THREAT RESEARCH

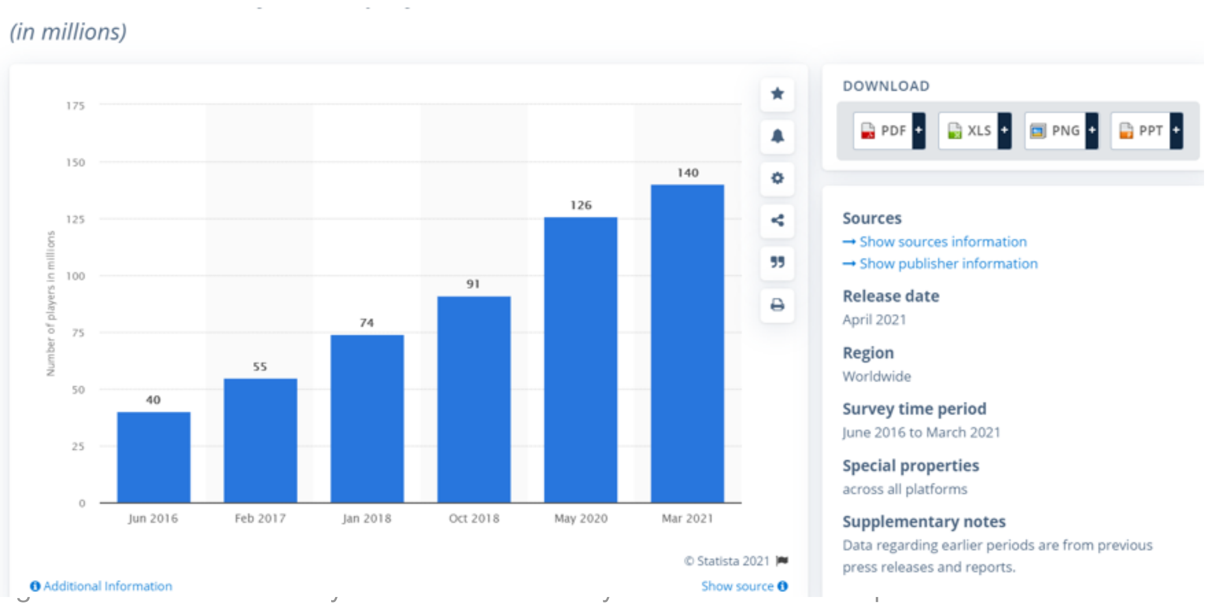
# Chaos Ransomware Variant in Fake Minecraft Alt List Brings Destruction to Japanese Gamers

By Shunichi Imano and Fred Gutierrez | October 28, 2021
**FortiGuard Labs Threat Research Report**

**Affected Platforms:** Windows
**Impacted Parties:** Japanese Minecraft Gamers
**Impact:** Potential loss of files and money due to file encryption and destruction and paying ransom
**Severity Level:** Medium

Minecraft is one of the most popular digital games in the world. It was originally released in May 2009 by Swedish game developer Mojang Studios, which was acquired by Microsoft in 2014 for US $2.5 billon. Initially released for the Windows, Mac, and Linux platforms, the game is now available on 22 platforms including video game consoles and mobile devices, including Android and iOS. As its gaming population has steadily grown, reaching more than 140 million monthly active players in August 2021, Minecraft has never been more popular 12 years after its initial release. Evidently, cybercriminals cannot pass up the opportunity to target such a large userbase.

FortiGuard Labs recently discovered a variant of the Chaos ransomware that appears to target Minecraft gamers in Japan. This variant not only encrypts certain files but also destroys others, rendering them unrecoverable. If gamers fall prey to the attack, choosing to pay the ransom may still lead to a loss of data. In this report we will take a look at how this new ransomware variant works.


*(in millions)*

Sources

Release date
April 2021

Region
Worldwide

Survey time period
June 2016 to March 2021

Special properties
across all platforms

Supplementary notes
Data regarding earlier periods are from previous press releases and reports.

# Ransomware Lure Being Posted to Japanese Minecraft Forums

Gamers create “alt” (alternative) accounts within Minecraft for various purposes (both good and bad): they allow them to antagonize/troll other players without having their main account banned, they provide cover for an alternative in-game identity/personality, they help avoid getting their main account banned for using cheats (gaining an unfair advantage over other gamers), etc. FortiGuard Labs has discovered a variant of Chaos ransomware being hidden in a file pretending to contain a list of “Minecraft Alt” accounts that leads us to believe that the effort is to target Minecraft gamers in Japan.

Even though they are often publicly available through Minecraft online forums, Alt Lists contain stolen accounts that gamers can use to do the things listed above. That’s what the threat actors behind this ransomware attack are using to lure victims to download and open the file.

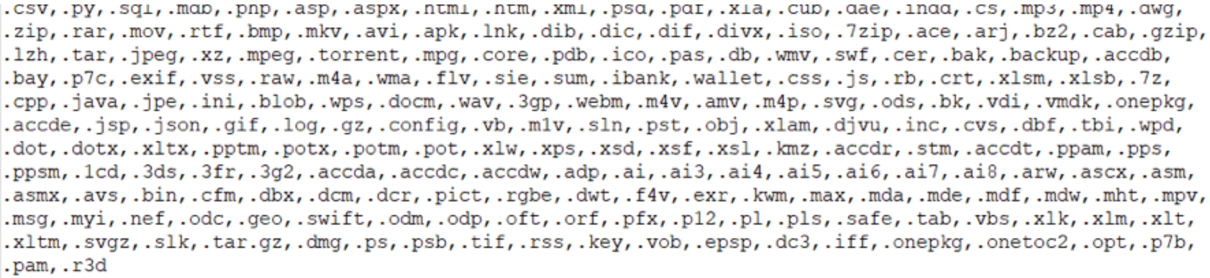
In this case, the file is an executable, but it uses a text icon to fool potential victims into thinking it is a text file full of compromised usernames and passwords for Minecraft. While we don’t know how this specific fake list is being distributed, it’s a safe guess that the file is being advertised on Minecraft forums for Japanese gamers.

# How the Executable Works

Once the executable file is opened, the malware searches for files smaller than 2,117,152 bytes  on the compromised machine and encrypts them. It then appends those files with four random characters chosen from “abcdefghijklmnopqrstuvwxyz1234567890” as a file extension.

But files larger than 2,117,152 bytes with specified file extensions are filled with random bytes so the victim will not be able to get those files back even if the ransom is paid. Having this destructive element changes this attack from a typical ransomware attack, and is a very troubling component.

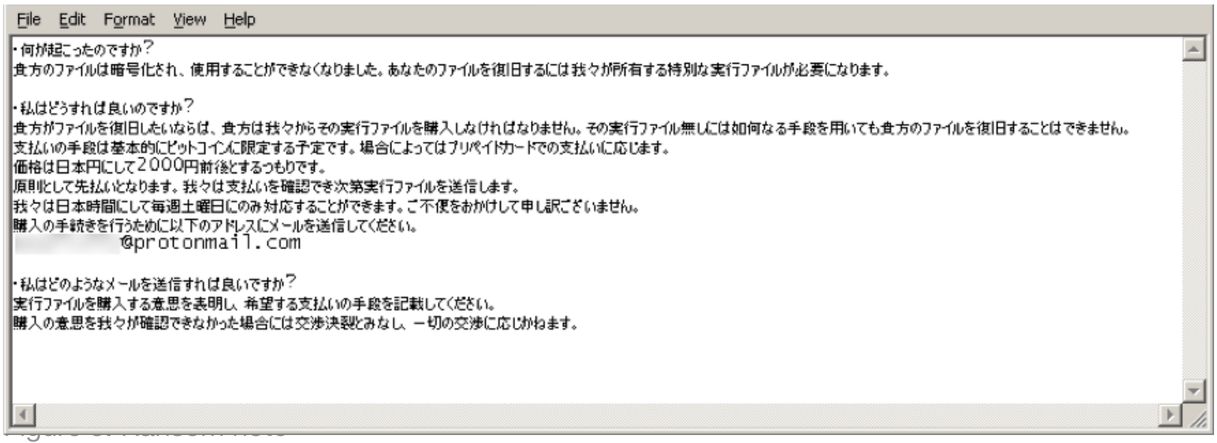
It is not known why the malware authors have chosen these file size values or why they choose to encrypt some and destroy others. But it is interesting to note that the Chaos malware was originally classified as a wiper malware with the ransomware component added later.



```
.csv,.py,.sql,.mdb,.php,.asp,.aspx,.html,.htm,.xml,.psd,.pdf,.xla,.cub,.dae,.indd,.cs,.mp3,.mp4,.dwg,
.zip,.rar,.mov,.rtf,.bmp,.mkv,.avi,.apk,.lnk,.dib,.dic,.dif,.divx,.iso,.7zip,.ace,.arj,.bz2,.cab,.gzip,
.lzh,.tar,.jpeg,.xz,.mpeg,.torrent,.mpg,.core,.pdb,.ico,.pas,.db,.wmv,.swf,.cer,.bak,.backup,.accdb,
.bay,.p7c,.exif,.vss,.raw,.m4a,.wma,.flv,.sie,.sum,.ibank,.wallet,.css,.js,.rb,.crt,.xlsm,.xlsb,.7z,
.cpp,.java,.jpe,.ini,.blob,.wps,.docm,.wav,.3gp,.webm,.m4v,.amv,.m4p,.svg,.ods,.bk,.vdi,.vmdk,.onepkg,
.accde,.jsp,.json,.gif,.log,.gz,.config,.vb,.m1v,.sln,.pst,.obj,.xlam,.djvu,.inc,.cvs,.dbf,.tbi,.wpd,
.dot,.dotx,.xltx,.pptm,.potx,.potm,.pot,.xlw,.xps,.xsd,.xsf,.xsl,.kmz,.accdr,.stm,.accdt,.ppam,.pps,
.ppsm,.1cd,.3ds,.3fr,.3g2,.accda,.accdc,.accdw,.adp,.ai,.ai3,.ai4,.ai5,.ai6,.ai7,.ai8,.arw,.ascx,.asm,
.asmx,.avs,.bin,.cfm,.dbx,.dcm,.dcr,.pict,.rgbe,.dwt,.f4v,.exr,.kwm,.max,.mda,.mde,.mdf,.mdw,.mht,.mpv,
.msg,.myi,.nef,.odc,.geo,.swift,.odm,.odp,.oft,.orf,.pfx,.p12,.pl,.pls,.safe,.tab,.vbs,.xlk,.xlm,.xlt,
.xltm,.svgz,.slk,.tar.gz,.dmg,.ps,.psb,.tif,.rss,.key,.vob,.epsp,.dc3,.iff,.onepkg,.onetoc2,.opt,.p7b,
.pam,.r3d
```

Once the attack takes place, a dropped ReadMe.txt files ask the victim to pay a ransom in either bitcoin or pre-paid cards. The requested amount to decrypt the files is equal to 2,000 yen (approx. US $17), which is dirt cheap compared to the amounts other ransomware attacks typically demand. The ransom note does not specify which type of pre-paid card the attacker wants. All kinds of pre-paid cards (online shopping, gaming, music, mobile phone charge and online streaming services) are available in convenience stores. Japan has more than 50,000 convenience store locations selling pre-paid cards and most are open 24/7.

The ransom note also states that the attacker is available only on Saturdays and apologizes for any inconvenience caused. The malware does not include code to identify the language setting of the compromised machine and the ransom note is available in Japanese only. This, combined with the formal language of the ransom note, indicates this Chaos ransomware variant specifically targets Japanese Windows users.



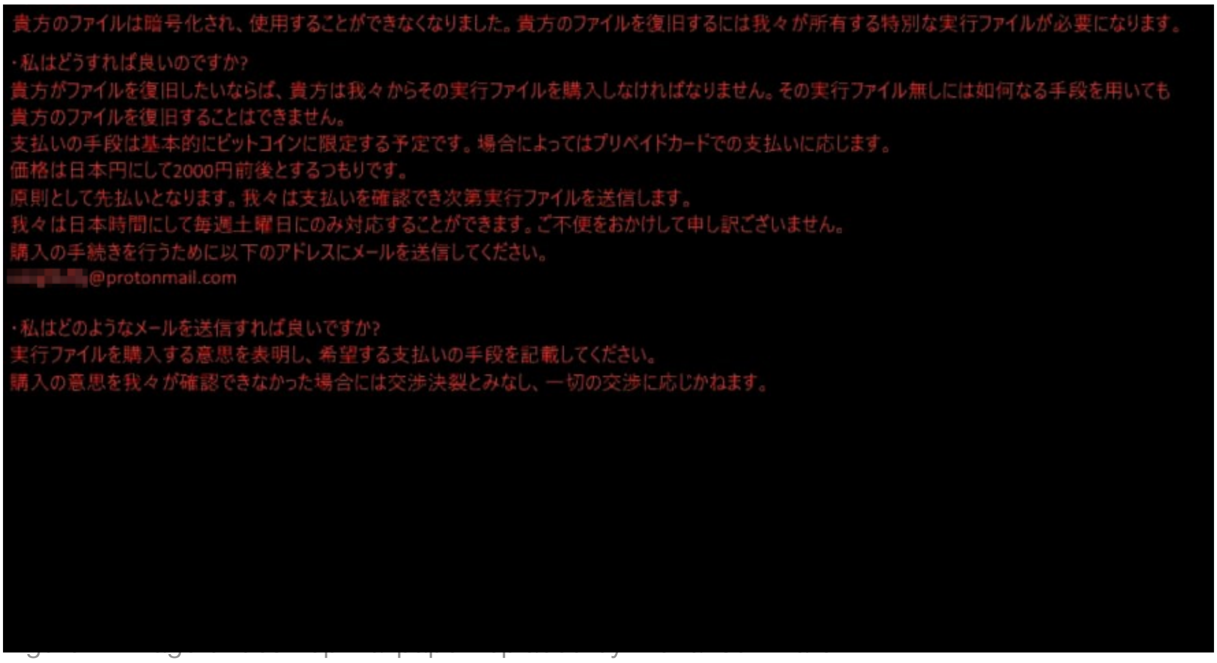
・何が起こったのですか?
貴方のファイルは暗号化され、使用することができなくなりました。あなたのファイルを復旧するには我々が所有する特別な実行ファイルが必要になります。

・私はどうすれば良いのですか?
貴方がファイルを復旧したいならば、貴方は我々からその実行ファイルを購入しなければなりません。その実行ファイル無しには如何なる手段を用いても貴方のファイルを復旧することはできません。
支払いの手段は基本的にビットコインに限定する予定です。場合によってはプリペイドカードでの支払いに応じます。
価格は日本円にして2000円前後とするつもりです。
原則として先払いとなります。我々は支払いを確認でき次第実行ファイルを送信します。
我々は日本時間にして毎週土曜日にのみ対応することができます。ご不便をおかけして申し訳ございません。
購入の手続きを行うために以下のアドレスにメールを送信してください。
[redacted]@protonmail.com

・私はどのようなメールを送信すれば良いですか?
実行ファイルを購入する意思を表明し、希望する支払いの手段を記載してください。
購入の意思を我々が確認できなかった場合には交渉決裂とみなし、一切の交渉に応じかねます。

The ransomware also deletes shadow copies from the compromised machine, which prevents the victim from being able to recover any files that had been encrypted, making it doubly destructive. FortiGuard Labs previously released a blog about shadow copy deletion carried out by ransomware. Luckily this Chaos ransomware variant does not have any code to steal data from the compromised machine.

The malware also changes the desktop wallpaper, perhaps to add more pressure to the victim to pay the ransom.



貴方のファイルは暗号化され、使用することができなくなりました。貴方のファイルを復旧するには我々が所有する特別な実行ファイルが必要になります。

・私はどうすれば良いのですか?
貴方がファイルを復旧したいならば、貴方は我々からその実行ファイルを購入しなければなりません。その実行ファイル無しには如何なる手段を用いても
貴方のファイルを復旧することはできません。
支払いの手段は基本的にビットコインに限定する予定です。場合によってはプリペイドカードでの支払いに応じます。
価格は日本円にして2000円前後とするつもりです。
原則として先払いとなります。我々は支払いを確認でき次第実行ファイルを送信します。
我々は日本時間にして毎週土曜日にのみ対応することができます。ご不便をおかけして申し訳ございません。
購入の手続きを行うために以下のアドレスにメールを送信してください。
[redacted]@protonmail.com

・私はどのようなメールを送信すれば良いですか?
実行ファイルを購入する意思を表明し、希望する支払いの手段を記載してください。
購入の意思を我々が確認できなかった場合には交渉決裂とみなし、一切の交渉に応じかねます。

## Conclusion - Chaos Ransomware Variant

There is nothing fancy about this Chaos ransomware variant nor its infection vector. However, despite its cheap ransom demand, its ability to destroy data and render it unrecoverable makes it more than a mere prank to annoy Japanese Minecraft gamers. Ransomware is still ransomware, and in this case, the victim may not be able to get their original files back, with or without making a ransom payment. The best advice is for players to stay off suspicious gaming cheat sites and simply enjoy the game the way it was meant to be played.

## Fortinet Protections

FortiGuard Labs has AV coverage in place for all of the malicious file samples in the report as:

MSIL/Filecoder.AGP!tr.ransom

Due to the ease of disruption, damage to daily operations , potential impact to the reputation of an organization, and the unwanted destruction or release of personally identifiable information (PII), etc., it is important to keep all AV and IPS signatures up to date.

## IOCs

### SHA2:

1a00c3f9173ee4c6f944e2dcebe44ca71f06455951728af06eba0f945e084907

aacce549a756cd942ee79f57625d0902ce79315f4e4bfb1381afa208599d7be5

*Learn more about Fortinet’s FortiGuard Labs threat research and intelligence organization and the FortiGuard Security Subscriptions and Services portfolio.*

*Learn more about Fortinet's free cybersecurity training, an initiative of Fortinet's Training Advancement Agenda (TAA), or about the Fortinet Network Security Expert program, Security Academy program, and Veterans program. Learn more about FortiGuard Labs global threat intelligence and research and the FortiGuard Security Subscriptions and Services portfolio.*