ASEC Report

Vol. 91

Q2 2018

AhnLab

ASEC REPORT

VOL.91 Q2 2018

ASEC (AhnLab Security Emergency Response Center) is a global security response group consisting of malware analysts and security experts. This report is published by ASEC and focuses on the most significant security threats and latest security technologies to guard against such threats. For further details, please visit AhnLab, Inc.'s homepage (www.ahnlab.com).

SECURITY TREND OF Q2 2018

Table of Contents

SECURITY ISSUE

- Executive Summary of Operation Red Gambler

Security Issue

Executive Summary of Operation Red Gambler

AhnLab has identified a hacker group that targeted South Korean users of gambling games for over 11 months from October of 2016 to August of 2017. This latest discovery is noteworthy for uncovering an operation that targeted individual users for financial gain instead of attempting to extract confidential information from enterprise systems.

AhnLab Security Emergency-response Center (ASEC) has termed the attack Operation Red Gambler after a close examination of the malware's methodology and target. This report examines the latest activities of the hacker group as well as the principal method of dissemination, changes in victim selection, and other detailed analysis of the attack.

Figure 1-1 | Online gambling game

Operation Red Gambler Attack Pattern

1. Overview

Online gambling sites offering poker or other card games allow players to bet their game money and collect their winnings. Such sites and games have long been targeted by criminals and con artists since in-game money

can be exchanged for real money via illegal game money exchanges or other nefarious channels.

Criminal organizations targeting such gambling sites are composed of the organizer, managers, grifters and malware developers as shown in Figure 1-2.

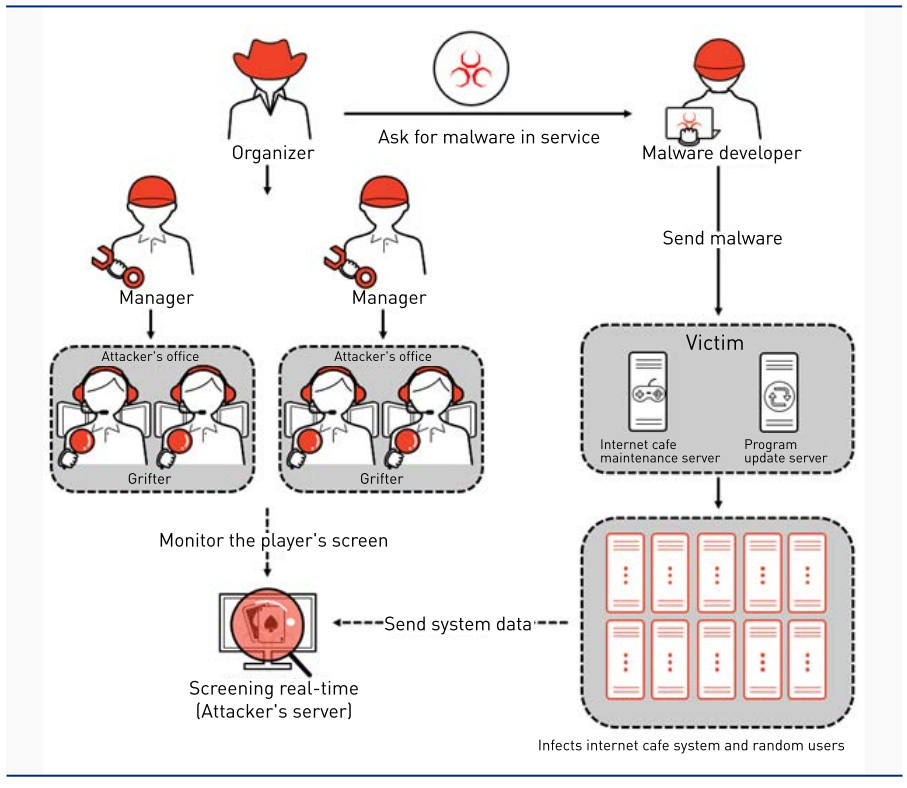


Figure 1-2 | Organizational structure of attack groups

2. Targets

The malware developed by this hacker group was first discovered in October of 2016, initially targeting multiple random users using utility programs. A new spate of attacks took place in January of 2017, which this time chose internet cafés as the new target. When the previous year's attacks on random users turned out to be less effective, the malware appears to have switched targets to internet cafés where multiple clients are controlled by one or a few maintenance servers. This new set of attacks continued until August of 2017.

3. Attack Pattern

To ensure the success of their attacks, the hacker group distributed their malware by doctoring the software setup file or manipulating the internet café's maintenance program.

3-1) Altering utility application setup files

Attacks using utility software as the vector began to turn up from October, 2016, with the point of origin identified as the utility's official website. The hacker group made changes to the setup

file uploaded and made available from the site's download page or altered the download link.

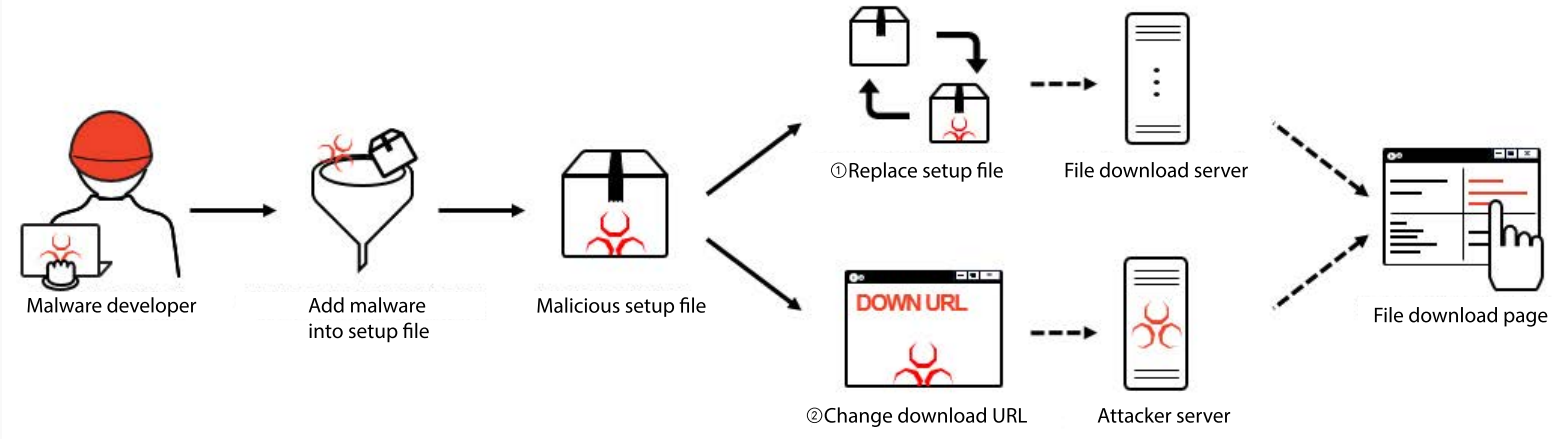


Figure 1-3 | Attack pattern using the utility software setup file

3-2) Propagation via internet café maintenance program

This form of attack via the maintenance programs used by internet cafés was discovered in the first half of 2017. The hacker group appeared to have disseminated their malware by exploiting the structure of most internet cafés that use a handful of servers to control a larger number of clients.

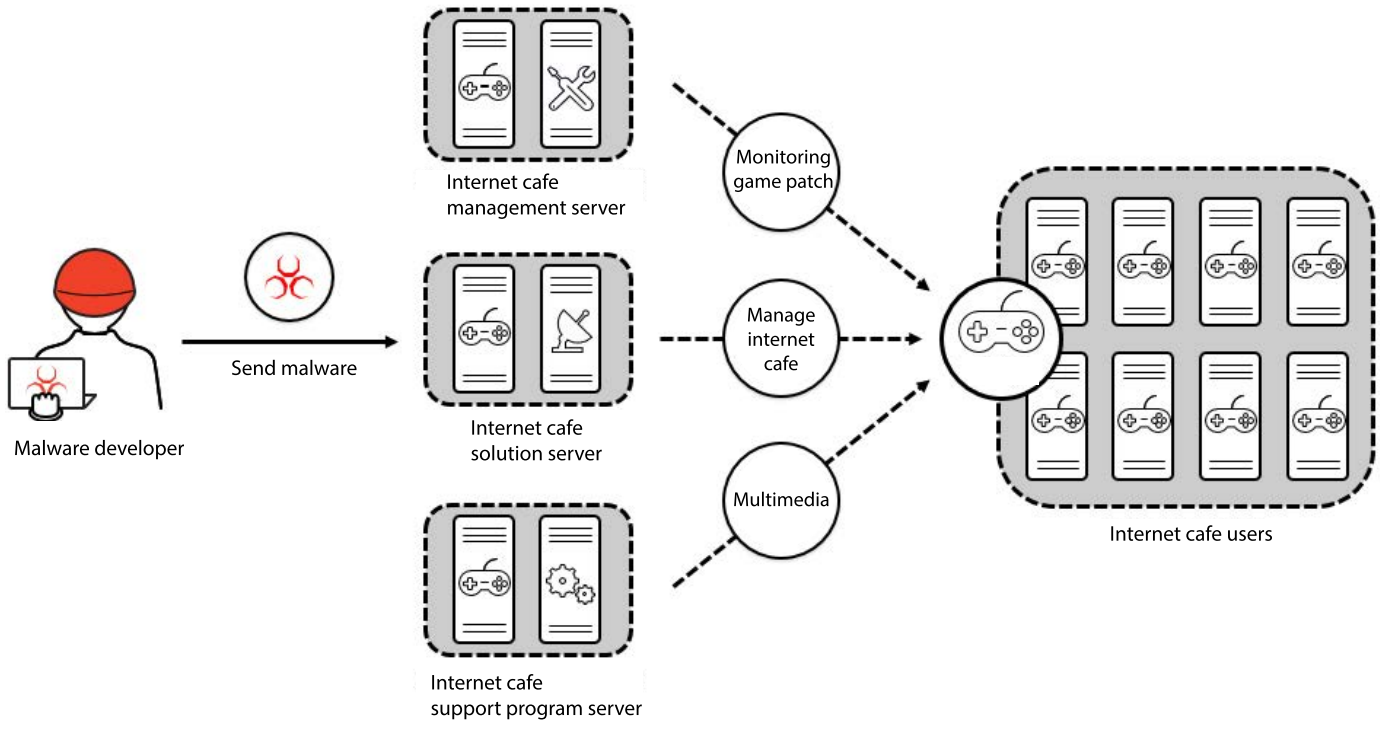


Figure 1-4 | Attack via internet café servers

Detailed Analysis

The malware employed by this attack group circumvents the user account control (UAC) function of Windows to run itself as administrator.

The UAC security feature was first introduced with Windows Vista, and limits what applications are run based on admin authorization in order to prevent security issues that may impact the system. Permission is based on administrator or user access, and tasks that can affect the system such as making changes to the registry or creating and deleting files in the system folder will first be checked by a user account control popup message demanding administrator access.

To skip over this procedure, the attack employs registry hijacking using the Microsoft management console (MMC). The MMC is a tool for managing the system's configurations through console document files (MSC files).

When Event Viewer, a Windows service that lets users view the event logs, is executed, data is read and run in two registry locations according to the assigned sequence. Since the process takes place at high integrity level, files can be run with administrator permission when adding file directory paths in the registry data.

The malware adds the location of the file in the registry data, then runs Event Viewer. The service then runs the malware with administrator permission, circumventing the UAC security feature.

Now executed with administrator rights, the malware activates its dropper function to decode two encrypted files embedded within itself, writing additional files to a directory location. These

additional files, taskeng.exe and wrmk.dll, are entered into the task scheduler and automatically run taskeng.exe activates wrmk.dll in pre-set intervals.

Having been activated with taskeng.exe, wrmk.dll then calls its internal function StartChk() to begin its malicious attack, and wrmk.dll uses the hook function SetWindowsHookExA() to inject itself into the current active process. This process continues for 24 hours, with five-second pauses between each cycle.

The injected library file then read the information of the target process. This information includes the file location and name, and wrmk.dll checks whether the process is a game on its list of targets for attack. If the process is verified as a target game, new threads for each type of game is called and the malware attempts to extract the user's in-game information.

The malware is armed with a memory hacking attack for extracting information, as the gambling game's user information is stored in a memory location.

The code for each type of game is different since each uses a different memory location for storing user information; nevertheless, the memory hacking code are all designed to identify the memory location to be hacked and extract information such as the game name and channel, and transmit the hijacked information to a C&C server. The code also takes a screenshot of the game that is underway, which is encrypted along with the user and game information acquired earlier and sent to the C&C server.

The names of the game being played, channel and match and the screenshot sent to the C&C

server can now be monitored by the attacker's master program. This allowed the attacker to essentially read all the cards of the players in the game, and set up the unsuspecting mark for a con.

A variant that appeared from the second half of 2017 shows marked differences from the previous strains, in that the shellcode and DLL are not created in-system but in a memory location.

The A attack group continued to disseminate different variants of this malware, apparently to deal with the fact that new gambling games constantly appear and internet cafés make use of recovery solutions to protect their systems.

Response from AhnLab

The relevant aliases identified by AhnLab's security solutions are as below:

- AhnLab MDS: Malware/MDP.Download
- AhnLab V3: Trojan/Win32.GameHack

Conclusion

Having mounted a series of attacks against targets in South Korea since 2016, this particular hacker group appears to have diversified its targets by initiating cyber attacks against individual users in addition to businesses and government organizations that it had targeted earlier.

The hacker group responsible for these attacks is expected to continue its malicious operations with the aim of profiting from its victims, and close cooperation between government agencies and data security companies as well as vigilance on the part of individual users will be required to prevent and deal with these attacks.

ANALYSIS IN-DEPTH

- From Variants to Kill Switches: All about GandCrab

Analysis-In-Depth

From Variants to Kill Switches: All about GandCrab

GandCrab has left an unmistakable trail of destruction in South Korea. First distributed via vulnerable web sites early this year, numerous new variants of the ransomware are being spotted in the second half of 2018 after April, spreading widely across the country. Especially worrisome have been new fileless variants that function not as a single executable file but run only in the system's memory to encrypt targeted files.

AhnLab's Security Emergency-response Center (ASEC) has been closely tracking GandCrab and its variant siblings. These efforts have led to the discovery of the ransomware's kill switch and a solution for preventing the damage from GandCrab, which was made available to clients using AhnLab's security solutions. This report provides a detailed review of the behaviors of different GandCrab variations, major infection vectors and the newly-discovered kill switch.

Propagation method

GandCrab infections primarily take the form of either a fileless infection or via an executable file.

1. Fileless distribution

Fileless variants of GandCrab can be classified into GandCrab v2.1, GandCrab v2.1 (internal

version 3.0.0), and GandCrab v3.0. Let us examine each version in further detail.

1-1) GandCrab v2.1

A version of GandCrab using the fileless technique was first discovered in early April, 2017. This variant was pushed out by the Magnitude exploit kit.

When a user lands on the source web site, the user's system is corralled into accessing certain URLs via mshta.exe, rundll32.exe and WMIC.exe, normal Windows processes. The URL contains the payload in JavaScript form.

When the malicious script is activated, the Base64-encoded DLL image embedded in the code is decoded and run in the memory. The decoded DLL image injects another DLL image, the core payload of GandCrab v2.1, into explorer.exe and runs it. Thus the fileless variant of GandCrab runs the payload in the system's memory instead of dropping or downloading the malicious JavaScript or PE image as a file.

AhnLab has verified a kill switch that prevents GandCrab's file encryption under certain parameters.

The presence of a particular 10-byte piece of data in a Text.txt file prevents the ransomware from encrypting any files in the directory or its subdirectories. In other words, placing a copy of the Text.txt file containing this set of data in each drive root directory will protect the drive's files from encryption. The following are examples of files that would be placed in particular hard drive root directories, with Figure 2-1 indicating the data inside Text.txt:

• C:\Text.txt (locks C drive from encryption)

• D:\Text.txt (locks D drive from encryption)

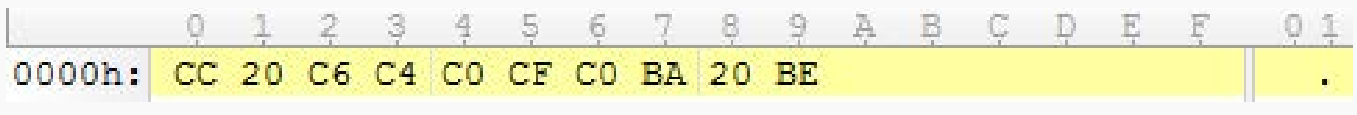
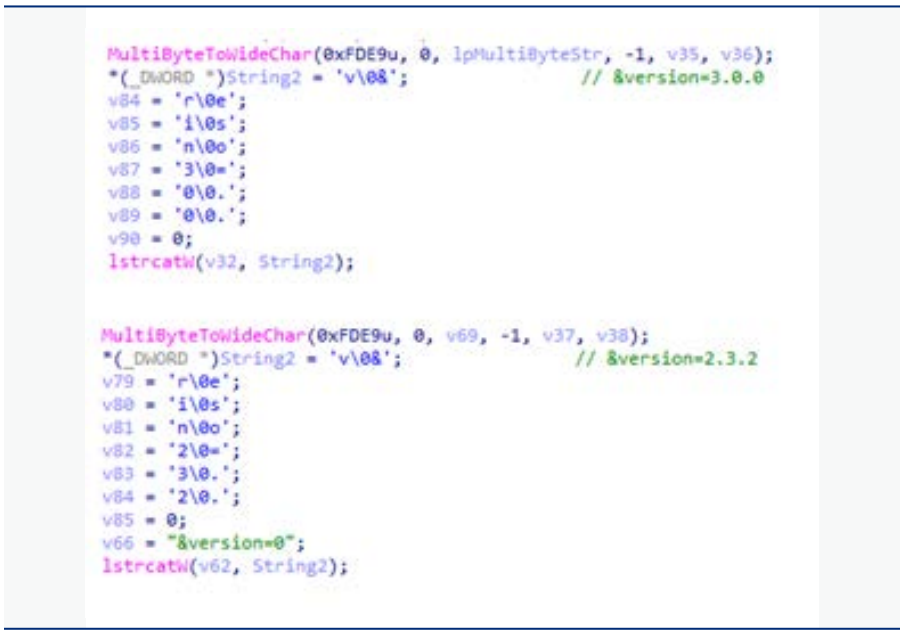


Figure 2-1 | Kill switch data inside Text.txt

1-2) GandCrab v2.1 (internal version 3.0.0)

The next variant to be examined is identical on the surface with the previously-discussed GandCrab v2.1, but contains a different hardcoded version within the DLL file that performs the actual encryption attack from what is displayed in the ransom note. Analysis revealed that while the ransom note displays the ransomware's version as GandCrab v2.1, the actual internal version that the attacker sees is v3.0.0, as shown in Figure 2-2. Another GandCrab variant that was discovered around the same time also indicated GandCrab v2.1 in the ransom note but v2.3.2 internally.



```
MultiByteToWideChar(0xFDE9u, 0, lpMultiByteStr, -1, v35, v36);
*(_DWORD *)String2 = 'v\0&';                    // &version=3.0.0
v84 = 'r\0e';
v85 = 'i\0s';
v86 = 'n\0o';
v87 = '3\0=';
v88 = '0\0.';
v89 = '0\0.';
v90 = 0;
lstrcatW(v32, String2);


MultiByteToWideChar(0xFDE9u, 0, v69, -1, v37, v38);
*(_DWORD *)String2 = 'v\0&';                    // &version=2.3.2
v79 = 'r\0e';
v80 = 'i\0s';
v81 = 'n\0o';
v82 = '2\0=';
v83 = '3\0.';
v84 = '2\0.';
v85 = 0;
v66 = "&version=0";
lstrcatW(v62, String2);
```

Figure 2-2 | GandCrab variants with different internal versions

The data, along with the encrypted system's unique ID and encryption key, is relayed to the attacker via HTTP connection. The DLL file designated internally as version 3.0.0 shows the binary build date as April 23, 2018 (UTC), indicating that the perpetrators have been engaged in fabricating and spreading malware until recently.

A kill switch that prevents GandCrab v2.1(internal version 3.0.0) from encrypting the affected system's files under certain conditions has also been found.

When GandCrab v2.1 is run, a popup window containing the message shown in Figure 2-3 appears if there is a file or folder named MalwarebytesLABs in the root C:\ directory. The malicious process halts itself before activating the file encryption phase of the attack until the user clicks on the popup message. When the message appears, the user should not click the "OK" button or close the popup, instead immediately shutting down the computer to prevent the ransomware from mangling the system's files.

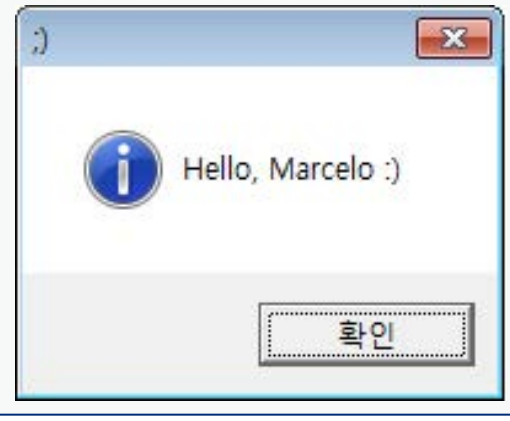


Figure 2-3 | Message popup that appears when GandCrab is run

As message only appears when the C:\MalwarebytesLABs file or folder is present, the following two countermeasures are available:

Method 1) Create a folder named 'MalwarebytesLABs' in the C:\ root directory.

Method 2) Create a file named 'MalwarebytesLABs' (no extension) in the C:\ root directory.

1-3) GandCrab v3.0

Following the appearance of GandCrab v2.0, a newer fileless version of the ransomware appeared around late April to early May, 2018. GandCrab v3.0 exhibits marked differences in its attack pattern compared to v2.0.

An examination of GandCrab v3.0's distribution script shows that it has been encoded as a

landing page of the Magnitude exploit kit. The script is subsequently decoded in two steps into different formats.

GandCrab v3.0 uses a fileless method instead of dropping the decoded .NET DLL into the local directory. In other words, the .NET DLL runs in the memory of iexplorer.exe in which the script has been executed.

When the DLL is run via the propagation script, a new thread is spawned where the shellcode contained in each file's variables array is run as a thread. The shellcode downloads and runs the DLL payload.

2. Distribution as an executable file

GandCrab ransomware that is distributed as an executable file can be classified into GandCrab v2.0, commonly disguised as a fake resume or a regular utility program, and GandCrab v3.0, masquerading as a resume file sent out in spammed email.

2-1) Disguised as an application or normal utility program (GandCrab v2.0)

Analysis of GandCrab ransomware collected by AhnLab revealed that GandCrab v2.0 spreads itself by masking its source, file name and other details as applications or ordinary utility programs.

2-2) Disguised as a resume via spammed emails (GandCrab v3.0)

In early May, version 3.0 of GandCrab appeared that used social engineering methods to target human resource managers using job search web sites by disguising itself as a job seeker's resume. A link in an email purporting to be from a prospective candidate tricks the

reader into clicking a link in the body of the email, which takes the user to a ransomware download page. The system becomes infected with GandCrab when the user downloads and runs a compressed file labeling itself as a resume.

The attacker tries to entice the unsuspecting user into clicking the link by adding a brief introductory message and phrasing such as “resume enclosed”. Clicking the link sends the user to the download page that contains the compressed malware file.

Uncompressing the file produces a script file as shown in Figure 2-4, which is obfuscated and appears to be indecipherable text.

```
040666271ie62703471267a677124312iie' +
'262b7170722073 6f797a293179202a2f207d202f2a206f2b6b6769386b3136767171613736296661343864733471292062712 02a2
f207d293b202f2a206424ie646921726f39' + '6268282824372978306d7161716f202826202a2f20';

function sfyqk(ntrzkmcvsemyr) {
    return (new Function(ntrzkmcvsemyr)());
}

function rmcvvwal(min, max) {
    return Math.floor(Math.random() * (max - min + 1)) + min;
}

function jspuqyyax(pmcoxdptrz) {
    var gccwd = pmcoxdptrz.toString();
    var ntrzkmcvsemyr = "";
    for (var i = 0; i < gccwd.length; i += 2) ntrzkmcvsemyr += String.fromCharCode(parseInt(gccwd.substr(
    i, 2), 16));
    return ntrzkmcvsemyr;
}
while (true) {
    var hljtnjwa = rmcvvwal(0, 107);
    var bmoxborozo = jspuqyyax(jrgamxplwy.replace(/i/g, hljtnjwa));
    if (bmoxborozo.indexOf("function") !== -1) {
        sfyqk(bmoxborozo);
        break;
    }
}
```

Figure 2-4 | Obfuscated script

Decoding the script reveals the ransomware delivery page URL and other information and the existence of a function that accesses the server to download and run the ransomware.

Infection and encryption methodology

1. Infection pattern

As noted above, the three versions of GandCrab ransomware reviewed in this report can be classified as v2.0, v2.1 and v3.0, with each version presenting slight differences in the encryption target, exceptions and other attack patterns.

As shown below, Table 2-1 outlines the similarities and differences between the various versions of GandCrab.

<table>
<tr><th></th><th>v2.0</th><th>v2.1</th><th>v3.0</th></tr>
<tr><td rowspan="6">Similarities</td><td colspan="3">Identical set of information transmitted to the C&C server:
- common IP, PC_USER, PC_NAME, PC_GROUP, language, OS version, OS bit,
identifier, file storage drive information</td></tr>
<tr><td colspan="3">Ransom note name (CRAB-DECRYPT.txt) and extension (CRAB) after encryption of affected files</td></tr>
<tr><td colspan="3">Encryption exception file paths and names (Table 6)</td></tr>
<tr><td colspan="3">Processes shut down (Table 7)</td></tr>
<tr><td colspan="3">List of antivirus products for verification (Table 8)</td></tr>
<tr><td colspan="3">Encryption method (see below for details)</td></tr>
<tr><td rowspan="4">Differences</td><td colspan="3">Extensions exempt from encryption</td></tr>
<tr><td>.ani, .cab, .cpl, .cur, .diagcab,
.diagpkg, .dll, .drv, .hlp, .icl,
.icns, .ico, .ics, .lnk, .key, .idx,
.mod, .mpa, .msc, .msp,
.msstyles, .msu, .nomedia,
.ocx, .prf, .rom, .rtp, .scr, .shs,
.spl, .sys, .theme,.themepack,
.exe, .bat, .cmd, .CRAB, .crab,
.GDCB, .gdcb, .gandcrab,
.yassine_lemmou</td><td>v2.0 plus one additional extension .ldf
(43 total)</td><td>Identical to v2.1(43 total)</td></tr>
<tr><td colspan="3">Desktop manipulation function</td></tr>
<tr><td>No changes to desktop</td><td>No changes to desktop</td><td>Desktop changed([Figure 2-5])</td></tr>
</table>

Table 2-1 | GandCrab similarities and differences by version

In addition, certain directories and file names are left untargeted by the ransomware's encryption, as shown in Table 2-2.

Untargeted file paths		Untargeted file names	
\ProgramData\	Ransomware	desktop.ini	boot.ini
\IETldCache\	\All Users\	autorun.inf	ntuser.dat.log
\Boot\	\Local Settings\	ntuser.dat	thumbs.db
\Program Files\	\Windows\	iconcache.db	CRAB-DECRYPT.txt
\Tor Browser\		bootsect.bak	

Table 2-2 | File locations and names left untouched

Processes that are shut down by GandCrab are shown as follows in Table 2-3.

msftesql.exe	xfssvccon.exe	ocomm.exe	onenote.exe
sqlagent.exe	mydesktopservice.exe	mysqld.exe	outlook.exe
sqlbrowser.exe	agntsvc.exeisqlplussvc.exe	mysqld-nt.exe	powerpnt.exe
sqlservr.exe	xfssvccon.exe	mysqld-opt.exe	steam.exe
sqlwriter.exe	mydesktopservice.exe	dbeng50.exe	thebat.exe
oracle.exe	ocautoupds.exe	sqbcoreservice.exe	thebat64.exe
ocssd.exe	agntsvc.exeagntsvc.exe	excel.exe	thunderbird.exe
dbsnmp.exe	agntsvc.exeencsvc.exe	infopath.exe	visio.exe
synctime.exe	firefoxconfig.exe	msaccess.exe	winword.exe
mydesktopqos.exe	tbirdconfig.exe	mspub.exe	wordpad.exe
agntsvc.exeisqlplussvc.exe			

Table 2-3 | Processes targeted for shutdown

Finally, GandCrab will change the desktop screen of the infected system. Figure 2-5 shows the desktop of a computer infected by GandCrab v3.0.

Figure 2-5 | Desktop screen of a system infected by GandCrab v3.0

2. Encryption methodology

As reviewed earlier in Table 2-4 outlining the various characteristic of each GandCrab version, the ransomware uses the same method for encrypting the infected system's files. The process is further explained below.

GandCrab versions after v2.0 use public key-based encryption. A random key byte is generating for each targeted file, which is then encrypted using AES-256 encryption with the random key byte encrypted again with the attacker's public key. To decrypt the affected files, this personal key would thus have to be acquired from the attacker.

GandCrab's encryption process is as follows: first, a pair of public and private keys is created locally, and the key values are transmitted to the attacker's C&C server. The attacker then sends his public key to the infected PC to be used to encrypt the random key value generated in the victim's local PC. In other words, the files cannot be recovered unless this personal key for the public key received from the attacker's C&C server is known.

Building a Connection

ASEC has analyzed the two attack groups, the hacking group for Operation Red Gambler and GandCrab. The malicious code used in the latest series of attacks was found to share notable similarities in their encryption and decryption code patterns with previous attacks, including the theft of authorization keys from I company in February of 2016, a hacking attack on a defense company in April of 2016 and a government agency two months later, and an ATM hacking incident in March, 2017.

Response from AhnLab

The relevant aliases identified by AhnLab's anti-malware solution, V3, are as below:

- Fileless variants of GandCrab

	Alias
Blocking network infiltration	malware_gandcrab_c2_init-1(HTTP)
Infection diagnostics	Malware/MDP.Ransom.M1928
	Malware/MDP.Create.M1925

- Executable-file strains of GandCrab

	Alias
Blocking network infiltration	malware_gandcrab_c2_init-1(HTTP)
Infection diagnostics	Malware/MDP.Ransom.M1171
	Malware/MDP.Create.M1179
	Malware/MDP.Ransom.M1907
File diagnostics	Trojan/Win32.RansomCrypt
	Trojan/Win32.Gandcrab
	Win-Trojan/Gandcrab.Exp

ASEC REPORT

Vol.91
Q2 2018

AhnLab

Contributors **ASEC Researchers**
Editor **Content Creatives Team**
Design **Design Lab**

Publisher **AhnLab, Inc.**
Website **www.ahnlab.com**
Email **global.info@ahnlab.com**