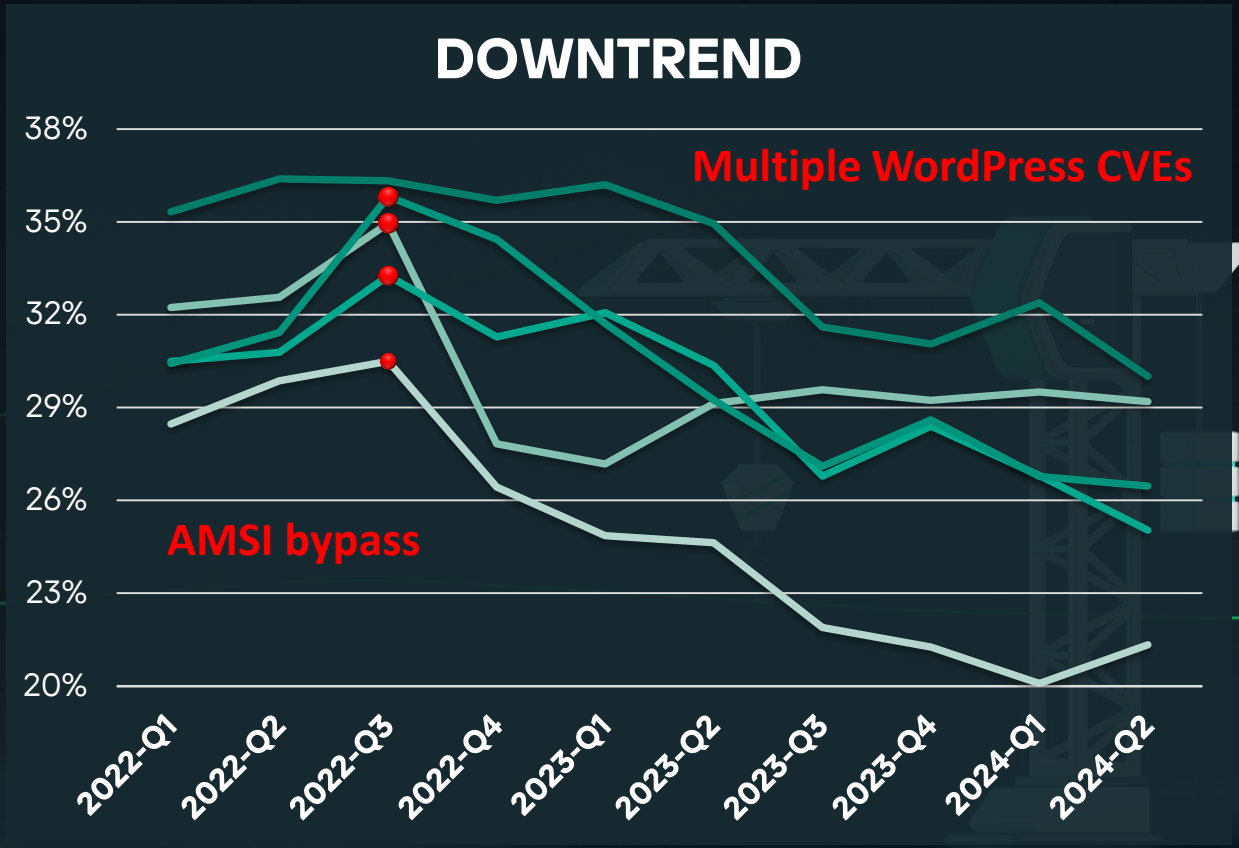
# ICS Threat statistics shows DOWNTREND

...

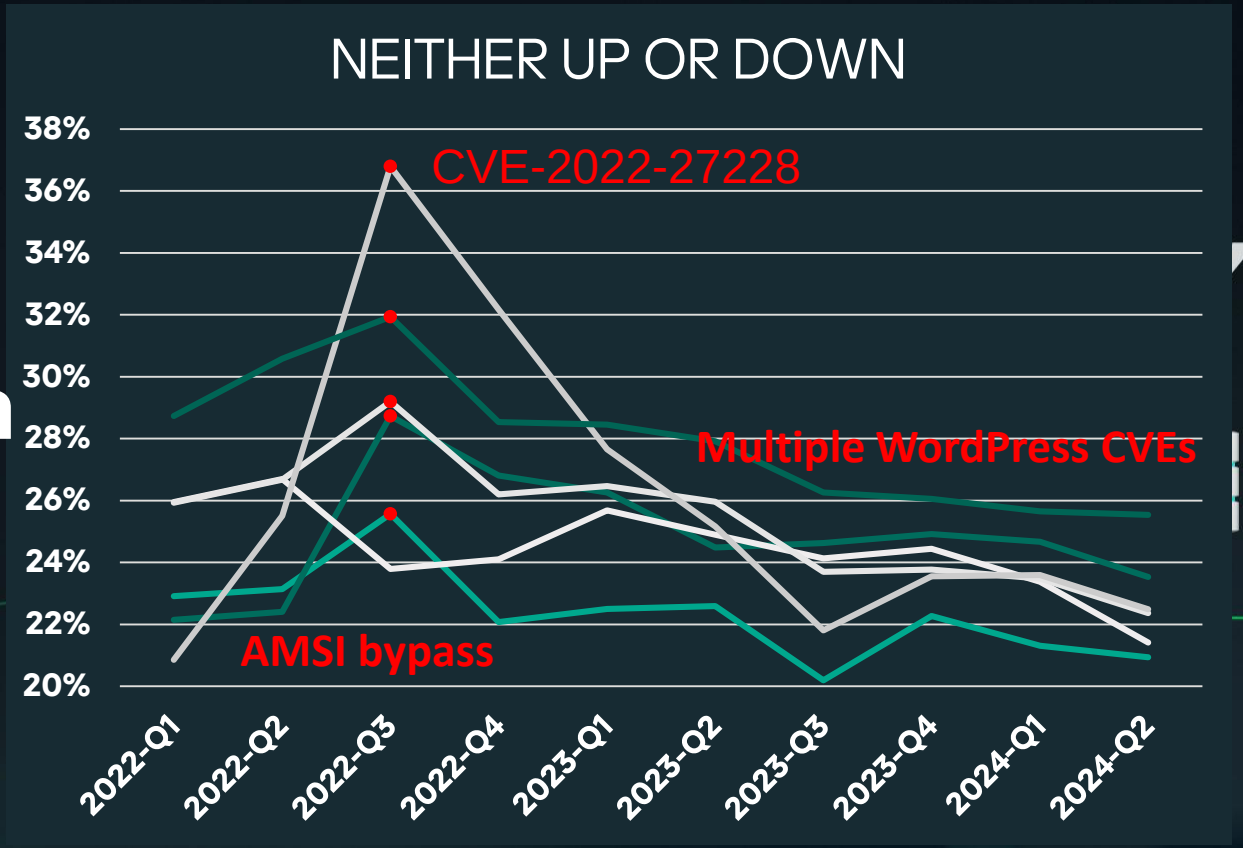
...AND



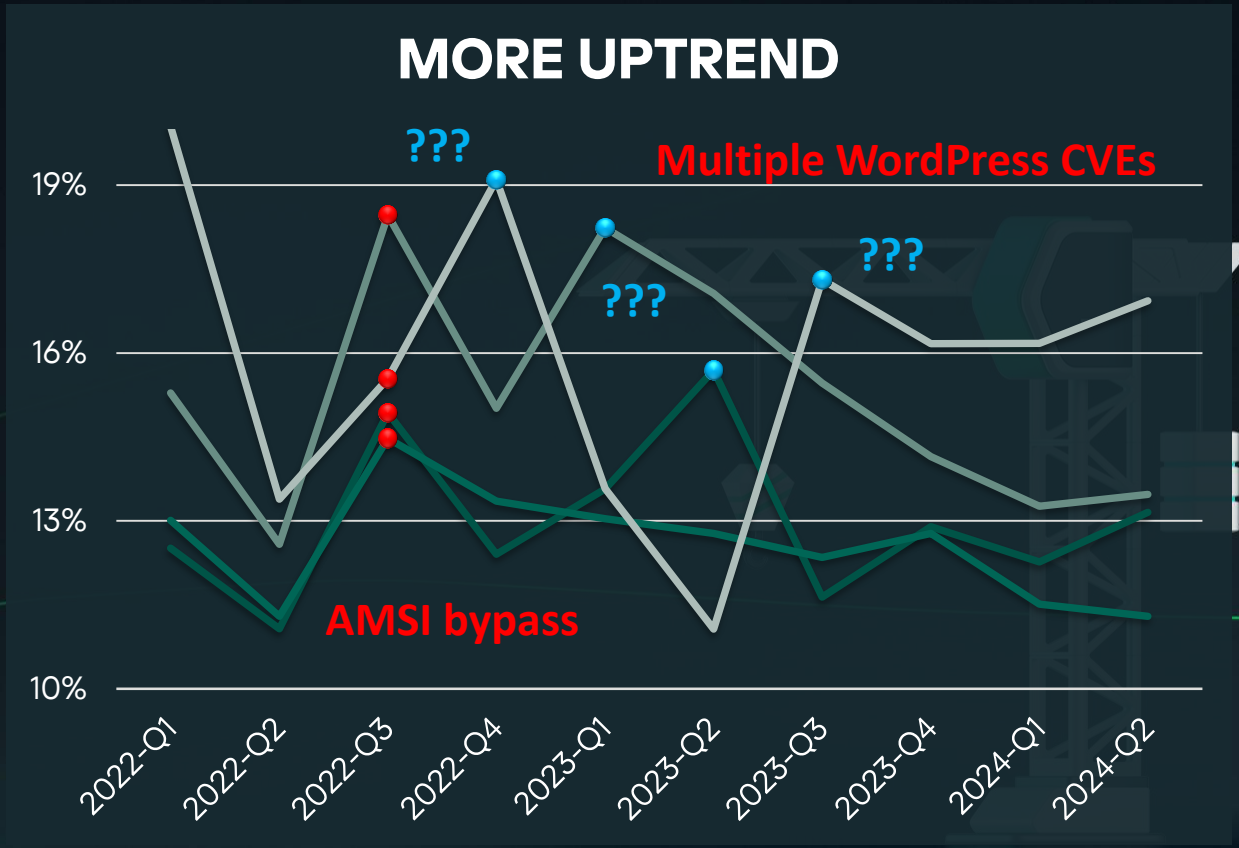
# Eastern Asia
# South-East Asia
# Middle East
# Central Asia
# Africa



# Russia
# Southern EU
# Eastern EU
# Southern Asia
# Latin America
# APAC



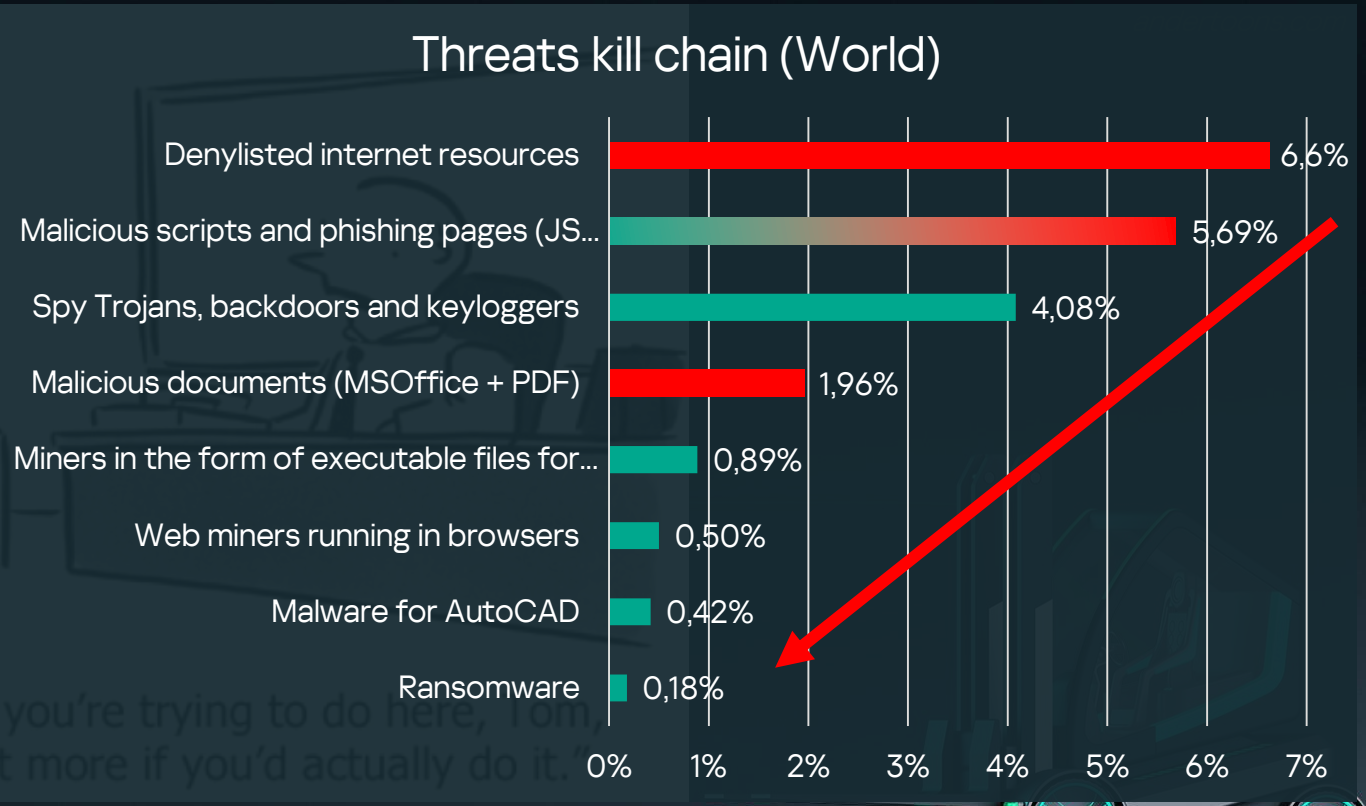
# Western EU
# Northern EU
# USA &
# Canada
# Australia &
# New Zealand




We don’t use WordPress in our OT network...

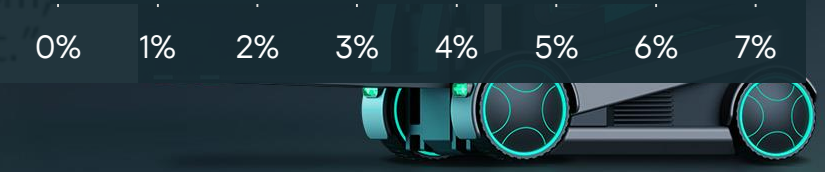
# It’s time to make your eyes wide open

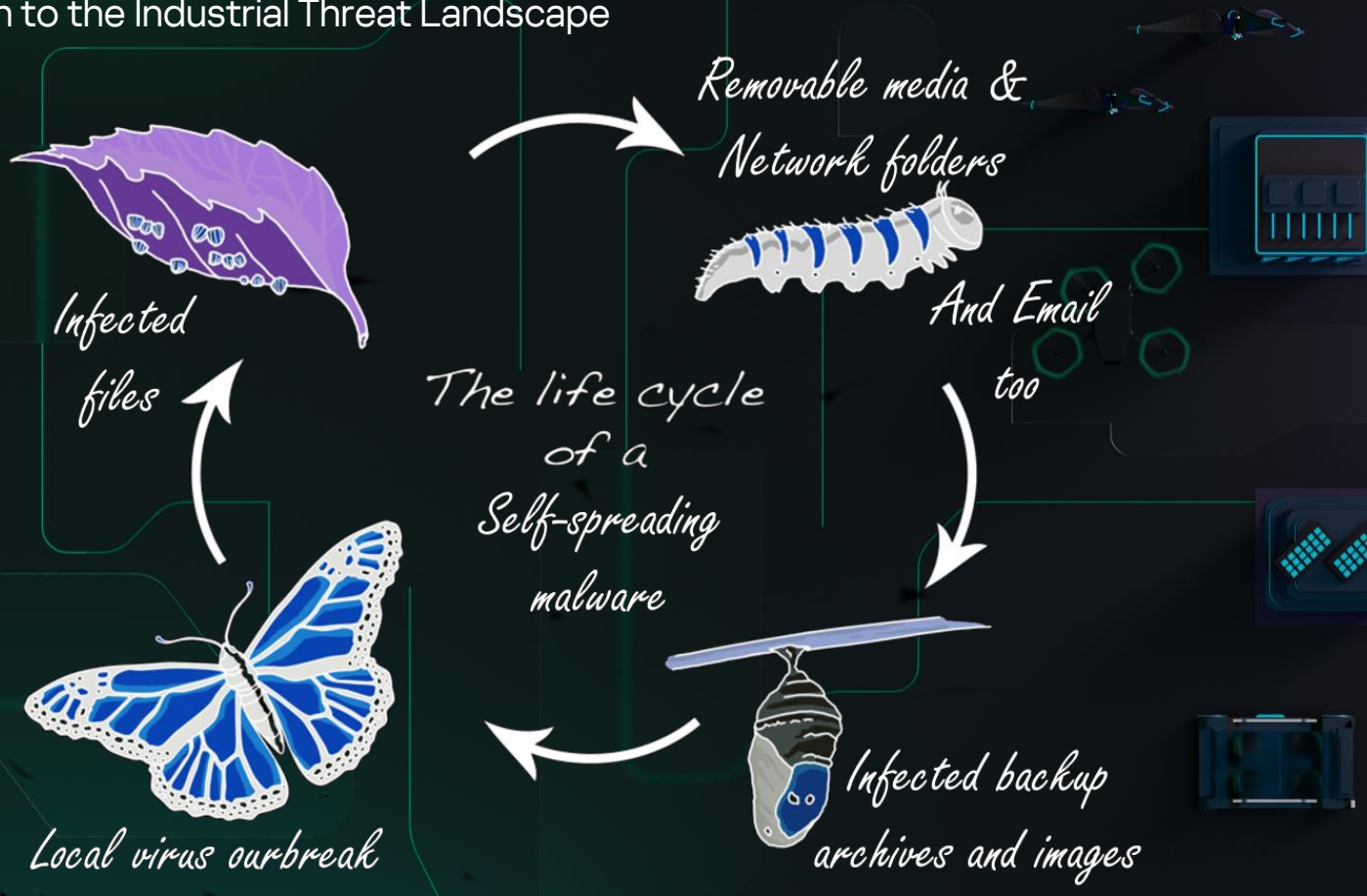



## Threats kill chain (World)

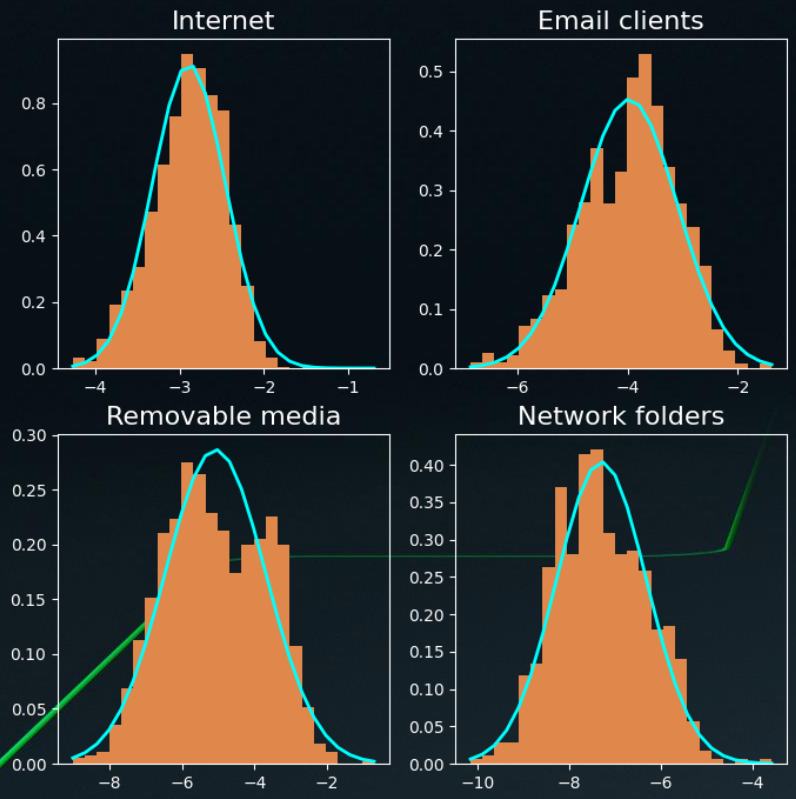
ics-cert@kaspersky.com

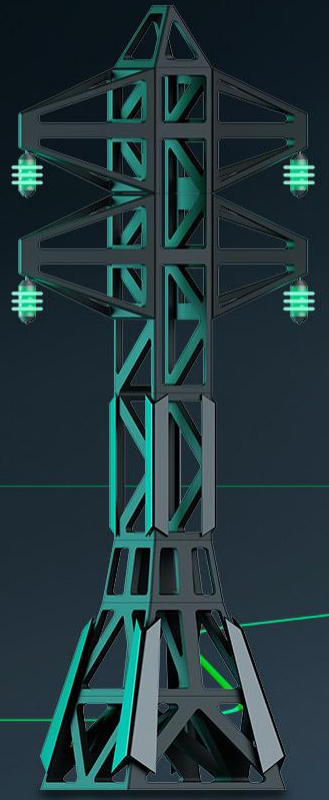



Removable media &
Network folders
And Email
too
Infected backup
archives and images
Local virus ourbreak
Infected
files
The life cycle
of a
Self-spreading
malware

# Normal distribution

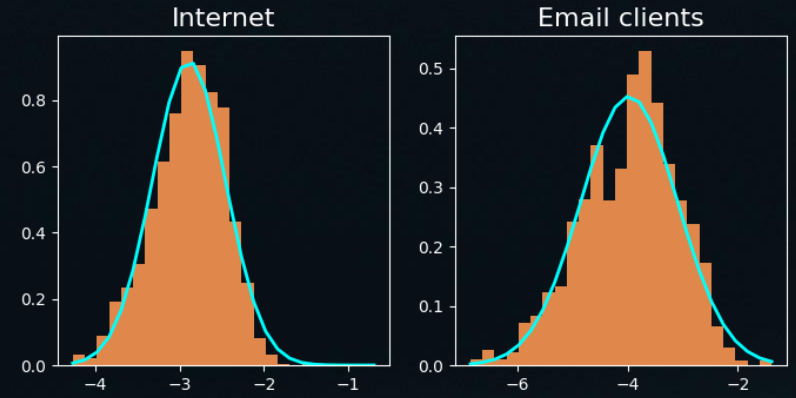




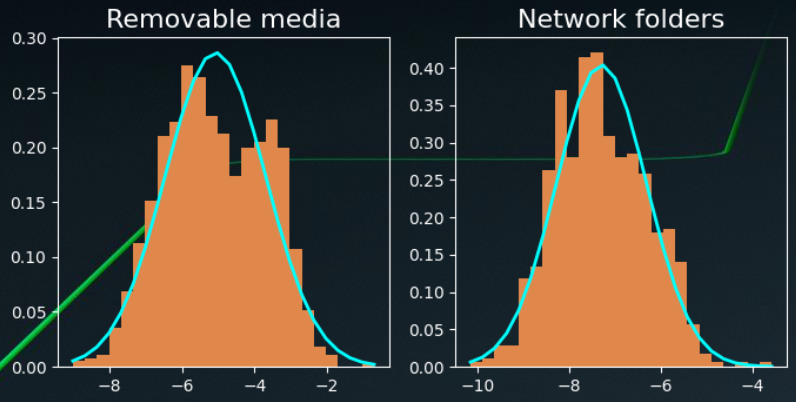
# Normal distribution





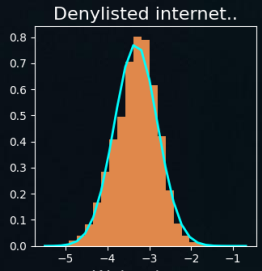


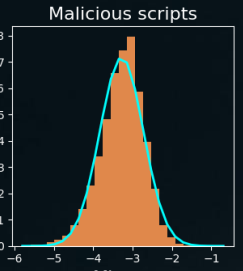


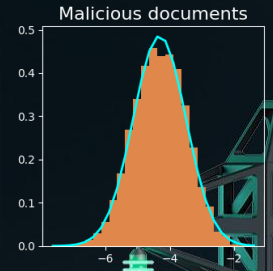


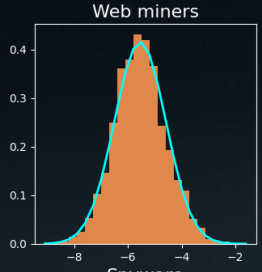


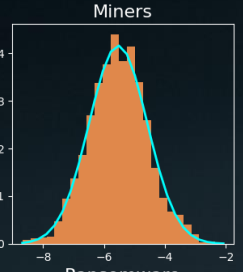


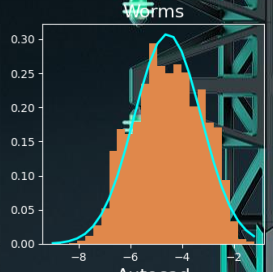


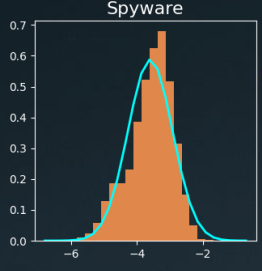



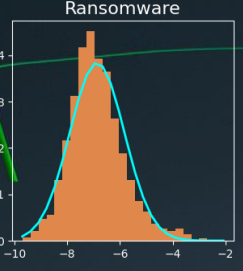



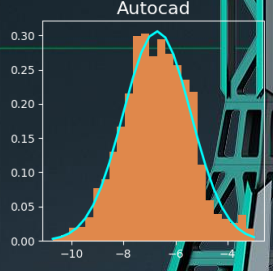



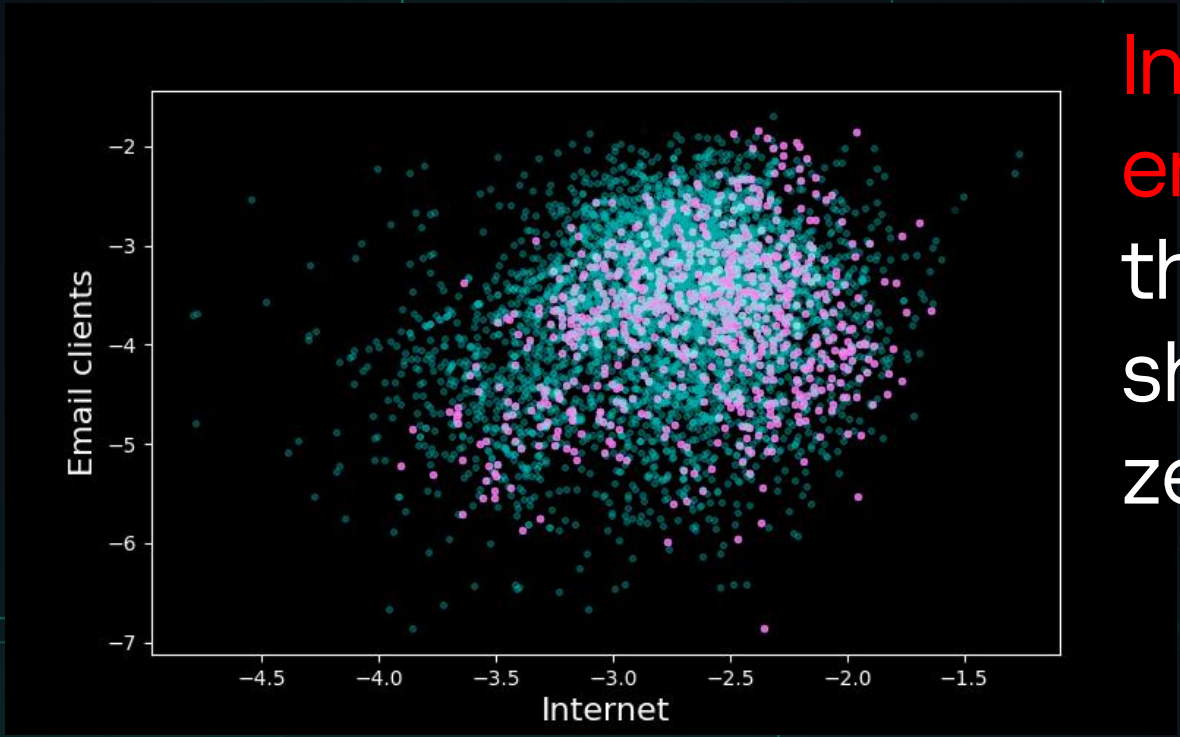



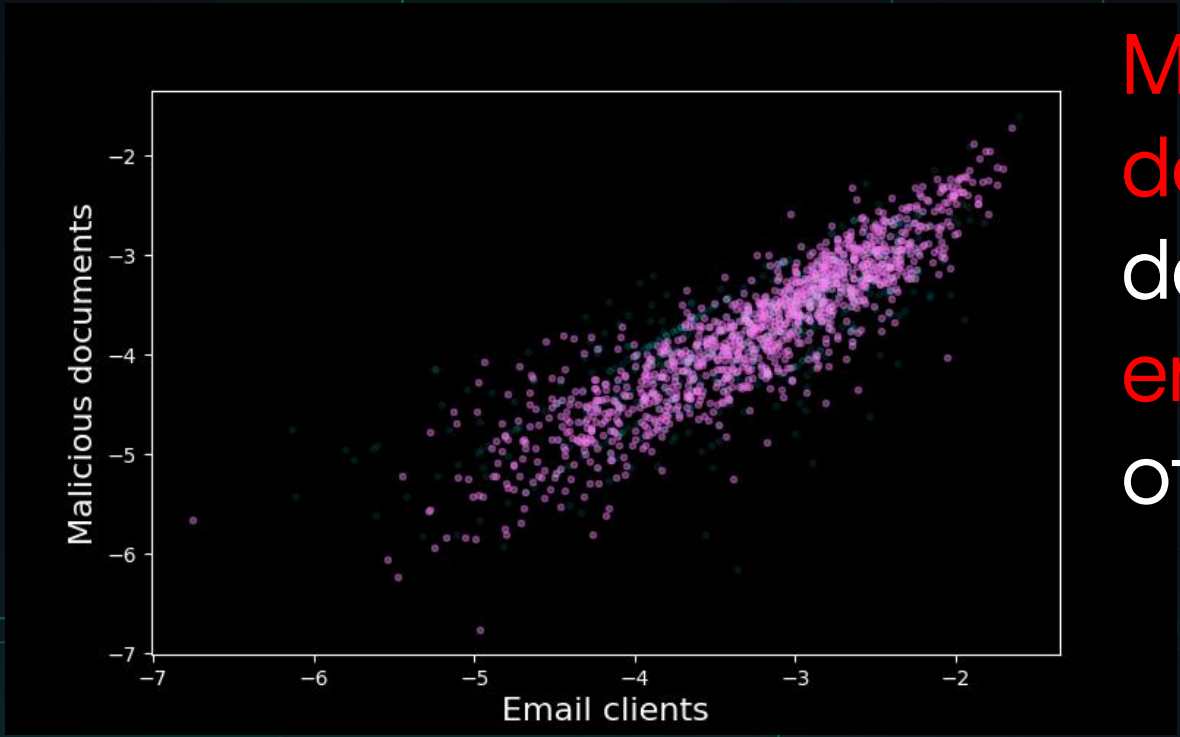



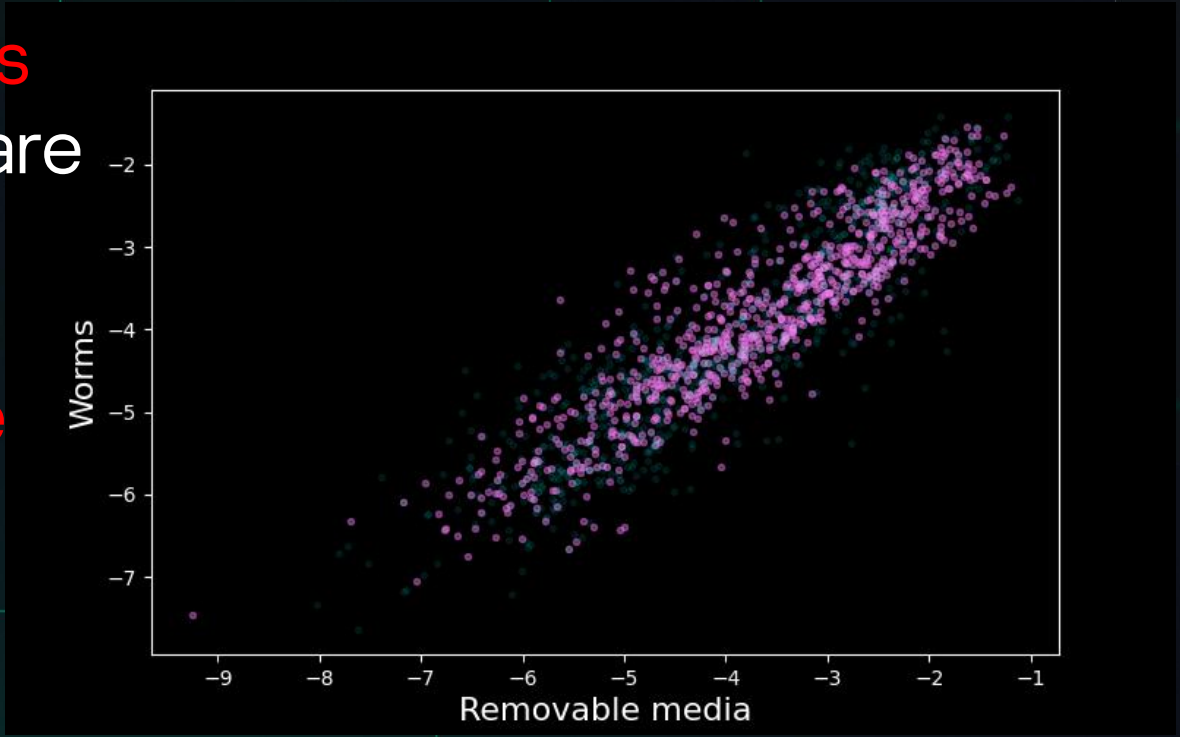



Internet and email clients threat sources shows almost zero correlation

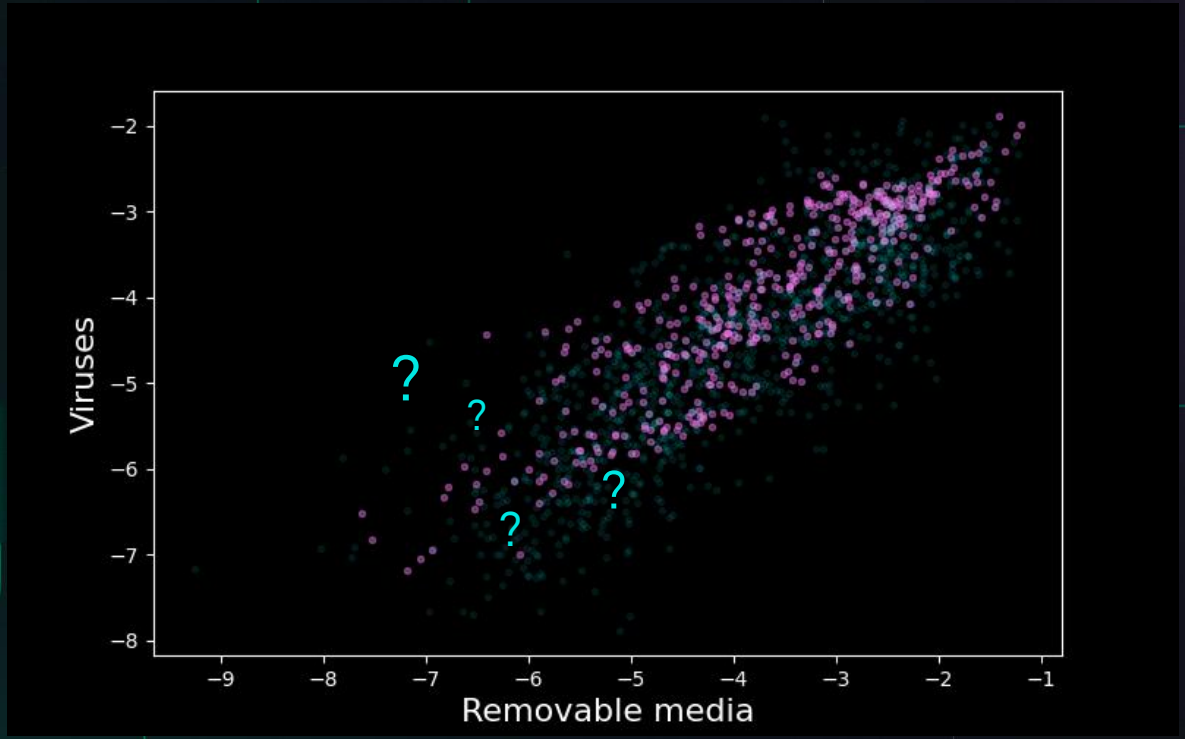



Malicious documents are delivered via email clients, of course ;)

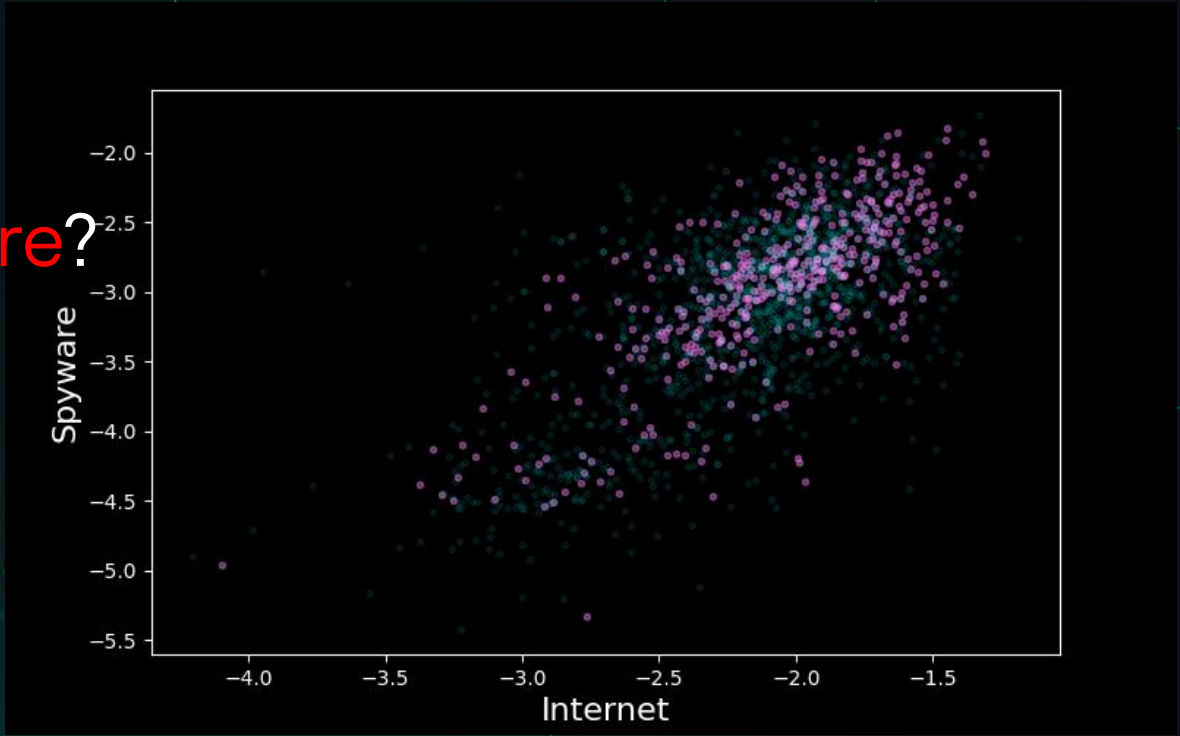
# And worms (for sure) are delivered via removable media



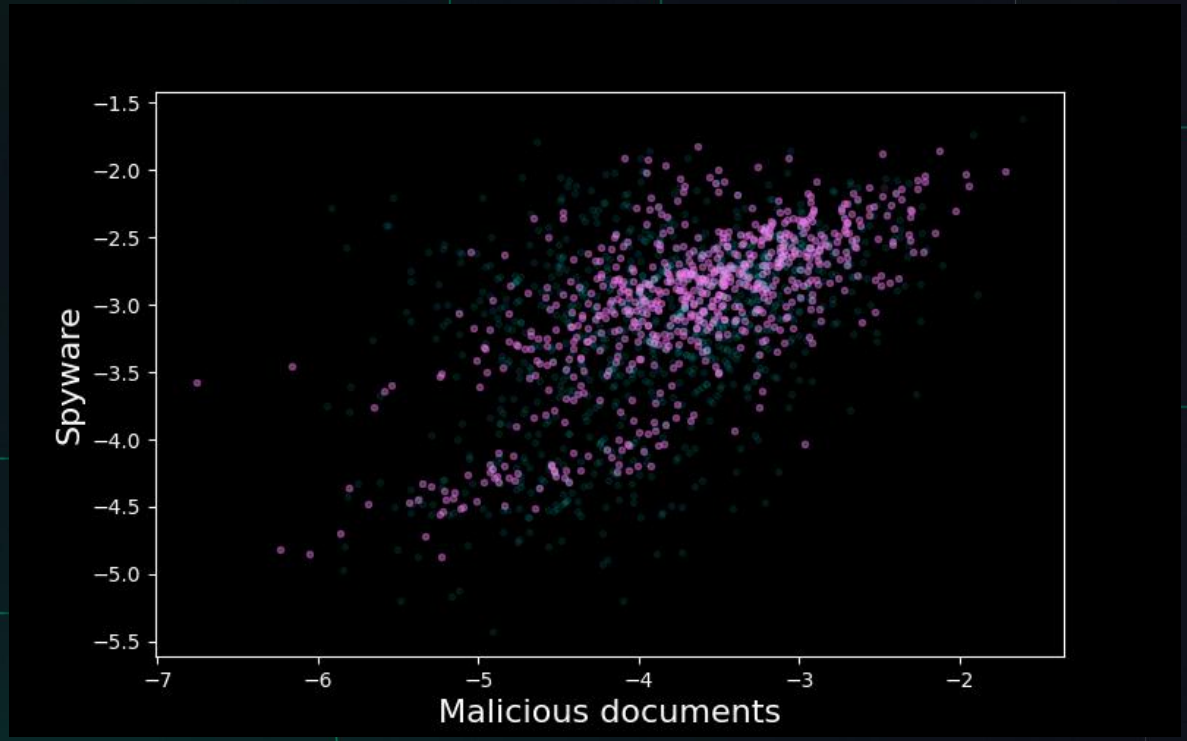
As well as viruses are delivered via removable media?



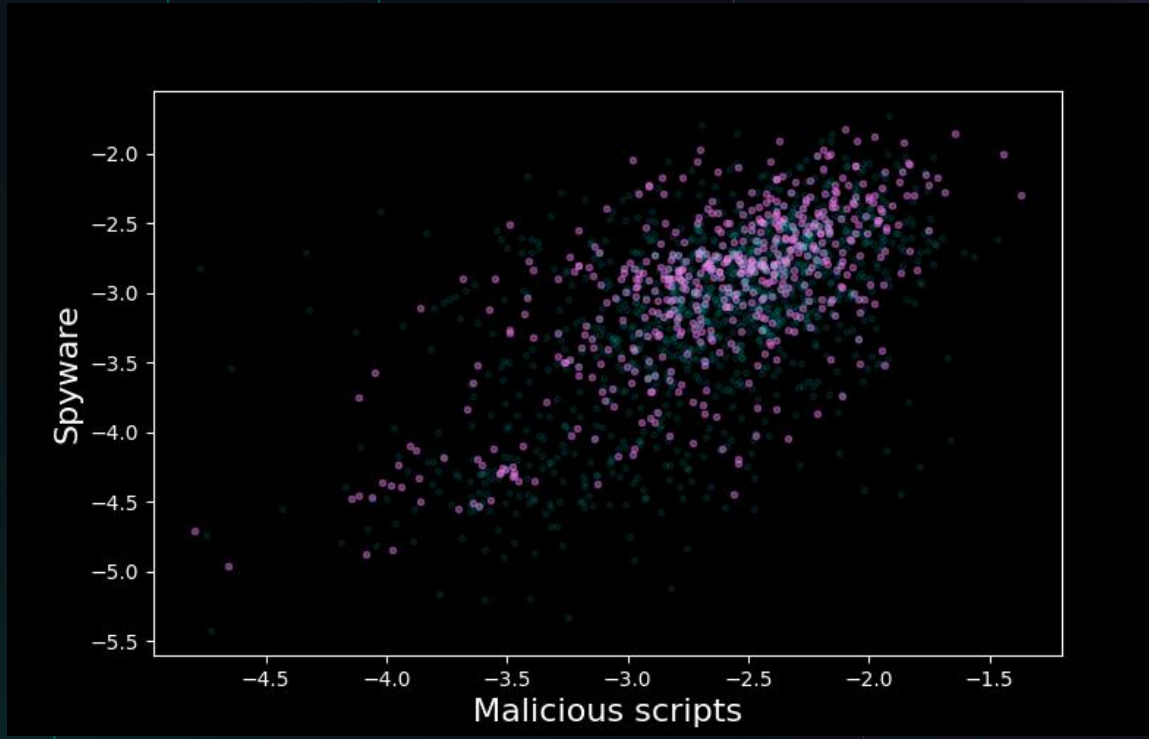
# How about Spyware?



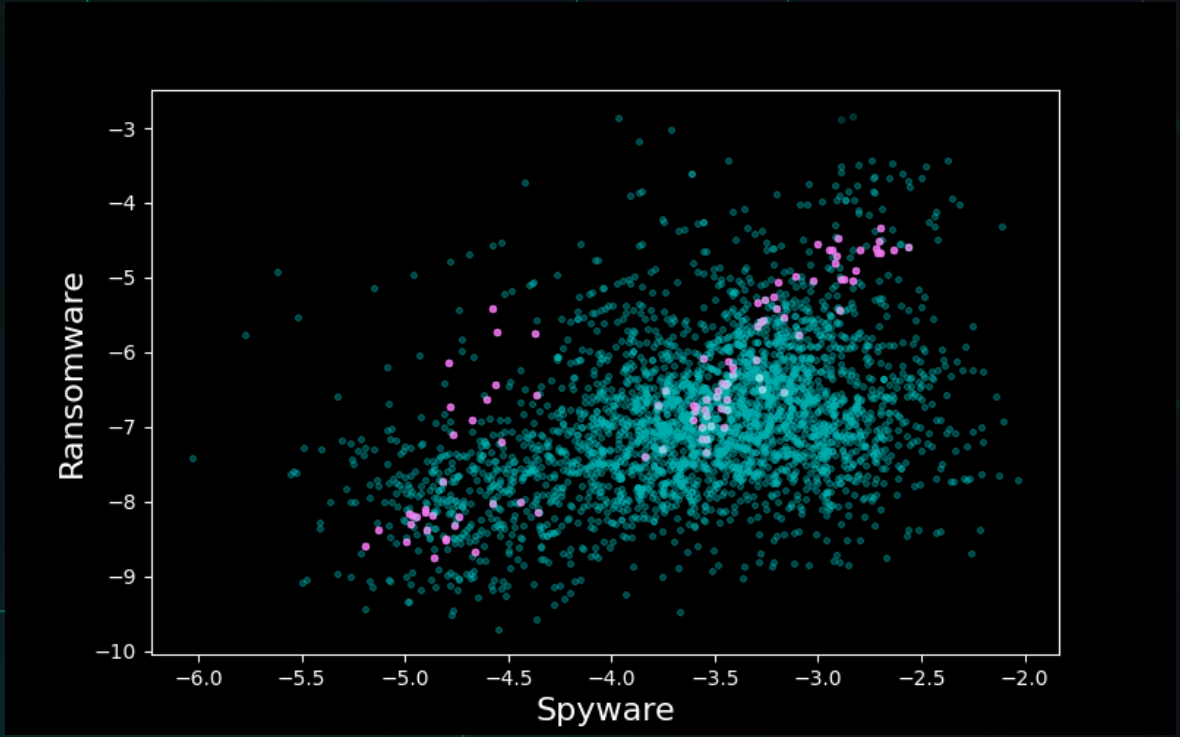
# How about Spyware?



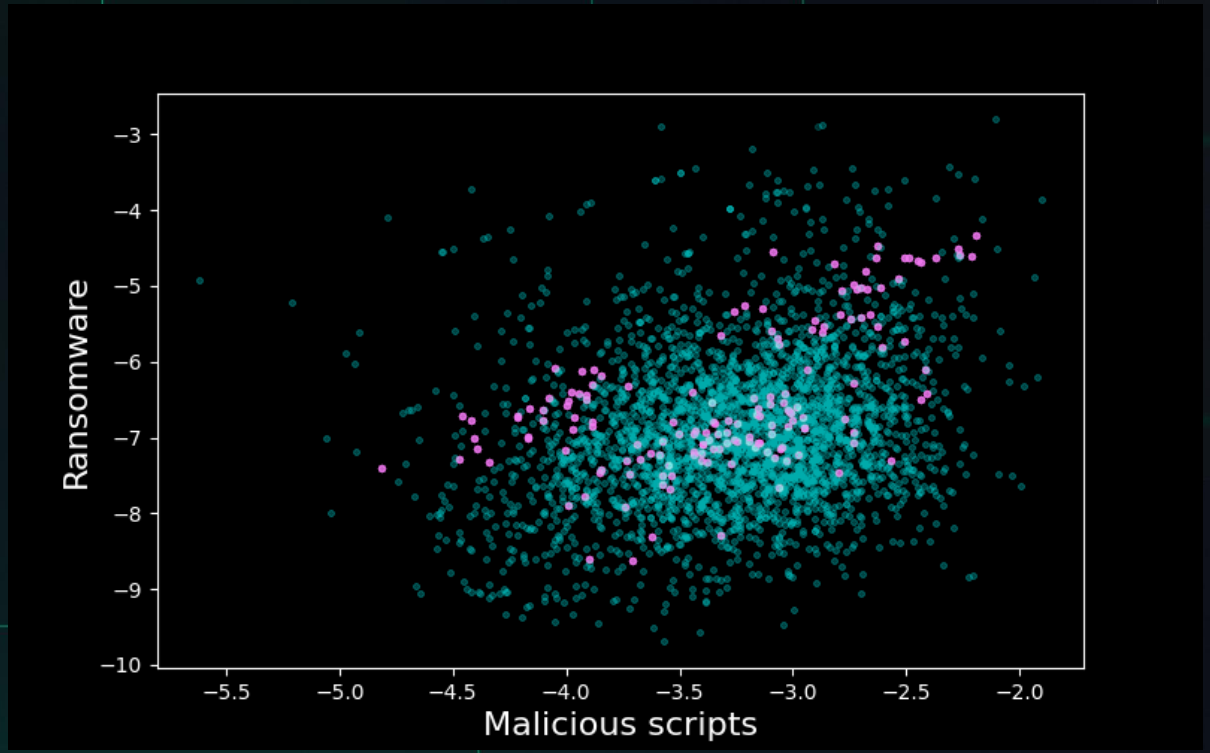
# How about Spyware?



# How about Ransom?

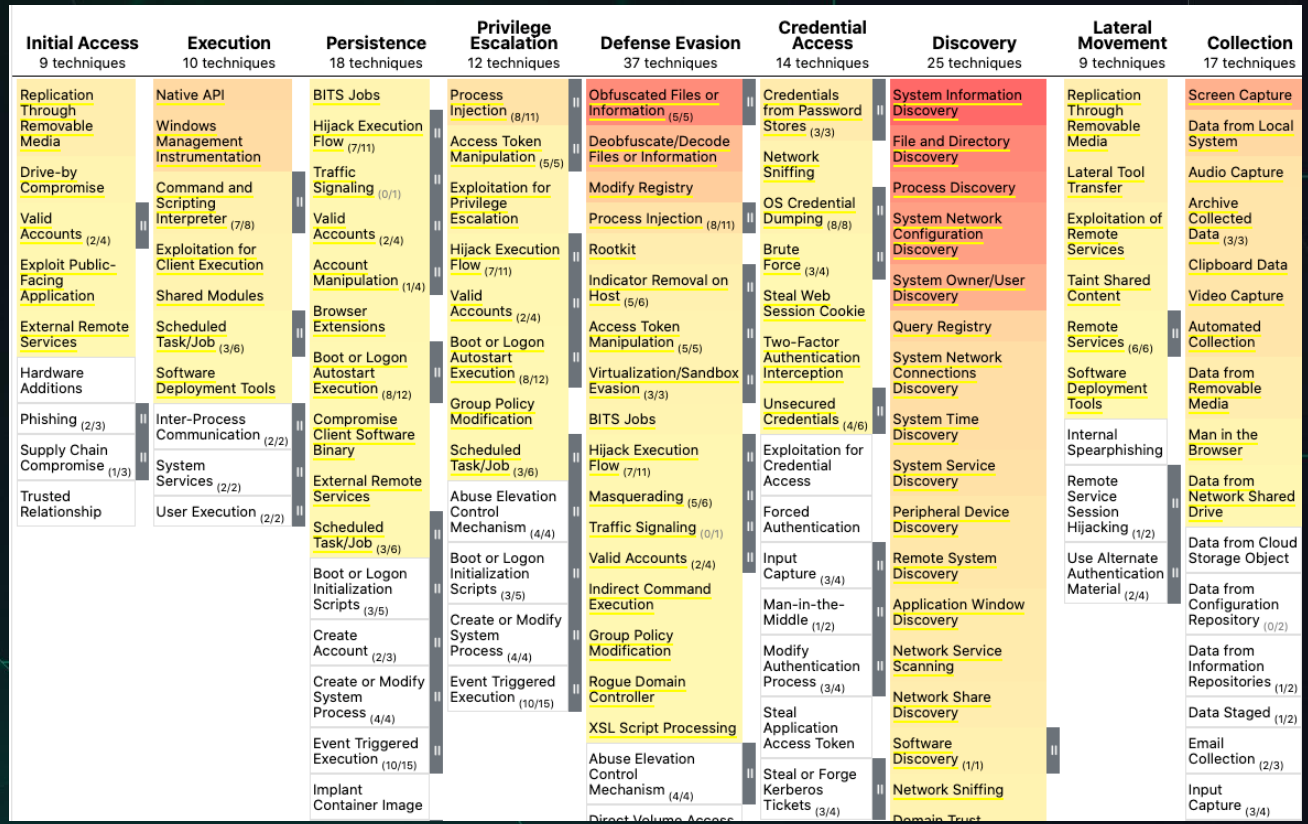


# How about Ransom?



# So what it all means?

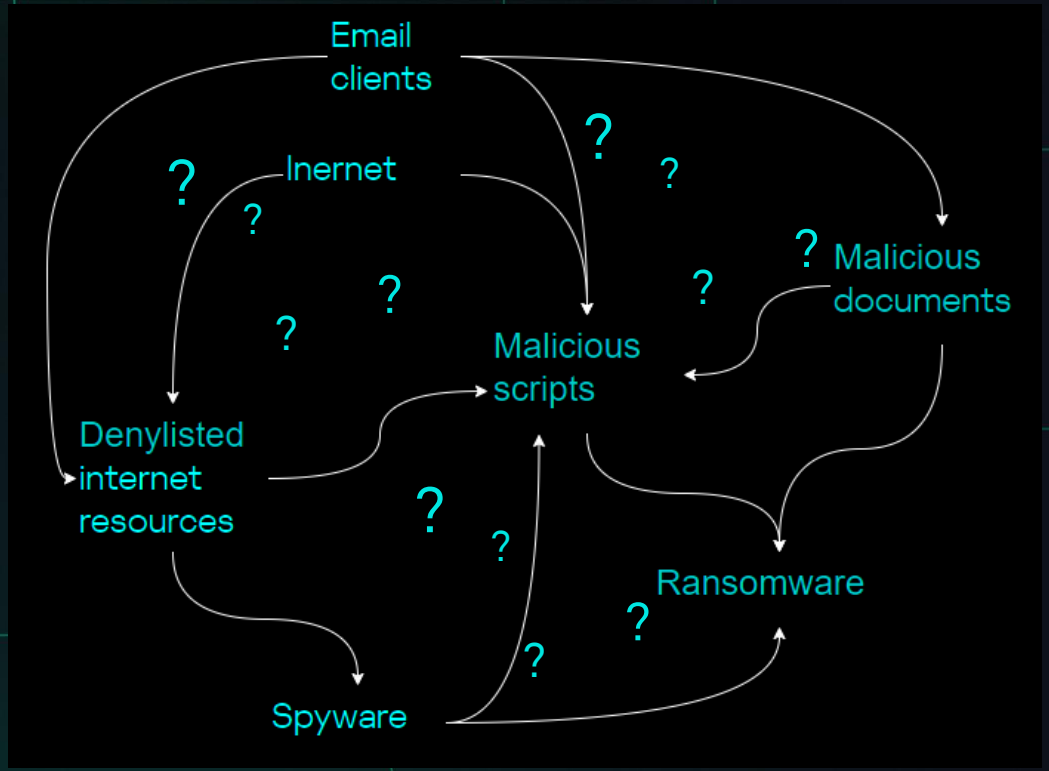




| Initial Access (9 techniques) | Execution (10 techniques) | Persistence (18 techniques) | Privilege Escalation (12 techniques) | Defense Evasion (37 techniques) | Credential Access (14 techniques) | Discovery (25 techniques) | Lateral Movement (9 techniques) | Collection (17 techniques) |
|---|---|---|---|---|---|---|---|---|
| Replication Through Removable Media | Native API | BITS Jobs | Process Injection (8/11) | Obfuscated Files or Information (5/5) | Credentials from Password Stores (3/3) | System Information Discovery | Replication Through Removable Media | Screen Capture |
| Drive-by Compromise | Windows Management Instrumentation | Hijack Execution Flow (7/11) | Access Token Manipulation (5/5) | Deobfuscate/Decode Files or Information | Network Sniffing | File and Directory Discovery | Lateral Tool Transfer | Data from Local System |
| Valid Accounts (2/4) | Command and Scripting Interpreter (7/8) | Traffic Signaling (0/1) | Exploitation for Privilege Escalation | Modify Registry | OS Credential Dumping (8/8) | Process Discovery | Exploitation of Remote Services | Audio Capture |
| Exploit Public-Facing Application | Exploitation for Client Execution | Valid Accounts (2/4) | Hijack Execution Flow (7/11) | Process Injection (8/11) | Brute Force (3/4) | System Network Configuration Discovery | Taint Shared Content | Archive Collected Data (3/3) |
| External Remote Services | Shared Modules | Account Manipulation (1/4) | Valid Accounts (2/4) | Rootkit | Steal Web Session Cookie | System Owner/User Discovery | Remote Services (6/6) | Clipboard Data |
| Hardware Additions | Scheduled Task/Job (3/6) | Browser Extensions | Boot or Logon Autostart Execution (8/12) | Indicator Removal on Host (5/6) | Two-Factor Authentication Interception | Query Registry | Software Deployment Tools | Video Capture |
| Phishing (2/3) | Software Deployment Tools | Boot or Logon Autostart Execution (8/12) | Group Policy Modification | Access Token Manipulation (5/5) | Unsecured Credentials (4/6) | System Network Connections Discovery | Internal Spearphishing | Automated Collection |
| Supply Chain Compromise (1/3) | Inter-Process Communication (2/2) | Compromise Client Software Binary | Scheduled Task/Job (3/6) | Virtualization/Sandbox Evasion (3/3) | Exploitation for Credential Access | System Time Discovery | Remote Service Session Hijacking (1/2) | Data from Removable Media |
| Trusted Relationship | System Services (2/2) | External Remote Services | Abuse Elevation Control Mechanism (4/4) | BITS Jobs | Forced Authentication | System Service Discovery | Use Alternate Authentication Material (2/4) | Man in the Browser |
| | User Execution (2/2) | Scheduled Task/Job (3/6) | Boot or Logon Initialization Scripts (3/5) | Hijack Execution Flow (7/11) | Input Capture (3/4) | Peripheral Device Discovery | | Data from Network Shared Drive |
| | | Boot or Logon Initialization Scripts (3/5) | Create or Modify System Process (4/4) | Masquerading (5/6) | Man-in-the-Middle (1/2) | Remote System Discovery | | Data from Cloud Storage Object |
| | | Create Account (2/3) | Event Triggered Execution (10/15) | Traffic Signaling (0/1) | Modify Authentication Process (3/4) | Application Window Discovery | | Data from Configuration Repository (0/2) |
| | | Create or Modify System Process (4/4) | | Valid Accounts (2/4) | Steal Application Access Token | Network Service Scanning | | Data from Information Repositories (1/2) |
| | | Event Triggered Execution (10/15) | | Indirect Command Execution | Steal or Forge Kerberos Tickets (3/4) | Network Share Discovery | | Data Staged (1/2) |
| | | Implant Container Image | | Group Policy Modification | | Software Discovery (1/1) | | Email Collection (2/3) |
| | | | | Rogue Domain Controller | | Network Sniffing | | Input Capture (3/4) |
| | | | | XSL Script Processing | | Domain Trust | | |
| | | | | Abuse Elevation Control Mechanism (4/4) | | | | |
| | | | | Direct Volume Access | | | | |

# So what it all means?





# That’s all

Thank you for your attention

**Subscribe to our reports: ics-cert@kaspersky.com**

Vladimir Dashchenko
Principal Security Researcher
Kaspersky ICS CERT
Vladimir.D.Dashchenko@Kaspersky.com

kaspersky