eBook

Forcepoint

Practical Guide to Combatting Ransomware

Table of Contents

Introduction

What is Ransomware?

Ransomware is a type of malware that encrypts an organization's files. The attacker then demands a ransom payment in return for the decryption "key" and may also threaten to publish the organization's data if the ransom is not paid.

How Does it Get In?

Ransomware attacks are typically carried out using a piece of malware that is disguised as a business document.

The user is tricked into downloading or opening, either as an email attachment or as a link to a document on a compromised website.

An Existential Threat

Times have changed. The global cost of ransomware in 2020 was put at $20 billion, with an average attack costing over $4 million[1]. Every 11 seconds a business will be attacked by ransomware in 2021. In 2020, 36% of victims paid the ransom. 17% of those who paid never recovered their data[2].

1 Source Betanews October 2020
2 Source Iumu

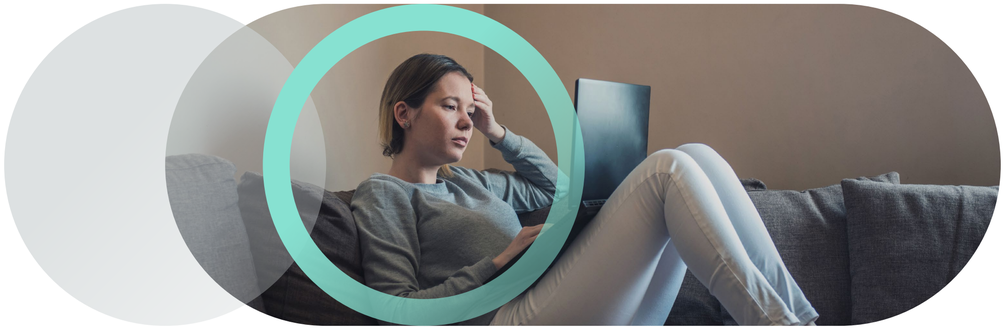
The first documented example of ransomware occurred in 1989 when 20,000 diskettes were infected with malware that hid directories and encrypted the names of the files.

The perpetrator demanded a ransom of $189 for the antidote to the virus.

Introduction

Read All About It

Ransomware is a costly and highly destructive threat to business with attackers moving beyond simply encrypting data to stealing it for profit or deliberate reputational damage.



Some prominent victims:

Maersk 2017:
All end-user devices, including 49,000 laptops and print capability, were destroyed. All 1,200 applications were inaccessible and approximately 1,000 were destroyed. Around 3,500 of 6,200 servers were destroyed. Chairman Jim Hagemann Snabe told the World Economic Forum in Davos that ransomware cost Maersk between $250 million and $300 million.

NHS 2017:
In May of 2017, the WannaCry ransomware attack infected more than 200,000 computers across 150 countries by sending phishing emails to vulnerable, older-version Microsoft system networks. The attack left the NHS with a £73million IT bill.

Travelex December 2019:
A ransomware attack forced the company to take down its websites across 30 countries in an attempt to contain the virus and protect data. Many of these were still offline two weeks later. In August 2020, the company went into administration, citing a combination of the ransomware attack and the coronavirus pandemic as key reasons for its failure.

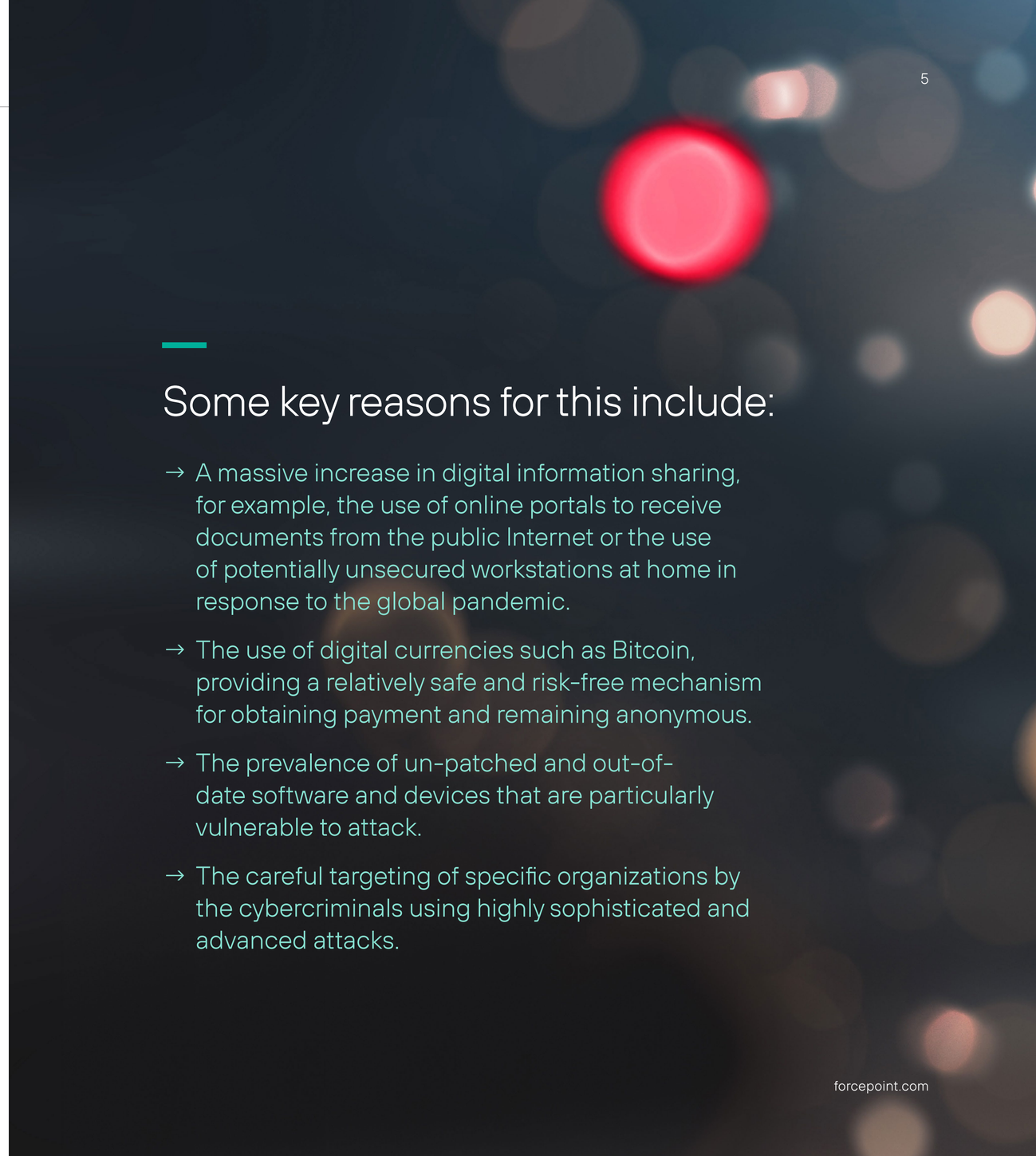
Redcar and Cleveland Council 2020:
135,000 people were without online public services after Redcar and Cleveland's website and computers were targeted in February. The attack on a council's computer systems is estimated to have cost more than £10m.

Garmin 2020:
Smartwatch and wearables maker Garmin reportedly paid criminals $10 million via an intermediary for the decryption keys that enabled it to return production systems to full working order after a ransomware attack took out websites, customer support, and user applications.

Introduction

Elevated Threat Level

Ransomware attacks are not new, but they are evolving and becoming more sophisticated. It seems likely that the criminals are ploughing their profits back into the tools and platforms they use, building up expertise, and targeting increasingly high-profile organizations, confident in the knowledge that they are unlikely to be brought to account. Four of the top five most dangerous pieces of malware were recorded in 2020[3] were ransomware.



Some key reasons for this include:

- → A massive increase in digital information sharing, for example, the use of online portals to receive documents from the public Internet or the use of potentially unsecured workstations at home in response to the global pandemic.
- → The use of digital currencies such as Bitcoin, providing a relatively safe and risk-free mechanism for obtaining payment and remaining anonymous.
- → The prevalence of un-patched and out-of-date software and devices that are particularly vulnerable to attack.
- → The careful targeting of specific organizations by the cybercriminals using highly sophisticated and advanced attacks.

Defending Your Organization From Ransomware

Make regular backups
Make regular backups and test that the restore procedure works correctly – don't just trust that it will work should it be needed! Don't leave backups and backup storage devices connected to the network where they could be compromised as a part of a ransomware attack. Ideally, locate backups off-site and make multiple copies of your data.

Prevent malware from being delivered
Reduce the risk of attack by controlling the likelihood of malicious content reaching your devices by only accepting the file types you would expect to receive, blocking websites that are known to be malicious, and actively inspecting content.

Prevent malware from running
Centrally manage devices in order to only permit applications trusted by the enterprise to run. Disable or constrain scripts and macros from running. Install security updates as soon as they become available in order to fix exploitable bugs in your products.

Prepare for an incident
Identify critical assets and determine the impact to these if they were affected by a malware attack. Develop an incident management plan that encompasses an internal and external communication strategy. Determine how you will respond to the ransom demand and the threat of your organizations data being published. Identify your legal obligations.

This advice is taken directly from the NCSC's extensive guidance, published in Mitigating Ransomware

Combatting the Threat

Step 1: Prevent

Identify Information Flows
Identify each of the key information flows into the organization, from email and Web browsing to file sharing and remote working. Each information flow needs to be robustly guarded.

Consider Segregating Networks
Pay particular attention to the information assets and personnel within the business. An effective backup strategy will help mitigate against the threat of an attacker encrypting your data, but it won't stop the attacker from publishing your data if they do get in and steal it.

It may be necessary to physically segregate networks to provide an additional layer of defence for high-value data and key staff members.

Invest in Advanced Protection
Ransomware attacks are getting more targeted and sophisticated every day. They are now being focussed specifically on individual organizations.

Each attack probably only gets used once, so it has a very short time to live. Next time it is used, a change is made to the attack and it is targeted at a new victim.

Ensure detection-based anti-virus defenses are kept up to date, but be aware that it is very difficult for cyber defences based on detection to keep up with the latest threats and the changes made to an attack each time it is used.

In addition, look to deploy an advanced protection solution that uses techniques such as transformation to ensure incoming files are safe. These techniques don't suffer from the shortcomings of detection-based defences and can be relied upon to only deliver safe, malware-free files. Advanced protection can be deployed on every information flow into the organization to protect from sophisticated attacks.

> Move Beyond Detection to prevent highly evasive attacks by carefully selecting a set of preventing controls that do not depend on the detection of threats. Gartner "Beyond Detection: 5 Core Security Patterns to Prevent Highly Evasive Attacks."
>
> Published: 25 March 2018

Backup Data
The most important part of any ransomware security strategy is regular data backups. Most companies do this, but surprisingly few run backup and restore drills.

Both processes are important. Restore drills are the only way to know ahead of time whether your backup plan is working. If you test your backup and restore drill regularly you can reduce the impact of the attack by having a safe, recent restore point.

Update and Patch
Ensure operating systems, security software, applications, and network hardware devices are fully patched and updated.

Many attacks take advantage of known vulnerabilities that manufacturers have patched. Failing to apply the patches quickly/in a timely manner leaves the door wide open to attackers.

Train Staff
Nine times out of ten, a ransomware attack begins with a seemingly innocent business document arriving as an email attachment, a download from a compromised website, or an upload from an untrusted or unprotected workstation.

Attackers make extensive use of social engineering techniques to persuade unwary staff into opening these documents, so it's vital to ensure every member of staff is educated to the potential danger.

Combatting the Threat

Step 2: Respond

Unplug Immediately

Immediately unplug all infected workstations and devices from the network. Make sure this includes any tablets and mobile devices that have been affected, ensuring both wireless and wired connections are disconnected.

> The ability to contain the incident is the key to recovering from it and having the business up and running before it takes out crucial data.

Contact the Authorities

A crime has been committed. Contact the relevant law enforcement authorities and report it.

Restore from Backup

Wipe all infected workstations and endpoints, reinstalling the operating systems and application software from scratch. Verify your backups have not been infected and restore your data from backup. Then reconnect to the network.

You should change the administrator access credentials for any system that hosts critical data assets such as customer details and monitor these systems closely for signs of activity that might indicate the attackers are still moving laterally inside the network or that the infection is still active.

Execute your Incident Response Plan

In parallel, you should execute your Incident Response Plan. An Incident Response Plan defines the roles and responsibilities of every member of the team in the event of an attack.

At a technical level, it defines who is responsible for restoring devices from backup, accessing off-site backups if these are required, which services need to be restored first, and when particular critical systems will be able to be brought back online.

At a broader business level, the plan specifies the stakeholders who need to be informed that an attack has taken place. In regulated environments, there will be a legal requirement to inform the relevant regulatory bodies as well as any customers who may be impacted.

> "Emergency response exercises failed to provide employees with decision-making experience in dealing with cyber-attacks"
>
> US Gas Pipeline Shut After Ransomware Attack, InfoSecurity Magazine 19th February 2020.

Combatting the Threat

Step 3: Review

Conduct a Forensic Analysis

Sometimes, ransomware is part of a sophisticated attack that involves multiple payloads. Perhaps the attackers have moved laterally within the network and installed keyloggers, stolen credentials, or opened up command and control channels, enabling them to enter the network remotely at a later date.

The only way to regain confidence in the integrity of the internal systems is to perform a comprehensive forensic analysis of the attack, including precisely how the initial compromise occurred. Companies without the internal skills and expertise to perform this type of forensic analysis should seek the assistance of digital forensic specialists to help them.

Review the Incident Response

You executed an Incident Response Plan. How effective was it? Were you able to contain the disruption and damage done by the attack? How long was it before you were able to resume "business as usual?" What lessons can you learn and apply going forward?

Increase Training

The vast majority of ransomware attacks are initiated by an unsuspecting user opening a document or clicking on a link. As part of the review, identify any additional training for staff to help them identify the tell-tale signs that a document is not all that it appears to be.

Focus on those most likely to be targeted and educate them to some of the more common techniques such as CEO fraud and social engineering techniques designed to appeal to our natural curiosity or desire to respond promptly to requests from authority.

Strengthen Boundary Protection

Existing detection based anti-malware defences need to be reviewed in the light of the attack. Office documents, images, and Adobe PDF files are all capable of carrying concealed malware.

The widespread use of these files makes them the prime carrier for initial infiltration of the network. If the existing defenses failed to detect the threat, they will need augmenting with more advanced protection that doesn't rely on detection to try and prevent an attack.

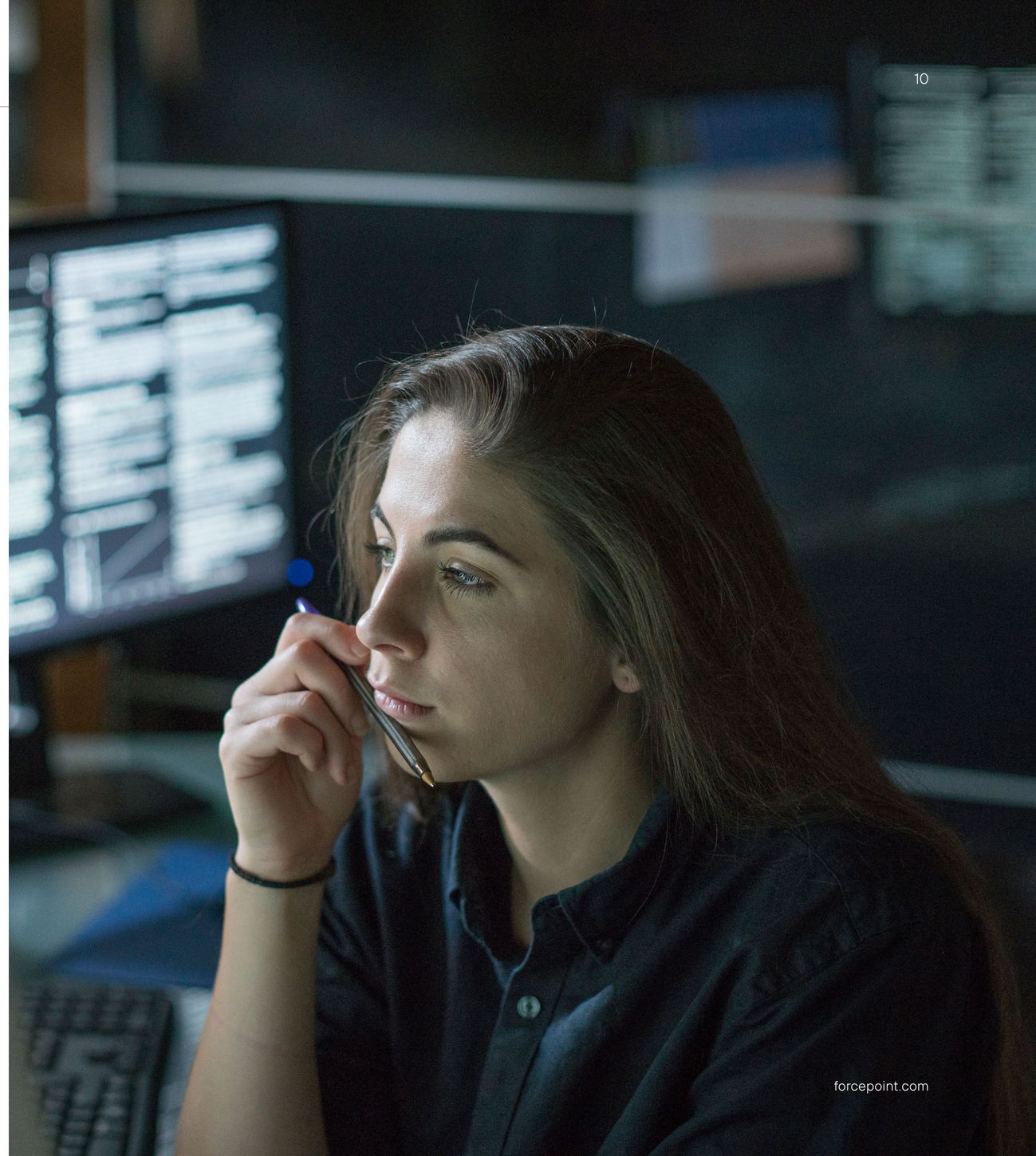
New techniques are now available that transform these and many other types of incoming files, making them safe without trying to detect the presence of the threat.

Summary

Ransomware is here to stay.

The best way to mitigate the threat is to prevent it from entering your organization. Although detection-based virus scanners can help, criminals are increasingly finding ways to evade detection. Combatting this problem requires additional defences that offer advanced protection, transforming incoming files to remove any threats and make them completely safe.

For more information, check out Forcepoint Zero Trust CDR



Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint simplifies security for global businesses and governments. Forcepoint's all-in-one, truly cloud-native platform makes it easy to adopt Zero Trust and prevent the theft or loss of sensitive data and intellectual property no matter where people are working. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on www.forcepoint.com, Twitter and LinkedIn.