NetWalker Ransomware - What You Need to Know | Tripwire

By Graham Cluley

Published: 2020-05-28 · Archived: 2026-04-05 23:21:41 UTC

What is NetWalker?

NetWalker (also known as Mailto) is the name given to a sophisticated family of Windows ransomware that has targeted corporate computer networks, encrypting the files it finds, and demanding that a cryptocurrency payment is made for the safe recovery of the encrypted data.

Ransomware is nothing new. Why should I particularly care about NetWalker?

NetWalker, like the Maze ransomware and a small number of other ransomware families, aggressively threatens to publish victims' data on the internet if ransoms are not paid.

So it's not just a case of reaching for your backup?

Well, that's a good start. If your backup is up-to-date and it hasn't been compromised by the attack then at least you can get your data back, and have some chance of getting your systems operational again. Of course, you'll want to ensure that your systems are properly secured and that hackers haven't maintained access to your systems, as it's possible you will fall victim again. But there remains the problem of the exfiltrated data. If that's released by the NetWalker gang then there are clear dangers - not only to your business, but also to your partners and customers. Rebuilding trust and your corporate reputation is not likely to be easy or inexpensive. This is worse than a regular ransomware attack.

Nasty. How do they infect your computer system in the first place?

The NetWalker gang has not been shy of exploiting the COVID-19 pandemic to infect computer systems, exploiting interest in information amongst the general population as well as targeting individuals and entities working in the health industry. Poisoned emails sent by the group disguise themselves to appear related to the Coronavirus crisis, but when recipients click on the attached Word or Excel file their computers are compromised. In addition the ransomware has masqueraded as the legitimate password management app Sticky Password. If a user ran the bogus version of Sticky Password, their files would begin to be encrypted.

Is that all?

Unfortunately not. The NetWalker gang sees itself very much as "ransomware-as-a-service" (RaaS), providing the tools and infrastructure for others to launch ransomware attacks in return for affiliate payments.

Affiliates?

I'm afraid so. As Advanced Intelligence describes, the NetWalker gang is posting on dark market forums, inviting other criminals to become affiliates and help them spread the ransomware. Preference is being given those with proven experience in cybercrime and existing access to corporate networks.

Woah! They're recruiting people who have already hacked into company networks?

Yes. I guess the thinking is, "if you've managed to compromise a company network and can't work out how to make any money out of it - here's our ransomware, go have some fun..."

Surely the authorities are going to be hunting for these guys?

I'm sure some are keen to apprehend them. However, the NetWalker gang notably prohibits affiliates from infecting systems belonging to Russia and the CIS - presumably in an attempt to prevent local law enforcement from being encouraged to investigate the hackers' profitable activities.

Does that mean the hackers behind NetWalker are likely to be from that part of the world?

I suspect there's a high probability of that.

What organisations has NetWalker managed to infect?

Victims have included Australian transportation and logistics firm Toll Group, the Champaign Urbana Public Health District (CHUPD) in Illinois, the city of Weiz in Austria, and most recently Michigan State University.

Sounds like they've been busy. How can I protect my business?

You should continue to follow best practices - that means making secure offsite backups, running up-to-date security solutions, and ensuring that your computers are properly patched against the latest vulnerabilities. In addition, ensure that any passwords are being used are unique and hard-to-crack, and that multi-factor authentication is in place to make it harder for unauthorised users to gain access to critical systems. In addition, raise awareness amongst your staff about security threats and the different tricks used by cybercriminals to gain access to sensitive data. And if you do have sensitive data (trust me, you do) make sure that whenever possible it is strongly encrypted.

If our company is hit by NetWalker, should we pay the ransom?

As I said previously with the Maze ransomware, ultimately that's a decision that only your business can make. Paying money to ransomware extortionists makes the problem worse for everyone on the internet as it encourages them to launch more attacks. But then you may understandably feel that your company has no choice if it wants to survive. Whatever you decide, work with law enforcement agencies to inform them about what has happened, and help them to investigate who might be behind the attacks. Check out this webinar to learn more about how leveraging basic security controls will help protect and detect ransomware attacks before significant damage is done: https://www.youtube.com/watch?v=udwr3V0ojIA&feature=emb_title

---

Editor's Note: *The opinions expressed in this guest author article are solely those of the contributor, and do not necessarily reflect those of Tripwire, Inc.*
