## Welcome Subscribers!

As you are all aware about the facts regarding the ransomware attacks are increasing rapidly from past few years. Consider the biggest hits till now, you will come across with well known name i.e.

- 1. CryptXXX
- 2. Dogspectus
- 3. Crypto Locker
- 4. Petya
- 5. Cerber
- 6. Locky

Now we have WCry/WannaCry and Uiwix .... Still to go!



# **Executive Summary**

Organizations affected across the world with the ransomware variant based malware known as "WCry/WannaCry". Major Ransomware attack of its kind named "CryptoWorm". Capability to scan & spread based on vulnerabilities (TCP port 445-SMB), dispersal as worm, compromise vulnerable hosts, encrypting files stored on. The worst part it's also deletes shadow copies by using vssadmin.exe, WMIC.exe & cmd.exe (if any on the victim's host so that will make difficult recovery model).

Note: Based on NSA's Leaked Exploits by Shadow Broker specifically related with SMB services for Windows.



For initial exploitation of SMB vulnerability, it primarily utilizes "ETERNALBLUE". Implantation of "DOUBLEPULSAR" backdoor happened on successful exploitation of victim's machine for further utilization in malware installation. What If the "DOUBLEPULSAR" backdoor is already present then it has the power to install ransomware payload which make WCry or WannaCry as "CryptoWorm".

# **Analysis**

Let's start with the psychiatry based on little machinery like execution \*&\* encryption flow of this ransomware.

# **Encryption Based Analysis**

WCry / WannaCry used two encryption algorithms for ransomware infection. Below are the details:

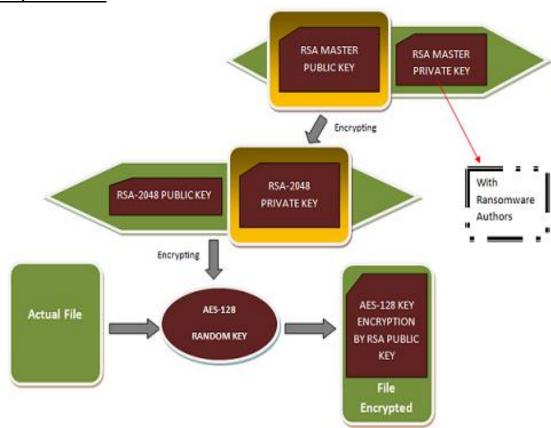
- ✓ AES (Advanced Encryption Standard)
- ✓ RSA (Ron Rivest, Adi Shamir and Leonard Adleman)

AES considered to be the well-built ciphers & would not be able to decrypt until or unless author make a mistake in the encryption code. Whereas RSA is also in combination with AES for unique public & private keys generation specifically for each file.

## Steps for encryption by WCRY / WannaCry are;

- I. Each file is encrypted by Random AES-128 Key.
- II. The key is further encrypted by RSA-2048 public key, and stored in **0000000.py** file.
- III. Private RSA key of the above public RSA key is further encrypted by RSA Master public key.
- IV. The private RSA key of the RSA Master public key is known only by the "Ransomware Authors".

# **Graphical presentation**



#### **Targeted files**;

```
.der, .pfx, .key, .crt, .csr, .p12, .pem, .odt, .sxw, .stw, .3ds,
.max, .3dm, .ods, .sxc, .stc, .dif, .slk, .wb2, .odp, .sxd, .std,
.sxm, .sqlite3, .sqlitedb, .sql, .accdb, .mdb, .dbf, .odb, .mdf,
.ldf, .cpp, .pas, .asm, .cmd, .bat, .vbs, .sch, .jsp, .php, .asp,
.java, .jar, .class, .mp3, .wav, .swf, .fla, .wmv, .mpg, .vob, .mpeg,
.asf, .avi, .mov, .mp4, .mkv, .flv, .wma, .mid, .m3u, .m4u, .svg,
.psd, .tiff, .tif, .raw, .gif, .png, .bmp, .jpg, .jpeg, .iso,
.backup, .zip, .rar, .tgz, .tar, .bak, .ARC, .vmdk, .vdi, .sldm,
.sldx, .sti, .sxi, .dwg, .pdf, .wk1, .wks, .rtf, .csv, .txt, .msg,
.pst, .ppsx, .ppsm, .pps, .pot, .pptm, .pptx, .ppt, .xltm, .xltx,
.xlc, .xlm, .xlt, .xlw, .xlsb, .xlsm, .xlsx, .xls, .dotm, .dot,
.docm, .docx, .doc,
```

# Fishy Security - Lab

# **Execution Based Analysis**

It begins with an initial bonfire or a killswitch (High level view as reported other researchers too), now execution begins when user downloads the attachments having (.js, .exe). In some circumstances they are also related with malicious macros which can be activated when user enables the content on a document.

#### Steps for encryption by WCRY / WannaCry are;

- I. Exploit ETERNALBLUE & spread to other hosts.
- II. Damaging process starts with laying foundation for.
- III. Starts encrypting files with above mentioned algorithms in combination with RSA and AES.

## **Graphical presentation**

