the Availability Digest

www.availabilitydigest.com
@availabilitydig

Do the Russians Have Your Tax Returns?

August 2015

In May, 2015, the U.S. Internal Revenue Service (IRS) announced that one of its systems had been breached and that the tax returns of over 100,000 taxpayers had been stolen. Three months later, the IRS tripled this estimate. Already, tax returns for $50,000,000 in fraudulent tax refunds have been filed.

The Hack

The "Get Transcript" Application

The hackers entered the IRS computer system that was running the "Get Transcript" application. The application allows taxpayers to get copies of their tax returns for prior years. This is often necessary for tasks such as applying for a mortgage or applying for college financial aid.

The Get Transcript application was used by 23 million U.S. taxpayers last year. Other IRS computer systems such as IRS' main system for handling tax return submissions were not involved in the breach.

The Initial Estimate

In mid-May, 2015, the IRS noticed unusual activity being experienced by the Get Transcript application. At first, they thought that the activity might be part of a Distributed Denial of Service (DDoS) attack intended to shut down the web site. However, they quickly determined it instead was caused by criminal hackers trying to gain access to taxpayer records. The IRS immediately shut down the application to prevent further breaches.

Upon further investigation, the IRS determined that the attack had been going on for four months since the previous February. It announced that the tax records of about 114,000 taxpayers had been compromised. These returns are full of personal information that is now available to the hackers. Another 100,000 attempts to access data were unsuccessful.

The Current Estimate

The IRS set out to investigate the millions of Get Transcript requests that had been made since the attack began. As a result, the agency tripled its estimate of the number of taxpayers who were affected. The IRS now says that 334,000 taxpayer accounts were breached and that another 280,000 attempts were unsuccessful.

How the Hackers Got In

In this attack, the cybercriminals did not secrete malware on the IRS system to give them a back door for access. Rather, they came in through the front door. Using social media such as Facebook, they acquired vast amounts of data about taxpayers. This included taxpayer names, Social Security numbers, birthdays, and street addresses, which allowed the cybercriminals to begin the logon procedure to the Get Transcript application. The attackers also had to determine (or guess) the answer to several personal security questions such as what high schools did taxpayers attend or what were the names of their first pets.

Armed with this information, the cybercriminals posed as legitimate taxpayers and logged in. They typically were not successful on the first attempt as they tried to guess the answers to personal security questions. However, often they were ultimately successful; and they then had full access to the taxpayers' tax returns. Based on the large increase in request traffic observed by the IRS, the guesses to personal security questions were probably automated by remote attack computers.

How did the agency determine that an account had been attacked? Perhaps it searched for accounts against which multiple attempts to open the account had been attempted unsuccessfully. If an account was ultimately opened after several tries, it was a successful breach. If an account failed to be opened after multiple tries, it was an attack that had failed.

Who Were the Hackers?

Studying the attack methods, the IRS came to the conclusion that the cyber breach originated in Russia. It believes that this was the work of an organized crime syndicate with an army of hackers that could submit such a mass of logon attempts to the Get Transcript application.

This attack came on the heels of a disclosure that Russian hackers had infiltrated the White House and the U.S. State Department computers. Security researchers had revealed in March how easy it was to hack the IRS systems. The IRS independent watchdog had recently issued a report saying that "computer security has been problematic with the IRS since 1997."

What is the Damage?

The damage of most concern is that the crooks now have a great deal of sensitive information about hundreds of thousands of American citizens. This information, which includes salary as well as the details of deductions taken by the victims, can be used to open bank accounts, obtain credit lines, and steal tax refunds in the future.

So far, the IRS has indicated that about 15,000 phony tax returns have been submitted in other peoples' names. The returns request tax refunds totaling USD $50,000,000.

What Is the IRS Doing About It?

The IRS immediately shut down the Get Transcript application. For several subsequent months, taxpayers had to request past tax returns be sent to them by mail. To make the request, they had to file a Form 4506, "Request for Copy of Return."

The IRS has now re-enabled the Get Transcript application. However, taxpayers must create a new logon and select new personal security questions.

A taxpayer now can lock or disable access to his account, and the IRS is trying to increase security with the right balance. It is trying to make access difficult for fraudsters but not too difficult for the average person trying to get hold of his previous years' returns.

The IRS is notifying by mail everyone whose account was attacked (whether successful or not). It is offering free credit monitoring for the taxpayers whose accounts were breached as well as giving those taxpayers an individualized six-digit PIN to use for authorization. The IRS will monitor these returns more closely next year, looking for signs of fraudulent returns.

The attack is under review by the Treasury Inspector General for Tax Administration and the IRS' Criminal Investigation Unit. It is also being investigated by the Department of Homeland Security and the Federal Bureau of Investigation (FBI).

The Lawsuit

A class-action lawsuit representing all of the taxpayers who were affected by the breach has been filed against the IRS for failing to secure its servers. The lawsuit states that "the IRS knew it was vulnerable and deliberately and intentionally decided not to implement the security measures needed to prevent the data breach."

Summary

Even though a lot has been made about the fact that the IRS systems may be vulnerable to attack, this data breach is concerning because its system was not hacked. Rather, a very sophisticated approach was taken. A massive amount of data was acquired on each of the taxpayers from non-IRS sources such as Facebook and was used to log on to the system as the taxpayers themselves. In effect, the hackers came in through the front door. Any system, no matter the amount invested in it to make it secure, is subject to this sort of attack.

Fortunately, such an attack should be easily discoverable because of an unexpected increase in the amount of traffic as faulty logons are retried until they are successful.

Acknowledgements

Information for this article came from the following sources:

IRS Hacked, 100,000 tax accounts breached, *USA Today*; May 26, 2015.
Criminals use IRS website to steal data on 104,000 people, *CNN*; May 26, 2015.
IRS Statement on the "Get Transcript" Application, *IRS*; May 26, 2015.
IRS believes massive data theft originated in Russia, *CNN*; June 4, 2015.
IRS Hack Bigger Than First Thought, *NPR*; August 17, 2015.
IRS hack far larger than first thought, *USA Today*; August 18, 2015.
Taxpayers Are Suing the IRS Over That Huge Hack, Of Course, *Gizmodo*; August 26, 2015.
IRS hit with lawsuit over recent taxpayer data hack, *Slash Gear*; August 26, 2015.
IRS Website