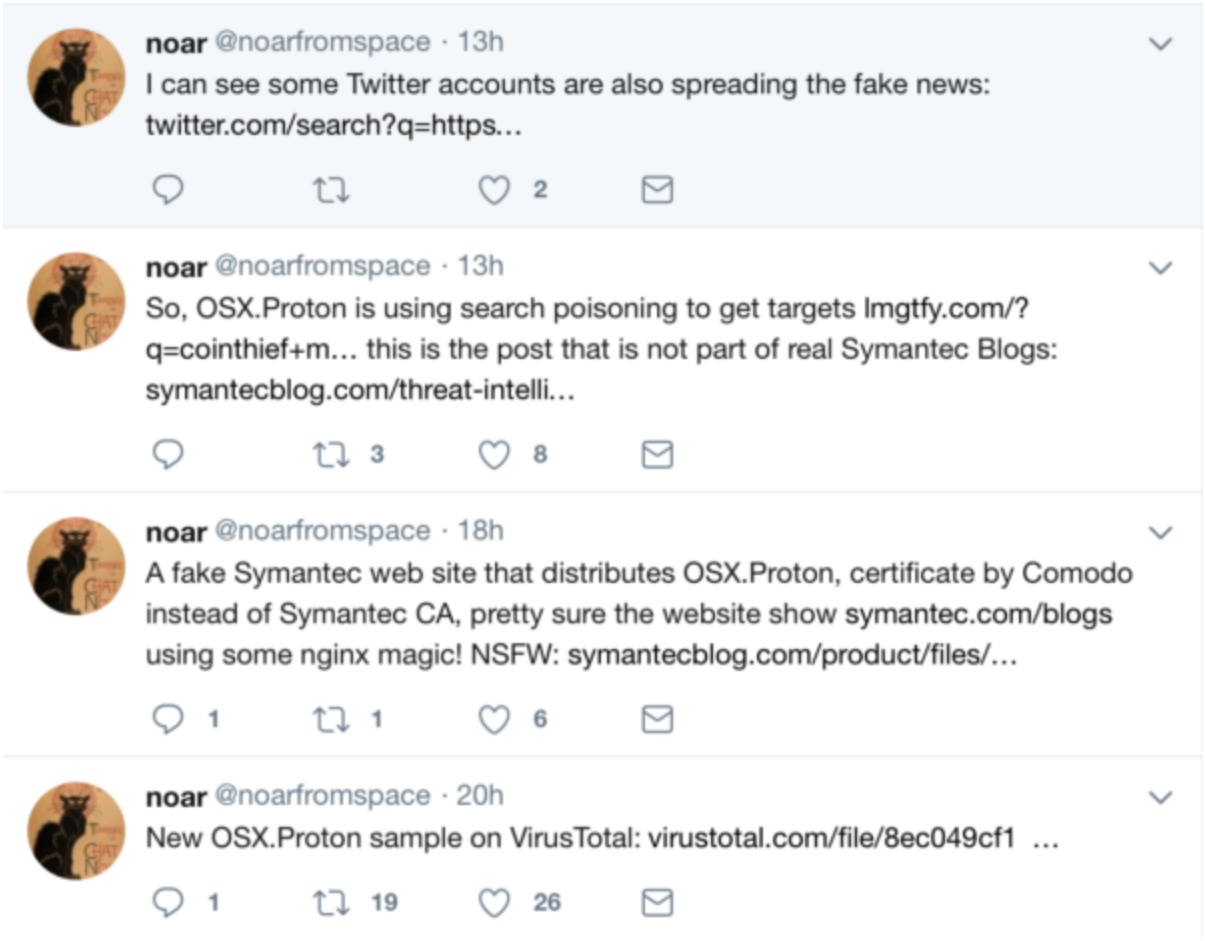
OSX.Proton spreading through fake Symantec blog

blog.malwarebytes.com/threat-analysis/mac-threat-analysis/2017/11/osx-proton-spreading-through-fake-symantec-blog/

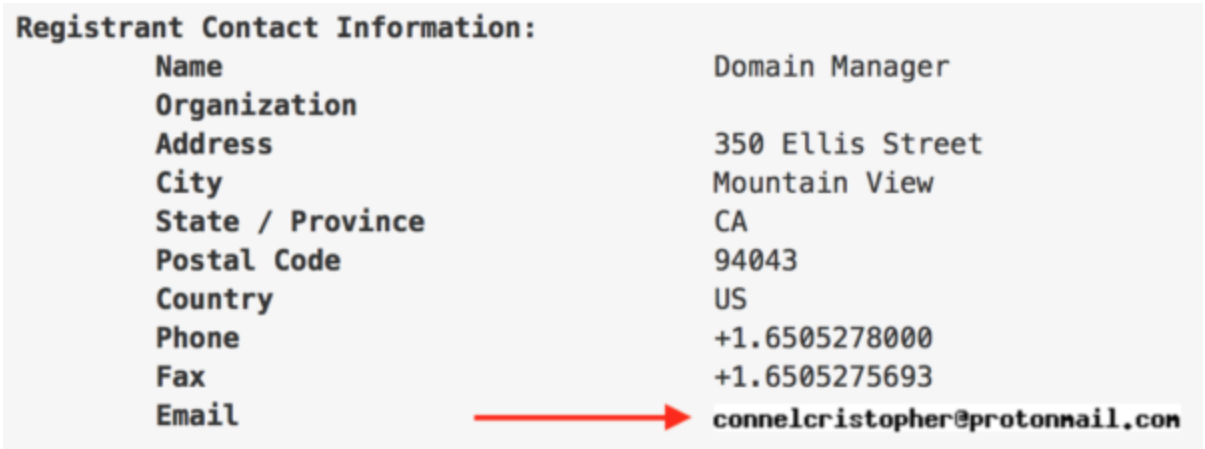
Thomas Reed November 20, 2017

Sunday night, a series of tweets from security researcher @noarfromspace revealed a new variant of the OSX.Proton malware, spreading in a concerning new method—spoofing security company Symantec's blog.

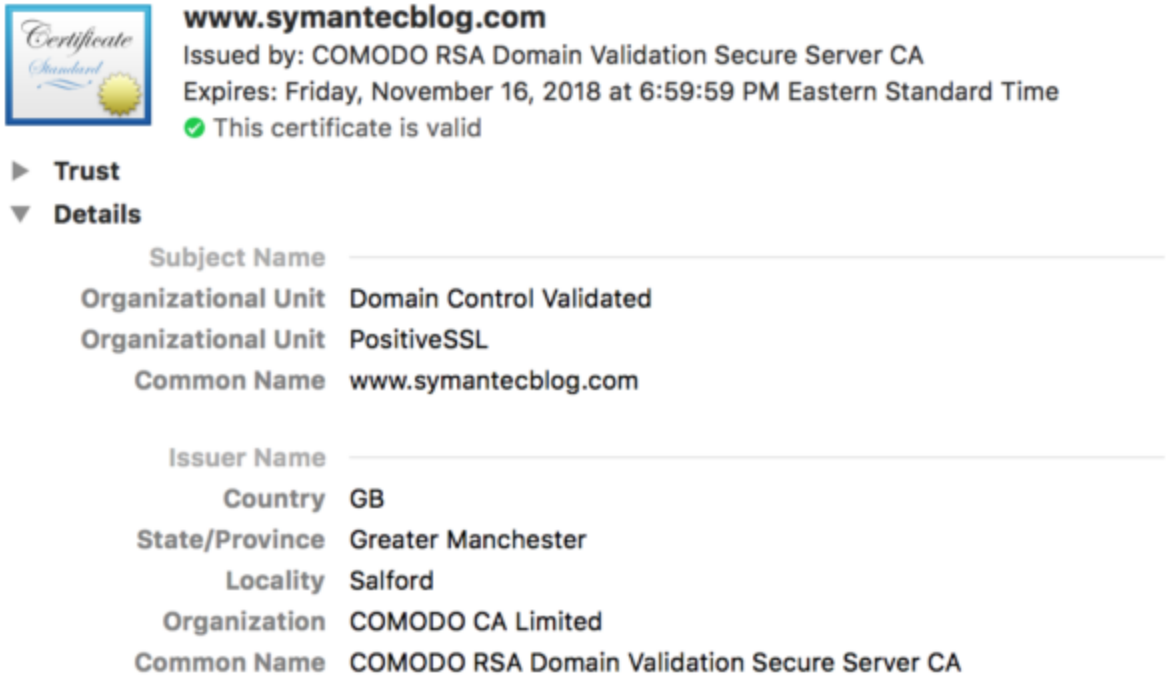


Method of infection

The malware is being promoted via a fake Symantec blog site at symantecblog[dot]com. The site is a good imitation of the real Symantec blog, even mirroring the same content. The registration information for the domain appears, on first glance, to be legitimate, using the same name and address as the legitimate Symantec site. The email address used to register the domain is a dead giveaway, however:



Even more suspicious is the certificate used by the site. It is legitimate SSL certificate, but was issued by Comodo rather than Symantec's own certificate authority.



The fake site contains a blog post about a supposed new version of CoinThief, a piece of malware from 2014. The fake post claims that a new variant of CoinThief has been spotted. In fact, as far as I've been able to determine, this is a made-up story, and no such new variant of CoinThief actually exists.

The fake post promotes a program called "Symantec Malware Detector," supposedly to detect and remove the malware. No such program actually exists.

Unfortunately, links to the fake post have been spreading on Twitter. Some of the accounts tweeting the link appear to be fake accounts, but others seem to be legitimate. Given the fact that the primary goal of the Proton malware is to steal passwords, these could be hacked accounts whose passwords were compromised in a previous Proton outbreak. However, they could also simply be the result of people being tricked into thinking the fake blog post is real.

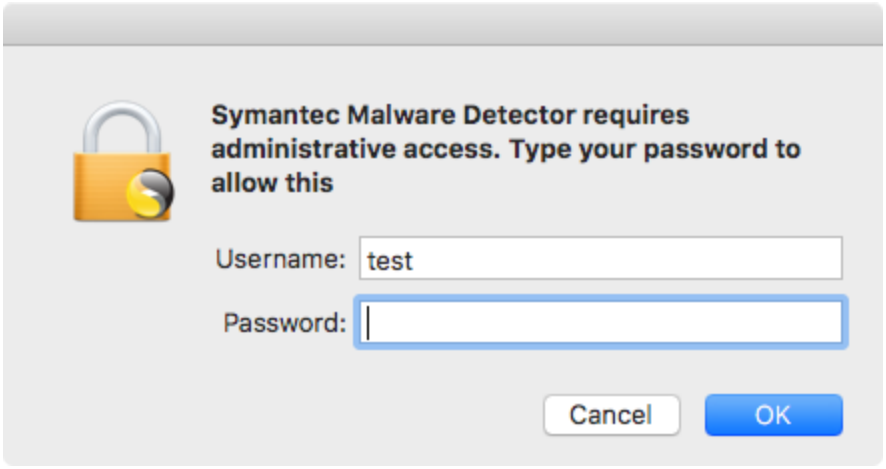
Users who download and run the "Symantec Malware Detector" will instead be infected with malware.

Malware behavior

When run, the malicious Symantec Malware Detector application displays a very simple window, using the Symantec logo:

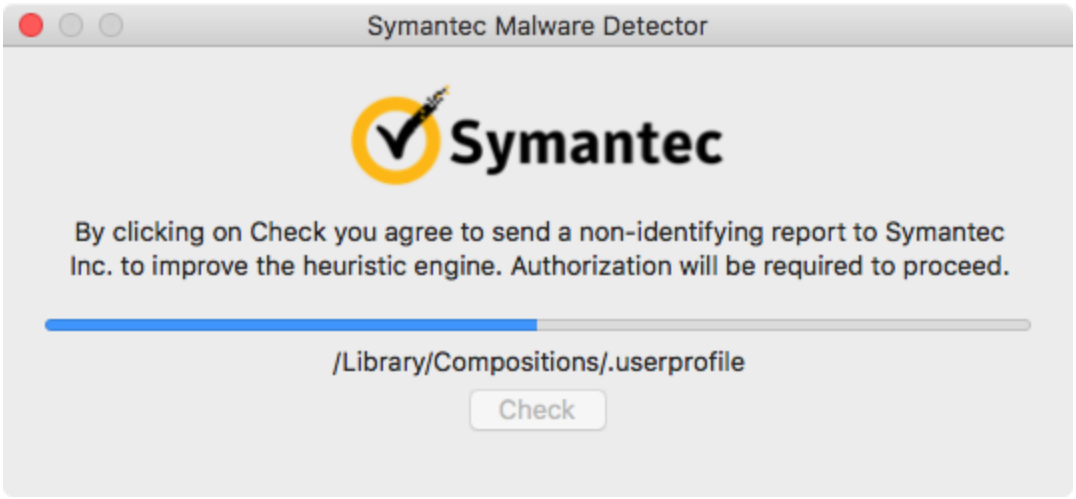
If the user quits the application at this point, the malware does not actually get installed. However, let's be honest—if you've been tricked into downloading and opening this application, you probably won't bail out at this point.

Clicking the "Check" button results in a request for an admin password:



The average Mac user has seen these kinds of password request many times before, so again, this is unlikely to raise suspicions among users who have gotten this far. In reality, this is a very well-done fake and will give the malware your password. (Unlike the legitimate password request this is designed to imitate, which does not give the requesting software the user's password.)

If an admin password is provided, the application displays a progress bar claiming to be scanning the computer.



In reality, however, the application has installed the Proton malware.

The malware will begin capturing information, including logging the user's admin password in clear text, among a lot of other personally-identifying information (PII) to a hidden file:

```
[...]
<metadata>
 <date>2017-11-19T20:29:19.801Z</date>
 <serial>*********</serial>
 <username>test</username>
 <fullname>test</fullname>
 <hostname>test%E2%80%99s Mac</hostname>
 <password>testpw</password>
 <os_version>10.12.6</os_version>
 <os_locale>en_US</os_locale>
</metadata>
[...]
```

The malware also captures and exfiltrates things like keychain files, browser auto-fill data, 1Password vaults, and GPG passwords. Since the malware has phished the user's password, the hackers will be able to decrypt the keychain files at a minimum.

Indicators of compromise

The Symantec Malware Detector application is, as far as I'm able to determine, a completely made-up name. If you see such an application—perhaps in the Downloads folder, or perhaps in the Applications folder, depending on where the user puts it—it should be deleted.

Symantec Malware Detector

If you are unsure of whether the application is actually malicious, you can check the code signature. Enter the following command in the Terminal, substituting the actual path:

```
codesign -dvvv "path/to/Symantec Malware Detector.app"
```

The malicious application has been signed by someone named Sverre Huseby, using a certificate with a team identifier of E224M7K47W. Anything signed with this certificate should be considered malicious.

Once this malicious “dropper” application has been run, the following paths will be found on the system:

```
/Library/LaunchAgents/com.apple.xpcd.plist
/Library/.cachedir/
/Library/.random/
```

The .random directory holds the malicious Proton executable, which is kept running by the com.apple.xpcd.plist launch agent. The .cachedir folder contains data that has been or will be exfiltrated.

In addition to these files, the /private/etc/sudoers file will have been modified. The following line will have been added to the end:

```
Defaults !tty_tickets
```

That line should be removed from the sudoers file.

Fortunately, Apple is aware of this malware and has revoked the certificate used to sign the malware. This will prevent future infections by the Symantec Malware Detector. Revoking the certificate will not, by itself, do anything to protect a machine that is already infected.

Implications

Malwarebytes for Mac will detect and remove Proton infections for free. If you find your Mac to be infected, it's quite easy to remove the malware. However, removing the malware is only a part of the solution.

Since Proton is designed to steal login credentials, you will need to take some emergency actions post-infection. You should treat all online passwords as compromised and change them all. Be sure, while you're at it, to use different passwords on every site, and use a password manager (such as 1Password or LastPass) to keep track of them. Since 1Password vaults are a target of Proton, be sure that you don't store your password manager's master password in your keychain or anywhere else on the computer. That should be the one and only password that you memorize, and it should be strong.

You should also enable two-factor authentication on every account that will allow you to do so. That will minimize the impact of such breaches in the future by ensuring that a hacker will need more than just your password to access your accounts.

In addition to passwords, you should consider any other information that may have been part of the compromise. For example, if you store credit card numbers or other sensitive data in the keychain, it should be treated as compromised and you should respond accordingly.

As always, if the machine that was compromised was issued to you by your employer, or has company data on it, you should notify IT immediately. Failure to do so could lead to a very serious breach of your company's systems.

Conclusion

Proton has been circulating for quite some time after its initial appearance in March. It has previously been distributed via a compromise of the Handbrake application and a similar compromise of a couple Eltima Software applications. It is highly likely that Proton will continue to circulate, and similar incidents will continue to occur.

Proton illustrates an increasing problem in the Mac community. The prevailing attitude that you can avoid Mac malware if you're careful enough is failing in the face of supply chain attacks, such as the hacks of the Handbrake and Eltima Software systems.

Further, so-called "fake news" being used to distribute malware is a highly dangerous threat. Many people these days are looking to download malware removal software for the Mac, due to the increasing prevalence of annoying Mac adware. Unfortunately, it is often the case that such software will be downloaded after a search that gives questionable results, or after seeing a recommendation from a hacked or fake account on social media or forums.

Macs are the targets of an increasing amount of malware. They can no longer be assumed to be safe. The old advice that “Macs don’t get viruses,” which can still be found echoing in many Mac-centric forums, has never been true, and this is becoming increasingly obvious to those following such events. Do not fall victim due to a false sense of security caused by the fact that you have a Mac!