Taiwan targeted with new cyberespionage back door Trojan

symantec.com/connect/blogs/taiwan-targeted-new-cyberespionage-back-door-trojan

March 28, 2016

Symantec Official Blog

Backdoor.Dripion was custom developed, deployed in a highly targeted fashion, and used command and control servers disguised as antivirus company websites.

By: Jon_DiMaggioSymantec Employee

- Created 29 Mar 2016
- : 日本語

View the indicators of compromise.

In late August 2015, Symantec identified a previously unknown back door Trojan (Backdoor.Dripion) infecting organizations primarily located in Taiwan, as well as Brazil and the United States. Dripion is custom-built, designed to steal information, and has been used sparingly in a limited number of targeted attacks. The attackers behind this campaign went to some lengths to disguise their activities, including using domains names disguised as antivirus (AV) company websites for their command and control (C&C) servers. These attacks have some links to earlier attacks by a group called Budminer involving the Taidoor Trojan (Trojan.Taidoor).

The threat posed by custom malware such as Dripion illustrates the value of multilayered security. Unknown threats may evade signature-based detection, but can be blocked by other detection tools which identify malicious behavior.

Background

Our investigation began when we received three file hashes, which we determined to have the functionality of a back door with information-stealing capabilities. The malware appeared to be new, rarely detected, and not publicly available. As we analyzed the binary and compared it against other known back door Trojans, we realized this was custom-developed malware.

Developing a back door with information-stealing capabilities designed to evade detection requires both knowledge and funding. Usually when we see a new back door Trojan like this, it is tied to organizations involved in cyberespionage campaigns.

Malware downloader

One of the first steps taken when investigating malware is to determine how it is getting onto a victim's computer. Many publicly available downloaders exist; however, only a few unique downloaders have been used over the past few years that have been exclusive to cyberespionage activity. Since Dripion appeared to be used by a single attacker against a small target group, we wanted to determine if the downloader could provide additional evidence to help attribute the threat to any known threat groups.

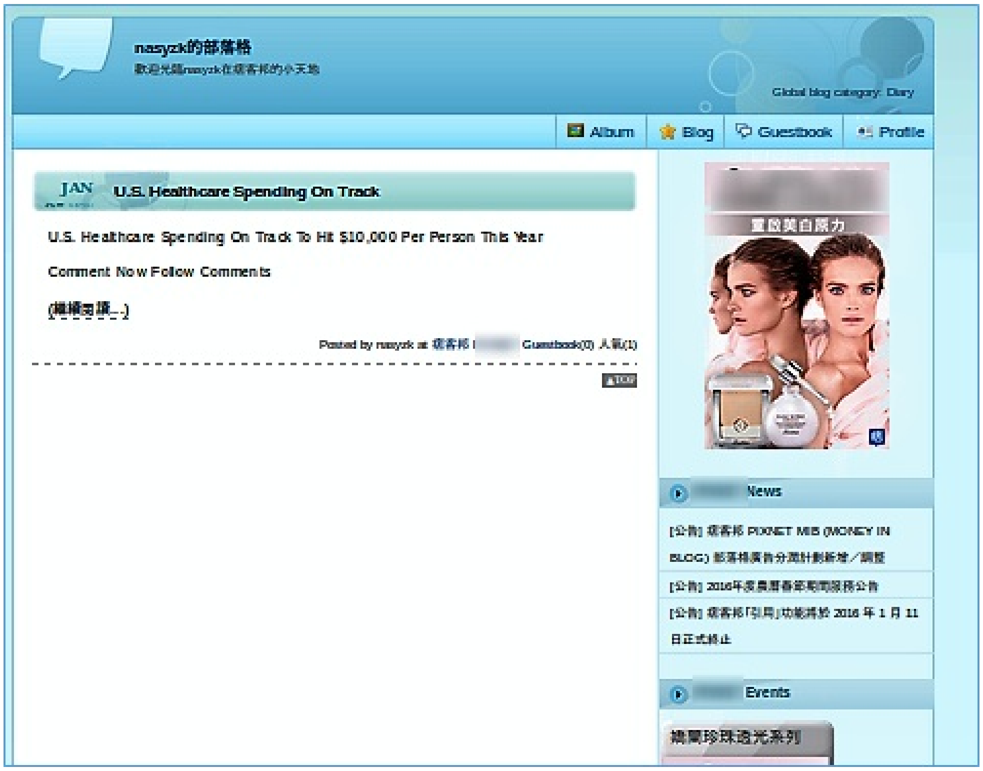
The downloader was identified as Downloader.Blugger (MD5: 260f19ef39d56373bb5590346d2c1811). It is not a new piece of malware, having been in existence since at least 2011. How the victim was infected with Blugger is currently unknown.

Blugger used encryption to make its infrastructure and commands queried in the URL requests harder to detect. After decrypting however, we identified the following URL requests:

- http://classic-blog.[REDACTED DOMAIN 1].com/nasyzk/20002630
- http://nasyzk.[REDACTED DOMAIN 2].net/blog/post/251315428

Both of the domains we analyzed in the URLs requested by the downloader are publicly accessible blogs. The downloader contacts these blog URLs in order to retrieve Dripion for installation.

The blog posts are primarily in English yet most of the targets are based in Taiwan. As illustrated in Figure 1, one of the blogs references US healthcare spending. It is unknown if the attacker created the blog or simply compromised another to use in their attacks. If the blog was compromised, then the attacker likely would not create posts themselves as it would show the blog's creator that something was awry. If the blog was created by the attacker, it may be an attempt to develop a blog with topics that would likely be of interest to the intended target. Most of the blogs were related to news events.



nasyzk的部落格

歡迎光臨nasyzk在痞客邦的小天地

Global blog category: Diary

U.S. Healthcare Spending On Track

U.S. Healthcare Spending On Track To Hit $10,000 Per Person This Year

Comment Now Follow Comments

(繼續閱讀...)

Posted by nasyzk at 痞客邦 [redacted] Guestbook(0) 人氣(1)

[redacted] News

[公告] 痞客邦 PIXNET MIB (MONEY IN BLOG) 部落格廣告分潤計劃新增／調整

[公告] 2016年度農曆春節期間服務公告

[公告] 痞客邦「引用」功能將於 2016 年 1 月 11 日正式終止

[redacted] Events

Figure 1. Screenshot of one of the blogs used to infect the victim with Dripion malware

The Dripion back door Trojan

Once Dripion is installed, the attacker can access the user's computer. Dripion has the functionally of a back door Trojan, letting attackers upload, download, and steal pre-determined information from the victim, and execute remote commands. Information such as the victim's computer name and IP address are automatically transmitted to the C&C server upon the initial infection.

Command	Description
GoSleep	Sleeps for 10 minutes
GoKill	Attempts to delete itself and ends its activities
GoBye	Disconnects from the computer
nodata	Similar to GoBye
Command	Execute command (lpCommandLine in CreateProcessA), redirect result through pipe to .tmp file and Download file
UpFile	Write data in file on victim's computer
DownFile	Write data to a remote open file (InternetWriteFile). The .tmp file used may be deleted after success operation.
ExecuteFile	Create a new process (CreateProcessA)

Table 1. Commands associated with the Dripion malware

Additionally, the developer of the Dripion malware used XOR encoding for both the binary configuration file (XOR: 0xA8) as well as network requests with the C&C server (XOR: 0xA3), to make detection more difficult.

Dripion has been identified in multiple variations and has version numbers hardcoded within the malware. This indicates that the attackers have the ability to both create and develop their own custom malware as well as update their code to provide new capabilities and make detection more difficult.

Ties to previous cyberespionage activity
The use of publicly accessible blogs to distribute malware is a tactic we have seen previously, but few cyberespionage groups have used this technique. Fewer still have used this strategy to deliver custom-developed malware not often seen in the wild.

The first piece of evidence pointing towards a link with previous cyberespionage campaigns was the use of the Blugger downloader, which has only been used by a group Symantec calls Budminer. This group has used Blugger to distribute its own custom malware known as Taidoor (Trojan.Taidoor). Symantec has previously written about Budminer's Taidoor campaigns. Significantly, this is the first time we have seen Blugger used to deliver malware other than Taidoor.

Further investigation uncovered a second tie with earlier Budminer activity. One of the Blugger samples associated with Dripion connected with a root domain also used in Taidoor-related activity.

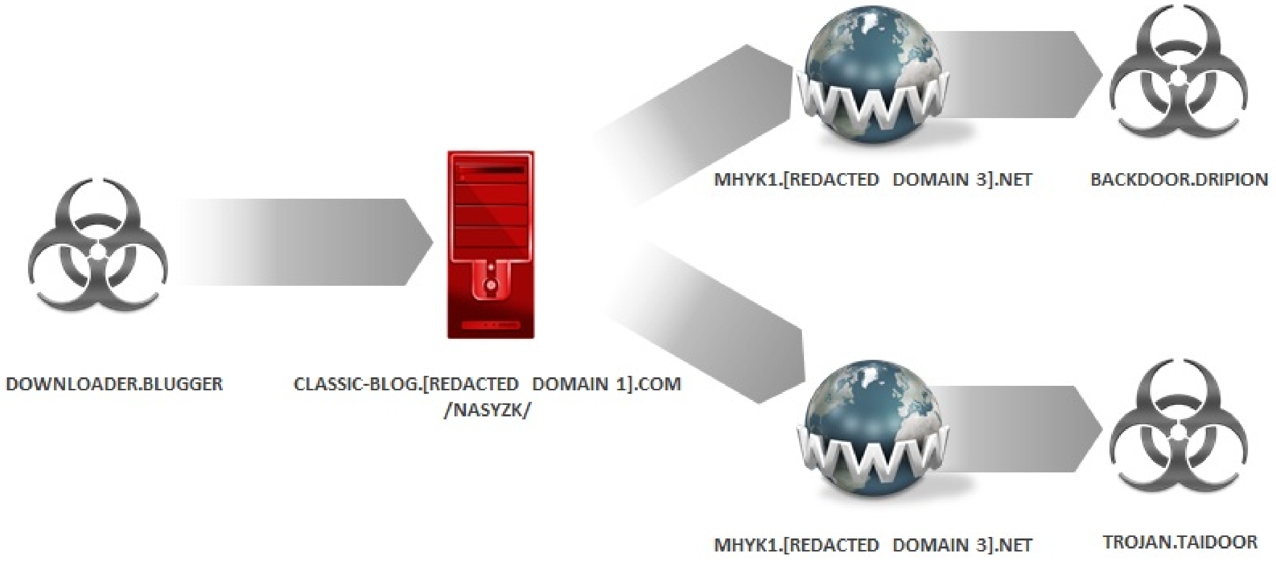

MHYK1.[REDACTED DOMAIN 3].NET
BACKDOOR.DRIPION
DOWNLOADER.BLUGGER
CLASSIC-BLOG.[REDACTED DOMAIN 1].COM /NASYZK/
MHYK1.[REDACTED DOMAIN 3].NET
TROJAN.TAIDOOR

Figure 2. Dripion and Taidoor share ties with the same root domain.

Both of the URL queries originated from the Blugger downloader which connected to the blog classic-blog.[REDACTED DOMAIN 1].com. They then call out to subdomains of the domain [REDACTED DOMAIN 3].net. Both Dripion and Taidoor not only connected to the same website (classic-blog.[REDACTED DOMAIN 1].com) but also used the same URL (classic-blog.[REDACTED DOMAIN 1].com /nasyzk/[ENCODED TEXT]) to obtain the encrypted C&C configuration.

Targeting

Symantec first identified activity involving Dripion in September 2015. Based on the timestamp of the earliest known sample however, Dripion may have been in existence since 2013. The Dripion activity that we have analyzed is extremely targeted and has involved far fewer victims compared to the number of users infected with Taidoor.

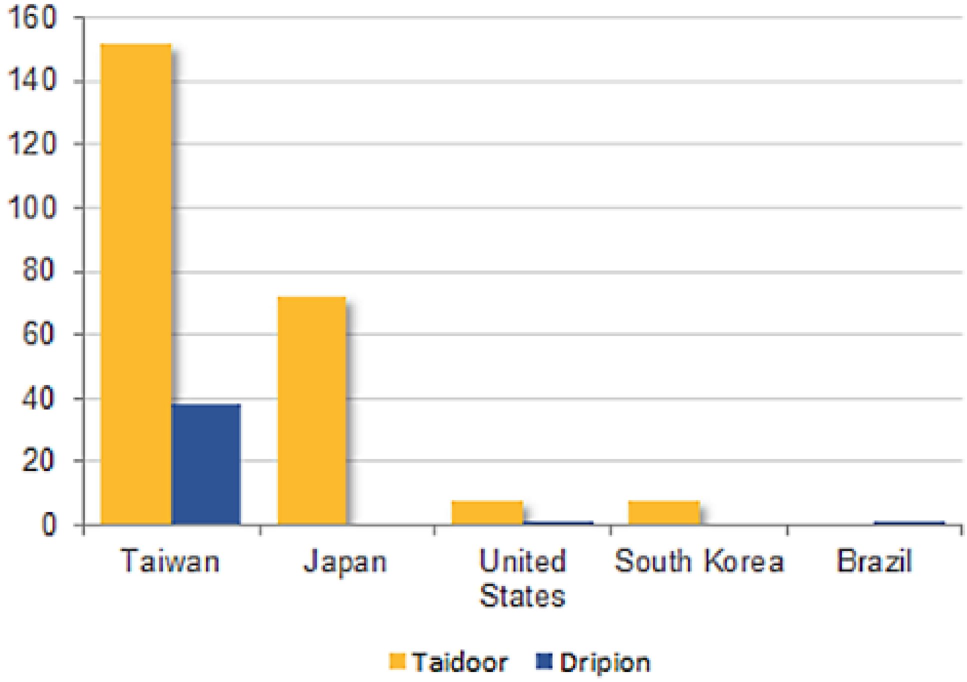


Figure 3. Detection of unique Dripion and Taidoor file hashes by region

The similarity between the two sets of activity is the number of unique file hashes found infecting users located in Taiwan.

Unfortunately, we need more data to determine if the timestamps associated with Dripion dating back to November 2013 (7ad3b2b6eee18af6816b6f4f7f7f71a6) are legitimate or if they have been forged. The earliest known Dripion activity we were able to validate took place in November 2014. Despite the one-year gap in activity, it is possible that campaigns involving Dripion happened during this period and went undetected due to its small target window.

Another interesting tactic used to deceive potential targets lies within the C&C infrastructure. The attackers created multiple domains with names similar to that of legitimate companies and websites in the antivirus community. For example the domains hyydn.nortonsoft[.]com and mhysix.mcfeesoft[.]com were both C&C domains used in attacks. Using typo-squat domains to mimic legitimate sites is a tactic frequently used to trick the targets as well as defenders, in an effort to make the domains blend in with normal activity.

Conclusion

We began this investigation with what we believed was a new campaign using an unidentified back door Trojan against targets primarily in Taiwan. As the investigation grew we found multiple ties between this newly discovered attack and activity associated with the Budminer cyberespionage group:

- Same unique downloader (not publicly available and only seen used in China-based cyberespionage activity)
- The unique downloader used by both Dripion and Taidoor encrypts data using the victim's MAC address as the RC4 key
- Use of the same blogs for distribution of malware (Taidoor and Dripion)
- Use of shared C&C infrastructure (at the root domain level)
- Similar targeting (primary location of targets is Taiwan)

We compared Dripion against Taidoor malware samples to determine if there was any shared code or if it may have originated from the same developer. Our findings concluded there were no similarities between the two malware families. However, the downloader used by both malware families has unique attributes, and we believe it to be from the same developer.

So what does all this mean? Attribution of cyberespionage groups is difficult and needs to be done carefully based on fact and not assumptions. We have a number of ties between the two sets of activity. Not all of the ties are strong on their own, but together provide a strong case that there is a relationship between the groups targeting Taiwan using Dripion and Taidoor malware.

Based on the evidence we have presented Symantec attributed the activity involving the Dripion malware to the Budminer advanced threat group. While we have not seen new campaigns using Taidoor malware since 2014, we believe the Budminer group has changed tactics to avoid detection after being outed publicly in security white papers and blogs over the past few years.

This investigation is just one example of Symantec’s ongoing effort to identify unknown emerging threats. By remaining one step ahead of adversaries, we can protect customers with intelligence driven security.

Mitigation advice

- Always keep your security software up to date to protect yourself against any new variants of this malware.
- Keep your operating system and other software updated. Software updates will frequently include patches for newly discovered security vulnerabilities which are frequently exploited by attackers.
- Delete any suspicious-looking emails you receive, especially if they contain links or attachments. Spear phishing emails are frequently used by cyberespionage attackers as a means of luring victims into opening malicious files.

Protection

Symantec and Norton products protect against these threats with the following detections:

Indicators of compromise

File hashes

- 2dd931cf0950817d1bb567e12cf80ae7
- 3652075425b367d101a7d6b6ef558c6c
- 59ff5624a02e98f60187add71bba3756
- 865d24324f1cac5aecc09bae6a9157f5
- eca0ef705d148ff105dbaf40ce9d1d5e
- f4260ecd0395076439d8c0725ee0125f
- 3652075425b367d101a7d6b6ef558c6c
- 285de6e5d3ed8ca966430846888a56ff
- 31f83a1e09062e8c4773a03d5993d870
- 4438921ea3d08d0c90f2f903556967e5
- 7ad3b2b6eee18af6816b6f4f7f7f71a6
- b594d53a0d19eaac113988bf238654d3
- c3e6ce287d12ac39ceb24e08dc63e3b5
- e0c6b7d9bdae838139caa3acce5c890d
- e7205c0b80035b629d80b5e7aeff7b0e
- c182e33cf7e85316e9dc0e13999db45e
- 272ff690f6d27d2953fbadf75791274c
- ae80f056b8c38873ab1251c454ed1fe9
- 260f19ef39d56373bb5590346d2c1811
- FE8D19E3435879E56F5189B37263AB06
- 68BEBCD9D2AD418332980A7DAB71BF79
- CBDE79B6BA782840DB4ACA46A5A63467

Infrastructure

- hyydn[.]nortonsoft.com
- mhysix[.]mcfeesoft.com
- gspt[.]dns1.us
- unpt[.]defultname.com
- 198.144.100.73
- 208.61.229.10
- 200.215.222.105
- 61.222.137.66
- 103.240.182.99

- Tags: Products, Endpoint Protection, Security Response, APT, Backdoor.Dripion, Cyberespionage, Downloader.Blugger, Taiwan, targeted attacks, Trojan.Taidoor, United States

- Subscriptions (0)