FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

15 JUL 2019

Alert Number

MC-000105-MW

WE NEED YOUR HELP!

If you find any of these indicators on your networks, or have related information, please contact **FBI CYWATCH immediately**.

Email:

cywatch@fbi.gov

Phone:

1-855-292-3937

**Note: By reporting any related information to FBI CyWatch, you are assisting in sharing information that allows the FBI to track malicious actors and coordinate with private industry and the United States Government to prevent future intrusions and attacks.*

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients in order to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber criminals.

This FLASH has been released **TLP:WHITE**: Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

Master Decryption Keys for GandCrab, versions 4 through 5.2

Summary

On 17 June 2019, the FBI, in partnership with law enforcement agencies from 8 European countries, as well as Europol and BitDefender, released a decryption tool applicable to all versions of GandCrab ransomware. The decryption tool can be found at www.nomoreransom.org. The collaborative efforts further identified the master decryption keys for all new versions of GandCrab introduced since July 2018. The FBI is releasing the master keys in order to facilitate the development of additional decryption tools.

GandCrab operates using a ransomware-as-a-service (RaaS) business model, selling the right to distribute the malware to affiliates in exchange for 40% of the ransoms. GandCrab was first observed in January 2018 infecting South Korean companies, but GandCrab campaigns quickly expanded globally to include US victims in early 2018, impacting at least 8 critical infrastructure sectors. As a result, GandCrab rapidly rose to become the most prominent affiliate-based ransomware, and was estimated to hold 50% of the ransomware market share by mid-2018. Experts estimate GandCrab infected over 500,000 victims worldwide, causing losses in excess of $300 million.

Master Decryption Keys

GandCrab v4 and 5

BwIAAACkAABSU0EyAAgAAAEAAQC77wJGC16Mco6goDGulTOC1meJMrLtkqgWCrwowU0+AKPcSEc96ZrBMa5BxegicGp
/dZiPxuvuZZsbltNNqj91C6V153HNiKB34MsvM6INq+TjQII/2ZVQpJJWqndhBXXyJYHaob4wp8vaK6OehasDjbvT8LuccZrU
mM/GwqhihDKFTBss/+TY2eUquxgGCGr02NGNAONB/OfFICXS3Uf/JwkfbTRsigrrqxNICfYkJJiEIt3BoRxgYwZx7gBKIbofr0w
D0sc/umQ5NbRECxdftSyMTrLmYbIjIU2t+9Qdlkuh/H+/mHi703Lx40YfA0wFGJbBR8CgbxcHERArLdTIeb+0g3U9aGAzu6R6
yFJmLub6RDJKrgarWp++KR09uKbAygsQOKRSJ7phrAo7DoaPeq+6iZ1KUjOBdGveYSaltFOlSEeOqNcBCKXf8gbd1UXc8+Cty
/0eVSwIY+LwWzmBdVD7XH42LBO9j2/irryjHQ2WLZGI5I854JlxCeDjgO7TV++RUzxdADB8ewANZih+yepnGK7SwrYl3aS3H
ZJ6U6G706Ix+C5JUG74jgeGFgEVRwUvibrV5IwpYetucmJHVvOWcFxwoy5/n1JmVN2y0Gqo4HDg9unsiq9nEJt/ujJNM8qzx
Ju2Zt5iFyEgkAw3FlB3mNpQ4Pe1hKsc+8CP1/ERhOCMHVewbW6Clh7MeL07qcODfNU/j5Ott4pFliGm1R1d3FA8OXFTwX
HjYEIRBwbBAe5WXe3KeNJMxL5ANZtUJz6C50g3zXI6lfmOJXBimFnSnXEGdOMyqB62tpFkzdw1QhzaV8sfEiMhU/TG1RATJ
GyCEWMVsXhhTm2HaepNq+30KrO24G3fIB8E9FbMyNlLMj+eEFSkpf/FAY7zPJ+xi02uJZSHgHAY+qhFpA3F8uNnCPhUMPa
eOgU55OhyUUcvgUHy4+nun3ajvJQItUYREhO6U7C2Z/DlLgrKslcmLMwuGVDa0kq92mnspwHXlZiSSbTWQQkaOQSJ1trCS
bnemNtDUWaAhW6jEQVbn8NVd3vJ4FKezgoIvAXhwKcpPbUvjj2EuL3fOElltB+wwu57V/45jZMSHvsWfi+vB2B42XIiU0y0lr
b8oFFFLByBNCbiqfmkID9rm6TYM4zcf51izQr+F2zEy31G2WgpcZp8jDvKyqNihZVvfeis7HFt4mG6dXTL5r2ATVRrMsaJJEk7s
vJv5M802hlFvg5lEApKDdL6URubHc7iqcjA//xjjd6eCPSrEMswPP6TN2j9CBAvW4Qo64/c+9js22PV78ushOowkob4wCp90k
KyZsELsYjP15oCYMkFBE8lsXC6i5bO/7BSGXDNbvVz4kV/hCOB3YsqwU2IF4/ME3ERDhM62zrNZeAyUf66BC6LGizxx/gxm9
oSn2A3F24LUc1oHwrpW8FLIx3LU0vBsH173GpfO+3WSKjbq9nUXR+cym6DBlutsrtafrf1SK65dgZ55WIHx34Jwh5FEjXaE8h
3f+b8HEok5lwKoO8cU6O+3ecdsaM=

GandCrab v5.0.4 - v5.1

BwIAAACkAABSU0EyAAgAAAEAAQCPuVnJ9eIt7iW/ocAMfJrrTaSnrcIfGmFHmkciEOpvDXFx+KSjXOwgWWVPn8Cs/1RoQY
LESNw2rLGjAxxg42/GTC8QTYU8n50I3JokQVIWjrhEoL5czMBkMJTo/MQjO9u6F/OKShMBz5tQim1oLq8UFu3YcuGZpvdr3
gfVWhQj1Yt7NceDPpr2cBZvP6nxEi9b2V8PLp1q8CfUdYUHabTkrO9A7mkszHFTqtzp7pwUmO4KvHGJU8nWkjqbmyy/Pgd
t6w1xrLy8oacfrVxA2nTamY1l+HQSNv/g17sgjJs9w624rFaxGPuystJHddPMzKGx4tv4KR2RvNGV2wxm4OGhL1XfrBAyeAJa
6mU/TtLPV1nxRB/66g7QA8i0m5YZd49RqhBhEG0Wx1g1iMWlBsnk4fiR593JSYJQc+/hcs8bQYO66eXL62vz00zdcGBjGJJQs
EikQrgAigApinO588NuwPNuOyejomwJYPHlgqKh2qfgTYHVpXNV4XN7eW8ZReShieGyX5yJYBolkJ3Za9oAravyjvOS+dklww
ZcENV1SEW6T2sI9PKe7sOzfCLR62gDHEWjAcsUVCacId4JEegVK9H6pbRjTQ8V5ecUHl/RqoTZ1eLeH55tdLEbCWk1K7RQZ
CwpmlKvSWd+jfIW5pa9qjBISXGyghyDiZdwaTWMtdkXqA/zhTd9/1hrmA5NKx0URx1gqJPySnIAPXoSzNdpjfCacLBTbkhn0
pbcXPdhpT5lqWikImK6vgRNewf9Idkoe6vTL/YzmaYOe43WvXyyajMr4JUzxXR2t0QnWQVPOyQrgYwas/PLs1vdSmsZkhD+
6Ni33wnbSJrk+hwmShUogcpvyiOLBb+jFYQFwlQbD1fxLgAmJu7Y1oWEUXf//ZLB0u2JA+H6hMBwAFs1i/4VA1OBNogFft7
S3Iy6S1Gva7+2Ft+VjAsugcuZLcd+Fj1Y+9ff3Zx24Vbwo+g6Ngxv2iYUTm8Ek+LXuyXn1RQcbEckI/lkNUmBT1YkTcUcpoPozb
WpvVbwv17oSnuckVSZLDJHpNbsNHvEEfVhlg7BjqH15+qUWttOX2uYJyN2aOwgFt5072KsW0ZHMh0pwewPW1bNdAdrD
mGSu89KxB+Hbj2IFEAWIjrnHTFhE62lHpyb/6TfIzv1eFfZUEYkwznkBqcASHHuoO7y/oERyRbmHcFg1bs1HlyRRIiwY5RC7aN
7b3ZnRr7AdbjZN0jFaJTZpNC28uDH2II1TlQ8fn7YlYQbS1a2Bvbz0FBb53nrUtrazZZHxE7M3DamtqTIWezL5X4YVcpP5M6NJ
3lr3QzNgJgmbciuo0BmCSg6WK7vJo6XHHneoNahSIPiUB27NJa11IRrSSiK08dinkp4+HBu+5H/wmJfbwcfXGA9rudEivLCZcG
Kcx/FUwY+5nE6TqYPYw48YPVxc81r5td44AoEBhMc5SBHrIpyQpQb2T5jE+jLeClcMec53+6voaVTtT33TrLxBKAF+gP7EIBgz
AeaGw2Jpm1R4w/ivtbe0zopLgA=

GandCrab v5.2

BwIAAACkAABSU0EyAAgAAAEAAQBtwvOCqX7rw/P9P/NqSFQEe621TAAfjoG2UUw6dgLDRWo66kSsANjkrb5Cxdy2zW9f
3+vu0TusoqUfwd6My8wJ0IEd0PpJ0V1IsHE504+zpG3oL8gMS7TPr3QvTMLMdMTKH/8f2LDCjfDfak/Zzz/tzm80KJ2eOQ1j
Tx+0Bn+j+Y0L0KzoiVJ2KpFbC5Gy2bkjYPLqkZ6Tx4NN7y6ekWkcLTMtyTgIqIchiJB4A+7xEtIkl80x5SyE4HTsyG/H9jIKQuYnU
etZREYIagscrJtfYLjeiZCzwdlqb0KjA7Vi9BY5jci5bEjrGKBOeVBeL1atKOqFldgB7Wxs4SkGw4Lb0xCs0WVMJJBWFJYlMNqSb
ATwmKdrYhpm4IPAISa3EhfKQjHB9vNKRyPm+9zCmw/Nz1gDBlYxGeR9Gwvd/ZnzVa7OKSaoOdTOuPEQkYTFPJ2L5s2Qv7
UyK3OzS5Va3er+20DB2NWm/FeVzXLwdhwEI8rM+rqlummMBWUJwPN1QP2/14ZRjaKFZFPByYhDVlSVDRSReXZ0xhjz9Z
gWGNJCA94N8lVbUbZ2NHTr7xGY9movIl1+zdfFXvTv+Km72m+xkHSHe/IRr2DrLMRGtTDjwrtaFwdNgDNhNRABTlsTc1sSn
3pE7owK/8HMvQG8K3YffEWNG9IeDoDSFCgiWZHk3bczBZAB9QqTI3zF3sx/lSQ0rMAKBsSVDW1mJs6VN5hc5oS78LQNKP
miZGqcD2ZtQOvNWQvZ/bX5RCCco3x7kg792SAsX0TI7IS+YunreAB7xkpbs0fhAWJNzNKRkRu2IWOtL7ePedmGoiH4jrrjkh
26rMCvfbM/G/w4J4dUhSXlU2EdnoT6QU0OWlSnCww/lbvkylpdd6j5kYH6TnVEzYbghOwcehcjtAoWECH9r4vF9prRVfYXy
pu/qbIljpCNmRsmraYDkX+0udTR9ILTKrZri4xVeDWbT0BpllQzChCd6KUrv526JZuYemlVxS/6+/mOLUP5RI6nUWi/oSlS8m
QgwYx0a2Kfk1HGMIjrGO2EQkty7LiFMf9E1ynqLaD4Uz+xzahY3UwPP9DdqkMxZ3eFebdU+uxUd0wGqXFZRCXfWgEIJe5z
43TXY3fSPXQN5K4YSU+5QRQ7pH+MXpk8gw/dKt4v7+eyMGqxlLtuid2uovYbQu+8lgda2ff2j0RRLu0b+VuoWkweUSxoNIH
aXhcnsLs432eA2w8txYFI1+uUKK1ecv1bolkvkai2ip53KVmW97g5+fZTXgNEPR7vdLeViYulD4RZINvZmQLgZQvPbS+cwMJK
gE7YnRQQTr9BUb+139PQY5w6PoRkpTUdoHSdfe9qaiTs3vy3uCHt4mR5ODZ5z25b2223wHVVbhdTXzTZj1GBm8b0q+PpS
Cpu/l2Iffdv40pb7ufk2ILGftvPjZVbwBNjAPVXLPDybCxtA2xpk4gby/DN9cBOBuEQMMiSnljQ7sf6QBaSJa/vgvy77VyiM8kJx
KBjXOrUlGz+4Li8eUdmYT6W8Dcutj5JmMA=

Recommended Ransomware Mitigations

The FBI recommends undertaking measures to secure systems against ransomware infection and to mitigate the impact of ransomware. Recommended measures include, but are not limited to, the following:

- Train personnel to identify phishing attempts and how to respond to them.
- Implement a strong patch management system and enable automatic patching.
- Implement auto updates for antivirus software.
- Implement the principle of least privilege and strictly manage privileged accounts.
- Implement a robust backup system and store backups offline
- Implement strong authentication requirements for remote desktop protocol (RDP)

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or the FBI's 24/7 Cyber Watch (CyWatch). Field office

contacts can be identified at www.fbi.gov/contact-us/field. CyWatch can be contacted by phone at (855) 292-3937 or by e-mail at CyWatch@fbi.gov. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact. Press inquiries should be directed to the FBI's National Press Office at npo@fbi.gov or (202) 324-3691.

Administrative Note

This product is marked **TLP:WHITE**. Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

For comments or questions related to the content or dissemination of this product, contact CyWatch.

Your Feedback on the Value of this Product Is Critical

Was this product of value to your organization? Was the content clear and concise? Your comments are very important to us and can be submitted anonymously. Please take a moment to complete the survey at the link below. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to such products. Feedback may be submitted online here:
https://www.ic3.gov/PIFSurvey

Please note that this survey is for feedback on content and value only. Reporting of technical information regarding FLASH reports must be submitted through FBI CYWATCH.