بسمه تعالی

گزارش تحلیل باج افزار SamSam

مقدمه :

مشاهده و رصد فضای سایبری در روزهای اخیر از افزایش فعالیت باج افـزار SamSam خبـر مـی‌دهـد. بـر اساس گزارشات واصله، شروع فعالیت این باج افزار در ماه های فوریه ، مارس و آوریل ۲۰۱۶ بوده اسـت. امـا فعالیت جدید این باج افزار در ماه های اخیر مجددا از سر گرفته شده است. *مشاهدات حاکی از آن است کـه باج افزار SamSam با هدف قرار دادن مراکز بهداشتی ، بیمارستان ها و همچنین کمپانی هـای بـزرگ در آمریکا شروع قدرتمندی در سال ۲۰۱۸ داشته است* . این نکته را باید در نظر گرفت که SamSam از طریق نفوذ به سرورها اقدام به نفوذ و آلوده‌سازی شبکه می‌نماید و دلیل موفقیت آن نیز همین نکته می باشد.

مشخصات فایل اجرایی :

نام فایل	samsam.exe
MD۵	e۲۶c۶a۲۰۱۳۹f۷a۴۵e۹۴ce۰b۱۶e۶۲bd۰۳
SHA-۱	c۶d۷c۲۷۰۷۰a۳۸۳۸e۲b۶ac۷e۹۷e۹۹۶b۰fe۶۵۶۰fe۲
SHA-۲۵۶	۸۹b۴abb۷۸۹۷۰cd۵۲۴dd۸۸۷۰۵۳d۵bcd۹۸۲۵۳۴۵۵۸efdf۲۵c۸۳f۹۶e۱۳b۵۶b۴ee۸۰۵
اندازه فایل	۲۱۲.۵ kb
کامپایلر	Microsoft visual C# v۷.۰ / Basic .NET

فایل اجرایی این باج افزار دارای سه بخش است :

نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	۶.۲۲	۸۱۹۲	۲۱۴۵۸۰	۲۱۵۰۴۰
.rsrc	۴.۱۱	۲۲۹۳۷۶	۱۴۵۶	۱۵۳۶
.reloc	۰.۱	۲۳۷۵۶۸	۱۲	۵۱۲

تحلیل پویا :

بررسی ها نشان می دهد که باج‌افزار SamSam اکثراً در حملات هدفمند بر ضد سازمان‌ها استفاده می‌شود. این باج افزار پس از نفوذ به یک سرور با راه‌اندازی ابزار متن باز JexBoss اقدام به نفوذ و افزایش دسترسی به شبکه می‌نماید. jexBoss ابزاری متن باز برای استفاده از برنامه های JBoss است. بعد از دسترسی به شبکه، این باج‌افزار اقدام به رمزگذاری رایانه هایی با سیستم عامل ویندوز می‌کند.

نتایج حاصل از بررسی ها نشان می دهد که این باج افزار فایل های سیستم قربانی را با ترکیبی از دو الگوریتم رمزنگاری RSA و AES رمزگذاری می کند . SamSam هیچگونه مکانیزمی برای مخفی سازی فعالیت های خود در سیستم ندارد .

از نکات جالب توجه این باج افزار می توان به عدم رمزگذاری فایل های سیستم قربانی در سیستم عامل های ویستا و ما قبل آن اشاره کرد ، همچنین این باج افزار هیچگونه سرور فرماندهی و کنترل (C&C) ندارد و به صورت مستقل عمل می کند.

بر همین اساس، باج افزار SamSam برای نفوذ به سیستم قربانی از ابزار های زیر استفاده می کند :

۱) JexBoss

این ابزار همانطور که گفته شد برای استفاده از برنامه های Jboss سرور ها استفاده می شود ، باج افزار برای نفوذ به سرور از این ابزار بهره می برد.

۲) tunnel.jsp که قسمتی از فریم ورک ReGeorg است

REGeorg برای ساختن پراکسی های Socks استفاده می شود ، باج افزار برای برقراری ارتباط از این پراکسی ها استفاده می کند.

باج افزار SamSam پس از ورود به سیستم قربانی، پیغام باج خواهی خود به نام HELP_DECRYPT_YOUR_FILES.html را در دسکتاپ قربانی و همچنین در کنار تمامی فایل های رمزگذاری شده قرار می دهد. تصویر زیر پیغام باج خواهی باج افزار SamSam را نشان می دهد.

#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 Bitcoin 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:

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: http://

*Our Bitcoin address:

#What is Bitcoin?

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

#How to buy Bitcoin?

There are many way to buy Bitcoin and deposit it into your account,
You can buy it with WesternUnion, Bank Wire, International Bank transfer, Cash deposit and etc

https://localbitcoins.com ---> Buy Bitcoin with WesternUnion or MoneyGram

https://coincafe.com/buybitcoinswestern.php ---> Buy Bitcoin fast and Secure with WesternUnion and Cash deposit

https://www.bitstamp.net ---> Buy Bitcoin with bank wire, International bank transfer, SEPA payment

https://www.kraken.com ---> Buy Bitcoin with bank wire, International bank transfer, SEPA payment

https://www.kraken.com ---> Buy Bitcoin with bank wire, International bank transfer, SEPA payment

https://www.ccedk.com ---> Buy Bitcoin with bank wire, International bank transfer, SEPA payment

https://bitcurex.com/ ---> Buy Bitcoin with bank wire, International bank transfer, SEPA payment

If you want to pay with your Business bank account you should create a business account in exchangers
they don't accept payment from third party

How to find the Bitcoin transaction reference?

Login into your blockchain account -> go to "My transaction" tab -> Click on your transaction -> In "Transaction Summary" page, You will find a "hash" with 64 characters long
Send us this hash with your comment on our blog + your computer name
*Your Computer name is

#How to use private Key?

We send you a simple software with your private Key
And you just need run this software on each computer that encrypted and all affected files will be decrypted

#deadline

You just have 7 days to send us the Bitcoin after 7 days we will remove your private key and it's impossible to recover your files

همانطور که ملاحظه می کنید در ابتدا مبلغ باج درخواستی به ازای هر سیستم ۱ بیت کوین بود و پس از مدتی این مبلغ به ۱/۵ بیت کوین افزایش یافت . باج افزار این گزینه را در اختیار قربانیان قرار می دهد که در ازای رمزگشایی تمام سیستم ها ۲۲ بیتکوین بپردازند.

در بعضی موارد نیز دیده شده که باج افزار مبلغ ۱/۷ بیت کوین از قربانی طلب کرده است.

در نهایت می توان نتیجه گرفت که این باج افزار یک کاربر یا یک سیستم را مورد هدف قرار نمی دهد بلکه با هدف قرار دادن یک سرور ، به شبکه سازمان نفوذ می کند .

تحلیل ایستا :

پس از بررسی کد منبع باج افزار SamSam توسط کارشناسان این مرکز، نتایج زیر حاصل گردید:

بررسی ها نشان می دهد که این باج‌افزار در شرایط خاصی قابل اجراست و همانطور که در تصویر زیر قابل ملاحظه است، ابتدا محیط اجرایی خود و سپس نسخه سیستم‌عامل میزبان را بررسی می‌کند. این باج‌افزار در سیستم‌عامل‌های ویندوز XP و ماقبل آن قابل اجرا نبوده و با فراخوانی متد killOpenedProcessTree فرآیند را از بین می‌برد.

```
private static void EncryptFile(string plainFilePath, string encryptedFilePath, byte[] key, byte[] iv, byte[] signatureKey, string
  rsaKey)
{
    if (encc.checkOSCompatibility())
    {
        encc.killOpenedProcessTree(plainFilePath);
    }
    if (File.Exists(encryptedFilePath))
    {
        File.Delete(encryptedFilePath);
    }
```

```
// Token: 0x06000002 RID: 2 RVA: 0x00002084 File Offset: 0x00000284
private static bool checkOSCompatibility()
{
    bool result = true;
    OperatingSystem osversion = Environment.OSVersion;
    if (osversion.Version.Major == 5)
    {
        result = false;
    }
    return result;
}
```

مواردی که در متغیرهای زیر دیده می‌شود نیز اطلاعات خوبی را همراه خود دارد.

با توجه به تصویر زیر، در می‌یابیم که فایل پیغام باج‌خواهی، یک فایل html و به نام HELP_DECRYPT_YOUR_FILES بوده و پسوند فایل‌های رمزگذاری شده نیز encryptedRSA. خواهد بود.

همچنین در متغیر sfd، با توجه به دریافت دایرکتوری فعلی به نظر می‌رسد که فایلی به نام selfdel.exe، فایل اجرایی باج‌افزار را حذف می‌کند.

```
// Token: 0x0400001E RID: 30
private static string comname = Program.ToHexString(Environment.MachineName);

// Token: 0x0400001F RID: 31
private static string publickey = "";

// Token: 0x04000020 RID: 32
private static string currentdir = Directory.GetCurrentDirectory();

// Token: 0x04000021 RID: 33
private static string helpfile = "HELP_DECRYPT_YOUR_FILES";

// Token: 0x04000022 RID: 34
private static string helpfileext = ".html";

// Token: 0x04000023 RID: 35
private static string sfd = Program.currentdir + "\\selfdel.exe";

// Token: 0x04000024 RID: 36
private static string ext_enc = ".encryptedRSA";
```

با بررسی های انجام شده مشخص گردید، تابع زیر به نام myeennc ، وظیفه اضافه کردن پسوند encryptedRSA. را به فایل‌های رمزگذاری شده دارد.

```
public static void myeennc(string pathfile)
{
    FileInfo fileInfo = new FileInfo(pathfile);
    try
    {
        DriveInfo driveInfo = new DriveInfo(pathfile);
        long availableFreeSpace = driveInfo.AvailableFreeSpace;
        long length = fileInfo.Length;
        if (length < availableFreeSpace && new FileInfo(pathfile).Length > 0L && !File.Exists(fileInfo.DirectoryName + "\\" +
          fileInfo.Name + Program.ext_enc) && !string.IsNullOrEmpty(Program.publickey))
        {
            Program.encryptFile(pathfile, Program.publickey);
            if (File.Exists(fileInfo.DirectoryName + "\\" + fileInfo.Name + Program.ext_enc))
            {
                FileInfo fileInfo2 = new FileInfo(fileInfo.DirectoryName + "\\" + fileInfo.Name + Program.ext_enc);
                if (fileInfo2.Length > length)
                {
                    fileInfo.Attributes = FileAttributes.Normal;
                    File.Delete(pathfile);
                    if (!File.Exists(pathfile))
                    {
                        File.WriteAllText(fileInfo.DirectoryName + "\\" + Program.helpfile + Program.helpfileext,
                          Program.FromHexString(Program.txthelp));
                    }
                }
            }
        }
    }
    catch (Exception)
    {
        if (File.Exists(fileInfo.DirectoryName + "\\" + fileInfo.Name + Program.ext_enc))
        {
            File.Delete(fileInfo.DirectoryName + "\\" + fileInfo.Name + Program.ext_enc);
        }
    }
}
```

تصویر زیر آرایه‌ای از پسوندهای مورد هدف این باج‌افزار را نشان می دهد.

```
// Token: 0x04000018 RID: 24
private static string[] types = new string[]
{
    "xls",
    ".xlsx",
    ".pdf",
    ".doc",
    ".docx",
    ".ppt",
    ".pptx",
    ".txt",
    ".dwg",
    ".bak",
    ".bkf",
    ".pst",
    ".dbx",
    ".zip",
    ".rar",
    ".mdb",
    ".asp",
    ".aspx",
    ".html",
    ".htm",
    ".dbf",
    ".3dm",
```

لیست کامل مجموعه فایل های هدف به شرح زیر است:

"xls",".xlsx",".pdf",".doc",".docx",".ppt",".pptx",".txt",".dwg",".bak",".bkf",".pst",".dbx",".zip",".rar",".mdb",".asp",".aspx",".html",".htm",".dbf",".۳dm",".۳ds",".۳fr",".jar",".۳g۲",".xml",".png",".tif",".۳gp",".java",".jpe",".jpeg",".jpg",".jsp",".php",".۳pr",".۷z",".ab۴",".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",".cdr۳",".cdr۴",".cdr۵",".cdr۶",".cdrw",".cdx",".ce۱",".ce۲",".cer",".cfp",".cgm",".cib",".class",".cls",".cmt",".cpi",".cpp",".cr۲",".craw",".crt",".crw",".phtml",".php۵",".cs",".csh",".csl",".tib",".csv",".dac",".db",".db۳",".db-journal",".dc۲",".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",".kc۲",".kdbx",".kdc",".key",".kpdx",".lua",".m",".m۴v",".max",".mdc",".mdf",".mef",".mfw",".mmw",".moneywell",".mos",".mov",".mp۳",".mp۴",".mpg",".mrw",".msg",".myd",".nd",".ndd",".nef",".nk۲",".nop",".nrw",".ns۲",".ns۳",".ns۴",".nsd",".nsf",".nsg",".nsh",".nwb",".nx۲",".nxl",".nyf",".oab",".obj",".odb",".odc",".odf",".odg",".odm",".odp",".ods",".odt",".oil",".orf",".ost",".otg",".oth",".otp",".ots",".ott",".p۱۲",".p۷b",".p۷c",".pab",".pages",".pas",".pat",".pcd",".pct",".pdb",".pdd",".pef",".pem",".pfx",".pl",".plc",".pot",".potm",".potx",".ppam",".pps",".ppsm",".ppsx",".pptm",".prf",".ps",".psafe۳",".psd",".pspimage",".ptx",".py",".qba",".qbb",".qbm",".qbr",".qbw",".qbx",".qby",".r۳d",".raf",".rat",".raw",".rdb",".rm",".rtf",".rw۲

",".rwl",".rwz",".s۳db",".sas۷bdat",".say",".sd۰",".sda",".sdf",".sldm",".sldx",".sql",".sqlite",".sqlite۳",".sqlitedb",".sr۲",".srf",".srt",".srw",".st۴",".st۵",".st۶",".st۷",".st۸",".std",".sti",".stw",".stx",".svg",".swf",".sxc",".sxd",".sxg",".sxi",".sxi",".sxm",".sxw",".tex",".tga",".thm",".tlg",".vob",".war",".wallet",".wav",".wb۲",".wmv",".wpd",".wps",".x۱۱",".x۳f",".xis",".xla",".xlam",".xlk",".xlm",".xlr",".xlsb",".xlsm",".xlt",".xltm",".xltx",".xlw",".ycbcra",".yuv"

شناسایی :

در حال حاضر یعنی در زمان نگارش این گزارش تعداد ۳۵ مورد از ۶۴ آنتی ویروس و آنتی بدافزار موجود در سامانه VirusTotal قادر به شناسایی این باج افزار بوده وآن را حذف یا غیرفعال می‌کنند.

Ad-Aware	Gen:Variant.Ransom.Samas.3	AegisLab	Gen.Variant!c
AhnLab-V3	Trojan/Win32.Samas.C1342294	ALYac	Gen:Variant.Ransom.Samas.3
Antiy-AVL	Trojan/Win32.SGeneric	Arcabit	Trojan.Ransom.Samas.3
Avast	Win32:Ransom-AYN [Trj]	AVG	Win32:Ransom-AYN [Trj]
Avira	TR/Samas.217600.1	AVware	Trojan.Win32.Generic!BT
BitDefender	Gen:Variant.Ransom.Samas.3	CAT-QuickHeal	Trojan.Inject.TL3
ClamAV	Win.Trojan.Samas-1	Comodo	UnclassifiedMalware
CrowdStrike Falcon	malicious_confidence_100% (W)	Cylance	Unsafe
Emsisoft	Gen:Variant.Ransom.Samas.3 (B)	Endgame	malicious (moderate confidence)
eScan	Gen:Variant.Ransom.Samas.3	ESET-NOD32	a variant of MSIL/Filecoder.Samas.A
F-Secure	Gen:Variant.Ransom.Samas.3	Fortinet	Ransomware.FDL!tr
GData	MSIL.Trojan-Ransom.SamSa.C	Ikarus	Trojan-Ransom.SamSam
K7AntiVirus	Riskware (0040eff71)	K7GW	Riskware (0040eff71)
Kaspersky	HEUR:Trojan.MSIL.Tpyn.gen	MAX	malware (ai score=99)
McAfee	Ransomware-SAMAS!E26C6A20139F	McAfee-GW-Edition	Ransomware-SAMAS!E26C6A20139F
Microsoft	Ransom:MSIL/Samas.A	NANO-Antivirus	Trojan.Win32.Samas.ebgnlh
Palo Alto Networks	generic.ml	Panda	Trj/GdSda.A
Qihoo-360	Win32/Trojan.627	Rising	Malware.Undefined!8.C (TFE:C:InSpTcyuQHT)
SentinelOne	static engine - malicious	Sophos AV	Troj/RansmSam-A
SUPERAntiSpyware	Ransom.SamSam/Variant	Symantec	Trojan.Gen
Tencent	Msil.Trojan.Samas.Aihw	TheHacker	Trojan/Filecoder.Samas.a
TrendMicro	Ransom_CRYPSAM.SM	TrendMicro-HouseCall	Ransom_CRYPSAM.SM
VIPRE	Trojan.Win32.Generic!BT	ViRobot	Trojan.Win32.Z.Samas.217600
Yandex	Trojan.Samas!	ZoneAlarm	HEUR:Trojan.MSIL.Tpyn.gen
Avast Mobile Security	Clean	Baidu	Clean
Bkav	Clean	CMC	Clean
Cyren	Clean	DrWeb	Clean
eGambit	Clean	F-Prot	Clean
Jiangmin	Clean	Kingsoft	Clean
Malwarebytes	Clean	nProtect	Clean
Sophos ML	Clean	TotalDefense	Clean
VBA32	Clean	WhiteArmor	Clean
Zillya	Clean	Zoner	Clean