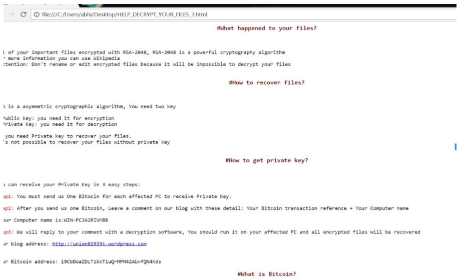
Technical Analysis of Samsam Ransomware.

by Abhishek Singh | Jan 24, 2018 | Blog |



file:///C:/Users/abhi/Desktop/HELP_DECRYPT_YOUR_FILES_3.html

```
#What happened to your files?

l of your important files encrypted with RSA-2048, RSA-2048 is a powerful cryptography algorithm
· more information you can use Wikipedia
:tention: Don't rename or edit encrypted files because it will be impossible to decrypt your files

#How to recover files?

A is a asymmetric cryptographic algorithm, You need two key

Public key: you need it for encryption
Private Key: you need it for decryption

 you need Private key to recover your files.
's not possible to recover your files without private key

#How to get private key?

u can receive your Private Key in 3 easy steps:

ep1: You must send us One Bitocin for each affected PC to receive Private Key.

ep2: After you send us one Bitcoin, Leave a comment on our blog with these detail: Your Bitcoin transaction reference + Your Computer name

our Computer name is:WIN-PC3A2RIVMBB

ep3: We will reply to your comment with a decryption software, You should run it on your affected PC and all encrypted files will be recovered

ur blog address: http://union83939k.wordpress.com

ur Bitcoin address: 19CbDoaZDLTzkkT1uQrMPM42AUvfQN4Kds

#What is Bitcoin?
```

Ransomware continues to represent the most critical threat facing organizations in 2018. In the latest breaches at Hancock Memorial Hospital, Adams Memorial Hospital, and Allscripts, SamSam ransomware was used to encrypt the files. In this blog, we dive into the technical details of the SamSam ransomware [1]. The blog then shares how the Samsam ransomware can be detected using a deception-based architecture.

Technical Details:

For the Samsam ransomware to execute, it will require input text file as the command line argument. The input text file will have the base64 encoded public keys in the XML format shown in figure 1.0

Search

Recent Posts

MarketWatch – This 18-Year-Old's Hacking Side Hustle Has Earned Him $100,000 — And It's Legal

BrightTALK – TAG-Cyber's Ed Amoroso Interviews Acalvio

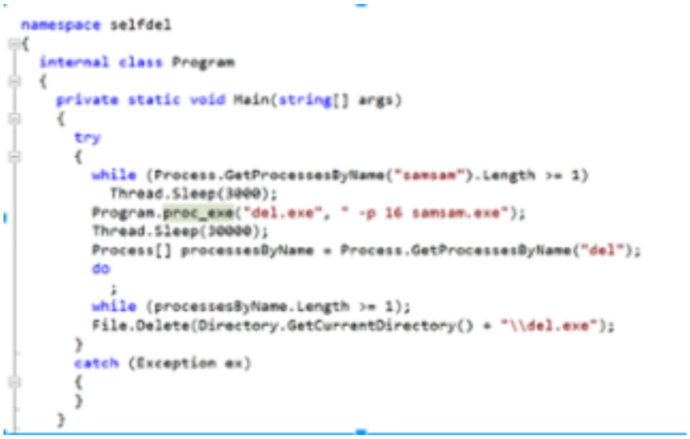
3 Minutes Until the Apocalypse – Technical White Paper

TAG Cyber Interview of Acalvio's John

<RSAKeyValue><Modulus>1wxu6kDpEJdGZiDDz9jgZAZaE22oaNbHcC1nLA3gsBj8YgHABpHh2clJElWfR4xl221gDSdapo
zmqEhM7HMLQJGO29p3QPTjLdbeeUhXpz8Qha8Bms/scyrdmj187lL6wOrg+jyQ6jjN+SWMPW6sxspKUkJm8xenLolZy
+rW3eAB8AtL7JRYosRx54kVOqksUIf9jcujwjgsJpg9xeNWueLQlKJyBLNuB1TssrbeinPkGtM6lt1nH0ct/ZfCWGudiryIknU
rpUqYJXOV0v3ii9GuV9hiirkUayY2GtqEAGKjN1oaGK188qvP9BcazxUTwNpHRHbGG2kP++06jXiARQ==</Modulus><E
xponent>AQAB</Exponent></RSAKeyValue>

Figure 1.0 Example RSA key in the format accepted by the Samsam ransomware.

When the ransomware code is executed, it drops two files selfdel.exe and del.exe. Selfdel.exe and del.exe are in the resource section of the ransomware file. The dropped file selfdel.exe as shown in figure 2.0 will get the process name Samsam, and sleep for 3000 milliseconds, after which it will delete the Samsam ransomware process.



```
namespace selfdel
{
  internal class Program
  {
    private static void Main(string[] args)
    {
      try
      {
        while (Process.GetProcessesByName("samsam").Length >= 1)
          Thread.Sleep(3000);
        Program.proc_exe("del.exe", " -p 16 samsam.exe");
        Thread.Sleep(30000);
        Process[] processesByName = Process.GetProcessesByName("del");
        do
          ;
        while (processesByName.Length >= 1);
        File.Delete(Directory.GetCurrentDirectory() + "\\del.exe");
      }
      catch (Exception ex)
      {
      }
    }
```

Figure 2.0 code of the selfdel.exe

The ransomware encrypts 328 file extensions.the list of file extensions are shown in figure 3.0 .Since the ransomware encrypts files with extension ".sql", ".sqlite", ".sqlite3", ".sqlitedb" it will encrypt databases.

Bradshaw Security Week – Outdated DoD IT Jeopardizes National Security: Report

Archives

July 2018

June 2018

May 2018

April 2018

March 2018

February 2018

January 2018

December 2017

November 2017

October 2017

September 2017

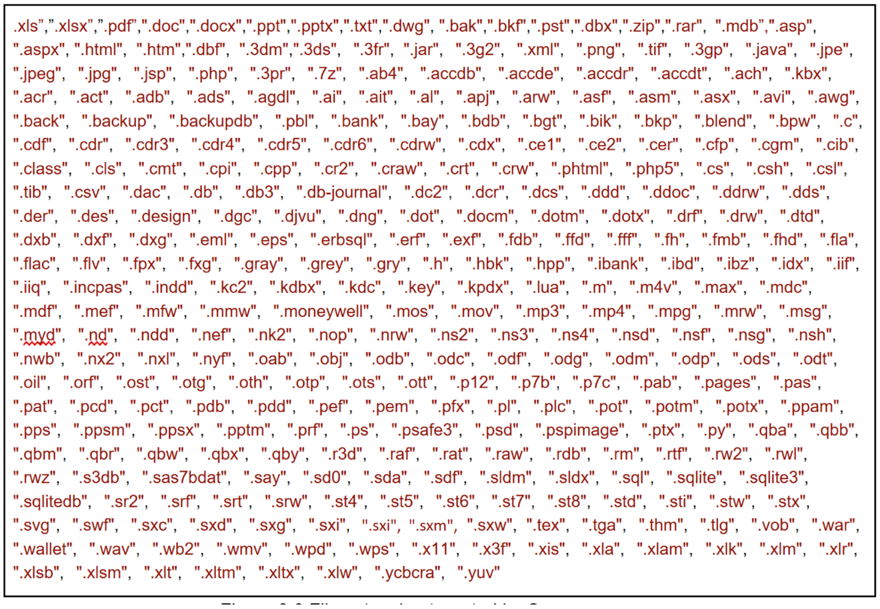
August 2017

July 2017

June 2017

May 2017

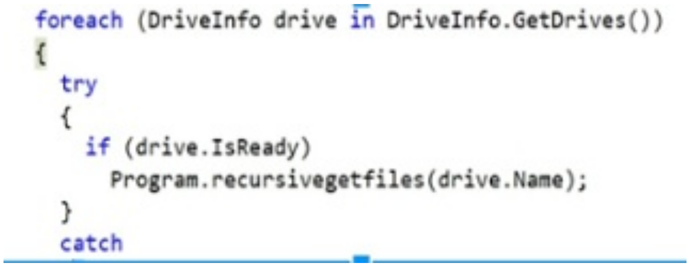
April 2017



```
.xls",".xlsx",".pdf",".doc",".docx",".ppt",".pptx",".txt",".dwg", ".bak",".bkf",".pst",".dbx",".zip",".rar", ".mdb",".asp",
".aspx", ".html", ".htm",".dbf", ".3dm",".3ds", ".3fr", ".jar", ".3g2", ".xml", ".png", ".tif", ".3gp", ".java", ".jpe",
".jpeg", ".jpg", ".jsp", ".php", ".3pr", ".7z", ".ab4", ".accdb", ".accde", ".accdr", ".accdt", ".ach", ".kbx",
".acr", ".act", ".adb", ".ads", ".agdl", ".ai", ".ait", ".al", ".apj", ".arw", ".asf", ".asm", ".asx", ".avi", ".awg",
".back", ".backup", ".backupdb", ".pbl", ".bank", ".bay", ".bdb", ".bgt", ".bik", ".bkp", ".blend", ".bpw", ".c",
".cdf", ".cdr", ".cdr3", ".cdr4", ".cdr5", ".cdr6", ".cdrw", ".cdx", ".ce1", ".ce2", ".cer", ".cfp", ".cgm", ".cib",
".class", ".cls", ".cmt", ".cpi", ".cpp", ".cr2", ".craw", ".crt", ".crw", ".phtml", ".php5", ".cs", ".csh", ".csl",
".tib", ".csv", ".dac", ".db", ".db3", ".db-journal", ".dc2", ".dcr", ".dcs", ".ddd", ".ddoc", ".ddrw", ".dds",
".der", ".des", ".design", ".dgc", ".djvu", ".dng", ".dot", ".docm", ".dotm", ".dotx", ".drf", ".drw", ".dtd",
".dxb", ".dxf", ".dxg", ".eml", ".eps", ".erbsql", ".erf", ".exf", ".fdb", ".ffd", ".fff", ".fh", ".fmb", ".fhd", ".fla",
".flac", ".flv", ".fpx", ".fxg", ".gray", ".grey", ".gry", ".h", ".hbk", ".hpp", ".ibank", ".ibd", ".ibz", ".idx", ".iif",
".iiq", ".incpas", ".indd", ".kc2", ".kdbx", ".kdc", ".key", ".kpdx", ".lua", ".m", ".m4v", ".max", ".mdc",
".mdf", ".mef", ".mfw", ".mmw", ".moneywell", ".mos", ".mov", ".mp3", ".mp4", ".mpg", ".mrw", ".msg",
".myd", ".nd", ".ndd", ".nef", ".nk2", ".nop", ".nrw", ".ns2", ".ns3", ".ns4", ".nsd", ".nsf", ".nsg", ".nsh",
".nwb", ".nx2", ".nxl", ".nyf", ".oab", ".obj", ".odb", ".odc", ".odf", ".odg", ".odm", ".odp", ".ods", ".odt",
".oil", ".orf", ".ost", ".otg", ".oth", ".otp", ".ots", ".ott", ".p12", ".p7b", ".p7c", ".pab", ".pages", ".pas",
".pat", ".pcd", ".pct", ".pdb", ".pdd", ".pef", ".pem", ".pfx", ".pl", ".plc", ".pot", ".potm", ".potx", ".ppam",
".pps", ".ppsm", ".ppsx", ".pptm", ".prf", ".ps", ".psafe3", ".psd", ".pspimage", ".ptx", ".py", ".qba", ".qbb",
".qbm", ".qbr", ".qbw", ".qbx", ".qby", ".r3d", ".raf", ".rat", ".raw", ".rdb", ".rm", ".rtf", ".rw2", ".rwl",
".rwz", ".s3db", ".sas7bdat", ".say", ".sd0", ".sda", ".sdf", ".sldm", ".sldx", ".sql", ".sqlite", ".sqlite3",
".sqlitedb", ".sr2", ".srf", ".srt", ".srw", ".st4", ".st5", ".st6", ".st7", ".st8", ".std", ".sti", ".stw", ".stx",
".svg", ".swf", ".sxc", ".sxd", ".sxg", ".sxi", ".sxi", ".sxm", ".sxw", ".tex", ".tga", ".thm", ".tlg", ".vob", ".war",
".wallet", ".wav", ".wb2", ".wmv", ".wpd", ".wps", ".x11", ".x3f", ".xis", ".xla", ".xlam", ".xlk", ".xlm", ".xlr",
".xlsb", ".xlsm", ".xlt", ".xltm", ".xltx", ".xlw", ".ycbcra", ".yuv"
```

Figure 3.0 File extension targeted by Samsam ransomware.

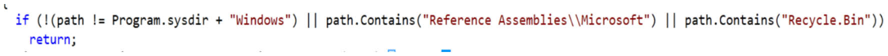
The ransomware code makes the call to the API DriveInfo.GetDrives() to get a list of all the logical drives in the computer and will encrypt the files in these drives. The ransomware will encrypt the files in shared mapped SMB drives, CD drives, attached removable drives to the computer. Backups from the endpoint can often be configured to access the database via the mapped logical drive. In such configuration, database files which can be accessed via the logical drives will also get encrypted.



```
foreach (DriveInfo drive in DriveInfo.GetDrives())
{
  try
  {
    if (drive.IsReady)
      Program.recursivegetfiles(drive.Name);
  }
  catch
```

Figure 4.0 showing call to get the logical drives to the computer.

If the path of the directory contains “Windows”, “Reference Assemblies\\Microsoft”, “Recycle.Bin” the files in these folders will be skipped and will not be encrypted.



```
if (!(path != Program.sysdir + "Windows") || path.Contains("Reference Assemblies\\Microsoft") || path.Contains("Recycle.Bin"))
  return;
```

March 2017

February 2017

January 2017

December 2016

November 2016

October 2016

September 2016

August 2016

July 2016

Categories

Analyst Reports

Blog

Data Sheets

E-Books

Events

In the News

Press Releases

Resources

T-Shirts

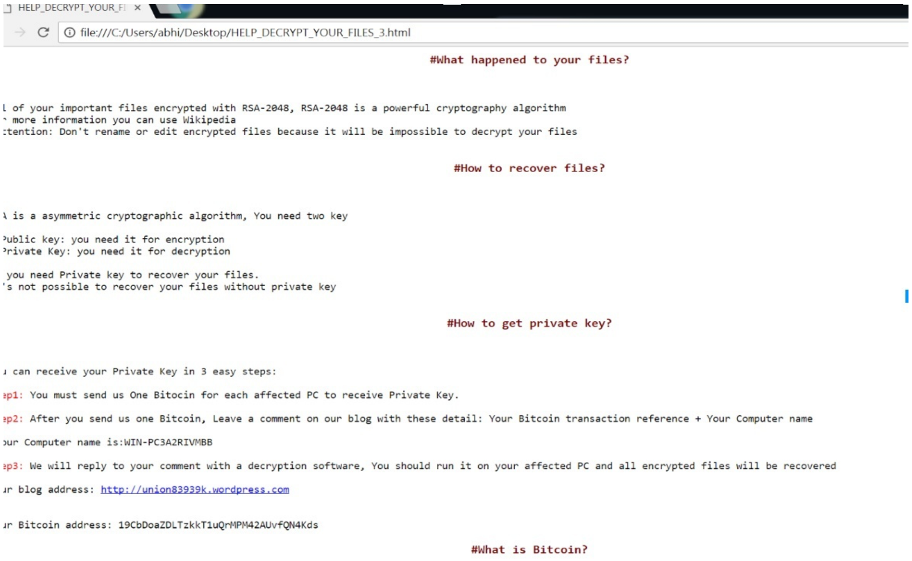
Video

Webinars

White Papers

Figure 5.0 code showing ransomware skipping file in specific folders.

To create the encrypted file, ransomware creates a new file, writes encrypted data to it and deletes the original file. The new encrypted file will have file extension .encryptedRSA appended to the original file name. HTML file titled "HELP_DECRYPT_YOUR_FILES" having the ransomware note gets dropped to the directory.

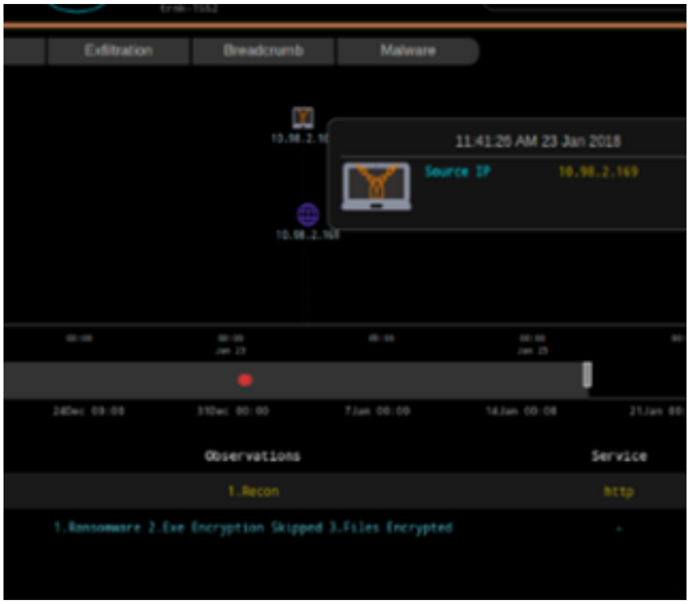

HELP_DECRYPT_YOUR_FI
file:///C:/Users/abhi/Desktop/HELP_DECRYPT_YOUR_FILES_3.html

```
                              #What happened to your files?

l of your important files encrypted with RSA-2048, RSA-2048 is a powerful cryptography algorithm
 more information you can use Wikipedia
tention: Don't rename or edit encrypted files because it will be impossible to decrypt your files

                              #How to recover files?

 is a asymmetric cryptographic algorithm, You need two key

ublic key: you need it for encryption
rivate Key: you need it for decryption

 you need Private key to recover your files.
's not possible to recover your files without private key

                              #How to get private key?

 can receive your Private Key in 3 easy steps:

ep1: You must send us One Bitocin for each affected PC to receive Private Key.

ep2: After you send us one Bitcoin, Leave a comment on our blog with these detail: Your Bitcoin transaction reference + Your Computer name

our Computer name is:WIN-PC3A2RIVMBB

ep3: We will reply to your comment with a decryption software, You should run it on your affected PC and all encrypted files will be recovered

r blog address: http://union83939k.wordpress.com

r Bitcoin address: 19CbDoaZDLTzkkT1uQrMPM42AUvfQN4Kds
                              #What is Bitcoin?
```

Figure 6.0 showing ransomware note

Deception based detection:

Deception-based architecture involves distributing breadcrumbs and lures on endpoints. When these breadcrumbs and lures are accessed, alerts from the breadcrumbs and lures will be generated and get validated by the proprietary algorithm for ransomware infection. The version of Samsam used in the breach will get detected by Shadowplex-R. Once the infected endpoint gets identified, it get isolated from the network to prevent the spread of infection.



Observations	Service
1.Recon	http
1.Ransomware 2.Exe Encryption Skipped 3.Files Encrypted	-

Detection of Samsam in Shadowplex-R

For further details about deception based architecture to prevent infection, I would encourage readers to read my blog Deception Centric Defense Against Ransomware. The blog details the advantages of deception based architecture over the traditional architecture to detect ransomware.

Conclusion:

Samsam ransomware gets activated by the threat actor after they have breached an organization, it becomes a challenge for the inline monitoring architecture to detect them. As discussed in the blog to execute samsam ransomware it requires the public key in a specific format from the command line argument. Detection architecture which relies on detonation in a virtualized environment to classify the file as malicious or benign, will not be able to provide public keys in the format which is required for samsam to execute and hence malware will not show its behavior when detonated in a virtualized environment. It will be a challenge for the detection architectures which relies on capturing the behavior in the virtualized environment to classify Samsam as malicious. Deception-based architecture detects and remediates during the execution of malware, hence it is a recommended architecture to prevent breaches and ransomware.

SHA256 of the analyzed file:

0f2c5c39494f15b7ee637ad5b6b5d00a3e2f407b4f27d140cd5a82
1ff08acfac

710a45e007502b8f42a27ee05dcd2fba

References:

[1] Allscripts recovering from ransomware attack that has kept key tools offline, https://www.csoonline.com/article/3250246/security/allscripts-recovering-from-ransomware-attack-that-has-kept-key-tools-offline.html.

Acalvio provides Advanced Threat Defense (ATD) solutions to detect, engage and respond to malicious activity inside the perimeter. The solutions are anchored on patented innovations in Deception and Data Science. This enables a DevOps approach to ATD, enabling ease of deployment, monitoring and management. Acalvio enriches its threat intelligence by data obtained from internal and partner ecosystems, enabling customers to benefit from defense in depth, reduce false positives, and derive actionable intelligence for remediation.