FinFisher: Internetprovider schieben Spitzelopfern Malware unter

Originalartikel

Backup

<html> <div class=„meldung_wrapper druckversion“>

```
          <!-- RSPEAK_STOP -->
  <!-- RSPEAK_STOP -->
  <figure class="aufmacherbild"><img
src="https://1.f.ix.de/scale/geometry/600/q75/imgs/18/2/2/8/2/8/5/9/binocula
rs-354623_1280-1c4a7748b30180a9.jpeg"/><figcaption><p
class="source">(Bild: pixabay.com)</p>
          </figcaption></figure><!-- RSPEAK_START --><!-- RSPEAK_START --><p
class="meldung_anrisstext"><strong>Eine neue Variante der  Spionage-Malware
FinFisher nutzt einen aufsehenerregenden Infektionsweg: Lokale
Internetprovider schleusen als Man-in-the-Middle vergiftete Versionen
vertrauensw&#252;rdiger Software wie TrueCrypt oder VLC Player auf die
PCs.</strong></p>
          <p>Antivirenforscher von ESET haben eine neue Variante der
&#220;berwachungssoftware FinFisher <b>entdeckt [1]</b>, die in mindestens
sieben Staaten zum Einsatz kam. Neben klassischen Infektionswegen konnten
sie in zwei Staaten beobachten, wie die Malware auf einem eher
ungew&#246;hnlichen Weg &#8211; n&#228;mlich unter Mitwirkung von
Internetprovidern &#8211; auf Rechner geschleust wurde. Um ausgew&#228;hlten
Opfern den Spionage-Trojaner unterzujubeln, leiteten sie beabsichtigte
Downloads legitimer Software um.<br/></p>
```

Immer dann, wenn ein Opfer eine gängige Software wie Putty, Skype, TrueCrypt, VLC Player, WhatsApp oder WinRAR herunterladen wollte, schickten die Provider dessen Browser per Umleitung (HTTP 307 Temporary Redirect) zu einem von den Angreifern kontrollierten Downloadserver. Die dort heruntergeladene Software war voll funktionsfähig, installierte aber in einigen Fällen den huckepack eingeschleusten Trojaner mit. Die Entscheidung über die Malware-Installation auf dem jeweiligen Zielrechner wurde serverseitig – also erst nach dem Redirect – getroffen. Nach welchen Kriterien dies geschah, ist bislang unklar. Laut ESET sind für die beschriebene Strategie weder ein Zero-Day-Exploit, wie er kürzlich im Zusammenhang mit FinFisher [2] beobachtet wurde, noch Administratorenrechte nötig. Wurde der Weg über den Provider tatsächlich gewählt, dann dürfte es der erste bekannt gewordene Einsatz einer auf WikiLeaks dokumentierten, FinFlyISP [3] genannten Deployment-Lösung sein, die exakt den beschriebenen Infektionsweg beherrschen soll.
 Motive unklar, Redirects noch immer aktiv Den Antivirenexperten von ESET zufolge wurde die betreffende FinFisher-Variante bislang schätzungsweise über 100 Mal in mindestens sieben Ländern installiert. Die Angriffe seien nicht großflächig, sondern sehr gezielt erfolgt. Auf Nachfrage von heise Security erklärte Candid Wüest, Principal Security Engineer bei Symantec, dass die entsprechenden exe-Files unter anderem in den USA, Frankreich, Deutschland, Japan gesichtet wurden, aber auch in Staaten mit Demokratiedefiziten wie der Türkei und

Ägypten. Auch Marco Preuss, Director des europäischen Global Research & Analysis Teams von Kaspersky, bestätigte Dateifunde auf Rechnern in der Türkei. Laut ESET sind die bereits im April 2016 von den Providern eingerichteten Umleitungen nach wie vor aktiv. Alle Opfer nutzten unverändert denselben, innerhalb eines Landes jeweils identischen Provider. Auf Nachfrage erklärte ESET, dass man aus Gründen des Datenschutzes und der Sicherheit nicht in der Lage sei, mit ihnen in Kontakt zu treten, um sie vor der womöglich noch immer bestehenden Gefahr zu warnen. Ungeklärt bleibt die Frage nach Tätern und Motiven. Hoher Aufwand, um unter dem Radar zu fliegen
 Gut einen Monat Arbeitszeit investierte der damit betraute ESET-Mitarbeiter in die Analyse der neuen FinFisher-Variante. Sie bringe diverse neue Methoden mit, um sich ihrer Entdeckung und anschließenden Untersuchung zu entziehen, darunter Techniken gegen Analysen in einer Sandbox, gegen das Debugging, gegen virtuelle Umgebungen und gegen Emulation. Der komplette Code des Schädlings sei gespickt mit Tricks gegen das Disassemblieren. Außerdem setzen die Programmierer auf eine bislang nicht gesehene, wahrscheinlich selbst entwickelte Methode zur Code-Virtualisierung zum Schutz ihrer Komponenten.<!– AUTHOR-DATA-MARKER-BEGIN –>

<!– RSPEAK_STOP –> (ovw [4]) <br class=„clear“/><!– RSPEAK_START –><!– AUTHOR-DATA-MARKER-END –>

```
      </div><hr/><p class="size80">
          <strong>URL dieses Artikels:</strong><br/>
https://www.heise.de/security/meldung/FinFisher-Internetprovider-schieben-Sp
itzelopfern-Malware-unter-3837645.html
      </p>
          <p class="size80">
              <strong>Links in diesem Artikel:</strong><br/>
&amp;#160;&amp;#160;[1]&amp;#160;https://www.welivesecurity.com/2017/09/21/new-finfisher
-surveillance-campaigns/<br/>
&amp;#160;&amp;#160;[2]&amp;#160;https://www.heise.de/security/meldung/Microsoft-Patchda
y-schliesst-FinFisher-Zero-Day-und-grosse-Bluetooth-Luecke-3829849.html<br/>
&amp;#160;&amp;#160;[3]&amp;#160;https://wikileaks.org/spyfiles4/documents/FinFly-ISP-Ca
talog.pdf<br/>
                  &amp;#160;&amp;#160;[4]&amp;#160;mailto:ovw@heise.de<br/></p>
```

</html>