COMPANY NAME HERE

PRONETWORK NEWS

Risk Management Tools for the Design Professional

February 2023 | Vol. XII No. 4

Kip Boyle

Kip Boyle is the Chief Information Security Officer (CISO) for several companies. He helps senior decision-makers overcome cybersecurity hurdles and manages unlimited cyber risks through rigorous prioritization. He's served as a Captain with the F-22 program in the US Air Force. In the private sectors he was a CISO for an insurance company, credit card processor, bank, credit union, and IT Managed Service Provider. He has also succeeded in other IT risk management roles in the financial services, technology, telecom, and logistics industries. He lives in Seattle with his wife and six kids.

Kip Boyle
Founder and CEO
Cyber Risk Opportunities
Email: info@cyberriskopportunities.com
Phone: (253) 234-5474

a/e ProNet
Lynda Colucci, Executive Director
info@aepronet.org

How to Protect Employees Who Are Extra Vulnerable to Malware

By Kip Boyle, Founder and CEO, Cyber Risk Opportunities

Cybersecurity people (like me) regularly tell everyone don't click on links or open up attachments that unexpectedly arrive in an email message.

Unfortunately, there are lots of people who go to work every day and can't possibly follow this advice. If they did, they would never get their work done and they would probably lose their job.

Accounts Payable is one affected workgroup I think about a lot, but there are also other workgroups like Sales, Customer Service, and Human Resources.

Their jobs require them to take greater risk every single day because they have to open up many emails from unknown senders. It's the nature of their work.

And, these people also have access to some of the most valuable digital assets we have, including our money and sensitive employee and customer data.

Cybercriminals are very well aware of this and they design attacks, usually phishing, based on these facts. And even though business email compromise is an threat, in this article, I really want to focus on malware that is designed to silently sneak into their workstations and to give criminals a foothold on their target.

Let's look at some reasons why these workgroups are extra vulnerable.

Accounts Payable is probably the easiest ones to understand. They get invoices by email from new suppliers all the time. And my observation is that they're not often told when new suppliers are contracted with.

Now, let's turn to Sales. What do you think is going on over in the Sales department that's causing them to open up a lot of unexpected email from unknown senders? Usually it's inbound sales inquiries. That's seen as a hot lead.

How about Customer Service? They're receiving inquiries and emails from alleged customers who need, who need support. And it's their job to respond and keep customers happy.

Let's look at Human Resources. Their job is to review and hire people which requires them to receive resumes, cover letters, and applications via email.

Now let's look a real attack that's designed to deliver malware via a phishing email.

RECENT BLOG POSTS

Scholarship Recipient Rebecca Rasmussen: My Work to Utilize the Finite Element Method To Create Computational Representations of Geometry Useful in Design, Analysis and Manufacturing Applications Read More

a/ePronet AIA David Lakamp Scholarship Winner, Sabrina Lem Read More

Scholarship Winner Jennifer Stieben's Collaboration on Bellevoir Ormsby Estate in Louisville Read More

Scholarship Winner Deanna Ho's Collaboration on Vehicle Bridge Read More

Rebecca Rasmussen a/e ProNet 2022 ACEC Scholarship Recipient Read More

a/e ProNet Announces Our Two Recipients for the 2022-2023 David W. Lakamp Scholarship Read More

PRONETWORK NEWS

November 2022 - Fees Quagmire by *David Benjamin*

Read More

a/e ProNet
Lynda Colucci, Executive Director

info@aepronet.org
aepronet.org

There was a phishing campaign where attackers were posing as job applicants and luring corporate hiring managers into downloading what they thought were resumes from job applicants. But the resumes were bogus and they contained a piece of malware called "More_Eggs".

But More_Eggs is actually a Remote Access Trojan (RAT) which is designed to silently steal user names and passwords for all kinds of accounts like bank, email, and remote access.

So, because of all the above, these workgroups in your organizations deserve more protection against malware than others.

And for those of us who don't have a big IT department, we need to do that in a minimum viable way.

What does "minimum viable" mean in this context?

It's answering the question "What's the least we can do to manage this risk down to an acceptable level without killing our productivity?"

Now, how will we deal with the elevated risk of malware for these workgroups?

It's not enough to give them the standard anti-malware package we give to everyone else.

What we need to do is turn their computer into an appliance.

That is, reconfigure their computer so that it can only run the programs that they need to do their job and nothing more.

And this is called Application Control and some people call it Application Whitelisting.

The idea is to block all malware from running no matter where it came from or what it is. What it's doing is flipping our defense from "here's the list of malware I don't want to run" over to "here's the list of things that I only want to run"

When we do this, any piece of malware that lands on the computer, by definition will not execute. It makes the consequences of opening a phishing message irrelevant.

This is the future of malware defenses. Antivirus vendors are already integrating Application Control of one kind or another into their product.

And the easiest way to test Application Control is to use Windows Defender Application Control (WDAC) which is built into every version of Windows 10 and above.

To get started, do a web search for "Windows Defender Application Control Wizard" and it will walk you through the set up.