New NSA Data Dump: ShadowBrokers Release UNITEDRAKE Malware

hackread.com/nsa-data-dump-shadowbrokers-expose-unitedrake-malware/

September 7, 2017

The ShadowBrokers is a group of hackers known for leaking exclusive information about the National Security Agency – NSA's hacking tools and tactics.

In their latest leak, they have released the UNITEDRAKE NSA exploit, which is a remote access and control tool that can remotely target Windows-based systems to capture desired information and transfer it to a server. It captures information using plugins to compromise webcam and microphone output along with documenting log keystrokes, carrying out surveillance and access external drives.

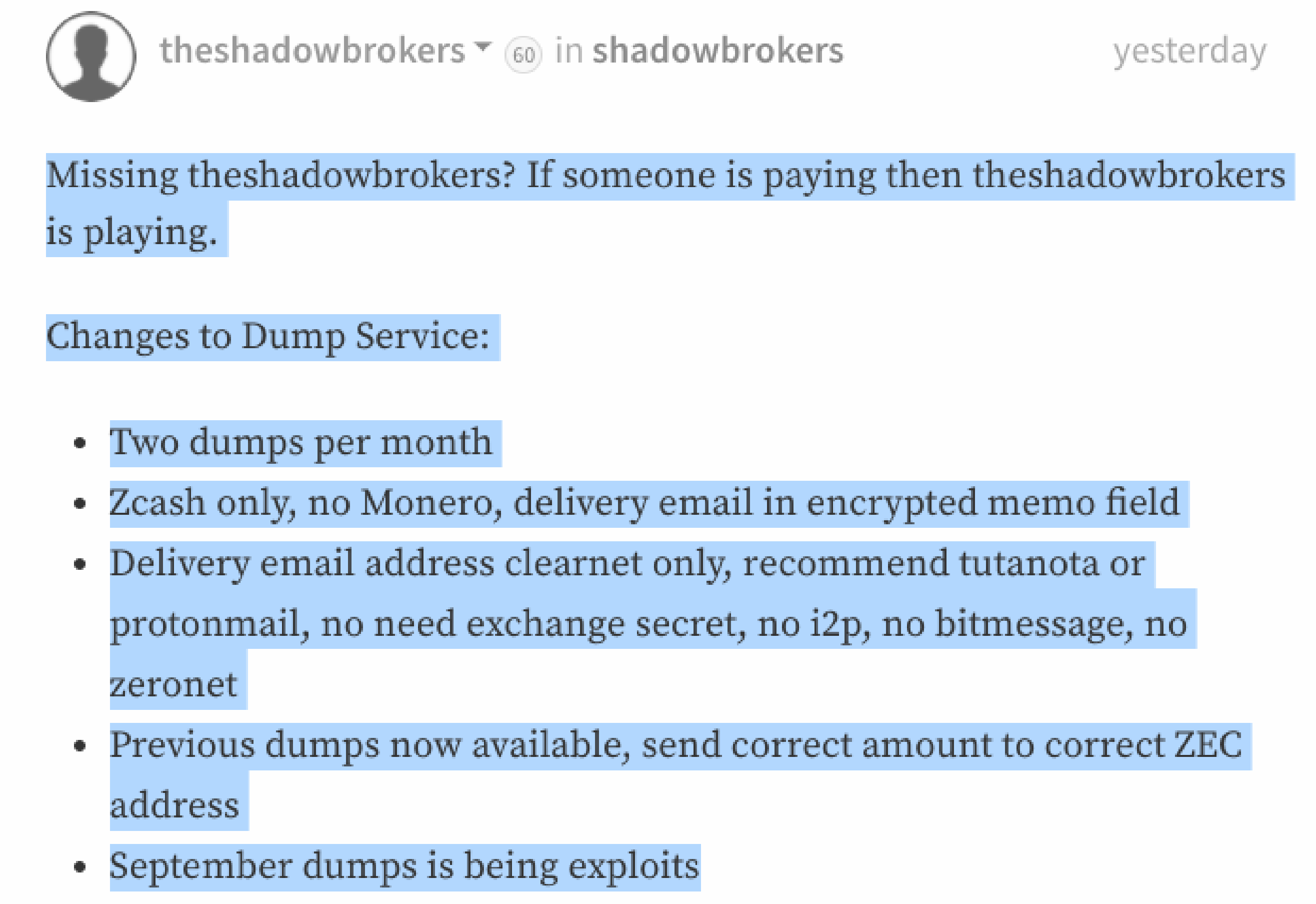
The modular malware UNITEDRAKE is compatible with systems running on Microsoft Windows XP, Vista, 7, 8 up to Windows Server 2012. UNITEDRAKE is described as a "fully extensible" data collection tool that is specifically developed for Windows machines to allow operators the chance of controlling a device completely.

As cited by ZDNet, the malware modules like FOGGYBOTTOM and GROK can successfully listen to and monitor communications, and keep a check on keystrokes, webcam, and microphone. When the task is completed, the malware is able to self-destruct. Understandably, the NSA developed this tool to carry out mass surveillance and performed bulk hacking.

We first heard about UNITEDRAKE RAT back in 2014 when former NSA contractor Edward Snowden exposed an array of confidential documents in a high-profile scandal exposing the espionage tactics used by the NSA for decades. Snowden revealed a glaring truth related to NSA spying tactics that the agency had been using multiple malware programs to infect not hundreds or thousands but millions of computers across the globe to acquire valuable, sensitive data.

On the other hand, ShadowBrokers group made headlines in 2016 when it claimed to have robbed various exploitation tools used by the NSA including the notorious ETERNALBLUE that was a vital component in the WannaCry ransomware campaign causing damages to systems worldwide. The claim was proved to be authentic by security experts as well.

ShadowBrokers has now decided to release two data dumps every month dubbed as the Monthly Dump Service. For its latest data dump, the group is expecting to receive 500 Zcash, a type of cryptocurrency, which facilitates secure, private transactions. It is worth noting that the current rate of Zcash is US$248 per unit or A$309.50 per unit.



theshadowbrokers 60 in shadowbrokers yesterday

Missing theshadowbrokers? If someone is paying then theshadowbrokers is playing.

Changes to Dump Service:

- Two dumps per month
- Zcash only, no Monero, delivery email in encrypted memo field
- Delivery email address clearnet only, recommend tutanota or protonmail, no need exchange secret, no i2p, no bitmessage, no zeronet
- Previous dumps now available, send correct amount to correct ZEC address
- September dumps is being exploits

Screenshot from ShadowBrokers's post on Steemit.

The data dump also includes a UNITEDRAKE manual, which means the group is trying to generate additional interest among cyber criminals, vendors, and government groups to subscribe to services which provide access to the stolen exploits and malware models.

According to ShadowBrokers, five NSA data dumps are in the pipeline currently and the group is demanding a whopping 16,000 Zcash for files to be released on November 15. Moreover, to further enlarge the profits, ShadowBrokers intend to make previous data dumps available again for purchase and this time the price range will be somewhere between 100 ZEC ($24,000) and 1600 ZEC ($3.8m).

The group's subscription service is currently operating discreetly. However, the members have started complaining about the tools not working as expected. A few months back one of its subscribers came out in public and complained that the "Wine of the month" club was a fake scheme.