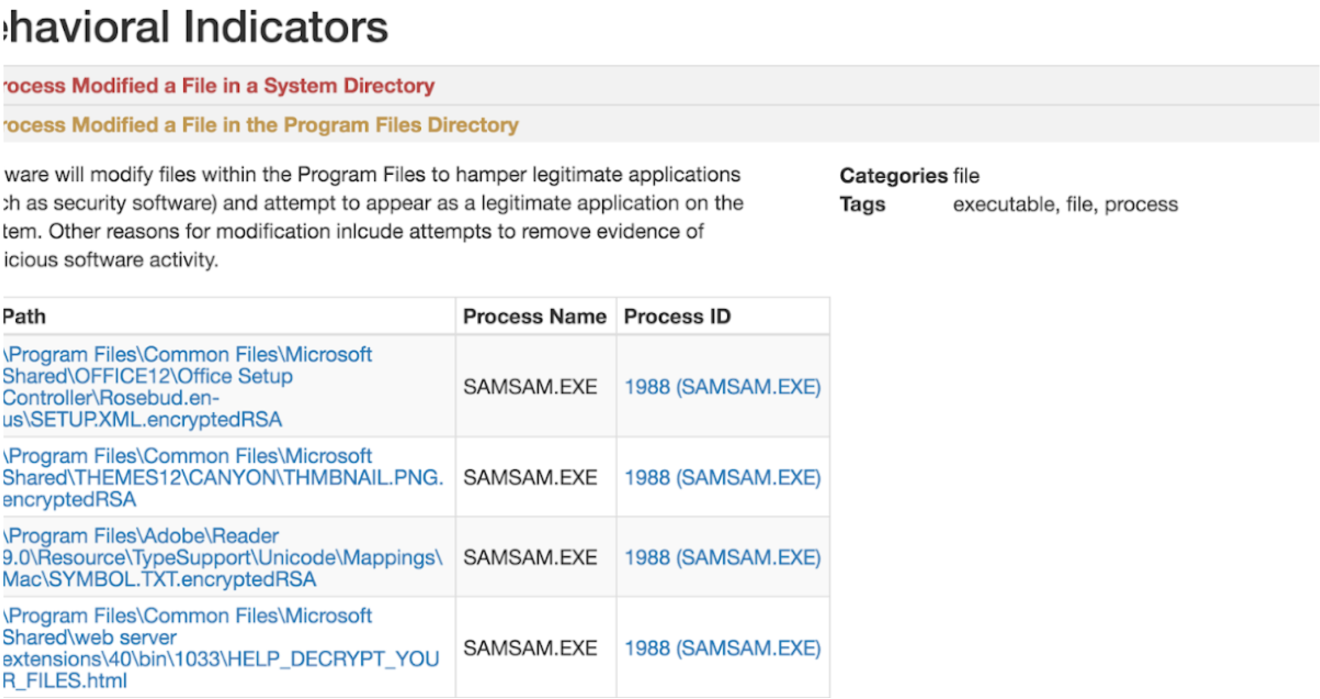
SamSam: The Doctor Will See You, After He Pays The Ransom

blog.talosintel.com/2016/03/samsam-ransomware.html



havioral Indicators

ocess Modified a File in a System Directory

ocess Modified a File in the Program Files Directory

ware will modify files within the Program Files to hamper legitimate applications h as security software) and attempt to appear as a legitimate application on the tem. Other reasons for modification inlcude attempts to remove evidence of icious software activity.

Categories file
Tags executable, file, process

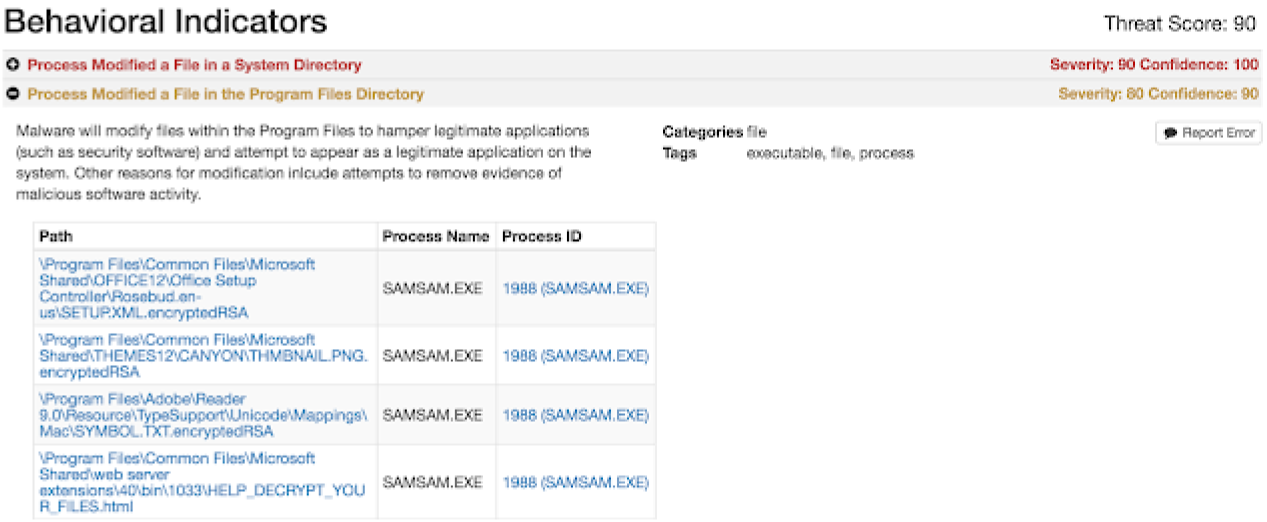
Path	Process Name	Process ID
\Program Files\Common Files\Microsoft Shared\OFFICE12\Office Setup Controller\Rosebud.en-us\SETUP.XML.encryptedRSA	SAMSAM.EXE	1988 (SAMSAM.EXE)
\Program Files\Common Files\Microsoft Shared\THEMES12\CANYON\THMBNAIL.PNG.encryptedRSA	SAMSAM.EXE	1988 (SAMSAM.EXE)
\Program Files\Adobe\Reader 9.0\Resource\TypeSupport\Unicode\Mappings\Mac\SYMBOL.TXT.encryptedRSA	SAMSAM.EXE	1988 (SAMSAM.EXE)
\Program Files\Common Files\Microsoft Shared\web server extensions\40\bin\1033\HELP_DECRYPT_YOUR_FILES.html	SAMSAM.EXE	1988 (SAMSAM.EXE)

Cisco Talos is currently observing a widespread campaign leveraging the Samas/Samsam/MSIL.B/C ransomware variant. Unlike most ransomware, SamSam is not launched via user focused attack vectors, such as phishing campaigns and exploit kits. This particular family seems to be distributed via compromising servers and using them as a foothold to move laterally through the network to compromise additional machines which are then held for ransom. A particular focus appears to have been placed on the healthcare industry.

Adversaries have been seen leveraging JexBoss, an open source tool for testing and exploiting JBoss application servers, to gain a foothold in the network. Once they have access to the network they proceed to encrypt multiple Windows systems using SamSam.

Technical Details

Upon compromising the system the sample will launch a samsam.exe process which begins the process of encrypting files on the system.



Behavioral Indicators

Threat Score: 90

Process Modified a File in a System Directory — Severity: 90 Confidence: 100

Process Modified a File in the Program Files Directory — Severity: 80 Confidence: 90

Malware will modify files within the Program Files to hamper legitimate applications (such as security software) and attempt to appear as a legitimate application on the system. Other reasons for modification inlcude attempts to remove evidence of malicious software activity.

Categories file

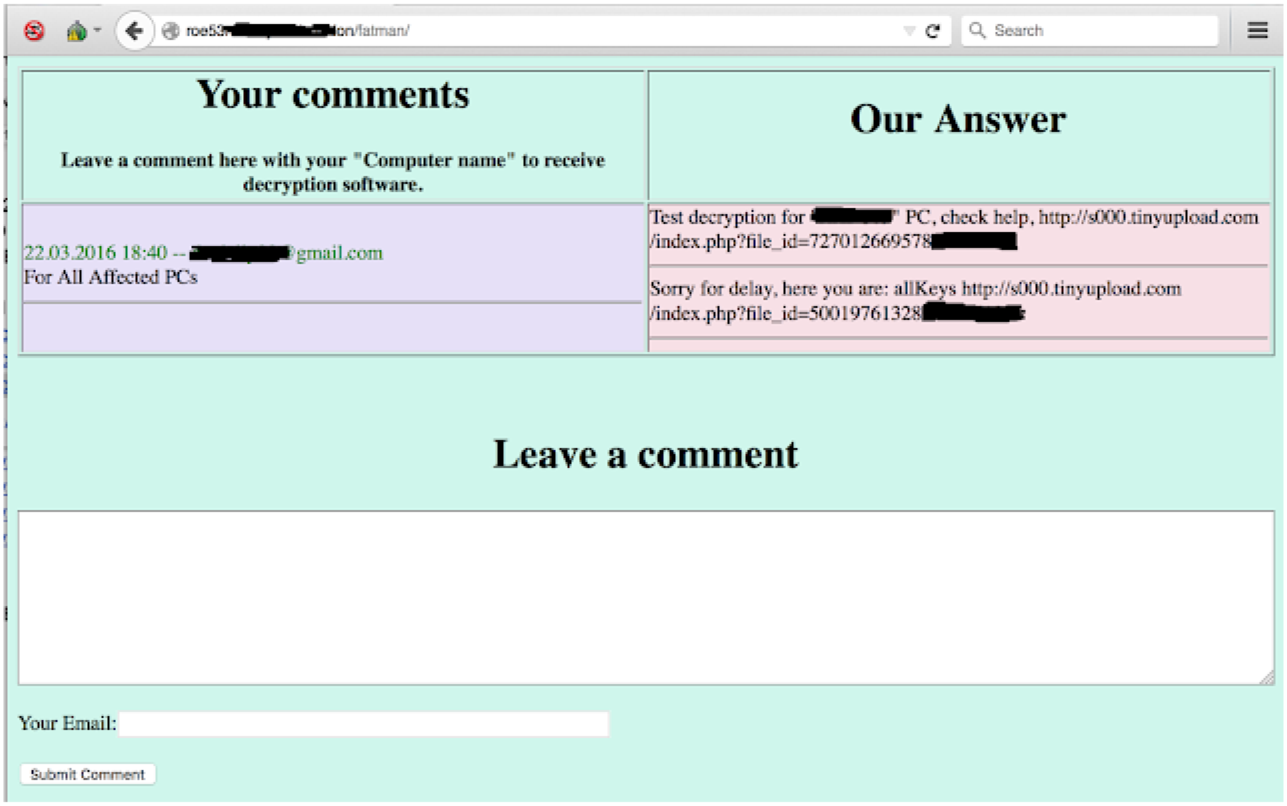
Tags executable, file, process

Path	Process Name	Process ID
\Program Files\Common Files\Microsoft Shared\OFFICE12\Office Setup Controller\Rosebud.en-us\SETUP.XML.encryptedRSA	SAMSAM.EXE	1988 (SAMSAM.EXE)
\Program Files\Common Files\Microsoft Shared\THEMES12\CANYON\THMBNAIL.PNG.encryptedRSA	SAMSAM.EXE	1988 (SAMSAM.EXE)
\Program Files\Adobe\Reader 9.0\Resource\TypeSupport\Unicode\Mappings\Mac\SYMBOL.TXT.encryptedRSA	SAMSAM.EXE	1988 (SAMSAM.EXE)
\Program Files\Common Files\Microsoft Shared\web server extensions\40\bin\1033\HELP_DECRYPT_YOUR_FILES.html	SAMSAM.EXE	1988 (SAMSAM.EXE)

SamSam encrypts various file types (see Appendix A) with Rijndael and then encrypts that key with RSA-2048 bit encryption. This makes the files unrecoverable unless the author made a mistake in the implementation of the encryption algorithms. The adversaries behind this ransomware variant did not go to any length to disguise or cover up the ransomware activity on the system. The samples Talos obtained are not packed and do not contain anti-debugging features.

One interesting note regarding the samples Talos has observed is that the malware will abort the encryption routine if the system is running a version of Microsoft Windows prior to Vista. This is likely done for compatibility reasons. Once installed on a machine there is no beaconing or C2 activity. The ransomware is effectively self sufficient.

Below is an example of the communication between a victim and the adversaries. Notice in this instance, the victim initially paid for one PC and followed up by paying for all affected PCs.



Your comments Leave a comment here with your "Computer name" to receive decryption software.	Our Answer
22.03.2016 18:40 -- [redacted]@gmail.com For All Affected PCs	Test decryption for [redacted]" PC, check help, http://s000.tinyupload.com/index.php?file_id=727012669578[redacted] Sorry for delay, here you are: allKeys http://s000.tinyupload.com/index.php?file_id=50019761328[redacted]

Leave a comment

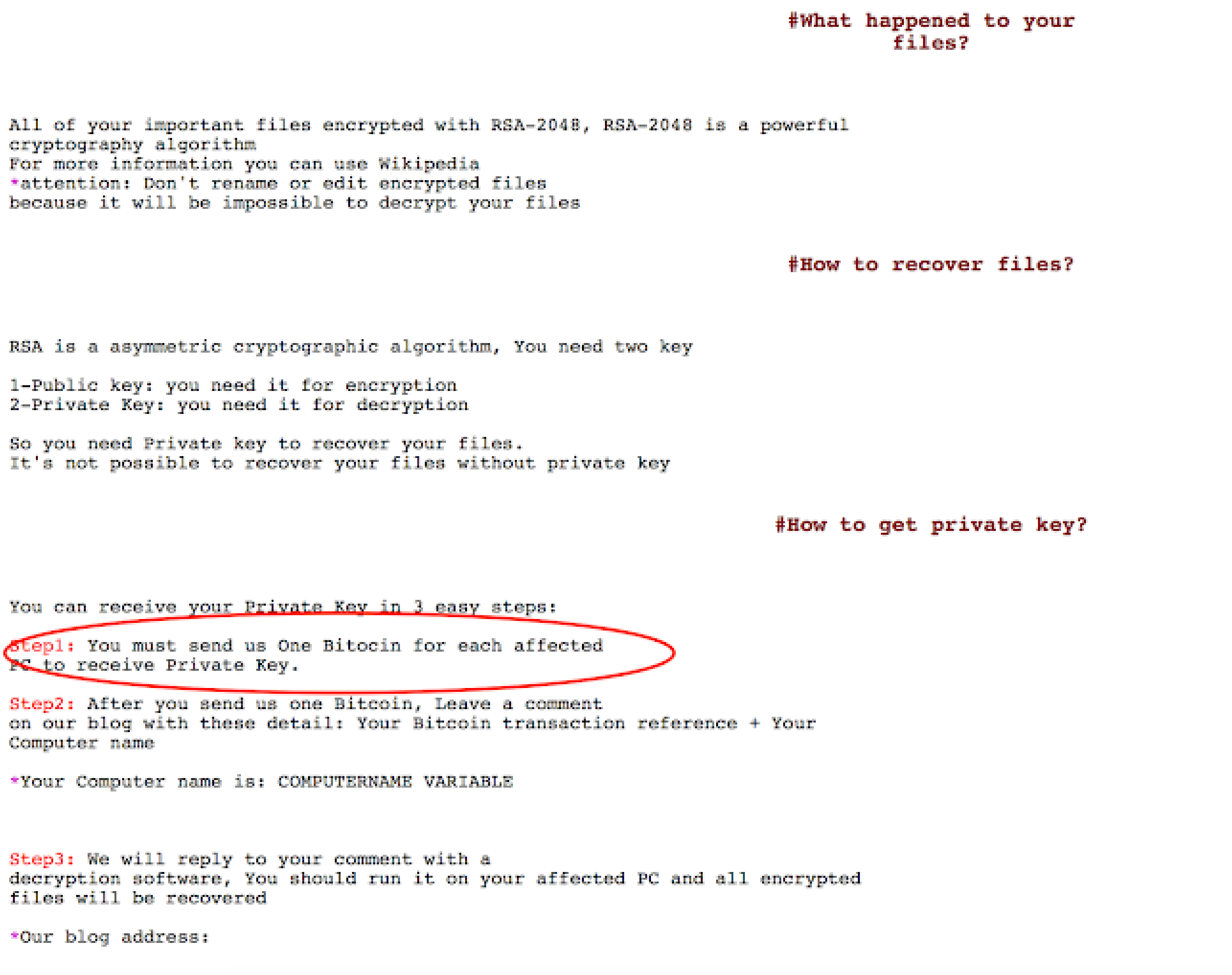
Your Email:

Tools

There were a couple of open source tools that were seen being leveraged by the adversaries. The first is JexBoss, which is a testing and exploitation framework for JBoss application servers. This was being used as an initial infection vector to gain a foothold in the network to spread the ransomware. The second is a component of REGeorg, tunnel.jsp. REGeorg is an open source framework to create socks proxies for communication. The file found in the samples is an unmodified version of the tunnel.jsp file that is being hosted by REGeorg (b963b8b8c5ca14c792d2d3c8df31ee058de67108350a66a65e811fd00c9a340c).

Payment Evolution

As we have monitored this activity, we have started to see changes in the amount and types of payment options available to victims. Initially, we saw a payment option of 1 bitcoin for each PC that has been infected.



#What happened to your files?

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

#How to recover files?

RSA is a asymmetric cryptographic algorithm, You need two key

1-Public key: you need it for encryption
2-Private Key: you need it for decryption

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

#How to get private key?

You can receive your Private Key in 3 easy steps:

Step1: You must send us One Bitocin for each affected
PC to receive Private Key.

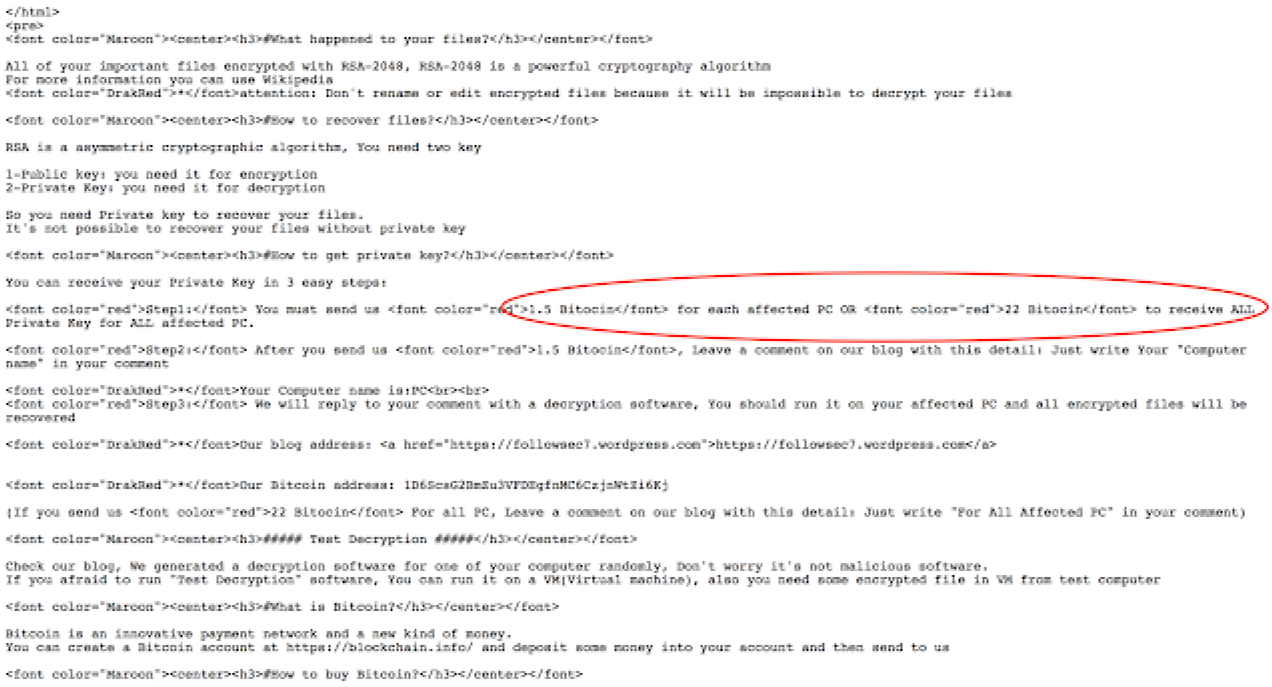
Step2: After you send us one Bitcoin, Leave a comment
on our blog with these detail: Your Bitcoin transaction reference + Your
Computer name

*Your Computer name is: COMPUTERNAME VARIABLE

Step3: 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

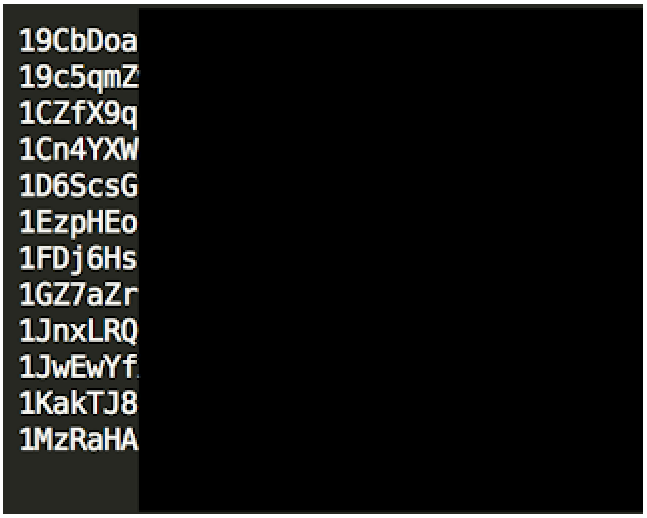
*Our blog address:

Later we saw the price for a single system has been raised to 1.5 bitcoin. It is likely the malware author is trying to see how much people will pay for their files. They even added an option for bulk decryption of 22 bitcoin to decrypt all infected systems. Below is an example of this evolution.



```
</html>
<pre>
<font color="Maroon"><center><h3>#What happened to your files?</h3></center></font>

All of your important files encrypted with RSA-2048, RSA-2048 is a powerful cryptography algorithm
For more information you can use Wikipedia
<font color="DrakRed">*</font>attention: Don't rename or edit encrypted files because it will be impossible to decrypt your files

<font color="Maroon"><center><h3>#How to recover files?</h3></center></font>

RSA is a asymmetric cryptographic algorithm, You need two key

1-Public key: you need it for encryption
2-Private Key: you need it for decryption

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

<font color="Maroon"><center><h3>#How to get private key?</h3></center></font>

You can receive your Private Key in 3 easy steps:

<font color="red">Step1:</font> You must send us <font color="red">1.5 Bitocin</font> for each affected PC OR <font color="red">22 Bitocin</font> to receive ALL
Private Key for ALL affected PC.

<font color="red">Step2:</font> After you send us <font color="red">1.5 Bitocin</font>, Leave a comment on our blog with this detail: Just write Your "Computer
name" in your comment

<font color="DrakRed">*</font>Your Computer name is:PC<br><br>
<font color="red">Step3:</font> 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

<font color="DrakRed">*</font>Our blog address: <a href="https://followsec7.wordpress.com">https://followsec7.wordpress.com</a>


<font color="DrakRed">*</font>Our Bitcoin address: 1D6ScsG2BmZu3VFDEgfnMC6CzjnWtZi6Kj

(If you send us <font color="red">22 Bitocin</font> For all PC, Leave a comment on our blog with this detail: Just write "For All Affected PC" in your comment)

<font color="Maroon"><center><h3>##### Test Decryption #####</h3></center></font>

Check our blog, We generated a decryption software for one of your computer randomly, Don't worry it's not malicious software.
If you afraid to run "Test Decryption" software, You can run it on a VM(Virtual machine), also you need some encrypted file in VM from test computer

<font color="Maroon"><center><h3>#What is Bitcoin?</h3></center></font>

Bitcoin is an innovative payment network and a new kind of money.
You can create a Bitcoin account at https://blockchain.info/ and deposit some money into your account and then send to us

<font color="Maroon"><center><h3>#How to buy Bitcoin?</h3></center></font>
```

Others have also seen samples that have increased the payment amount to 1.7 bitcoin per PC. During our investigation we found multiple different bitcoin wallets being presented to users, some had 0 bitcoins associated with them others had significant amounts. The total amount of bitcoin in these wallets was at least ~275 which equates to approximately $115,000 USD. Below is a screen capture showing some of the obfuscated wallets. They have been obfuscated so that we can continue to monitor their activity.



```
19CbDoa
19c5qmZ
1CZfX9q
1Cn4YXW
1D6ScsG
1EzpHEo
1FDj6Hs
1GZ7aZr
1JnxLRQ
1JwEwYf
1KakTJ8
1MzRaHA
```
[redacted]

IOCs

Hashes

036071786d7db553e2415ec2e71f3967baf51bdc31d0a640aa4afb87d3ce3050
553967d05b83364c6954d2b55b8cfc2ea3808a17c268b2eee49090e71976ba29
a763ed678a52f77a7b75d55010124a8fccf1628eb4f7a815c6d635034227177e
6bc2aa391b8ef260e79b99409e44011874630c2631e4487e82b76e5cb0a49307

7aa585e6fd0a895c295c4bea2ddb071eed1e5775f437602b577a54eef7f61044

939efdc272e8636fd63c1b58c2eec94cf10299cd2de30c329bd5378b6bbbd1c8

45e00fe90c8aa8578fce2b305840e368d62578c77e352974da6b8f8bc895d75b

979692a34201f9fc1e1c44654dc8074a82000946deedfdf6b8985827da992868

0f2c5c39494f15b7ee637ad5b6b5d00a3e2f407b4f27d140cd5a821ff08acfac

946dd4c4f3c78e7e4819a712c7fd6497722a3d616d33e3306a556a9dc99656f4

e682ac6b874e0a6cfc5ff88798315b2cb822d165a7e6f72a5eb74e6da451e155

58ef87523184d5df3ed1568397cea65b3f44df06c73eadeb5d90faebe4390e3e

ffef0f1c2df157e9c2ee65a12d5b7b0f1301c4da22e7e7f3eac6b03c6487a626

89b4abb78970cd524dd887053d5bcd982534558efdf25c83f96e13b56b4ee805

Conclusion

The SamSam campaign is unusual in that it is taking advantage of remote execution techniques instead of targeting the user. Adversaries are exploiting known vulnerabilities in unpatched JBoss servers before installing a web shell, identifying further network connected systems, and installing SamSam ransomware to encrypt files on these devices.

Ransomware continues to persist as a successful cyber crime business model. This technique is proving to be a profitable affair for criminals and will continue to be a threat to the internet at large until a more profitable technique is discovered. Protection against such threats is best achieved using a multi-tier defense architecture to ensure potential threats are scanned multiple times. However, one of the most effective ways to protect yourself is by simply backing up valuable files. Victims often find that at the moment when backups are most needed, they are either non-existent or incomplete. These lapses provide the revenue stream that is currently fueling the development of ransomware.

Coverage

The following Snort rules and ClamAV signatures address this threat. Please note that additional rules may be released at a future date and current rules are subject to change pending additional vulnerability information. For the most current rule information, please refer to your Defense Center, FireSIGHT Management Center or Snort.org.

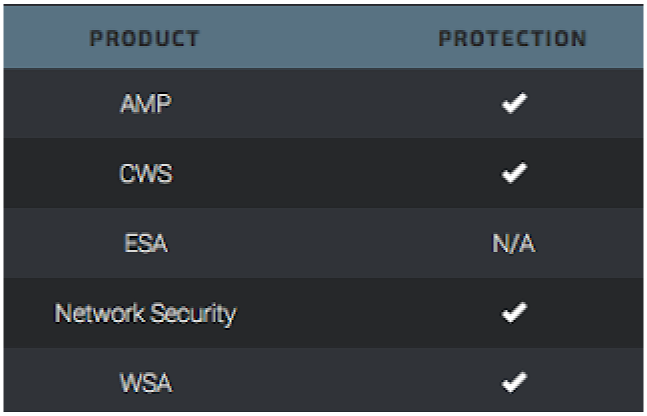
Snort Rules

- JBoss Server Vulnerabilities: 18794, 21516-21517, 24342-24343, 24642, 29909
- Samsam Malware: 38279-38280, 38304

ClamAV Signature Family

Win.Trojan.Samas

Additional ways our customers can detect and block this threat are listed below.



PRODUCT	PROTECTION
AMP	✓
CWS	✓
ESA	N/A
Network Security	✓
WSA	✓

Advanced Malware Protection (AMP) can detect and prevent the execution of this malware on targeted systems.

CWS or WSA web scanning can prevent access to malicious websites and detects malware used in these attacks.

Network Security encompasses IPS and NGFW. Both have up-to-date signatures to detect malicious network activity that this campaign exhibits.

Reference

- https://blogs.technet.microsoft.com/mmpc/2016/03/17/no-mas-samas-whats-in-this-ransomwares-modus-operandi/
- http://www.intelsecurity.com/advanced-threat-research/content/Analysis_SamSa_Ransomware.pdf
- http://www.bleepingcomputer.com/forums/t/607818/encedrsa-ransomware-support-and-help-topic-help-decrypttxt/

Appendix A: File Types Targeted for Encryption

The following file types are targeted for encryption:

.3dm, .3ds, .3fr, .3g2, .3gp, .3pr, .7z, .ab4, .accdb, .accde, .accdr, .accdt, .ach, .acr, .act, .adb, .ads, .agdl, .ai, .ait, .al, .apj, .arw, .asf, .asm, .asp, .aspx, .asx, .avi, .awg, .back, .backup, .backupdb, .bak, .bank, .bay, .bdb, .bgt, .bik, .bkf, .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, .cs, .csh, .csl, .csv, .dac, .db, .db-journal, .db3, .dbf, .dbx, .dc2, .dcr, .dcs, .ddd, .ddoc, .ddrw, .dds, .der, .des, .design, .dgc, .djvu, .dng, .doc, .docm, .docx, .dot, .dotm, .dotx, .drf, .drw, .dtd, .dwg, .dxb, .dxf, .dxg, .eml, .eps, .erbsql, .erf, .exf, .fdb, .ffd, .fff, .fh, .fhd, .fla, .flac, .flv, .fmb, .fpx, .fxg, .gray, .grey, .gry, .h, .hbk, .hpp, .htm, .html, .ibank, .ibd, .ibz, .idx, .iif, .iiq, .incpas, .indd, .jar, .java, .jin, .jpe, .jpeg, .jpg, .jsp, .kbx, .kc2, .kdbx, .kdc, .key, .kpdx, .lua, .m, .m4v, .max, .mdb, .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, .pbl, .pcd, .pct, .pdb, .pdd, .pdf, .pef, .pem, .pfx, .php, .php5, .phtml, .pl, .plc, .png, .pot, .potm, .potx, .ppam, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .prf, .ps, .psafe3, .psd, .pspimage, .pst, .ptx, .py, .qba, .qbb, .qbm, .qbr, .qbw, .qbx, .qby, .r3d, .raf, .rar,, .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, .tib, .tif, .tlg, .txt, .vob, .wallet, .war, .wav, .wb2, .wmv, .wpd, .wps, .x11, .x3f, .xis, .xla, .xlam, .xlk, .xlm, .xlr, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .xlw, .xml, .ycbcra, .yuv, .zip