Sneak Preview: N-able and DNSFilter Integration

By Jay Pitzer
Security

Two million—that's the rough number of new phishing sites found by Google in 2020. It makes sense this activity would pick up. News events in 2020, from the elections to the pandemic, made it easier for cybercriminals to take advantage of the confusion.

RELATED PRODUCT

N-central

Get that single view of network operations that will help you manage all client systems and conquer IT complexity.

Some phishing sites are obvious fakes. But cybercriminals have grown increasingly adept at creating expert-level forgeries that can trick even the most seasoned security professional, let alone a less savvy user. And it goes beyond sites aimed at stealing someone's personal information—some fake sites can automatically launch malicious scripts or start a ransomware drive-by download.

That's why we're proud to announce our partnership with DNSFilter. DNSFilter provides next-generation protection against malicious sites and will soon be integrated within N-able™ N-central®. (We are also actively working on an RMM integration.)

Why DNS filtering?

Cybercriminals have an advantage over the average person. They know at least a few people will click if they send out a large volume of emails, texts, or social media posts. From there, the victim can easily get taken in by a reasonably convincing website. The fake website can either seek to have a user give up personal details or it can cause them to unwittingly download malware onto their local machine.

While some malicious sites may seem like obvious fakes, cybercriminals have grown increasingly adept at creating near-perfect forgeries of certain websites. People can easily fall victim to these, particularly if they're in a state of mind conducive to making automatic decisions, such as when they're tired, facing time pressure (e.g., "act now to avoid an IRS audit"), or fearful.

The pandemic unfortunately offers a striking example of how cybercriminals can take advantage of users during a time of both fear and confusion. As people seek information on vaccines, they're often confused by news accounts, afraid of getting the wrong vaccine, and frustrated at the length of time they've spent dealing with lockdown and quarantine orders. These often cause people to no longer think critically when receiving an email or text. Some common scams around this involve ads trying to trick people into signing up for early vaccine access or sending "vaccine appointments" through what appear to be event marketing sites. Even if someone doesn't click to a site seeking personal information, they could easily land on a site that then downloads malware.

While user training helps, the previous examples show training isn't a panacea. Instead, you want to augment these methods with content filtering. Traditional content filtering systems will check the URL or IP address of a site against a list of

known malicious sites in its database and, if it finds a match, block the page from loading for the end user.

This certainly helps for known sites. But there's a problem—as the stat in the opening paragraph shows, we're seeing new malicious sites coming online at a frenetic pace that makes it hard for the industry to keep up.

DNSFilter uses artificial intelligence to analyze sites across a number of dimensions to determine if they're malicious. For instance, rather than a static web content filtering database, DNSFilter analyzes everything from URLs to logos to favicons to help detect malicious sites. It can even check for behavioral issues such as launching a malicious download without user interaction. This allows DNSFilter to categorize sites as malicious in real-time.

Beyond dealing with the proliferation of malicious sites, DNSFilter is also particularly useful in the current environment where many people work remotely. Often, a lot of this filtering would happen at the network firewall level. However, with more people working from home we can no longer rely on the corporate network to protect end users. An endpoint-based content filtering solution helps keep users safe wherever they sit.

The benefits for MSPs

Our partnership with DNSFilter will help MSPs take a proactive approach toward keeping users away from malicious sites. Once we release the integration in N-central (and RMM after that), you can add a new important service to help secure your customers and operate it from the same dashboard you use to remotely manage and help secure the rest of your customers' IT estates. On top of that, you'll be able to report on any malicious sites blocked for your customers, helping you reinforce the value of your services.

The DNSFilter integration is coming soon. We hope you're as excited about it as we are about offering it to you.