VOTIRO

Malicious Macros:

The Holes in Microsoft Software That Hackers Hope You Don't Know About

Table of Contents

Malicious Macros:

The Holes in Microsoft Software That Hackers Hope You Don't Know About

A macro is a mini program that is designed to automate a task within a larger program in order to make the user experience faster and easier. Macros are a legitimate and important component of any productivity software, including common Microsoft Office software for creating documents, spreadsheets, and presentations. Macros for Microsoft Office are currently written in Visual Basic for Applications (VBA) and work within most Office programs for both Windows and Macintosh, including Word, Excel, Outlook, PowerPoint, Project, Access, Publisher, and Visio. Unfortunately, these efficiency-drivers are easily compromised by hackers. Cybercriminals have figured out that by hiding their malicious code inside Office macros, they have a good chance of tricking a victim into triggering the payload.

What's a

Malicious Macro?

Macro malware – also known as macro viruses – take advantage of the VBA programming in Microsoft Office macros to surreptitiously inject a user's system with malware. Cybercriminals embed malicious code in the macros, causing the malware to run as soon as the macros are opened. Trend Micro reports that Microsoft Office files are the most common file types used in targeted attacks. Microsoft itself admits that 98% of threats targeting its Office Suite use macros.

98% of threats targeting its Office Suite use macros

How Are

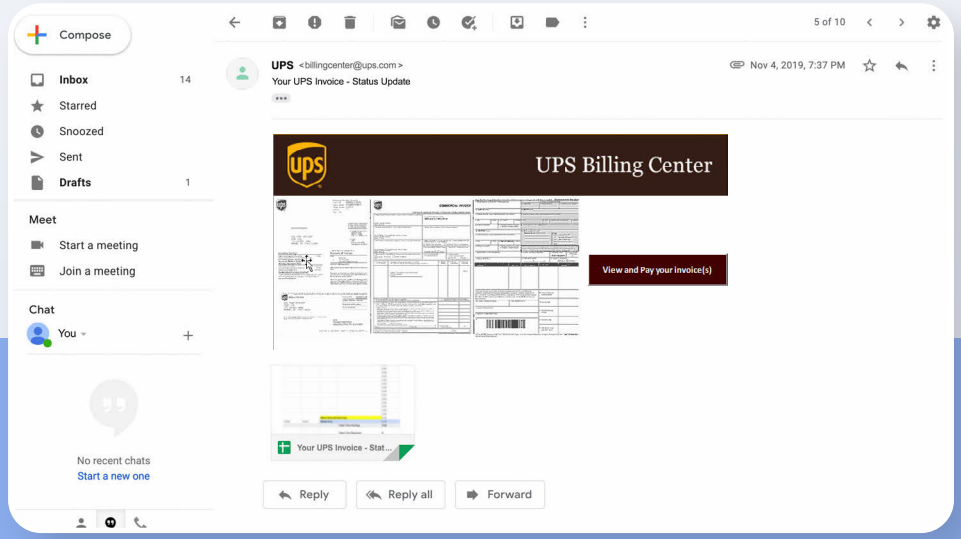
Malicious Macro Viruses Delivered?

More than a decade ago, macro malware was a common attack method because Microsoft Office software allowed macros to execute automatically whenever a document was opened. In current times, Microsoft has fixed this vulnerability and macros are disabled by default. This means hackers must find creative ways to convince users to **enable macros** so that their malware can execute.

Oftentimes, hackers use social engineering methods to transmit macro malware through phishing emails containing malicious attachments. In fact, a 2019 report by Verizon indicates that 94% of malware was delivered via malicious email attachments. Symantec adds that 48% of malicious email attachments are Microsoft Office files.

These attachments use names that are intended to fool people into opening them, sometimes appearing as bills, delivery information, or legal documents, among others. When the user opens the attachment, there is often some innocent-looking content and a request for the user to enable macros. When the macro is enabled, malware can spread quickly and infect Office files. For example, the virus can corrupt text documents, compromise stored data, or gain access to the user's email contacts in order to further spread the malware. A wide range of external payloads can be retrieved from remotes URL, including ransomware, banking Trojans, or backdoors into enterprise networks.

These phishing attempts are hitting their mark. 62% of businesses experienced phishing and social engineering attacks in 2018, according to Cybint Solutions.

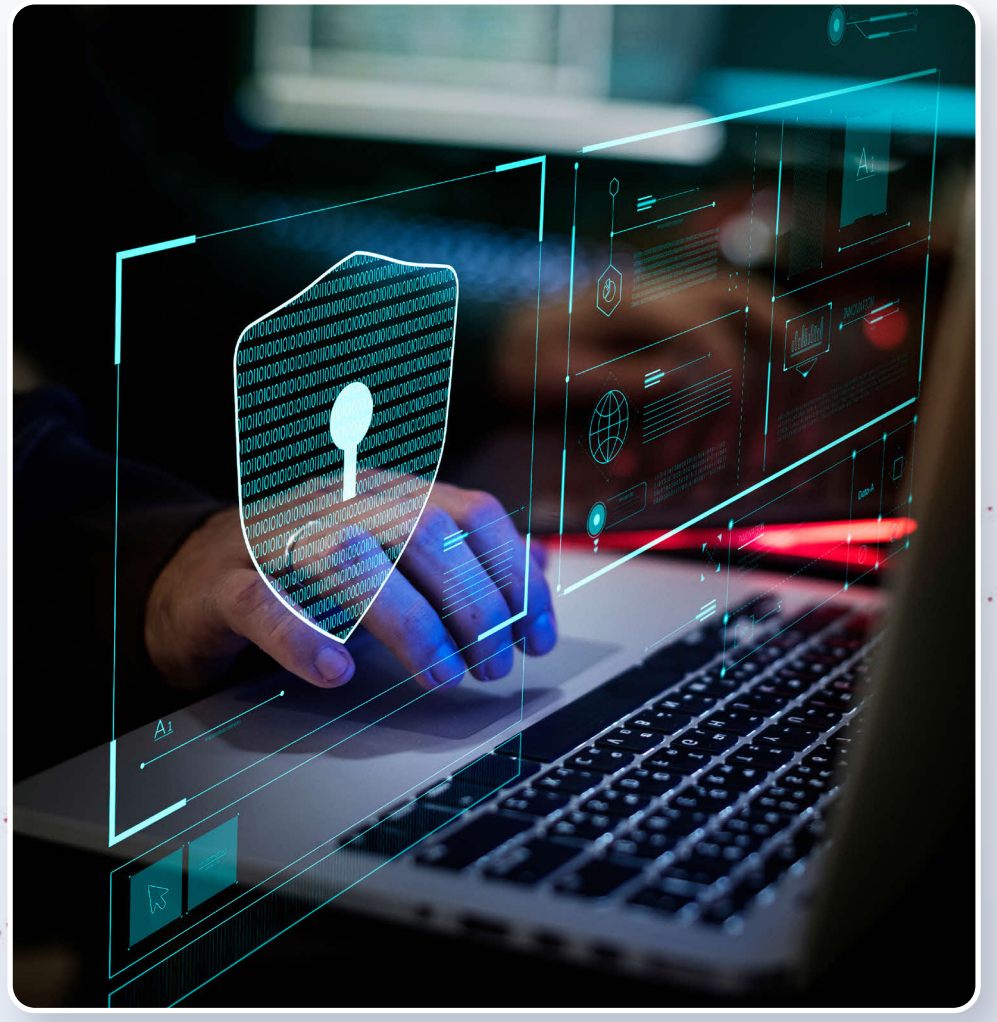


Example of phishing email with malicious attachment that looked like it originated from the UPS delivery service. The hackers placed the payload—the macro—inside the Excel spreadsheet, which then injected the ransomware into the user's machine.

Why Macro Viruses Have Become

the Weapon of Choice for Hackers

Microsoft Office VBA macros are an especially attractive target for cybercriminals because the attack surface is so large: Microsoft Office is used by 1.2 billion users. With increasingly advanced social engineering techniques, the likelihood of an unsuspecting user triggering the macro virus is high. In addition, the wide range of macros that can be developed opens the door to a massive amount of zero-day threats — meaning a vulnerability has been discovered but no patch for it has been developed. In fact, zero-day attacks have become more prevalent and are increasing in frequency; new or unknown zero-day attacks are expected to more than double in the coming year, according to the 2020 Annual Study on the State of Endpoint Security Risk by the Ponemon Institute.



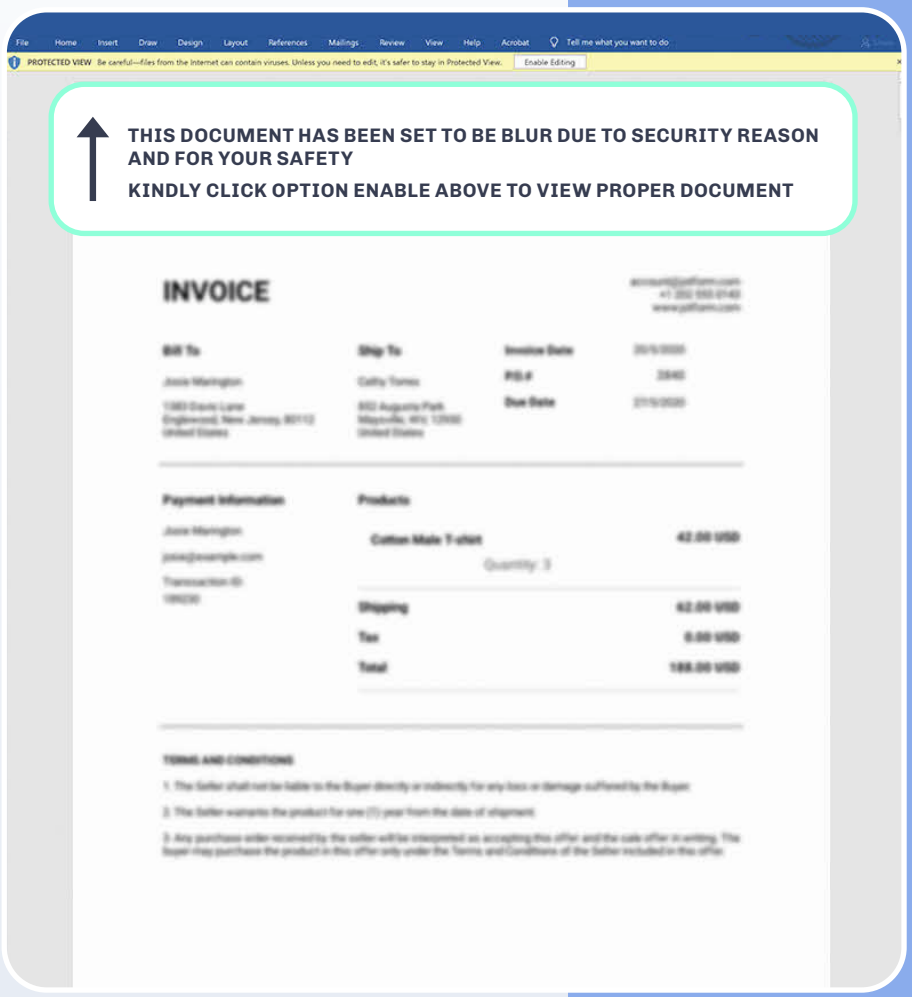
History of

Macro Viruses

The first macro virus—known as Concept—appeared in July 1995 and targeted Microsoft Word. The first macro virus targeting Excel —XM_LAROUX— appeared shortly thereafter. When enabled, both macros displayed a dialogue box with cryptic text and the OK button, but with no additional payloads. In 1999, a macro virus called Melissa was one of the first to be weaponized and become widespread. When a user opened the malicious Microsoft Word document, the virus accessed the user's Outlook account and mass-emailed itself to the user's contact list, impacting the performance of business email servers worldwide.

After Microsoft began making security updates to Office, hackers focused their efforts elsewhere and macro-based malware attacks declined. Then, starting in 2014, they began to make a comeback with at least 75 different variants appearing in one year. For example, in the Napolar/Solarbot trojan attack, a blurred image is placed within the document, using the social engineering concept of curiosity to entice the user to enable the macro in order to see the image. Sometimes instructions for enabling the macro is provided, along with an arrow pointing to the right button to click.

According to Proofpoint, there was a 600% increase in email attachment malware attacks from 2014 to 2015. Since then, these file-borne macro attacks have increased as attackers developed more sophisticated social engineering tactics to trick their targets. Today, this macro malware poses an increased threat to cybersecurity.



Source:
https://www.virusbulletin.com/uploads/pdf/magazine/2014/vb201407-VBA.pdf

Recent

Macro Virus Attacks

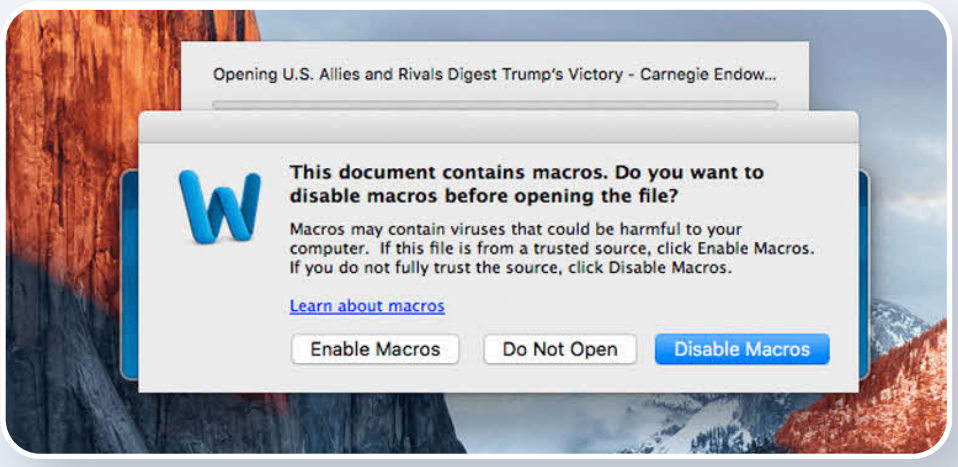
In February 2017, Mac users received emails with a Microsoft Word attachment entitled, "U.S. Allies and Rivals Digest Trump's Victory – Carnegie Endowment for International Peace.docm." When the attachment was opened, the user was prompted with a dialog box to enable macros. Once macros were enabled, the malicious payload would download malware from an external website controlled by the attackers.

In September 2017, the Locky ransomware launched 20 million email-based malicious macro attacks in a single day. The emails looked like they were originating from Herbalife in order to trick recipients into opening the malicious attachment. The hackers continuously changed the names of payload files and the domains used for downloading secondary payloads in order to stay ahead of anti-virus engines.

In June 2019, hackers exploited an **old Microsoft Office vulnerability** to install a trojan via emails carrying malicious RTF documents. The infection targeted Windows users who did not have the 2017 patch installed, enabling the attack to execute when users opened the RTF document—without requiring them to enable macros first.

Also in 2019, a new campaign appeared that used malicious macro functions in an Excel attachment to compromise Windows PCs even though they had been properly patched. When opened, the .xls file runs a series of complex macro functions that ultimately downloads and runs the notorious FlawedAmmyy RAT (remote-access trojan). The virus runs directly in memory, which allows the malware to avoid detection from antivirus products that scan files only on disk. This campaign, attributed to the well-known TA505 group, targeted Korean-speaking Windows users, while similar campaign s targeted users in Chile, Mexico, China, and Taiwan.

Most recently, since the COVID-19 outbreak in the first quarter of 2020, Trend Micro has reported a significant uptick in phishing and file-borne malware attacks, including those utilizing macro viruses.



What Has

Windows Done to Help Prevent Macro Viruses?

Microsoft has reported experiencing macro malware threats from a wide range of virus families, including Ransom:MSIL/Swappa, Ransom:Win32/Teerac, TrojanDownloader:Win32/Chanitor, TrojanSpy:Win32/Ursnif, Win32/Fynloski, and Worm:Win32/Gamarue.

To combat these threats, Microsoft has changed its default settings in recent versions of Office. In Microsoft Office 2007 and all later versions, if you open a file that contains a macro, the file will open but the macro will be disabled. A message is displayed with the option of enabling the macros in that file if the user is sure the macro is secure. While this is a step in the right direction, not all users understand the danger of enabling macros and hackers are getting better and better and enticing users to enable the malicious macros, as demonstrated in this document.

In March 2016, Microsoft added an additional security feature with the goal of helping to alleviate the problem of malicious macros. System administrators now have the option to completely block macros from executing in Office files downloaded from online sources. Again, while definitely helpful, admins must take action for this feature to be enabled and may choose to allow macros if they are needed for workforce productivity. With over 155 million Office 365 business users as of 2018, the number of professional teams using Admin-permitted macros has never been greater.

In addition, Microsoft has been investing in its own built-in anti-virus product, called Windows Defender, which – like any antivirus product – cannot detect zero-day threats.

What Can You Do to

Prevent Damage From Malicious Macros?

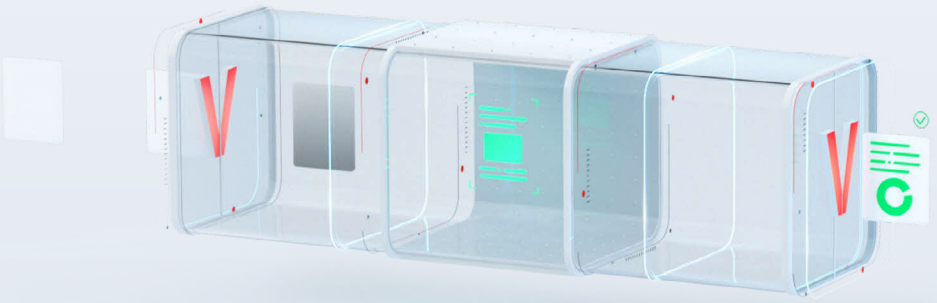
Knowledge is the best weapon when it comes to prevention. Companies are advised to implement phishing training to raise awareness among employees about the possibility of phishing, what phishing looks like, and what not to do when faced with a suspicious email. Every employee must be told never to enable macros from an untrusted source. **However**, even when every employee within the organization – including executives – are educated about the possibility of phishing schemes and how to correctly handle suspicious emails, breaches do still occur.

Send-from email addresses/servers can be spoofed so it appears as if the email is legitimate, or a trusted third-party may be sending a compromised email without even realizing it. Though phishing training will reduce the organization's susceptibility to phishing, it will never result in 100% coverage as there will always be user error, and advanced, sophisticated attacks can trick even cybersecurity professionals.

The only way to stop macro-based threats including zero-day malware that can't be detected by traditional protection solutions is to invest in a solution that neutralizes all malicious elements in any and all incoming files.

Votiro's Secure File Gateway—powered by patented Positive Selection™ technology—is the only file security solution that ensures all files that enter your organization are completely safe. Unlike detection-based file security solutions that scan for suspicious elements and block some malicious files, Positive Selection singles out only the safe elements of each file, so you can be 100% confident that your files are secure.

Built with deep expertise in the architecture of every file format, the Secure File Gateway understands and protects all file types—from .ppt, docs, pdfs and image files, all the way to more complex formats like Autodesk files. With Secure File Gateway you're covered for even the most obscure, challenging file types that no NGAV or Sandbox can possibly detect.



Votiro's Secure File Gateway Solution

- **Same Exact Files, Minus The Risk:** Positive Selection guarantees you receive the exact same file, while getting rid of all potential risk. That way, your file remains 100% authentic and functional, yet 0% dangerous.
- **Nothing But Business:** You won't even know it's there. Unlike other slow, time-consuming solutions, the Secure File Gateway eliminates weaponized files without disrupting your business for even a single moment.
- **Get Rid of The Overhead:** Blocking and quarantining files doesn't just cost your business time. It raises your overhead. With Votiro, you don't block or quarantine anything. Files smoothly enter your organization the instant they're received, drastically reducing your overhead.

Key Features

- ✔ **Fits Right In. Won't Ever Know It's There.**
  - Easy implementation: less than 10 minutes
  - Seamless integration with existing solutions
  - Blazing fast: ultra-low latency
  - Supports both cloud & on-prem
  - Zero training required
- ✔ **Integrates easily into your existing security infrastructure**
- ✔ **Maximizes productivity with zero interruption to business processes**
- ✔ **Runs at sub-second latency and minimal TCO**
- ✔ **Streamlines management with comprehensive dashboard for FTE reduction**

Your Next Step

Experience 100% Secure For Yourself

See for yourself how easy it is to safeguard your organization with the Votiro Secure File Gateway. Sign up for a live demo

About
Votiro

Votiro introduces Secure File Gateway - the only solution that guarantees complete protection from weaponized files. Unlike detection-based file security solutions that scan for suspicious elements and block some malicious files, Votiro's revolutionary Positive Selection technology singles out only the safe elements of each file, ensuring every file that enters your organization is 100% safe. Founded in 2010 by leading file security experts, Votiro's new approach to file security works invisibly in the background, completely eliminating threats while ensuring zero interruption to business.

Votiro is a Gartner Cool Vendor award winner and certified by the International Standard of Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408). Votiro has also been recently recognized as Best CDR Provider by the 2020 Cybersecurity Excellence Awards and named a Bronze winner in the Hot Security Technology Category by the 2020 Infosecurity Products Guide Awards. To learn more, visit www.votiro.com or contact us at info@votiro.com.