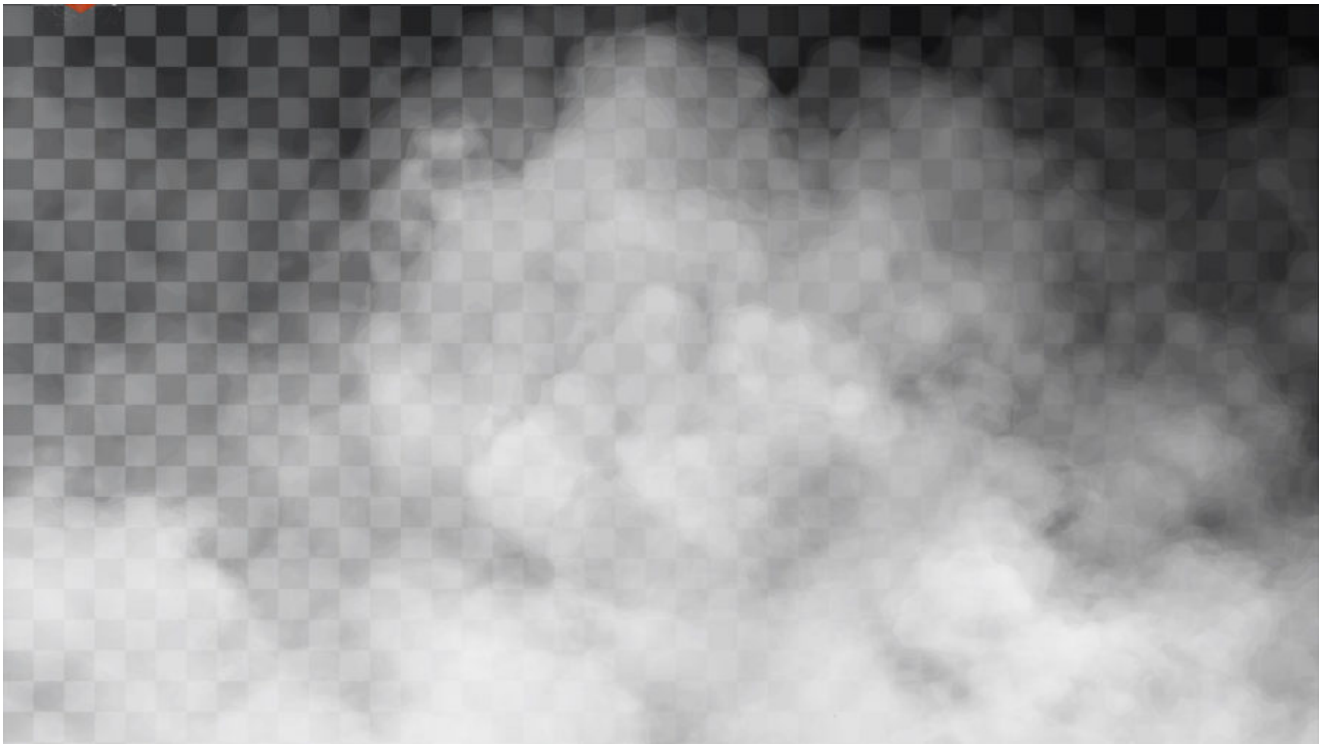
Fake Spectre and Meltdown patch pushes Smoke Loader malware

blog.malwarebytes.com/cybercrime/2018/01/fake-spectre-and-meltdown-patch-pushes-smoke-loader/

Jérôme Segura January 12, 2018

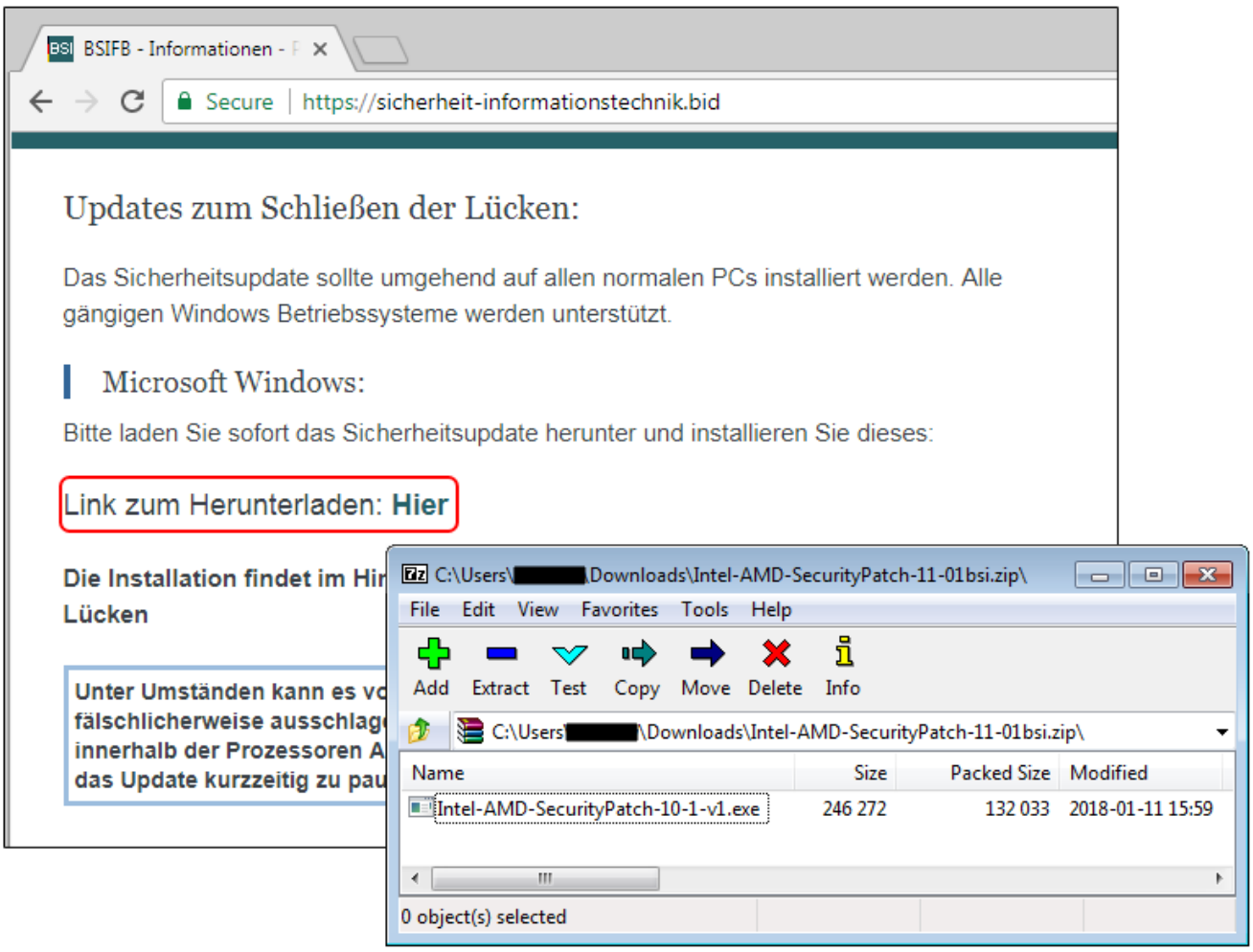


The Meltdown and Spectre bugs have generated a lot of media attention, and users have been urged to update their machines with fixes made available by various vendors.

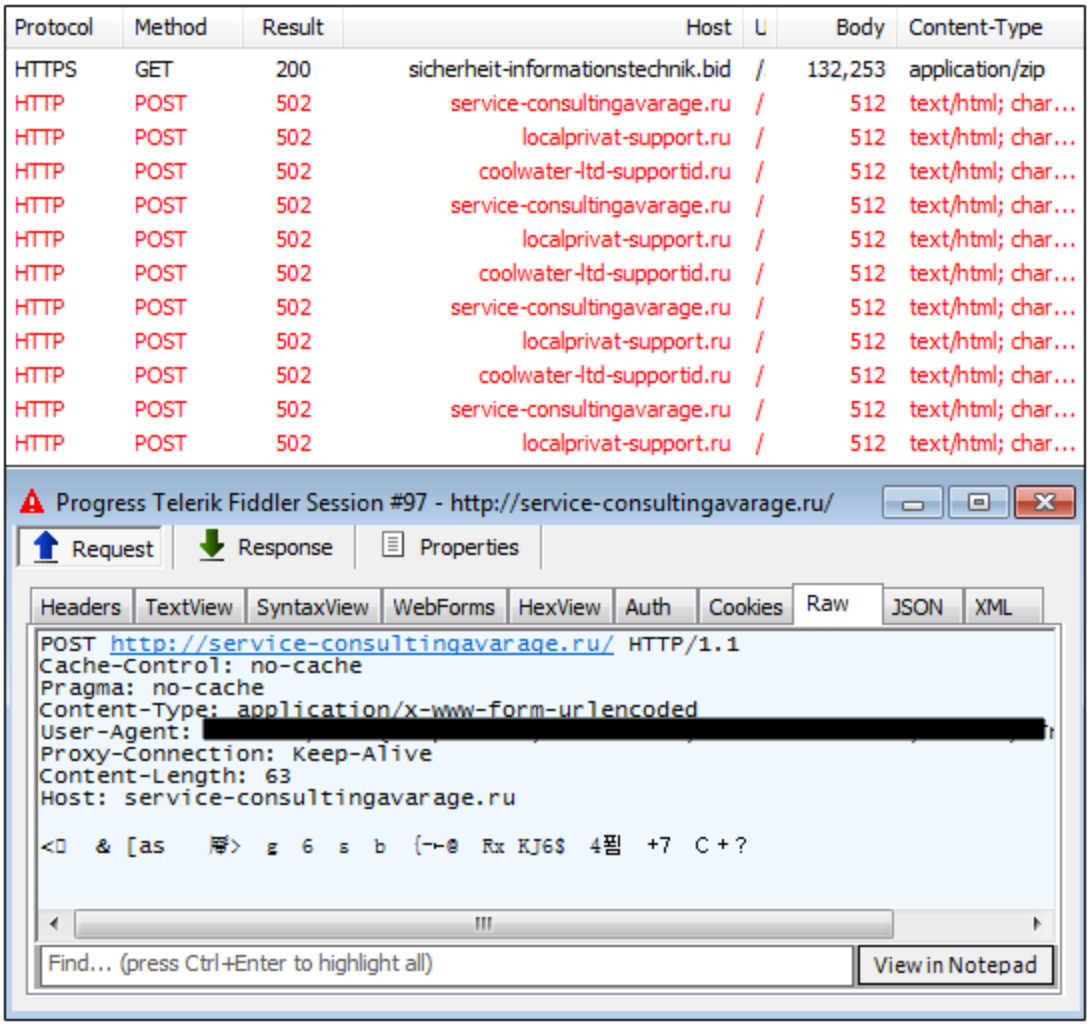
While some patches have created more issues than they fixed, we came across a particular one targeted at German users that actually is malware. In fact, German authorities recently warned about phishing emails trying to take advantage of those infamous bugs.

We identified a recently registered domain that is offering an information page with various links to external resources about Meltdown and Spectre and how it affects processors. While it appears to come from the German Federal Office for Information Security (BSI), this SSL-enabled phishing site is not affiliated with any legitimate or official government entity.

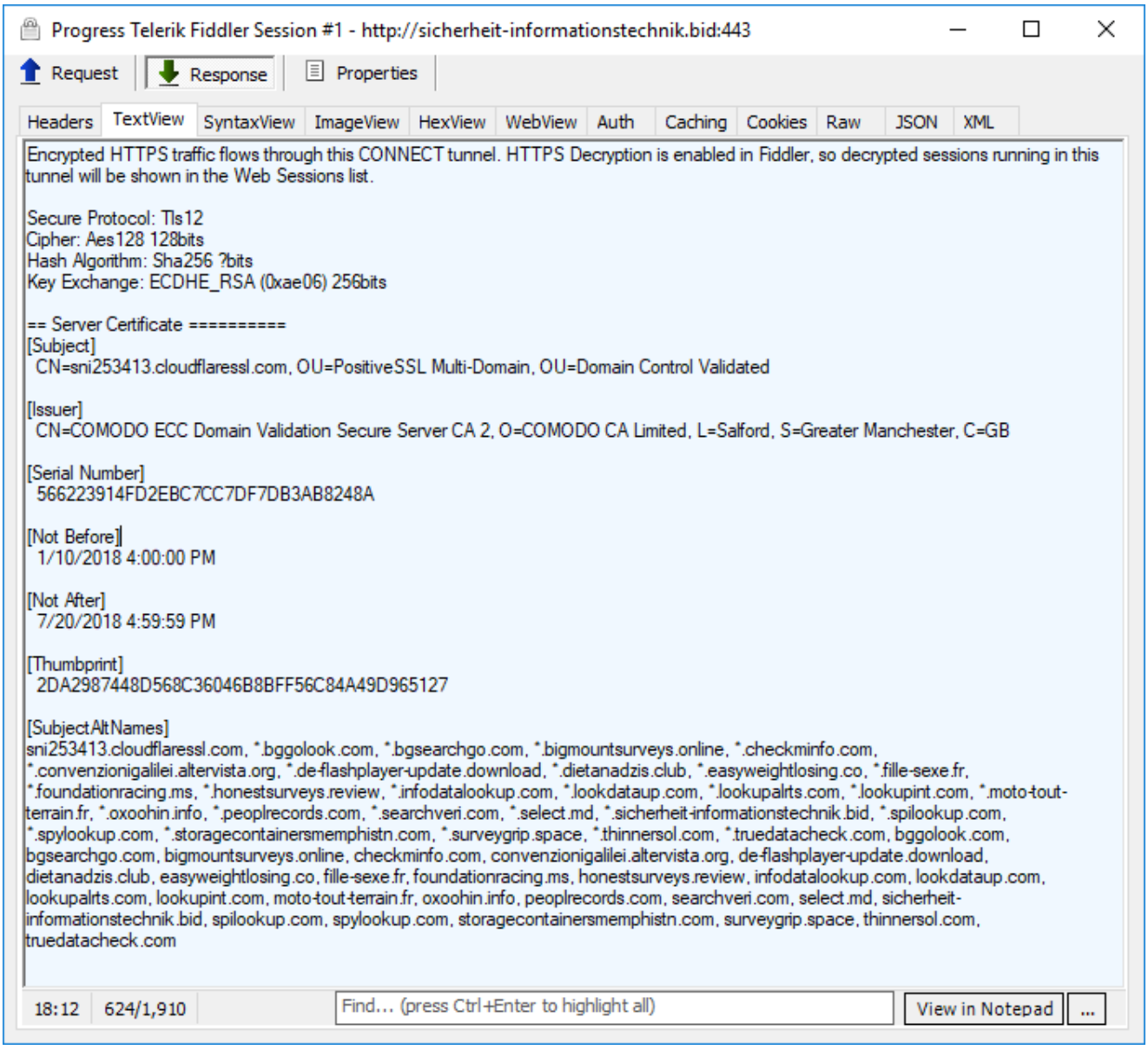
Moreover, the same fraudulent domain has a link to a ZIP archive (*Intel-AMD-SecurityPatch-11-01bsi.zip*) containing the so-called patch (Intel-AMD-SecurityPatch-10-1-v1.exe), which really is a piece of malware.



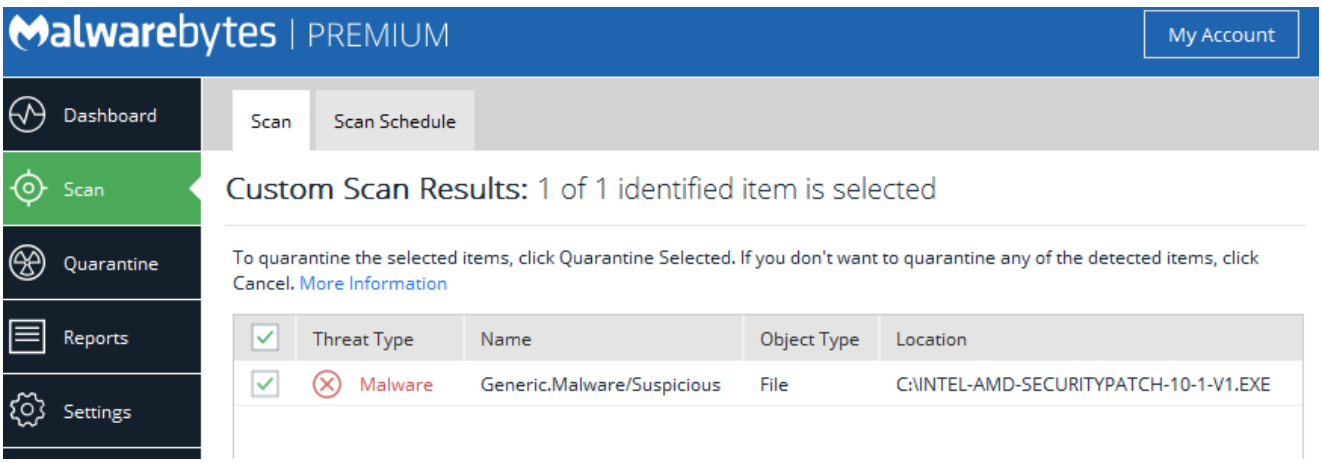
Upon running it, users will infect themselves with Smoke Loader, a piece of malware that can retrieve additional payloads. Post-infection traffic shows the malicious file attempting to connect to various domains and sending encrypted information:



The Subject Alternative Name field within the abused SSL certificate shows other properties associated with the .bid domain, including one that is a German template for a fake Adobe Flash Player update.



We immediately contacted Comodo and CloudFlare to report on this abuse and within minutes the site did not resolve anymore thanks to CloudFlare's quick response. Malwarebytes users were already protected at zero-hour against this malware.



Online criminals are notorious for taking advantage of publicized events and rapidly exploiting them, typically via phishing campaigns. This particular one is interesting because people were told to apply a patch, which is exactly what the crooks are offering under disguise.

It's always important to be cautious, especially when urged to perform an action (i.e. calling Microsoft on a toll-free number, or updating a piece of software) because there's a chance that such requests are fake and intended to either scam you or infect your computer. There are very few legitimate cases when vendors will directly contact you to apply updates. If that is the case, it's always good to verify this information via other online resources or friends first.

Also, remember that sites using HTTPS aren't necessarily trustworthy. The presence of a certificate simply implies that the data that transits between your computer and the site is secure, but that has nothing to do with the intentions or content offered, which could be a total scam.

Indicators of compromise

Fraudulent site:

```
sicherheit-informationstechnik[.]bid
```

Fake patch (Smoke Loader):

```
sicherheit-informationstechnik.bid/Download/Sicherheitsupdate/Intel-AMD-
SecurityPatch-11-01bsi.zip
CD17CE11DF9DE507AF025EF46398CFDCB99D3904B2B5718BFF2DC0B01AEAE38C
```

Smoke Loader callbacks:

```
coolwater-ltd-supportid[.]ru
localprivat-support[.]ru
service-consultingavarage[.]ru
```