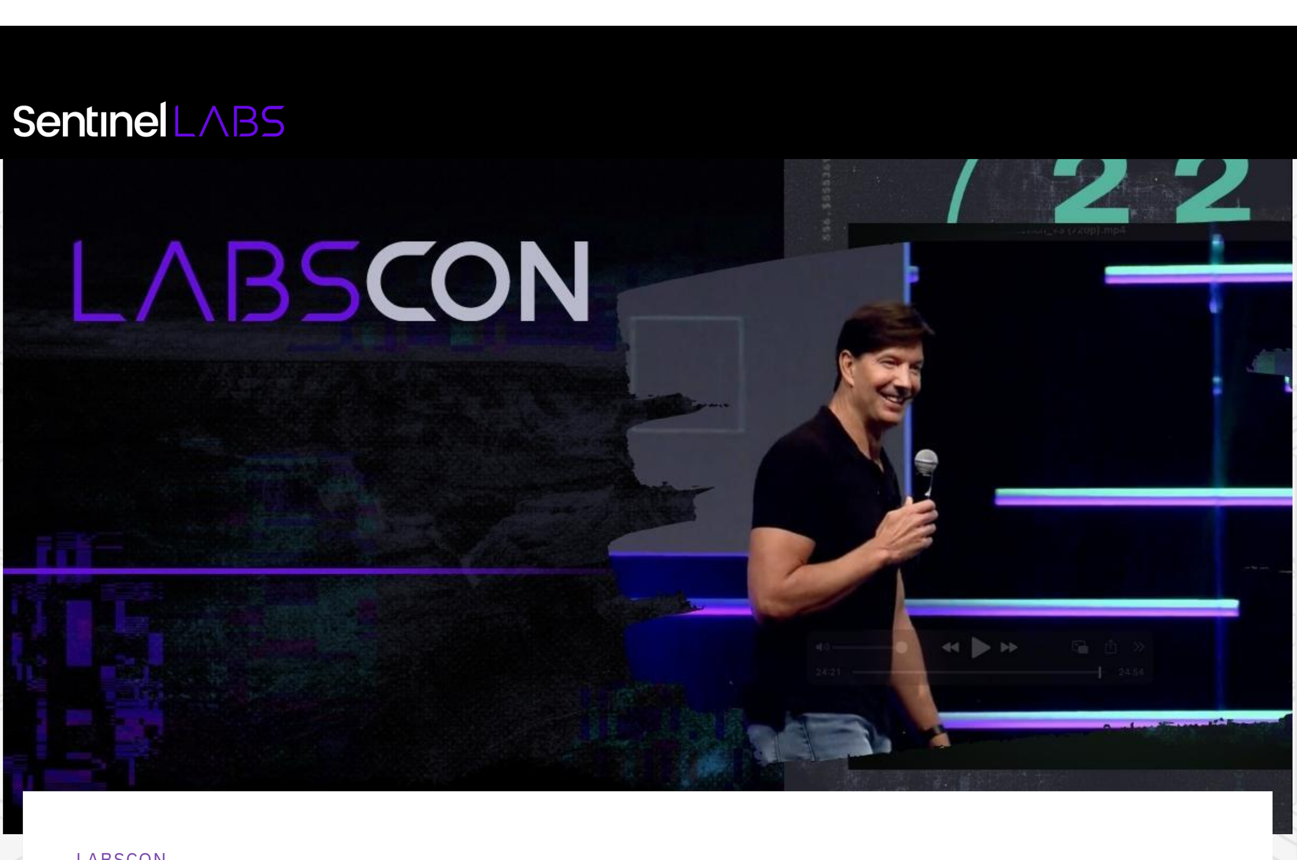
SentinelLABS



LABSCON

The Life and Times of SysInternals | How One Developer Changed the Face of Malware Analysis

JUAN ANDRÉS GUERRERO-SAADE / MARCH 29, 2023

When we first set down the idea of starting a SentinelLabs conference, we decided that the central tenet of the con would be to create a stage to showcase the best research, recognize potential contributions, and amplify them. As LABScon evolved and we were crafting the agenda, Ryan Naraine and I developed a shortlist of 'dream talks' we'd love to see on the first day Keynote stage. One idea that kept percolating up to the top was 'can we get Mark Russinovich to give us a history of SysInternals?' We eventually realized more than a talk, we were expressing a lasting admiration that deserves greater recognition. So as we set about convincing Mark to join our stage for this coveted talk, we sneakily set about creating our first 'LABScon Lifetime Achievement Award'.

Mark Russinovich (Left) receiving LABScon Lifetime Achievement Award from Ryan Naraine (Right)

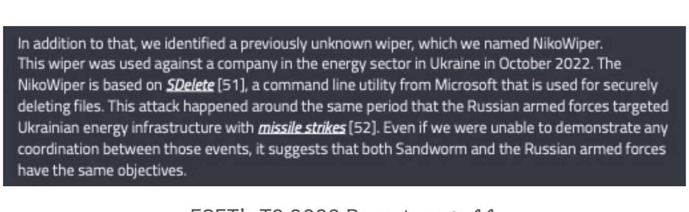
Mark Russinovich is now a recognizable commodity in the computing industry and prominently holds the position of Microsoft Azure's Chief Technology Officer but to the malware analysis industry he's a different figure altogether– Mark is the father of the SysInternals Suite. Early Windows sysadmins and malware analysts came to rely on this handy suite of tools for their day-to-day work.

The suite includes well-known tools like Process Explorer, System Monitor (SysMon), and Process Monitor (ProcMon). Though malware analysis is now a well-established subset of reverse engineering, it originally arose in part from using utilities to track OS quirks as they interacted with malware. To this day, dynamic analysis 101s kick off with SysInternals tools.

Mark Russinovich describing his early journey into computing

As Mark mentions in the talk, defenders weren't the only ones that saw the utility of SysInternals tools. Attackers have also adopted tools like PsExec and Sdelete for crucial parts of their operations. PsExec started out as a tool to allow sysAdmins to execute commands remotely. Those admins in turn realized its convenient ability to spawn remote processes. That same ability is now enthusiastically applied by ransomware operators and other attackers looking to move laterally and spread across an enterprise.

More recently, as cyber operations pepper the Ukrainian landscape in the midst of the Russian invasion, not all wipers have been purpose built by the attackers. On top of the approximately 15 wipers (that we know of) being used in Ukraine since February 2022, MSTIC researchers also spotted abuse of Sdelete in data destruction operations. While Sdelete was designed as a utility to securely erase files on Windows systems, it's just as useful to threat actors like 'IRIDIUM' who'll rename it 'cdel.exe' and effectively use it as a wiper. More recently, ESET also announced their discovery of a new wiper based on Sdelete that they call 'NikoWiper' used against the Ukrainian energy sector.

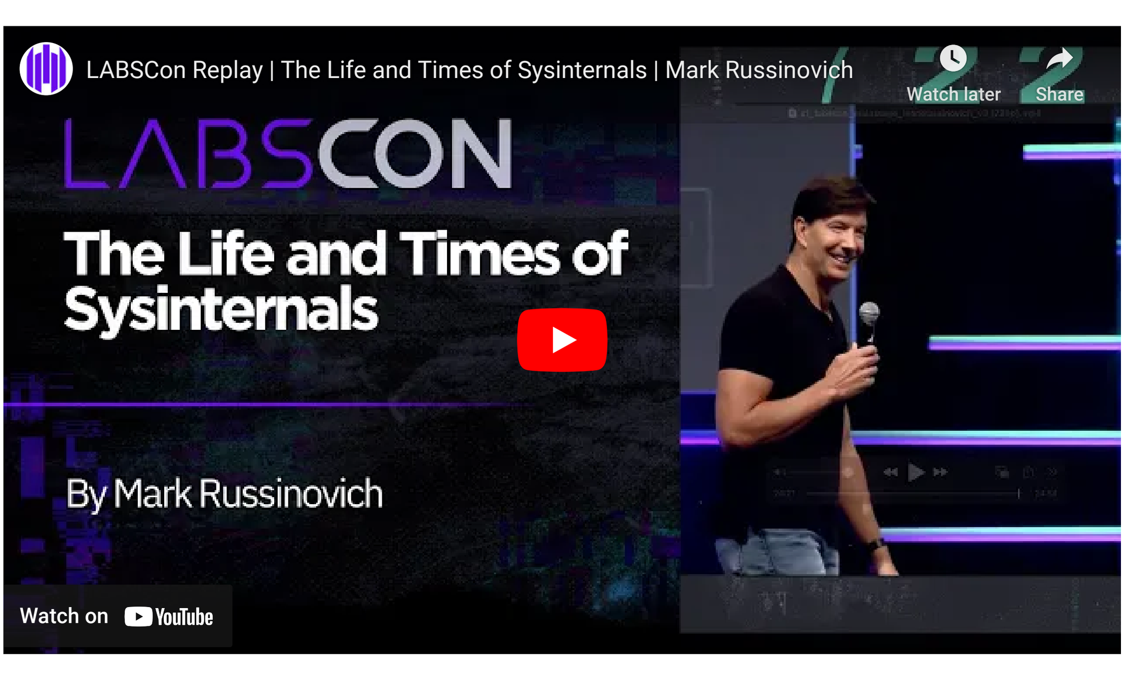


In addition to that, we identified a previously unknown wiper, which we named NikoWiper. This wiper was used against a company in the energy sector in Ukraine in October 2022. The NikoWiper is based on *SDelete* [51], a command line utility from Microsoft that is used for securely deleting files. This attack happened around the same period that the Russian armed forces targeted Ukrainian energy infrastructure with *missile strikes* [52]. Even if we were unable to demonstrate any coordination between those events, it suggests that both Sandworm and the Russian armed forces have the same objectives.

ESET's T3 2022 Report, page 11

Abusing great tools is a staple of the dual-use nature of technology but it's undeniable that the SysInternals Suite has done orders of magnitude more good in the hands of sysadmins, defenders, and malware analysts. Mark was also kind enough to share a demo preview of a special capability meant to address some of these abuses (kept as TLP:RED) for the LABScon audience. It's worth noting as an example of Mark's continued commitment to the SysInternals tools as he continues to contribute features and bug fixes to this day.

It's in that spirit of appreciation that we recognize Mark Russinovich as our first LABScon Lifetime Achievement Award. We hope you'll join us in congratulating him and enjoy his keynote: 'The Life and Times of SysInternals'



LABSCON SYSINTERNALS

JUAN ANDRÉS GUERRERO-SAADE

Juan Andrés is Senior Director of SentinelLabs and an Adjunct Professor of Strategic Studies at Johns Hopkins School of Advanced International Studies (SAIS). Juan Andrés was Chronicle Security's Research Tsar, founding researcher of the Uppercase team. Prior to joining Chronicle, he was Principal Security Researcher at Kaspersky's GReAT team focusing on targeted attacks and worked as Senior Cybersecurity and National Security Advisor to the Government of Ecuador. His joint work on Moonlight Maze is now featured in the International Spy Museum's permanent exhibit in Washington, DC.