The Continuing Evolution of Samas Ransomware

secureworks.com/blog/samas-ransomware

Kevin Strickland

Continued development of this malware indicates the threat actors are persistent Tuesday, May 3, 2016 *By: Kevin Strickland*

Ransomware has evolved from single-system infections to enterprise compromises.

In some of the more well-known and better publicized ransomware cases, a user either receives and executes a malicious attachment or is the victim of an exploit kit such as Angler, resulting in one system being infected with ransomware. The ransomware encrypts specific files on the system and may encrypt files on mapped network drives. Some ransomware variants also target and encrypt files on unmapped, open network shares that can be accessed using the user's credentials.

In the first quarter of 2016, SecureWorks analysts identified a trend of more extensive, enterprise-wide ransomware infections. Instead of only one system being affected, a significant percentage of systems within the compromised infrastructure exhibited signs of ransomware infection. This type of ransomware attack has had a significant impact on organizations in several verticals, including hospitality, healthcare, education, and manufacturing. No single industry appears to be targeted more than another. During one incident, SecureWorks analysts found that more than 30% of the organization's systems were infected with ransomware, including a server hosting the cloud backup application. The client could not properly restore encrypted documents, causing a significant strain on the company and its employees. The threat actors used tactics and techniques popular with dedicated adversaries and infected the systems with the ransomware variant known as Samas (also known as SamSam).

Samas ransomware is documented in several security articles, blogs, and forums, including a blog post published by the SecureWorks Counter Threat Unit™ (CTU) research team on March 30, 2016. Threat actors established a foothold within the infrastructure, harvested credentials, used the stolen credentials to conduct reconnaissance and map the compromised infrastructure, and later deployed and executed the Samas ransomware on multiple systems. The damage inflicted by this malware prompted the U.S. Federal Bureau of Investigation (FBI) to “[ask] business and software security experts for emergency assistance in its investigation.”

As the Samas ransomware has become more prevalent, low-level indicators such as file hashes, ransom note “help” files, and encrypted filename extensions have been publicly released. Additionally, the antivirus industry is attempting to keep pace with updates to detect

the ransomware. The release of this information benefits two groups: victims and the Samas malware author(s). Affected organizations can more efficiently identify the ransomware, decreasing the time spent on containment and eradication. The malware authors react to the publicized information by modifying their code, effectively nullifying many of the published indicators, in some cases, avoiding detection by traditional antivirus applications. SecureWorks analysts have identified updated versions of the Samas ransomware, indicating that the authors have been modifying their code.

The Samas ransomware is a .NET compiled binary, and the primary filename associated with the ransomware is samsam.exe. An initial samsam.exe variant analyzed by SecureWorks contained a compile date in January 2016 and a file description field of “MicrosoftSAM.” SecureWorks analysts identified three additional variants of the Samas ransomware (see Table 1).

Name	Compile date	File description field
mikoponi.exe	March 2016	MiCro Oragns
RikiRafael.exe	Early April 2016	Microsoft BenchMark CPU
showmehowto.exe	April 24, 2016	Adobe Flash Player

Table 1. Samas variants identified by SecureWorks analysts.

As illustrated in Figures 1-4, each of the four variants were identified by a unique Program Database (PDB) file string embedded within the file. The PDB file stores debugging information for an application and often indicates the original name of the program.

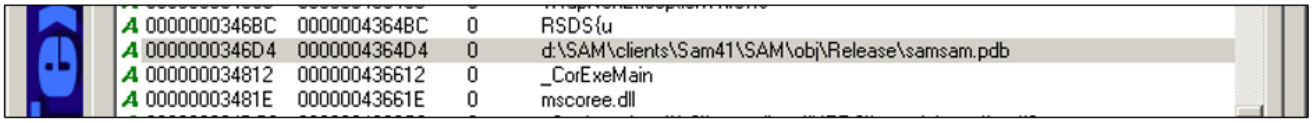

Figure 1. PDB file string for samsam.exe. (Source: SecureWorks)

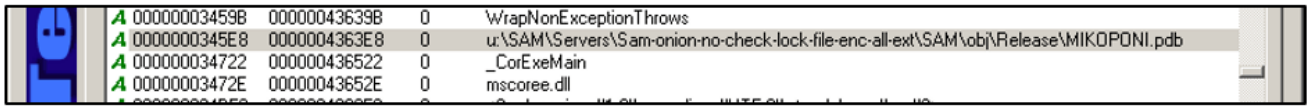

Figure 2. PDB file string for mikoponi.exe. (Source: SecureWorks)

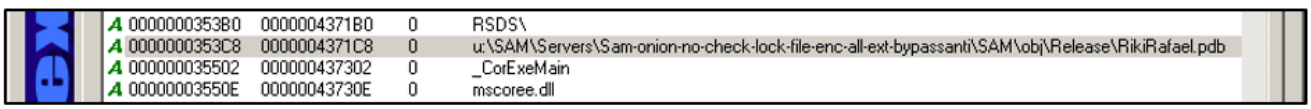

Figure 3. PDB file string for RikiRafael.exe. (Source: SecureWorks)

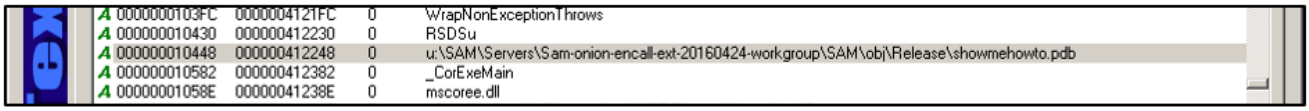

Figure 4. PDB file string for showmehowto.exe. (Source: SecureWorks)

The older Samas variants contained two hidden executables within the portable executable (PE) resource section: del.exe and selfdel.exe. The del.exe file is the legitimate Microsoft SysInternals SDelete application. Tests of the ransomware indicate that selfdel.exe is used to delete both samsam.exe and del.exe from the infected system.

In the more recent mikoponi.exe and RikiRafael.exe variants, both executables contained one binary (SDelete) hidden in the resource section. Instead of using two executables, these variants create a Windows batch script (see Figure 5) to delete itself.

```
1  @echo off
2  SETLOCAL EnableExtensions
3  set "EXE=RikiRafael.exe"
4  set "DEL=C:\ProgramData\BackupHomeDir\macrosoft10.exe"
5  set "PEXE=C:\Users\Windows7\Desktop"
6  :loop
7  FOR /F %%x IN ('tasklist /NH /FI "IMAGENAME eq %EXE%"') DO IF %%x == %EXE% goto FOUND
8  goto END
9  :FOUND
10 ping 127.0.0.1 -n 5 > NUL
11 goto loop
12 :END
13 "%DEL%" -p 16 "%PEXE%\%EXE%" -accepteula
14 DEL "%DEL%"
15 DEL "%~f0"
```

Figure 5. Extracted batch script from Samas sample. (Source: SecureWorks)

The batch script sets three variables: the Samas executable name (EXE), SDelete (DEL), and the Samas executable process path (PEXE). A FOR loop is created, executing ‘tasklist' in search of the running Samas process. If the process is still running, the batch script continues to run in a loop, creating a delay by pinging the local host five times and the repeating the search process. If the process is not found, SDelete (DEL) executes and deletes the Samas ransomware. The batch script then deletes both SDelete and itself.

As an additional forensic indicator, a registry key is created when SDelete executes with the “-accepteula” parameter (which is required the first time it is executed on any system), which indicates that the end-user license agreement (EULA) was accepted. The key is created within the profile of the user who executed SDelete (e.g., HKEY_CURRENT_USER\Software\Sysinternals\SDelete).

The most recent Samas variant observed by SecureWorks analysts as of this publication (showmehowto.exe) uses a batch script but forgoes the use of SDelete, leaving the malware on the system. Within one month, the Samas authors developed two variants, and each iteration made past low-level threat indicators obsolete.

All of the Samas variants analyzed by SecureWorks are .NET compiled binaries with code obfuscation. Using a decompiler tool, several attributes of the recent variants can be identified, notably the ransom note filenames and the extension of the encrypted files. The samsam.exe variant created ransom note files labeled HELP_DECRYPT_YOUR_FILES and used the extension .encryptedRSA.

Figure 6 shows code extracted from the RikiRafael variant's binary, including several variables used throughout the program. The variables contain an unusual amount of characters, and the values of these variables are stored as hexadecimal (HEX) values (see Figures 7 and 8). This style of coding is often described as obfuscation and is used to hide a program's true intent from security tools and analysts. The ASCII representation of the HEX value in Figure 7 is HOW_TO_DECRYPT_FILES, and the ASCII representation of Figure 8 is .justbtcwillhelpyou.

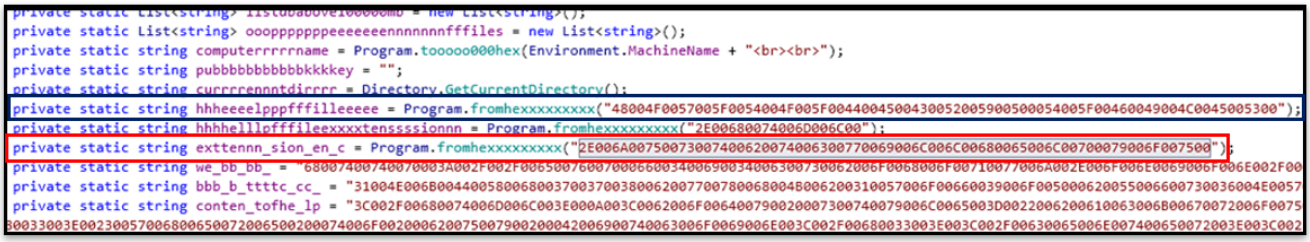

Figure 6. Code from RikieRafael.exe. (Source: SecureWorks)

Figure 7. RikiRafael.exe hexadecimal representation of the HOW_TO_DECRYPT_FILES string. (Source: SecureWorks)

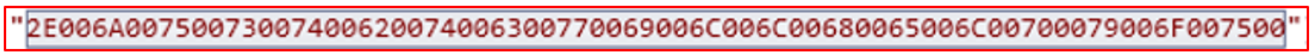

Figure 8. RikiRafael.exe hexadecimal representation of the justbtcwillhelpyou string. (Source: SecureWorks)

Both the mikoponi and RikiRafael Samas variants label their ransom note files HOW_TO_DECRYPT_FILES. The files encrypted by the mikoponi variant use the extension .encryptedAES, while files encrypted by the RikiRafael variant use the extension .justbtcwillhelpyou. The showmehowto.exe variant labels ransom note files HELP_FOR_DECRYPT_FILE and uses the .btc-help-you extension.

Based on the analyzed Samas samples, the core code of the Samas ransomware has not drastically changed. However, the continued development of the ransomware binaries indicate that the threat actors are persistent and will continue to deliver updated versions to evade detection and continue their campaign. Endpoint detection mechanisms such as the SecureWorks Advanced Endpoint Threat Detection (AETD) service goes beyond the detection of low-level threat indicators, applying behavioral analysis and human intelligence to detect the adversary and protect your endpoints.