

Import 2022-11-30 11:16

快讯：利用namesilo Parking和Google的自定义页面来传播恶意软件



Alex.Turing, Hui Wang, YANG XU

Nov 11, 2021 • 5 min read

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，域名停靠期间(Domain Parking)，页面显示内容是被域名停靠供应商强制限定的，域名实际拥有者并不能修改其页面内容。但在这个案例中，域名停靠供应商允许域名拥有者自定义停靠页面。攻击者利用了这一点，再加上Google提供的自定义页面来传播自己的木马。

这样做有两个显而易见的好处：一方面攻击者几乎不需要为恶意代码的传播付出任何带宽和服务器的费用；另一方面攻击者将自己的恶意行为隐藏在大型互联网基础服务供应商的巨大流量中，所谓大隐于市，以此隐藏自己的行踪使得更难被检测和追踪。

在我们的DNSMon/DTA监测数据中显示，这种趋势在最近几月有上升迹象，值得安全社区注意。

缘起

在10.13号，我们的BotnetMon根据样本网络流量，发现一个可疑的GoELF样本，会请求一个已知的可疑域名 `www[.]hellomeyou.cyou`，这个域名在之前腾讯安全团

队的一篇挖矿木马报告中被披露过。

该样本是一个Miner/Downloader，业界公开的沙箱、引擎或报告已有具体分析，我们不再赘述。但是我们注意到，www.hellomeyou.cyou 历史上的DNS解析一直是 CNAME 到一个parking域名 parking.namesilo.com

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

parking的域名一般都是注册但未启用，为何能成为恶意样本传播的一环，这让我们非常好奇。

登陆namesilo的用户服务界面得知，其ParkingPage 是用户可以自己定义内容的，进而给了黑客团伙的利用机会。

*You must have a valid Google AdSense account to receive revenue.

Please use the options below to configure your selected parked domains. As you make changes, the preview panel below will automatically update to give you an idea what your pages will look like. You can modify your settings at any time, and the changes you make will be reflected on your parked pages immediately after submitting your modifications below.

The screenshot shows the 'Content Configuration' section of the NameSilo parking page setup. It includes fields for 'META content' (Title and Description) and 'Home Page Content'. A 'Check spelling' button is also present. A note at the bottom right of the page states: 'Tip: If you are not getting relevant (or any) content displayed on either the YouTube video page, Twitter page, or both, try removing any detailed keywords. We have found the best results by starting with only the single most important keyword, viewing the results, and then adding more detailed keywords to try and fine tune.'

Ads and Tracking

Content Configuration

You can use these configuration options to control the content that will be displayed on your selected parking domains:

META content

You can use the fields below to control the META content associated with your selected parking domains.
*Please enter %%DOMAIN%% where you would like the domain name to appear

META Title:

META Description:

Home Page Content

You may enter a custom home page message for your parked pages below.
*Please enter %%DOMAIN%% where you would like the domain name to appear

Home Page Content:

Check spelling

Keyword Selections

The keywords you enter below will control the types of content that get displayed on your YouTube video and Twitter pages (if you select to use them).

Tip: If you are not getting relevant (or any) content displayed on either the YouTube video page, Twitter page, or both, try removing any detailed keywords. We have found the best results by starting with only the single most important keyword, viewing the results, and then adding more detailed keywords to try and fine tune.

我们DNSMon系统中对该网站的多次历史快照显示，页面的title是一个恶意样本链接，页面的description是xmrig配置。

同时，description中还有对github和google的链接的利用，进一步分析可知，都是恶意软件传播中的一环。其中，google的自定义页面中包含了一个base64编码的xmrig挖矿软件。

很多文章都曾提到过parking和黑产的关系，但大都是指的一个普遍现象：一个域名被注册后，在没有修改DNS记录将其映射到自己的IP之前，基本都是parking状态，可能会被做一段时间的广告推广，可能会用来做引流，可能会涉及二次买卖，之后DNS记录变化，域名被映射到黑客自己控制的IP上，非parking状态，进而被黑产使用。

当前案例，是利用了“用户可控”的parking页面，在保持parking状态的时候，用于恶意软件推广。黑客不需要有自己的机器和IP，就只用域名注册商提供的parking的页面，以及google的自定义页面，来传播自己的木马。黑客团伙利用这些“公共设施”来组织自己的恶意软件传播链条，以部分的逃避跟踪和拦截。

最开始腾讯文中的分析，猜测“hellomeyou这个网站被攻击后，在网站中嵌入了这些内容。”，应该是不准确的，这是黑客团伙刻意的利用。

拓展

通过页面相似性关联分析，我们在历史数据中一共获取了8条类似配置的web记录：

对应捕获到2个样本

我们回溯了360Netlab BotnetMon 中，涉及到 parking.namesilo.com 的恶意样本的历史情况，可以看到从6月份开始有了一个明显的突增。这个突增可能意味着该种利用方式、或者parking域名其他的利用方式，被黑客组织用的越来越多。

总结

IOC:

```
485baeb56cde578cdfe8f88a04e29212  
96dc8dc5bf8f6e62c3ce5219e556ba3  
f06d38aa4f472a7e557069cc681d997c  
f24dc9c47d3698d94d60a08258bd2337  
f6321c2f3bc22085e39d9f54e2275ece
```

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

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

上述的分析过程，融合了PDNS、Web数据、样本以及沙箱等多维度的数据。我们近期推出了DTA产品，从DNS流量数据入手，深入分析客户流量，利用高质量威胁情报以及关联分析、机器学习、行为分析等技术，帮助客户及时定位未知威胁、高级威胁，降低攻击影响面，提升情报生产及安全运营能力。



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](#)

— 360 Netlab Blog - Network Security Research Lab at 360 —

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·

Import 2022-11-30 11:16

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

Abstract Recently, we found a suspicious GoELFsample, which is a downloader 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

DDoS

Abcbot, an evolving botnet

Background Business on the cloud and security on the cloud is one of the industry trends in recent years.

360Netlab is also continuing to focus on security incidents and trends on the cloud from its own expertise in the technology field. The following is a recent security incident we observed,

持续监测

See all 249 posts →



Nov 12,

3 min



2021

read



Nov 9,

2021

10 min



read