Nickname:
Password: 6-20 characters long
Public Terminal
Log In Forgot your password?
Sign in with
Google
Facebook
Twitter
LinkedIn

Close

Researchers Catch Microsoft Zero-Day Used To Install Government Spyware (vice.com)

Posted by BeauHD on Tuesday September 12, 2017 @08:05PM from the quick-on-your-feet dept.

An anonymous reader quotes a report from Motherboard: *Government hackers were using a previously-unknown vulnerability in Microsoft's .NET Framework, a development platform for building apps, to hack targets and infect them with spyware, according to security firm FireEye. The firm revealed the espionage campaign on Tuesday, on the same day Microsoft patched the vulnerability. According to FireEye, the bug, which until today was a zero-day, was being used by a customer of FinFisher, a company that sells surveillance and hacking technologies to governments around the world. The hackers sent a malicious Word RTF document to a "Russian speaker," according to Ben Read, FireEye's manager of cyber espionage research. The document was programmed to take advantage of the recently-patched vulnerability to install FinSpy, spyware designed by FinFisher. The spyware masqueraded as an image file called "left.jpg," according to FireEye.*

→

J.J. Abrams To Direct Star Wars: Episode IX; Premiere Date Pushed To December 2019
Google Engineer's Leaked 'Gender Diversity' Essay Draws Massive Response
Outsourced IT Workers Ask Sen Feinstein For Help, Get Form Letter in Return
Developer Accidentally Deletes Three-Month of Work With Visual Studio Code
The Working Dead: Which IT Jobs Are Bound For Extinction?
After Healthcare Defeat, Can The Trump Administration Fix America's H-1B Visa Program?
Submission: Researchers Catch Microsoft Zero-Day Used To Install Government Spyware

Why Bats Crash Into Windows

Researchers Catch Microsoft Zero-Day Used To Install Government Spyware More | Reply Login
Researchers Catch Microsoft Zero-Day Used To Install Government Spyware

Post Load All Comments
Search 35 Comments Log In/Create an Account
Full 3 Abbreviated 19 Hidden
Comments Filter:
- All
- Insightful
- Informative
- Interesting
- Funny

Score: 5 4 3 2 1 0 -1

The Fine Print: The following comments are owned by whoever posted them. We are not responsible for them in any way.

"to governments around the world"... (Score:2)
by turkeydance (1266624)
More | Reply Login
yep. yours, too, and to all the places you'll go.

Nickname:
Password: 6-20 characters long
Public Terminal
Log In Forgot your password?
Close
Close

Re: (Score:2)
by ls671 (1122017)
Interesting, is it a zero-day or a backdoor?

- **Re: Purpose of using Zero Day moniker? (Score:1)**
by Anonymous Coward
Also, if MS put out a patch today then it wasn't a zero day until today.
Zero day = the manufacturer doesn't know about it at all. Not how many days has a patch been available.
If it's a backdoor then it was never a zero day as the manufacturer always knew it was there.

- **Re: Purpose of using Zero Day moniker? (Score:2)**
by Monster_user (5075027)
Microsoft knew about it for far further back than today. To patch an exploit, it first has to be reported. Then it has to be reported by a reputable source, with information on how to recreate it, in order to prove there is a flaw that can be exploited. Then the developers have to come up with a solution to the exploit, and then spend man hours coding the remedy into a patch. The patch must then be tested to make sure it doesn't break existing functionality. If it breaks anything then a judgement call re

- **Re: (Score:2)**
by courteaudotbiz (1191083)
It's not a backdoor nor a vulnerability. It's a government feature that was discovered and MS locked the feature. Now the 3 letters agencies will have to revert to their other features to get into people's computers.

- **Re: (Score:2)**
by ls671 (1122017)
Come on Courteau! Yourself and I know that In Canada, they are called; 4 letter agencies. Thanks for adapting to the American way still...

NORTH KOREA or THE NSA (Score:4, Insightful)
by Anonymous Coward on Tuesday September 12, 2017 @08:15PM (#55185121)
Who has caused the most damage for American citizens?
NORTH KOREA or THE NSA?
Reply to This Share
twitter facebook linkedin
Flag as Inappropriate
2 hidden comments

- **Re:NORTH KOREA or THE NSA (Score:4, Insightful)**
by Opportunist (166417) on Tuesday September 12, 2017 @08:26PM (#55185179)
This is pretty much why I can't help but snicker every time someone says "But the Russians...". The harm "the Russians" can do to you are minimal compared to what your very own government can.
Reply to This Parent Share
twitter facebook linkedin
Flag as Inappropriate
8 hidden comments

- **Re: NORTH KOREA or THE NSA (Score:1)**
by Anonymous Coward
The NSA doesn't care about elections. They will get funded no matter who is elected.
There was, however, a concerted effort by the media to skew election polling results so they could keep saying the other guys are losing. They were wrong BTW. The media is always full of shit. Especially how badly they're covering EquiFUCKED, trying to do everything they can to not blame Equifuckers...

- **Re: (Score:2)**
by Opportunist (166417)
Like it would be any different for the average person if the other branch of The Party ruled.

- **Re: (Score:2)**
by Ol Olsoc (1175323)
This is pretty much why I can't help but snicker every time someone says "But the Russians...". The harm "the Russians" can do to you are minimal compared to what your very own government can.
I wonder if we might be able to concentrate on more than one issue at a time.
1 hidden comment

- **Re: (Score:2)**
by Opportunist (166417)
So? Nothing a few nukes can't fix.
And the fun part about the US' nukes is that the average person has no control over them. That's what you still need your army for.

- **Re: (Score:2)**
by Opportunist (166417)
Unlikely. He doesn't like faggy fawning of people over him.

- **Re: (Score:2)**
by Opportunist (166417)
Again, you live in the delusion that the other side of The Party does anything different. Care to show me the difference between 2000-2008 and 2008-2016 in US politics?

- **Re: (Score:2)**
by Plus1Entropy (4481723)
I think that's a bit disingenuous. Both things are threats to our liberty, in different ways and to different degrees. Just because I am concerned about Russia interfering in our elections doesn't mean that I am not concerned about

the rise of the surveillance state.
1 hidden comment

Re: (**Score:1**)
by Anonymous Coward
p>How do we begin to fix it? Vote in the Democratic primary (The Rethuglicans are lost) and vote for the candidate most likely to actually work toward cutting down the surveillance state. And NEVER vote for a Rethuglican. Vote a straight Democratic ticket in EVERY general election, not just the Presidential ones.
A better way to fix it is to break the chains binding you to a particular party. The "us versus them" mentality is a distraction. It has been carefully cultivated by both parties in varying degrees, blinding people to the fact that neither the Democrat nor Republican parties represent the average person, regardless whether you believe they did at some point in the past.
We are mice voting for white versus black cats.

Re: (**Score:2**)
by Opportunist (166417)
Holy shit, someone gets it.

Re: (**Score:2**)
by rtb61 (674572)
Good PR schtick but the reality is the whole world is concerned about the US hacking their elections, from extortion, to colour revolutions, coups against democracies to turn them into autocracies who will ruthlessly exploit their citizens at the behest of US corporations, to out and out invasion and mass murder of the population. Now all of these are proven facts and histories and not some bullshit about Russia spending $100,000 buying advertisements or foreign citizens reporting the crimes of the US gover

Re: (**Score:2**)
by grep -v '.*' * (780312)
"Oh, them? It never changes," she said. "It's always: location, location, location."

Re: (**Score:2**, **Interesting**)
by Marlin Schwanke (3574769)
Who has caused the most damage for American citizens?
NORTH KOREA or THE NSA?
Or state-sponsored hackers, fighting an undeclared cyber-war? 99% of the American citizenry were enjoying their usual lives, un-molested, prior to said hackers, oh, and of course, "patriotic" leakers, sharing our state secrets and many of our own cyber-war weapons with our "friends" at Wiki-Leaks. Dear Julian, having absolutely no compunctions, if it increases his importance and fluffs his, umm, ego has done quite a bit of damage. Did was really need him to out the basis for the recent ransom-ware attack

Re: (**Score:2**)
by Macfox (50100)
The concept of transparency and accountability must be new to you.
The NSA was checking everyone's front door, so they could gain access "if" they ever needed to, but claiming they have your interest at heart.

Re: (**Score:2**)
by Marlin Schwanke (3574769)
The question was, “Who has caused the most damage for American citizens?” The NSA’s activities are certainly objectionable but how much real damage have they done to American citizens?

Re: (**Score:2**)
by Macfox (50100)
So far Kim has done Jack all, but thrown a few insults and made threats. The NSA in its irresponsible handling of sensitive data and munitions has cost the Americans much more indirectly.

Software proprietors cause massive damage. (**Score:2**)
by jbn-o (555068)
Who has caused the most damage for American citizens?
Software proprietors, regardless of nationality, current employment, or current residence. Brad Kuhn said it well in his blog post, "Software Freedom Doesn't Kill People, Your Security Through Obscurity Kills People [ebb.org]".

Re: (**Score:2**)
by Gravis Zero (934156)
Who has caused the most damage for American citizens?
NORTH KOREA or THE NSA?
Microsoft.

Re: (**Score:2**)
by (4475953)
Neither of them. The American citizens themselves, by electing Donald Trump as a president - and previously Bush Jr. and his regime, who probably caused the biggest damage to the US so far that any government has ever caused.

Not much of an exploit (**Score:2**)
by fustakrakich (1673220)
The guy still had to download and open the Word doc.
And I hope FireEye isn't trying to claim to be some kind of hero in this. The timing of their "revelation" is highly suspicious.
1 hidden comment

Re: (**Score:1**)
by Anonymous Coward
I'm safe. I don't have Office.
I'm human, and I don't have office either.
how is life as a safe?
1 hidden comment

Re: (**Score:1**)
by fustakrakich (1673220)
And furthermore, anyone who doesn't believe in full public disclosure upon discovery is a *BLEEEEE..*

Re: (**Score:2**)
by Koby77 (992785)
Hasn't microsoft missed a patch tuesday in the past, causing a researcher to reveal a zero day because of a time limit policy on withholding the vulnerability from the public? I agree the timing is suspicious, but it may be that FireEye said "We're revealing it on 9/12/2017, so you better not miss patch tuesday, but if you do release then everything will be okay." I'm just pointing that out as a possibility; we may never know what is said behind the scenes.

We need a survey! (**Score:2**)
by Snotnose (212196)
Questions: Are you surprised by this?

a) No
b) Yes
c) I'm a clueless asshat, can I read a story now?

The dark covenant (**Score:3**)
by lucm (889690) on Tuesday September 12, 2017 @08:58PM (#55185301)
Those guys are playing with evil forces.
FireEye analyzed a Microsoft Word document where attackers used the arbitrary code injection to download and execute a Visual Basic script that contained PowerShell commands.
RTF -> VBScript -> PowerShell -> Chtulhu awakens

Reply to This Share

twitter facebook linkedin
Flag as Inappropriate
1 hidden comment

Re: (**Score:3**)
by Mal-2 (675116)
Why is it that Windows & Linux are always getting hacked but you never hear about exploits for the Mac huh?
What gives!?
Because you're not paying attention.
https://www.exploit-db.com/exploits/36692/ [exploit-db.com]

Re: (**Score:2**)
by Bite The Pillow (3087109)
That's why no one here RTFs Anything.

What Brian LaMacchia said about .NET security (**Score:2**, **Interesting**)
by Anonymous Coward
Brian Malacchia was one of the authors of .NET. I had the pleasant experience of hearing him speak at MIT about the upcoming "Trusted Computing" software. What made it fun was that Richard Stallman was in the room, which Brian was *not* expecting, and proceeded to call into question the entire "Microsoft holds the private keys, and revolcation keys for all your hardware and software" security model. Brian pointed out that if Microsoft ever did the pernicious tricks Richard Stallman was worried about, that h

Re: (**Score:2**)
by basecastula (2556196)
out of points. interesting

Related Links **Top of the: day, week, month.**
- 1122 comments Google Engineer's Leaked 'Gender Diversity' Essay Draws Massive Response
- 813 comments Outsourced IT Workers Ask Sen Feinstein For Help, Get Form Letter in Return
- 765 comments Developer Accidentally Deletes Three-Month of Work With Visual Studio Code
- 581 comments The Working Dead: Which IT Jobs Are Bound For Extinction?
- 566 comments After Healthcare Defeat, Can The Trump Administration Fix America's H-1B Visa Program?

next

Why Bats Crash Into Windows
73 comments

previous

JJ. Abrams To Direct Star Wars: Episode IX; Premiere Date Pushed To December 2019
89 comments

53 of 53 loaded

Gosh that takes me back... or is it forward? That's the trouble with time travel, you never can tell." -- Doctor Who, "Androids of Tara"

Working...