Acronis

MSPs and Cyber insurance:

Upselling security to help clients get coverage

An MSP webinar

January 23, 2024 – 10:00 CET

Acronis

- The conference is being recorded
- We will email you a link to the recording afterwards
- Please submit your questions through the Zoom Q&A interface

#CyberFit

Jeff Hardy

Global Solutions Marketing Manager
Acronis

Joining us today

Joseph Brunsman

Managing Member
Brunsman Advisory Group

Candid Wuest

VP Product Management
Acronis

Stephen Nichols

Director of Solutions Engineering, NAM
Acronis

Today’s Agenda

00:00–00:03	Introduction and Housekeeping
00:03–00:18	Cyberthreat Update – Candid Wuest
00:18–00:30	Cyber Insurance and Risk: A conversation with Joseph Brunsman
00:30–00:40	Configuring Acronis: A demo by Stephen Nichols
00:40–00:50	Panel Discussion
00:50–00:57	LIVE Q&A
00:57–01:00	Wrap-up

Acronis

Cyberthreat update

Candid Wüest

VP of Product Management

#CyberFit

Malware growth

300,000
new malware samples per day in 2024

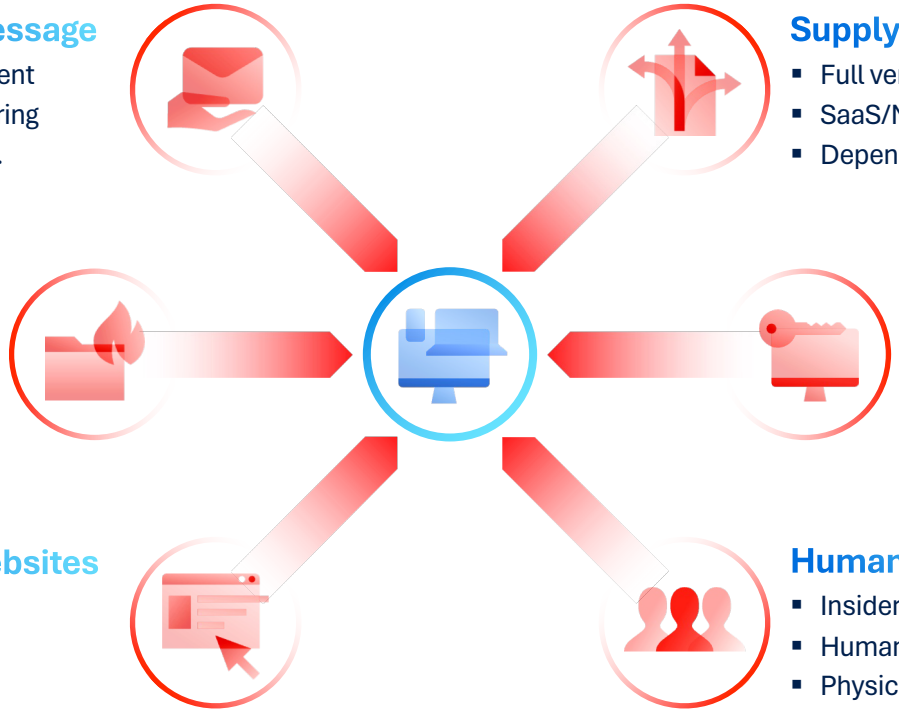
<2 days
average lifetime of malware

Typical cyberattack vectors

How are attackers getting into corporations?

Malicious message
- Email attachment
- Social engineering
- ChatGPT & Co.

Supply chain attack
- Full vendor compromise
- SaaS/MSP takeover
- Dependency infection



Service exploitation
- Unpatched service
- Fileless attacks
- Misconfiguration

Known credentials
- Brute force password
- Credential stuffing / phishing
- Paid dropper / Initial Access Broker

Malicious Cloud/Websites
- Abusing trusted location
- Manual download
- Redirect / site take over

Human factor
- Insider help
- Human error / complexity
- Physical access

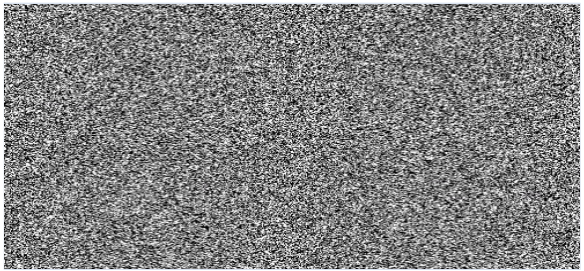
Malicious emails and useful tools

QR Codes + MFA proxy

- Emails with QR codes to hide the URLs from filtering
- Hijack sessions to bypass MFA
  e.g. W3ll's phishing kit that bypasses MFA and hijacks Microsoft 365 accounts

Living off your infrastructure

- Use your tools to deploy malware
  e.g. PSA, RMM and GPO
- Install & abuse clean applications
- MFA fatigue/bombing/SIM swapping



Modify protection tools

- Delete security logs & backups
- Uninstall security tools
- Add exclusions for C:\
- Use backup to exfiltrate data

Ransomware is dead – long live ransomware

Still easy to distribute – and still highly profitable

Increase the pressure

- Contact end-customers directly
- Trigger privacy fines, e.g., GDPR
- DDoS attacks to distract SOC

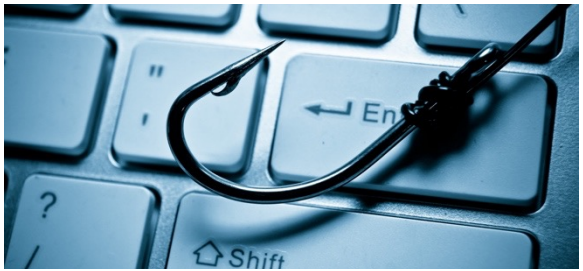
Know the target

- Find the data storage and read emails
- Learn from incident response plan
- Solve real support case to gain trust

Adapt the techniques

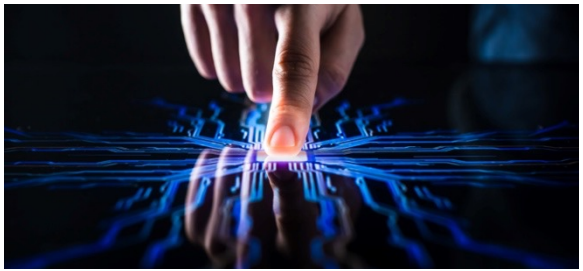
- Dual-encryption with two families
- Going after cloud data
  - E.g. Sphinx searching for Azure keys

Recovering from large-scale attacks can be a challenge



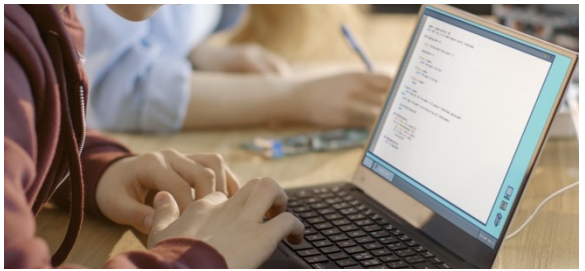
Business impact analysis

Non-existing or untested incident response plans, which are not maintained, are a big business risk.



Recovery speed & resources

Prolonged downtime impacts productivity and revenue. Attacks consume a lot of IT resources.



Digital fallout

Attacks can lead to significant data loss, brand reputation damage and erode customer trust and loyalty.

Acronis

Cyber Insurance and Risk

Joseph Brunsman

Managing Member
Brunsman Advisory Group

#CyberFit

Acronis

Additional materials

Thru-Partner Marketing Kit

Training:
Acronis #CyberFit Cloud Tech Associate Advanced Security with EDR 2023

Training:
Acronis #CyberFit Cloud Sales Associate Advanced Security with EDR 2023

#CyberFit

Acronis
Cyber Foundation
Program

Share the success of your growing business by helping others

Get your free
CSR in a Box
training kit