Science Translations
Established 1990
PC410.COM™
PC Updater News

Norton’s Last Gasp is Crypto Mining

Norton really isn’t what they were; they have a history of merging with companies with either good or so-so products, and then gradually letting them die. Symantec, which was the company name and the trademark for corporate/enterprise security products, sold its Symantec brand name and the enterprise services parts of the company to Broadcom back in 2019. What was left was rebranded NortonLifeLock, named after the Lifelock brand, which had been acquired in an earlier acquisition back in 2017. Lifelock was the company selling security services on television, with the founder’s social security number on billboards and buses, guaranteeing 100% identity protection. As a result, he was hacked 13 times during 2007 and 2008. That founder resigned, and is probably still dealing with the consequences of those hacks. The Federal Trade Commission issued a $100 million penalty against LifeLock for their advertising deceptions. That was in 2015.

More here, in the History section:
https://en.wikipedia.org/wiki/LifeLock

Norton security products, in the meantime, are known among technicians for creating a heavy load on computers, so that the computers slow down or become usuable, with a broken uninstall program that tends to disable the internet. (I will not uninstall Norton 360 remotely. Hands-on only. I don't install it. No exceptions.) So it has not been a recommended product since back in the MS-DOS days, when founder Peter Norton still owned it and ran it. But he sold to Symantec in 1990, and those products now are not remotely what they were.

Cryptomining?

First, what is cryptocurrency? Well, it is an attempt to create an inflation-proof digital currency that is secure and untraceable, with no way to create a transaction reversal or chargeback. It got the inflation-proof part right by using cryptography mathematics to permanently limit the number of 'coins' that are created. However, government agencies have managed to trace and reverse transactions, and of course, these are the payments typically used for ransomware.

Bitcoin and the other crypto currencies are not coins; they have no physical existence beyond being computer files. It isn't a stock, a bond, or any other type of financial security, not a representation of investment or ownership, in anything. It has no government backing and no central authority 'in charge' of it. It's just a digital file with internal digital proof of authenticity. As such, it has all the intrinsic value of whatever the market will bear, so it could easily go to zero value.

And Cryptomining is basically using computer power to calculate and create those digital files. The way that the math works, there is a fixed number of coins possible, and they're progressively more difficult to mine or calculate as the number of coins found approaches the limit. At this point, it costs too much in electrical power to bother creating your own coins by mining, at least for the original crypto currency, BitCoin.

Norton

So the current Norton 360, from the company now known as NortonLifeLock, is installing a background crypto-mining program, by default, while installing their security software. It is running background calculations to mine Ethereum crypto currency, and creating a wallet for users with their 'balance,' which can be moved over to an account over at Coinbase.com, which can be very loosely described as an online storage and exchange area for crypto currencies.

NortonLifeLock keeps a 15% commission, and there is also an exchange fee when moving the currency.

They're claiming that mining is off by default, but some users are having trouble disabling it. So does NortonLifeLock keep all the mined crypto currency that is not redeemed, whenever an account expires? Great revenue model for them, I suppose. Of course, most computers running their product would take the lifetime of the computer to mine a dollar's worth of currency. It's not remotely efficient, and yes, ALL background processing slows down computers, increases electrical usage, and heats the processor, which shortens hardware life.

Yes, crypto mining can be turned off; there are directions online. My own directions are to uninstall the product, AFTER checking if there is a balance due to you for crypto mining on the computer. And because Norton has a long history of unauthorized credit card auto-billing at more than the original transaction amount, close the account with NortonLifeLock, and get a confirmation email for that closure.

This is all sad. The Norton Utilities were the best available products in their category, starting back in 1982. They were quite usable in the 1990's, immediately after the Symantec merger. I used to specialize in installing their PC Anywhere product for remote access, around the turn of the century. And then one or two of their products became unusable each year after that. At this point, there's nothing worthwhile left. All gone

.

Avira, and maybe Avast, and More

Avira is a well-known antivirus (endpoint security) product, with a popular free version. But it's going the way of Norton 360. NortonLifelock bought Avira in January 2021, and now there is an Ethereum cryptominer in Avira. An opt-in is reportedly required to start earning crypto currencies, and there's even a caution to opt out if the country the computer is in prohibits Ethereum. (list below)

But there's more. Last August, NortonLifeLock announced an agreement to buy another antivirus vendor, Avast. And Avast also owns antivirus vendor AVG, and the Piriform products CCleaner and Speccy.

Background:

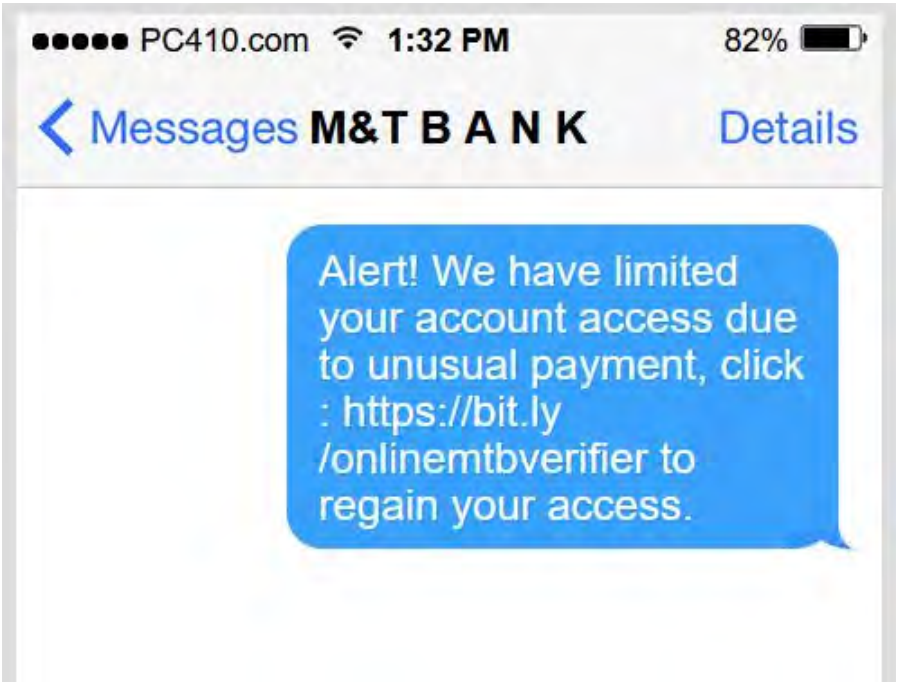
https://krebsonsecurity.com/2022/01/norton-360-now-comes-with-a-cryptominer/

This video explains BitCoin very well, but it gets heavily into all the mathematics and it's lengthy; it's from 2011, 2 years after BitCoin began. Skip ahead to the 42 minute mark:
https://www.youtube.com/watch?v=XQPSwA2Itbs

Countries where cryptocurrencies are illegal:
https://www.investopedia.com/articles/forex/041515/countries-where-bitcoin-legal-illegal.asp

That Text is NOT from your Bank

I received this fake message last week. It's a smish, a phishing attempt that arrives as a text message. First warning sign: none of my banks have my cell number, and I don't do business with this particular bank. But the bank they're warning about is local, so I'll show you what's happening:



The link is to Bit.ly, the link shortener, and it redirects to what was, on the day it arrived, a fake login for M&T Bank. The page looked like this:

It's fake; look at the web address on the top line. Maritime Funtime's web site was hacked, and showing a copy of the M&T Bank login. (It's fixed, since then, just in case you wanted to visit them; they're in eastern Canada.)

Looks like the usual attack: There's an urgent message to log in, a shortened link to some other domain, a web site that looks good, but has the wrong domain name. It's harvesting login credentials, which will be followed up soon after with account emptying. I'll also guess that it was sent to every phone number with a Maryland area code that was known to the criminals behind it.

False Urgency Syndrome

This is a standard pattern of an email phish, a phone hoax, or a bad text message. There's the message that requires immediate action because it's scary or an alleged authority or known name has said something that you must act on. (Fake) Then there's a link that's either misleading or disguised (Fake), and finally a login page that will 'fail' when you log in, because the whole point was to collect your login for something, maybe a bank, your email account, or even an online shopping account like Amazon.

What to do?

Well, delete it. If you have already clicked into something like this and given away your account name and password, contact your real bank, and reset your password, and add a fraud alert to your account there. Stop using that password, everywhere, forever. It's known to be matched with your email account, and it will be tested at the top 40 banks and the top online vendors for gift cards. Reminder: Never use the same password online at more than one site.

When in doubt, ignore the link, and go directly to the source. M & T bank is at mtb.com. Amazon is at Amazon.com. You should have a bookmark or list of the companies you do business width. So type the address in the address bar of the browser, all the way at the top of the browser, and press Enter. From there, check your account for alerts. Ignore all forms of contact shown in the 'urgent' message, and log in just as you would normally.

As for next time: Slow down, be suspicious, and don't follow links from text messages or from emails.

For computer help, call 410-871-2877
Missed a newsletter? Back Issues

Mailing address:
Science Translations
PO Box 1735
Westminster, MD 21158-5735