ShadowBrokers are back demanding nearly $4m and offering 2 dumps per month

securityaffairs.co/wordpress/62770/hacking/shadowbrokers-return.html

September 6, 2017

The dreaded hacking group ShadowBrokers posted a new message, promising to deliver two data dumps a month as part its monthly dumps.

The notorious group ShadowBrokers is back with announcing new interesting changes to their Dump Service.

The hackers published a new message on the Steemit platform announcing new changed to their service.

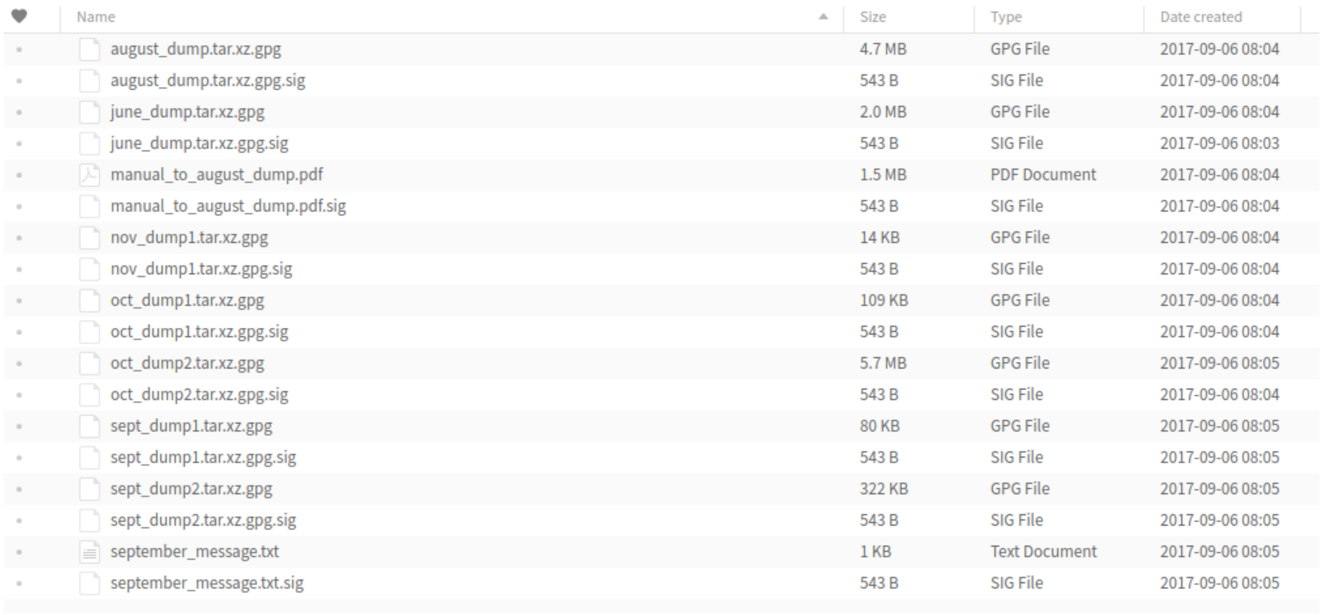
"*Missing theshadowbrokers? If someone is paying then theshadowbrokers is playing.*"

The hacker group made headlines in April after publicly leaking exploits allegedly stolen from the NSA-Linked group Equation Group.

The changes for the Dump Service included 2 dumps per month and the possibility to pay only with ZCash cryptocurrency:

- 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 exploit

Below the "price list" shared by the group, it includes old dumps and future dumps, from June 30 until November 15.



Name	Size	Type	Date created
august_dump.tar.xz.gpg	4.7 MB	GPG File	2017-09-06 08:04
august_dump.tar.xz.gpg.sig	543 B	SIG File	2017-09-06 08:04
june_dump.tar.xz.gpg	2.0 MB	GPG File	2017-09-06 08:04
june_dump.tar.xz.gpg.sig	543 B	SIG File	2017-09-06 08:03
manual_to_august_dump.pdf	1.5 MB	PDF Document	2017-09-06 08:04
manual_to_august_dump.pdf.sig	543 B	SIG File	2017-09-06 08:04
nov_dump1.tar.xz.gpg	14 KB	GPG File	2017-09-06 08:04
nov_dump1.tar.xz.gpg.sig	543 B	SIG File	2017-09-06 08:04
oct_dump1.tar.xz.gpg	109 KB	GPG File	2017-09-06 08:04
oct_dump1.tar.xz.gpg.sig	543 B	SIG File	2017-09-06 08:04
oct_dump2.tar.xz.gpg	5.7 MB	GPG File	2017-09-06 08:05
oct_dump2.tar.xz.gpg.sig	543 B	SIG File	2017-09-06 08:04
sept_dump1.tar.xz.gpg	80 KB	GPG File	2017-09-06 08:05
sept_dump1.tar.xz.gpg.sig	543 B	SIG File	2017-09-06 08:05
sept_dump2.tar.xz.gpg	322 KB	GPG File	2017-09-06 08:05
sept_dump2.tar.xz.gpg.sig	543 B	SIG File	2017-09-06 08:05
september_message.txt	1 KB	Text Document	2017-09-06 08:05
september_message.txt.sig	543 B	SIG File	2017-09-06 08:05

The amount of money requested by ShadowBrokers is substantially increased compared to the initial demand of 100 ZEC (~24k USD) in June, when the hackers started their first monthly dump service. Now, the hackers are offering the exploits for 16,000 ZEC, which amounts to $3,914,080.

ShadowBrokers leaked the manual for the NSA exploit dubbed UNITEDRAKE, it is one of the implants used by the NSA's elite hacking unit TAO (Tailored Access Operations).

> Here's UNITED RAKE (Windows tool) from the Shadow Brokers dump mentioned in a Snowden document https://t.co/1hQAz2Annd pic.twitter.com/Drljghk9Ka
>
> — Joseph Cox (@josephfcox) September 6, 2017

According to the leaked manual, UNITEDRAKE implant is a "fully extensible remote collection system designed for Windows targets".

> BREAK! #ShadowBrokers just leaked the manual for #UNITEDRAKE https://t.co/SJazaxidXS
>
> — Rickey Gevers (@UID_) September 6, 2017

> Turns out Kaspersky had a post about UNITEDRAKE dated March 11th 2015. They called UNITEDRAKE EquationDrug. https://t.co/MBw9OI7A6w
>
> — Rickey Gevers (@UID_) September 6, 2017

Files, Signed Message, Manual to August Dump:

https://mega.nz/#F!QGAyVTJL!0cJlvWpQ4dPcKLu-oN766w

Stay Tuned!

Written by: @GranetMan and Pierluigi Paganini

Granet is a young and Junior IT Security Researcher, he is passionate in Linux, Arduino, Digital Forensics, Cyber Security, Free software and Malware Analysis

Pierluigi Paganini

(Security Affairs – ShadowBrokers, hacking)

CybercrimeEquation groupHackingmalwareMicrosoftNSAShadow brokerswannacry ransomware

Share On

Back to top

- Home
- Cyber Crime
- Cyber warfare
- APT
- Data Breach
- Deep Web
- Digital ID
- Hacking
- Hacktivism
- Intelligence
- Internet of Things
- Laws and regulations
- Malware
- Mobile
- Reports
- Security
- Social Networks
- Terrorism

- ICS-SCADA
- EXTENDED COOKIE POLICY
- Contact me