THE SHADOW BROKERS VULNERABILITY EQUITIES PROCESS: NSA HAS HAD AT LEAST 96 DAYS TO WARN MICROSOFT ABOUT THESE FILES

On January 8, Shadow Brokers announced an auction of Windows Warez, with lists of the exploits he/they had for sale (these two posts from Malware Jake provide analysis of them). Four days later, SB released a different set of Windows exploits, a more dated set that (SB claimed) Kaspersky Labs had had some visibility onto. The Windows files released today include the ones offered for sale back in January, down to the version numbers. Compare, in particular, the touch, exploit, and payloads with this screencap. SB announced Fuzzbunch and DanderSpritz in January, too.

```
Plugin Category: touch
======================

  Name                    Version
  ----                    -------
  Architouch              1.0.0
  Domaintouch             1.1.1
  Eclipsedwingtouch       1.0.4
  Educatedscholartouch    1.0.0
  Emeraldthreadtouch      1.0.0
  Erraticgophertouch      1.0.1
  Esteemaudittouch        2.1.0
  Explodingcantouch       1.2.1
  Iistouch                1.2.2
  Namedpipetouch          2.0.0
  Printjobdelete          1.0.0
  Printjoblist            1.0.0
  Rpctouch                2.1.0
  Smbtouch                1.1.1
  Webadmintouch           1.0.1
  Worldclienttouch        1.0.1

fb > show exploit

Plugin Category: exploit
========================

  Name                    Version
  ----                    -------
  Easybee                 1.0.1
  Easypi                  3.1.0
  Eclipsedwing            1.5.2
  Educatedscholar         1.0.0
  Emeraldthread           3.0.0
  Emphasismine            3.4.0
  Englishmansdentist      1.2.0
  Erraticgopher           1.0.1
  Eskimoroll              1.1.1
  Esteemaudit             2.1.0
  Eternalromance          1.4.0
  Eternalsynergy          1.0.1
  Ewokfrenzy              2.0.0
  Explodingcan            2.0.2
  Zippybeer               1.0.2

fb > show payload

Plugin Category: payload
========================

  Name              Version
  ----              -------
  Doublepulsar      1.3.1
  Jobadd            1.1.1
  Jobdelete         1.1.1
  Joblist           1.1.1
  Pcdlllauncher     2.3.1
  Processlist       1.1.1
  Regdelete         1.1.1
  Regenum           1.1.1
  Regread           1.1.1
  Regwrite          1.1.1
  Rpcproxy          1.0.1
  Smbdelete         1.1.1
  Smblist           1.1.1
  Smbread           1.1.1
  Smbwrite          1.1.1
```

That's a critical detail for the debate going on on Twitter and in chats about how shitty it was for SB to release these files on Good Friday, just before (or for those with generous vacation schedules, at the beginning of) a holiday weekend. While those trying to defend against the files and those trying to exploit them are racing against the clock and each other, it is not the case that the folks at NSA got no warning. NSA has had, at a minimum, 96 days of warning, knowing that SB could drop the files at any time.

The big question, of course, is whether NSA told Microsoft what the files targeted. Certainly, Microsoft had not fully responded to that warning, as hackers have already gotten a number of these files to work.

With WikiLeaks's Vault 7 files, it's at least possible the CIA doesn't know precisely what got leaked to WikiLeaks, even though the government immediately identified when and how the files were breached. The NSA cannot make that claim here, at least not with the Windows files. SB was kind enough to provide warning. The question is, what did NSA do with that warning.

The fact that SB provided that warning, though, should have very serious ramifications for the Vulnerabilities Equities Process, under which the NSA is supposed to consider whether it is better to alert companies to exploits or to sit on them and use them. It's one thing to decide NSA's spying takes precedence over the security of the customers of big American companies. It's another thing to keep those exploits in a way that makes them vulnerable to theft, as both CIA and NSA have done.

But it should be beyond question that when an intelligence agency gets a very detailed list of a group of exploits a malicious entity plans to release, the agency should warn the American companies affected.

Update: Microsoft told Sam Biddle they haven't heard from any "individual or organization."

> A Microsoft spokesperson told The Intercept “We are reviewing the report and will take the necessary actions to protect our customers.” We asked Microsoft if the NSA at any point offered to provide information that would help protect Windows users from these attacks, given that the leak has been threatened since August 2016, to which they replied “our focus at this time is reviewing the current report.” The company later clarified that “At this time, other than reporters, no individual or organization has contacted us in relation to the materials released by Shadow Brokers.”

I think there’s actually some wiggle room in there. We shall see how long it takes MSFT to patch this stuff.

Update: MSFT released a statement that said all but three of these had been addressed. Three of them were addressed in their March update, and another this year. Which would suggest NSA did warn them.