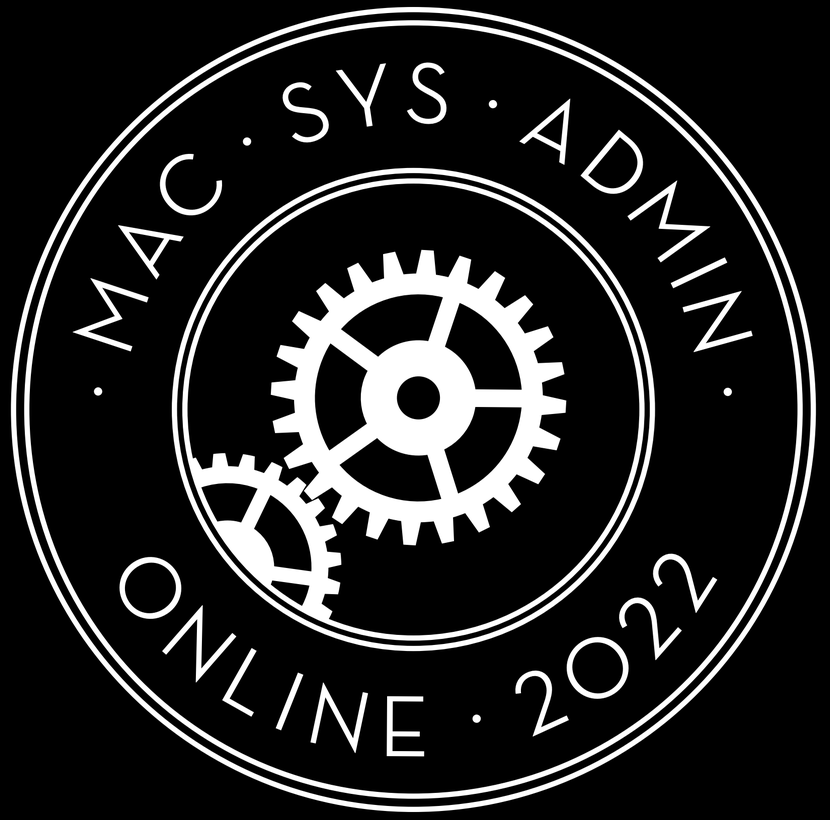
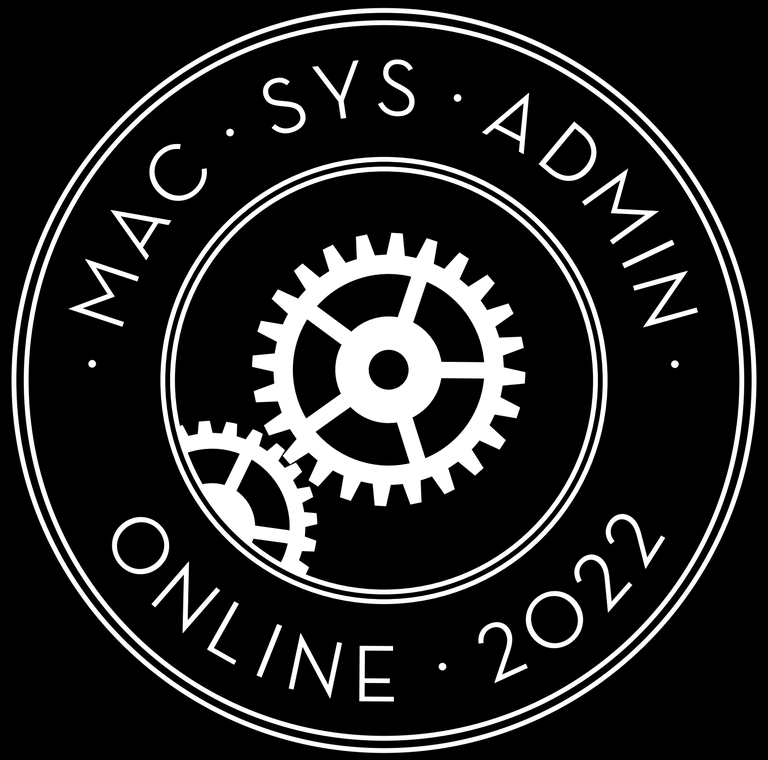
MacSysAdmin 2022

Patrik Jerneheim
MacSysAdmin AB



Welcome


MAC · SYS · ADMIN ·
ONLINE · 2022

MSA 22 - Speakers

“Sharing knowledge
is the most fundamental
act of friendship.

*Because it is a way you can give
something without loosing something.”*

–Richard Stallman

John Sutcliffe

Marc Nahum

Joel Cedano

Grace Picking

Charles Edge

Tim Perfitt

Ed Marczak

Søren Theilgaard

Rich Trouton

Csaba Fitzl

Arek Dreyer

Greg Neagle

Luke Allen

Tom Bridge

Jason Dettbarn

Neil Johnson

Armin Briegel

Emily Kausalik-Whittle

Henry Stamerjohann

Patrick Wardle

Jon Hoeg

Howard Oakley

Tim Standing

W Andrew Robinson

Robin Laurén

Michael Epping

Duncan McCracken

MSA 22 - Schedule

The Schedule

Published day-by-day

at 9:30 CET (UTC+2)

What are state machines

and why would you want to use them?

2022

Tim Standing - Other World Computing

State machines are used extensively by hardware engineers to handle events in everything from toasters to jet engines. But they're also a powerful tool for those of us writing software. I have come to rely on them when I write code which communicates with a server or code which can encounter a myriad of errors. In this session, we'll design and implement a state machine in Python to notarize a file by sending it to Apple's servers.

Unmasking WindTape

Analyzing an APT macOS malware specimen

2022

Patrick Wardle - Objective See

The offensive macOS cyber capabilities of the WINDSHIFT APT group provide us with the opportunity to gain insight into the Apple-specific approaches employed by an advanced adversary. In this paper, we'll comprehensively dissect OSX.WindTape, a second-stage tool utilized by the WINDSHIFT APT group when targeting Apple systems.

First we'll discuss the malware's anti-analysis mechanisms, and then once these have been thwarted, we'll explore its capabilities. To conclude, we'll present heuristic methods that can generically both detect and prevent WindTape, as well as other advanced macOS threats.

The Achilles heel of Endpoint Security

2022

Csaba Fitzl - Offensive Security

macOS introduced the EndpointSecurity framework in macOS Catalina to provide a generic security framework for third party applications. All EndpointSecurity client requires the user the provide Full Disk Access rights. If this permission is not granted, the client can't register and operate. While this is a preventive control for installing such software, it turns out to be the "Achilles heel" of the entire concept. Once this permission is revoked, the client becomes non functional, and thus trivial to disarm. To reset FDA permissions we can use tccutil. Originally it could be used to reset ES client permissions without any control, which was an issue.

In this talk I will show the evolution of tccutil, how and what kind of mitigations Apple added to the utility after my report and then how I bypassed it in various ways. Apple then went on and redesigned the whole control embedded in the tool, which I will also discuss. Although it seems to be ok now it is still vulnerable under certain conditions. At the end I will also briefly talk about the untold power of "Full Disk Access", and how it becomes (in my opinion) a single point of failure control in the operating system.

Security for Humans, revisited

2022

Robin Laurén - Reaktor

What is a human and how does it relate to security? How should one talk about security with humans? What are the relative strengths and weaknesses of humans related to security? Also, are you a human and if so, should you worry?

The Schedule

Three Live Sessions

at 15:00 CET (UTC+2) on Tue. Wed. & Thu.

Tuesday | Wednesday | Thursday | Friday

Welcome

2022
Patrik Jerneheim - MacSysAdmin
Hello and welcome to the MacSysAdmin 2022 Online Conference. Get the latest and greatest on the when and where around this online event.

Please join us for a short session about what to expect from the **MacSysAdmin 2022 Online Conference**.

Advanced Apple MDM Solution Designed for Security, Scalability & Exceptional Service Delivery

Addigy

2022
Jason Dettbarn - Addigy

How Apple silicon Macs manage their cores,

and why that's important for users.

2022
Howard Oakley - Eclectic Light Company
Managing processors with multiple identical cores isn't that complex, and a matter of coping with priorities and balancing load. To manage the CPU cores in an Apple silicon chip a decision has to be made as to which type of core to

What's New in IT?

2022
Live Presentation

Leveling Up

Managing admin rights in the enterprise

2022
Rich Trouton - SAP
A fundamental and controversial issue for enterprise Mac admins is the management of admin rights for their user community. Some say granting admin is fine, others think it's a bad idea and yet others have regulatory requirements which govern what can be done.

Like other enterprise environments, SAP has had to deal with the issue of admin rights for their users and developed a tool called Privileges to manage them. Join me for a discussion of the pros and cons of admin rights in general and how SAP arrived at developing and using Privileges for their solution to the issue.

XCreds

macOS login window authentication to your Open ID Connect Provider

2022
Tim Perfitt - Twocanoes Software
Learn about the open source project for macOS: XCreds.

MSA 22 - Sponsors

iMazing

किकी
Samarthan AB

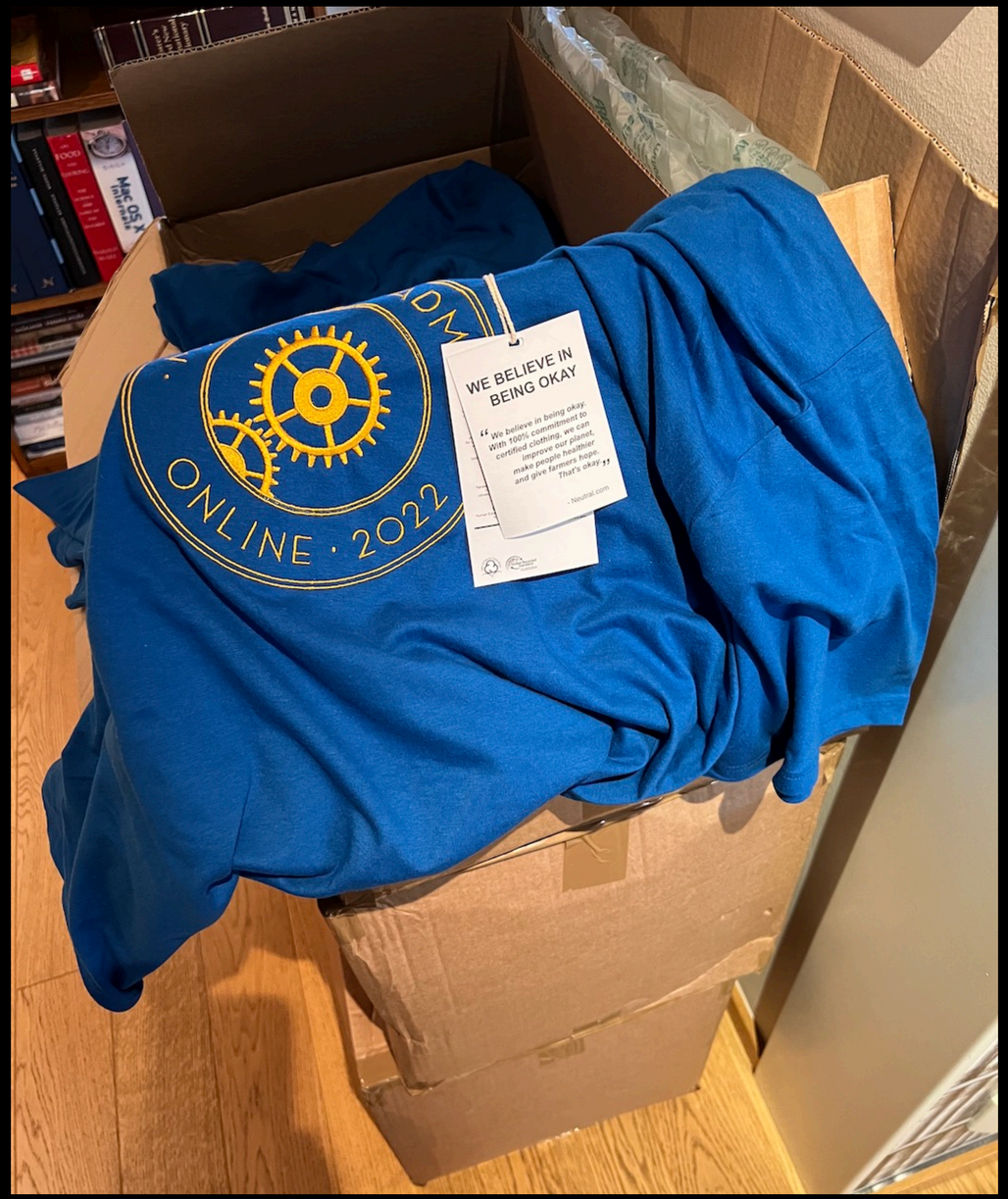
loopnet

Thank You!

MSA 22 - T-shirts

The T-shirt

We are shipping!

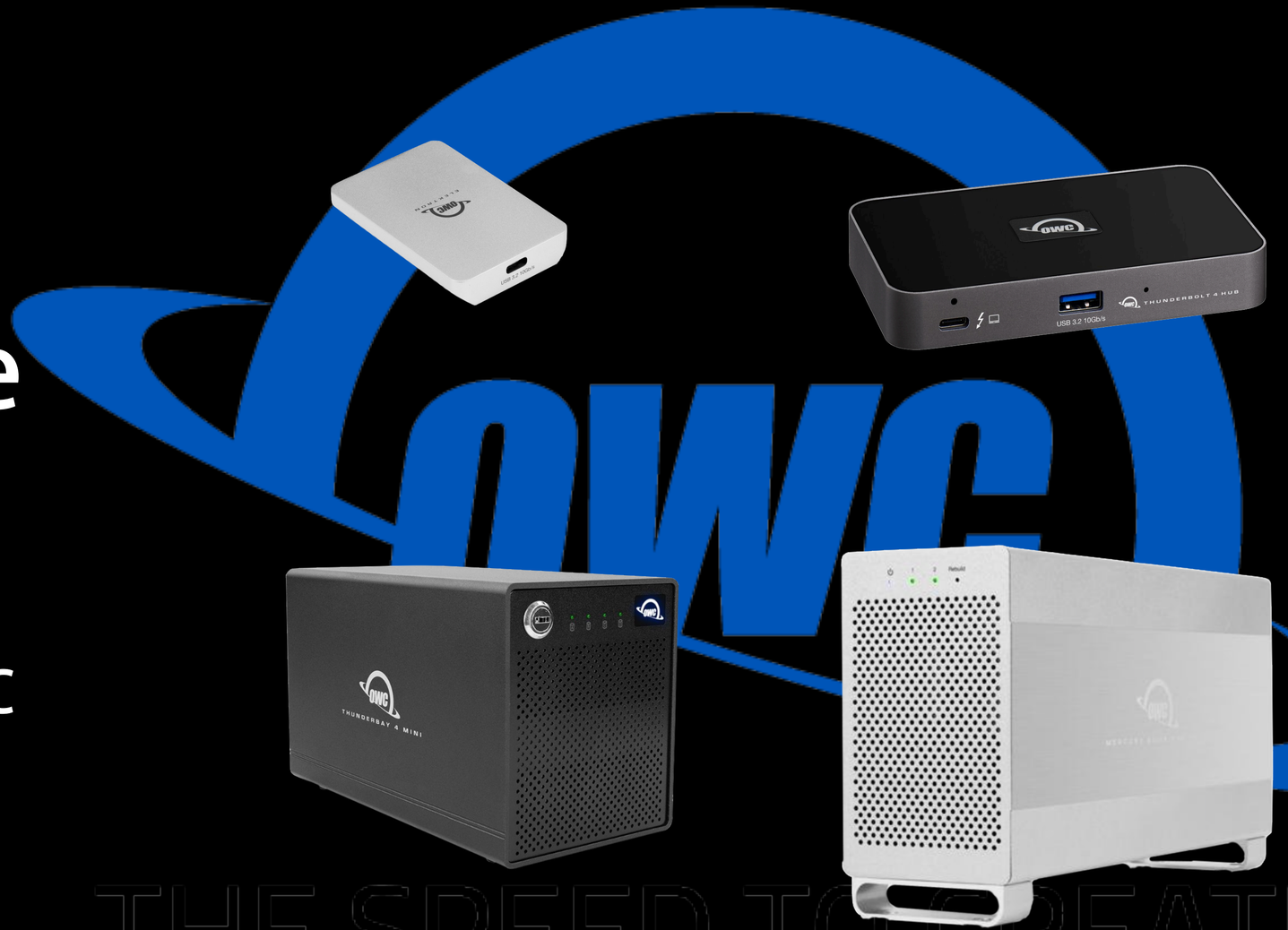


Thank You!

MSA 22 - Raffle

The Raffle

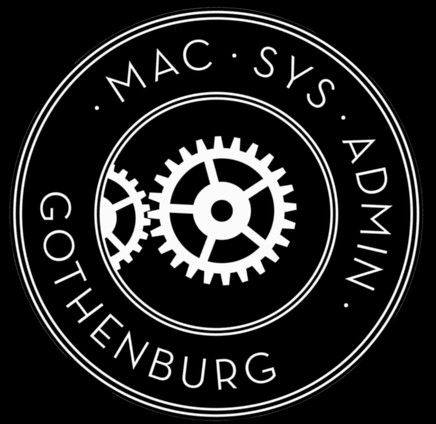
Amazing prizes
provided by OWC



THE SPEED TO CREATE.
THE CAPACITY TO DREAM

Have fun!

…one more thing



MacSysAdmin Conference

October 3 - 6 2023 in Göteborg