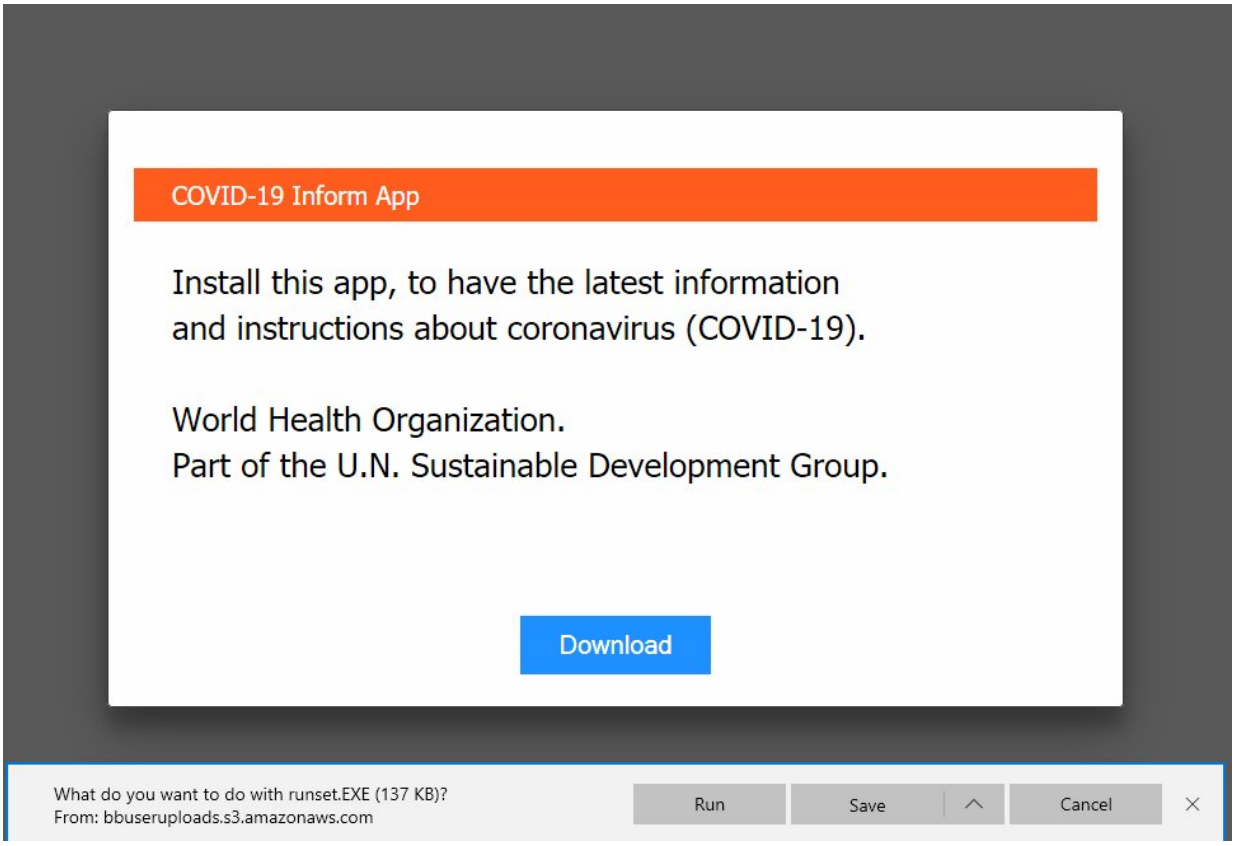
Router phishing scam targets global fear over coronavirus

March 27 2020, by Peter Grad



Credit: bitdefender

There is no tragedy serious enough that creeps somewhere around the world won't take advantage of. The cybersecurity organization Bitdefender reported this week that phishing scams preying on people's

fears about coronavirus have been detected among users of Linksys and D-Link routers.

Taking advantage of routers with weak passwords, hackers reroute critical DNS IP addresses so that users seeking information about epidemic-related web sites are quietly redirected to malicious ones. The hackers mask their ruse by displaying innocuous web address names and recreating the page design of legitimate sites. When users land on the fake pages, a pop-up window instructs them to click on a link for an app providing "the latest information and instructions about coronavirus (COVID-19)."

The site falsely claims the information is provided by the World Health Organization.

If clicked, a trojan program in installed on the user's computer that can steal sensitive information. The malware, the Oski data stealer, can capture user keystrokes, take screenshots and monitor web activity, including retrieving passwords, email contents and financial transactions. It can also commandeer attached microphones and webcams.

Users without strong security measures and system passwords leave themselves highly vulnerable to such criminal activity. According to Bitdefender, DNS settings "work like a phone book… In a nutshell, DNS works pretty much like your smartphone. …Whenever you want to call someone you just look up their name instead of having to memorize their phone number."

"Once attackers change the DNS IP addresses," said Bitdefender in an advisory released Wednesday, "they can resolve any request and redirect users to webpages that attackers control, without anyone being the wiser."

Users are advised to turn off remote administration on their routers and update their systems with strong passwords. Cloud accounts should also be secured. In addition, carefully inspect email and web addresses for slight spelling variances from legitimate sites, don't click on links from unknown recipients and check www.charitynavigator.org to confirm the legitimacy of charity organizations. Also update anti-virus and malware programs.

Bitdefender estimated 1,193 downloads of the spyware globally, mainly by users in France, Germany and the United States. The source of the assault is unknown but Oski malware is commonly found on dark web forums based in Russia.

Online criminal activity always spikes during tragedy. Hours after the 9/11 Trade Tower attacks, digital scam artists posing as Red Cross volunteers were soliciting funds for victims and their families. Phishing scams proliferated after fires in Australia, California, Spain and Portugal; hurricanes in Texas and Puerto Rico; and earthquakes in Japan, Haiti and Mexico.

The global extent of the coronavirus epidemic provides rich mining opportunities for thieves. As of noon Friday, 558,358 people were infected worldwide, and 25,262 have died.

Perhaps the best advice in today's world comes from Frank Abagnale, an American security consultant best known for his career as a con man and check forger during his teenage years—he was portrayed by Leonardo DiCaprio in the 2002 movie "Catch Me If You Can."

"People need to be more aware and educated about identity theft," Abagnale once said. "You need to be a little bit wiser, a little bit smarter and there's nothing wrong with being skeptical. We live in a time when if you make it easy for someone to steal from you, someone will."

More information: labs.bitdefender.com/2020/03/n … to-host-infostealer/