SwiftOnSecurity **@SwiftOnSecurity** *Tue Jan 05 19:02:26 +0000 2021*

Consulting with internal teams on how ActiveX works this is how I earn that Cyber paycheck

Me in 2010: This is the biggest waste of my life imaginable this is dead-end technology

Me in 2020: welcome to my presentation on ActiveX

Fun fact for years Flash would just ignore your administrative settings file if you created it with Notepad. **https://t.co/ARHiOKjLQY**

I don't like getting on video calls because then people can look in my eyes and see how dead I am inside

InfoSec benefits from a wide variety of experience and backgrounds. Some of the stuff I'm getting asked, you just wouldn't have a way to easily know.

But there's a lot of other stuff my Ops path has never taught me. That's the point of having a team of people when possible.

Let's talk about the experience path I took from cybersecurity to operations back to cybersecurity again and how each step of the way made the next possible.

The story starts – as most do – with Croatian adware, a tool from a developer from Holland, Oracle, and Mark Russinovich.

Anyway I'm working in 2008 in entry Helpdesk supporting mostly unmanaged Windows XP computers with unmanaged antivirus. And they're all remote.

You can't reimage them you just got to fix them over remote control.

It was 2008 so a lot of adware and toolbars.

One of the core disinfection tools was "HijackThis" which showed various autorun hooks and ways IE was being modified, and let you remove them. It was hyper-effective. You could lay waste to the kingdom of satan.

And it showed custom tooling could fix problems in other programs.

Anyway, the company implemented a server-based CRM system called Siebel. It's user interface was 15+ different ActiveX controls. In IE6. With everyone with admin.

They corrupted and broke all the time. Other techs reimaged these PCs. But I thought, "isn't this like a toolbar?"

So I used HijackThis to remove Siebel ActiveX controls. They would then reinstall, and the PC would work! No reimaging! So everybody assigned these tickets to me. I did it all day.

But it was boring and figured, there's got to be a better way. If this tool can do it, I can do it

So, how do I find out how HijackThis removes ActiveX controls? With Process Monitor by **@markrussinovich**.

I watched what it did to the registry and implemented those actions as batch commands with .reg. Alongside RegEdit search, I found out how to comprehensively wipe ActiveX.

I now had a tool (more complicated than it sounds) that when run as admin could fix an employee's computer in several seconds instead of hours.

Because I knew it had to be possible. I remember the night I finished it, and the first call where I used it.

It was god damn magic.

Anyway, this tool would go on to be used by all agents and it would largely save the deployment of Siebel at the company. They had spent 30+ million dollars at that point.

And I was hired full time instead of as an hourly temp.

A few years later...

Using my Process Monitor knowledge, I would go on to detect a novel version of the Ilomo worm spreading from the domain controllers, later named Clampi.D by Symantec and credited to me. (Not publicly)

Here's the last tweet in the thread, scroll up.

Several years after that... **https://t.co/1EAZYd8sqt**
We had a problem. We ran two different Oracle cores, named internally ERP and OPM.

The interface, like Siebel, was ActiveX. But two different versions, both of which were trash, especially when running at the same time, which they always did.

The company accepted this.
By this time I was the tech at a call center. And these ActiveX would routinely crash and leave hanging EXE resident until reboot. It was even worse in Win7.

What's the plan? We just won't upgrade to Win7. Upgrading Oracle is stupid complicated and tens of millions of dollars.
Eventually I got so sick of this, just as a professional and as a human with standards, I was determined to find a solution.

I had fixed ActiveX before. I had a basic knowledge to jump from. But this was a new problem.

ActiveX was called Jinitiator and there were two versions.
I knew from research that Jinitator was a fork of Java JRE.

So I thought... what if I tricked Oracle into loading consumer Java... instead of Jinitiator? Using the registry?

It had better process isolation and years of fixes for crashes. It was insane. But I was going to try it
So I reimaged computers, loading Process Monitor, and observed how Internet Explorer loads ActiveX controls and Oracle initializes.
Pure reverse engineering. No documentation.

I spent two weeks, several hours a day, trying to trick it to accept Java's DLL. Rise RegEdit Repeat.
And then.

Then there was the day.

I got Oracle ERP and OLM to load inside Java 6.

I showed it to my supervisor, I started deploying 1 at a time, and the world changed.
It was faster. It rarely crashed. Multi monitor. It saved customers often waiting for employees to reboot.
Why did I do this. It wasn't my responsibility. Literally, the business accepted it for years.

Because I was on the floor. I listened to employees who suffered. Tales of angry customers waiting.

I was the one who took the calls. I had skin in the game.

I knew I could do it.
I was hired as a temp to plug in machines on an internal volleyball court and answer questions from other temps in an event that lasted 3 months.

I am now a Security Engineer for a Fortune 100.

Not because I am unique. But because I knew I could make a difference. That was it.

So I ask, do you let people make a difference.