GandCrab

GandCrab ransomware is a type of malware that encrypts a victim's files and demands ransom payment in order to regain access to their data. GandCrab targets consumers and businesses with PCs running Microsoft Windows.

Also for Windows, iOS, Android, Chromebook and For Business

GandCrab

On May 31, 2019 the cybercriminals behind the GandCrab ransomware did something unusual within the world of malware. They announced they were shutting down operations and potentially leaving millions of dollars on the table.

“All good things come to an end” they wrote in a self-congratulatory post appearing on a notorious cybercrime forum. Since launching in January 2018, GandCrab’s authors claimed to have brought in over $2 billion in illicit ransom payments and it was time “for a well-deserved retirement.”

“We successfully cashed this money and legalized it in various spheres of white business both in real life and on the Internet,” the post continued. “We have proved that by doing evil deeds, retribution does not come.”

Affiliated partners, those who helped spread the ransomware for a share of the profits, were encouraged to shut down operations while victims were told to pay up now or lose their encrypted data forever.

The post ended with a pithy thank you to everyone in the affiliate community for “all the hard work.”

they really retiring? More importantly, is the GandCrab ransomware still a threat to consumers?

In this article we'll attempt to answer all of those lingering questions, provide resources for victims, and put an epilogue on the story of GandCrab.f

What is GandCrab?

First observed in January of 2018, GandCrab ransomware is a type of malware that encrypts victims' files and demands ransom payment in order to regain access to their data. GandCrab targets consumers and businesses with PCs running Microsoft Windows.

Sounding like a sexually transmitted disease, one might think a name like "GandCrab" has something to do with the ransomware's infectious nature and propensity for spreading across business networks. According to *ZDNet*, however, GandCrab's name may be derived from one of its creators who goes by the online handle "Crab" or "Gandcrab."

GandCrab does not infect machines in Russia or the former Soviet Union—a strong indicator that the author or authors are based in the region. Little else is known about the GandCrab crew.

GandCrab follows an affiliate marketing business model, aka Ransomware-as-a-Service (RaaS), in which low-level cybercriminals do the heavy lifting of finding new victims while the threat authors are free to tinker with and improve their creation.

laptops, computers, etc. Each review includes a unique link that allows visitors to buy the featured item on Amazon. In exchange for sending the customer to Amazon you get a percentage of the purchase price.

As it applies to GandCrab, the threat authors give their technology away to other enterprising cybercriminals (i.e., affiliates). From there it's up to the affiliates to figure out how they'll find new customers (i.e., victims). Any ransoms paid are split between the affiliate and the GandCrab crew 60/40 or as high as 70/30 for top affiliates.

Cybersecurity journalist Brian Krebs reports one top earned $125,000 in commissions over the course of one month.

Using the affiliate model, criminals with limited technical know-how are able to get in on the ransomware action. And with low-level criminals responsible for finding and infecting machines, GandCrab's creators can focus on revising their software, adding new features, and improving its encryption technology. All told, there are five different versions of GandCrab.

Upon infection, ransom notes are placed prominently on the victim's computer, directing them to a website on the Dark Web (the hidden part of the web you need a special browser to see).

Landing on the English language version of the website, victims are shown the typo-riddled message "WELCOME! WE ARE REGRET, BUT ALL YOUR FILES WAS INFECTED!"

Later versions of the ransom website feature Mr. Krabs from the animated kids show "Spongebob Square Pants". Apparently, cybercriminals aren't too worried about copyright violations.

To allay any fears about paying the ransom, GandCrab allows victims to decrypt one file of their choosing for free.

GandCrab payments are made through an obscure cryptocurrency called Dash—valued by cybercriminals for its extreme focus on privacy. Ransom demands are set by the affiliate, but usually fall somewhere between $600 and $600,000. Upon payment, victims can immediately download the GandCrab decryptor and regain access to their files.

If victims have any issues with paying the ransom or downloading the decryptor tool, GandCrab provides 24/7 "free" online chat support.

authors are free to tinker with and improve their creation.

What is the history of GandCrab?

You'd be remiss for thinking ransomware was a recent invention. In fact, all forms of ransomware, GandCrab included, have followed a basic template set thirty years ago by an early form of computer virus.

The first proto-ransomware arrived in 1989—literally arriving in victims' mailboxes. Known as the AIDS computer virus, AIDS spread via 5.25" floppy disk sent to victims via snail mail. The disk was labelled "AIDS Information" and included a short survey designed to measure an individual's risk of catching the AIDS virus (the biological one).

Loading the survey initiated the virus, after which the virus would lay dormant for the next 89 boot ups. Upon starting their computer for the 90th time, victims would be met with an on-screen notification requesting payment for "your software lease." If victims tried to access their files, they'd find all of their file names had been scrambled.

Ransom payments were to be sent to a PO box in Panama and, in return, victims received a "renewal software package" that would reverse the quasi-encryption.

The method of operation for GandCrab and other modern ransomware threats remains relatively unchanged since the days of the AIDS computer virus. The only difference is today's cybercriminals have a vast arsenal of advanced technologies by which to target, infect, and victimize consumers.

When first observed back in January of 2018, GandCrab spread through malicious ads (aka malvertising) and bogus pop-ups served up by compromised websites. Upon landing on a malicious site, victims would receive an on-screen alert prompting them to download a missing font. Doing so would install the ransomware.

At the same time as the font infection campaign, GandCrab also spread via malware-laden email attachments (aka malspam) spewed out from a botnet of hacked computers (botnets are also used for DDoS attacks). In a textbook example of social engineering trickery, these emails featured the subject line "Unpaid invoice #XXX." Motivated by fear, curiosity, or greed, victims opened the email and the attached, malware-laden "invoice."

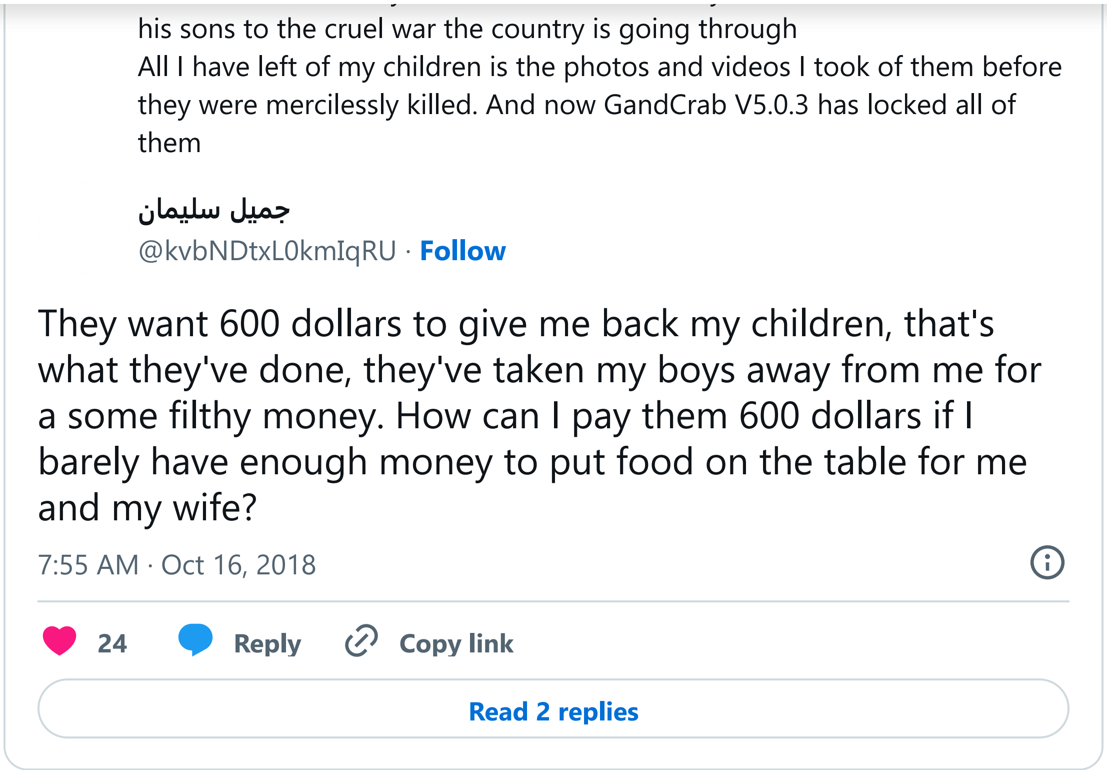
advantage of weaknesses or vulnerabilities on a target system in order to gain unauthorized access to that system. An exploit kit is a plug-and-play package of various technologies designed to take advantage of one or more exploits.

The Malwarebytes Labs team reported on at least four different exploit kits being used to spread GandCrab, which you can read about:

- GandCrab ransomware distributed by RIG and GrandSoft exploit kits (updated)
- Vidar and GandCrab: stealer and ransomware combo observed in the wild
- Magnitude exploit kit switches to GandCrab ransomware

In February of 2018, a month after GandCrab was first spotted in the wild, cybersecurity company Bitdefender released a free GandCrab decryption tool. This prompted GandCrab's authors to release a new version of their ransomware with new encryption technology. As it stands the newest version of the decryption tool works on GandCrab versions 1, 4, 5.01, and 5.2. To this day, there is no free decryption tool available for GandCrab versions 2 and 3.

In October 2018, a victim of the Syrian Civil War called out the creators of GandCrab as "heartless" for encrypting the photos of his dead children. In response, the GandCrab crew released the decryption key for any GandCrab victims located in Syria and added Syria to the list of countries not targeted by the GandCrab ransomware.



his sons to the cruel war the country is going through
All I have left of my children is the photos and videos I took of them before they were mercilessly killed. And now GandCrab V5.0.3 has locked all of them

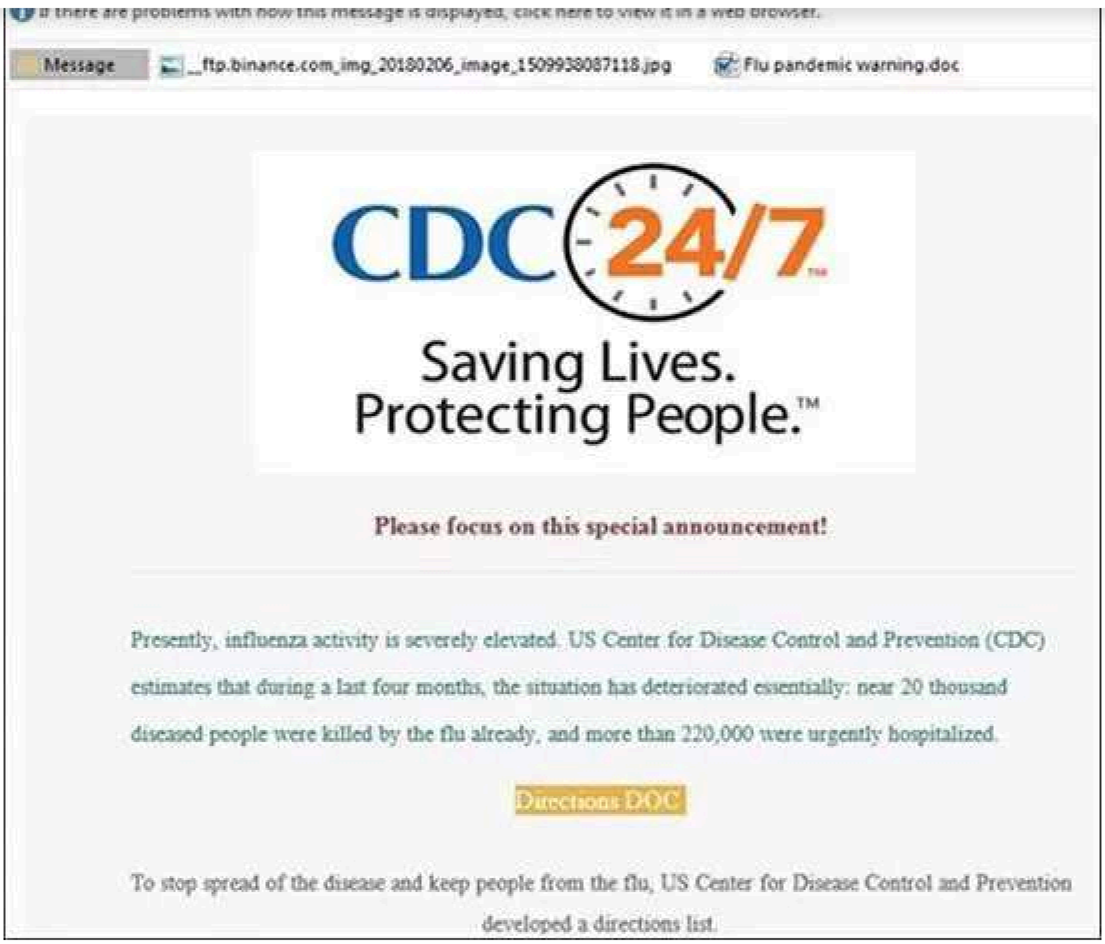
جميل سليمان
@kvbNDtxL0kmIqRU · Follow

They want 600 dollars to give me back my children, that's what they've done, they've taken my boys away from me for a some filthy money. How can I pay them 600 dollars if I barely have enough money to put food on the table for me and my wife?

7:55 AM · Oct 16, 2018

In January of 2019, affiliates were first seen using what's known as a remote desktop protocol (RDP) attack. With this kind of attack, the perpetrators scan a given network for systems that are set up for remote access; that is, a system that a user or administrator can log in to and control from another location. Once the attackers find a system setup for remote access, they will attempt to guess the login credentials using a list of common usernames and passwords (aka a brute force or dictionary attack).

At the same time, GandCrab affiliates took advantage of a long, severe flu season (21 weeks) by spreading the ransomware via phishing emails supposedly from the Centers for Disease Control and Prevention (CDC), bearing the subject "Flu pandemic warning." Opening the attached malware-laden Word document initiated the ransomware infection.



If there are problems with how this message is displayed, click here to view it in a web browser.

Message
__ftp.binance.com_img_20180206_image_1509938087118.jpg
Flu pandemic warning.doc
CDC 24/7
Saving Lives. Protecting People.™

Please focus on this special announcement!

Presently, influenza activity is severely elevated. US Center for Disease Control and Prevention (CDC) estimates that during a last four months, the situation has deteriorated essentially: near 20 thousand diseased people were killed by the flu already, and more than 220,000 were urgently hospitalized.

Directions DOC

To stop spread of the disease and keep people from the flu, US Center for Disease Control and Prevention developed a directions list.

Thanks to its army of affiliates, diverse attack methodology, and regular code revisions, GandCrab quickly became the most common ransomware detection amongst business and consumer targets for 2018, as reported in the Malwarebytes Labs State of Malware report.

In spite of its success, or perhaps because it, GandCrab called it quits in May of 2019—a year and a half after launching. Cybersecurity researchers have floated a number of theories as to why.

GandCrab isn't as successful as its creators made it out to be. We don't really know how much money the GandCrab crew made. Their claim of $2 billion dollars in earnings may be inflated and here's why: Cybersecurity researchers developed free GandCrab decryption tools for previous versions of the ransomware. Barely two weeks after the GandCrab crew announced they were pulling up stakes, researchers at Bitdefender released a final decryption tool capable of decrypting the latest version of GandCrab. With wider public awareness of the free decryptor tools, more and more potential victims avoid paying any potential ransom.

world with devious new threats, outside the watchful eye of cybersecurity researchers and law enforcement. Sure enough, cybersecurity researchers at Malwarebytes reported on a new strain of ransomware that bore a conspicuous resemblance to GandCrab.

Known as Sodinokibi (aka Sodin, aka REvil), this ransomware was spotted in the wild nearly two months after GandCrab called it quits and researchers immediately drew comparison to the defunct ransomware. As of yet, there's no smoking gun implicating the GandCrab crew as the bad guys behind Sodinokibi, but it's a safe bet.

For starters, Sodinokibi follows the same ransomware-as-a-service model—the GandCrab crew owns and supports the software, allowing any would-be cybercriminal to use it in exchange for a cut of the profits.

Sodinokibi follows the same iterative update process as GandCrab. To date, there have been six versions of Sodinokibi.

Sodinokibi employs some of the same infection vectors, namely exploit kits and malicious email attachments. In a new twist, however, the criminals behind Sodinokibi have started to use managed service providers (MSP) to spread infections. In August of 2019, hundreds of dental offices around the country found they could no longer access their patient records. Attackers used a compromised MSP, in this case a medical records software company, to deploy the Sodinokibi ransomware across dental offices using the record keeping software.

Finally, Sodinokibi's ransom note and payment site bear more than a little resemblance to those of GandCrab.

How to protect yourself from GandCrab

Though the Malwarebytes Data Sciences team reports GandCrab detections are in sharp decline, we still have Sodinokibi and other strains of ransomware to contend with. That being said, here's how-to protect yourself from GandCrab and other ransomware.

- **Back up your files.** With regular data backups, a ransomware infection becomes a small, if annoying, inconvenience. Simply wipe and restore your system and move on with your life

- **Be wary of emails attachments and links.** If you receive an email from a friend, family member, or coworker and it just sounds weird—think twice. If the email is from a company

- **Patch and update regularly.** Keeping your system up-to-date will stop attackers from taking advantage of exploits that can be used to gain unauthorized access to your computer. Exploits, as you may recall, are the main method by which GandCrab infects target systems. Similarly, if you have old, outdated software on your computer you aren't using anymore—delete it.

- **Limit remote access.** The best way to protect against a Remote Desktop Protocol (RDP) attack is to limit remote access. Ask yourself, does this system really need to be accessed remotely? If the answer is yes, at least limit access to the users who really need it. Better yet, implement a virtual private network (VPN) for all remote users, doing so negates any possibility of an RDP attack.

- **Use strong passwords and don't reuse passwords across sites.** In the event that a system absolutely needs to be accessed remotely, be sure to use a strong password with multi-factor authentication. Granted, remembering unique passwords for all of the various sites and applications you use is a difficult if not impossible task. Fortunately, a password manager can do that for you.

- **Use cybersecurity software.** For example, Malwarebytes Premium for Windows blocks Trojans, viruses, malicious downloads, bad links, and spoofed websites so ransomware, like GandCrab, and other malware infections can never take root on your system.

How to remove GandCrab

If you've already fallen victim to GandCrab, there's a good chance you don't need to pay the ransom. Instead, follow these steps to remove GandCrab from your PC.

1. **Show file extensions in Windows.** By default, Microsoft Windows hides file extensions (like .exe and .doc) and you'll need see these extensions before you can move on to step two. In short, open File Explorer, click the View tab, then check the File Name Extensions box.
2. **Determine the GandCrab version.** Now that you can see file extensions, you can figure out which version of GandCrab you have by verifying the extensions on your encrypted files.

- GandCrab version 2 and 3 gives the .crab extension.
- GandCrab version 4 gives the .krab extension.
- GandCrab version 5 gives a randomized 5 letter extension.

- **Download the decryptor.** As mentioned earlier in this piece, there's a free GandCrab decryptor for GandCrab versions 1, 4, 5.01, and 5.2. If your file extensions match these aforementioned versions, you're all good. Unfortunately, there is no free decryption tool available for GandCrab version 2 and version 3.
- **Don't pay the ransom.** If you've been infected by GandCrab version 2 or version 3 you might be tempted to pay the ransom—don't. Assuming the GandCrab servers are still operational, the FBI, Europol, and INTERPOL all recommend not paying the ransom. There's no guarantee you'll get your files back and doing so marks you as a soft target for future ransomware attacks.

Cyberprotection for every one.

Cybersecurity info you can't live without

Want to stay informed on the latest news in cybersecurity? Sign up for our newsletter and learn how to protect your computer from threats.

Email Address

Email Address

Sign Up

COMPUTER SECURITY

Rootkit Scanner

Trojan Scanner

e Antivirus

PRIVACY PROTECTION

Privacy VPN (Virtual Private Network)

Digital Footprint Scan

Dark Web Monitoring