COMPUTER NEWS from the

JULY 2017 Volume 5 NO.7

As found on the web and other sources.

Now you can't even trust your mouse!

New Attack Method Delivers Malware Via Mouse Hover

By Kelly Sheridan in Darkreading.com

'Mouseover' technique relies on users hovering over hyperlinked text and images in Microsoft PowerPoint files to drop Trojan.

Researchers have found a new form of attack that abuses the action of hovering over hyperlinked text and images in a Microsoft PowerPoint presentation.

Trend Micro researchers discovered the "mouseover" technique, used by a Trojan downloader also found in a spam campaign hitting EMEA businesses in the manufacturing, education, pyrotechnics, logistics, and device fabrication industries. The downloader they analyzed delivers a version of the OTLARD banking Trojan, also known as GootKit.

"This is the first occurrence of malware using the 'hover' method to initiate a download that we know of," says Mark Nunnikhoven, Trend Micro's VP of cloud security.

GootKit first appeared in 2012 and grew into an information-stealing Trojan with remote access, persistence, network traffic monitoring, and browser manipulation capabilities. It has traditionally been used to steal banking credentials from European financial businesses.

Today's news is less about the capabilities of GootKit and more about its new method of delivery, which is likely to fall under users' radar.

"While GootKit is known malware, businesses should be more concerned about this latest technique as it shows none of the usual indicators of an infected document," he explains. This is novel because it abuses the previously safe user practice of hovering over a link before clicking.

The malware arrives as a spam email disguised as a purchase order or invoice with a malicious PowerPoint Open XML Slide Show (PPSX), or PowerPoint Show (PPS) file attached. These two file types differ from PowerPoint presentation files (PPT or PPTX), which can be edited. A PPS or PPSX file directly opens into presentation mode.

Once the file is downloaded and opened, it requires user interaction to work. This involves hovering over text or photo embedded with a malicious link, which triggers a mouseover action. From there, they need to enable the content to run when they see a security alert.

The mouseover technique relies heavily on social engineering. Microsoft disables the content of suspicious files by default; a feature part of Protected View in later versions of Office. That's why victims need to open the file and enable malware to run on their machine.

"This technique only targets PowerPoint files," says Nunnikhoven. "I would expect it to expand to other Microsoft Office documents shortly since they support similar functionality."

This tactic won't work in Microsoft PowerPoint Online or "Web mode" in Office 365 because neither have the same actions functionality as offline/desktop versions. Office 365 users can still get hit if they access their accounts and open the bad file via locally installed PowerPoint.

The mouseover tactic is a more streamlined vector for cybercriminals because it doesn't rely on additional or initial vectors to deliver the payload. Office documents are popular in malware attacks because of how often they are used to send information throughout the enterprise, says Nunnikhoven. PDF files are frequently used by cybercriminals for the same reason.

Most malware authors and operators rely on old techniques like banking Trojans, targeted attacks, and malicious macros and shortcut (LNK) files in ransomware. Today's news is a sign that many are experimenting with new techniques.

The implications of this discovery are dangerous. Features like macros and mouse hover have legitimate use cases but could be disastrous under control of a threat actor. A socially engineered email and mouse hover, and maybe a click, is all that's necessary to infect a victim.

There are ways businesses can protect themselves. "The most effective technique against this attack is Web filtering," says Nunnikhoven. "Preventing systems from reaching the sites where malware is hosted is the best way to stop this attack."

End users should use Protect View, which lets them read content while cutting the chance of infection. IT and system admins can lessen the risk by disabling macros, OLEs, and mouse hovers by disabling these features on machines or employing group policies that block users from running them.

If features like mouse hover and macros are critical to business processes, Trend Micro suggests enabling them only in the applications and software that use them, or only allowing signed or approved macros.

Kelly Sheridan is Associate Editor at Dark Reading. She started her career in business tech journalism at Insurance & Technology and most recently reported for InformationWeek, where she covered Microsoft and business IT. Sheridan earned her BA at Villanova University

---

Does My Email or IP Address Reveal my Physical Location?

Category: Privacy From “askbobrankin.com”.

A concerned reader asks: 'Can someone find a user's identity (name, home address, etc.) simply by having their email or IP address? I'm asking because I posted to an online forum, and both my email and IP address were displayed publicly. Does that give others the ability to find my actual geographic location? Can I be tracked down in any way?' Read on to learn the answer to this common question...

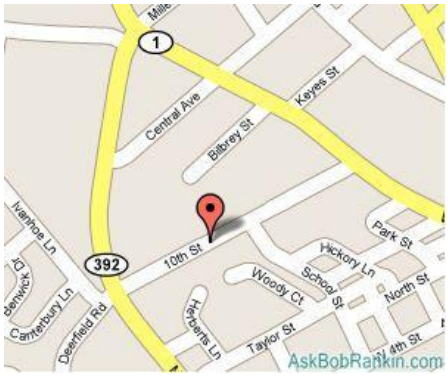
Are You Invisible Online?

It's true that your IP address is no secret. It's a basic part of internet communication protocols to send your IP address whenever you connect to a website, send an email, make a forum/blog post, chat, play an online game, etc. Without your IP address, the computer on the other end wouldn't know where to send the reply. Think of it as the return address on an envelope.

But that doesn't mean that Evildoers can find your home address if they know your IP address. Knowing your IP address does NOT give anyone the power to hack into your computer, NOR does it reveal who or where you are. Typically, each time you go online (if you have dialup) or each time you start your computer (if you have cable, fiber or dsl) you will be assigned an IP address, randomly selected from a pool of IP's assigned to your Internet Service Provider (ISP).

Finding the Physical Address for an IP Address

A person MIGHT be able to get a general idea of your geographic location, based on your IP address, by doing a lookup using a free Geo-IP database, but that will only tell them the physical location of your Internet Service Provider -- not YOUR home address. Keep in mind that when you're at work, your ISP might be your employer. (One easy way to find your current IP address is with the IP Chicken website.)



If you use a large regional or nationwide ISP, the IP lookup probably reveals nothing of interest -- either the location of your ISP's local switching facility, or a placeholder address that corresponds to the center of the town where you live. The IP address for most dialup users will be the location of the ISP's central office. For AOL subscribers, your IP address lookup will always show the location as Dulles, Virginia -- regardless of where you live. And if you're connecting to a public wifi hotspot in an airport, library or coffee shop, the IP address will be associated with the wireless service provider - not you at all.

Bottom line: The address returned by an IP lookup *could* be within a few miles of your home, or it could be wrong by several orders of magnitude.

When The Law Comes A Knockin'

Of course there is an exception to every rule. If Joe or Jane User calls your ISP and wants to know who was using a certain IP address last Tuesday, the ISP will tell them to go away. But if

an officer of the law hands your ISP a court order to reveal that information, they must do so. Your ISP's logs will enable them to determine which customer was using a certain IP address on a certain date and time, and they must reveal that information if a court has found probable cause that a crime was committed by that person.

For the truly paranoid (or the criminally inclined) there are ways to surf the web anonymously. The Anonymizer service will act as a proxy between you and your ISP, and they claim that your information cannot be subpoenaed because they do not store it. See I Always Feel Like Somebody's Watching Me and Will a VPN Make You Safer Online? for more information about anonymous web browsing options.

What About Email Addresses?

The same concepts apply to your email address. The part that follows the "@" sign is the domain name. This can be your ISP, your employer, a webmail provider, or an email forwarding service. Given the domain name, one can determine the owner's physical location, but nothing personally identifying about the email user without a court order.

Of course, if your email address is something like Jsmith90210@acme-widgets.com, then you're leaving little to the imagination of a determined hacker or stalker. Web-based email accounts are not truly anonymous, either. Even if you don't provide your real name when signing up, they can capture your IP address and track you through your ISP if necessary. But again, a court order would be needed.

Other Considerations

It's much more likely that you or your children will reveal your physical location the old fashioned way -- by just blurting it out. Kids who chat or play online games should be reminded often that they should never reveal any personal information, including their last name, phone number or home address. And of course, when you make an online purchase, you're explicitly providing your home address to the merchant.

Oh, and if you have any spyware or viruses on your system, all bets are off. These things are designed to violate your privacy. If you need help with scanning your system for malware and other unwanted pests, see my article on free anti-virus software for details on how to protect yourself from those risks.

Your thoughts on this topic are welcome. Post your comment or question TO “ASKBOBRANKIN.COM”..

Does this mean that my home is no longer a Castle?

D.C. Circuit Court Issues Dangerous Decision for Cybersecurity: Ethiopia is Free to Spy on Americans in Their Own Homes

By Nate Cardozo From WWW.EFF.org.
March 14, 2017

The United States Court of Appeals for the District of Columbia Circuit today held that foreign governments are free to spy on, injure, or even kill Americans in their own homes--so long as they do so by remote control. The decision comes in a case called Kidane v. Ethiopia, which we filed in February 2014.

Our client, who goes by the pseudonym Mr. Kidane, is a U.S. citizen who was born in Ethiopia and has lived here for over 30 years. In 2012 through 2013, his family home computer was attacked by malware that captured and then sent his every keystroke and Skype call to a server controlled by the Ethiopian government, likely in response to his political activity in favor of democratic reforms in Ethiopia. In a stunningly dangerous decision today, the D.C. Circuit ruled that Mr. Kidane had no legal remedy against Ethiopia for this attack, despite the fact that he was wiretapped at home in Maryland. The court held that, because the Ethiopian government hatched its plan in Ethiopia and its agents launched the attack that occurred in Maryland from outside the U.S., a law called the Foreign Sovereign Immunities Act (FSIA) prevented U.S. courts from even hearing the case.

The decision is extremely dangerous for cybersecurity. Under it, you have no recourse under law if a foreign government that hacks into your car and drives it off the road, targets you for a drone strike, or even sends a virus to your pacemaker, as long as the government planned the attack on foreign soil. It flies in the face of the idea that Americans should always be safe in their homes, and that safety should continue even if they speak out against foreign government activity abroad.

Factual background

Mr. Kidane discovered traces of state-sponsored malware called FinSpy, a sophisticated spyware product which its maker claims is sold exclusively to governments and law enforcement, on his laptop at his home in suburban Maryland. A forensic examination of his computer showed that the Ethiopian government had been recording Mr. Kidane's Skype calls, as well as monitoring his (and his family's) web and email usage. The spyware was launched when Kidane opened an attachment in an email. The spying began at his home in Maryland.

The spyware then reported everything it captured back to a command and control server in Ethiopia, owned and controlled by the Ethiopian government. The infection was active from October 2012 through March 2013, and was stopped just days after researchers at the University of Toronto's Citizen Lab released a report exposing Ethiopia's use of FinSpy. The report specifically referenced the very IP address of the Ethiopian government server responsible for the command and control of the spyware on Mr. Kidane's laptop.

We strenuously disagree with the D.C. Circuit's opinion in this case. Foreign governments should not be immune from suit for injuring Americans in their own homes and Americans should be as safe from remote controlled, malware, or robot attacks as they are from human agents. The FSIA does not require the courts to close their doors to Americans who are attacked, and the court's strained reading of the law is just wrong. Worse still, according to the court, so long as the foreign government formed even the smallest bit of its tortious intent abroad, it's immune from suit. We are evaluating our options for challenging this ruling.

NOW SOMETHING FOR MAC USERS.

New Malware-as-a-Service Offerings Target Mac OS X

By Kelly Sheridan in “darkreading.com”.

MacSpy and MacRansom are two early variants of malware-as-a-service portals targeting the broader population of Mac users.

Threat actors are setting their sights on Mac OS with MacSpy and MacRansom. The two malware-as-a-service (MaaS) offerings were created to take advantage of the growing Mac user base.

The concept of MaaS is not new; however, malware authors have historically targeted more popular Windows devices.

"The fact that this is a focused effort for just Mac OS makes it unique," says Peter Ewane, security researcher at AlienVault.

Researchers at AlienVault discovered MacSpy in May 2017 through an advertisement for the service. The free variant of the Mac RAT is primarily used to collect various pieces of user data, which can include browser history, screenshots, clipboard data, and other information.

Cybercriminals collect the data through clipboard data scraping, keylogging, voice recording, and browser data harvesting, Ewane explains. They trick their victims into executing the malware, or obtain physical access to the device, to get what they're looking for.

"The business impact can vary depending on what data is collected," Ewane explains. "For example, getting the username and password for an email account is a much smaller impact than the attacker potentially getting a private key for a web service."

There is also a paid version of MacSpy, which costs an unknown number of Bitcoins and comes with additional features including the abilities to retrieve any files and data on the Mac, encrypt the user directory in seconds, or disguise the program in any legitimate file format.

MacSpy is not widespread at this time and seems to be in a "beta" test mode. It is not known to exploit any vulnerabilities, says Eware. Victims can verify whether they have been infected by checking for a launch entry "/Library/LaunchAgents/com.apple.webkit.plis".

MacRansom is the only other known variant of MaaS targeting Mac devices. The ransomware-as-a-service (RaaS) offering was discovered by Fortinet researchers around the same time AlienVault found MacSpy.

Fortinet reports this could be the first known occurrence of RaaS targeting Mac OS. MacRansom shares web portal similarities with MacSpy and it's believed the two were developed by the same malware author.

The malware customers must directly contact the MacRansom author and can set a trigger time to launch their attack. When they do, the ransomware begins to lock files and can encrypt a maximum of 128.

After it encrypts targeted files, MacRansom encrypts both com.apple.finder.plist and the original executable. It changes the Time Date Stamp; this way, even if recovery tools are used to retrieve the files, they will be rendered unusable. The ransomware demands 0.25 Bitcoin (~$657 USD) and provides an email address for decryption.

"Even if it is far inferior from most current ransomware targeting Windows, it doesn't fail to encrypt victim's files or prevent access to important files, thereby causing real damage," say Fortinet's Rommel Joven and Wayne Chin Yick Low, who also express concern that copycats will generate additional variants of MacRansom.

The MacSpy authors, currently unknown, state they created this malware in response to Apple products gaining popularity in recent years, AlienVault reports. During their time in the field, the authors explain, they noticed a lack of "sophisticated malware for Mac users" and created MacSpy because they believed "people were in need of such programs on MacOS."

Higher rates of business adoption are likely part of the motivation. "One could say Mac OS adoption by [the] enterprise is making them a more interesting target to malware authors," adds Ewane. Security teams can protect their organizations with up-to-date antivirus and endpoint protection, he says, as well as user training.

Kelly Sheridan is Associate Editor at Dark Reading. She started her career in business tech journalism at Insurance & Technology and most recently reported for InformationWeek, where she covered Microsoft and business IT. Sheridan earned her BA at Villanova University. View Full Bio

Are Your Devices Listening and Recording Everything?

Category: Gadgets , Privacy From “askbobrankin.com”.

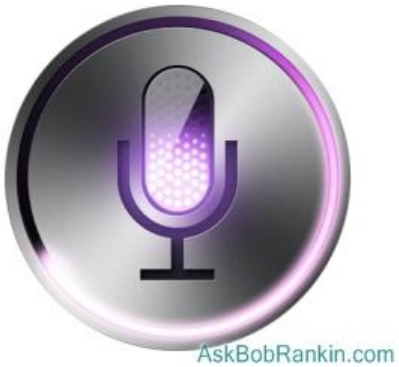
As the Internet of Things (IoT) expands, many people are becoming concerned about which of these “smart” devices are listening to them, what they are recording, what is transmitted to their creators, and how to stop the eavesdropping. So-called “digital assistants” such as Apple’s Siri, Google Assistant, Amazon Alexa are under heightened suspicion because they are voice-activated. Are these tools always listening, recording, and sharing our private conversations with unknown parties? Read on for answers...

Which Devices Are Listening to You?

First off, it’s important to note there’s a big difference between “listening” and “recording.” Yes, digital assistants are always listening. So are smart TVs, smartphones, and anything else that is voice-activated. There is no other way they can respond to voice commands. But they don’t record everything they hear, or transmit it back to the Mother Ship.

Every voice-activated device has a “wake-word” that tells it the following words are intended as a command for it to process. “Siri, call John Doe,” “Alexa, what’s the weather like,” "Hey Cortana, launch Microsoft Word" or “OK, Google, find me a good restaurant nearby” are examples of wake-words followed by commands. Once a command is processed, the digital assistant goes back to “sleep,” passively listening for its wake-word.

Only these commands, plus the digital assistant’s response, are recorded and stored on the servers of the assistant’s creator. The purpose is to train the assistant to better understand your spoken commands and respond appropriately. For example, “OK, Google, I said ‘what’s the weather,’ not ‘what’s leather.’”



In an Arkansas murder case, prosecutors demanded from Amazon all recordings that a suspect's Echo device had made on the day of the crime. This action fed rumors that Alexa records more than just commands. But that's simply not true. To Amazon's credit, the company refused to turn over said recordings without a search warrant, until the suspect himself gave the okay.

If you're still nervous about a digital assistant eavesdropping on non-command verbalizations, you can buy an Amazon Tap device that requires your physical touch on a button to commence listening and recording.

Smartphones may be listening to you, too. You can stop that in Android by going to Settings > Privacy and safety > App permissions and looking for the "microphone" entry, which lists all apps that have access to the phone's mic. Turn off said access as you wish. On iOS devices, the path to the microphone entry is Settings > Privacy.

Smart TVs May Be a Dumb Idea

Smart TVs are made by people who literally don't know what they're doing. When LG Electronics was asked if its smart TVs record non-command conversations, the company replied, in essence, "We'll have to look into that and get back to you." Furthermore, the TV's setting to toggle collection of viewing info did nothing when switched to "off." Data continued to be transmitted to an unknown destination.

Vizo, maker of inexpensive and popular smart TVs, was smacked down for spying on its customers by the FTC in February, 2017. The company agreed to pay a $2.2 million fine and stop collecting data on viewing habits without permission.

The CIA and the UK's spy agency, MI5, collaborated on hacking smart TVs, according to documents in a batch of top-secret material released by Wikileaks in March, 2017. It turns out that smart TV programmers aren't very smart; a South Korean hacker documented 10 security vulnerabilities that gave him root access to a smart TV made by "an unnamed vendor." Bottom line: if a hacker can get access to the home network, he can take complete control of the TV's microphone, motion sensors, camera, and Internet connection. https://goo.gl/f2pWSn

It may be best to buy a "dumb" TV, or disconnect a smart TV from the Internet if you already have one. You can reset the smart TV to factory defaults and set it up all over again. When it asks for your WiFi password, don't provide it. If it asks you to plug in an Ethernet cable, don't do that either. (Of course, that will eliminate the TV's ability to stream online content such as Netflix, Hulu or Amazon Prime.)

How to Manage What Your Gadgets Hear

It may be comforting to know that Cortana on Windows 10 doesn't start listening until you click on the search box. Also, both the Amazon Echo and the Google Home have mute buttons, which temporarily disable the microphone. If you want to minimize the devices that are always

listening to you in your home, opt for the Amazon Tap, or the Alexa remote for Fire TV, which require you to push a button to enable voice commands.

Alexa users can find a running list of their queries in the Alexa app in Settings > History. If a user has several Alexa devices in their arsenal, each one has its own listenable queue of requests.

Google and Amazon provide ways to review and manage the audio clips that their digital assistants have recorded. Google users can find everything they've asked Google Assistant to do by visiting myactivity.google.com. You can even listen to and delete the audio clips stored there. Amazon Alexa users can do the same by visiting amazon.com/myx and clicking the "Your Devices" tab; select your Alexa and click "Manage voice recordings" to review or delete items.

To manage the Cortana data stored on your Windows 10 computer, select Cortana from the Start Menu, and click the Notebook item in the left sidebar. From there, you can view and delete entries in Cortana's "Notebook," which contains all the information Cortana has stored for you.

Do you use voice activated devices? Are you concerned about what they might be recording? Your thoughts on this topic are welcome. Post your comment or questions to "askbobrankin.com"...

NO COMMENT

Old Men have 2 motivations: hunger and hanky panky, and they can't tell them apart.
If you see a gleam in his eyes, make him a sandwich.