INFO SECURITY FIRMS AND THEIR ANTIVIRUS SOFTWARE MONITORED (HACKED?) BY NSA, GCHQ

[NSA slide indicated info sec AV firms targeted for surveillance]

Let's call this post a work in progress. I'm still reading through a pile of reporting from different outlets to see if it's all the same information but rebranded, or if there's a particular insight one outlet picked up, missed by the rest. Here are a few I've been working on today:

> 7:03 am — Popular Security Software Came Under Relentless NSA and GCHQ Attacks (The Intercept)
>
> 7:12 am — US and British Spies Targeted Antivirus Companies (WIRED)
>
> 9:48 am — Spies are cracking into antivirus software, Snowden files reveal (The Hill)
>
> 12:18 pm — GCHQ has legal immunity to reverse-engineer Kaspersky antivirus,

crypto (Ars Technica-UK)

12:57 pm* — US, UK Intel agencies worked to
subvert antivirus tools to aid hacking
[Updated] (Ars Technica)(*unclear if this is
original post time or time update posted))

~3:00 pm — NSA Has Reverse-Engineered
Popular Consumer Anti-Virus Software In
Order To Track Users (TechCrunch)
(post time is approximate as site only
indicates rounded time since posting)

The question I don't think anyone can answer yet
is whether the hack of Kaspersky Lab using Duqu
2.0 was part of the effort by NSA or GCHQ,
versus another nation-state. I would not be
surprised if the cover over this operation was
as thin as letting the blame fall on another
entity. We've seen this tissue paper-thin cover
before with Stuxnet.

For the general public, it's important to note
two things:

— Which firms were not targeted (that we know
of);

— Understand the use of viruses and other
malware that already threaten and damage
civilian computing systems only creates a bigger
future threat to civilian systems.

Once a repurposed and re-engineered exploit has
been discovered, the changes to it are quickly
shared, whether to those with good intentions or
criminal intent. Simply put, criminals are
benefiting from our tax dollars used to help
develop their future attacks against us.

There's a gross insufficiency of words to
describe the level of shallow thinking and
foresight employed in protecting our interests.

And unfortunately, the private sector cannot
move fast enough to get out in front of this
massive snowball of shite rolling towards it and
us.

EDIT — 5:55 pm EDT —

And yes, I heard about the Polish airline LOT getting hit with a DDoS, grounding their flights. If as the airline's spokesman is correct and LOT has recent, state-of-the-art systems, this is only the first such attack.

But if I were to hear about electrical problems on airlines over the next 24-48 hours, I wouldn't automatically attribute it to hacking. We're experiencing effects of a large solar storm which may have caused/will cause problems over the last few hours for GPS, communications, electricals systems, especially in North America.

EDIT — 1:15 am EDT 23JUN2015 —

At 2:48 pm local time Christchurch, New Zealand's radar system experienced a "fault" — whatever that means. The entire radar system for the country was down, grounding all commercial flights. The system was back up at 4:10 pm local time, but no explanation has yet been offered as to the cause of the outage. There were remarks in both social media and in news reports indicating this is not the first such outage; however, it's not clear when the last fault was, or what the cause may have been at that time.

It's worth pointing out the solar storm strengthened over the course of the last seven hours since the last edit to this post. Aurora had been seen before dawn in the southern hemisphere, and from northern Europe to the U.S. Tuesday evening into Wednesday morning. It's possible the storm affected the radar system — but other causes like malware, hacking, equipment and human failure are also possibilities.