SECURITY

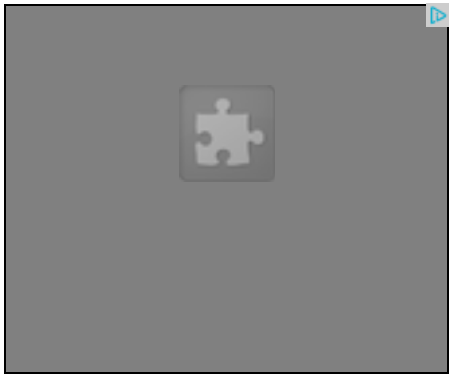
Snowden leak: Microsoft added Outlook.com backdoor for Feds

NSA praises Redmond for 'collaborative teamwork'

By Iain Thomson in San Francisco, 11th July 2013

There are red faces in Redmond after Edward Snowden released a new batch of documents from the NSA's Special Source Operations (SSO) division covering Microsoft's involvement in allowing backdoor access to its software to the NSA and others.

Documents seen by *The Guardian* detail how the NSA became concerned when Microsoft started testing Outlook.com, and asked for access. In five months Microsoft and the FBI created a workaround that gives the NSA access to encrypted chats on Outlook.com. The system went live in December last year – two months before Outlook.com's commercial launch.

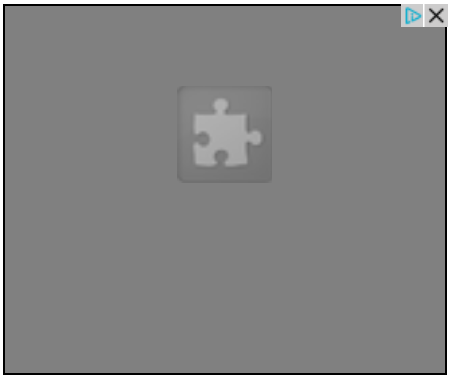


Those Outlook users not enabling encryption get their data slurped as a matter of course, the documents show. "For Prism collection against Hotmail, Live, and Outlook.com emails will be unaffected because Prism collects this data prior to encryption," an NSA newsletter states.

Microsoft's cloud storage service SkyDrive is also easy to access, thanks to Redmond's work with the NSA. The agency reported on April 8, 2013 that Microsoft has built PRISM access into Skydrive in such a way as to remove the need for NSA analysts to get special authorization for searches in Microsoft's cloud.

"Analysts will no longer have to make a special request to SSO for this – a process step that many analysts may not have known about," the leaked NSA document states. "This new capability will result in a much more complete and timely collection response. This success is the result of the FBI working for many months with Microsoft to get this tasking and collection solution established."

The documents also detail how Microsoft and Skype have also been working with the intelligence agencies to install monitoring taps. Work began on integrating Prism into Skype in November 2010, they state, three months before the company was issued with an official order to comply by the US Attorney General.



Data collection began on February 6, 2011, and the NSA document says the planned systems worked well, with full metadata collection enabled. It praised Microsoft for its help, saying "collaborative teamwork was the key to the successful addition of another provider to the Prism system."

Work to integrate Skype into Prism into Skype didn't stop there, however. In July 2012 an NSA newsletter states Microsoft installed an upgrade that tripled the amount of Skype videos that can be monitored by NSA analysts.

"The audio portions of these sessions have been processed correctly all along, but without the accompanying video. Now, analysts will have the complete 'picture'," it says.

In a statement, Microsoft said that it only complies with legal demands for customer information for law enforcement and national security purposes, and that the company isn't involved in giving "the kind of blanket orders discussed in the press over the past few weeks."

"When we upgrade or update products legal obligations may in some circumstances require that we maintain the ability to provide information in response to a law enforcement or national security request. There are aspects of this debate that we wish we were able to discuss more freely," it said.

Not that Microsoft hasn't been making a big thing about the privacy of its communications systems in the past. Its Gmail Man ad campaign lambasted Google for snooping in people's mail to match them with advertisers, and the tagline "Your email is your business" seems somewhat ironic these days. The advert is no longer on Microsoft's YouTube channel.

The leaked documents come from the NSA's Special Source Operations (SSO) division, which handles commercial company liaison for data collection by the agency. The documents show that, once collected by Prism, the NSA shares its data directly with the CIA and FBI via a custom application.

"The FBI and CIA then can request a copy of Prism collection of any selector..." the document says. "These two activities underscore the point that Prism is a team sport!"

In a joint statement, Shawn Turner, spokesman for the director of National Intelligence, and Judith Emmel, spokeswoman for the NSA, told *The Guardian* that the wiretapping referred to in the document was court-ordered and was subject to judicial oversight.

"Not all countries have equivalent oversight requirements to protect civil liberties and privacy," they said. "In practice, US companies put energy, focus and commitment into consistently protecting the privacy of their customers around the world, while meeting their obligations under the laws of the US and other countries in which they operate." ®

Agentless Backup is Not a Myth

MORE READING
Skype
Microsoft
Nsa
Prism
Outlook

COMMENTS

Post your comment | House Rules | Send Corrections

Highly Rated | **All Reader Comments (118)**

Suburban Inmate Posted Thursday 11th July 2013 22:26 GMT

Report abuse

Speaking as a tinfoil headed nutjob...

This Snowden chap is really making my hobby bloody difficult! How am I supposed to be a paranoid loony if everything I spout turns out to be **true**?

69 0

David D. Hagood

Posted Thursday 11th July 2013 21:16 GMT

Report abuse

You mean, above and beyond

You mean, an audit above and beyond every line of code being visible to anybody who pulls down the kernel source from git.kernel.org, including about 10 thousand very experienced programmers world-wide, many of whom work for governments not-at-all friendly to the US, who can evaluate the security impact of all that code?

Let me guess: your next post will be about how we have to distrust AES, because "the NSA maded it" (hint: no, the folks who created AES were Belgian mathematicians, and the algorithm was vetted by cryptographers around the planet before the NSA simply said "yes, that'll do, we approve using that").

20 1

RobHib

Posted Thursday 11th July 2013 23:45 GMT

Report abuse

Not a bit surprised. Ask youself these questions about Windows privacy.

Years ago it occurred to me to ask the question 'why is it so hard to clean traces of one's activity out of Windows?' Since then, it's become much harder to do so despite the obvious security concerns. Ask yourself why it's so.

Windows is so hard to clean properly that it's almost an impossible task, moreover, after purging the known user activity there's no way of actually interrogating the O/S to see if one has actually gotten all of it and that the O/S is actually clean--Microsoft hasn't provided a facility to do this. In fact, it's so hard that it's earlier to purge the disk completely with DBAN--Darik's Boot And Nuke which also erases every trace of Windows, alternatively one can put the disk into a metal shredder or run over it with steamroller or forklift to rid oneself of the history and other telltale metadata.

Also ask yourself why Microsoft didn't include another root directory alongside 'Documents and Settings' say perhaps called 'Configuration, Logs and Activity' (a single and only place for all such data) with the ability to easily delete all or part of its contents. Simply deleting all files (either by simple or secure delete) would restore Windows to a default state (a la a 'pre-installed' laptop with programs). A similar arrangement could be used to purge programs and user accounts.

Of course there's the obvious reasons: it was more work for Microsoft, and/or that Microsoft made it deliberately difficult so users would delete all of Windows prior to the sale/disposal of a PC so that another copy of Windows would have to be purchased by a new owner; or that deliberate obfuscations within Windows made it easier to protect copyright/rego of both Windows and installed programs.

Such excuses alone would have been plausible back in the days of Windows NT, Windows 2000 and perhaps even XP but look at what's happened since then: one has to completely re-evaluate the situation when one looks at later Windows O/Ses. Take Windows 7 for instance, it's a nightmare to purge all the logs let alone all the other associated metadata--just finding everything is a mammoth task in itself.

Remember also that in later Windows O/Ses such as Windows 7 that Microsoft has not only turned on dozens more log files and retained much more metadata but it has also mandated NTFS and outlawed FAT32 for the Windows installation volume. NTFS uses both Streams and a MFT (Master File Table), which are difficult to purge. When files are deleted the MFT remains full of the file particulars. Even if purged using special sanitising software, remnants of the file entries are still there. The only truly effective way to clean a NTFS volume is to copy all remaining/active/wanted files to a FAT32 volume then clean--completely purge the NTFS Volume with say DBAN--then reformat it and then copy the wanted files back from the FAT32 volume.

Frankly, the totally inadequate situation of being unable to purge NTFS volumes of remnant metadata and such from within Windows is just absurd--so much so that it must have been deliberately planned this way to make it so difficult.

Despite all the obvious hoo-hah over security in recent years, Microsoft has still not provided any services or facilities whatsoever to clean up/purge the O/S of user activity. In fact, Microsoft has just made matters worse. Instead (it seems to me as a cover), Microsoft has provided users with so-called security features such as the annoying and essentially useless User Account Control (UAC). These may be of some help with simple viruses but they're totally useless when someone or a government agency wants information about the user's PC activity.

So after several decades and many versions of Windows why wouldn't Microsoft do things correctly?

It seems damn clear to me--and it ought to be so even to Blind Freddy--that Microsoft is under pressure to ensure that when a Windows O/S comes into the possession of law enforcement and or other Government agencies that it's comparatively easy to analyse in great detail what the user has been doing on his/her PC--even if he/she has gone to considerable lengths to clean up traces of this activity.

Frankly, I am simply amazed that these massive and glaring privacy anomalies within Windows aren't the subject of massive user outrage; especially go given that they've been going on for such a long time.

Is this just user complacency or is it massive user ignorance?

15 0

Previous Story Next Story

MORE FROM THE REGISTER

97

Snowden: US and Israel *did* create Stuxnet attack code

UK is 'radioactive' and 'Queen's selfies to the pool boy' slurped

44

Android sig vuln exploit SEEN IN THE WILD

Tiny script is a big headache

40

Emergency alert system easily pwnable after epic ZOMBIE attack prank

Private crypto keys found in firmware - where were their BRRAAAIINNNS?

MORE FROM THE REGISTER

Send us News Tips Week's Headlines Reg Archive Top 20 Stories eBooks Webcasts