Nuclear missile contractor hacked in Maze ransomware attack

nakedsecurity.sophos.com/2020/06/04/nuclear-missile-contractor-hacked-in-maze-ransomware-attack/

By Lisa Vaas 04 Jun 2020

The US is protected by what's known as a nuclear triad: a three-pronged attack force that consists of land-launched nuclear missiles, nuclear missiles on submarines, and aircraft equipped with nuclear bombs and missiles.

One of the triad's legs – the land-based LGM-30 Minuteman intercontinental ballistic missile (ICBM) – has been kicked by hackers who've inflicted Maze ransomware on the computer network of a Northrup Grumman contractor.

Sky News reported on Wednesday that the contractor, Westech International, has confirmed that it's been hacked and that its computers have been encrypted. It's not yet clear if the extortionists managed to steal classified military information. Investigations to identify exactly what they got away with are still ongoing.

However, the attackers have already leaked files that suggest they had access to sensitive data – including payroll and emails – that they copied before they encrypted it, Sky News reports. They're threatening to publish all of the files.

Unauthorized access to data about intercontinental ballistic nuclear missiles would be bad enough, but depending on what the attackers accessed, the attack could have yet more serious repercussions, given Westech's client list.

That list includes US military branches, government infrastructure agencies, and major military contractors, including the Army, the Air Force, the Navy, Joint Service Agencies, the Commerce Department, the Energy Department, the General Services Administration, Booz Allen Hamilton, General Dynamics Information Technology, Lockheed Martin Information Technology, and more.

Minuteman III missiles

Minuteman III missiles are stored in hundreds of protected underground launch facilities operated by the Air Force Global Strike Command. Westech reportedly provides Northrup Grumman with engineering and maintenance support for the missiles.

Each ICBM contains multiple thermonuclear warheads that can be delivered further than 6,000 miles: roughly, about one-fourth of the planet's circumference or, as Sky News notes, the distance between London and Buenos Aires. They can hit speeds of up to Mach 23: that's 17,508 miles/28,176 kilometers per hour.

The time frame of the attack, extortion demands and publishing of Westech's sensitive data haven't been disclosed. The firm told Sky News that it immediately initiated an investigation and contained its systems after learning about the hack. It's also working with an independent computer forensic firm to "analyze its systems for any compromise and to determine if any personal information is at risk."

Northrup Grumman and the Department of Defense (DoD) reportedly declined to comment.

About Maze

Maze ransomware is a new-ish ransomware strain that's also been used recently against Cognizant, a large US IT services company that disclosed that it had fallen victim in April.

Westech International is just the latest in a string of Maze attacks. As SophosLabs described last month in a report – titled **Maze ransomware: extorting victims for 1 year and counting –** Maze has been in the news quite frequently recently, notably because the gang who created it have been in the vanguard of a new wave of "double-whammy" ransomware attacks.

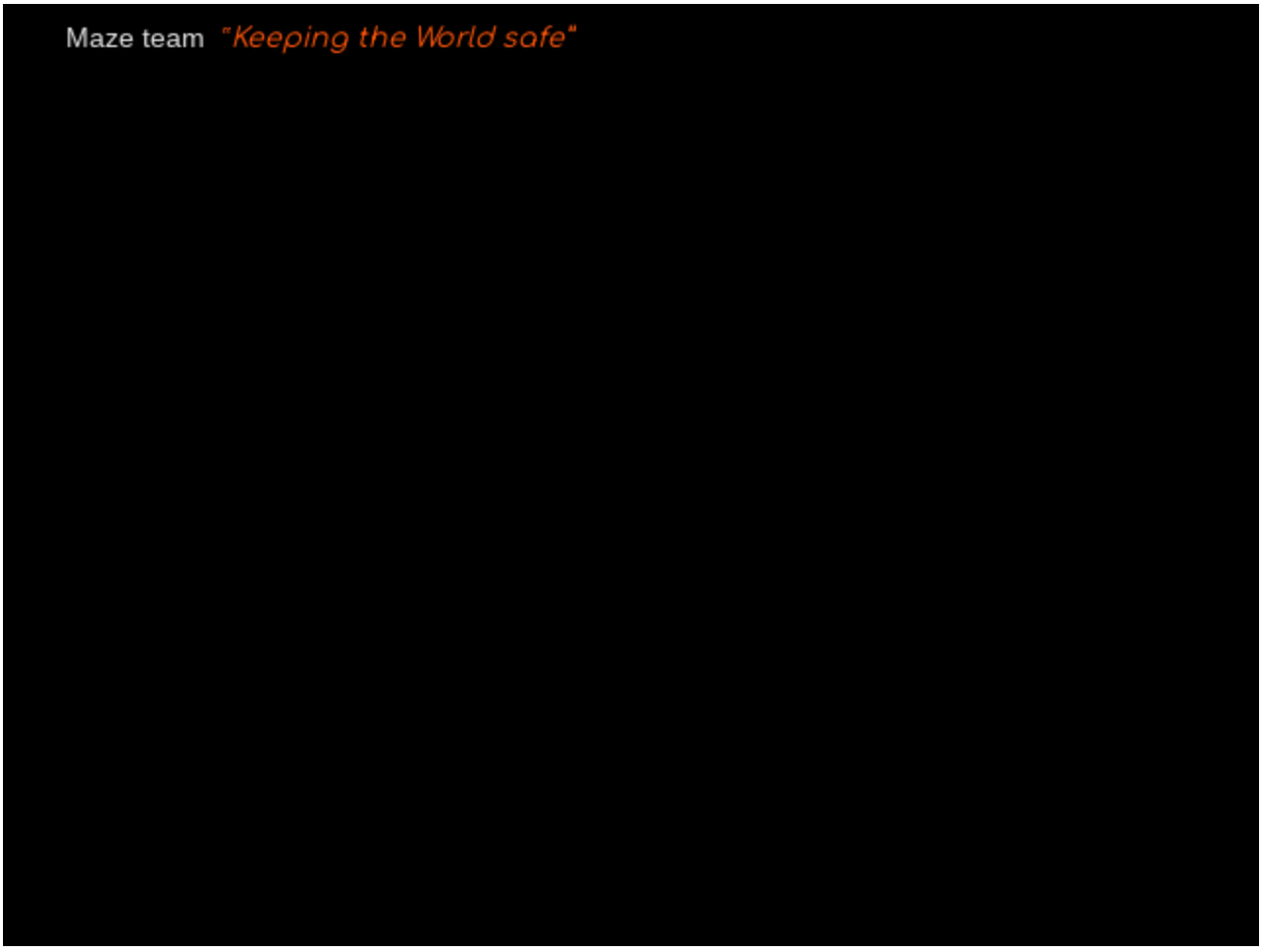
Here's how it works, according to Naked Security's Paul Ducklin: The crooks confront you with not one but two reasons to pay the extortion money:

- **Pay up to get the decryption key to recover your precious files**, which we scrambled with the malware.
- **Pay up to stop us releasing your precious files**, which we took copies of before we scrambled them.

Westech's saga is in keeping with how Maze operators work: they follow through on threats of public exposure of stolen data by posting it in public data dumps – what are also known as name-and-shame sites. If no payment is forthcoming, they'll offer it up on cybercrime forums. From the SophosLabs report:

> The Maze gang has made public exposure central to their 'brand' identity, and actively seeks attention from press and researchers to promote their brand—and make it easy for victims who might hesitate to pay them to find out their reputation.

"Brand identity?" Oh, yes, in all its animated glory. The ransomware has been around for more than a year, though it was originally known simply as ChaCha, after the encryption algorithm it used. In May 2019, its criminal operators adopted its current name, Maze, and have come up with their own visual branding:



How the Maze virus greets victims on its website.

I checked in with Westech International on Wednesday to see how it's doing with its recovery, whether there's any update on its investigation, and what the contractor's thinking might be vis-a-vis paying the ransom – a sum that hasn't been disclosed. I'll update this article if I hear back.

Pay or pray?

The answer, in a nutshell, is Please Don't Pay. There are very good reasons not to.

According to the State of Ransomware 2020 global study conducted earlier this year on Sophos's behalf, paying ransoms costs more than reinstating data using backups.

You might well ask how that could be, given that downtime is often cited as the most expensive part of a ransomware attack. The rationale is simply that the cost of recovery is always high, coming in at an average of $732,000. Paying the ransom on top of that simply doubles the bill.

As noted by Naked Security's John E. Dunn, this explains why extortionists almost always send back encryption keys when paid: if they didn't, then victims' doubt would "quickly destroy the whole extortion racket as companies knuckled down to do the hard work themselves."

That could explain why ransomware attackers are increasingly threatening to leak sensitive data stolen during the attack, as was done in the Westech incident: the threat is an added incentive to pay up.

What to do?

Organizations shouldn't despair. There are ways to limit the effect of ransomware attacks. The first step: assume that an attack is inevitable, and prepare for it.

Our advice:

- Make and test a **backup plan**, including storing data offsite where attackers can't locate it.
- **If you're buying cyber-insurance**, make sure it covers ransomware.
- Don't forget to **protect data in the cloud** as well as central data.
- **Use dedicated anti-ransomware protection**. Twenty-four percent of survey respondents that were hit by ransomware were able to stop the attack before the data could be encrypted.
- **Lock down Remote Desktop Protocol (RDP)**. Criminal gangs exploit weak RDP credentials to launch targeted ransomware attacks. Turn off RDP if you don't need it, and use rate limiting, two-factor authentication (2FA) or a virtual private network (VPN) if you do.
- **Pick strong passwords and use multi-factor authentication (MFA) as often as possible.** And don't re-use passwords, ever.
- **Patch early, patch often**. Ransomware like WannaCry and NotPetya relied on unpatched vulnerabilities to spread around the globe.

It's also worth reading Naked Security's advice on common mistakes that make ransomware easier to pull off from the attacker's point of view. For more detailed advice, please check out our end of ransomware page.

Latest Naked Security podcast

LISTEN NOW

Click-and-drag on the soundwaves below to skip to any point in the podcast. You can also listen directly on Soundcloud.