**Newly Detected Malware Uses NSA Exploit To Mine Monero, Over 500K PCs Infected**

[Cryptocurrency mining](https://cointelegraph.com/tags/mining) botnet [malware](https://cointelegraph.com/tags/malware%22%20%5Ct%20%22_blank) Smominru has infected more than 526,000 computers using a leaked NSA exploit, The Hacker News [reported](https://thehackernews.com/2018/01/cryptocurrency-mining-malware.html%22%20%5Ct%20%22_blank) yesterday, Jan. 31.

Software [security](https://cointelegraph.com/tags/security%22%20%5Ct%20%22_blank) researchers from cybersecurity company [Proofpoint](https://www.proofpoint.com/us%22%20%5Ct%20%22_blank) have detected a new global botnet called Smominru, also known as Ismo, that uses a National Security Agency (NSA) exploit EternalBlue to spread [Monero](https://cointelegraph.com/tags/Monero%22%20%5Ct%20%22_top) mining malware.

The EternalBlue exploit was leaked by the so-called [Shadow Brokers](https://cointelegraph.com/news/us-spooks-compromised-swift-banking-network-hackers-group%22%20%5Ct%20%22_top) hackers who were reportedly also behind the 2017 widespread [WannaCry](https://cointelegraph.com/tags/wannacry%22%20%5Ct%20%22_top) ransomware threat, according to The Hacker News.

Proofpoint reported that the Smominru botnet has been infecting computers since May 2017, mining about 24 Monero coins per day. To date, the botnet has reportedly managed to mine about 8,900 Monero, or about [$2.1 million](https://coinmarketcap.com/currencies/monero/) at press time. The highest number of Smominru-infected PCs has been found in Russia, India, and Taiwan, researchers said.

According to Proofpoint, cybercriminals are targeting vulnerable version of Windows, also using a leaked NSA protocol exploit called EsteemAudit.

According to thehackernews.com, the experts also notified DDoS protection service [SharkTech](https://sharktech.net/%22%20%5Ct%20%22_blank)where Smominru’s command and control infrastructure has been detected, however, they didn’t get a response.

As Cointelegraph [reported](https://cointelegraph.com/news/crypto-mining-malware-epidemic-55-of-businesses-affected-worldwide-including-youtube%22%20%5Ct%20%22_blank) Jan. 28, a massive Monero-mining malware attack via online ads,  mostly attributed to the controversial cryptocurrency mining and advertising platform [Coinhive](https://cointelegraph.com/news/showtime-latest-secret-crypto-pirate-miner%22%20%5Ct%20%22_top), has affected a huge number of users and online businesses worldwide, including Youtube.

**ПЕРЕВОД**

Использование эксплойта АНБ для майнинга Monero замечено вновь, более 500 000 компьютеров заражено

Вчера, 31 января, социальный новостной сайт Hacker News сообщил, что криптовалютный вирус-майнер Smominru заразил более 526 000 компьютеров, используя эксплойт, похищенный у Агентства Национальной Безопасности.

Специалисты по безопасности программного обеспечения из компании Proofpoint, специализирующейся на кибербезопасности, обнаружили новый глобальный ботнет под названием Smominru, известный также как Ismo, который использует эксплойт EternalBlue, принадлежащий Агентству Национальной Безопасности (АНБ), с целью распространить вирус-майнер на Monero.

По данным Hacker News, в 2017 году эксплойт EternalBlue был похищен так называемой хакерской группой Shadow Brokers, создателями масштабного вируса-вымогателя WannaCry.

Proofpoint сообщает, что ботнет Smominru заражает компьютеры с мая 2017 года, добывая около 24 токенов Monero в день. На сегодняшний день ботнету удалось получить около 8 900 токенов Monero или приблизительно 2.1 миллиона долларов. По словам специалистов, наибольшее количество компьютеров Smominru заразил в России, Индии и на Тайване.

По словам Proofpoint, киберпреступники нацелены на компьютерную уязвимость в Windows, используя похищенный у АНБ эксплойт EsteemAudit, который может атаковать протокол.

Согласно thehackernews.com, эксперты также уведомили сервис защиты от DDoS-атак SharkTech, на котором были замечены команды и инфраструктура Smominru, однако ответа не поступило.

Согласно сообщению от Cointelegraph 28 января, крупная атака вирус-майнера на Monero через рекламу в интернете, которая главным образом была связана с противоречивым видом майнинга криптовалют и рекламной платформой проекта Coinhive, негативно воздействовала на большое количество пользователей и онлайн бизнес по всему миру, включая Youtube.