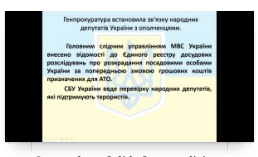
SECURITY ALERTS

Alert: Microsoft Zero Day from Sandworm Cyberspies!

STEVE · OCTOBER 16, 2014 · 3 MIN READ

If you read the tech headlines Tuesday, you might have noticed that there was another "Russian hack." This time, however, consumers and small businesses weren't the target. This time, things were political.

Reports indicate the discovery of a brand new zero day vulnerability affecting all supported versions of the Windows operating system. That's Windows Vista through Windows 8.1, but interestingly enough not Windows XP. In a nutshell, vulnerability CVE-2014-4114 allows attackers to remotely execute malicious code through shared Microsoft Office documents. In general, "malicious code" means instructions to download and execute any sort of malware. In observed cases, this malware is one called "Black Energy," and it has been used in attempts to steal sensitive information. According to reports, a group of attackers used CVE-2014-4114 to serve Black Energy to the Ukrainian government through spear-phishing emails.



Screenshot of slide from malicious Powerpoint that leveraged CVE-2014-4114

More specifically, these emails contained an attached Powerpoint presentation that leveraged the zero day vulnerability. As yet, the extent to which information was exfiltrated from this attack is unknown – however, further investigation has revealed that the attackers in question have been using malware to spy on governments since 2009.

They're called "The Sandworm Team"

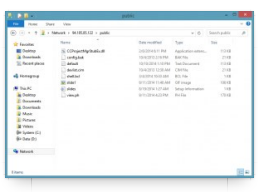
According to independent researchers, September's spear-phishing campaign was the first time CVE-2014-4114 was used; however, it was not the first time the group that used it has attacked. In fact, researchers claim that the group – known as "The Sandworm Team," due to their penchant for making references within their code to Frank Herbert's *Dune* – has been targeting a number of governmental organizations for the last 5 years.

Notable targets have included:

- NATO
- Attendees of the 2014 GlobSec conference
- A "specific" yet undisclosed Western European government
- An undisclosed Polish energy firm
- An undisclosed French telecommunications firm

In all cases, methods to infection have been the same. Targets are first socially engineered into opening malicious attachments, under the pretense that they contain confidential or valuable political information. In reality, these attachments are weaponized exploits designed to download malware... that actually steals exactly the type of information the phish promises to provide.

In the specific case of CVE-2014-4114, we have a previously undisclosed vulnerability which actually leverages a design flaw in Microsoft Office applications. This flaw allows the attackers to download malware via Windows Network over the Internet.

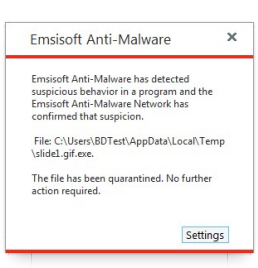


Windows network share operated by The Sandworm Team

What is concerning about this exploit in particular is that typically recommended zero day counter measures, such as Microsoft's Enhanced Mitigation Experience Toolkit, do not protect unpatched systems. Furthermore, the malicious server in use actually appears to be located in Stockholm, Sweden, despite claims that The Sandworm Team is Russian.

Protecting yourself from this zero-day

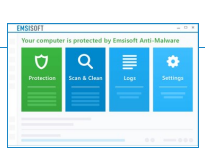
As an Emsisoft user, the most important thing you need to know about CVE-2014-4114 is that you are protected. As soon the news broke, our analysis team began testing the Black Energy payload served by the zero day exploit. They found that Emsisoft's Behavior Blocking technology prevents Black Energy from executing automatically, without any user intervention required.



Despite the fact that you may just be an everyday user – without confidential, governmental documents saved on your computer – protecting yourself from this attack is still important. In the hours that follow any zero day disclosure, copycat cybercriminals will often emulate the reported attack to send out malware before the issue is patched. Utilizing a proactive anti-malware that can prevent infection from unregistered threats is one of the best ways to avoid this. Of course, not opening shady emails helps a lot too.

In the specific case of CVE-2014-4114, it is fortunate that the researchers who disclosed did so in a responsible manner. October 14th was Microsoft's "Patch Tuesday," the day on which all supported operating systems receive their monthly updates; and, due to collaboration, a patch for the zero day was included. For anyone using Emsisoft, this means that no direct action is required. Simply allow your computer to update the next time it asks to do so. In the meantime, we'll have your back.

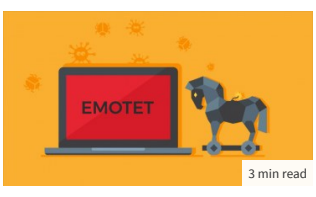
Have a great (Sandworm-free) day!



For the original disclosure, see iSight's post on Sandworm.

Steve
Freelance writer and security enthusiast based in the USA.

What to read next

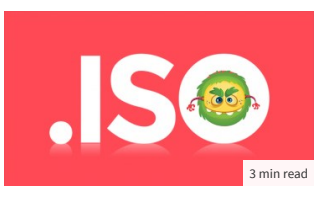


3 min read

SECURITY ALERTS

Emotet trojan is back with a vengeance

Emotet is back. The infamous trojan now features an all-new email harvesting module that is helping malware authors create scarily realistic malicious emails.

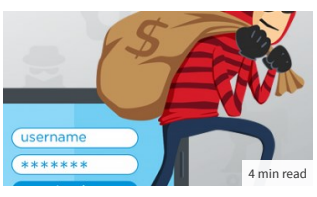


3 min read

SECURITY ALERTS

Beware: New wave of malware spreads via ISO file email attachments

We've seen a spike in malware concealed in ISO file email attachments. Learn more about this new threat and how you can protect yourself against ISO malware.



4 min read

MOBILE MALWARE · SECURITY ALERTS

Mobile malware targets Android users

Your mobile phone is the journal of your digital life. Who is reading yours? Emsisoft explores mobile malware and the best ways for you to prevent it.

Reader Comments