Malware stored in Google Sites sends data to the MySQL server

Recently, security researchers have found some malware hosted on the Google Sites platform to build on websites. However, the real threat lies in the fact that a fraudster who steals information can take advantage of this flaw to send the victim's data to their own controlled MySQL server simply and quickly. .

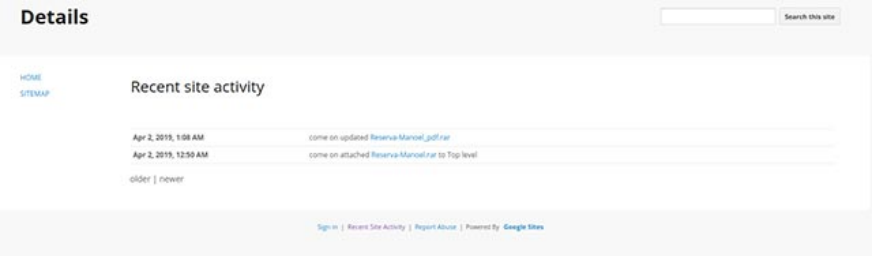
Recently, security researchers have found some malware hosted on the Google Sites platform to build on websites. However, the real threat lies in the fact that fraudsters steal information can take advantage of this vulnerability to send victim data to their own controlled MySQL server in a simple and quick way.

1. Apple updates XProtect to block 'Windows' malware on a Mac

This newly discovered malware is named LoadPCBanker. In essence, it is an executable file disguised as a PDF file containing the reservation information of a guest house or hotel, and also 'residing' in the File Cabinet's storage space for Google Site.

Accordingly, the name of the extracted PDF file will be "PDF Request Details MANOEL CARVALHO hospedagem familiar detalhes PDF.exe". Based on the name of the extracted PDF file, it can be seen that the attacker is targeting English-speaking and / or Portuguese-speaking victims.

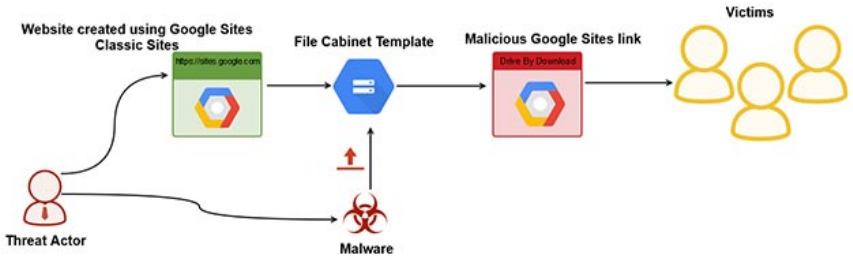
Security researchers in Netskope have officially reported on related Google sites that hosted malware on April 12. However, Google has not taken any action to prevent or fix the problem. At the time of writing, the malware samples are still stored and downloadable!



1. Malicious ad campaigns abuse Chrome to steal 500 million iOS user sessions

When using VirusTotal's malware scanning service, the researchers noted that 47 out of 66 anti-virus tools were listed on the VirusTotal platform, which could detect the malicious code.

"Attackers are more likely to use the Google sites to create an arbitrary website, then use the cabinet file template to upload payloads and finally send the resulting URL to potential targets," experts said. security expert Netskope said.



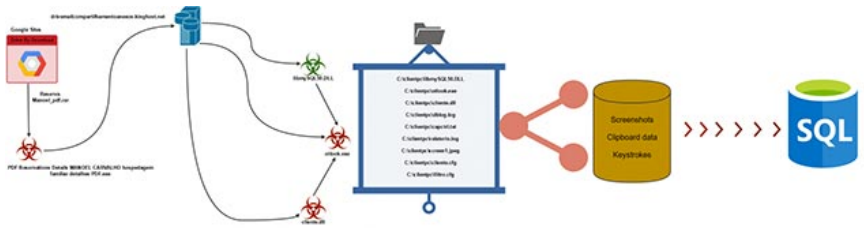
1. Adblock Plus filter can be exploited to run malicious code

When launched, the fake PDF will silently create a directory and download the payloads named libmySQL50.DLL, otlook.exe and cliente.dll from the Kinghost file hosting site.

It can be clearly seen that the payload 'otlook.exe' is so named in order to impersonate the Microsoft Outlook email application. In fact, this payload is 'a dangerous information stealer', can take screenshots, record the data stored in the clipboard and also record the login passwords on the victim system.

Besides, it also functions as a downloader for files that contain login information and connection details for SQL databases that receive stolen information. This file will then be updated continuously with new access information.

In order to 'transport' data more efficiently, more malicious code will take advantage of the help of the DLL component, which is a library that facilitates connection to database servers easily. easier.



1. Reveal personal data of more than 1.3 million people from a vulnerability in web application

A obtained database record shows that there are two information tables: The first table displays information about the infected system, while the other one contains information about the stolen clipboard data as follows:

```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| album              |
| information_schema |
+--------------------+
2 rows in set (0.69 sec)

mysql> show tables;
+---------------------------+
| Tables_in_album           |
+---------------------------+
| CLIPBOARD                 |
| MAQUINA                   |
+---------------------------+
2 rows in set (0.24 sec)
```

"During the analysis, we have determined that the attacker seems to be particularly interested in monitoring a specific system of devices and taking screenshots of some information from victim computers. This result was obtained after we noticed a lot of feedback from infected computers, but only a few were actively monitored, "the team said.

Besides, the researchers also believe that in fact, there was a similar type of malware that appeared around the beginning of 2014. Meanwhile, recent offensive campaigns began to be recorded from about February this year. It is still unclear whether there is only one person behind all of these attacks, or malware code shared with various cybercrime organizations.