MalwareJake

Ramblings about security, rants about insecurity, occasional notes about reverse engineering, and of course, musings about malware. What more could you ask for?

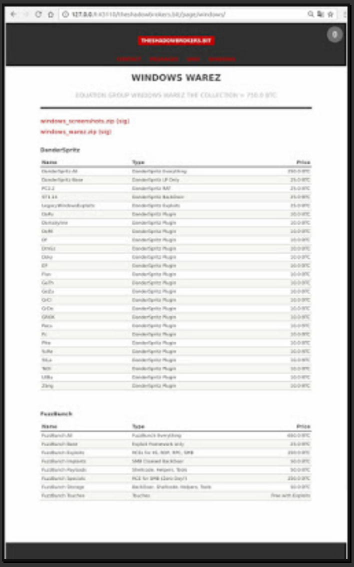
Sunday, January 8, 2017

Implications of the newest Shadow Brokers offerings

Shadow Brokers are at it again, this time ofering apparent Windows exploits and toolkits. The timing of this does not seem coincidental. If Shadow Brokers are to be believed, they've been holding the tools for some time and just now releasing the Windows toolkits. Previously they have released other tool sets, but nothing that operated against or exploited Windows.

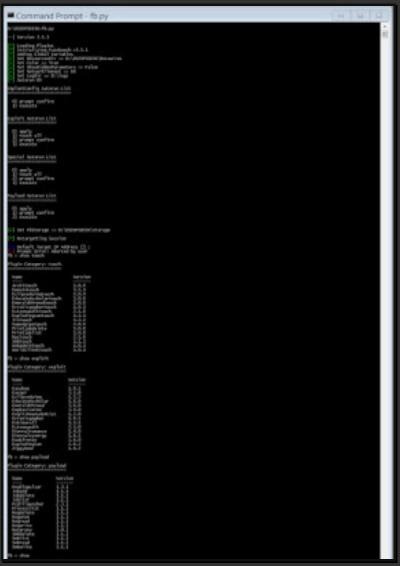
The Tools

What of the tools? There's little specific infomation about the tools, but I've included some images here from Twitter. In the last I've embedded tweets, but when accounts get suspended, the tweets are no longer available. It's at least plausible that this account will be suspended...



WINDOWS WAREZ

This screenshot shows the price for individual components. Most interesting perhaps is the fact that the exploits contain a possible SMB zero day exploit. For the price requested, one would hope it is a zero day. The price is far too high for an exploit for a known vulnerability



Command Prompt - fb.py

This screenshot shows a number of names of apparent tools in the dump. Of particular interest are the version numbers. Note that most of the tools have apparently been through multiple revisions, adding apparent legitimacy to the claim that these exploits are real.Though another

Followers

Blog Archive

▼ 2017 (9)
- ▼ January (9)
  - Shadow Brokers - Russian thoughts?
  - Blind recruiting on LinkedIn - advice to recruiter...
  - Novel malware sandbox evasion
  - More finds from the Shadow Brokers dump
  - Implications of the newest Shadow Brokers offering...
  - Putting science in CTI with GRIZZLY STEPPE usage
  - The JAR did more harm than good
  - What should CTI teams be telling leadership?
  - Russian election hacking sanctions

► 2016 (113)

► 2015 (62)

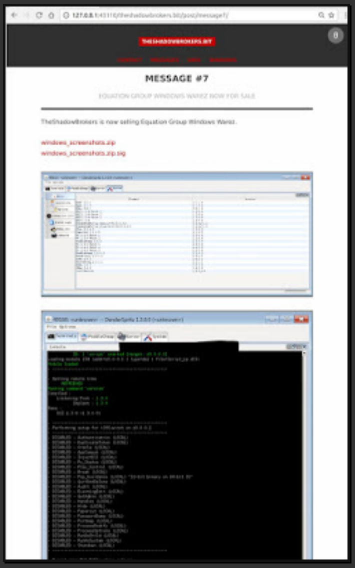
► 2014 (25)

► 2013 (27)

Contributors

- Jacob Williams
- Jake Williams

that might be interesting. Of particular interest is WorldClientTouch - suggesting that perhaps one of the code-named exploits work against MDaemon's web based email client?



MESSAGE #7

EQUATION GROUP WINDOWS WAREZ NOW FOR SALE

TheShadowBrokers is now selling Equation Group Windows Warez.

windows_screenshots.zip
windows_screenshots.zip.sig

Finally, this screenshot seems to show someinformation about the tools available. Some capabilities like "GetAdmin" and "PasswordDump" seem rather obviously needed capabilities.

However, the listed plugin "EventLogEdit" is significant for digital forensics and incident response (DFIR) professionals investigating APT cases. While we understand that event logs can be cleared and event logging stopped, surgically editing event logs is usually considered to be a very advanced capability (if possible at all). We've seen rootkit code over the years (some was published on the now defunct rootkit.com) that supported this feature, but often made the system unstable in the process.

Knowing that some attackers apparently have the ability to edit event logs can be a game changer for an investigation. If Shadow Brokers release this code to the world (as they've done previously), it will undermine the reliability of event logs in forensic investigations. Cyberark recently claimed that event logs might be subject to tampering, though it doesn't appear that they were discussing the Shadow Brokers capability specifically

The Timing
So what do we make of the timing? It's hard believe that the timing is purely coincidental and has nothing to do with the release by US intelligence about the Russian hacking of the DNC.

The theory that immediately comes to mind is that Shadow Brokers are Russian or Russian operatives and the release of the Windows toolkit is retaliation for the report. Unlike previous dumps, this dump goes a bit further, showing screenshots of the GUI tools and execution of some scripts. However, it is important to note that no tools are offered for proof of the dump this time. Only screenshots and descriptions of the tools are offered.

An alternative theory is that Shadow Brokers are not Russian and are timing this release to shift the blame to Russia. There's unfortunately no way to test this theory.

Finally, there's the theory that the timing of this latest Shadow Brokers release has nothing to do with the intelligence community report. This seems the least likely. Shadow Brokers must have known that people would make this analytic leap, so even if they scheduled this release some time ago, the decision to go ahead given the release of the report on Russian hacking was done with the understanding that connections would be made.

Conclusion
Regardless of your feelings on timing or what we know of the tools themselves, this is certainly an interesting development.

Posted by Jacob Williams at 2:46 AM

G+1 +3 Recommend this on Google

No comments:

Post a Comment

Note: Only a member of this blog may post a comment.

Comment as: Google Accour ▾

Publish Preview

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)