WannaCry Ransomware Attack

WannaCry Fidye Yazılımı Nedir?

Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

English

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

bitcoin ACCEPTED HERE

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Copy

About bitcoin

How to buy bitcoins?

Contact Us

Check Payment

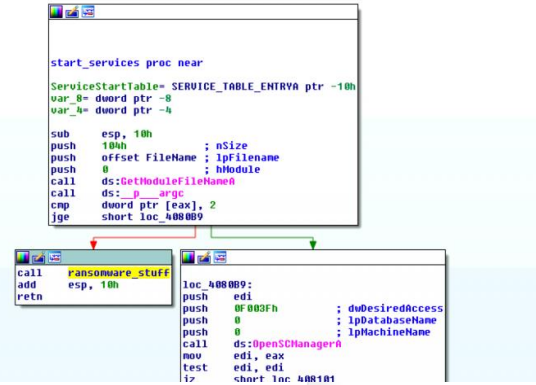
Decrypt

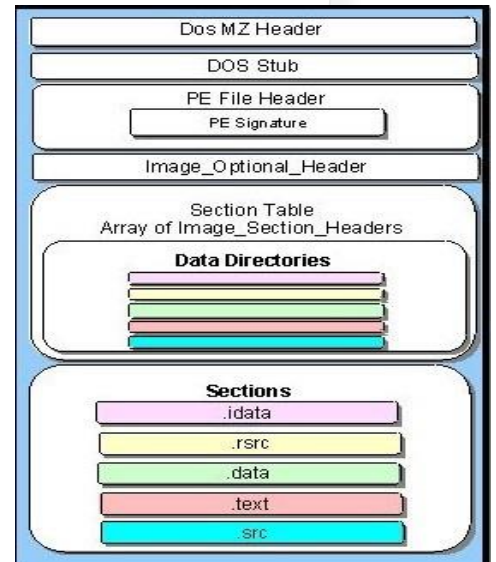
```
Decompile: something_interesting - (wannacry)

undefined4 something_interesting(void)

{
  HINTERNET hInternet;
  HINTERNET hinternet_return;
  int i;
  char *strange_url;
  char *strange_url_copy;
  char strange_url_buffer [57];

  i = 14;
  strange_url = s_http://www.iuqerfsodp9ifjaposdfj_004313d0;
  strange_url_copy = strange_url_buffer;
  while (i != 0) {
    i = i + -1;
    *(undefined4 *)strange_url_copy = *(undefined4 *)strange_url;
    strange_url = strange_url + 4;
    strange_url_copy = strange_url_copy + 4;
  }
  *strange_url_copy = *strange_url;
  InternetOpenA((LPCSTR)0x0,1,(LPCSTR)0x0,(LPCSTR)0x0,0);
  hinternet_return = InternetOpenUrlA(hInternet,strange_url_buffer,(LPCSTR)0x0,0,0x84000000,0);
  if (hinternet_return == (HINTERNET)0x0) {
    InternetCloseHandle(hInternet);
    InternetCloseHandle(0);
    FUN_00408090();
    return 0;
  }
  InternetCloseHandle(hInternet);
  InternetCloseHandle(hinternet_return);
  return 0;
}
```





WannaCry Nedir?

- WannaCry, siber suçlular tarafından para çalmak için kullanılan, bir tür kötü amaçlı yazılım olan, şifreli fidye yazılımlarına örnek olarak gösterilebilir.
- Fidye yazılımı, değerli dosyaları şifreleyerek okumanızı ya da bilgisayarınızı kilitleyerek kullanmanızı engeller.
- Şifreleme yöntemini kullanan fidye yazılımına şifreli fidye yazılımı adı verilir. Bilgisayarınızı kilitleyene ise kilitleyici fidye yazılımı adı verilir.
- Diğer şifreli fidye yazılımı türleri gibi WannaCry da verilerinizi rehin alarak sizden fidye ister.
- WannaCry, işletim sistemi Microsoft Windows olan bilgisayarları hedef alır. Verilerinizi şifreler ve geri vermek için kripto para birimi Bitcoin cinsinden fidye talep eder.

Kim ve Nasıl?

- “TheShadowBrokers” isimli hacker grubu, Nisan ayında National Security Agency’in (NSA) FUZZBUNCH isimli exploit kitini sızdırdı. Sızdırılan bu zafiyet kiti içerisinde bir çok exploit bulunmaktadır. İlgili exploitlerden EternalBlue exploiti yine exploit kiti içerisinde bulunan DOUBLEPULSAR payloadı ile birlikte kullanıldığında Windows işletim sistemlerindeki SMB servisinin zafiyetini kullanarak yönetici haklarında komut çalıştırılmasına olanak sağlamaktadır.
- Aynı zamanda, fidye yazılımı herhangi bir kullanıcı etkileşimi gerektirmeksizin bulaştığı ağda MS17-010 zafiyetinin olduğu sistemleri tarayarak bulmakta ve zafiyet barındıran sistemleri de etkilemektedir.

MS17-010 (CVE-2017-0144) kodu ile isimlendirilen bu zafiyet WannaCry adlı bir fidye yazılımı tarafından kullanılmaya başlandı.

Zararlı Fidye Yazılımı Nasıl Yayılmaktadır?

- Wannacry wormu Windows SMB protokolünü kullanarak yayılmaktadır. NSA tarafından bu açıklığı barındıran sistemlere sızmak için kullanılan bir exploit, NSA'den bu bilgiler sızdırıldığında internet üzerinden yayınlanmaya başladı. Açıklanan belgeler ve bilgiler ışığında biri ya da birileri tarafından bu zafiyeti istismar eden fidye zararlı yazılımı geliştirilerek internete sunuldu.

WannaCry Fidyesinin Ödenmemesi Durumunda Ne Olur?

- Saldırganlar 300 dolar değerinde bitcoin talep etti ve daha sonra fidye talebini 600 dolarlık bitcoin'e çıkardı. WannaCry fidye yazılımı saldırısının kurbanlarına, üç gün içinde fidyeyi ödemezlerse dosyalarının kalıcı olarak silineceği söylendi.Fidye ödemeleri konusunda yapılması gereken, baskıya boyun eğmemektir. Verilerin iade edileceğine dair bir garanti olmadığından ve her yapılan ödeme suçluları ve suçu teşvik edip gelecekte de benzer saldırıların gerçekleşmesine neden olacağından bu durumlarda asla fidye ödemeyin.

Nasıl Önlem Alabilir?

- Kullanılan Microsoft Windows işletim sistemlerinin güncellemelerini kontrol edip 14 Mart 2017 de yayınlanan MS17-010 kodlu yamanın yüklendiğinden emin olunması gereklidir.
- Internete hizmet veren sistemlerden 445/TCP portu açık olan varsa bunları kapatılması.
- Antispam servisinizi oltalama saldırılarına karşı güçlendirin, SPF, DMARC,DKIM kontrolleri mutlaka gerçekleştirin.
- Çalışanlarınızı siber saldırılara karşı bilinçlendirecek bir eğitim programı uygulayın.
- Ağınızdaki güvenlik zafiyetlerini keşfedip erken önlem almak için sızma testi (penetrasyon) mutlaka yaptırın.
- Düzenli olarak yedek almayı ihmal etmeyin.

Hangi İşletim Sistemleri Etkilenmektedir?

- Aktif kullanılan tüm Microsoft Windows işletim sistemleri Wannacry zararlı fidye yazılımından etkilenmektedir.
- Windows XP
- Microsoft Windows Vista SP2
- Windows 7
- Windows 8.1
- Windows RT 8.1
- Windows 10
- Windows Server 2008 SP2 and R2 SP1
- Windows Server 2012 and R2
- Windows Server 2016

WannaCry Saldırısının Nasıl Bir Etkisi Oldu?

- WannaCry fidye yazılımı saldırısı dünya genelinde 230.000 bilgisayarı etkiledi.
- Etkilenen ilk şirketlerden biri de İspanyol operatör şirketi Telefónica'ydı. 12 Mayıs'a kadar Birleşik Krallık'taki binlerce NHS hastanesi ve ameliyatı etkilendi.
- NHS hastane vakıflarının üçte biri saldırıdan etkilendi. Korku verici bir şekilde ambulanslar yanlış yönlendirildi ve acil tıbbi müdahaleye ihtiyacı olan insanlar mağdur oldu. Saldırı sonucunda 19.000 randevunun iptal edilmesi nedeniyle NHS'nin 92 milyon sterlin kaybettiği tahmin ediliyor.
- Fidye yazılımı Avrupa'nın da ötesine yayıldı ve 150 ülkedeki binlerce bilgisayarı kullanılmaz hale getirdi. WannaCry fidye yazılımı saldırısı, dünya genelinde önemli bir finansal etki yarattı. Bu siber suçun dünya çapında 4 milyar dolarlık kayba yol açtığı tahmin edilmektedir.

Kaynakça

- https://www.kaspersky.com.tr/resource-center/threats/ransomware-wannacry
- https://www.bgasecurity.com/2017/05/10-soruda-wannacry-siber-saldirisi/
- https://tr.wikipedia.org/wiki/WannaCry