Office of the NEW YORK STATE
COMPTROLLER

Local Government Management Guide
Ransomware

New York State Comptroller
THOMAS P. DiNAPOLI

OCTOBER 2019

Table of Contents

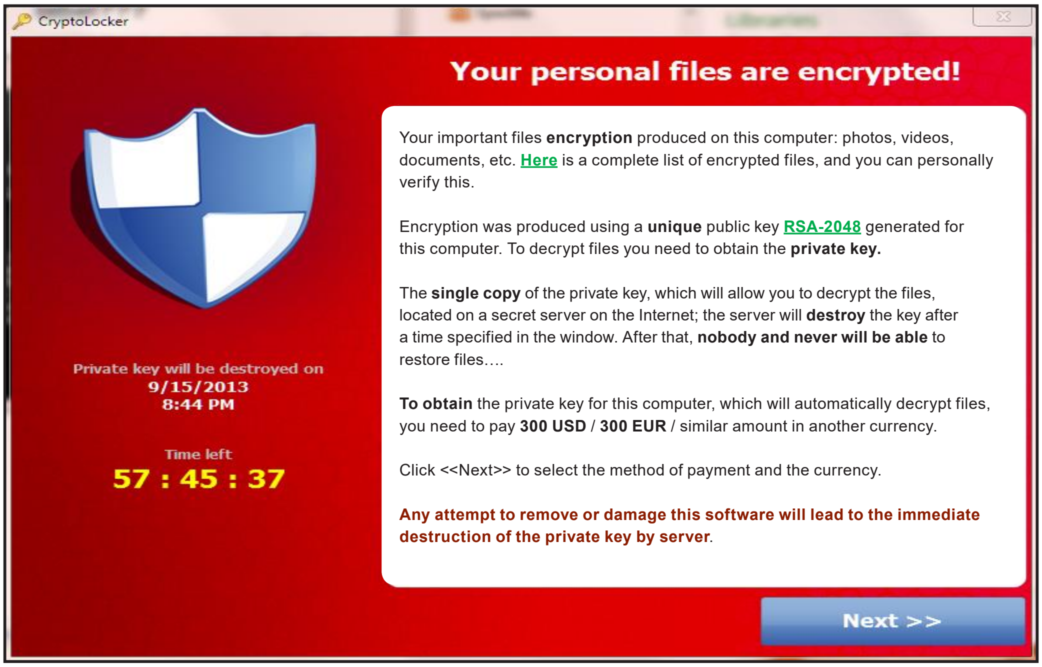
Ransomware

Imagine being locked out of your computer because it has been infected with malware, or having data and records deleted or stolen and then being contacted by someone demanding a fee or fine (ransom) to regain access to the computer system and data.

Malicious software, or malware, refers to software programs that are designed to harm computer systems. These programs can wreak havoc on both systems and electronic data by, for example, deleting files, gathering sensitive information such as passwords without the computer user's knowledge and making systems inoperable. Computer users can inadvertently install malware on their computers by many methods, including opening email attachments, downloading content from the Internet or merely visiting infected websites.

Ransomware is a unique type of malware that prevents access to a user's computer or electronic data. Criminals create links and websites that install ransomware on the computers of unsuspecting users and then display messages demanding payment in exchange for restoring the computer to its functioning state. The message may even falsely claim to originate from a law enforcement agency and demand that the recipient pay a fine to avoid prosecution for illegal activity (e.g., using unauthorized software, downloading illegal content from the Internet) detected on the computer and regain access to the system or files. A typical ransomware demand may appear in the form shown in Figure 1.[1]

Figure 1. **Typical Ransomware Demand**



Your personal files are encrypted!

Private key will be destroyed on
9/15/2013
8:44 PM

Time left
57 : 45 : 37

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in the window. After that, **nobody and never will be able** to restore files….

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD** / **300 EUR** / similar amount in another currency.

Click <<Next>> to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Criminals have used ransomware to target home computers, financial institutions, government agencies, academic institutions and other organizations. Instances of ransomware are increasingly affecting users worldwide and are unlikely to subside anytime soon, as they generate a significant amount of revenue for cybercriminals.

New York State Technology Law (State Technology Law) requires municipalities and other local agencies to have a breach notification policy or local law.[2] Such policy or local law must require that notification be given to certain individuals when there is a breach of the security of the system as it relates to private information.

Instances of ransomware are increasingly affecting users worldwide and are unlikely to subside anytime soon, as they generate a significant amount of revenue for cybercriminals.

While New York State Information Security Policy requires State government entities to notify the Cyber Incident Response Team (CIRT) of any cyber incident which may have a significant or severe impact on operations or security, or which involves digital forensics, to ensure proper incident response procedures, coordination and oversight,[3] there currently is no similar type of requirement or mechanism for cyber incidents involving local governments. Such a requirement could help increase awareness of cyber incidents among local governments and standardize responses.

Proper information technology (IT) security and preparation can reduce the risk of a local government becoming a victim of ransomware and data breaches. Appropriate measures include restricting user access, including administrative privileges;[4] applying software patches and updates in a timely manner; installing and keeping antivirus protection up-to-date; providing IT security training to all employees; implementing and enforcing an acceptable-use policy; and maintaining offline backup copies of all critical data.

Ransom Demands

Before paying a ransom demand:

- Contact cyber security experts, who can help determine the best way to proceed and may be able to lend free technical expertise necessary to investigate and resolve the problem. A few organizations that investigate and provide this guidance include:
    - Center for Internet Security's (CIS) Multi-State Information Sharing & Analysis Center (**https://www.cisecurity.org/ms-isac/**);
    - New York State Office of Information Technology Services (**http://www.its.ny.gov/incident-reporting**); and
    - Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) (**us-cert.gov/ics**).
- Consult insurance providers. Depending on the nature of the incident and the type of insurance coverage the entity has, officials should consider contacting their insurance provider to report the incident.
- Consult legal counsel. Individuals and organizations that demand ransoms for the safe return of the functionality of computer systems are breaking the law. Their attempts to extort money should be discussed with the entity's legal counsel who can assist with reporting the incident to law enforcement. In addition, depending on the nature of the incident, there may be breach notification requirements. Legal counsel can assist in determining if the incident has triggered the notification requirements and in complying with those requirements, as necessary.

A local government or school district may ultimately have to pay money to regain access to its computer system and data, but should do so only after obtaining technical assistance and advice from experts.

> Legal counsel can assist in determining if the incident has triggered the notification requirements and in complying with those requirements, as necessary.

Best Practices

Policies and procedures that can help to reduce the chances of being a victim of ransomware, or help you understand what happened and restore systems if an incident occurs, include the following:

- Restrict user access, including administrative privileges, based on jobs, tasks and assignments, to limit the extent of damage ransomware could cause.

- Apply software patches and updates in a timely manner to minimize vulnerabilities that could be used to infect computers with ransomware.

- Install and keep antivirus protection up-to-date to detect known ransomware.

- Provide employees with cybersecurity training to help them recognize problems before they occur.

- Maintain offline, offsite backups of applications and data to ensure successful recovery from a ransomware attack.

- Enable and review audit logs to determine how a ransomware attack occurred and whether private information was breached.

- Adopt a breach notification policy or local law consistent with State Technology Law requirements to ensure individuals are properly notified if their private information is breached.

- Adopt a disaster recovery plan that includes procedures and information to aid in effectively responding to and recovering from ransomwareand other events that impair or potentially impair IT security; test the recovery plan periodically.

> Restrict user access, including administrative privileges, based on jobs, tasks and assignments, to limit the extent of damage ransomware could cause.

Notes

[1] From the Federal Bureau of Investigation's Internet Crime Complaint Center at **http://www.ic3.gov/media/2013/131028.aspx**.

[2] Section 208 (8) of the State Technology Law requires municipalities and other local agencies to have adopted a breach notification policy or local law consistent with the requirements contained in Section 208 by April 6, 2006. Pursuant to Section 208, notification is required to be given to certain individuals when there is a "breach of the security of the system" as it relates to "private information." "Breach of the security of the system" is generally defined as meaning unauthorized acquisition of computer data which compromises the security, confidentiality, or integrity of personal information maintained by the entity. "Private information" is defined as personal information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired: (1) Social Security number; (2) driver's license number or non-driver identification card number; or (3) account number, credit or debit card number, in combination with any required security code, access code, or password which would permit access to an individual's financial account.

[3] See New York State Office of Information Technology Services at **https://www.its.ny.gov/incident-reporting**.

[4] Administrative privileges allow users to access all data on a system, including data created and stored by other users; make changes to the settings configured on the system, including disabling antivirus software; create new user accounts; or change the levels of privileges granted to existing user accounts.

Contacts

Office of the NEW YORK STATE

COMPTROLLER

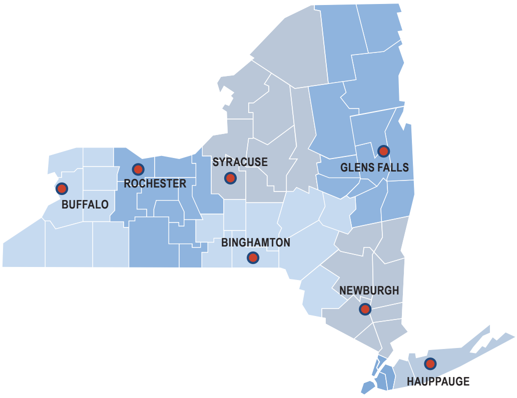
New York State Comptroller

THOMAS P. DiNAPOLI

Division of Local Government and School Accountability

110 State Street, 12th floor, Albany, NY 12236
Tel: 518.474.4037 • Fax: 518.486.6479
Email: localgov@osc.ny.gov

www.osc.state.ny.us/localgov



Executive • 518.474.4037
Elliott Auerbach, Deputy Comptroller
Tracey Hitchen Boyd, Assistant Comptroller
Randy Partridge, Assistant Comptroller

Audits, Local Government Services and Professional Standards • 518.474.5404
(Audits, Technical Assistance, Accounting and Audit Standards)

Local Government and School Accountability Help Line • 866.321.8503 or 518.408.4934
(Electronic Filing, Financial Reporting, Justice Courts, Training)

Division of Legal Services

Municipal Law Section • 518.474.5586

New York State & Local Retirement System

Retirement Information Services
Inquiries on Employee Benefits and Programs
518.474.7736

Technical Assistance is available at any of our Regional Offices

BINGHAMTON REGIONAL OFFICE
Tel 607.721.8306 • **Fax** 607.721.8313 • **Email** Muni-Binghamton@osc.ny.gov
Counties: Broome, Chenango, Cortland, Delaware, Otsego, Schoharie, Sullivan, Tioga, Tompkins

BUFFALO REGIONAL OFFICE
Tel 716.847.3647 • **Fax** 716.847.3643 • **Email** Muni-Buffalo@osc.ny.gov
Counties: Allegany, Cattaraugus, Chautauqua, Erie, Genesee, Niagara, Orleans, Wyoming

GLENS FALLS REGIONAL OFFICE
Tel 518.793.0057 • **Fax** 518.793.5797 • **Email** Muni-GlensFalls@osc.ny.gov
Counties: Albany, Clinton, Essex, Franklin, Fulton, Hamilton, Montgomery, Rensselaer, Saratoga, Schenectady, Warren, Washington

HAUPPAUGE REGIONAL OFFICE
Tel 631.952.6534 • **Fax** 631.952.6091 • **Email** Muni-Hauppauge@osc.ny.gov
Counties: Nassau, Suffolk

NEWBURGH REGIONAL OFFICE
Tel 845.567.0858 • **Fax** 845.567.0080 • **Email** Muni-Newburgh@osc.ny.gov
Counties: Columbia, Dutchess, Greene, Orange, Putnam, Rockland, Ulster, Westchester

ROCHESTER REGIONAL OFFICE
Tel 585.454.2460 • **Fax** 585.454.3545 • **Email** Muni-Rochester@osc.ny.gov
Counties: Cayuga, Chemung, Livingston, Monroe, Ontario, Schuyler, Seneca, Steuben, Wayne, Yates

SYRACUSE REGIONAL OFFICE
Tel 315.428.4192 • **Fax** 315.426.2119 • **Email** Muni-Syracuse@osc.ny.gov
Counties: Herkimer, Jefferson, Lewis, Madison, Oneida, Onondaga, Oswego, St. Lawrence

STATEWIDE AUDIT
Tel 315.793.2484

Contact

Office of the New York State Comptroller
Division of Local Government and School Accountability

110 State Street, 12th floor
Albany, NY 12236
Tel: (518) 474-4037
Fax: (518) 486-6479
or email us: localgov@osc.ny.gov

www.osc.state.ny.us/localgov/index.htm

Like us on Facebook at facebook.com/nyscomptroller
Follow us on Twitter @nyscomptroller

Released October 2015

Updated October 2019