Posted on

BitRAT Disguised as Windows Product Key Verification Tool Being Distributed

The ASEC analysis team has recently discovered BitRAT which is being distributed via webhards. Because the attacker disguised the malware as Windows 10 license verification tool from the development stage, users who download illegal crack tools from webhard and install it to verify Windows license are at risk of having BitRAT installed into their PC.

The following shows a post that was uploaded to webhard, one that harbors the malware. The title is [New][Quick Install]Windows License Verification[One-click].

Figure 1. Post disguised as download of Windows license verification tool — 1

Figure 2. Post disguised as download of Windows license verification tool — 2

A compressed file named 'Program.zip' is downloaded, and it is compressed and locked with a password '1234'. It contains a Windows 10 license verification tool named 'W10DigitalActivation.exe'.
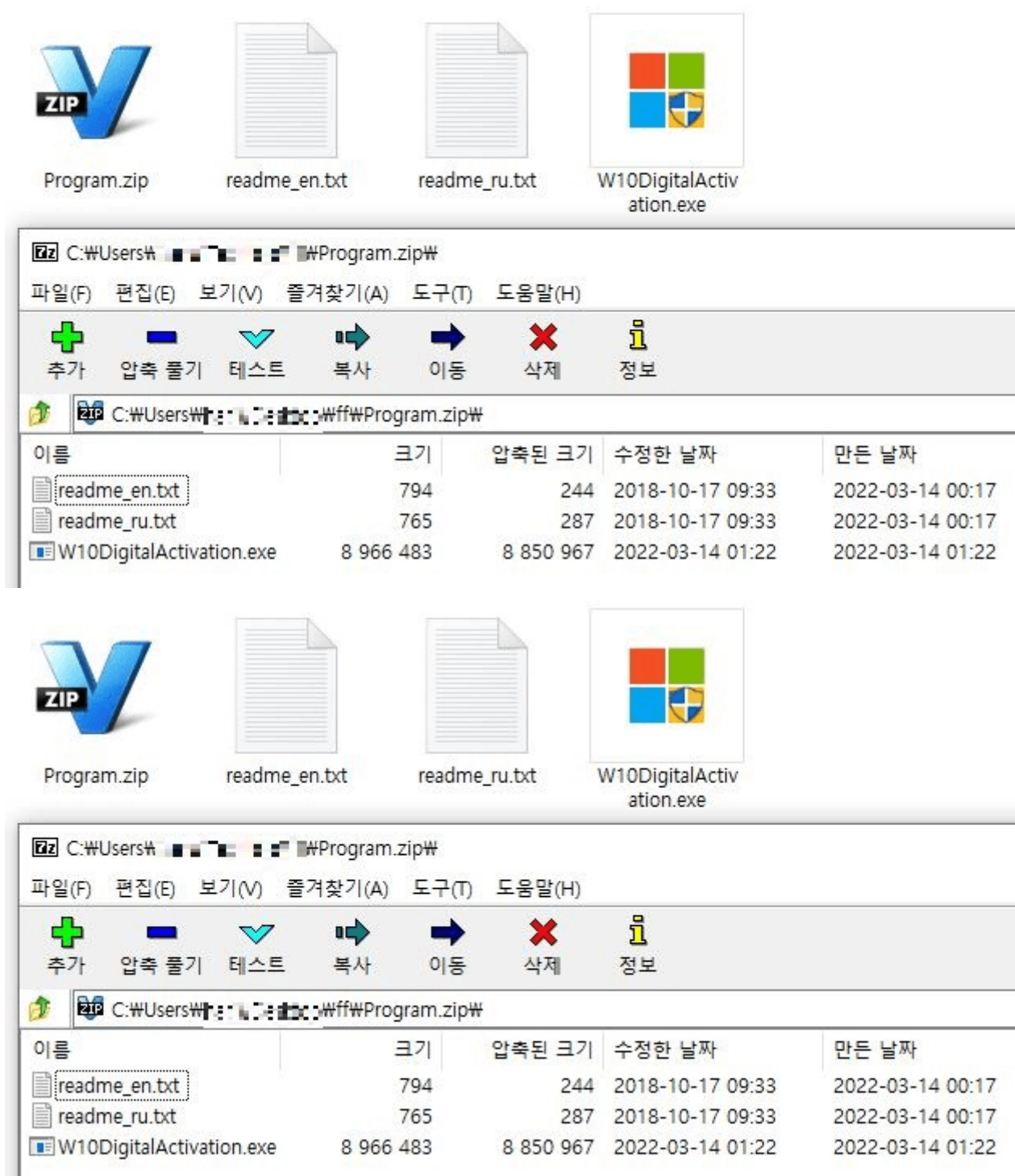
Figure 3. Files included in compressed file

'W10DigitalActivation.exe' is a 7z SFX file that carries an actual verification tool called 'W10DigitalActivation.msi' and the malware named W10DigitalActivation_Temp.msi. When the user double-clicks the file, it installs both files concurrently. As both the malware and the verification tool are run at the same time, the user is tricked into thinking that the tool is running properly as shown below.
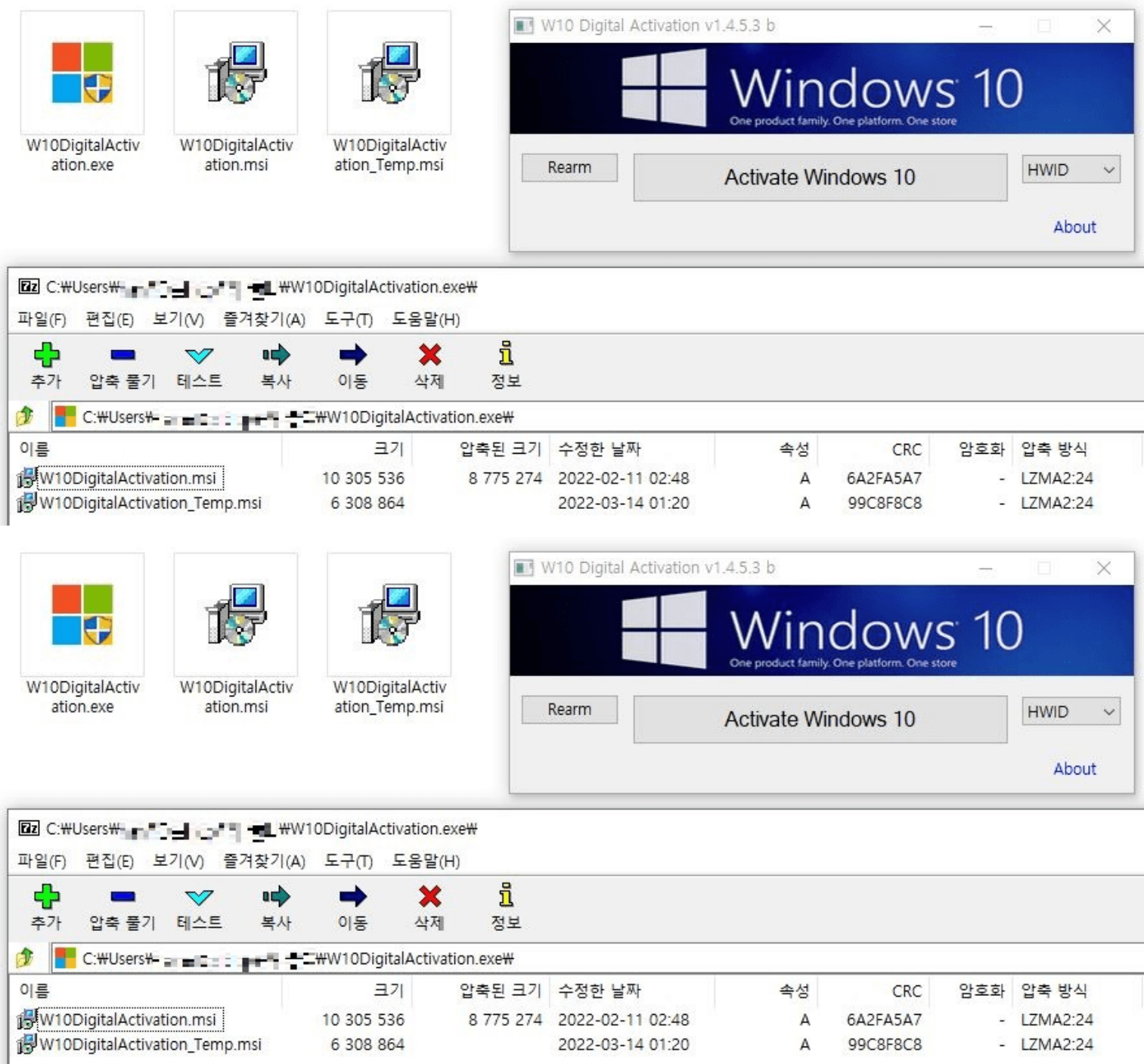
Figure 4. Malware inside 7z SFX file

Unlike its name, 'W10DigitalActivation_Temp.msi' is a downloader with exe extension that downloads additional malware. When run, it connects to following C&C servers it harbors internally, exchanging encrypted strings. Afterward, it decrypts the strings to ultimately acquire a download URL for the additional payload.
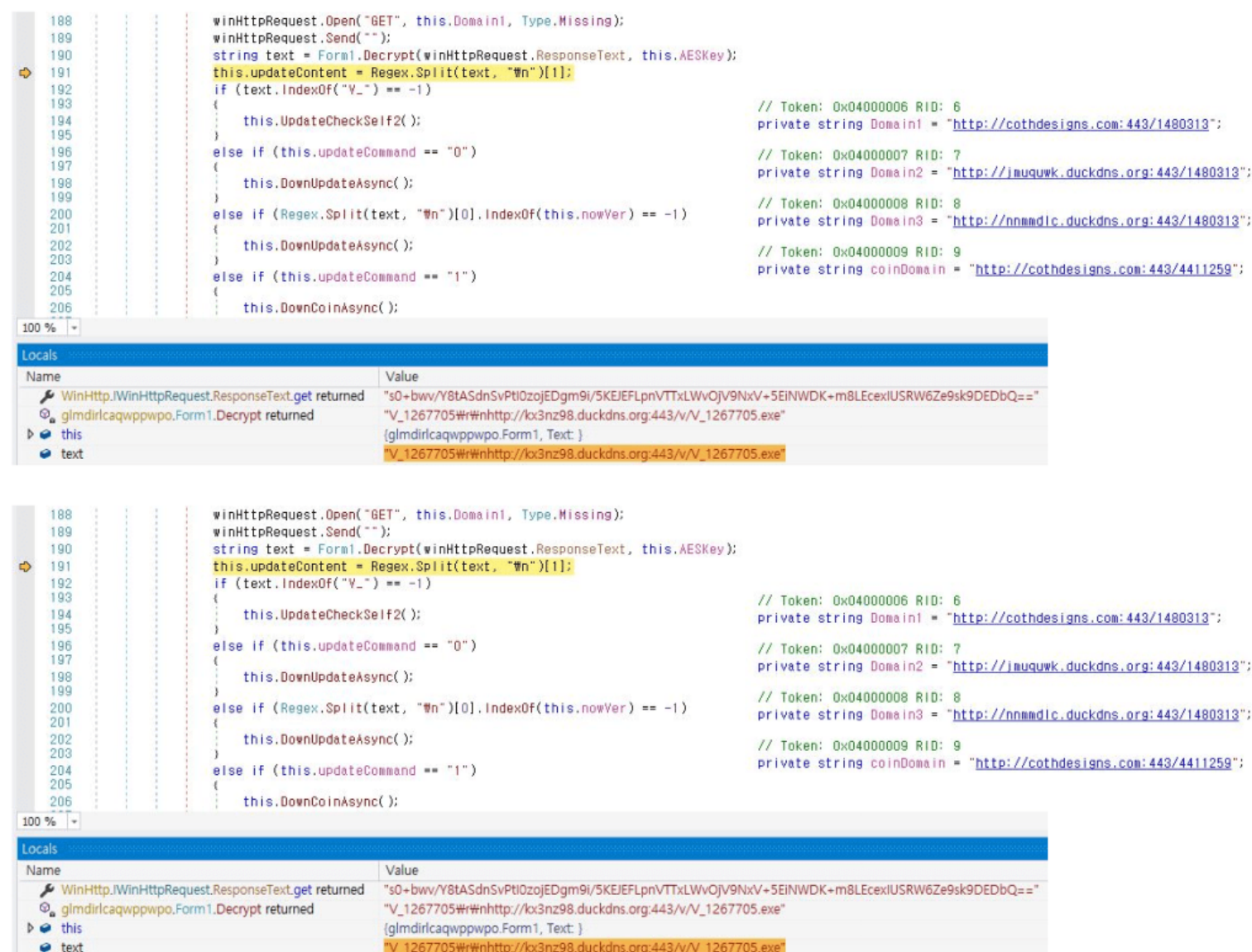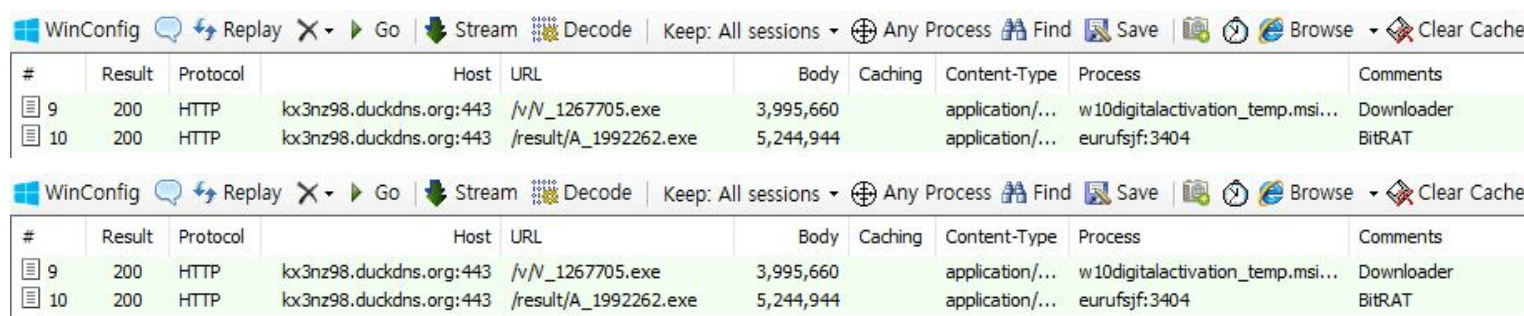

Figure 5. C&C URL of downloader malware

The downloader installs the malware into the Windows startup program folder and deletes itself. Normally, the first file that is installed is a downloader of the same kind, and the downloader run this way ultimately installs BitRAT into the path %TEMP% as 'Software_Reporter_Tool.exe'.

#	Result	Protocol	Host	URL	Body	Caching	Content-Type	Process	Comments
9	200	HTTP	kx3nz98.duckdns.org:443	/v/V_1267705.exe	3,995,660		application/...	w10digitalactivation_temp.msi...	Downloader
10	200	HTTP	kx3nz98.duckdns.org:443	/result/A_1992262.exe	5,244,944		application/...	eurufsjf:3404	BitRAT

#	Result	Protocol	Host	URL	Body	Caching	Content-Type	Process	Comments
9	200	HTTP	kx3nz98.duckdns.org:443	/v/V_1267705.exe	3,995,660		application/...	w10digitalactivation_temp.msi...	Downloader
10	200	HTTP	kx3nz98.duckdns.org:443	/result/A_1992262.exe	5,244,944		application/...	eurufsjf:3404	BitRAT

Figure 6. Downloading downloader and BitRAT

Note that this downloader is equipped with additional features and is not a simple program by any means. As shown in the figure below, one of its features uses a powershell command to add the Windows startup program folder——where the downloader will be installed——as an exclusion path for Windows Defender, and adding the BitRAT process name 'Software_Reporter_Tool.exe' as an exclusion process for Windows Defender.

Figure 7. Adding as Windows Defender exclusion path

Seeing how this malware uses webhard which is considered as the most-used file-sharing platform in Korea and includes Korean characters in its code as shown in the figure below, it appears that the attacker is a Korean speaker.

```
// Token: 0x06000006 RID: 6 RVA: 0x000022D0 File Offset: 0x000004D0
private static bool IsAdministrator()
{
    WindowsIdentity current = WindowsIdentity.GetCurrent();
    return current != null && new WindowsPrincipal(current).IsInRole(WindowsBuiltInRole.Administrator);
}

// Token: 0x06000007 RID: 7 RVA: 0x000022F8 File Offset: 0x000004F8
private bool check2019(string path)
{
    FileInfo fileInfo = new FileInfo(path);
    Console.WriteLine("생성 시간 : " + fileInfo.CreationTime.ToString());
    return fileInfo.CreationTime.ToString().Substring(0, 4) == "2019";
}

// Token: 0x06000006 RID: 6 RVA: 0x000022D0 File Offset: 0x000004D0
private static bool IsAdministrator()
{
    WindowsIdentity current = WindowsIdentity.GetCurrent();
    return current != null && new WindowsPrincipal(current).IsInRole(WindowsBuiltInRole.Administrator);
}

// Token: 0x06000007 RID: 7 RVA: 0x000022F8 File Offset: 0x000004F8
private bool check2019(string path)
{
    FileInfo fileInfo = new FileInfo(path);
    Console.WriteLine("생성 시간 : " + fileInfo.CreationTime.ToString());
    return fileInfo.CreationTime.ToString().Substring(0, 4) == "2019";
}
```

Figure 8. Code that contains Korean characters

The malware that is ultimately installed is a RAT (Remote Access Trojan) malware called BitRAT. BitRAT has been in sale via a hacking forum since 2020 and is being continuously used by attackers.

Figure 9. Image of BitRAT introduction — 1
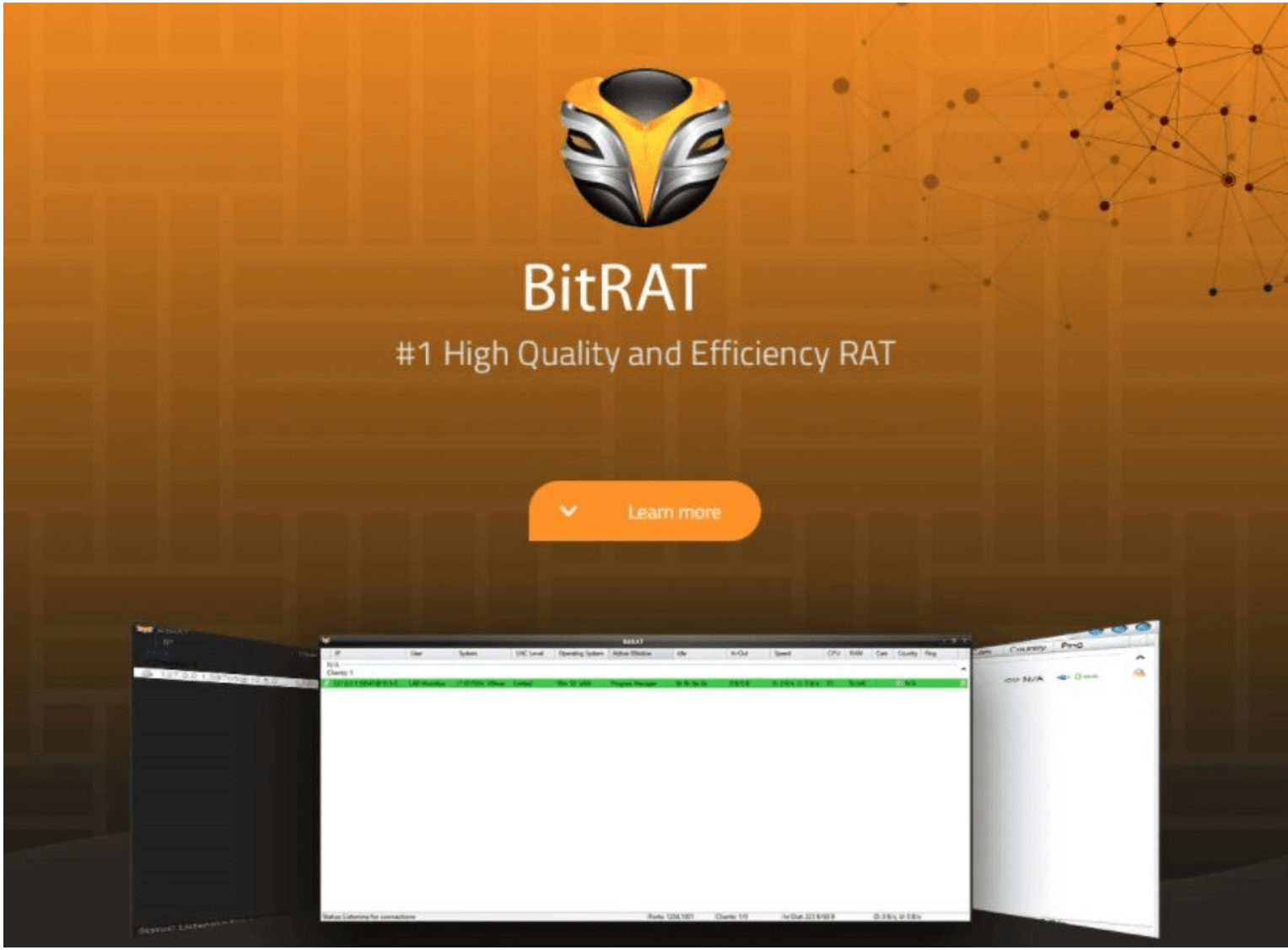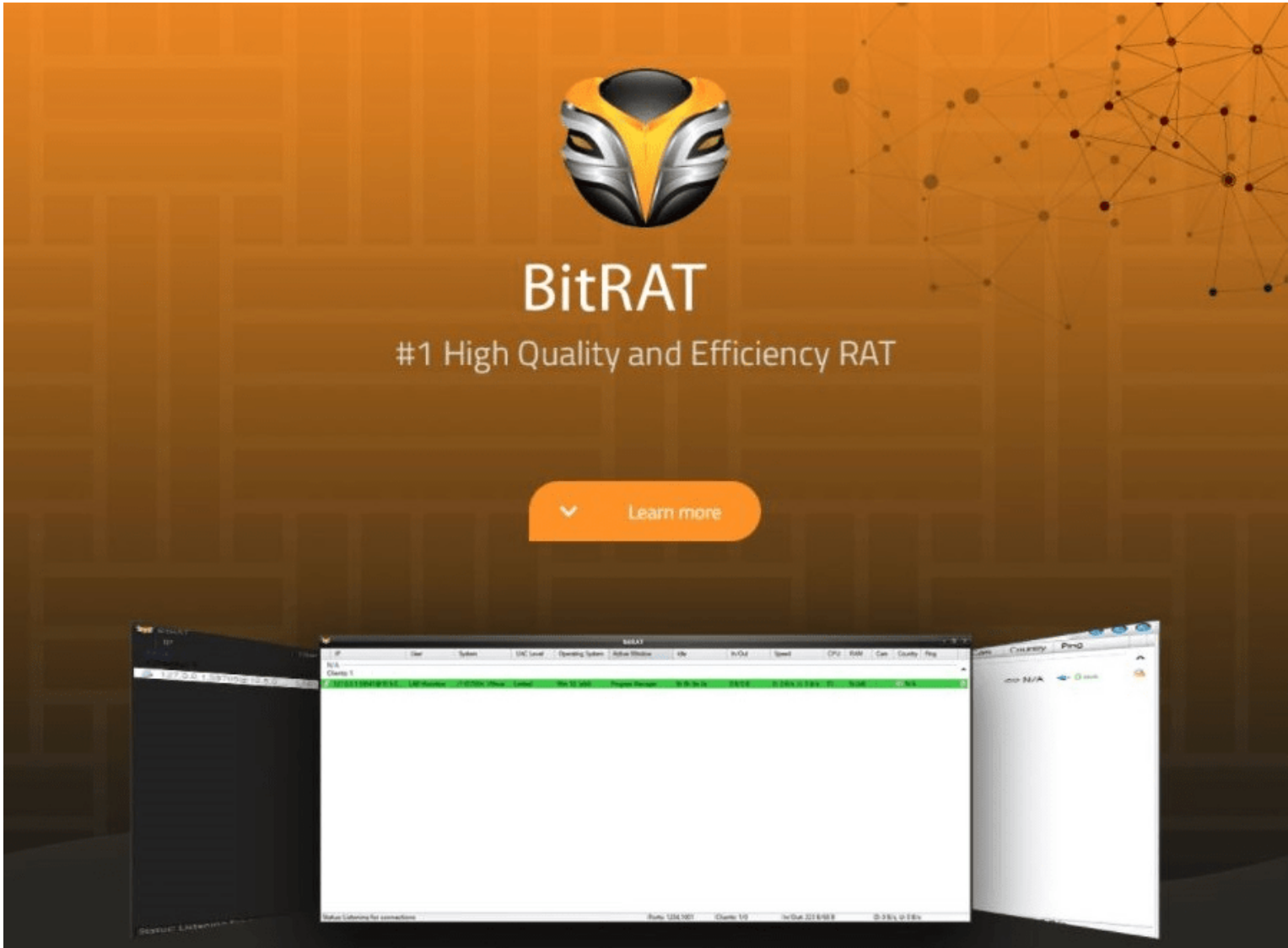
Figure 10. Image of BitRAT introduction — 2

Because BitRAT is a RAT malware, its attacker can gain control of the system infected with it. BitRAT not only provides basic control features such as running process tasks, service tasks, file tasks, and remote commands, but also provides extra options such as various info-stealing features, HVNC, remote desktop, coin mining, and proxies.
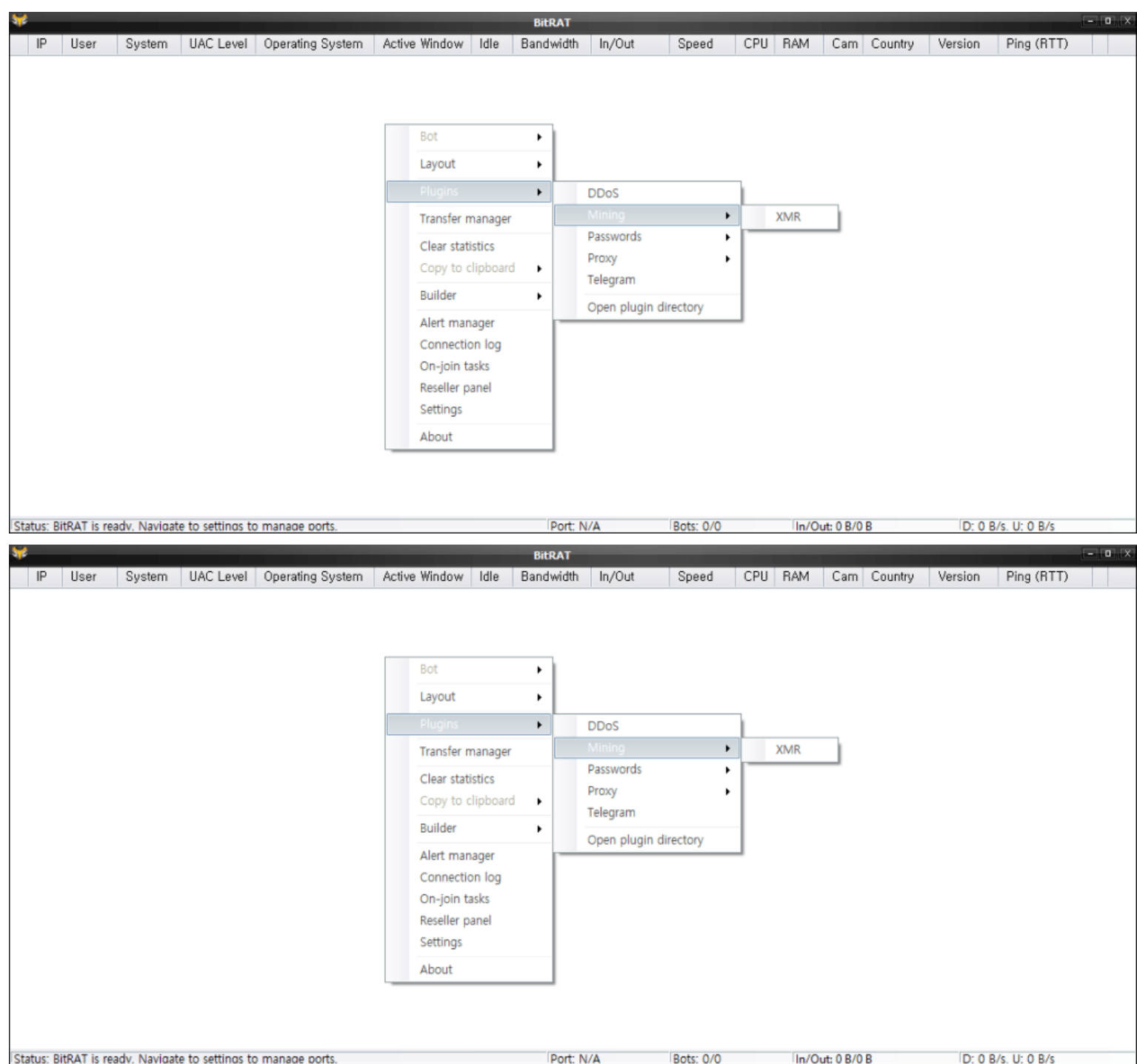
Figure 11. BitRAT C&C panel

The following is the list of the features that BitRAT provides.

1. Network Communication Method — Encrypted communication using TLS 1.2 — Communication using Tor

2. Basic Control — Process manager — Service manager — File manager — Windows manager — Software manager

3. Information Theft — Keylogging — Clipboard logging — Webcam logging — Audio logging — Application (e.g. Web browsers) account credential theft

4. Remote Control — Remote desktop — hVNC (Hidden Desktop)

5. Proxy — SOCKS5 Proxy: port forwarding feature using UPnP — Reverse Proxy: SOCKS4 Proxy

6. Coin Mining — XMRig CoinMiner

7. etc. — DDoS attack — UAC Bypass — Windows Defender deactivation

Note that BitRAT uses the revealed TinyNuke's code, just like AveMaria. The following is a comparison of TinyNuke's hVNC (routine related to Hidden Desktop) and BitRAT's code.

Figure 12. TinyNuke and BitRAT's hVNC routine

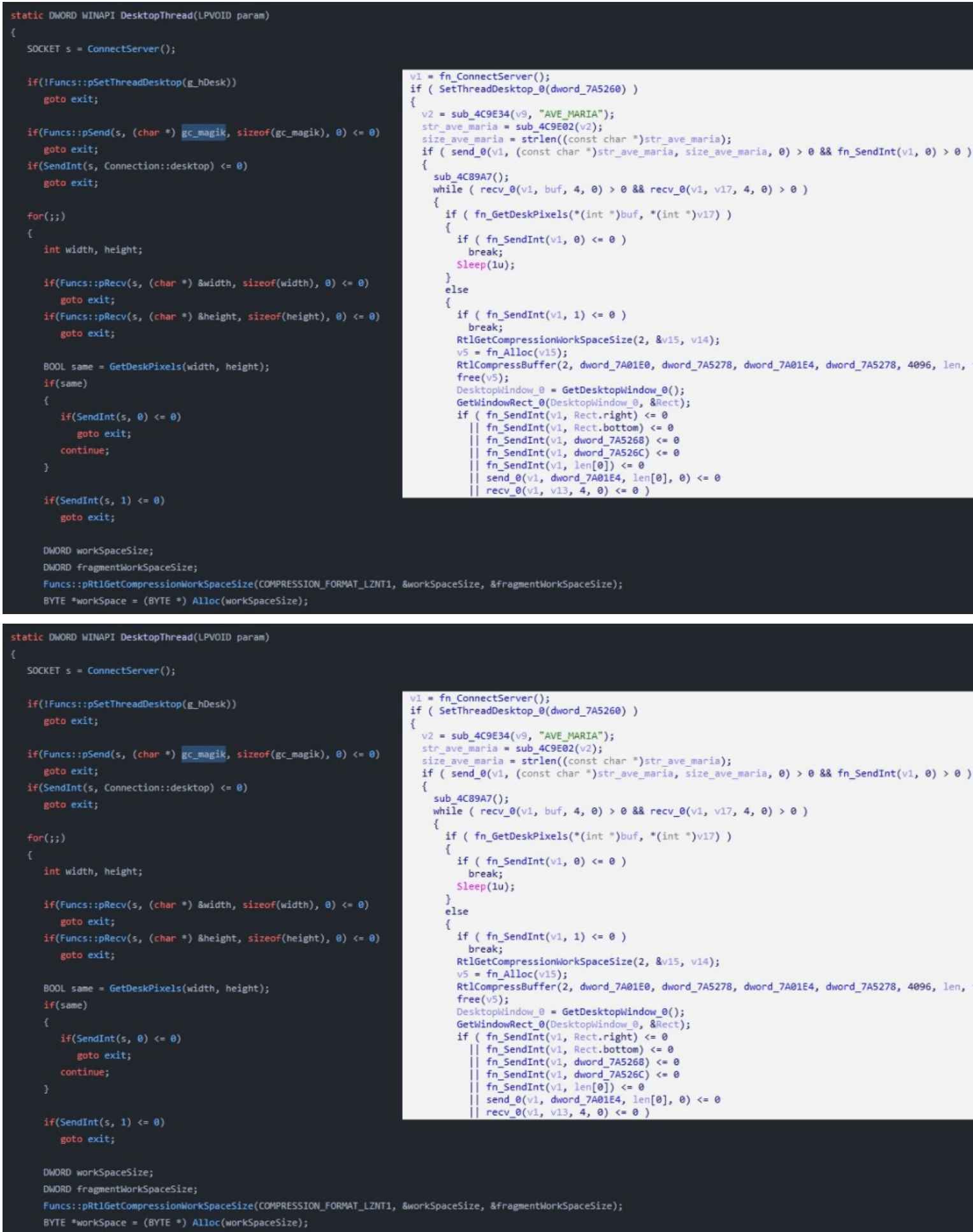TinyNuke verifies and uses a signature string called 'AVE_MARIA' in Reverse SOCKS4 Proxy and Hidden Desktop feature. AveMaria, on the other hand, adopted Reverse SOCKS4 Proxy feature from TinyNuke, and the name was given based on the string. BitRAT used Hidden Desktop feature, and the signature string is the same.

Note that TinyNuke was used by the Kimsuky group in the past. Among myriad of features, only the Hidden Desktop feature was adopted and used.

- [ASEC Blog] VNC Malware (TinyNuke, TightVNC) Used by Kimsuky Group
- [ASEC Blog] AveMaria malware being distributed as spam mail

As shown in the examples above, the malware is being distributed actively via file-sharing websites such as Korean webhards. As such, caution is advised when running executables downloaded from a file-sharing website. It is recommended for the users to download products from the official websites of developers.

AhnLab's anti-malware software, V3, detects and blocks the malware above using the aliases below.

[File Detection] — Trojan/Win.MalPacked.C5007707 (2022.03.12.04) — Dropper/Win.BitRAT.C5012624 (2022.03.16.02) — Downloader/Win.Generic.C5012582 (2022.03.16.01) — Downloader/Win.Generic.C5012594 (2022.03.16.01) — Backdoor/Win.BitRAT.C5012593 (2022.03.16.01) — Backdoor/Win.BitRAT.C5012748 (2022.03.16.02)

[Behavior Detection] — Malware/MDP.AutoRun.M1288

[IOC] Dropper MD5 6befd2bd3005a0390153f643ba248e25

Downloader malware MD5 60ee7740c4b7542701180928ef6f0d53 c4740d6a8fb6e17e8d2b21822c45863b

BitRAT MD5 b8c39c252aeb7c264607a053f368f6eb e03a79366acb221fd5206ab4987406f2 ea1b987a7fdfc2996d5f314a20fd4d99 54ef1804c22f6b24a930552cd51a4ae2

Downloader malware's C&C Server — hxxp://cothdesigns[.]com:443/1480313 — hxxp://cothdesigns[.]com:443/4411259 — hxxp:// jmuquwk.duckdns[.]org:443/1480313 — hxxp://nnmmdlc.duckdns[.]org:443/1480313

Additional Payload Download URL — Downloader — hxxp://kx3nz98.duckdns[.]org:443/v/V_1267705.exe — hxxp://108.61.207[.]100:443/v/ V_5248849.exe

Additional Payload Download URL — BitRAT — hxxp://kx3nz98.duckdns[.]org:443/v/A_1992262.exe — hxxp://108.61.207[.]100:443/result/ A_1146246.exe

BitRAT C&C — z59okz.duckdns[.]org:5223 — cothdesigns[.]com:80

Subscribe to AhnLab's next-generation threat intelligence platform 'AhnLab TIP' to check related IOC and detailed analysis information.

Categories:Malware Information

Tagged as:BitRAT, rat, TinyNuke, webhard