Import 2022-11-30 11:16

Malware uses namesilo Parking pages and Google's custom pages to spread

Alex.Turing, **Hui Wang**, **YANG XU**

Nov 12, 2021 • 3 min read

Abstract

Recently, we found a suspicious GoELFsample, which is a downloder mainly to spread mining malwares. The interesting part is that we noticed it using namesilo's Parking page and Google's user-defined page to spread the sample and configuration. Apparently this is yet another attempt to hide control channel to avoid being tracked|monitored|blocked from the malicious actor and it probably has served them well.

The exact sample had been reported by Tencent security team, but the analysis of the propagation is not quite accurate. It is often thought that during the domain parking period (Domain Parking), the content displayed on the page is managed by the domain parking provider, and the actual owner of the domain cannot modify its page content. However, in this case, the domain parking provider allows the domain owner to customize the parking page. The attacker took advantage of this, along with the custom pages provided by Google, to spread his malware.

This has two obvious benefits: on the one hand, the attacker hardly needs to pay any bandwidth and server costs for the malicious code distribution; on the other hand, as the bots 'talk' to the domain parking provider and google, the control traffic totally blends in, making it very difficult to be monitored and blocked.

From our DNSMon/DTA monitoring data, we see this new trend has shown signs of increase in recent months.

Origins

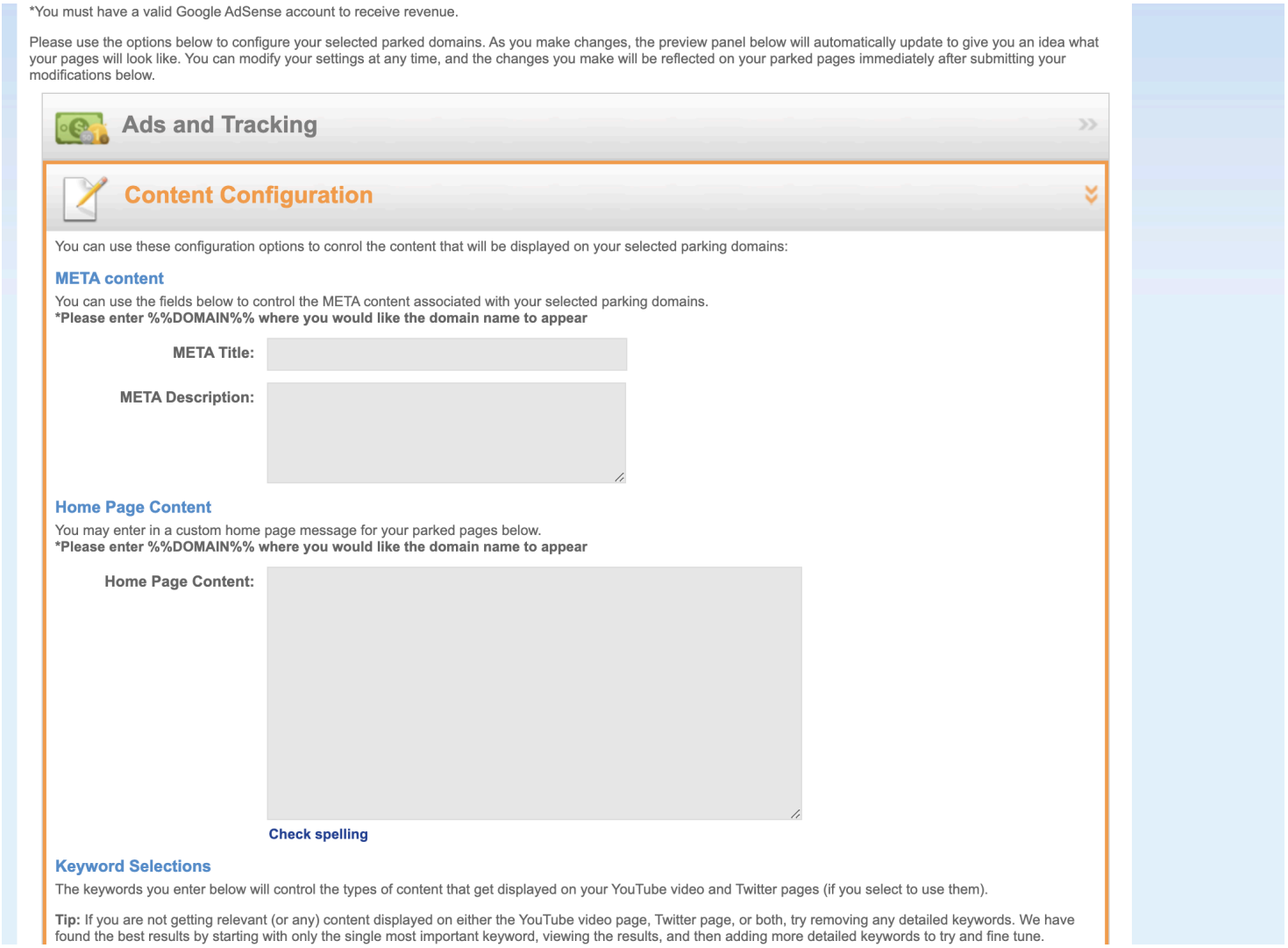
On 10.13, our BotnetMon IDed a suspicious GoELF sample that would request a known suspicious domain www[.]hellomeyou.cyou, which Tencent had covered in a previous mining malware report.

There is nothing particularly interesting regarding to the mining part, however, we noted that the DNS resolution of www.hellomeyou.cyou has historically been CNAME to a parking domain parking.namesilo.com

```
2020-11-09 2021-11-07 19904   www.hellomeyou.cyou CNAME   parking.namesilo.com
```

The parking domains are usually registered but not activated, how could they be a part of the malicious sample distribution?

Logging into namesilo's user service interface, we learned that its ParkingPage is user-definable content, which in turn gives hacker groups the opportunity to exploit it.



Multiple historical snapshots of the site in our DNSMon system showed that the title of the page was a malicious sample link, and the description of the page was xmrig configuration.

At the same time, there is also the exploitation of github and google links in the description, which further analysis shows that both are a part of malware

distribution channel. Among them, google's custom page contains a base64 encoded xmrig mining software.

When talk about Parking domain related security issues, many articles out there would refer to some well known problems, mainly Malvertising and abuse related.

In this case, it is different. This particular case uses the “user-customize" parking page directly for its control channel. Hackers do not need to have their own machines and IPs, they just use the parked pages provided by the domain registrar, as well as the custom pages of google(see the following snapshot) to help spreading their malware. By doing this, the malicious actor totally goes under the radar because all the control channel traffic use these totally legit "public facilities”

Correlation

Through the page similarity correlation analysis, we see a total of 8 web records with similar configurations in the historical data.

	Tbeg	Tend	Src	URL	Title
+	2021-06-16	2021-06-16 07:21:34	hspike,domain	http://json.hvtde6ew5.top/	http://138.124.180.20:8080/Cabbie
+	2021-06-23	2021-06-23 02:59:49	nad,domain	http://www.hellomeyou.cyou/	http://35.182.200.15:8083/zi
+	2021-06-28	2021-06-28 03:38:32	nad,domain	http://hideme.cyou/	http://138.124.180.20:8080/Cabbie
+	2021-06-28	2021-06-28 09:04:44	nmd,domain	http://gannimachoubi.cyou/	http://35.182.200.15:8083/choubi
+	2021-06-28	2021-06-28 21:16:18	nmd,domain	http://www.gannimachoubi.cyou/	http://35.182.200.15:8083/choubi
+	2021-08-31	2021-09-05 10:36:59	spike,nd	http://www.hellomeyou.cyou	http://35.182.200.15:8083/zi
+	2021-11-09	2021-11-09 17:20:57	webdb	http://www.hideme.cyou	http://138.124.180.20:8080/Cabbie
+	2021-11-09	2021-11-09 16:40:14	webdb	http://www.gannimachoubi.cyou	https://sites.google.com/view/hellomeyou/yyyyy/zhu

Corresponding to the capture of 2 samples

We retraced the history of the malicious samples involving parking.namesilo.com in our BotnetMon and could see an upward trend since June this year, looks like this technique might have been working well, we will keep an eye on it.

IOC

```
485baeb56cde578cdfe8f88a04e29212
96dc8dcd5bf8f6e62c3ce5219e556ba3
f06d38aa4f472a7e557069cc681d997c
f24dc9c47d3698d94d60a08258bd2337
f6321c2f3bc22085e39d9f54e2275ece

hideme.cyou
hellomeyou.cyou
gannimachoubi.cyou
hvtde6ew5.top

https://sites.google.com/view/dogtoken/Home
https://sites.google.com/view/tabjoy/
```


0 Comments

Login

G

Start the discussion...

LOG IN WITH

OR SIGN UP WITH DISQUS

Name

Share

Best Newest Oldest

Be the first to comment.

Subscribe Privacy Do Not Sell My Data

Import 2022-11-30 11:16

快讯：使用21个漏洞传播的DDoS家族WSzero已经发展到第4个版本

P2P Botnets: Review - Status - Continuous Monitoring

P2P 僵尸网络：回顾·现状·持续监测

See all 249 posts →

滥用ClouDNS服务，github.com无辜躺枪

摘要 威胁情报的应用，始终存在着“漏报”和“误报”的平衡，为了减少可能的误报带来的业务影响，你的威胁情报白名单中是否静静的躺着 www.apple.com、www.qq.com、www.alipay.com 这样的流行互联网业务域名呢？你的机器学习检测模型，依照历史流量，是否会自动对 .qq.com、.alipay.com 这样的...

Nov 18, 2021 · 11 min read

和Google的自定义页面来传播恶意软件

摘要 近期，我们发现一个GoELF可疑样本，分析得知是一个downloder，主要传播挖矿。有意思的地方在于传播方式，利用了namesilo的Parking页面，以及Google的用户自定义页面来传播样本及配置，从而可以躲避跟踪。 该样本最开始被友商腾讯安全团队捕获，不过传播链条分析中，对namesilo parking域名的分析不太准确。往往大家以为，域名...

Nov 11, 2021 · 5 min read