Pinnacle Computer Services
SOLUTIONS FOR BUSINESS

netwrix

Defending Against Crypto-Ransomware

Contents

1. Introduction

Ransomware is one of the fastest growing classes of malicious software. In recent years, ransomware has evolved from a simple lock screen with the ransom damage into far more dangerous variants, such as crypto-ransomware.

Unlike traditional malware, crypto-ransomware doesn't steal information. Instead, it encrypts a victim's documents, spreadsheets, pictures, videos and other files, and then demands a ransom to unlock the encrypted files — a form of digital blackmail. The ransom amount varies, from $150–$500 for an individual to thousands of dollars for an organization. The payment goes through systems that are hard to trace, such as wire transfers, premium-rate text messages, pre-paid voucher services like Paysafecard, or the digital currency Bitcoin.

While ransomware attacks have been around for years, security experts say they've become far more dangerous recently because of advances in encryption and other technologies. A crypto-ransomware attack can take hostage not only data stored on a company's individual computers,[1] but also the files on its servers and cloud-based file-sharing systems — leading to financial losses, stopping business in its tracks and potentially damaging the organization's reputation. According to a report prepared by the Cyber Threat Alliance (CTA), CryptoWall version 3.0 alone has already cost victims $325 million.

2. How Ransomware Is Delivered to a User's Computer

Criminals use many different methods to propagate crypto-ransomware, including the following:

- Email attachments containing malware or malicious macros Infected
- disks or other malvertising
- Drive-by downloads that exploit redirects and software vulnerabilities

2.1 Email Attachments Containing Malware or Malicious Macros

In most cases, malware arrives in an email attachment. The email often purports to be from a known entity, such as a bank or colleague, and has an attention-grabbing Subject line, such as "Dear Valued Customer", “Undelivered Mail Returned to Sender" or "Invitation to connect on LinkedIn."

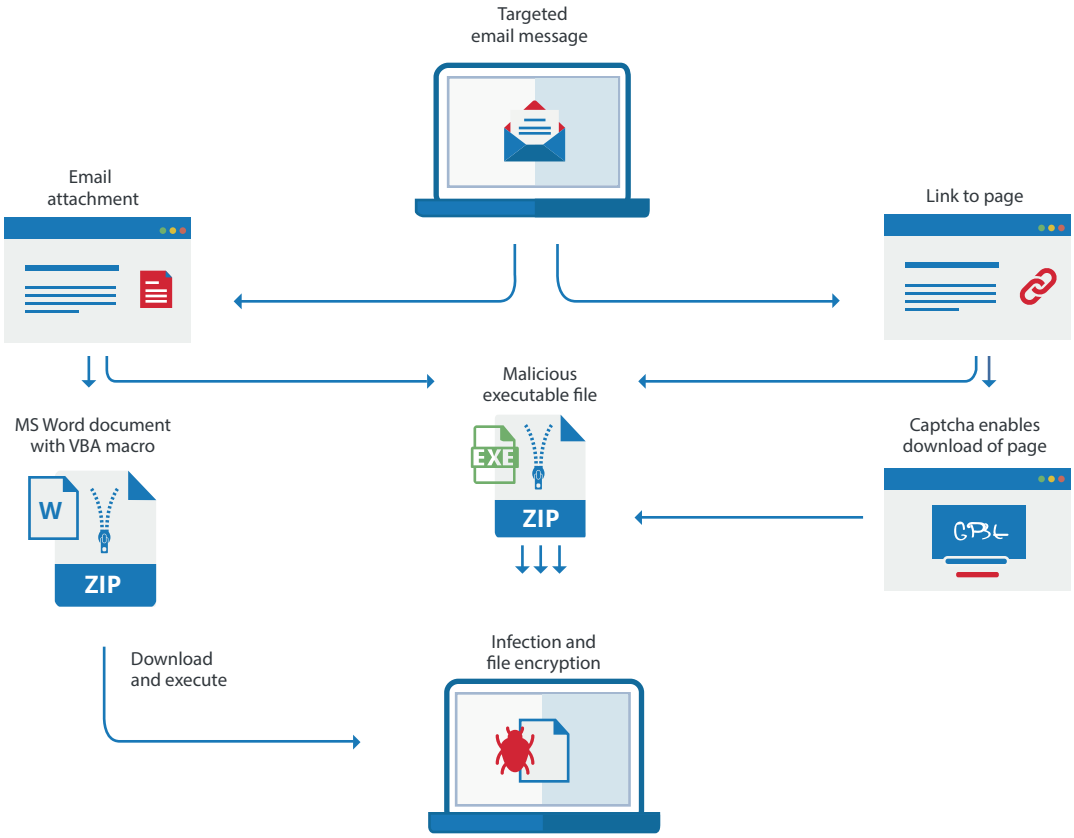


Figure 1. Methods of ransomware delivery via email

The names of the attachments are chosen to disguise their true nature. In particular, the name often includes a common extension such as ".doc" or ".xls", so if display of file extensions is disabled in the system settings, the user will think the file is a Word or Excel document. For example, the full file name might be "Paper.doc.exe" but the user will see only "Paper.doc" and be misled into thinking the file is harmless.

Or the attachment might actually be a .doc file, but include malicious macros. If a user opens such document and macros are enabled in Microsoft Office (which they are by default), malware installation begins automatically. If macros have been disabled, the user will see blocks of garbled text and a note such as, "Enable macro if the data encoding is incorrect." If the user enables macros, the malware will then infect the system.

2.2 Infected Disks and Other Malvertising

Files containing malware or malicious macros can also be provided to potential victims on disks or other malvertising. Once the user opens the file, the ransomware spreads.

2.3 Drive-by Downloads, Redirects and Exploits

Users can also inadvertently become victims simply by visiting a compromised web page — for example, by downloading malicious code via banner ads in Flash after multiple malicious redirects, as illustrated in Figure 2. These "drive-by downloads" usually exploit a security flaw or other vulnerability in a browser, app or operating system, often because the software has not been kept up to date with patches.

For example, CryptoWall uses the Angler, Neutrino and Nuclear exploit kits to load. It can exploit vulnerabilities in web browsers, Java and PDFs, but the most common vulnerabilities are in Flash.

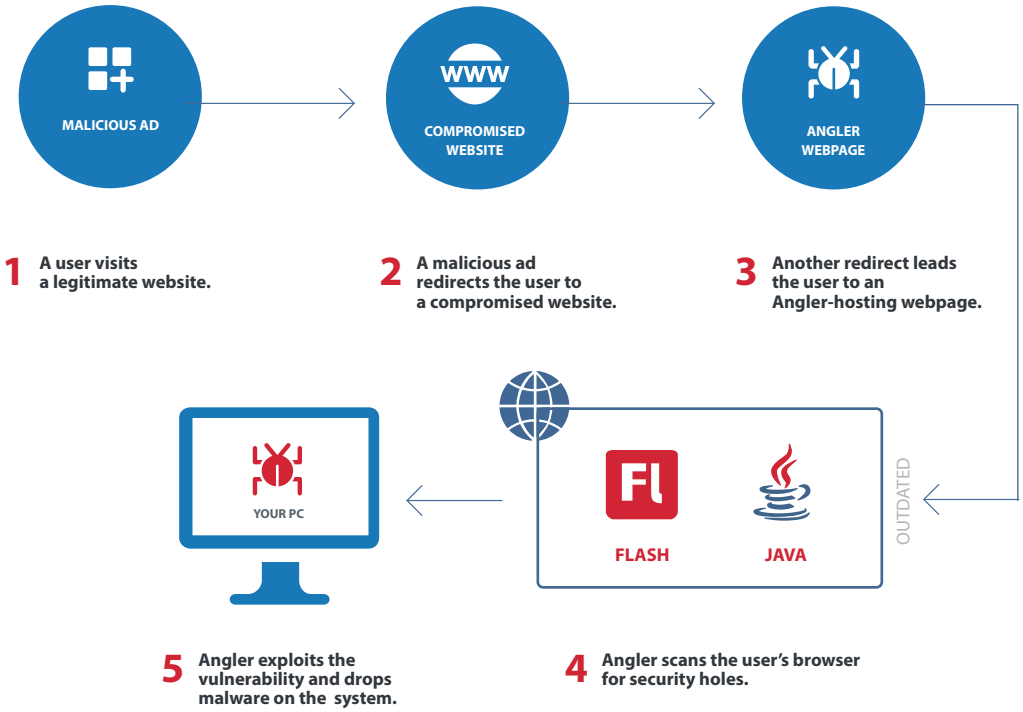


Figure 2. How criminals use web redirects and exploit software vulnerabilities to deliver malware

3. Stages of Crypto-Ransomware Infection

Crypto-ransomware infection typically consists of the following steps:

1. Break-in

A user unintentionally opens a malicious file propagated via a compromised website or infected email attachment, thereby releasing a ransomware client.

2. Installation

The malware copies itself into various locations in the system, such as:

- <%appdata%>
- <%startup%>
- <%rootdrive%>/random_folder/
- A %WINDOWS% directory with a random name, such as "%WINDOWS%\ycizilys.exe"

Then it edits the registry so it will start automatically after every system reboot.

3. Encryption key generation

The ransomware client builds an SSL connection with a command and control server, and generates a public-private key pair to encrypt its victim's files. The client might use the Tor network to anonymize the traffic and make tracing the crime more difficult. Some crypto-ransomware can generate a key pair locally on the infected machine; in that case, the user's machine does not need to be connected to internet for the malware to encrypt the files.

Crypto-ransomware uses strong encryption modes such as RSA-2048, which virtually eliminates the possibility of the user discovering the key to decrypt the files.

4. Data encryption

Using the victim's access rights, the crypto-ransomware scans all available physical and cloud-based drives for files to encrypt, and encrypts the files.

5. Extortion

The malware displays a ransom note with instructions for how the victim can pay a ransom to unlock the encrypted data.

4. Best Practices to Apply Immediately

Analysis of reported crypto-ransomware attacks reveals several reasons why the attacks were successful:

- Systems were weakly protected.
- Employees had little or no cyber security education, so they would click on almost anything.
- The organizations were using outdated software and equipment that left numerous security holes to be exploited.

Decoding files encrypted by ransomware can take months or even years, if it is possible at all. Therefore, it is critical to take steps to prevent infection and be prepared to restore from backup if prevention fails. Specific measures include the following:

- **Back up your systems regularly and keep a recent backup off site.** If you suffer a ransomware attack, you can easily restore your files from the backup. To protect your backups, encrypt them and store them outside your network (for example, on cloud storage).
- **Properly configure access to shared folders.** If you use a shared network folder, create a separate network share for each user. Since malware spreads using its victim's access rights, track use of network shares to make sure that access is restricted to the fewest users and systems possible. Otherwise, the infection of one computer can lead to the encryption of all documents in all folders on the network.
- **Restrict user permissions to "Read" whenever possible.** Without full control rights, crypto-ransomware cannot access and encrypt files.
- **Install the latest patches and updates.** Updating your operating systems and applications helps protect against drive-by download attacks that exploit software vulnerabilities. Pay particular attention to Adobe Flash, Microsoft Silverlight and web browsers.
- **Configure Group Policy properly:**
  - **Block macros** from running in Office files from the internet.
  - **Block executable extensions.** Use the Software Restriction Policy to prevent executables from being run. This policy blocks script execution and launch attempts by files that have been extracted from compressed formats.
  - **Block AutoPlay** to disable software execution from removable media.
  - **Blacklist all applications from running on workstations** and granularly whitelist only trusted ones using the Application Control Group Policy.

- **Blacklist Tor IP addresses.** Some malware uses the Tor network for command-and-control purposes. By blocking Tor IP addresses, you can prevent some ransomware from fully installing.
- **Properly configure your web filter, firewall and antivirus software** to block access to malicious websites and to scan all files that are downloaded.
- **Educate your employees and executives** about how to spot phishing emails. Help them enable display of file extensions, and teach them to be wary of the common malware extensions, including .exe, .com, .js, .wbs, .hta, .bat and .cmd.
- **Set .JS files to open with Notepad by default.** This protects against JavaScript-borne malware.

5. How Netwrix Auditor Can Limit the Damage from Crypto-Ransomware

Building multiple layers of security against crypto-ransomware is the most effective way to avoid business downtime, financial losses and damage to your reputation. The Netwrix Auditor platform enables you to mitigate the risk of malware spreading across your network, detect activity indicative of a malware attack in progress, and granularly restore lost files.

5.1 Establish and Enforce a Least-privilege Model

- Review the Account Permissions report regularly to ensure that the permissions assigned to each user account accord with the employee's role, and that no permissions are assigned to "Everyone." You can also use this report after an attack to determine which files the infected account had access to, in order to outline the potential area of infection.

Account Permissions

Shows accounts with permissions granted on files and folders.

User Account: ENTERPRISE\J.Carter

Object Path	Permission	Means Granted
\\fs1\shared	Full Control	Directly
\\fs1\shared\Accounting	Full Control	Group
\\fs1\shared\Contractors	Full Control	Directly
\\fs1\shared\Finance	Full Control	Directly
\\fs1\shared\Human Resources	Full Control	Directly
\\fs1\shared\IT	Full Control	Group

- Check who has access to critical files and folders, and verify that this list is limited to users with a legitimate business need for this data.

Object Permissions by Object

Shows file and folder permissions granted to accounts, grouped by object path.

Object: \\fs1\shared\Finance (Permissions: Different from parent)

Account	Permissions	Means Granted
ENTERPRISE\A.Kowalski	Full Control	Group
ENTERPRISE\A.Watson	Full Control	Group
ENTERPRISE\Administrator	Full Control	Group
ENTERPRISE\G.Brown	Full Control	Group
ENTERPRISE\J.Carter	Full Control	Directly
ENTERPRISE\P.Anderson	Full Control	Group
ENTERPRISE\T.Simpson	Full Control	Directly
fs1\Administrator	Full Control	Group

- Identify users with permissions for files and folders that they do not use. Remove those excess permissions to limit the infection area in case of an attack.

Excessive Access Permissions

Shows accounts with permissions for infrequently accessed files and folders.

Object: \\fs1\shared (Permissions: Different from parent)

Account	Permissions	Access Granted	Days Inactive
ENTERPRISE\A.Watson	Full Control	Group	0
ENTERPRISE\Administrator	Full Control	Group	0
ENTERPRISE\B.Atkins	Full Control	Directly	0
ENTERPRISE\D.Galaher	Full Control	Group	0
ENTERPRISE\G.Molls	Write and list folder contents	Directly	0

- Constantly review changes to permissions, including changes to security group membership, to detect and remediate improperly delegated access rights in a timely manner.

Security Groups Membership Changes

Shows changes to members of security groups, and affected parent groups.

Group name: \com\enterprise\Managers\Managers

Action	Member	Who	When
Added Where:	enterprise.com/Managers/Henry Smith dc1.enterprise.com	ENTERPRISE\ J.Carter	1/11/2016 4:17:22 AM
Removed Where:	enterprise.com/Inactive Users/Charles Hoffman dc1.enterprise.com	ENTERPRISE\ J.Carter	8/17/2015 6:57:32 PM

Group name: \com\enterprise\Production\Production

Action	Member	Who	When
Added Where:	enterprise.com/Inactive Users/Nick Key dc1.enterprise.com	ENTERPRISE\ J.Carter	5/30/2016 4:15:14 PM

5.2 Control What Applications Can Run in Your Environment

- Monitor changes to Group Policy, including Software Restriction Policy settings, to ensure your application whitelists are not modified improperly.

Software Restriction Policies Changes

Shows changes to the Software Restriction Policies settings.

Action	What	Who	When
Modified	Software Restriction Policy	ENTERPRISE\J.Carter	6/30/2016 3:18:28 PM
Where:	dc1. enterprise.com		
Path:	Computer Configuration (Enabled)/Policies/Windows Settings/Security Settings/ Software Restriction Policies/ Designated File Types/ADE		
Removed	File Extension: BAT; File Type: Windows Batch File;		
Removed	File Extension: EXE; File Type: Application;		

- Review all changes to the Windows registry startup keys, paying particular attention to the Run key settings. If ransomware has already changed these settings, Netwrix Auditor will show you the path to its execution file, facilitating the removal and remediation process.

Search WHO ACTION WHAT WHEN WHERE

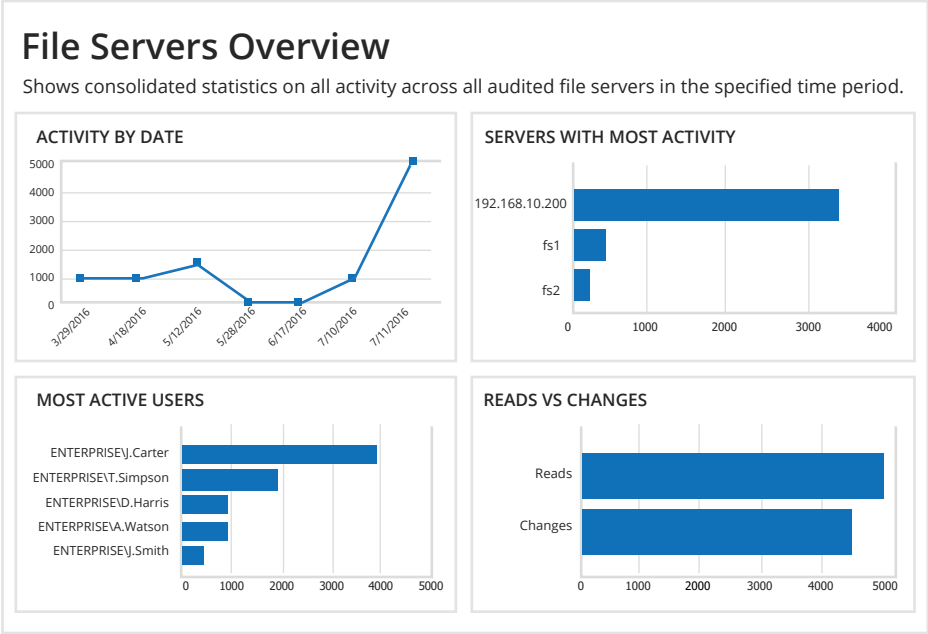
When "Today" | Object Type "Registry Key" | Audited system "Windows Server" | SEARCH

Who	Object type	Action	What	Where	When
ENTERPRISE\ J.Carter	Registry Key	Modified	Registry\HKEY_LOCAL_ MACHINE \software\ Wow6432Node \Microsoft\Windows \CurrentVersion\Run	ws1. enterprise.com	1/28/2016 3:48:53 PM

Added Umbrecrypt (REG_SZ): C:\Windows\Umbercrypt.exe

5.3 Detect an Attack in Process and Determine Which User Account Is Spreading the Crypto-Ransomware

- Detect abnormal spikes in user activity on your file servers and quickly drill down into details to gain more insight.



- Subscribe to threshold-based reports on user activity to be notified whenever a user exhibits behavior that matches a known crypto-ransomware pattern, such as modifying a large number of files in a short time.

User Activity Summary

Shows the most active users. Use this report to detect suspicious user activity such as high numbers of failed access attempts or file reads.

Who	Changes	Reads	Failed Attempts	Deletions
ENTERPRISE\J.Carter	1502	1502	867	1490
ENTERPRISE\MEA_FS	0	0	56	0
ENTERPRISE\T.Simpson	38	9	3	3
NT AUTHORITY\SYSTEM	0	2	0	0
system	9	0	0	0

- Enable additional early warnings about activity that fits ransomware patterns by integrating Netwrix Auditor with your existing SIEM solution.

5.4 Optimize the Data Recovery Process

- Get a complete list of files and folders that were deleted by the infected user account and restore them granularly from backup instead of having to restore all file servers.

Files and Folders Deleted

Shows removed files and folders with their attributes.

Action	Object Type	What	Who	When
Removed Where:	File fs1	\\fs1\shared\Finance2016\bills.rtf	ENTERPRISE\J.Carter	7/18/2016 5:02:02 PM
Removed Where:	File fs1	\\fs1\shared\Finance2016\cache_11_10_15.rtf	ENTERPRISE\J.Carter	7/18/2016 5:02:03 PM
Removed Where:	File fs1	\\fs1\shared\Finance2016\Budget.xlsx	ENTERPRISE\J.Carter	7/18/2016 5:02:04 PM
Removed Where:	File fs1	\\fs1\shared\Human Resources\users.csv	ENTERPRISE\J.Carter	7/18/2016 5:02:05 PM

6. About Netwrix Auditor

Netwrix Auditor is a visibility and governance platform that enables control over changes, configurations and access in hybrid cloud IT environments to protect unstructured data regardless of its location. The platform provides security analytics to detect anomalies in user behavior and investigate threat patterns before a data breach occurs.

Netwrix Auditor includes applications for Active Directory, Exchange, Office 365, Windows file servers, EMC storage devices, NetApp filer appliances, SharePoint, SQL Server, VMware and Windows Server. Empowered with a RESTful API and user activity video recording, the platform delivers visibility and control across all of your on-premises and cloud-based IT systems in a unified way.

More than 150,000 IT departments worldwide rely on Netwrix Auditor to detect insider threats on premises and in the cloud, pass compliance audits with less expense, and increase the productivity of IT security and operations teams. The product has earned over 90 awards from leading industry publications, including SC Magazine, Windows IT Pro, Redmond Magazine and WindowSecurity.com.

On-Premises Deployment

Download a
free 20-day trial

netwrix.com/go/freetrial

Virtual Appliance

Download
our virtual machine image

netwrix.com/go/appliance

Cloud Deployment

Deploy Netwrix Auditor
in the Cloud

netwrix.com/go/cloud

7. About Netwrix Corporation

Netwrix Corporation was first to introduce visibility and governance platform for on-premises, hybrid and cloud IT environments. Founded in 2006, Netwrix has earned more than 90 industry awards and been named to both the Inc. 5000 and Deloitte Technology Fast 500 lists of the fastest growing companies in the U.S.

For more information, visit www.netwrix.com

Corporate Headquarters:
300 Spectrum Center Drive, Suite 1100, Irvine, CA 92618
Phone: 1-949-407-5125 **Toll-free:** 888-638-9749 **EMEA:** +44 (0) 203-588-3023
netwrix.com/social