PRACTICAL CONSIDERATIONS FOR LEGACY COMMODITY MALWARE CLEANUP IN OT

JAN HOFF & LESLEY CARHART
INDUSTRIAL INCIDENT RESPONSE, DRAGOS, INC

⬇️ Get the Whitepaper ⬇️

WHO ARE WE

Jan Hoff

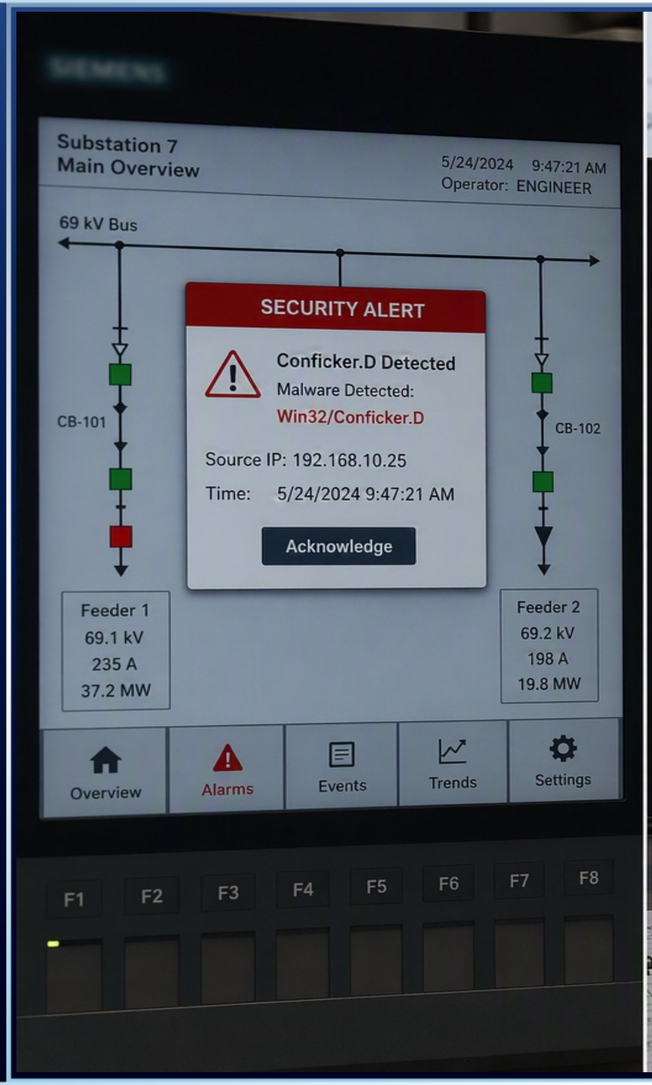
Digital Forensics and Incident Response Lead
Dragos Germany

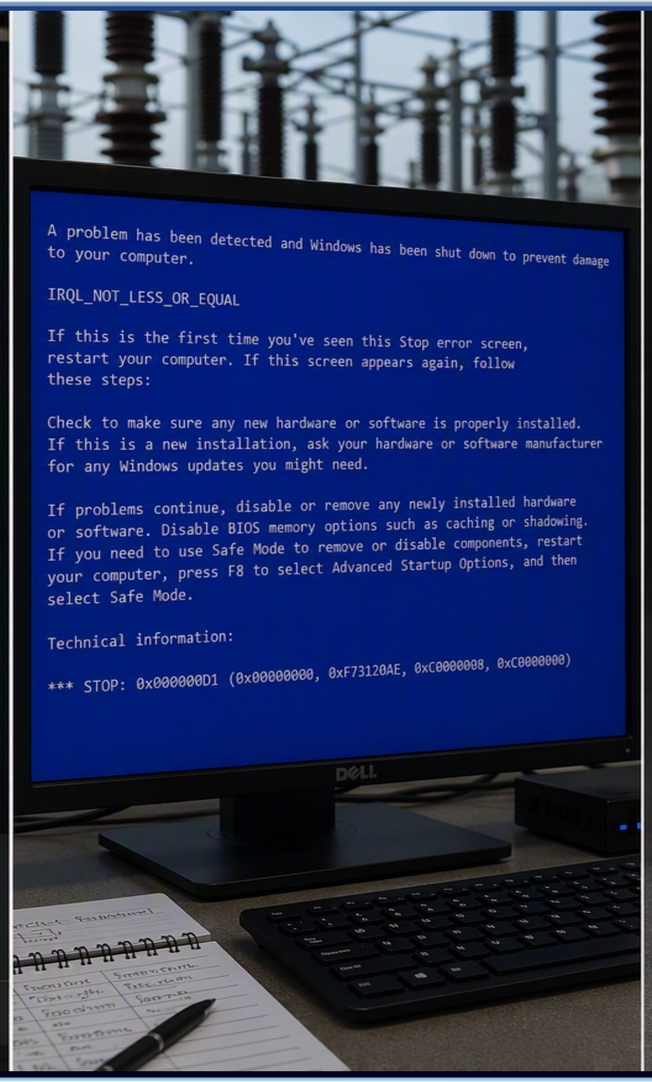
- 15 years in critical infrastructure - offensive and defensive track
- Worked at two of Europe's major energy companies
- Lecturer, University of Applied Sciences, Germany
- Based in Essen, Germany

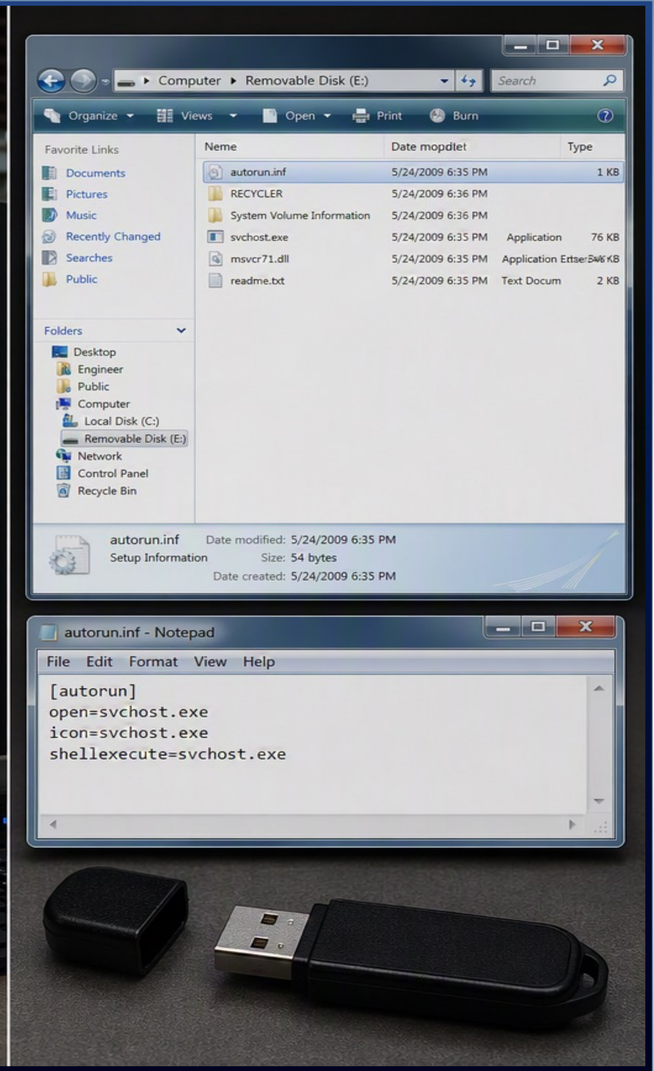
Lesley Carhart

Principal Industrial Incident Responder
Dragos Australia

- 18 years experience in OT incident response and forensics
- Background in aviation and manufacturing DFIR
- SANS ICS515 instructor
- Based in Melbourne, Australia


Substation 7
Main Overview
5/24/2024 9:47:21 AM
Operator: ENGINEER
69 kV Bus
SECURITY ALERT
Conficker.D Detected
Malware Detected:
Win32/Conficker.D
Source IP: 192.168.10.25
Time: 5/24/2024 9:47:21 AM
Acknowledge
CB-101
CB-102
Feeder 1
69.1 kV
235 A
37.2 MW
Feeder 2
69.2 kV
198 A
19.8 MW
Overview
Alarms
Events
Trends
Settings
F1
F2
F3
F4
F5
F6
F7
F8

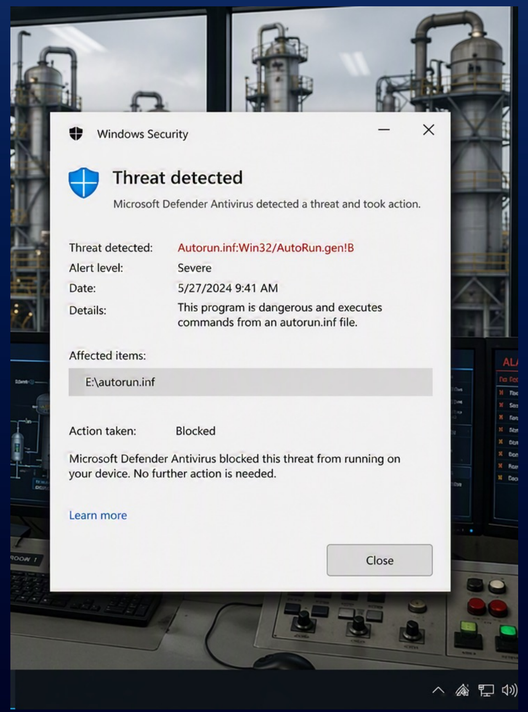

A problem has been detected and Windows has been shut down to prevent damage to your computer.
IRQL_NOT_LESS_OR_EQUAL
If this is the first time you've seen this Stop error screen, restart your computer. If this screen appears again, follow these steps:
Check to make sure any new hardware or software is properly installed. If this is a new installation, ask your hardware or software manufacturer for any Windows updates you might need.
If problems continue, disable or remove any newly installed hardware or software. Disable BIOS memory options such as caching or shadowing. If you need to use Safe Mode to remove or disable components, restart your computer, press F8 to select Advanced Startup Options, and then select Safe Mode.
Technical information:
*** STOP: 0x000000D1 (0x00000000, 0xF73120AE, 0xC0000008, 0xC0000000)
DELL


Computer ▸ Removable Disk (E:)
Search
Organize
Views
Open
Print
Burn
Favorite Links
Documents
Pictures
Music
Recently Changed
Searches
Public
Folders
Desktop
Engineer
Public
Computer
Local Disk (C:)
Removable Disk (E:)
Network
Control Panel
Recycle Bin
Name
Date modified
Type
autorun.inf 5/24/2009 6:35 PM 1 KB
RECYCLER 5/24/2009 6:36 PM
System Volume Information 5/24/2009 6:36 PM
svchost.exe 5/24/2009 6:35 PM Application 76 KB
msvcr71.dll 5/24/2009 6:35 PM Application Extension 346 KB
readme.txt 5/24/2009 6:35 PM Text Document 2 KB
autorun.inf Date modified: 5/24/2009 6:35 PM
Setup Information Size: 54 bytes
Date created: 5/24/2009 6:35 PM
autorun.inf - Notepad
File Edit Format View Help
[autorun]
open=svchost.exe
icon=svchost.exe
shellexecute=svchost.exe

MORE (COMMODITY AND LEGACY) MALWARE IN OT

- **Dragos Incident Response and Telemetry**
  - Increased retainer activations
  - Better visibility == more detections
  - xOT and IT integrations == more detections
  - Better governance == more detections

- **Dragos Intelligence Fabric** confirms trend
- Infections may be present **for years**



CUSTOM OT MALWARE VS. LEGACY MALWARE

CUSTOM OT MALWARE

TRISIS · Stuxnet · Industroyer

2014 Xt 2016 EI

VS

ORIGIN

Nation-state / APT

State-sponsored, targeted, long-term

TARGET

Specific OT systems

PLCs, RTUs, Safety Instrumented Systems

DELIVERY

Supply chain / targeted intrusion

Spear-phishing, hardware implants

DETECTION

Rare — no AV signatures

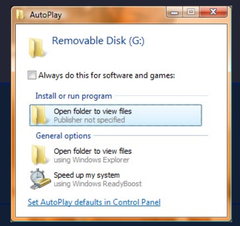
Custom protocols, long dwell time

OT IMPACT

Designed to cause operational failure. Rare, but consequences can be severe.

COMMODITY LEGACY MALWARE

Conficker · Sality · Ramnit



ORIGIN

Organised criminal groups

Financially motivated, opportunistic

TARGET

Any reachable Windows host

No OT knowledge required

DELIVERY

Opportunistic vectors

USB, network scanning, removable media

DETECTION

Signatures exist

But most OT hosts run no AV

OT IMPACT

Not designed for OT — but causes instability, spreads across networks, degrades systems over time.

YES, OT SYSTEMS WITH CONFICKER IN 2026

- OT has up to **20+ year old hardware/software**
- **Infections can linger** for years
  - Cybersecurity passive control atrophy
  - Lack of monitoring
  - Out-of-date and lax cybersecurity controls
  - Increased network connectivity

- Analysers, Cranes, HMI, Weighbridges, CNC Machines, Building Automation, and many more

COMMODITY LEGACY MALWARE – HERE TO STAY

Sality

ACTIVE SINCE 2003

ATTRIBUTES

- File infector
- P2P botnet
- USB spread
- Polymorphic
- Kills AV processes

OT IMPACT

- **PLC & HMI workstations**
  Trojanized PLC password tools — Automation Direct, Omron, Siemens · 2022

Conficker

ACTIVE SINCE 2008

ATTRIBUTES

- SMB worm
- MS08-067
- USB spread
- Password brute-force
- Disables Windows Update

OT IMPACT

- **Nuclear power plant**
  Introduced via removable media · 2016

Ramnit

ACTIVE SINCE 2010

ATTRIBUTES

- File worm
- Credential theft
- USB & network spread
- Remote desktop
- Modular plugins

OT IMPACT

- **Engineering workstations**
  Mitsubishi GX Works executables infected · 2 incidents, 2024

Gammima

DETECTED SINCE 2007

ATTRIBUTES

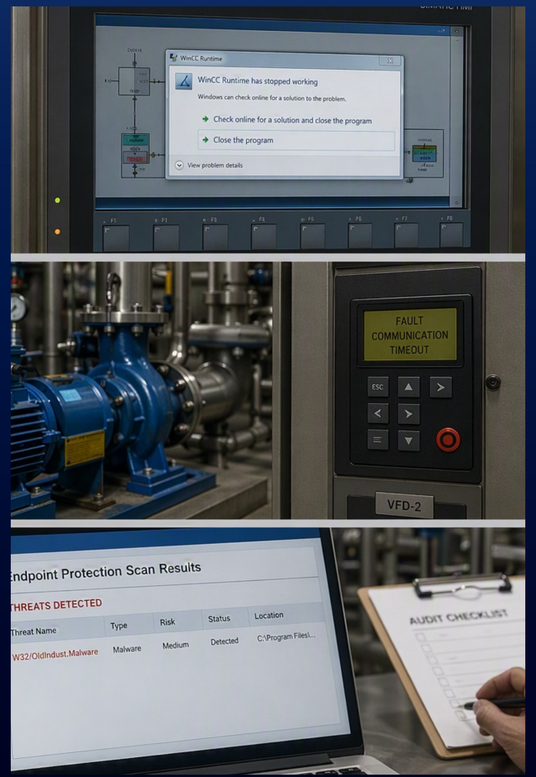
- USB worm
- Credential theft
- No C2
- Spreads all drives

OT IMPACT

- **International Space Station**
  NASA laptops infected via astronaut USB · 2008 · No mission system impact

WHY SHOULD ASSET OWNERS CARE?

- Older systems are **less stable and fault-tolerant**
- **Regulatory & compliance** requirements
- Changing **risk appetite**
- Remaining susceptible legacy systems are often **“crown jewel”** systems
  - Challenging or impossible to **replace**
  - Rarely **backed up** sufficiently
  - Likely not under **support**



MALWARE CHALLENGES FOR OT

OT Environments Constraints

- **Safety and reliability** first
- **Uptime** requirements
- Lack of approved/supported and functional **tooling**
- Lack of **visibility** (and potential re-infection)
- **Reliance on modern tools** and approaches
- No easy replacements, access, upgrade, and restoration

OT DFIR is not IT DFIR

- **Limited antivirus** and agent support
- **Unexpected consequences** of analysis and remediation
- **Less classic forensic** evidence collection and analysis – we know how this malware works
- **Deep embedding** of old infections

BOTTOM LINE: Do not approach this like modern ransomware remediation on modern computers

YOU FOUND $MALWARE – NOW WHAT?!?

Get the Whitepaper

- **“Do not panic! – You are not alone!”**
- IT playbooks likely will not help and could result in damage and disruption
- Risk management guides three different paths

PATH 01

Immediate Cleanup

Remove now. Accept the operational disruption to eliminate the threat completely.

PATH 02

Planned Cleanup

Schedule remediation during a downtime window. Balance thoroughness with operational continuity.

PATH 03

Leave in Place

Accept the risk formally. Understand the consequences and monitor accordingly.

OPTION ONE – IMMEDIATE CLEANUP

OPTION 01

Immediate Cleanup

Act now, restore fast

FOR

- Compliance met immediately
- Instability removed now
- Fastest resolution timeline

AGAINST

- Significant operational downtime
- High resource demand
- Cleanup failures can worsen impact
- Missed systems means starting over

USE WHEN

Regulatory deadline is imminent or active threat actor presence is confirmed

OPTION 02

Planned Cleanup / Upgrade

Controlled remediation window

FOR

- No immediate ops disruption
- Resources and risk pre-planned
- Can modernize patch and security posture
- Lower risk of missing infected systems

AGAINST

- Major upgrades are costly
- Infection persists during planning window
- Unforeseen impacts still possible

USE WHEN

Environment is stable, threat is latent, and planning time is available

OPTION 03

Indefinite Infection

Accept and monitor

FOR

- No disruption to current operations
- Irreplaceable systems unchanged
- No immediate resource expenditure

AGAINST

- Instability grows as hardware ages
- Regulatory and compliance exposure
- Lateral spread risk to partners and segments
- Can be repurposed by threat actors

USE WHEN

Systems are truly irreplaceable, threat is headless, and risk is formally accepted

OPTION TWO – PLANNED CLEANUP

OPTION 01

Immediate Cleanup

Act now, restore fast

FOR

- Compliance met immediately
- Instability removed now
- Fastest resolution timeline

AGAINST

- Significant operational downtime
- High resource demand
- Cleanup failures can worsen impact
- Missed systems means starting over

USE WHEN

Regulatory deadline is imminent or active threat actor presence is confirmed

OPTION 02

Planned Cleanup / Upgrade

Controlled remediation window

FOR

- No immediate ops disruption
- Resources and risk pre-planned
- Can modernize patch and security posture
- Lower risk of missing infected systems

AGAINST

- Major upgrades are costly
- Infection persists during planning window
- Unforeseen impacts still possible

USE WHEN

Environment is stable, threat is latent, and planning time is available

OPTION 03

Indefinite Infection

Accept and monitor

FOR

- No disruption to current operations
- Irreplaceable systems unchanged
- No immediate resource expenditure

AGAINST

- Instability grows as hardware ages
- Regulatory and compliance exposure
- Lateral spread risk to partners and segments
- Can be repurposed by threat actors

USE WHEN

Systems are truly irreplaceable, threat is headless, and risk is formally accepted

OPTION THREE – INDEFINITE INFECTION

OPTION 01

Immediate Cleanup

Act now, restore fast

FOR

- Compliance met immediately
- Instability removed now
- Fastest resolution timeline

AGAINST

- Significant operational downtime
- High resource demand
- Cleanup failures can worsen impact
- Missed systems means starting over

USE WHEN

Regulatory deadline is imminent or active threat actor presence is confirmed

OPTION 02

Planned Cleanup / Upgrade

Controlled remediation window

FOR

- No immediate ops disruption
- Resources and risk pre-planned
- Can modernize patch and security posture
- Lower risk of missing infected systems

AGAINST

- Major upgrades are costly
- Infection persists during planning window
- Unforeseen impacts still possible

USE WHEN

Environment is stable, threat is latent, and planning time is available

OPTION 03

Indefinite Infection

Accept and monitor

FOR

- No disruption to current operations
- Irreplaceable systems unchanged
- No immediate resource expenditure

AGAINST

- Instability grows as hardware ages
- Regulatory and compliance exposure
- Lateral spread risk to partners and segments
- Can be repurposed by threat actors

USE WHEN

Systems are truly irreplaceable, threat is headless, and risk is formally accepted

DECISION CRITERIA

PATH 01

Immediate Cleanup

1

Remove now. Accept the operational disruption to eliminate the threat completely.

PATH 02

Planned Cleanup

2

Schedule remediation during a downtime window. Balance thoroughness with operational continuity.

PATH 03

Leave in Place

3

Accept the risk formally. Understand the consequences and monitor accordingly.

- **Operational constraints**
  - Uptime and process sensitivity block standard cleanup
- **Incomplete scope**
  - One missed system restarts the entire cycle
- **Legacy environments**
  - Tooling support is nearly absent, systems may already be failing
- **Visibility gaps**
  - Without inventory and passive tooling, scope is unknowable

WHAT DO YOU NEED TO KNOW? DECISION CHECKLIST

1 THREAT INTELLIGENCE 0/1

- [ ] **MALWARE VARIANTS**
  What variants are present, and how do they function, connect, and spread?

2 SCOPE & VISIBILITY 0/2

- [ ] **ASSET VISIBILITY**
  Do we have adequate maps, inventory, and visibility to understand infection spread?
- [ ] **INFECTION COUNT**
  How many systems are infected vs. clean vs. vulnerable vs. patched?

3 PATCHABILITY 0/2

- [ ] **SYSTEM AGE & PATCH SUPPORT**
  How old are infected systems, and what patches (including emergency/unofficial) are supported?
- [ ] **PATCH PERMISSION**
  Will the vendor and site personnel permit these patches?

4 ANTIMALWARE ASSESSMENT 0/6

- [ ] **SUPPORTED TOOLS & LICENCES**
  What antimalware tools are supported on those operating systems, and are licences still available?
- [ ] **REAL-TIME VS. MANUAL**
  Do they run in real time, or require human operation?
- [ ] **CENTRAL LOGGING/MANAGEMENT**
  Do they have any central logging or management?
- [ ] **CLEANING EFFICACY**
  Will they reliably clean the malware variants observed?
- [ ] **PROCESS DISRUPTION RISK**
  May they be process disruptive?
- [ ] **VENDOR & ENGINEER APPROVAL**
  Are they permitted by the vendors and engineers?

5 REMEDIATION PLANNING 0/4

- [ ] **OS UPGRADE PATH**
  Can the system operating systems be upgraded by the vendor, and what is the cost?
- [ ] **DOWNTIME WINDOW**
  When is the next potential downtime window?
- [ ] **GOLD IMAGES**
  Do clean backup or gold images exist?
- [ ] **NETWORK ISOLATION FALLBACK**
  Can we implement network controls to partially isolate systems that cannot be remediated?

BUILDING A REMEDIATION PROJECT

- Identify an **appropriate time window**
- Understand **resource requirements** and **stakeholders** (people, process, technology)
- Confirm the **state of the environment and infections** are well understood and visible
- Ensure **potential side effects** of both cleanup and persistent infection have been risk assessed - working with engineering and vendors

CLEANING OUT THE CABINET

CLEANUP STRATEGY

- Identify all **online and offline** reinfection vectors
- Identify all impacted assets
- Isolate segments; **clean piece by piece**; No reconnection until clean
- **Remove unneeded** infected or vulnerable devices
- Deploy **permitted antimalware** (incl. open-source)

PREVENT REINFECTION

- Removable device and transient asset **policies**
- Removable device and transient asset and **identification and controls**
- Network shares & attached **storage**
- Remote access / internet **connectivity**
- **Patches** (even emergency or unofficial) when permitted and safe

UNTOUCHABLE HOSTS

- Strong **network controls** around all unremediated hosts
- Implement **network detection** around isolated systems
- **Plan replacement** or upgrade

CLEANING VALIDATION

- **Validate cleanup** using network detection, IOC-based hunting, and/or host forensic spot-checks
- Do **site walks and interviews** where needed to ensure all computers are accounted for
- Build stronger architectural, defensive, monitoring, and incident response capabilities moving forward
  - **SANS Five Critical Controls** for Industrial Cybersecurity

KEY TAKEAWAYS

- Legacy commodity malware **is already living** in most OT networks.
- **SANS 5 Critical Controls** provide the foundation for detecting and responding to legacy malware.
- Analysing and remediating like modern enterprise malware **may disrupt operations more than the infection does**.
- **Develop a plan** based in understood and **calculated risk** and **seek help if needed**!

Conficker has done more damage to industrial orgs than China, Russia, and Iran combined.
When you do not maintain your OT networks, do not have backups, and cannot do anything beyond trying to keep people out - Conficker will catch up to you eventually

– Robert M. Lee,
CEO, Dragos

THANK YOU

⬇️ Get the Whitepaper ⬇️