SOPHOS
Cybersecurity evolved.

nutmeg CONSULTING

How to stay protected against Ransomware

Businesses large and small are under threat from increasingly aggressive and brutal ransomware attacks. Loss of access to critical files, followed by a demand for payment, can cause massive disruption to an organization's productivity.

But what does a typical attack look like? And what security solutions should be in place to give the best possible defense?

This paper examines commonly used techniques to deliver ransomware, looks at why attacks are succeeding, and gives ten security recommendations to help you stay secure.

Ransomware – a brief introduction

Ransomware is still one of the most widespread and damaging threats that internet users face. Since the infamous CryptoLocker first appeared in 2013, we've seen a new era of highly targeted file-encrypting ransomware variants delivered through spam messages and exploit kits, extorting money from home users and businesses alike.

The current wave of ransomware families can have their roots traced back to the early days of Fake AV, through "Locker" variants and finally to the file-encrypting variants that are prevalent today. Each distinct category of malware has shared a common goal – to extort money from victims through social engineering and outright intimidation. The demands for money have grown more forceful and audacious with each iteration with some hackers now demanding millions.

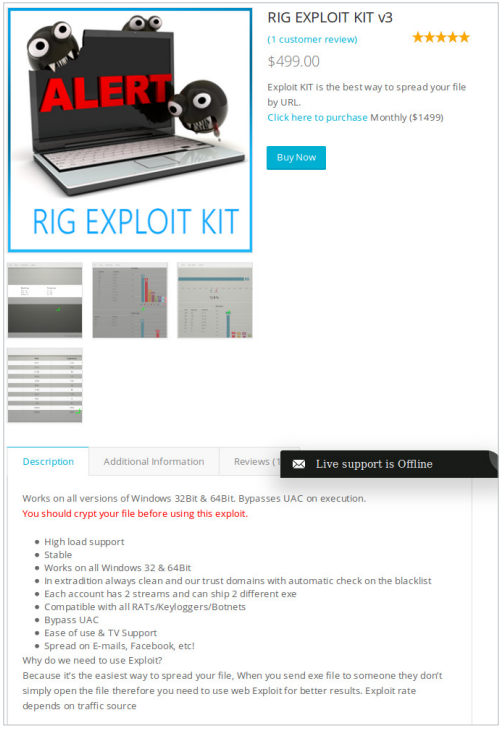
Despite rumors of the demise of ransomware, it is still very much alive and kicking. A Sophos survey of 3,100 organizations found that 30% of cyberattack victims had been hit by ransomware. Additionally, and of concern, nine in 10 respondents said their organization was running up to date cybersecurity protection at the time of the attack.

Why are ransomware attacks so successful?

Most organizations have at least some form of IT security in place. So why are ransomware attacks slipping through the net?

1. Hacking is becoming easier while attackers are becoming more sophisticated in their approach

- 'Exploit as a Service' (EaaS) programs that take advantage of vulnerabilities in existing software products are increasingly accessible. These kits make it simple for less tech-savvy criminals to initiate, complete, and benefit from a ransomware attack.
- Criminals use skillful social engineering to prompt users to run the ransomware's installation routine. They try to trick users into activating the ransomware with emails that encourage the recipient to click on a link or open a file, for example: "My organization's requirements are in the attached file. Please provide me with a quote."
- Producers of ransomware operate in a highly organized fashion. This includes providing a working decryption tool after the ransom has been paid, although this is by no means guaranteed.



2. Security problems at affected companies

- Systems are often unpatched leaving them unnecessarily vulnerable to threats
- Inadequate backup strategy and lack of disaster recovery practice/plan (backups not offline/off-site)
- Updates/patches for operating system and applications are not implemented swiftly enough or at all
- Dangerous user permissions (users work as administrators and/or have more file rights on network drives than necessary for their tasks)
- Lack of user security training ("Which documents may I open and from whom," "What is the procedure if a document looks malicious," "How do I recognize a phishing email?")
- Lack of layered security strategy so attackers often only need to overcome a single hurdle

- Inconsistent or incomplete security policies that leave gaps through which attackers can enter
- Conflicting priorities ("We know that this method is not secure but our people have to work...")
- Poorly configured IT security (badly regulated external access, e.g. Remote Desktop Protocol exposed)

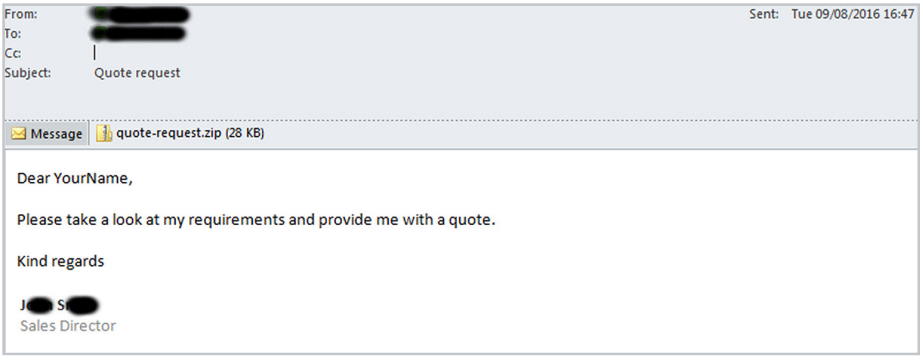
How does a ransomware attack happen?

There are multiple ways that a ransomware attack starts. Common techniques include:

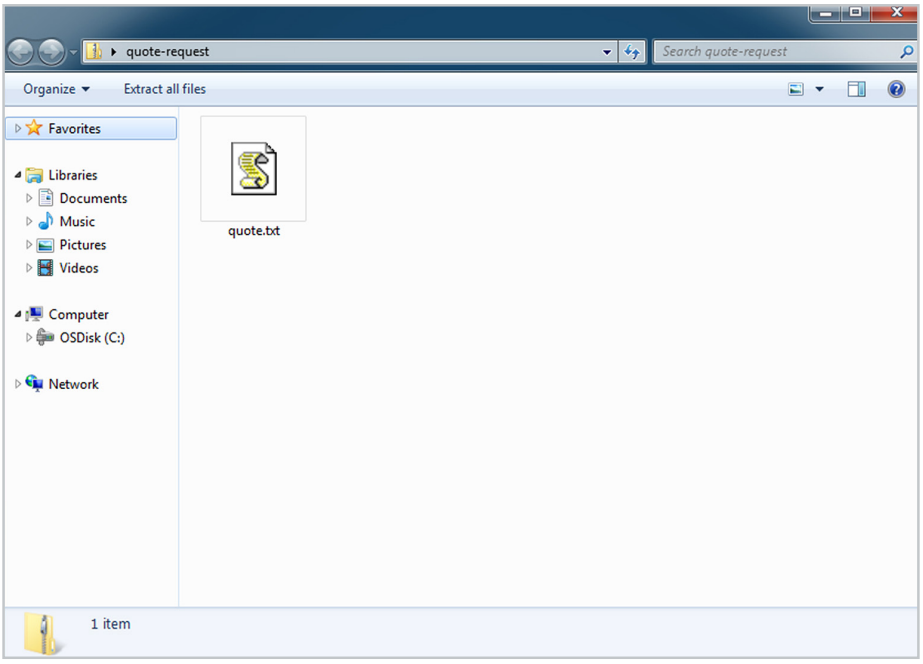
- Malicious emails
- Poisoned websites redirecting you to exploit kits
- Remote Desktop Protocol (RDP) and other remote access holes

Malicious emails

Today's criminals are crafting emails that are indistinguishable from genuine ones. They are grammatically correct with no spelling mistakes, and often written in a way that is relevant to you and your business.



In this example, the zip file appears to contain an ordinary .txt file.



However, when the file is executed, the ransomware is downloaded and installed onto your computer. In this example the Trojan horse is actually a JavaScript file disguised as a .txt file, but there are many other variations on the malicious email approach, such as a Word document with macros, and shortcut (.lnk) files.

Poisoned websites redirecting you to exploit kits

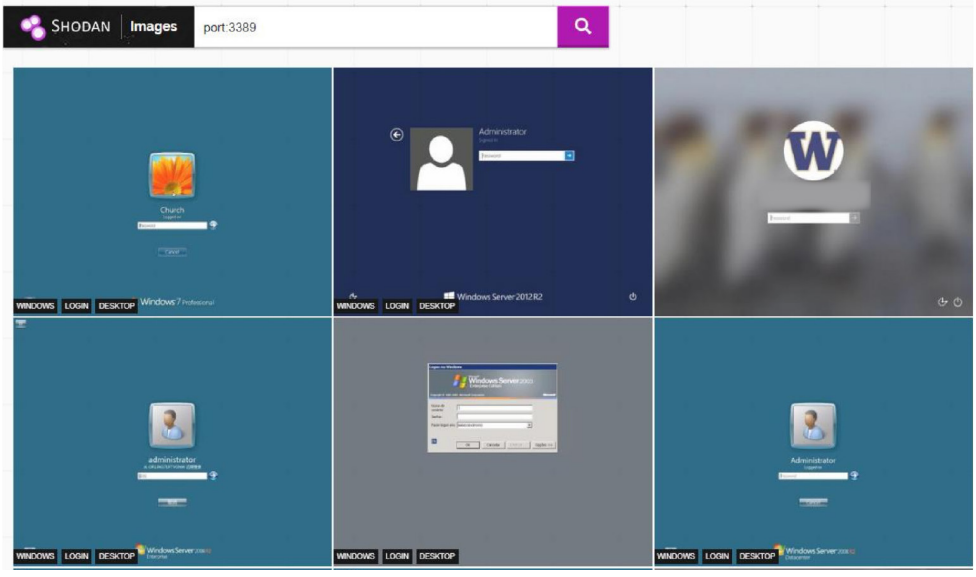
Another common way to get infected is by visiting a legitimate website that has been infected with an exploit kit. Even popular websites can be temporarily compromised. Exploit kits are black market tools that criminals use to exploit known or unknown vulnerabilities (such as zero-day exploits).

You browse to the hacked website and click on an innocent-looking link, hover over an ad, or in many cases just look at the page. And that's enough to download the ransomware file onto your computer and run it, often with no visible sign until after the damage is done.

RDP

RDP is what allows people to control Windows computers via a full graphical user interface, over the internet. The millions of internet-connected computers running RDP includes everything from cloud-hosted servers to Windows desktops used by remote workers, and each one is a potential gateway into an organization's internal network.

While RDP is an immensely useful tool for organizations, RDP servers are protected by no more than a username and password, and many of those passwords are bad enough to be guessed, with a little (sometimes very little) persistence.



6 of 5.2 million exposed RDP ports utilizing a simple and free search engine

For more information on securing you RDP servers, read our white paper RDP Exposed – The Threat That's Already at Your Door.

How do ransomware attacks unfold?

After initial exposure, attacks typically fall into two different categories:

'Fire and forget'

These types of automated attacks target multiple organizations with the hope of securing a high quantity of smaller ransoms. Think back to WannaCry. Thousands and thousands of organizations were hit by WannaCry at the same time. These hackers use automated, 'fire and forget' techniques, where the attack is launched and spread to as many computers as possible. Due to the automation and number of attacks, the attacker is oblivious to the stages of the attack.

A typical attack of this nature looks like this:

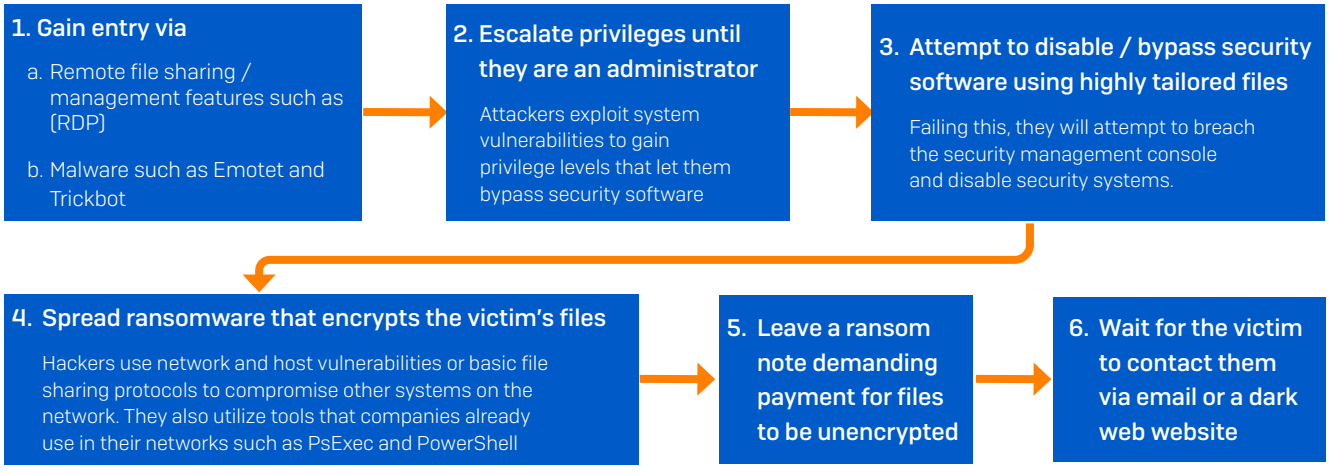
1. Gain entry via
    a. Opened attachments/links from mass phishing emails
    b. Visiting compromised/poisoned websites (while being secretly redirect to another IP hosting an exploit kit)
2. This then triggers a download of the ransomware which executes and encrypts files
3. A ransom note is generated demanding payment for files to be unencrypted
4. Wait for the victim to contact them via email or a dark web website

Should the chain break at any stage, the attack automatically ends.

Targeted ransomware

Targeted ransomware is a very manual attack, typically focuses on one victim at a time and often demands much higher ransom fees. The attackers gain access to the network and move laterally; identifying high value systems in the process. Strains of this type of ransomware, overcome challenges as they arise, making them particularly deadly.

A typical targeted ransomware attack looks like this:



10 best security practices to apply now

Staying secure against ransomware isn't just about having the latest security solutions. Good IT security practices, including regular training for employees, are essential components of every single security setup. Make sure you're following these 10 best practices:

1. Patch early, patch often

Malware that doesn't come in via a document often relies on security bugs in popular applications, including Microsoft Office, your browser, Flash, and more. The sooner you patch, the fewer holes there are to be exploited.

2. Backup regularly and keep a recent backup copy off-line and off-site

There are dozens of ways other than ransomware that files can suddenly vanish, such as fire, flood, theft, a dropped laptop, or even an accidental delete. Encrypt your backup and you won't have to worry about the backup device falling into the wrong hands. Furthermore, a disaster recovery plan that covers the restoration of data and whole systems.

3. Enable file extensions

The default Windows setting is to have file extensions disabled, meaning you have to rely on the file thumbnail to identify it. Enabling extensions makes it much easier to spot file types that wouldn't commonly be sent to you and your users, such as JavaScript.

4. Open JavaScript (.JS) files in Notepad

Opening a JavaScript file in Notepad blocks it from running any malicious scripts and allows you to examine the file contents.

5. Don't enable macros in document attachments received via email

Microsoft deliberately turned off auto-execution of macros by default many years ago as a security measure. A lot of infections rely on persuading you to turn macros back on, so don't do it!

6. Be cautious about unsolicited attachments

The crooks are relying on the dilemma you face knowing that you shouldn't open a document until you are sure it's one you want, but you can't tell if it's one you want until you open it. If in doubt leave it out.

7. Monitor administrator rights

Constantly review admin and domain admin rights. Know who has them and remove those who do not need them. Don't stay logged in as an administrator any longer than is strictly necessary and avoid browsing, opening documents, or other regular work activities while you have administrator rights.

8. Stay up to date with new security features in your business applications

For example, Office 2016 now includes a control called "Block macros from running in Office files from the internet," which helps protect against external malicious content without stopping you from using macros internally.

9. Regulate external network access

Don't leave ports exposed to the world. Lock down your organization's RDP access and other management protocols. Furthermore, use two-factor authentication and ensure remote users authenticate against a VPN.

10. Use strong passwords

It sounds trivial, but it really isn't. A weak and predictable password can give hackers access to your entire network in a matter of seconds. We recommend making them impersonal, at least 12 characters long, using a mix of upper and lower case and adding a sprinkle of random punctuation Ju5t.LiKETh1s!

Working with a Managed Security Services Provider

Managing your cybersecurity system and keeping it active and updated is a full-time job that most business owners simply do not have time for. Partnering with a managed service provider (MSP) solves this problem for you by offering custom cybersecurity solution services to suit your business needs.

MSPs are organizations that work as an extension of your business to fill any IT security gaps through offerings like software deployment, ongoing maintenance, monitoring, reporting and more. These types of managed security services are critical for businesses without the required resources or expertise to ensure a strong security posture – giving you time back to run your business. As your trusted advisor of technology and security, we will partner with you to learn your business, then build the security policies to protect your data. Finally, you also get tailored reports with information you need to make informed business decisions.

To learn more about how **Nutmeg Consulting** can help secure your business from cyberthreats, please contact: **info@nutmegit.com**

Nutmeg Consulting, LLC
35 Philmack Drive B206
Middletown, CT 06457
860-256-4822

nutmegit.com
Email: info@nutmegit.com

Sophos delivers industry leading cybersecurity solutions to businesses of all sizes, protecting them in real time from advanced threats such as malware, ransomware, and phishing. With proven next-gen capabilities your business data is secured effectively by products that are powered by artificial intelligence and machine learning.

2021-24-02 (NP)