Combating RANSOMWARE:

Practice, Strategies and Defenses

Ransomware is a threat to Netizens, one that has become increasingly popular with criminals in the recent past. Combating this challenge requires not only the development of new technologies but also good Internet practices on the part of the users.

RAVI VIJAYVARGIYA
Sr. Technical Director
ravi.vijay@nic.in

C. SREENIVASA RAO
Technical Director
csr@nic.in

K.B. HARIHARAN
Scientist-D
kbh@nic.in

Edited by
MOHAN DAS VISWAM

Ransomware is a type of malware that can be covertly installed on a computer without the knowledge or intention of the user and restricts access to the infected computer system in some way. True to its name, it then demands that the user pays a ransom to the malware operators to remove the restriction.

User awareness about this type of infection and its ill effects will greatly help in minimizing threat to digital assets. This article deals with the characteristics of Ransomware malware, its effects, propagation methods and measures to be taken to prevent a Ransomware infection.

UNDERSTANDING RANSOMWARE

Ransomware is different from the typical forms of malware. Most malwares work in the background and rarely make their presence felt, even to sophisticated antivirus software. However, Ransomware makes it presence known openly in order to intimidate the users. It prevents or limits users from accessing their system. This type of malware forces its victims to pay the ransom through certain online payment methods in order to grant access to their systems or to get their data back.

Cybercriminals are now using the most modern cryptography to encrypt stolen files and have gotten increasingly better at making their dangerous links and downloads seem perfectly benign.

For example, a hacker might pose as your service company in an email stating that they need you to fill out an attached form or else your service will be cut off/stopped. Or a hacker might even use social engineering to pose as someone in your contact list to get you to click on a link in an email. Once you click the link or visit the malicious website, the files are installed on your system under the radar, without you being any wiser.

It's worth adding that Ransomware's communication protocols have been upgraded from plain text (HTTP) to Tor and HTTPS, making encrypted calls to C&C servers almost impossible to track through network traffic monitoring. File encryption has also been revamped to use crypto-libraries that perform strong, asymmetric cryptography rather than using

Unwitting users get Ransomware unknowingly downloaded on their system by visiting malicious or compromised websites. It can also arrive as a payload, either dropped or downloaded by other malware. Some Ransomware is delivered as attachments to spammed email.

short-length keys or hard-coded ones. Earlier samples such as Cryptolocker, Cerber3 and Cryptowall first contacted the server and perform encryption afterwards.

Ransomware is a very challenging threat for both users and anti-malware companies, as it boasts of impressive capabilities and an unprecedented success rate in extorting money from its victims.

The ransom prices vary, ranging from $USD 24 to more than $USD 600, or its bitcoin equivalent. It is important to note, however, that paying the ransom does not guarantee that users can eventually access the infected system. There is no guarantee that the victim will get their data back, or that the attacker will not leave other forms of malware running on the system. Cyber criminals will return to someone who paid, so payment to recover your files simply confirms that you will be a good target for future attacks and scams.

Users may encounter this threat through a variety of means. Unwitting users get Ransomware unknowingly downloaded on their system by visiting malicious or compromised websites. It can also arrive as a payload, either dropped or downloaded by other malware. Some Ransomware is delivered as attachments to spammed email.

Once executed in the system, a Ransomware can either (a) lock the computer screen or (b) encrypt predetermined files with a password. In the first scenario, a Ransomware shows a full-screen image or notification, which prevents victims from using their system. This also shows the instructions on how users can pay for the ransom. The second type of Ransomware locks files like documents, spreadsheets and other important files.

Most Ransomware campaigns begin with a phishing attack. Over time, they have become more sophisticated, many now specifically and meticulously crafted to the locale of victims that are being targeted.

DEVELOPMENTS IN RASOMWARE TECHNOLOGIES

VIRTUAL CURRENCY:

Virtual currency is anonymous, at least until it is exchanged for conventional money. Bitcoinhas fuelled a surge in the number of cyber attacks where computers and personal data are held hostage in return for ransoms paid in the almost-anonymous virtual currency.
Cyber attackers prefer to demand ransoms in Bitcoin because it is much harder to trace than credit card payments in conventional currencies. Using Bitcoin is the online equivalent of leaving a suitcase full of cash in a park.

TOR NETWORK:

By using the Tor network, attackers can more easily hide the location of their control servers, which store the victims' private keys. Tor makes it possible to maintain the criminal infrastructure for a long time and to even rent the infrastructure to other attackers so they can run affiliate campaigns.

TARGETING MASS-STORAGE DEVICES:

In August 2014, some Ransomware began targeting network attached storage (NAS) disk and rack stations. The malware exploits vulnerabilities in unpatched versions of the NAS servers to remotely encrypt all data on the servers using both RSA 2,048-bit keys and 256-bit keys.
Most malware execute with the same privileges as the victim executing the payload. If the person getting compromised has administrative privileges, the malicious code will have access to the same resources.

Some of the Anti-Virus software gives limited protection from the infection of Ransomware by limiting access to malicious websites hosting Ransomware variants, and blocks IP addresses and C&C servers that Ransomware variants access. Some of the solutions also block mails that carry Ransomware.

PROPAGATION PREVENTIONS

A common vector to introduce these threats into office environments is via spam emails with attachments. They appear from legitimate sources and encourage users to click on them.
The following configurations can help provide another layer of defense:

- **Block double extension attachments:** Configure email service to block mail attachments with double extensions.
- **File Filtering:** Configure mail service to block files with the file extensions like .SCR, .EXE and .CAB files reaching user's desktops.
- **Check the content** of the mail messages you receive and send. The mail attachments have become a very common

Screen of Cryptolocker Ransomware

Tips to prevent Ransomware infections

- **Backup your files regularly.**
- **Apply software patches as soon as they become available. Some Ransomware arrives via vulnerability exploits.**
- **Bookmark trusted websites and access these websites via bookmarks.**
- **Download email attachments only from trusted sources. Do not open emails or attachments from unverified or unknown senders.**
- **Many system vulnerabilities commonly abused by Ransomware can be patched. To minimize the Ransomware infection, it is utmost necessary to patch Operating Systems, and most commonly used applications like browsers, Java, Adobe Reader, Flash and other applications.**
- **Enable pop-up blockers on browsers.**
- **Scan your system regularly with anti-malware.**

The only method which saves you after infection from the loss of data is Backup. Maintaining regular backup minimizes the loss of files and documents.

method for propagating malware. For this reason, practices like checking the sender of a message, taking care withoffers that sound just too tempting to resist, checking that it is really an email that has been sent, and not clicking on suspicious links are basic measures to take in order to avoid falling victim to tricks that might result in infection.

- **The antivirus solution** will prevent the malicious code from executing itselfto infect your system—provided it's updated regularly and configured with the correct settings.
- **Updating your software** is essential for preventing more infections. If you have antivirus software, it's important for the virus signatures to be up to date and for its settings to be configured correctly, so that this type of threat is detected and blocked—and in a timely manner so they can't take advantage of security flaws.

So, by combining the use of good security practices and a security solution to protect you from malware, as well as staying aware of these risks and the ways to protect yourself, it is possible to minimize security events involving information and new threats. These attacks, despite becoming increasingly sophisticated, continue to use known methods of propagation.

The best way to keep your files protected from Ransomware is through strong endpoint security. One should create backups of all important data, and ensure that those backups are blocked off by a partition, so they can't be encrypted by malware. You should also take an extra step and encrypt the backup files themselves. Continuous endpoint monitoring can also help to spot Ransomware before it can do any damage. Also, an application control that allows only the known application to run plays a major role to protect your valuable data.

SUMMARY

Ransomware can be a devastating attack on your system, locking you out of your files and data. The easiest way to protect yourself from such malicious attacks is to not allow the files to get to your system in the first place. Observing safe practices while surfing the Internet and downloading files and maintaining a baseline of security measures can ward off such attacks without much effort.

For further information, please contact:

RAVI VIJAYVARGIYA
Sr. Technical Director
HoD, Network Security Division
NIC HQ, Lodhi Road, New Delhi 110 003
Email: ravi.vijay@nic.in
Phone: 011-24305122