https://www.infosecurity-magazine.com/news/phishing-campaigns-target-sports/

18 JUN 2018 [NEWS](https://www.infosecurity-magazine.com/news/)

Phishing Campaigns Target Sports Fans, Consumers

[Kacy Zurkus](https://www.infosecurity-magazine.com/profile/kacy-zurkus/) News Writer

Two phishing campaigns have been targeting consumers of both the FIFA World Cup and one of its longtime partners, [Adidas](https://www.adidas.com/us). One campaign attempts to lure victims into clicking on a malicious link under the guise of downloading a World Cup schedule of fixtures and a result tracker, while the second promises a “free” $50-per-month subscription for Adidas shoes.

Today [Check Point](https://www.checkpoint.com/) announced that it has discovered a new phishing campaign linked to the start of the World Cup that targets soccer fans. A known malware that is often used to install potentially unwanted programs (PUPs) and toolbars, adware or system optimizers called DownloaderGuide is embedded in the attachment. Researchers discovered nine different executable files delivered in emails with the subject: “World\_Cup\_2018\_Schedule\_and\_Scoresheet\_V1.86\_CB-DL-Manager.”

First identified on 30 May, Check Point said the campaign peaked on 5 June but has re-emerged since the start of the games. “Events that attract huge amounts of popular interest are seen by cyber-criminals as a golden opportunity to launch new campaigns,” Maya Horowitz, Check Point’s threat intelligence group manager, said in today’s press release.

“With so much anticipation and hype around the World Cup, cyber-criminals are banking on employees being less vigilant in opening unsolicited emails and attachments. As such, it is critical that organizations take steps to remind their employees of security best practices to help prevent these attacks being successful," Horowitz said.

The second phishing campaign, which targets Adidas customers, uses a different tactic, luring victims in with a homographic link that uses a vertical line in place of where the “i” in Adidas should be. “The use of punycode-based homoglyph email and web domains are an increasingly used technique to spoof users in email phishing attacks,” said Matthew Gardiner, cybersecurity expert, [Mimecast](http://www.mimecast.com/).

“Given the thousands of possible iterations of a domain that are now possible with these internationalized domain names and the thousands of available top-level domains that are also available, such as .co, .cf, .ml and many others, there is no possibility of preregistering these domains to keep them out of the hands of the bad actors. The only reasonable approach is to have automated email security controls to detect these types of impersonation attacks to protect your organization. Expecting your users to figure it out is increasingly unrealistic,” Gardiner said.

https://www.infosecurity-magazine.com/news/phishing-campaigns-target-sports/

钓鱼攻击新目标：各国球迷和体育消费者

Kacy Zurkus

6月18日

最近，FIFA世界杯的消费者和FIFA长期合作商家阿迪达斯分别遭受到了两起钓鱼攻击。其中一起是引诱球迷点击下载可获得世界杯赛程和结果的恶意链接，而另一起则是欺骗消费者可以免费获得每月50美金的阿迪达斯鞋类优惠券。

6月18日, Check Point发布消息称其发现了一起与世界杯有关的新钓鱼攻击活动。该攻击的主要手段是引诱球迷们去下载可获得世界杯赛程和结果的恶意文件。打开该文件后会有一个嵌入了名为DownloaderGuide的恶意软件变种的附件，这个恶意软件变种通常用来自动安装一些恶意程序 ，工具栏，广告插件或者是系统优化程序。Check Point研究人员发现，这个攻击活动所包含的9个不同的可执行文件，都是通过一封标题为“World\_Cup\_2018\_Schedule\_and\_Scoresheet\_V1.86\_CB-DL-Manager.”的邮件发送的。

据Check Point表示，这个钓鱼攻击最早是于5月30日发现的，在6月5日活跃度达到一个小高峰。世界杯球赛开幕后又再次活跃。Check Point的威胁情报部门负责人Maya Horowitz在6月18日的媒体报道中表示：“但凡有备受瞩目的事件或活动出现，都会被网络犯罪分子视为发动新攻击活动的最佳机会。参与世界杯的人群众多，各种宣传报道铺天盖地，网络犯罪分子就利用警惕性较低的员工，引诱他们点开由攻击者发送的邮件和其中的附件。所以，各机构必须采取措施，提醒员工做好安全防范，防止这些攻击者达到目的。”

第二个针对阿迪达斯消费者的钓鱼攻击活动则使用了不同的手段，诱使受害者去点击的对应链接是用了一条垂直的线替换了ADIDAS中原有的字母“i”。Mimecast公司的网络安全专家Matthew Gardiner表示：“在邮件钓鱼攻击中，越来越多攻击者使用基于punycode的同形异义钓鱼攻击。”

Gardiner还表示：“由于可以使用的域名成千上万，越来越多顶级域名如.co, .cf, .ml等可供注册，机构已经无法通过预先注册所有相关域名来阻拦黑客利用虚假域名发动攻击。（我认为）唯一可行的办法就是通过邮件安全性自动检测工具去检测这些伪装攻击，从而达到保护企业的目的，毕竟指望用户自己去发现问题已经不可靠了。”

这就迫使恶意文档检测引擎在这方面有很好的防护措施。针对于电子邮件附件的恶意文件，目前大多数引擎主要是针对于可执行文件检测的比较多，而对于文档类型的很少，有的甚至检测不到，这就使这些基于文档的攻击更容易成果，并且具有针对性。

面对与这样的攻击我们建议对于个人用户，

1. 提高对电子有点附件的安全意识，谨慎打开未知邮件的链接和附件
2. 对于未知的域名连接和未知文件，谨慎访问与下载
3. 安装并及时更新使用的防病毒程序，保证数据安全

对于企业用户来说：

1. 在防火墙上添加基于文档的检测模组
2. 及时更新厂家提供的软件

蓝盾在这方面专门针对于恶意文档检测，使用人工智能的方法，能快速有效的检测基于文档的攻击，包括其变异病毒的攻击，并且准确率达到业界水平，并具有一定的抗逃逸能力。按照模块化的思想，我们把基于AI的PDF分类器看作一个独立的检测模组，并把此检测模块集成到安全产品防火墙中。AI引擎带来的优势却是非常明显的。一方面，此引擎本无需频繁更新，一般正常AI引擎的平均更新周期为半年，而规则引擎则为2周；第二方面是AI引擎卓越的低计算资源消耗。