5 Dangerous File Types and How to Mitigate the Risks

Introduction

In the world of bring-your-own-device (BYOD) policies and the internet of things (IoT), we can open files on many types of devices. You probably know that opening files or attachments on any device that isn't properly secured can put you and your company at risk—but how do you know which files might be malicious? For that matter, what is the best way to counter them? Many breaches and infections start with an internal user innocently opening a legitimate-looking file.

This paper discusses some of the most common file types adversaries are using to infiltrate organizations. It's critical to understand how attackers are using these files and the steps you can take to mitigate related risks. We will look at the current state of the threat landscape, discuss some prominent malicious file types, and lay out some best practices for protecting your organization.

Threat Landscape Overview

In 2019, the global average cost of a data breach was US$3.92 million,[1] a 1.5% increase from 2018. This shows that threat actors have no intention of slowing down. With increasing attack volumes and the development of more sophisticated tools and tactics, the threat landscape has become immeasurably broad. Every new device, operating system, and piece of software developed potentially expands the attack surface area, creating new threat vectors for adversaries to exploit.

As threats grow in sophistication, cybersecurity companies are developing many tools and technologies to keep pace. With improvements in security posture at the organizational level, however, employees and their endpoints are increasingly becoming targets. According to the 2019 Verizon Data Breach Investigations Report, email was the most common point of entry for malware delivery.[2] It's clear that adversaries are relying on human judgment. If they are able to exploit human vulnerability, it's game over.

Attackers are creating and delivering malware on a massive scale, typically through automated means. Malware toolkits, coupled with specialized delivery services, have made it easy to quickly deploy thousands of malicious files around the globe. Palo Alto Networks tracked the global delivery of one malware family and observed more than 45,000 unique sessions within only 30 minutes.

For many organizations, breaches begin with seemingly innocuous, business-related file types combined with various ways to trick users into opening them. Knowing these potentially risky file types, and the tactics adversaries use to compromise a network, is crucial to developing a mitigation strategy that will safeguard your organization's data, users, and reputation.

Top 5 Dangerous File Types

Portable Executable

Portable executable (.PE) is a format for executable files, object code, and Dynamic Link Libraries (DLLs) used in 32-bit or 64-bit Windows® operating systems. While the common executable file extension is .EXE, a multitude of files with different extensions—such as font (.FON) or screensaver (.SCR) files—behave no differently from executable files in the context of the operating system. This is significant because adversaries can leverage these file types to bypass security controls within an organization.

Attackers typically rely heavily on social engineering tactics to deliver malware disguised as legitimate files. For example, a cybercriminal might imitate a trusted vendor and send an email that asks the recipient to review an attachment. The attachment contains a malicious file coded to display a .PDF icon with an .EXE file extension. However, because Windows hides the extensions of known file types by default, the victim will simply see the icon and assume the file is legitimate. Once the victim executes the attachment, the adversary's first objective is complete. Many email systems can prevent the delivery of .PE files, so adversaries may instead deliver emails that contain a URL hosting malicious files on external resources. Adversaries also frequently leverage encryption to bypass security controls an organization may have in place.

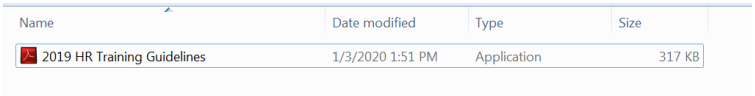

Figure 1: An .EXE file with a .PDF icon

Android Package Kit

Android Package Kit (.APK) is a format for archive files that the open source Android® operating system uses for the installation and distribution of mobile applications. With more than 2.5 billion active Android devices worldwide,[3] this extremely large attack surface is very enticing for threat actors. Given the popularization of BYOD policies, organizations should be cognizant of the risk of employees downloading apps laden with malicious code. A compromised device could lead to stolen credentials, data theft, and lateral movement across the network.

To succeed, malicious .APK files typically require human interaction. For example, an employee could receive an email, seemingly from HR, announcing a new HQ app for ordering lunch in the office. The legitimate-looking email prompts the victim to download the app via the link provided.

Google does have security controls within the Google Play® Store, where most users download applications, but it is also possible to install apps from third-party sources, which introduces risk. Moreover, there have recently been multiple high-profile instances of seemingly legitimate applications being removed from official app stores due to the inclusion of malicious code. In January 2020, for instance, Google confirmed that it had removed around 1,700 apps from the Google Play Store for carrying the Joker malware, which signed victims up for subscription-based services without their knowledge.[4]

Portable Document Format

Portable Document Format (.PDF) is a format that provides an electronic image of text and/or graphics that can be viewed, printed, and electronically transmitted. In addition to text and graphics, .PDF files can also contain interactive elements (e.g., blank text fields, hyperlinks) and higher level application data. In 2019 alone, 250 billion .PDF files were opened in Adobe products,[5] making this one of the most popular and ubiquitous document types in business today. Consequently, it can be a dangerous tool in cybercriminals' hands.

1. Larry Ponemon, "What's New in the 2019 Cost of a Data Breach Report," Security Intelligence, July 23, 2019, https://securityintelligence.com/posts/whats-new-in-the-2019-cost-of-a-data-breach-report.
2. "2019 Data Breach Investigations Report," Verizon, May 8, 2019, https://enterprise.verizon.com/resources/reports/dbir.
3. Russell Brandom, "There are now 2.5 billion active Android devices," The Verge, May 7, 2019, https://www.theverge.com/2019/5/7/18528297/google-io-2019-android-devices-play-store-total-number-statistic-keynote.
4. "Google Confirms 'Malicious' Security Threats Hiding On Play Store: Delete These 12 Apps Now," Forbes, February 21, 2020, https://www.forbes.com/sites/zakdoffman/2020/02/21/google-confirms-malicious-security-threats-hiding-on-android-play-store-delete-these-12-apps-now.
5. "Adobe Fast Facts," Adobe, January 2020, https://www.adobe.com/content/dam/cc/en/fast-facts/pdfs/fast-facts.pdf.

Cybercriminals routinely use .PDF files to lure victims into downloading and executing malicious payloads. Attackers can embed encrypted objects and code in .PDF files to circumvent traditional analysis methods. Once a user opens an infected file, these hidden objects can be executed and give the adversary the opportunity to run malicious code.

Microsoft Office Documents

Most businesses rely on Microsoft Office documents to run day-to-day operations efficiently, and cybercriminals also favor the use of Office applications to compromise Windows PCs en masse. Verizon's 2019 Data Breach Investigations Report touts that 94% of malware was delivered via email, with 45% of it contained in Office documents.[6] By disguising malware this way, threat actors can bypass legacy security controls. In most instances, fraudulent Office documents contain malicious macros (i.e., scripts that contain commands for automating tasks in various applications) or embedded objects. Office applications such as Word and Excel support macros written in Visual Basic for Applications (VBA), which can be used for malicious activities.

Microsoft has put protections in place to mitigate the use of malicious macros but cannot remove support altogether since macros are still used for legitimate purposes. Consequently, threat actors exploit this function through social engineering to trick victims into enabling macros. Adversaries have also developed new methods of delivering malicious code, such as leveraging Object Linking and Embedding (OLE) functions within Microsoft Office Suite.

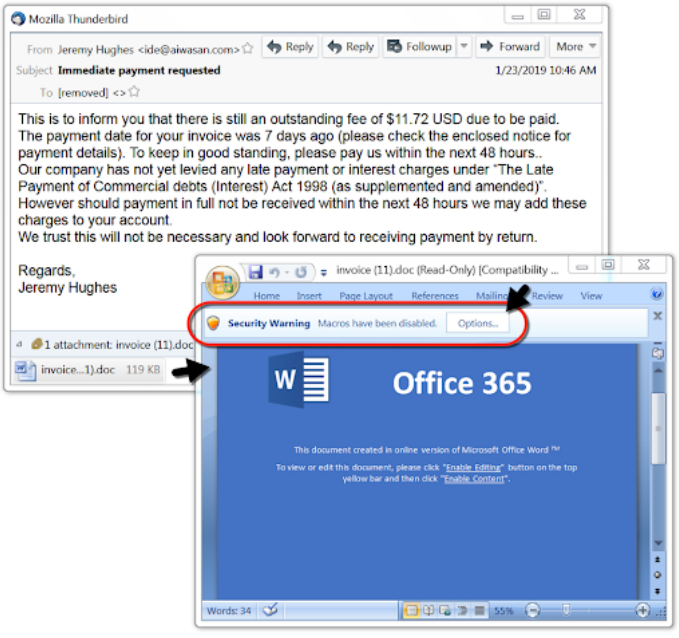

Figure 2: Phishing email containing a malicious Word document

PowerShell

PowerShell® is a scripting language that uses the extension .PS1. Originally designed to automate Windows administrative tasks, PowerShell has become a powerful and efficient tool for automation and optimization, used by administrators, IT, and sometimes developers. Of course, threat actors have discovered the power and flexibility of PowerShell as well. It should be noted that PowerShell scripts are rarely delivered as is, but rather embedded in Microsoft Office formats. This additional layer lets attackers easily avoid detection by traditional security tools.

An attacker may use a mass mailer to send a malicious email to many individuals, which could result in several employees in a given organization receiving the same email. See figure 2 for a typical example. A document attached to such a message can contain malicious macros that, once enabled, will launch PowerShell, which then executes scripts in the background to fetch and install malware. Even though PowerShell does not allow scripts to be executed by default, threat actors can get around this by, for instance, altering run parameters to allow a given instance of PowerShell to run scripts, or by using base-64 encoding to obfuscate the script, making it difficult for static analysis to detect.

Mitigation Techniques

It would be impossible to block every risky file type without impeding business productivity, but organizations with the right tools and tactics in place can avoid many of these threats. Here are some practical steps you can take to reduce the attack surface and mitigate risk.

1. Enable File Blocking

Blocking high-risk file types commonly used to carry malware is one of the first steps to reducing your attack surface without hindering user experience. Palo Alto Networks Next-Generation Firewalls use file blocking profiles to block specific file types over specified applications and in the specified flow direction—inbound, outbound, or both—as set by an administrator. Administrators can also configure custom block pages that will appear when users attempt to download a blocked file type. This allows users to carefully consider whether or not to download potentially malicious files.

You can also segment file blocking to prevent or allow certain downloads based on a user's role or groups. For instance, you can block downloads of .FON files by employees in Accounting but allow them in Marketing. Palo Alto Networks User-ID™ technology enables you to identify all users on your network and enforce user- and group-based policies on the firewall. This greatly reduces your attack surface and risk exposure without impeding daily business activities.

You can also combine file blocking with URL Filtering to enhance security around potential downloads. URL Filtering automatically blocks known malware sites, phishing sites, and adult content sites. Customizable URL profiles allow you to determine specific websites that should always be blocked or allowed, helping you monitor and control how users access the web over HTTP and HTTPS.

6. "2019 Data Breach Investigations Report," Verizon, May 8, 2019, https://enterprise.verizon.com/resources/reports/dbir.

2. Enforce SSL/TLS Decryption

Encrypted traffic, increasingly prevalent today, is a double-edged sword. On one hand, some encrypted traffic is protected by privacy regulations: Healthcare, government, military, banking, and online shopping traffic can contain personal data and, therefore, should remain encrypted. On the other hand, traffic visibility is crucial for file blocking and malware analysis to fight both commodity threats and sophisticated attacks—not knowing what hides in encrypted traffic can leave organizations blind to simple things like accidental downloads of malicious files.

To protect privacy and keep modern environments secure, selectively enabling Secure Sockets Layer (SSL) and Transport Layer Security (TLS) decryption is critical. Palo Alto Networks Next-Generation Firewalls make it easy to determine which URL categories to leave encrypted while decrypting all other traffic. Combined with URL Filtering, this prevents users from visiting risky websites, such as those with self-signed, untrusted, or expired certificates, in addition to blocking websites using vulnerable encryption protocols, such as TLS 1.0, or weak cipher suites (specified in the SSL handshake). Our Next-Generation Firewalls allow you to configure the TLS versions and cipher suites that must not be allowed.

3. Automatically Analyze Allowed Business File Types

Today's automatically generated threats focus on evading security controls and rendering traditional solutions, like antivirus or email security, useless. On top of that, it's impossible to block every single risky file type since .PDF and .DOC files, among others, are required for many daily business activities. Thus, allowed file types need to be continuously analyzed for malicious activity. Unfortunately, manually analyzing files with traditional security solutions is ineffective and unscalable.

The cloud-delivered WildFire® malware prevention service uses data and threat intelligence from the industry's largest global community, applying advanced analysis to automatically identify unknown threats and stop attackers in their tracks. With WildFire, you get immediate, automated protection across the network, stopping malware, malicious URLs, command and control, and attacks that leverage DNS. WildFire keeps your organization safe without any operational impact on Next-Generation Firewalls or other Palo Alto Networks services.

You can get deeper threat information, including attribution and context, with AutoFocus™ contextual threat intelligence service. With intelligence from the global user base of WildFire customers, you also get the "community effect"—once a given attack campaign has been analyzed in any WildFire instance, protections are delivered to customers worldwide.

WildFire can analyze and automatically deploy protections for a multitude of file types, beyond the five most dangerous ones, as well as malicious URLs and phishing links in emails.

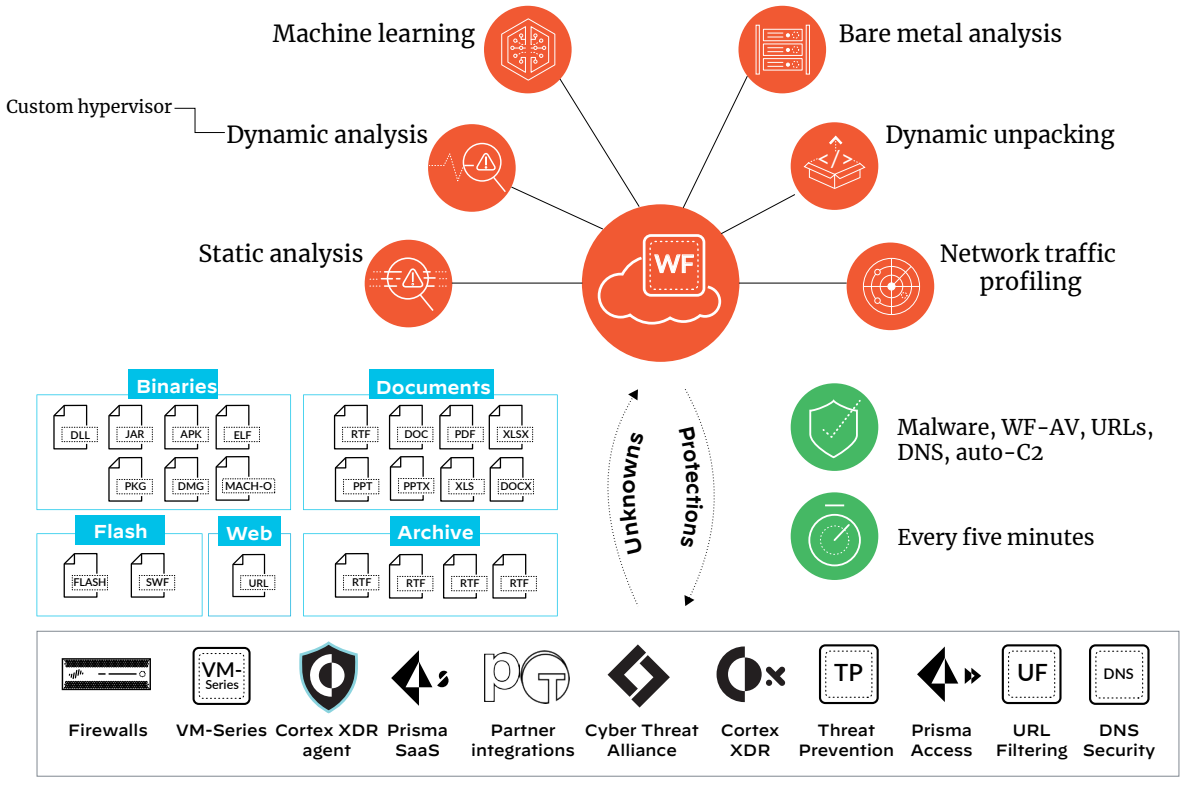

Figure 3: WildFire analysis, sensors, and enforcement points

4. Automatically Prevent Zero-Day Exploits and Malware

Traditional malware analysis and sandboxing techniques simply can't keep pace with modern exploits. Many of the tools and tactics used to deliver malware embedded in common file types have become more sophisticated and evasive. WildFire goes beyond legacy technology to keep you a step ahead. Using shared community-sourced threat data and advanced analysis, it immediately shares protections across the network, endpoint, and cloud.

You get peace of mind knowing WildFire automatically delivers protections every five minutes to prevent successful cyberattacks, including malicious files. Moreover, WildFire reduces the volume of alerts and data your analysts need to manually process, freeing them up to prioritize more critical work. Finally, with regional clouds, WildFire can handle information that falls under regional privacy regulations, such as the General Data Protection Regulation (GDPR) or California Consumer Privacy Act (CCPA).

WildFire®

33,000+ customers with thousands more every quarter

230,000 daily protections delivered to the Security Operating Platform® within 5 minutes

1.1M+ malware variants covered with just one protection

5. Take a Best Practice Assessment (BPA)

Even with the right tools and technologies, it can be difficult to know if your security posture is following best practices. Protecting your organization from malicious files requires properly configured policies and tools. To help you ensure your security is where it should be and maximize your investment, Palo Alto Networks offers the Best Practice Assessment (BPA). This free evaluation analyzes your configurations to pinpoint exactly how well each capability measures up to best practices.

The assessment consists of two parts: the assessment itself and the Security Policy Capability Adoption Heatmap. The heatmap analyzes how your organization is using security capabilities across your architecture. Using a tech support file, the heatmap breaks down the data into percentages so you can determine, of all of the rules enabled, what portion of them are actually applying valid profiles throughout the platform. Once you've analyzed and measured your adoption, you'll want to verify that things are configured in the best possible way.

To ensure your configurations are optimized, the BPA produces a curated set of recommendations to improve your Next-Generation Firewall and network security policies. The BPA is great for building confidence in your controls and measuring progress along the way. You can run assessments on demand to track your adoption of core prevention capabilities, such as App-ID™, User-ID™, and SSL Decryption, all of which can help prevent risky file types from penetrating your organization. Continuing to optimize your security tools will ensure you're in the best position possible to mitigate attacks.

Putting It All Together

With 41.6 billion devices expected to be connected to the internet by 2025,[7] accidents are bound to happen. Without the right security in place, a malicious file or link puts your users, your data, and your company at risk. Since it's impossible to simply block all file types from your organization, you need to take the proper precautions to mitigate the risks of potentially malicious file types infecting your organization. By deploying a Next-Generation Firewall with capabilities such as WildFire, Threat Prevention, and URL Filtering, as well as incorporating file blocking, decryption rules, and continuous monitoring of allowed file types, you can significantly reduce the risks. Whether from risky file types or malicious links, you can be confident that Palo Alto Networks products will safeguard your data and protect your network.

Visit us online to learn more about our Next-Generation Firewalls and WildFire.

7. Carrie MacGillivray and David Reinsel, "Worldwide Global DataSphere IoT Device and Data Forecast, 2019-2023," IDC, May 2019, https://www.idc.com/getdoc.jsp?containerId=US45066919.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com