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

[**Davey Winder**](https://www.forbes.com/sites/daveywinder/)

Senior Contributor

*Veteran cybersecurity and tech analyst, journalist, hacker, author*

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](https://www.forbes.com/sites/daveywinder/2020/03/05/beware-of-this-new-windows-10-ransomware-threat-hiding-in-plain-sight/) 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](https://www.forbes.com/sites/daveywinder/2020/03/19/coronavirus-pandemic-self-preservation-not-altruism-behind-no-more-healthcare-cyber-attacks-during-covid-19-crisis-promise/) 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](https://www.forbes.com/sites/daveywinder/2020/03/21/fbi-coronavirus-warning-significant-spike-in-covid-19-scams-targeting-these-three-states/), 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](https://www.bleepingcomputer.com/news/security/netwalker-ransomware-infecting-users-via-coronavirus-phishing/), this new NetWalker campaign was detected by [MalwareHunterTeam](https://twitter.com/malwrhunterteam" \o "https://twitter.com/malwrhunterteam" \t "_blank). 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](https://www.theregister.co.uk/2020/03/12/ransomware_illinois_health/" \o "https://www.theregister.co.uk/2020/03/12/ransomware_illinois_health/" \t "_blank) 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](https://blogs.quickheal.com/mailto-ransomware-hiding-under-explorer-exe/). 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](https://www.forbes.com/sites/daveywinder/2020/03/21/work-from-home-hackers-make-130000-in-48-hours-from-windows-10-exploits/).

Memo

To: All Staff

Subject: Urgent Cybersecurity Notice: Protecting Against NetWalker Ransomware Threat

Team,

I need to bring something serious to your attention. Our organization, along with many others in the healthcare sector, is currently under attack by cybercriminals using a new and dangerous Windows ransomware campaign. These attackers are exploiting the ongoing COVID-19 pandemic as a means to infiltrate our systems and hold our data hostage.

This situation is not just about technology; it's about the safety and security of our patients and our staff. The thought of cybercriminals infiltrating our systems and compromising patient data is deeply concerning and could have far-reaching consequences. We cannot afford to underestimate the gravity of this threat.

I understand that many of you are already under immense pressure due to the pandemic, and the last thing you need is to worry about cybersecurity. But the reality is, we must all be vigilant and proactive in protecting our organization against these threats.

Given our current remote working environment, it's crucial that we adapt our communication strategies to ensure that everyone receives this important message. We will leverage a combination of technology tools and modalities to disseminate information in a clear and concise way:

1. Email: We will send out regular email updates to all staff members, outlining the latest developments regarding the NetWalker ransomware threat and providing guidance on how to stay safe online.
2. Virtual Meetings: We will schedule virtual town hall meetings and departmental briefings to discuss cybersecurity best practices and address any concerns or questions that staff may have.
3. Intranet: We will update our intranet with dedicated cybersecurity resources, including FAQs, training materials, and contact information for reporting suspicious activity.
4. Instant Messaging: We will utilize instant messaging platforms to send out real-time alerts and reminders about cybersecurity risks and preventative measures.
5. Training Modules: We will develop interactive online training modules covering topics such as phishing awareness, password security, and safe browsing habits.

This is not just a technology issue; it's a cultural issue. We need to foster a culture of cybersecurity awareness and accountability across our organization. Each and every one of us plays a crucial role in protecting our systems and data.

I know that we are all facing unprecedented challenges right now, but I have full confidence in our ability to overcome this threat together. By working together and prioritizing cybersecurity, we can safeguard the integrity of our operations and protect the well-being of our patients.

Thank you for your attention to this matter.

Sincerely,

Leadership

[PSA]

Attention all healthcare workers, staff, and stakeholders of our hospital chain. Today, I bring to your attention a critical matter that affects us all: the recent cyberattack targeting healthcare organizations, including our own. As we navigate through these challenging times, it's essential that we address the incident with clarity and urgency.

First and foremost, let's acknowledge the social and emotional impact of this cyberattack. For healthcare workers already under immense pressure due to the pandemic, the threat of cybercrime adds an extra layer of stress and anxiety. We understand the gravity of this situation and want to assure you that your well-being is our top priority.

From a cultural standpoint, we must recognize the importance of fostering a cybersecurity-conscious environment. Each of us plays a crucial role in protecting our organization against threats like these. It's not just about technology; it's about instilling a mindset of vigilance and accountability across our entire workforce.

On the technical front, our IT team is working tirelessly to implement safeguards and raise awareness about cybersecurity best practices. We're leveraging advanced security solutions and conducting regular training sessions to ensure that every member of our team is equipped to recognize and respond to potential threats.

Looking ahead, we're committed to future-proofing our organization against similar attacks. This means investing in robust cybersecurity infrastructure, establishing comprehensive backup strategies, and staying informed about emerging threats and best practices.

Finally, in terms of policy moving forward, we're reviewing and updating our cybersecurity protocols to strengthen our defenses and prevent future attacks. We're implementing measures to secure remote work environments and ensuring that our staff is well-trained in cybersecurity awareness.

In closing, I want to emphasize that we're in this together. By working collaboratively and prioritizing cybersecurity, we can protect the integrity of our operations and safeguard the well-being of our patients. Thank you for your attention, and please remember to stay vigilant.

[End of PSA]