forbes.com

Healthcare Workers Targeted By Dangerous New Windows Ransomware Campaign Using Coronavirus As Bait

Davey Winder

3–4 minutes

Cybercriminals are targeting healthcare workers

with a new Windows ransomware campaign

Getty

Cybercriminals, who truly deserve the epithet of cyberscum, are attacking healthcare targets with a new and dangerous Windows ransomware campaign.

At the start of March, I warned how a new Windows ransomware threat was hiding in plain sight. That threat was NetWalker, and it's now being used by cybercrime groups, who truly deserve the epithet of cyberscum, as the payload of phishing attacks. Phishing attacks that are targeting those in the healthcare sector.

Cybercrime groups continue to exploit COVID-19 in search of profit

Some cybercrime groups have now promised not to target healthcare organizations during the ongoing coronavirus crisis. Those criminals, the operators of the prolific and devastating DoppelPaymer and Maze ransomware threats,

didn't say they would stop attacking everyone else, though. Cybercriminal groups are driven by greed and will use whatever methods they can to reach the destination of maximum profits. This has been very evident as the FBI confirmed when it warned of a significant spike in COVID-19 scams, with people living in areas of high coronavirus infection rates being targeted the most.

New NetWalker campaign uses coronavirus bait to lure healthcare workers

According to Bleeping Computer, this new NetWalker campaign was detected by MalwareHunterTeam. NetWalker is the latest variant of what used to be known as the Mailto ransomware threat. It has been seen in the wild attacking mainly government agencies and enterprise targets. However, according to Vitali Kremez, head of SentinelLabs and a specialist in investigating complex cyberattacks, not only does this new NetWalker campaign use Coronavirus

emails as the lure, but it has been seen actively attacking targets in the healthcare sector. This should come as no great surprise, as NetWalker already hit the Champaign Urbana Public Health District (CHUPD) in Illinois earlier this month.

What is NetWalker?

NetWalker itself is a threat that can hide in plain sight, injecting malicious code into Windows Explorer using a technique known as process hollowing. Long story short, it's all about evading detection and whitelisting or signature-based detection in particular. Security solutions using behavioral detection methodologies, such as Windows Defender, should be useful in protecting your systems against such attacks. However, should your files get encrypted, there is, for now, no known free decryptor tool, so a solid backup strategy is the order of the day here. That, and ensuring that everyone is aware of the increased phishing risk at the moment, especially with more people working from home.

Keep on top of the COVID-19 cyber scams and stay safe out there

Forbes has compiled a running list of coronavirus-themed online threats which I'd recommend regularly checking to keep abreast of the latest COVID-19 scam activity.

Follow me on Twitter or LinkedIn. Check out my website or some of my other work here.