KREBS: MICROSOFT SOFTWARE IS FULLY HACKED AND INSECURE

When Identity Thieves Hack Your Accountant

The **Internal Revenue Service** has been urging tax preparation firms to step up their cybersecurity efforts this year, warning that identity thieves and hackers increasingly are targeting certified public accountants (CPAs) in a bid to siphon oodles of sensitive personal and financial data on taxpayers. This is the story of a CPA in New Jersey whose compromise by malware led to identity theft and phony tax refund requests filed on behalf of his clients.

Last month, KrebsOnSecurity was alerted by security expert **Alex Holden** of Hold Security about a malware gang that appears to have focused on CPAs. The crooks in this case were using a Web-based keylogger that recorded every keystroke typed on the target's machine, and periodically uploaded screenshots of whatever was being displayed on the victim's computer screen at the time.

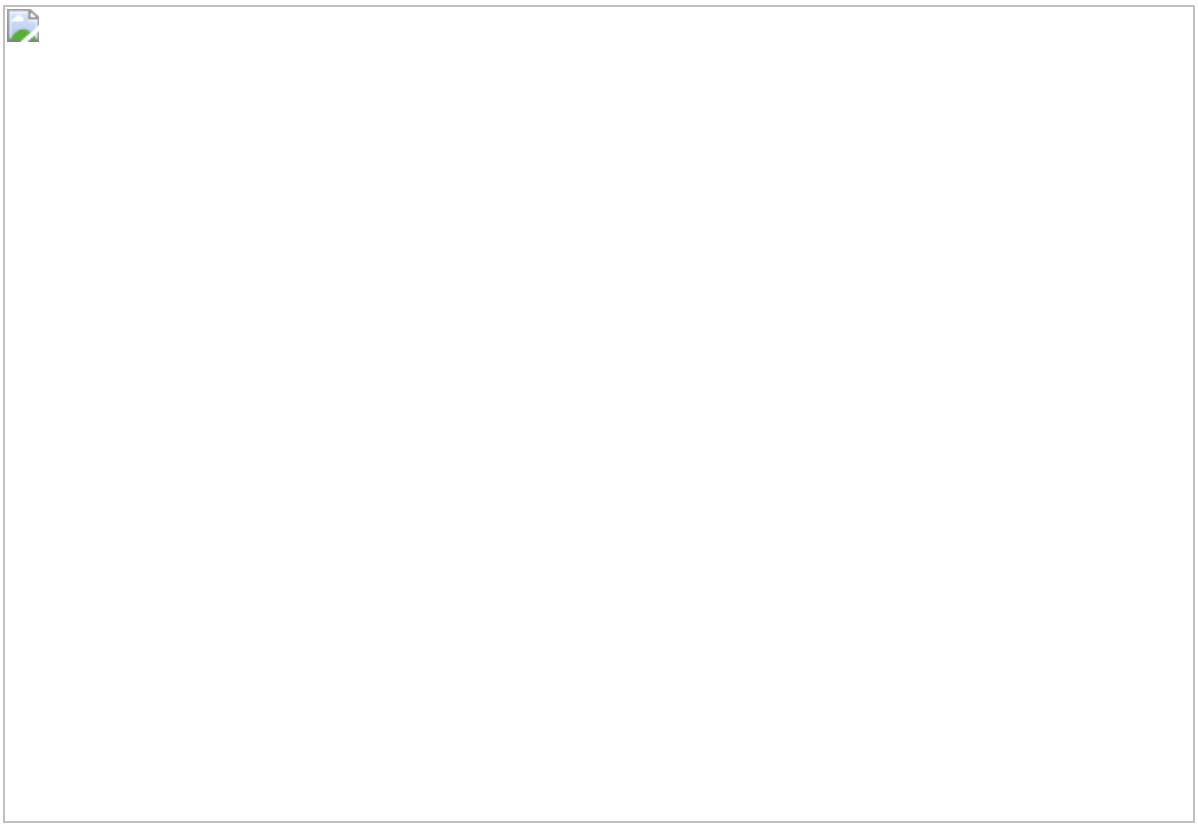
If you've never seen one of these keyloggers in action, viewing their output can be a bit unnerving. This particular malware is not terribly sophisticated, but nevertheless is quite effective. It not only grabs any data the victim submits into Web-based forms, but also captures any typing — including backspaces and typos as we can see in the screenshot below.

The malware records everything its victims type (including backspaces and typos), and frequently takes snapshots of the victim's computer screen.

Whoever was running this scheme had all victim information uploaded to a site that was protected from data scraping by search engines, but the site itself did not require any form of authentication to view data harvested from victim PCs. Rather, the stolen information was indexed by victim and ordered by day, meaning anyone who knew the right URL could view each day's keylogging record as one long image file.

Those records suggest that this particular CPA — "John," a New Jersey professional whose real name will be left out of this story — likely had his computer compromised sometime in mid-March 2018 (at least, this is as far back as the keylogging records go for John).

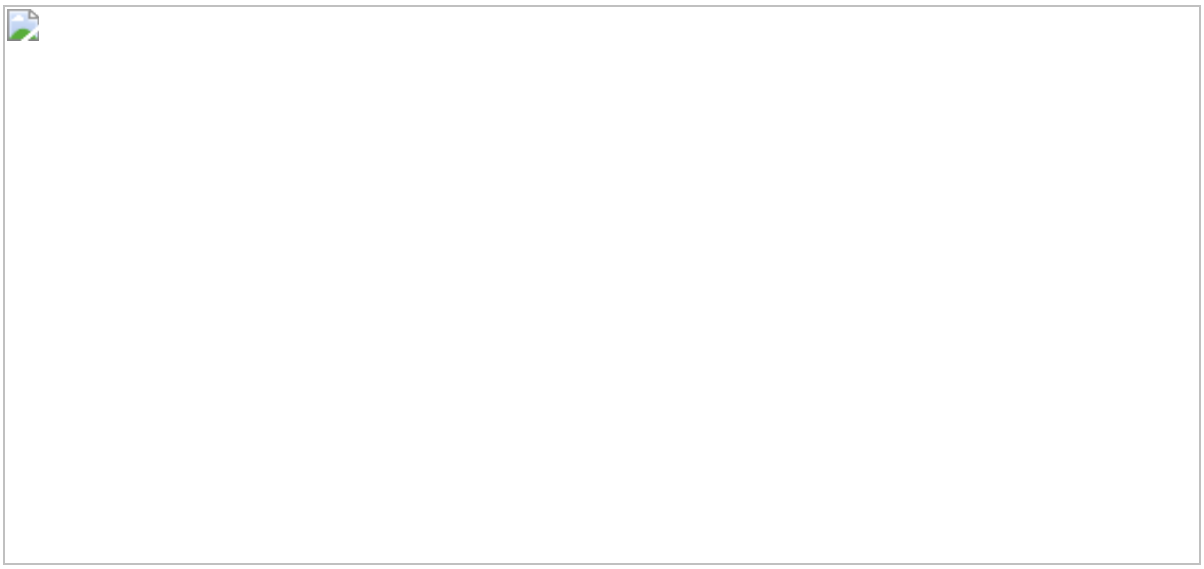
It's also not clear exactly which method the thieves used to get malware on John's machine. Screenshots for John's account suggest he routinely ignored messages from **Microsoft** and other third party Windows programs about the need to apply critical security updates.



Messages like this one — about critical security updates available for QuickBooks — went largely ignored, according to multiple screenshots from John's computer.

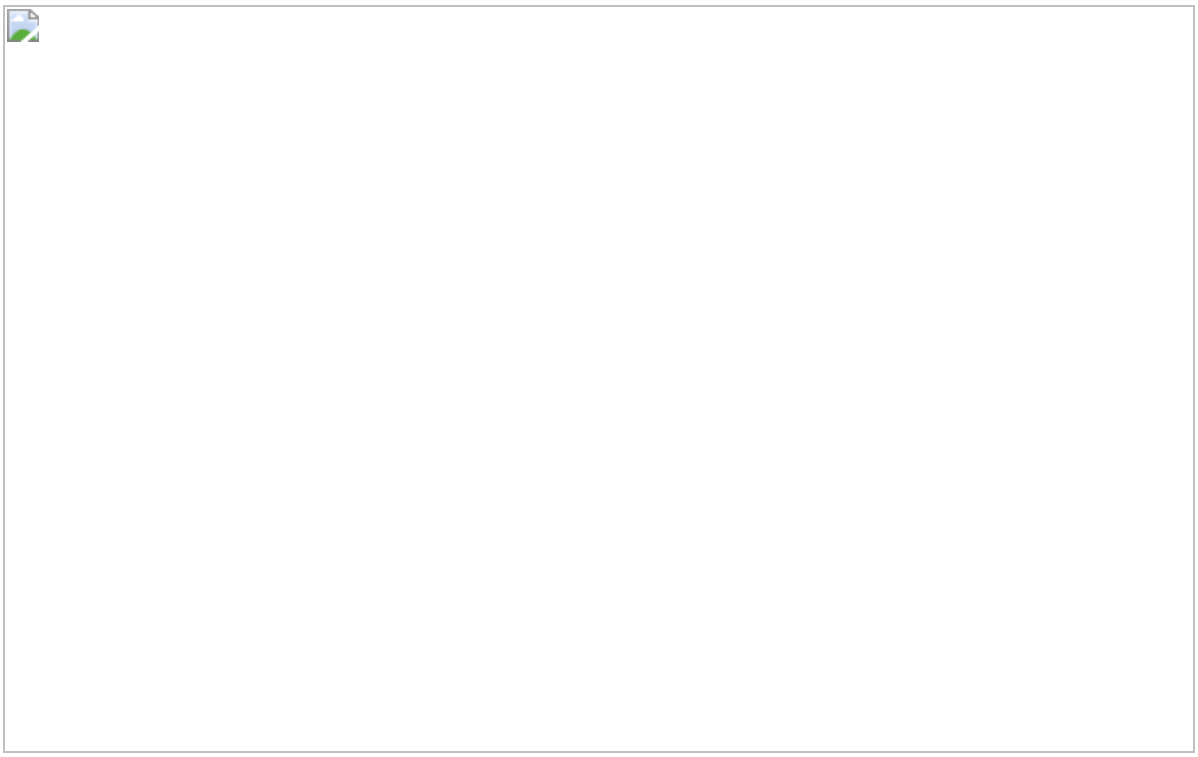
More likely, however, John's computer was compromised by someone who sent him a booby-trapped email attachment or link. When one considers just how frequently CPAs must need to open **Microsoft Office** and other files submitted by clients and potential clients via email, it's not hard to imagine how simple it might be for hackers to target and successfully compromise your average CPA.

The keylogging malware itself appears to have been sold (or perhaps directly deployed) by a cybercriminal who uses the nickname **ja_far**. This individual markets a $50 keylogger product alongside a malware "crypting" service that guarantees his malware will be undetected by most antivirus products for a given number of days after it is used against a victim.



Ja_far's sales threads for the keylogger used to steal tax and financial data from hundreds of John's clients.

It seems likely that ja_far's keylogger was the source of this data because at one point — early in the morning John's time — the attacker appears to have accidentally pasted ja_far's jabber instant messenger address into the victim's screen instead of his own. In all likelihood, John's assailant was seeking additional crypting services to ensure the keylogger remained undetected on John's PC. A couple of minutes later, the intruder downloaded a file to John's PC from file-sharing site **sendspace.com**.



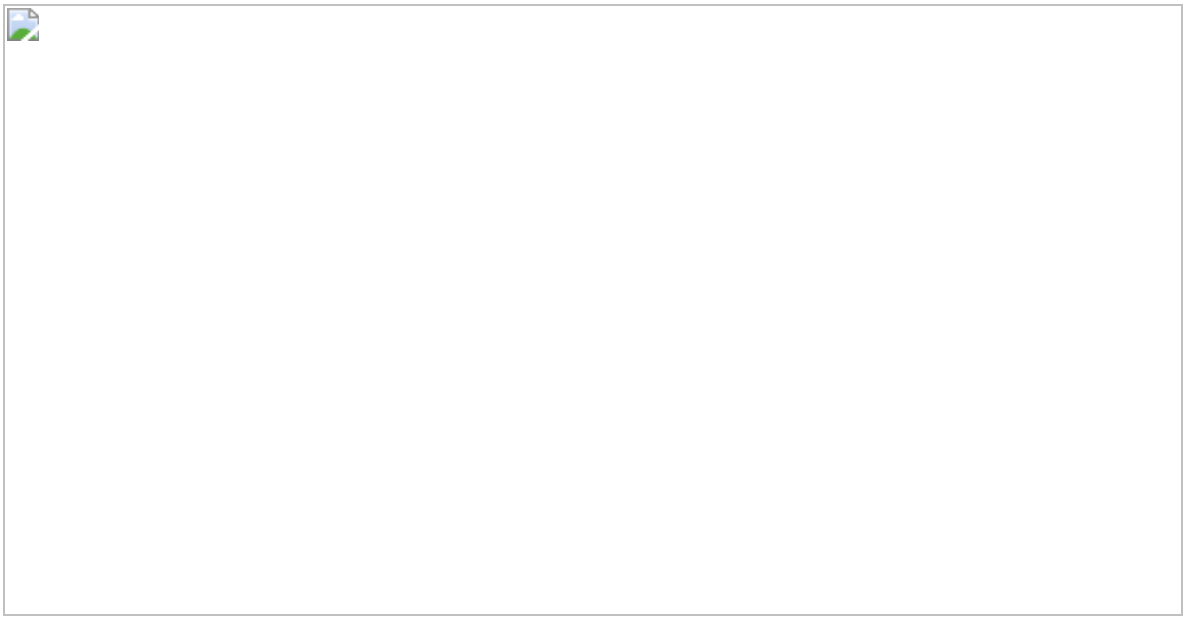
The attacker apparently messing around on John's computer while John was not sitting in front of the keyboard.

What I found remarkable about John's situation was despite receiving notice after notice that the IRS had rejected many of his clients' tax returns because those returns had already been filed by fraudsters, for at least two weeks John does not appear to have suspected that his compromised computer was likely the source of said fraud inflicted on his clients (or if he did, he didn't share this notion with any of his friends or family via email).

Instead, John composed and distributed to his clients a form letter about their rejected returns, and another letter that clients could use to alert the IRS and New Jersey tax authorities of suspected identity fraud.

Then again, perhaps John ultimately *did* suspect that someone had commandeered his machine, because on March 30 he downloaded and installed **Spyhunter 4**, a security product by **Enigma**

Software designed to detect spyware, keyloggers and rootkits, among other malicious software.



Evidently suspecting someone or something was messing with his computer, John downloaded the trial version of Spyhunter 4 to scan his PC for malware.

Spyhunter appears to have found ja_far's keylogger, because shortly after the malware alert pictured above popped up on John's screen, the Web-based keylogging service stopped recording logs from his machine. John did not respond to requests for comment (via phone).

It's unlikely John's various clients who experience(d) identity fraud, tax refund fraud or account takeovers as a result of his PC infection will ever learn the real reason for the fraud. I opted to keep his name out of this story because I thought the experience documented and explained here would be eye opening enough and I have no particular interest in ruining his business.

But a new type of identity theft that the IRS first warned about this year involving CPAs would be very difficult for a victim CPA to conceal. Identity thieves who specialize in tax refund fraud have been busy of late hacking online accounts at multiple tax preparation firms and using them to file phony refund requests. Once the IRS

processes the return and deposits money into bank accounts of the hacked firms' clients, the crooks contact those clients posing as a collection agency and demand that the money be "returned."

If you go to file your taxes electronically this year and the return is rejected, it may mean fraudsters have beat you to it. The IRS advises taxpayers in this situation to follow the steps outlined in the Taxpayer Guide to Identity Theft. Those unable to file electronically should mail a paper tax return along with Form 14039 (PDF) — the Identity Theft Affidavit — stating they were victims of a tax preparer data breach.

Tax professionals might consider using something other than **Microsoft Windows** to manage their client's data. I've long dispensed this advice for people in charge of handling payroll accounts for small- to mid-sized businesses. I continue to stand by this advice not because there isn't malware that can infect **Mac** or **Linux**-based systems, but because the vast majority of malicious software out there today still targets Windows computers, and you don't have to outrun the bear — only the next guy.

Many readers involved in handling corporate payroll accounts have countered that this advice is impractical for people who rely on multiple Windows-based programs to do their jobs. These days, however, most systems and services needed to perform accounting (and CPA) tasks can be used across multiple operating systems — mainly because they are now Web-based and rely instead on credentials entered at some cloud service (e.g., **UltraTax**, **QuickBooks**, or even **Microsoft's Office 365)**.

Naturally, users still must be on guard against phishing scams that try to trick people into divulging credentials to these services, but when your entire business of managing other people's money and identities can be undone by a simple keylogger, it's a good idea to do whatever you can to keep from becoming the next malware victim.

According to the IRS, fraudsters are using spear phishing attacks to compromise computers of tax pros. In this scheme, the "criminal singles out one or more tax preparers in a firm and sends an email posing as a trusted source such as the IRS, a tax software provider or a cloud storage provider. Thieves also may pose as clients or new prospects. The objective is to trick the tax professional into disclosing sensitive usernames and passwords or to open a link or attachment that secretly downloads malware enabling the thieves to track every keystroke."

The IRS warns that some tax professionals may be unaware they are victims of data theft, even long after all of their clients' data has been stolen by digital intruders. Here are some signs there might be a problem:

- Client e-filed returns begin to be rejected because returns with their Social Security numbers were already filed;
- The number of returns filed with tax practitioner's Electronic Filing Identification Number (EFIN) exceeds number of clients;
- Clients who haven't filed tax returns begin to receive authentication letters from the IRS;
- Network computers running slower than normal;
- Computer cursors moving or changing numbers without touching the keyboard;
- Network computers locking out tax practitioners.

Tags: alex holden, crypting service, Form 14039, Hold Security, irs, ja_far, Microsoft Office 365, QuickBooks, Spyhunter, tax refund fraud, UltraTax, xkey@exploit.im