Future ICS Security News

News about control system security incidents that you might see in the not too distant future. Any similarity to real people, places or things is purely imaginary.

Sunday, September 12, 2021

VaxSurge Ransomware

The Federal Bureau of Inquiry announced this morning that it was investigating a new ransomware campaign targeted at local public health agencies. While the attack was encoding files at the affected agencies the attacker has not been demanding a monetary ransom. Instead, they are unlocking files once the agency has published a notice in the local newspaper that they were not supporting the President's new mandatory COVID-19 vaccination program.

"We have been notified by twenty local public health agencies about successful attacks since yesterday morning," Johnathan Quest, spokesperson for the FBI, told reporters this morning; "Since the attacks appear to have started on Saturday, we expect to receive more notifications on Monday when many of these organizations return to normal workhours."

The National Critical Infrastructure Security Operations Center (CI-SOC), working with the Delano, Georgia Health Department, has determined that the attackers have delivered the ransomware via a letter emailed to the Department. "The email was apparently sent by a compromised email server in the Department of Health and Medical Services. It purportedly came from the Office for COVID Vaccinations," General Turgidson explained at an unusual Sunday press conference at CI-SOC.

A spokesperson for the Department confirmed that there was no such office in DHMS.

A technician from the CI-SOC, speaking on background, told reporters that this was not a very sophisticated ransomware program. Instead of trying to penetrate the organization network before announcing its presence, the ransomware encrypted the machine at the point of infection before it started penetrating the network. Promptly unplugging the connections to the network effectively stopped the spread of the ransomware.

Turgidson reported that the infected email included a Microsoft Word document entitled "Mandatory COVID-19 Vaccination Surge". It contained an ActiveX-control that exploited the newly reported 0-day Microsoft® MSHTML Remote Code Execution Vulnerability. "The rapid exploitation of the Microsoft vulnerability and the use of the old-school ransomware program do not paint a consistent picture of this attacker," Turgidson explained; "That combined with an exploitation of a SolarWinds compromised mail system is causing us all sorts of investigative headaches."

CI-SOC is calling this the VaxSurge malware campaign because of that term is used in a comment line in the malware code sample that they are working on.

CAUTIONARY NOTE: This is a future news story –

PJCoyle at 1:04 PM

Share

No comments:

Post a Comment

Home ›

View web version

About Me

PJCoyle

Patrick Coyle is a freelance writer dealing with chemical security and safety issues. He has 15 years experience in the US Army with extensive experience in training development, delivery and evaluation. He spent 20 years working in the chemical process industry developing and improving chemical manufacturing processes with a large emphasis on chemical and process safety. He currently writes a daily blog, the Chemical Facility Security News, examining the issues associated with the Chemical Facility Anti-Terrorism Standards administered by the Department of Homeland Security.

View my complete profile