Insights

Pragmatic cyber security advice for senior executives

Optimising phishing and malware defences with threat intelligence

Technical Viewpoint

Christo Butcher
Global head Threat Intel
managed services, Fox-IT

Global. Transformative. Resilient.

Optimising phishing and malware defences with threat intelligence

Christo Butcher
Global head Threat Intel managed services, Fox-IT

Phishing and malware attacks against operational technologies increased sharply in the last quarter, by 60%. With these attacks evolving rapidly, Christo Butcher, Global head Threat Intel managed services, Fox-IT, discusses how threat intelligence can optimise your defences against phishing and malware.

The rise in attacks on operational technologies – which monitor and control industrial equipment – is part of a long-term trend. Why? The bad guys are just upping their game.

How can organisations reduce the likelihood that one of these cyber attacks will be successful and cause major financial, operational and reputational damage?

Any cybersecurity policy should prioritise prevention, detection and response.

In this article, I'm going to focus on prevention, with guidance which can be applied across sectors.

60%
increase of phishing and malware attacks against operational technologies in the last quarter

Prevention

This is the most important of the three-pronged defence. As we all know, prevention is better than cure.

A great example of high-value prevention is multi-factor authentication. On the one hand, it is relatively easy to setup and doesn't cost much. On the other, it gives a high security return because it stops attackers from using stolen passwords.

If you enable multi-factor authentication, even if your credentials are stolen, the impact is much less. If you don't have multi-factor authentication and the bad guys steal your password, they have access to your account. With multi-factor authentication, hackers will struggle to log in to your account. Low-hanging fruit like this is often built into business software.

Besides multi-factor authentication, organisations should also make it difficult for phishing emails to reach their users. Implement anti-phishing and anti-email spoofing technologies. They are often built into software products, including Office 365; you just need to set it up.

Such security features analyse emails and block suspicious, phishing-like emails in which fraudsters try to trick the recipients into revealing valuable personal details such as usernames and passwords.

Another defence against phishing is thinking about your organisation's digital footprint. If you have a lot of information about your organisation and your users, you are making it easier for an attacker to collect information and write a convincing phishing attack.

And don't forget the human factor. Educate your employees and suppliers about cyber security risks, especially from phishing. Phishing emails will sneak through even the most well defended corporate networks.

Make it easy for users to do something about it. Train them so they know how to spot phishing emails.

You can train them using simulations to test users – for example using phishing emails, designed by ethical hackers, to see how they respond. This will help users spot and record phishing emails, and who to send their report to – for example your company's cyber security officer. It should be standard practice.

Let's be clear.

We're not talking about spending a lot of money on new technology. It's about using existing procedures and technologies more efficiently.

PREVENTION TOP TIPS

Set up Multi-factor authentication

Implement Anti-phishing and anti-email spoofing technologies

Think about your organisation's digital footprint

Educate your employees and suppliers about cyber security risks

Malware threats

As well as trying to steal your user credentials, phishing emails might try to install malware on systems.

When you get a phishing email with an attachment and you open it, very often that attachment will try to deploy malware. Make sure that your endpoint, such as your laptop, is hardened so that it's more difficult for attackers to deploy malware.

That's where out-of-the-box products are often not so great, because attackers buy the standard IT tools and practice on them and try to find security flaws in the standard configuration.

Keep your security tools and procedures up-to-date, and configure them appropriately for your situation. Sticking to this best practice will make it harder for cyber criminals to infiltrate your company's network.

There are three levels of threat intelligence

Strategic

Mid-level

Base-level

Threat intelligence

This is about understanding the threats you face; how serious they are, and how you can protect your organisation against them.

There are three levels of threat intelligence – strategic (the highest level, for example, global trends in cyber security threats); mid-level ("tactics, techniques and procedures" or "TTP" in industry jargon), which has more detail on security threats, and the bottom, most basic level, which includes information about the "fingerprint" of, say, malware and other basic details.

Of these three, the middle layer is the most useful type of threat intelligence for organisations. It helps organisations prioritise cyber security risks, map them against their IT systems, pinpoint potential weaknesses and strengthen them. How could cyber criminals attack my organisation, get into my network and take it over. How can I stop them?

New technologies

Could advances in security software help stem the rising tide in phishing and malware attacks on operational technologies?

NCC Group has developed machine learning technology

FIND OUT MORE >

Machine learning, a type of artificial intelligence, is one of the most promising new technologies.

NCC Group has developed machine learning technology to detect anomalies in a network, which could be security threats. This means looking at a network to see what is normal and then when something abnormal happens flagging it. This technology is gaining a lot more traction and becoming more feasible for businesses.

Machine learning looks especially promising for OT environments due to network communications and the general behaviour of systems being more predictable than in IT environments, with a more diverse user base. That makes it easier to detect anomalies because the baseline is more stable.

Buying new technologies isn’t a magic solution to evolving cyber security threats. It’s often unnecessary.

Most organisations already have more than enough technologies and procedures to deal with changing security threats.

Much of the proven security technology is built into companies’ existing IT systems. The key thing is to use threat intelligence to protect yourselves and configure your platforms. Your first step should be to invest time in understanding the security threats facing your organisation. After you’ve done that, you can update your security to fix any weaknesses – and better protect your organisation.

The key thing is to use threat intelligence to protect yourselves and configure your platforms.

About Insights

nccgroup

Insights is a program designed for sharing pragmatic cyber security insights with senior executives. You can expect a magazine and interactive online event about a trending topic each quarter. Register here for the free virtual Insights event: Growing Threats.

About NCC group

It's a new era of risk. Defy it with NCC Group's end-to-end cyber security and resilience solutions, and confidently embrace technology to support sustainable growth and success.

From governments to tech giants, financial institutions to expanding businesses, for over 30 years we have proudly provided them with strong security solutions...and with a global team of over 2,400 experts, we're ready to do the same for you.

With NCC Group, take your business to the next level. Unleash innovation without the obstacle of cyber threats.

More than a solution. **A partner.**

You're not alone on your security journey. NCC Group is your partner. Be it rolling up our sleeves with your in-house team or developing strategy with your board, we help you have control over your appropriate level of security. Yes, we deliver industry leading security solutions, but we'll also reduce stress, save your business time, and help you prepare for, or even face, a crisis together.

www.nccgroup.com