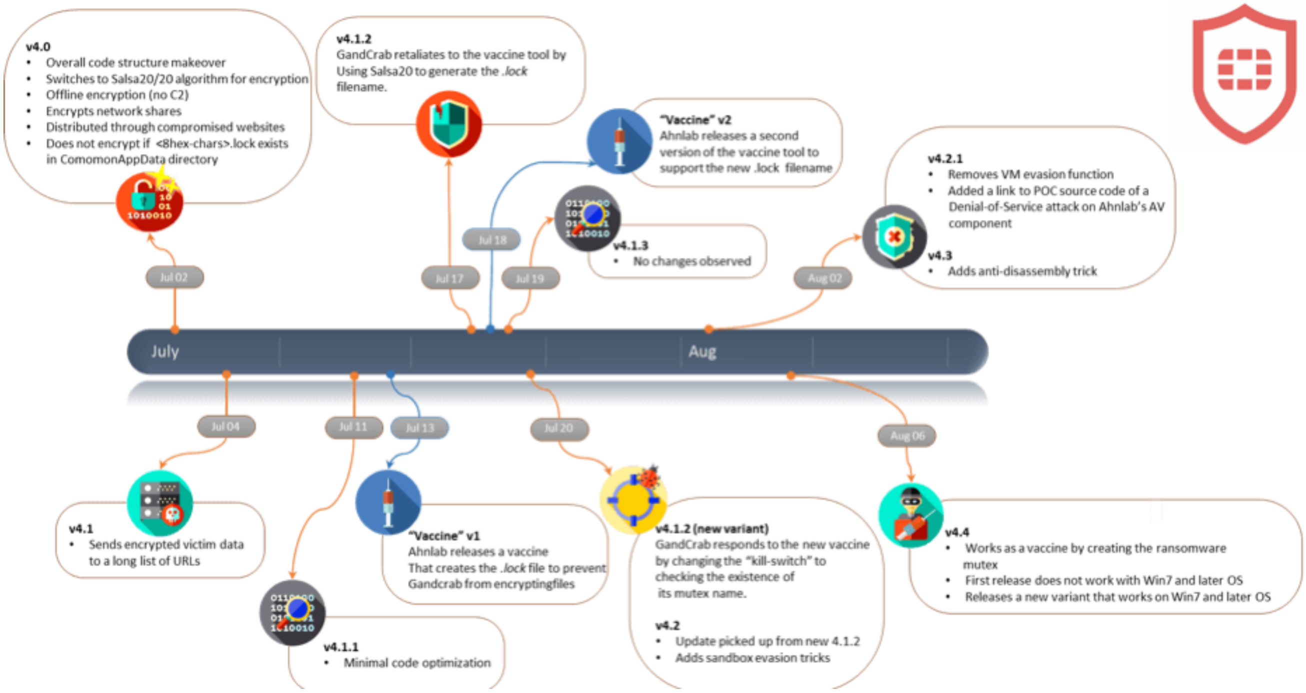
GandCrab Threat Actors Retire...Maybe

fortinet.com/blog/threat-research/gandcrab-threat-actors-retire.html

June 24, 2019



v4.0
- Overall code structure makeover
- Switches to Salsa20/20 algorithm for encryption
- Offline encryption (no C2)
- Encrypts network shares
- Distributed through compromised websites
- Does not encrypt if <8hex-chars>.lock exists in ComomonAppData directory

v4.1.2
GandCrab retaliates to the vaccine tool by Using Salsa20 to generate the *.lock* filename.

"Vaccine" v2
Ahnlab releases a second version of the vaccine tool to support the new .lock filename

v4.1.3
- No changes observed

v4.2.1
- Removes VM evasion function
- Added a link to POC source code of a Denial-of-Service attack on Ahnlab's AV component

v4.3
- Adds anti-disassembly trick

v4.1
- Sends encrypted victim data to a long list of URLs

v4.1.1
- Minimal code optimization

"Vaccine" v1
Ahnlab releases a vaccine That creates the *.lock* file to prevent Gandcrab from encryptingfiles

v4.1.2 (new variant)
GandCrab responds to the new vaccine by changing the "kill-switch" to checking the existence of its mutex name.

v4.2
- Update picked up from new 4.1.2
- Adds sandbox evasion tricks

v4.4
- Works as a vaccine by creating the ransomware mutex
- First release does not work with Win7 and later OS
- Releases a new variant that works on Win7 and later OS

In a surprising announcement two weeks ago, the threat group behind the malware operation GandCrab announced that they had shut down their operations. Until that point, GandCrab had been one of the most active malware campaigns of the past year, both in terms of distribution and rapid development. FortiGuard Labs has covered their progress in a series of articles, as well as in a presentation at AVAR2018.

In an announcement as novel and cavalier as the threat actors themselves – reflecting their public persona since they first surfaced – they have now made a grand exit by thanking their affiliates and detailing their earnings.

They claim that their Ransom-as-a-Service (RaaS) operation had a total of $2 billion in earnings. In a pay scheme of 60%-40% (70%-30% in some cases), giving the larger percentage of the payments to their affiliates, they claim that they personally earned $150 million from their operations.

Figure 1: GandCrab announces retirement (image from twitter: @CryptoInsane)

Arrival on the Ransomware Scene

GandCrab first appeared on exploit.in, a Russian hacking forum, on January 28, 2018, at a time when file-encrypting malware distribution was seemingly declining. Despite this, GandCrab was able to make a significant impact, infecting more than 50,000 victims in just their first month of operation.

They were also notable at the time because they were the first criminal organization to only accept DASH cryptocurrency as ransom payment, although they later decided to accept other cryptocurrencies. They also hosted their C2s using the .BIT TLD using a centralized DNS server (a.dnspod.com), which nominally claimed to mirror the namespace of Namecoin. While .BIT is commonly associated with the NameCoin organization for their decentralized DNS project, GandCrab's association with NameCoin was later debunked by the organization.

Figure 2: GandCrab's advertisement post in the Russian forum exploit.in (image from twitter: @CryptoInsane)

Aggressive Distribution

GandCrab's aggressive distribution network was built through its affiliate program and partnerships with other services, such as the binary crypter NTCrypt, along with other actors with expertise in distribution through RDP and VNC. At first, they only targeted western countries, primarily in Latin America. Later, they expanded to partnering with malware distributors in China and South Korea, with our detection of a spam campaign delivering a GandCrab payload targeting South Korea as recently as last April.

An Unusual But Probably Effective Marketing Tactic

Due to the rapid development of GandCrab, FortiGuard Labs as well as other security researchers have been actively monitoring changes between releases. In addition to new features, these have also included public stunts through novelty messages that the threat actors embedded to their binaries as a way to taunt researchers and security organizations. This approach created noise, which may have made them arguably one of the most covered and talked about Ransomware families of the past year. This unusual strategy demonstrated an almost unprecedented level of criminal bravado, and even a sense of invincibility, since they were able to release public announcements that messed with the security community without any repercussions.

Figure 3: Messages embedded by threat actors to taunt researchers and organizations

In another unusual marketing tactic, GandCrab actors also used reports from security companies to promote the success of their service, while mocking their adversaries.

Figure 4: GandCrab advertisement using reports from security companies as their signature

Agile Development

Part of GandCrab's success was due to their use of an agile development approach that enabled rapid releases of new versions. This was best described in our article on the development of GandCrab v4.x. A detailed discussion of the full timeline of GandCrab development can also be found in our AVAR2018: GandCrab Mentality presentation.

Figure 5: GandCrab v4.0-v4.4 timeline

Bugs, Breaches, and GandCrab's Demise

Using this agile development approach enabled them to successfully evade detection by many security companies. A good example of this is when Ahnlab released a vaccine tool to prevent the malware from executing in a system by creating a file that the malware checked before performing its encryption routine. This started a tit-for-tat between the two, which even led to the threat actors disclosing a Denial-of-Service attack POC against one of Ahnlab's products. This was also discussed in our article on the GandCrab v4.x timeline.

However, GandCrab was no exception to the drawbacks of using a fast-paced development approach, as bugs and loopholes began to be discovered in distributed versions. For instance, in the very early versions of the malware they were using hardcoded RC4 keys to encrypt their outbound traffic that also contained the private keys, which would have enabled to the decryption of the victim's ransomed files. Another simple but serious slip-up was when they failed to set a flag when generating their RSA keys. This led to a copy of the private key being stored locally on the victim's system. We also discussed a bug that we found when they first added the feature that changed the wallpaper of their victims. However, they quickly fixed these mistakes in the next release.

But perhaps their biggest mishap – one that we believe led to their eventual demise – were breaches to their server-side infrastructure, which led to leaks of the private keys of victims. A month after their operation began, BitDefender, in collaboration with Europol, released a free decryption tool for victims of GandCrab v1. At the time, there was very limited information as to how they were able to do this – at least until the ransomware perpetrators themselves announced that their payment page has been compromised, which we suspect led to the creation of the decryption tool.

Figure 6: GandCrab posts about the breach to their payment page

We believe that similar breaches eventually led to the subsequent release of the decryption tool used to decrypt files encrypted by new versions of the malware. In fact, just two weeks after GandCrab's retirement announcement, BitDefender released a new version of a decryption tool that supports the latest (v5.2) version of the malware.

Solution

FortiGuard customers are protected by the following:

- Latest versions of GandCrab are detected by our specific and heuristic detections
- FortiSandbox rates the GandCrab's behavior as high risk

Conclusion

GandCrab was a Ransomware-as-a-Service malware managed by a criminal organization known to be confident and vocal, while running a rapidly evolving ransomware campaign. Through their aggressive, albeit unusual, marketing strategies and constant recruitment of affiliates, they were able to globally distribute a high volume of their malware.

However, through a recent forum post, the GandCrab team has now publicly announced the end of a little more than a year of ransomware operations, citing staggering profit figures. However, considering how witty and novel this threat group has been throughout the course of their campaign, it wouldn't be a surprise if this retirement announcement was just another of their many public stunts. If there's one thing that sets these threat actors apart from other groups, it is that they are unpredictable; so there is always the possibility that they might re-surface in one form or another. In the meantime, FortiGuard Labs will continue to monitor for any new activities from this group.

-= FortiGuard Lion Team =-

Learn more about FortiGuard Labs and the FortiGuard Security Services portfolio. Sign up for our weekly FortiGuard Threat Brief.

Read about the FortiGuard Security Rating Service, which provides security audits and best practices.