OPSWAT.

USE CASE

Disarming Malicious Emails and Attachments

Why Other Email Security Are Inefficient Against Zero-Day Attacks

Table of Contents

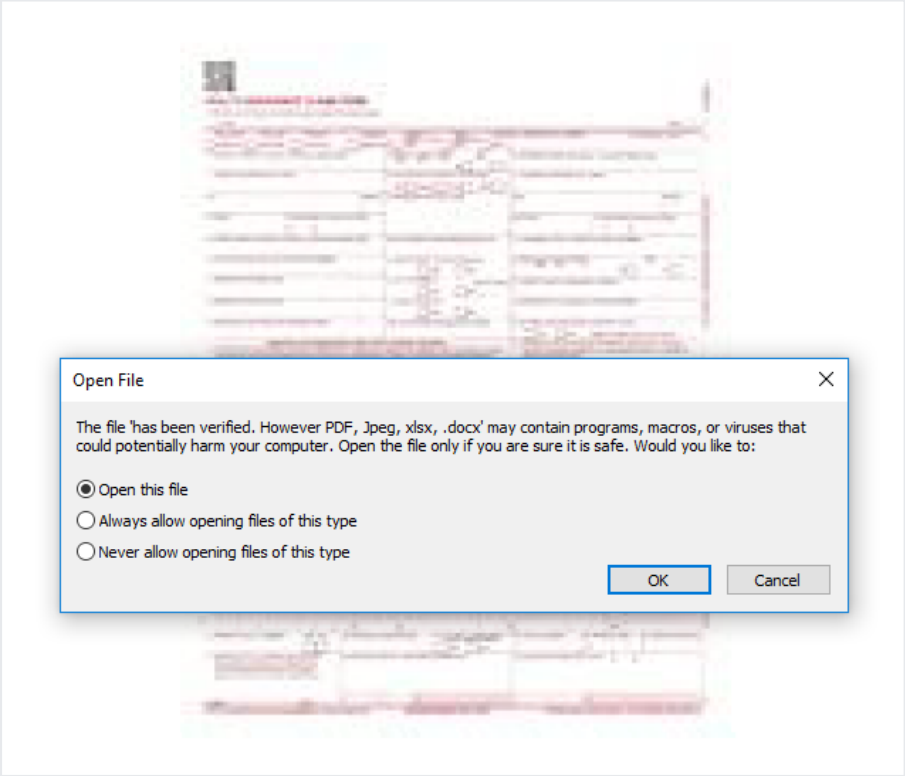
An Emerging New Threat: Attacks with PDF Attachments

Email security should be a top priority as it is still the number one initial attack vector for data breaches, according to IBM. Despite this, sophisticated email attacks continue to effectively take their victims, exploiting the human factor, which has been involved in 82% of all breaches this year. Unfortunately, a malware distribution campaign using PDF attachments has been identified in the last month, with hackers finding a new way to smuggle malware onto victims' devices.

How The Attack Happened

The new cybercrime campaign, discovered by HP Wolf Security, leveraged unsuspecting user behavior to distribute the Snake Keylogger onto vulnerable endpoints by PDF files.

The threat actors first sent an email with the subject line Remittance Invoice to trick the victims into thinking they'll be getting paid for something. When the PDF was opened, Adobe Reader prompted the user to open an embedded document, a DOCX file which contained malicious codes. The confusing thing is that the embedded document is named *has been verified*. This makes the victim think that the PDF reader has scanned the file and it is ready to use.



The Word file is likely to contain a macro that, if enabled, will download a rich text file (RTF) from a remote location and run it. The file would then attempt to download the Snake Keylogger malware.

For most cyberattacks to succeed, the targeted endpoints must still be vulnerable to unknown vulnerabilities. However, this time, attackers did not send the malicious code but tricked the victim into downloading it, bypassing detection-based gateway defenses.

The cybersecurity community believes that many of the security breaches were avoidable. For instance, the current flaw was identified in 2017 and the recent series of attacks could have been prevented if all device administrators keep their operating systems up to date.

According to Verizon's DBIR, there are four major paths to corporate information: credentials, phishing, exploiting vulnerabilities, and botnets. Failing to block just one of the paths can lead to network intrusions. In this case, the attackers used two elements to execute an attack: a well-choreographed email phishing scam to mislead unsuspecting users, and an exploited vulnerability to install malicious files.

Commonly Used Protection Measures

Since the new cybercrime campaign used email to distribute the Snake Keylogger to vulnerable endpoints via PDF files, traditional security best practices would not have worked properly due to the following reasons:

- Exploits for vulnerabilities emerge in days, but it takes organizations weeks or months to patch.
- Traditional email security solutions struggle to prevent zero-day attacks since no anti-virus signatures exist to detect them.
- Sandbox solutions have emerged as one approach for advanced threat detection, but they are not well-suited for email since they require additional processing time before delivery.
- Beyond the negative impact on productivity, certain email security threats can evade sandbox detection.

In this case, these two methods were applied:

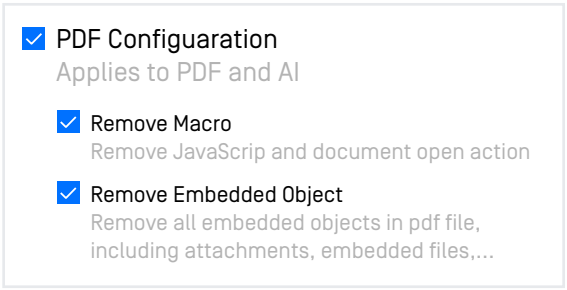
1. Action-Delayed Execution

If hackers want to make sure their malware doesn't execute in a sandbox environment, a common approach is to wait for end-user interaction. This could be the click of the mouse, typing on the keyboard, or opening a specific application. Their options are, unfortunately, extremely varied.

2. Trojans and Macros

Trojan files are almost as old as ancient Greece, so anti-virus and sandboxing solutions can detect quite a few types of Trojan files. Detection-based solutions tend to fail once the malware is hidden in macro-enabled Microsoft Office documents. The only downside of macro-based attacks is that they require the end-user to enable them, so they are frequently paired with a social-engineering attack.

The Zero-Trust Philosophy



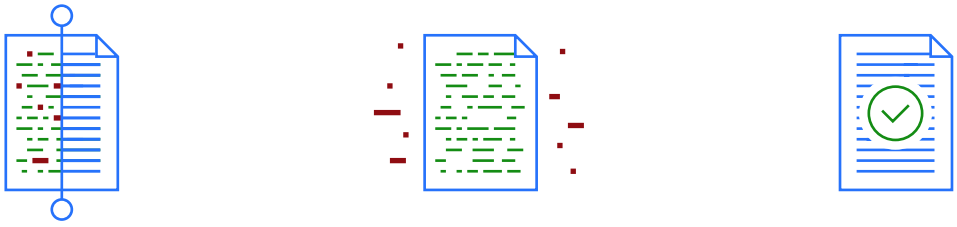
Organizations should assume that all emails and attachments are malicious. Common productivity files, such as Word documents or PDFs, may be infected with malware and zero-day attacks. However, it is unrealistic to block access to email or Word documents. Anti-virus and sandbox solutions are limited by their ability to detect advanced attacks. As we have seen with the attack above, using only detection-based protection is fundamentally a flawed approach. Instead, organizations should adopt a zero-trust security approach with a proactive solution called CDR, which treats all files as malicious and cleans them in real-time. A sanitized version of the documents can be immediately delivered to the user without hindering productivity. Meanwhile, organizations can conduct further detection-based analyses for hard-to-find threats. Once these analyses are done and threats neutralized, the files are restored to their original states and delivered to the users in full.

What is CDR?

CDR stands for content disarm and reconstruction. CDR, also known as data sanitization, is an advanced threat prevention technology that does not rely on detection. It follows the zero-trust philosophy and assumes all files are malicious. It also sanitizes and rebuilds each file to ensure full usability with safe content. This means that files are dissected and anything that has the potential to be dangerous is removed—and then the file is reassembled. CDR Technology is highly effective at preventing known and unknown threats, including zero-day targeted attacks and threats that are equipped with malware evasion technologies, such as Fully Undetectable Malware, VMware Detection, Obfuscation, and many others.

How Does CDR Work?

CDR follows a three-step process:



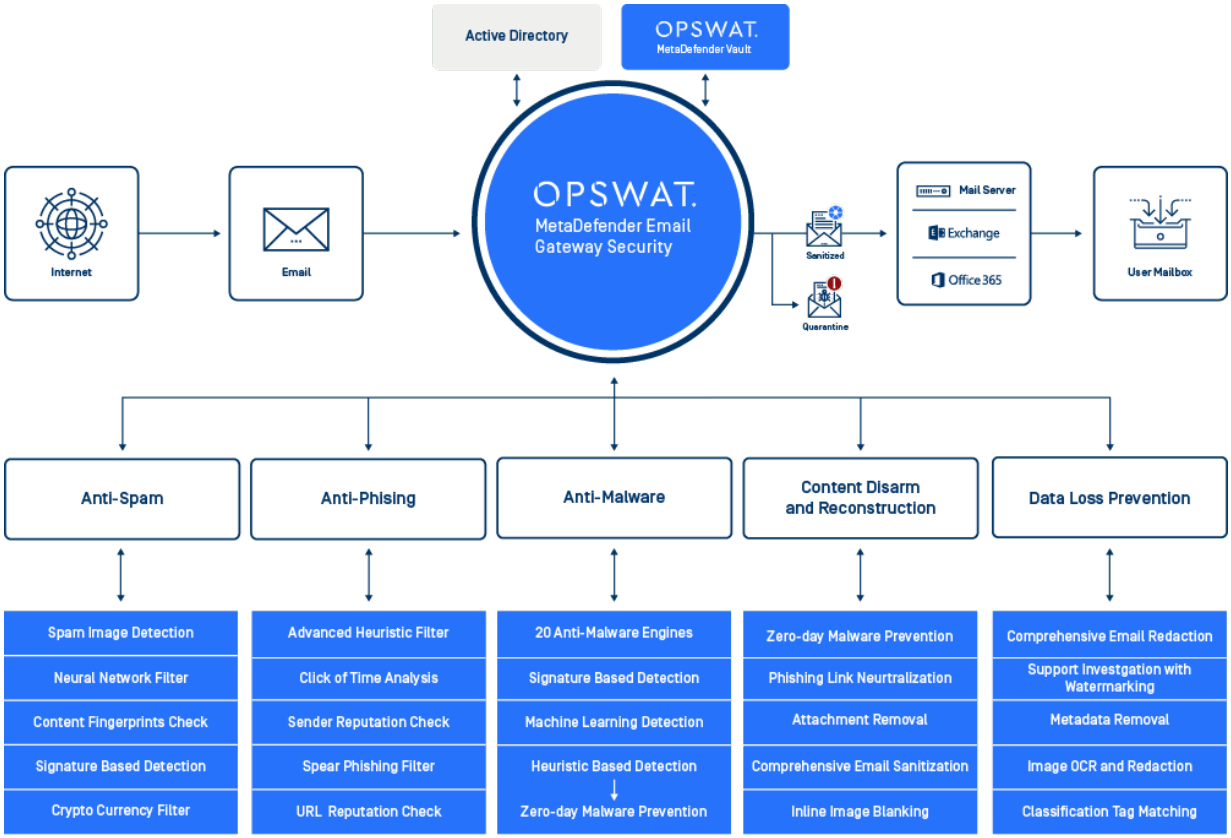
1. Verify file type and identify all active embedded content in the file
2. Remove all potentially malicious content and reconstruct the file with only its legitimate components
3. Use regenerated threat-free file with full functionality and quarantine the original file

Using CDR Technology in Email Security to Combat Zero-day Threats

MetaDefender Email Gateway Security is the solution to these types of threats. It provides a comprehensive approach to disarming attachments, email bodies, and headers by removing all potentially malicious content and reconstructing it as a clean file. Thus, these files are fully usable and secure, providing adequate protection for users against the attacks described above.

OPSWAT protects organizations from exploits and weaponized content without the need for detection.

Our solutions are 30 times faster than sandbox detection as well, making them the premier choice for high-pressure OT environments and critical infrastructure.



About OPSWAT

To learn more about how you can fill email security gaps to protect your organization from advanced threats, **download our free whitepaper**, "Best Practices for Email Security and Critical Infrastructure Protection".