



A private sector perspective on ransomware, its threats and evolution over time

Alexandru Catalin COSOI, Bitdefender



Bitdefender®



INTERPOL



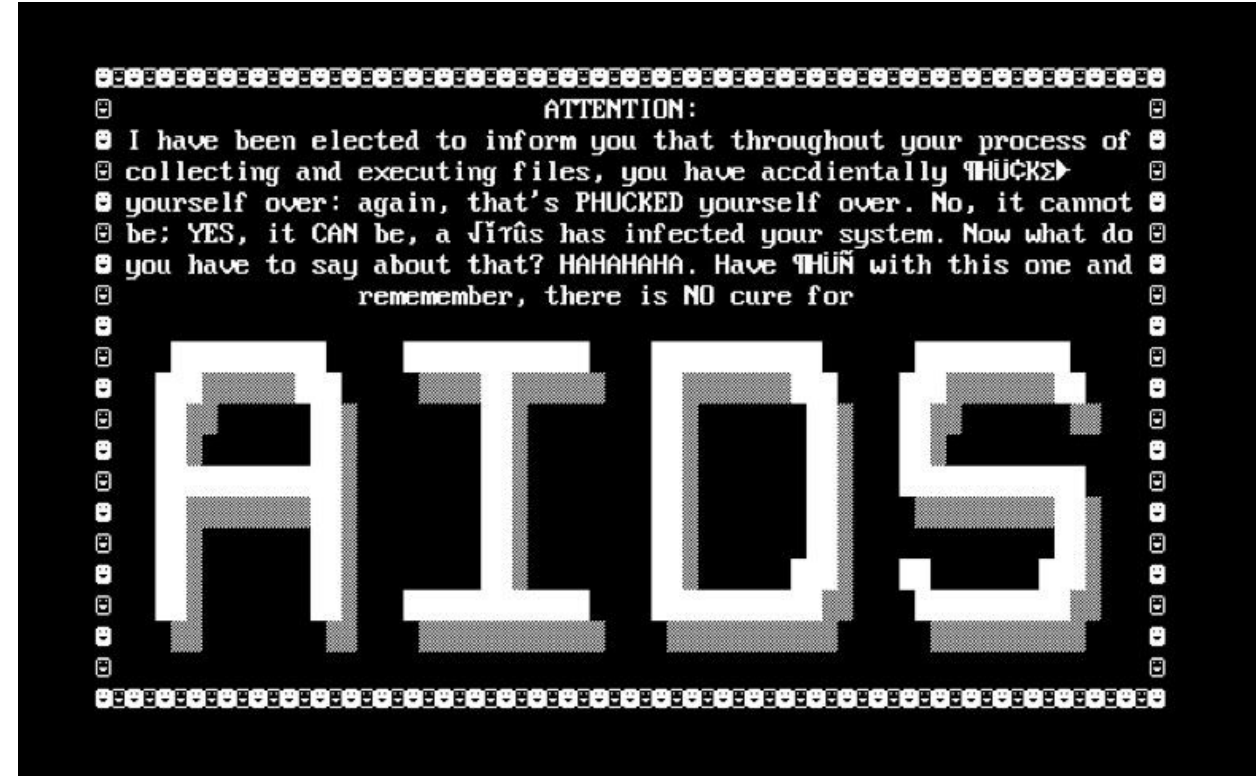
COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

32 Years of Ransomware


- | 1989 : AIDS Trojan demands cash ransom
- | 2005 : GPCode ransomware
- | 2010 – 2012: Screen lockers (Reveton, WinLocker)
- | 2014: Welcome to hell (Cryptolocker, Cryptowall)
- | 2014 – 2018: democratized access to ransomware
- | 2016: KeRanger & Linux Encoder (Mac OS & Linux)
- | 2017: GoldenEye/NotPetya & WannaCry
- | 2018: GandCrab and other RaaS families
- | 2019: 12 new ransomware families every month
- | 2021: High profile targets, critical infrastructure victims



GandCrab Ransomware

- highly organized ransomware group
- russian speaking
- highly vocal on exploit.in forum
- ransom fee depending on the infected machine and its contents
- average 1400\$ USD for home user
- average 10.000\$ USD for computer in SMB.
- the most prevalent ransomware family in 2018 and H1 2019 (almost 50% “marketshare”)
- officially “retired” in June 2019

If the payment isn't made until `2/15/2019, 6:49:35 PM`, the cost of decrypting files will be doubled
Countdown to double price: **Time is up. Price is doubled!**




What's the matter?

Your computer has been infected with `GandCrab Ransomware`.
All your files have been encrypted and you are not able to decrypt it by yourself.
To decrypt your files you have to buy `GandCrab decryptor`.

The price is - `9700 USD`

What can I do to get my files back?

You should buy our software `GandCrab Decryptor`. It will scan your PC, network share, all connected devices and check for encrypted files and decrypt it. Current price: `9700 USD`. We accept cryptocurrency `DASH` and `Bitcoin`



Attack Vectors


- DOC files with macro inside or laced PDF files
- Zipped JS downloaders attached to malspam
- cracks, lots of cracks
- exploit kits
- direct break-in via RDP or stolen credentials
- renting access to already infected computers


 **Ronald Bate**
@rlbate22 Follow 

Replying to @bbotezatu

GandCrab 5.2 is out and flourishing - unfortunately the celebration is over, our MSP has been attacked and all of their clients are frozen, including us. How far along is Bitdefender with the next generation of the 5.2 decryptor???

7:20 PM - 3 Mar 2019


 1   

 **J.D. Greene**
@greenedude Follow 

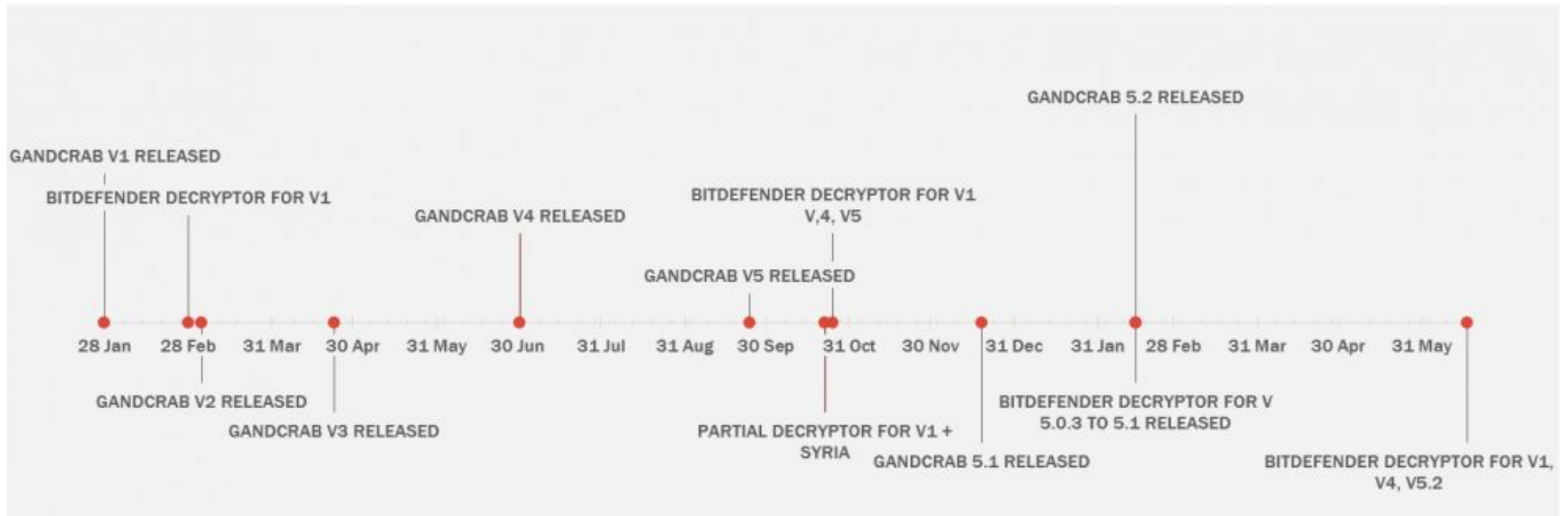
Replying to @tamas_boczan

All of our clients (1500+) just got hit with 5.2. Do you know if they have a decryptor tool yet for 5.2?

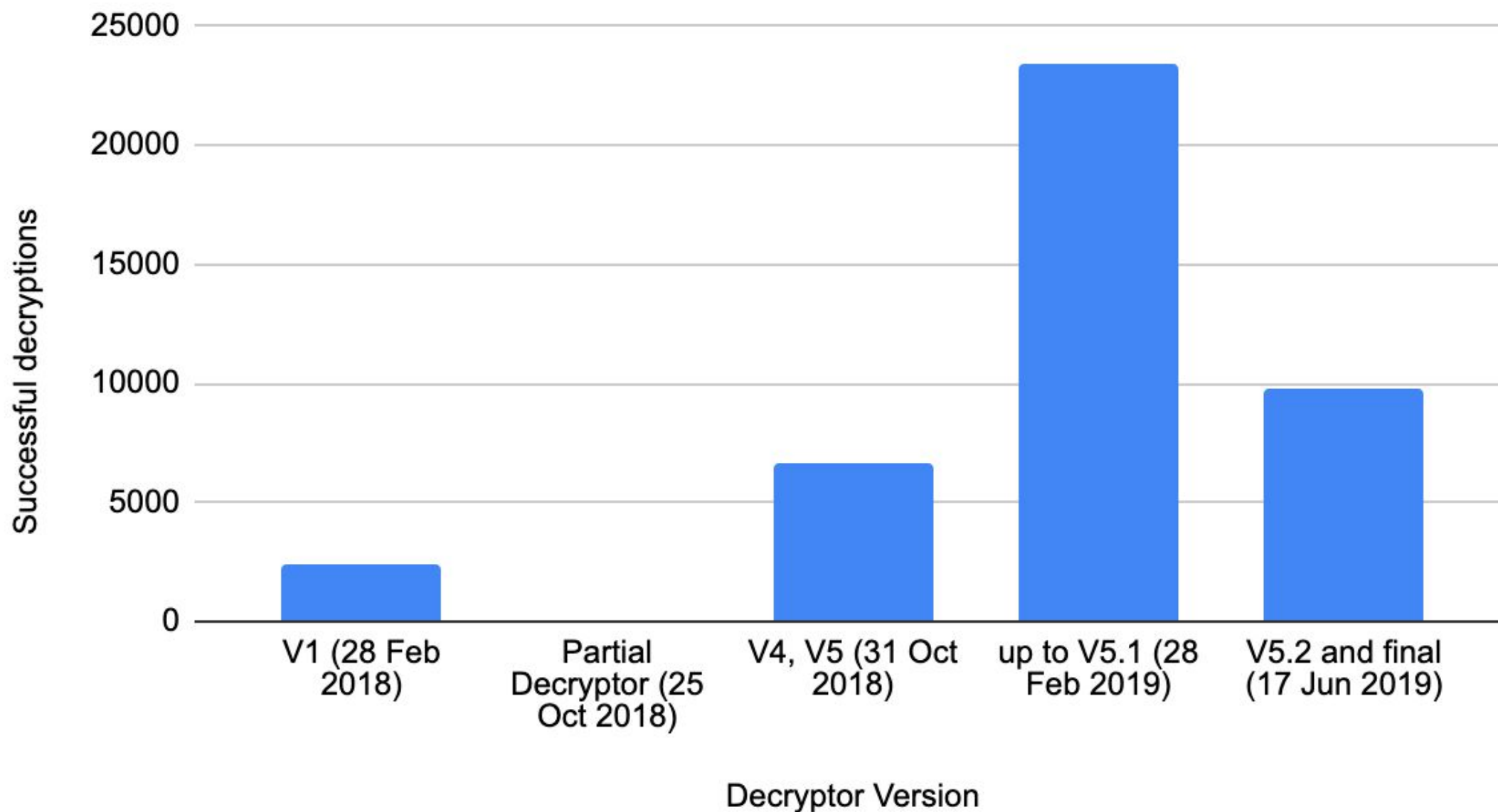
7:55 AM - 27 Feb 2019

 1   

#	Exension	Ransom Note Info
v1	.GDCB	---= GANDCRAB =---, the extension: .GDCB
v2	.GDCB	---= GANDCRAB =---, the extension: .GDCB
v3	.CRAB	---= GANDCRAB V3 =--- the extension: .CRAB
v4	.KRAB	---= GANDCRAB V4 =--- the extension: .KRAB
v5	.([A-Z]+)	---= GANDCRAB V5.0.2 =--- the extension: .HHFEHIOL



Successful decryptions vs. Decryptor Version



Gandcrab

(\ /) _ (\$ _ \$) _ (\ /)



Seller

424 posts

Joined

12/18/17 (ID: 84324)

Activity

virology

Posted 18 hours ago

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 come to an 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.



REvil (a.k.a. Sodinokibi) in 30 seconds

Short for Ransomware Evil, REvil is a private RaaS operation that first emerged in 2019. Deeply tied with the now-defunct GandCrab RaaS group, REvil leverages affiliates to infect companies and extort money. Since 2019, REvil has made a name and became the most common ransomware variant in the second quarter of 2021.

REvil has managed to compromise thousands of businesses around the world and was known to extort much larger payments from victims than the average market price. Companies that did not pay and attempted to restore from backups were blackmailed with the publication of their stolen confidential information.

International Cooperation

- Romanian authorities have arrested two affiliates of the Sodinokibi/REvil ransomware family responsible for 5,000 infections.
- Since February 2021, law enforcement officers have arrested three other affiliates of Sodinokibi/Revil, bringing the total of Sodinokibi arrests to five, as well as two suspects connected to GandCrab.
- These are among the results of Operation GoldDust, a coordinated effort involving 19 law enforcement organizations (local LEAs in Australia, Belgium, Canada, France, Germany, the Netherlands, Luxembourg, Norway, Poland, Romania, South Korea, Sweden, Switzerland, Kuwait, the United Kingdom and the United States, as well as Europol, Interpol and Eurojust).

Public Private Partnerships (PPP)



The Bitdefender DRACO Team provided cybersecurity consulting and guidance especially in areas of cryptography, forensics, and OSINT investigations and suspect identification, that helped the law enforcement consortium in this operation minimize the impact of successful ransomware attacks, and eventually led to arrests. This collaboration with law enforcement is a prime example of the public and private sector working together to significantly disrupt cybercriminal activities.

Ransomware best practices

- Ransomware attacks usually start with email phishing and social engineering. Educate and continuously train employees on the dangers of clicking links and opening attachments from unknown sources.
- Make sure security platforms such as endpoint detection and response (EDR) and extended detection and response (XDR) are updated with indicators of compromise (IOCs) to look for REvil and other popular ransomware families.
- Consider the managed detection and response (MDR) model to supplement an in-house security teams' ability to perform active threat hunts.
- Minimize your attack surface and ensure legacy services or other unneeded services (such as RDP) are not exposed to the Internet.



B

PROTECTING 500 MILLION USERS WORLDWIDE