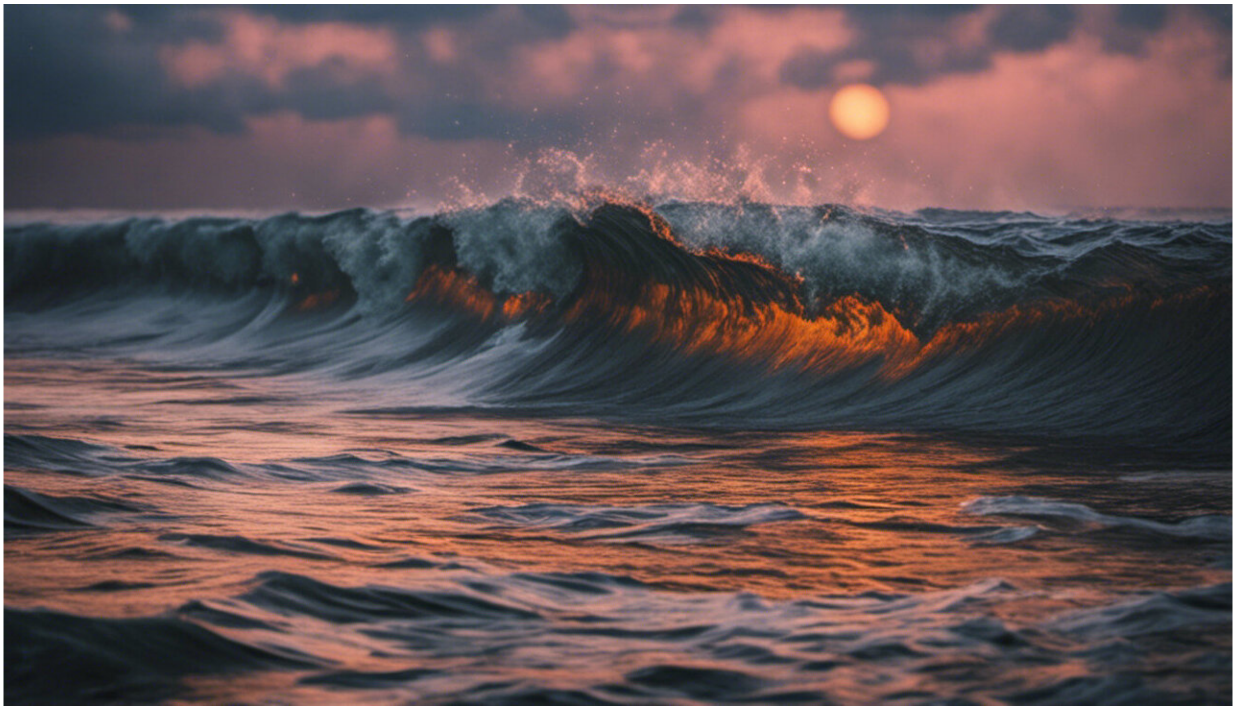
# What is ransomware and how to protect your precious files from it

February 18 2016, by Zubair Baig And Nikolai Hampton, Edith Cowan University



Credit: AI-generated image (disclaimer)

What would it mean if you lost all of your personal documents, such as your family photos, research or business records? How much would you pay to get them back? There's a burgeoning form of cybercrime that hinges on the answers to these questions.

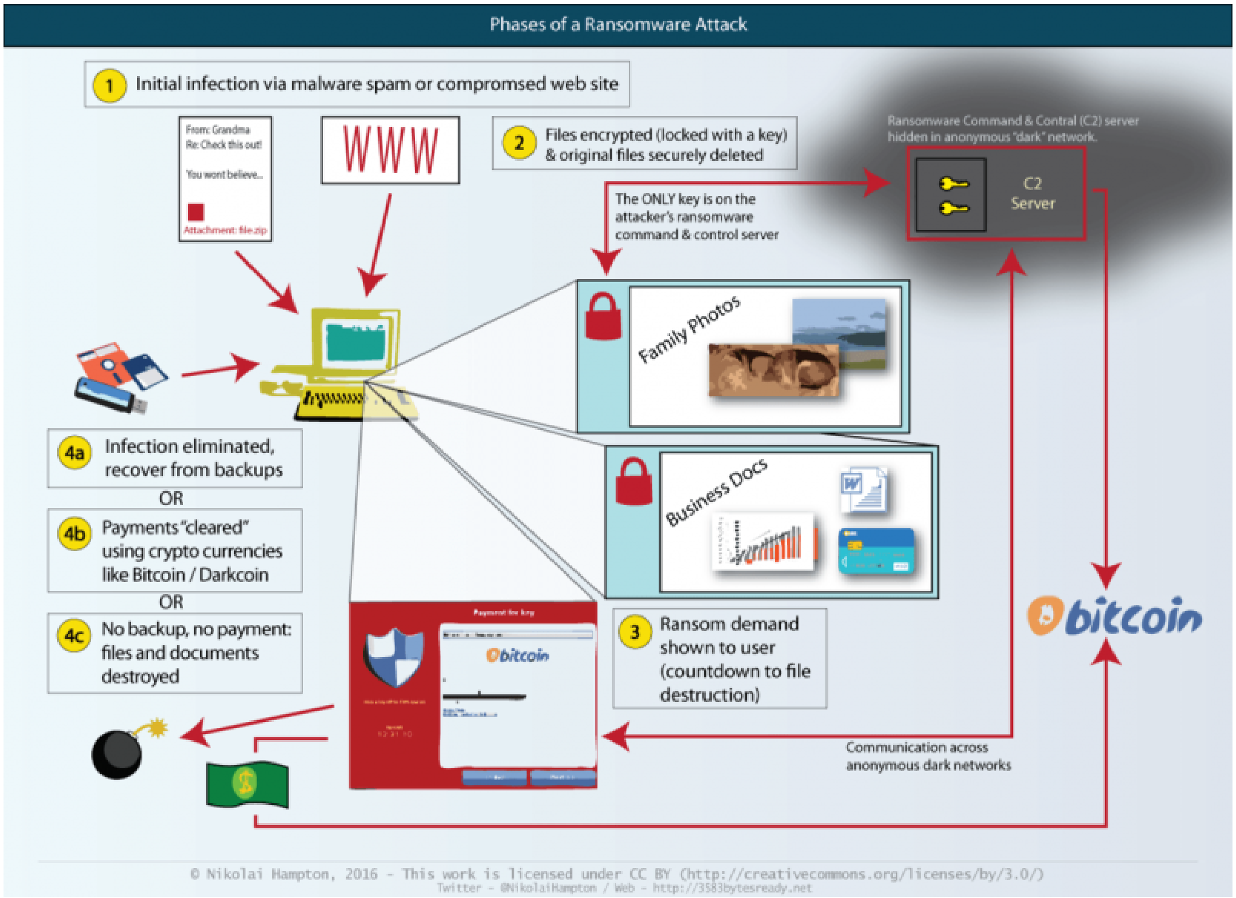
You have probably heard of viruses and malware. These dangerous pieces of software can make their way into your computer and wreak havoc. Malware authors are intent on stealing your data and disrupting the proper functioning of your digital devices.

Then there is ransomware. This is crafted by cyber-criminals for extorting data from innocent users, and is rapidly becoming a threat to individuals, small business and corporate users alike.

Unlike malware, ransomware does not steal data. Rather, it holds it captive by encrypting files and then displaying a ransom note on the victim's screen. It demands payment for the cyber-extortion and threatens obliteration of data otherwise.

While the concept of ransomware has existed for more than 20 years, it wasn't until 2012 that several key technological advances aligned and allowed it to flourish.

Now ransomware has evolved. It combines file encryption, it uses "dark" networks to conceal the attacker, and uses (or, rather, misuses) cryptocurrencies, such as Bitcoin, to prevent law enforcement from tracing the ransom payment back to the attacker's den.


Phases of a Ransomware Attack
1 Initial infection via malware spam or compromsed web site
From: Grandma
Re: Check this out!
You wont believe...
Attachment: file.zip
WWW
2 Files encrypted (locked with a key) & original files securely deleted
The ONLY key is on the attacker's ransomware command & control server
Ransomware Command & Contral (C2) server hidden in anonymous "dark" network.
C2 Server
Family Photos
Business Docs
4a Infection eliminated, recover from backups
OR
4b Payments "cleared" using crypto currencies like Bitcoin / Darkcoin
OR
4c No backup, no payment: files and documents destroyed
Payment for key
bitcoin
3 Ransom demand shown to user (countdown to file destruction)
bitcoin
Communication across anonymous dark networks
© Nikolai Hampton, 2016 - This work is licensed under CC BY (http://creativecommons.org/licenses/by/3.0/)
Twitter - @NikolaiHampton / Web - http://3583bytesready.net

Phases of a ransomware attack. Credit: NikolaiHampton on Twitter

For a small upfront cost and with low risk of getting caught, ransomware developers can net good returns: industry estimates range from 1,000% to 2,000% return on investment.

## What's driving ransomware proliferation?

Paying small ransom amounts is quite simply adding to the problem. If you don't, you lose your data; if you do pay, then you contribute to a worsening problem.

Yet for ransomware creators, it's a lucrative business. Industry figures vary greatly, but reports suggest that developers can earn more than US$1 million per year, which is enough to attract skilled programmers and engineers.

There have been many reports of Australian businesses paying ransoms. Even the authorities aren't safe, with several police departments in the US having paid ransoms in order to recover files. And we've even seen reports that FBI experts have advised victims to "just pay the ransom" if they need their data.

The biggest concern with ransomware is the rate at which it is adapting to combat security protections. We recently examined the evolution of ransomware and found that ransomware developers are learning from their mistakes in previous versions. Each generation includes new features, and improved attack strategies.

We also found that over 80% of recent ransomware strains were using advanced security features that made them difficult to detect, and almost impossible to "crack". Things don't look good for end-users; ransomware is increasingly using advanced encryption, networking, evasion and payment technologies. The developers are also making fewer mistakes and writing "better" software.

It's not a stretch to imagine a ransomware developer currently working on ways to attack even corporate databases, or versions that lay low while they identify all of your backup disks.

## How to protect yourself

Recovering files from ransomware is impossible without the attacker's approval, so you need to avoid data loss in the first place. The best thing you can do is practice good "digital hygiene":

- Don't fall prey to social engineering or phishing, which is where an attacker attempts to have you reveal sensitive information to them. If you receive a suspicious email from your grandma or work colleagues, ask yourself whether it's unusual before you click. If you're not sure, contact the sender via a different medium, such as giving them a phone call, to cross-check
- Don't install any software, plugins or extensions unless you know they're from a reputable source. If in doubt, ask and only rely on trusted download sources. And certainly don't be tempted to pick up USB sticks found on your pathway
- Update your software (comprising your operating system, web browser and other installed sofware) regularly to ensure you are always running the latest versions
- Back up! Important documents need to be treated like valued possessions. Grab a hand full of USB keys and rotate your backups daily or weekly, and don't leave USB keys plugged in (current malware strains can scan removable USB disks). Having multiple copies means the adversarial effort on holding you for ransom is pretty much worthless.

Ransomware is a very real threat. Its rapid growth is being driven by the low risk to attackers and good financial returns. We all need to stay ahead of the game. Let's start now and be safe not sorry!

*This article was originally published on* The Conversation. *Read the* original article.

Source: The Conversation

Citation: What is ransomware and how to protect your precious files from it (2016, February 18) retrieved 10 April 2024 from https://phys.org/news/2016-02-ransomware-precious.html