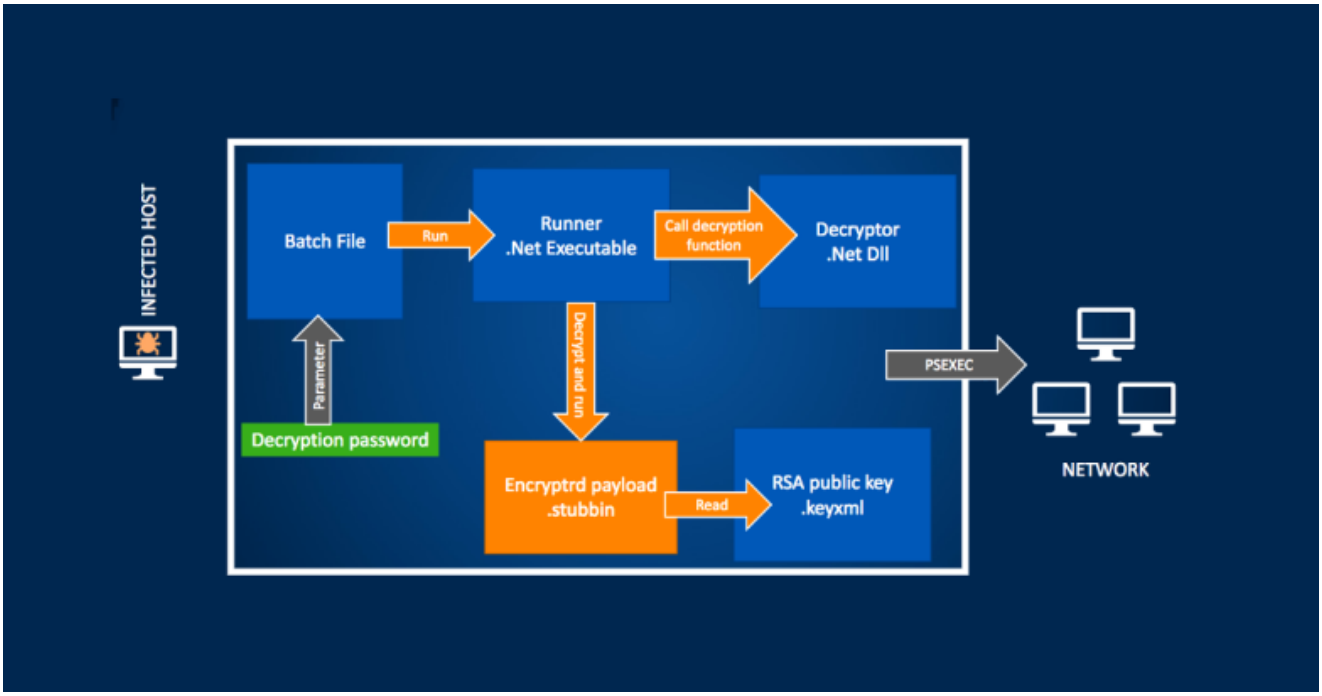
“SamSam” ransomware – a mean old dog with a nasty new trick

nakedsecurity.sophos.com/2018/05/01/samsam-ransomware-a-mean-old-dog-with-a-nasty-new-trick-report/

By Paul Ducklin 01 May 2018



One cybersecurity catchphrase you’ll hear these days is that “X is the new ransomware”.

That’s because the ransomware scene is no longer clearly dominated by long-running, well-known “brand names” (so to speak) such as CryptoLocker, TeslaCrypt or Locky.

In other words, many people are convinced that ransomware has had its day, is dying out, and new threats are taking over.

A popular value for the variable X in the equation above is *cryptojacking*, where crooks sneakily insinuate cryptocurrency mining software onto your computer or into your browser.

Rather than snatching away your files, like ransomware does, cryptojackers steal your processing power and your electricity instead.

This means that the crooks earn a tiny bit of money from every victim for as long as they’re infected, rather that taking the all-or-nothing approach of ransomware, where victims face a stark choice: pay and win, or refuse and lose.

The thing is, neither cryptojacking, nor indeed any other cyberthreat, is the “new ransomware”.

If you must know, RANSOMWARE is the new ransomware.

As often happens in the world of cybercrime, old threats stay with us for ages, and new threats simply add themselves to the mix rather than taking over. (Do you seriously think that we'll ever see the end of spam, for example?)

This year, we've seen a carefully orchestrated ransomware campaign known as **SamSam**, where the crooks have settled on a new mode of operation.

Instead of blasting out one copy of the malware out to thousands of potential victims over a day or two, the crooks blast thousands of copies of the malware onto computers inside a single organisation, pretty much all at once…

…and then, almost casually, they offer a "volume discount" to fix the entire company in one fell swoop.

SophosLabs just published an intriguing technical paper about the SamSam menace, and in the sample discussed in the paper, the malware includes a BAT file that lets the crooks set their price point for each attack:

```
@echo off
SET runner=mswinupdate.exe
SET password=%1
SET path=xxxxxxxxxx
SET totalprice=5
SET priceperhost=0.8
```

The prices above are denominated in BTC (Bitcoin), with BTC0.8 being the cost to decrypt an individual computer, and BTC5 being the price of a "master key" to decrypt as many as you want.

The Bitcoin prices seem to be adjusted, based on the BTC-to-US$ exchange rate at the time of the attack, so that the all-you-can-eat discount price works out at about $45,000 each time.

At the equivalent of $7,200 per PC, but "just" $45,000 to decrypt your whole company, it's almost as though the criminals are doing you a favour!

We don't know why the price is $45,000. For all we know, that number was picked because it's below certain reporting thresholds, or because the crooks want to pick the highest value they dare without getting into corporate board-level approval territory. All we can say is that $45,000 is a lot of money.

Learn more about this new trend in ransomware by reading the paper now. (No registration required.)

SamSam ransomware chooses its targets carefully

READ NOW ▶

By Dorka Palotay and Peter Mackenzie, SophosLabs

A Sophos Whitepaper April 2018