Paper

Bitdefender®

Everything you need to know about the WannaCry Ransomware

Executive summary

For the past decade or so, increasing tensions between International governments have led to what IT security experts call today "cyberterrorism" – the use of cyberweapons (hacks) to spy on or to commission cyber-attacks overseas. A fair portion of these hacks eventually end up on the 0-Day market as leaked goods, where average cybercriminals can grab the exploit, package it as a new form of malware, and use it for personal gain.

The most recent such example occurred on May 12, 2017 when an unknown group of hackers deployed what was to become the most dangerous ransomware attack ever recorded. **WannaCry**, as the malware is dubbed, leverages a (now patched) 0-Day vulnerability developed by hackers contracted by the NSA.

WannaCry has (so far) infected hundreds of thousands of endpoints in more than 100 countries, causing turmoil for big companies, governmental agencies, and regular users alike. The media has had a blast covering the incident. The hackers, for their part, fetched more than $80,000 in ransom money (and counting). This whitepaper explores the particularities of the WannaCry ransomware and its implications, and offers a look at the technology behind Bitdefender's unrivaled detection process.

Key findings

- The WannaCry ransomware leverages an exploit developed by the NSA
- Malware spread to more than 200,000 endpoints in 3 days' time
- Attack caused major disruption to hospitals, telecom companies, gas and utilities plants
- Independent researcher stopped the spread of the malware through accidental "kill switch"
- Technical analysis suggests that WannaCry authors are one-off hackers
- WannaCry v. 2.0 quickly emerged continuing to spread the malware
- Hackers have amassed more than $80,000 in bitcoins (and counting)
- Bitdefender first security solution to proactively protect against WannaCry

Context

Ransomware is a relatively time-tested piece of malware that encrypts user data and demands a ransom, usually in the form of electronic currency, to decrypt the files.

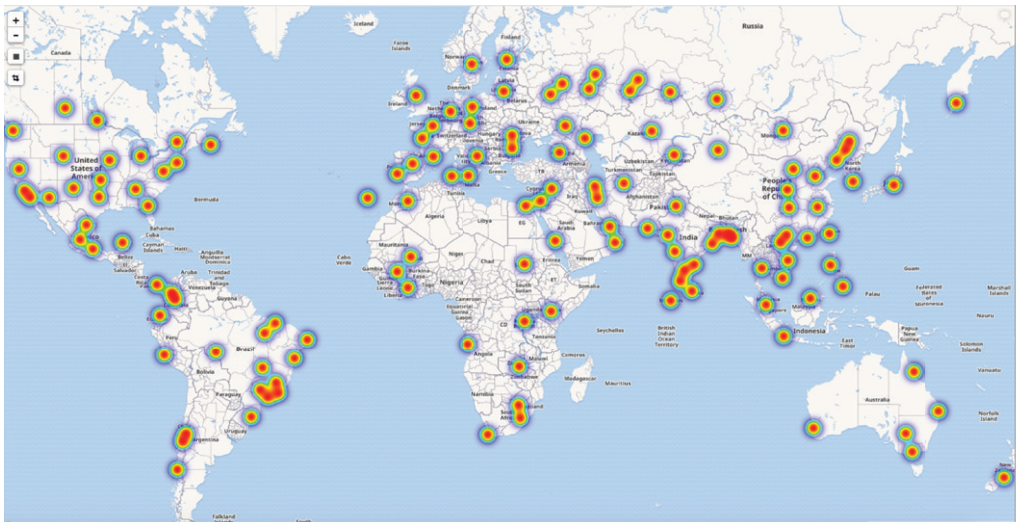
On May 12th, the WannaCryptor (WannaCry) ransomware family infected thousands of computers across the world. In just 24 hours, the number of infections spiked to 185,000 machines in more than 100 countries. That number has more than doubled since.

The attack, it turned out, proved particularly dangerous for businesses because it takes just one employee to become infected for the attack to spread in the entire network, without the endpoint user's interaction. The reason is that WannaCry relies on a worm component that leverages a recently discovered vulnerability, affecting most Windows operating systems in use today, including 2008, 2008 R2, 7, 7 SP1.

The attacks have caused major disruption to hospitals, telecom companies or gas and utilities plants. Among the organizations that took the worst hits is the UK's National Health Service (NHS).

The vector of infection is similar to the one exhibited by the Conficker worm discovered in 2008. Conficker used flaws in Windows and dictionary attacks on administrator passwords to propagate while forming a botnet. Because of its combined use of several malware

techniques, the worm has been particularly difficult to forestall. If history is any indication, WannaCry's wormable component, the EternalBlue exploit, will be used in several new forms of malware in the coming months.



Heatmap of WannaCry infections reported around the globe.

Technical dive into the sample

WannaCry – also dubbed Wanna Decrypter 2.0, WCry, WanaCrypt and WanaCrypt0r – exploits a Windows Server Message Block (SMB) flaw that Microsoft patched almost two months ago (as per the MS17-010 security bulletin). The malware leverages a wormable exploit to spread automatically.

The ransomware binary file contains a number of files embeddes into a ZIP archive password-prtected with the WNcry@2ol7 password. Upon extraction, these files reveal a number of ransom notes translated in a number of languages including Bulgarin, Chinese, Croatian, Czech, Danish, Dutch, English, Filipino, Finnish, French, German, Greek, Indonesian, Italian, Japanese, Korean, Latvian, Norwegian, Polish, Portuguese, Romanian, Russian, Slovak, Spanish, Swedish, Turkish and Vietnamese.

Along with these language files, there are a number of other resources, including the Bitcoin wallets where the payments should be made in, a list of hard-coded command and control servers registered on the TOR network, as well as a minified TOR application that is installed before connecting to the C&Cs.

Other files present in the ZIP archive are as follows: a file holding the list of formats to be encrypted, an image file with text-based instructions that gets set as wallpaper, a tool that elevates the malware's privileges, a second tool, a decryption utility that monitors the Bitcoin transaction and decrypts if a ransom has been paid.

Before dropping anything, the isolated WannaCry samples ping a website to see if it responds. If the respective website (http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com) IS accessible, the payload execution stops. If the website is inaccessible, the malware goes on with the unpacking process.

One of the samples we analyzed (db349b97c37d22f5ea1d1841e3c89eb4) uses source code from [RiskSense's implementation] of the MS17-010 payload. Additionally, buffers form the [PacketStorm implantation of MS17-010] can also be found in the analyzed sample.

Digging into the decryptor

The decryptor component ships with a private RSA key. It is used to decrypt the decryption key for the payload, as the payload is encrypted symmetrically with the AES-ecb128 algorithm.

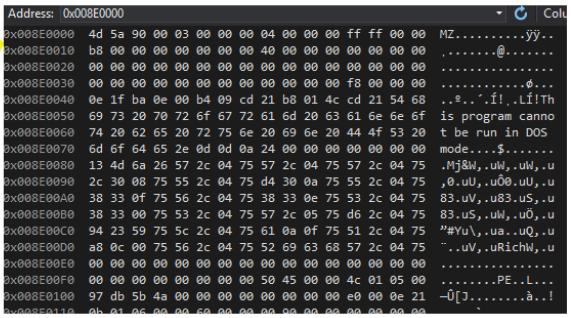
[WannaCrypt 2.0] Malware partially cracked

Payload decryption is made with AES_cbc_128 and an IV={0}. The RSA key decrypts the AES128 key for the payload – algorithm replication:

```
if (s_size_2 < 0x6400000)
{
    CryptDecrypt(hkey, 0, TRUE, 0, local_buf, &size_decrypt);
    memcpy(USER_AES_KEY, local_buf, sizeof(USER_AES_KEY));

    //aes_init
    buffer_in = (BYTE*)VirtualAlloc(0, 0x10118, MEM_COMMIT, PAGE_READWRITE);
    buffer_out = (BYTE*)VirtualAlloc(0, 0x10118, MEM_COMMIT, PAGE_READWRITE);
    ReadFile(hf, buffer_in, 0x10118, &read, 0);
    AES_set_decrypt_key(USER_AES_KEY, 128, &aes_ctx);

    i = 0;
    memset(ivec, 0, 16);
    while (i < 0x10118)
    {
        AES_ecb_encrypt(buffer_in + i, buffer_out + i, &aes_ctx, AES_DECRYPT);
        for (j = 0; j < 16; j++)
            buffer_out[i+j] ^= ivec[j];
        memcpy(ivec, buffer_in + i, 16);
        i += 16;
    }
}
```



Mutex check

```
int __stdcall TaskStart(HMODULE hModule, int a2)
{
  void *v2; // eax@9
  int v3; // esi@10
  HANDLE v4; // eax@17
  HANDLE v5; // eax@19
  HANDLE v6; // ebx@21
  HANDLE v7; // eax@21
  HANDLE v8; // eax@23
  HANDLE v10; // esi@28
  WCHAR PathName; // [sp+10h] [bp-214h]@3
  char v12; // [sp+12h] [bp-212h]@3
  __int16 v13; // [sp+216h] [bp-Eh]@3
  int v14; // [sp+220h] [bp-4h]@9

  if ( a2 || CheckMutexPresence() )
    return 0;
  PathName = word_1000D918;
  memset(&v12, 0, 0x204u);
  v13 = 0;
  GetModuleFileNameW(hModule, &PathName, 0x103u);
```

```
signed int __cdecl CheckMutexPresence()
{
  HANDLE v0; // esi@1
  signed int result; // eax@3

  v0 = CreateMutexA(0, 1, "MsWinZonesCacheCounterMutexA");
  if ( v0 && GetLastError() == 183 )
  {
    CloseHandle(v0);
    result = 1;
  }
  else
  {
    result = 0;
  }
  return result;
}
```

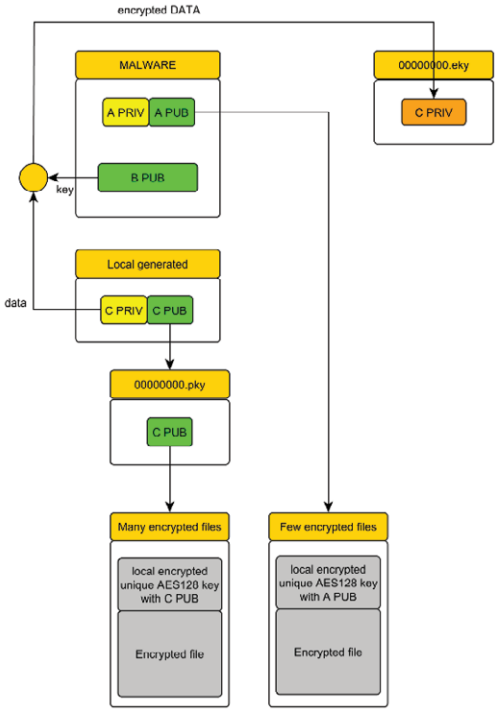
Second mutex check (private key present):

```
sprintf(res_fname, "%08X.res", 0);
sprintf(pky_fname, "%08X.pky", 0);
sprintf(eky_fname, "%08X.eky", 0);
if ( CreateMutex(0) || PrivateKeyExists(0) )
{
  v10 = CreateThread(0, 0, sub_10004990, 0, 0, 0);
  WaitForSingleObject(v10, 0xFFFFFFFFu);
  CloseHandle(v10);
  return 0;
}
v2 = operator new(0x28u);
v14 = 0;
if ( v2 )
  v3 = InitCriticSec(v2);
```

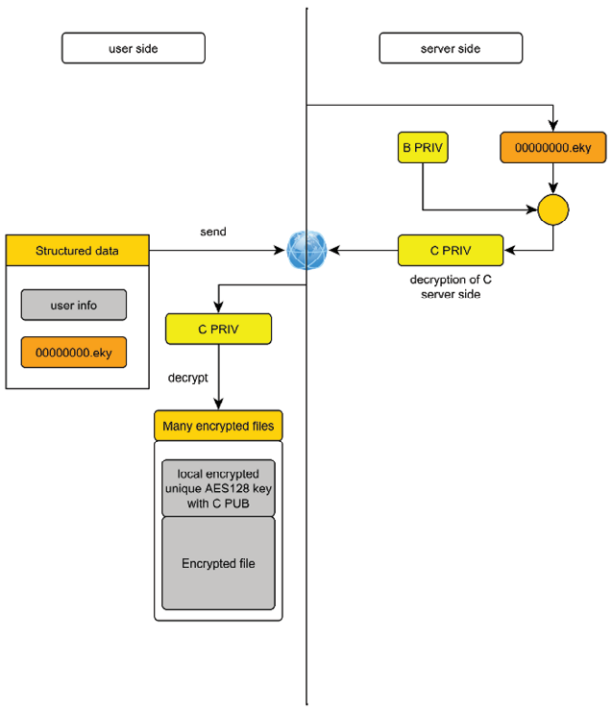
```
signed int __cdecl CreateMutex(int a1)
{
  HANDLE v1; // eax@1
  signed int result; // eax@2
  HANDLE v3; // esi@3
  char Name; // [sp+4h] [bp-64h]@3

  v1 = OpenMutexA(0x100000u, 1, "Global\\MsWinZonesCacheCounterMutexW");
  if ( v1 )
  {
    CloseHandle(v1);
    result = 1;
  }
  else
  {
    sprintf(&Name, "%s%d", "Global\\MsWinZonesCacheCounterMutexA", a1);
    v3 = CreateMutexA(0, 1, &Name);
    if ( v3 && GetLastError() == 183 )
    {
      CloseHandle(v3);
      result = 1;
    }
    else
    {
      sub_100013E0(v3);
      result = 0;
    }
  }
  return result;
}
```

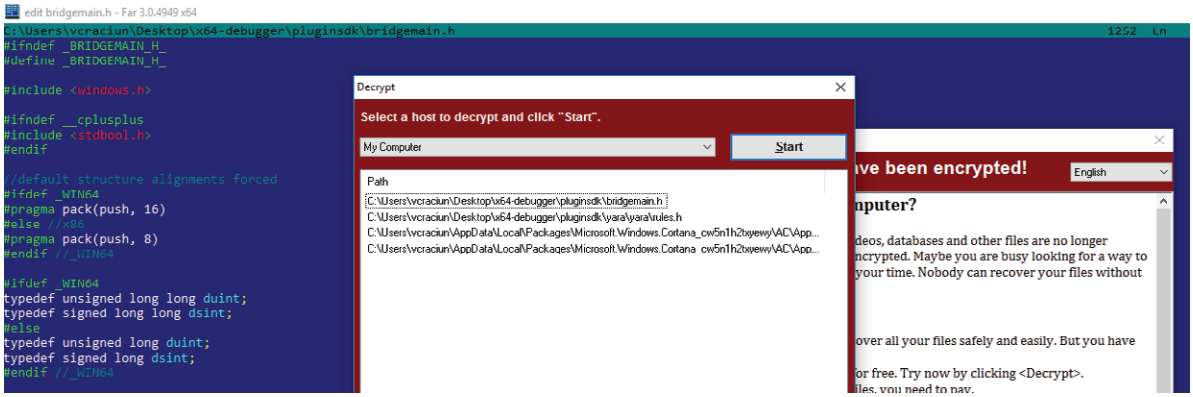
Encryption:



Decryption:



Decryption of a few samples:



"Killswitch"

As the ransomware was making the rounds collecting thousands by the hour from victims worldwide, an independent security researcher (that goes by the malwaretech handle) accidentally found a killswitch that stopped the spread of the malware – *version 2.0 would later emerge to continue to collect ransom money from new victims.*

His only action was to register the domain name pinged by the malware in order to spread. Once registered, the domain – now a valid one – prevented the worm component from replicating the malware across other endpoints on a network.

```
int __stdcall WinMain(HINSTANCE hInstance, HINSTANCE hPrevInstance, LPSTR lpCmdLine, int nShowCmd)
{
  HINTERNET handle; // esi@1
  HINTERNET _result; // edi@1
  int result; // eax@2
  const CHAR szUrl; // [sp+8h] [bp-50h]@1
  char v8; // [sp+40h] [bp-18h]@1
  int v9; // [sp+41h] [bp-17h]@1
  int v10; // [sp+45h] [bp-13h]@1
  int v11; // [sp+49h] [bp-Fh]@1
  int v12; // [sp+4Dh] [bp-Bh]@1
  int v13; // [sp+51h] [bp-7h]@1
  __int16 v14; // [sp+55h] [bp-3h]@1
  char v15; // [sp+57h] [bp-1h]@1

  memcpy((void *)&szUrl, "http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com", 0x38u);
  v8 = aHttpWww_iuqerf[56];
  v9 = 0;
  v10 = 0;
  v11 = 0;
  v12 = 0;
  v13 = 0;
  v14 = 0;
  v15 = 0;
  handle = InternetOpenA(0, 1u, 0, 0, 0);
  _result = InternetOpenUrlA(handle, &szUrl, 0, 0, 0x84000000u, 0);
  if ( _result )
  {
    InternetCloseHandle(handle);
    InternetCloseHandle(_result);
    result = 0;
  }
  else
  {
    InternetCloseHandle(handle);
    InternetCloseHandle(0);
    check_params();
    result = 0;
  }
  return result;
}
```

Exit if connection is successfull

The main application (the main dropper which contains the exploit) has execution conditions tied to a particular URL: http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com. The application halts execution if interrogation of InternetOpenUrlA() ends with success.

Recommendations

As of now, EternalBlue is no longer a 0-Day exploit. But that doesn't make it any less dangerous, as many computers out there remain unpatched, or are not running any anti-malware solutions. Despite the apparently massive scale of this attack, WannaCry actually took little advantage of the military-grade EternalBlue exploit. The hackers were also quite imprudent. They hard coded their Bitcoin wallets into the malware, and they used a rudimentary decryption key delivery system – no way to track each victim to send them back the decryption key once they've paid the ransom money. However, for all their (apparent) amateurism, it worked. And the malware continues to rake in cash for the authors.

Steps to avoid WannaCry infection:

1. Install the Microsoft-issued patch
2. Disable the Server Message Block service on the computer if patching is impossible.
3. Back up your data on offline media. The ransomware malware will encrypt files on external drives, such as external hard drives, USB sticks, or any network or cloud file store if connected to the compromised computer.
4. Update your software – make sure you have all Windows updates installed
5. Use a trusted security solution. You can find out more about the performance of your security solution in reports issued by independent anti-malware testing organizations:

Bitdefender Active Threat Control (ATC) and Hypervisor Introspection (HVI)

To protect your business against WannaCry and other similar ransomware waves, all of Bitdefender's endpoint security solutions employ effective machine-learning-based detection.

Bitdefender **Active Threat Control** (ATC) is a pro-active and dynamic detection technology, based on monitoring processes and system events, and tagging suspicious activities. It has been designed to act against never-before-seen threats based on their behavior.

To further enhance protection against similar attack waves, businesses can completely seal their infrastructure against zero-days or unpatched vulnerabilities by employing **Hypervisor Introspection** (HVI) to protect their virtual workloads.

HVI is able to pick up exploits by looking directly into the memory. Before the exploit can compromise your systems, HVI will block it. On endpoints, protection against WannaCry is ensured by machine learning. The more systems are protected, the less leverage the malware has to spread.

Conclusion

Bitdefender has been training models for detecting and thwarting ransomware for years using patented machine learning algorithms. With the introduction of machine learning technologies for detection purposes in 2009, Bitdefender has become the undisputed leader in malware detection and prevention. To date, 10 percent of Bitdefender patents pertaining to machine-learning algorithms for detecting malware and other online threats, deep learning and anomaly-based detection techniques.

In addition to the next generation detection technologies, Bitdefender's revolutionary Hypervisor Introspection technology allows unparalleled visibility from the hypervisor level while enforcing the integrity of the antimalware solution.

Authors

Filip TRUTA - Security Specialist
Vlad CRACIUN - Malware Researcher

Bitdefender is a global security technology company that delivers solutions in more than 100 countries through a network of value-added alliances, distributors and reseller partners. Since 2001, Bitdefender has consistently produced award-winning business and consumer security technology, and is a leading security provider in virtualization and cloud technologies. Through R&D, alliances and partnership teams, Bitdefender has elevated the highest standards of security excellence in both its number-one-ranked technology and its strategic alliances with the world's leading virtualization and cloud technology providers. More information is available at
http://www.bitdefender.com/

FOR MORE INFORMATION VISIT: enterprise.bitdefender.com

BD-Business-Aug.01.2017-TK#: crea1572