Computer Security

07r. Assignment 6 review

Paul Krzyzanowski • David Domingo • Ananya Jana

Rutgers University

Spring 2019

Assignment 6 Review: malware

Question 1

What is the primary disadvantage of signature-based malware detection?

From Morton Christiansen, *Bypassing Malware Defenses*, SANS Institute Information Security Reading Room, May 7, 2010.

"The disadvantage with this approach is its ineffectiveness in detecting new variants of an old piece of malware."

Malware researchers & anti-malware companies collect examples of known malware. It would be too cumbersome to download and match

A "signature" is a set of bytes in the malware that we think are unique to a particular piece of malware: if we see them then we're pretty sure it's dangerous code. It's far more efficient (and safer) than having a version of every known piece of malware in your system.

The problem is that if someone creates new code, it will not match other signatures.

Question 2

What are three techniques that malware packers use?

1. **XORing the malware**
   - This is an example of a simple stream cipher. The key determines which bits get flipped.
2. **Compression of malware**
   - Compression removes information redundancy and, in the process, obscures the content.
3. **Encryption of malware**
   - Encryption changes the content.

From the paper:

"Packers may be used to pack an executable using techniques ranging from simple XORing of the malware to compression and even encryption hereof. The malware is then unpacked during runtime."

Question 3

How does the use of packers make it more difficult to detect malware?

A packer changes the representation of the malware code. This usually results in anti-virus software being unable to detect it.

1. ***XORing the malware***
   - The key determines which bits get flipped. Unless you decode the content, you cannot search for a signature.
2. ***Compression of malware***
   - You cannot search for a specific bit pattern unless you decompress the data … or have signatures for the output of any of several dozen common compression algorithms.
3. ***Encryption of malware***
   - You cannot scan for a signature unless you know the key and can decrypt it. The key is typically somewhere in the unpacking code (or may be downloaded from the network).

The best you can do is detect the presence of an unpacker

Question 4

What technique does the author discuss as a possible mechanism for malware to communicate with a server if it has no direct access to the Internet?

Use a DNS query (to the local DNS resolver) that will contact the adversary's DNS server and return encoded commands instead of legitimate addresses.

The malware can do a domain name lookup (e.g., look up *secret.pk.org*).

The DNS server within the organization will make a series of requests over the Internet, ultimately contacting the name server in charge of *pk.org*, which is run by the adversary

The adversary can return any encoded data – it doesn't have to be a valid IP address.

The malware can query any domain – it doesn't have to be a valid system (e.g., *here_is_my_response.pk.org*).

Question 5a

Anti-malware software and file filters need to be aware of potentially harmful files that can host or conceal malware.

(a) How many forms of compression formats does the paper list?

25

7-zip, ace, ARJ, bzip, bzip2, cabinet, gzip, disk image, ISO-9660 CD image, LHA archive, LZH archive, RAR split archive, RAR archive, RAR recovery volume, tar, tar-zip, tar-bzip, tar-bzip2, tar-gzip, uuencode (2 forms), xx-encode, UNIX compression, zip split compression, zip compression.

This shows that it's not trivial to just decompress a file while scanning for malware or search for a signature within a compressed file.

Question 5b

Anti-malware software and file filters need to be aware of potentially harmful files that can host or conceal malware.

(b) How many types of Microsoft Office related file types does the paper list?

41

csv, doc, docm, docx, dot, dotm, …xltm, xltx, xlw

Microsoft office files can carry malicious scripts, embed malicious executables, or have links to malicious sites.

They are commonly used and shared as part of normal business operations in many (most) companies, so people expect to receive them.

Question 6a,b

Watch/listen to the interview with Amit Serper on OSX.Pirrit malware/adware.

(a) How does the macOS **LaunchAgent** mechanism help malware?

It enables it to be started whenever a system boots up.

(b) List two ways in which users end up using to get Pirrit onto their systems.

Three mechanisms are presented:

1. **Custom installers**: File download sites create their own installers that install legitimate software plus the malware.
2. **Cracks**: Torrent files for cracks often contain malware instead of the crack.
3. **Misleading download links**: Ads on file download sites can disguise themselves as download links and will serve the malware.

The end