Pawn Storm Abuses OAuth In Social Engineering Attacks

By By: Feike Hacquebord Apr 25, 2017 Read time: 3 min (841 words)

Published: 2017-04-25 · Archived: 2026-04-05 19:17:31 UTC

Pawn Storm is an active and aggressive espionage actor group that has been operating since 2004. The group uses different methods and strategies to gain information from their targets, which are covered in our latest researchnews article. However, they are particularly known for dangerous credential phishing campaigns. In 2016, the group set up aggressive credential phishing attacks against the Democratic National Convention (DNC), German political party Christian Democratic Union (CDU), the parliament and government of Turkey, the parliament of Montenegro, the World Anti-Doping Agency (WADA), Al Jazeera, and many other organizations.

This blog post discusses how Pawn Storm abused Open Authentication (OAuth) in advanced social engineering schemes. High profile users of free webmail were targeted by campaigns between 2015 and 2016.

How is OAuth abused?

OAuth is a way of authorizing third party applications to login to users' online accounts for social media sites, gaming sites, and services like free webmail. The big advantage is that users don't have to reveal their password; instead, the third party applications get a token that can be used for authentication.

While OAuth offers convenience and can be usefully applied in different ways, it may also expose the user to risks. Threat actors can get through the background checks that service providers do before authorizing applications for OAuth use. These actors can then integrate OAuth into advanced social engineering schemes. Some internet service providers only require an email address and a website for third party applications to use OAuth. Because of these policies, experienced actor groups like Pawn Storm can take advantage of OAuth for their credential phishing schemes.

Figure 1. The sequence of Pawn Storm's OAuth abuse

A dissection of Pawn Storm OAuth attacks

In these attacks a user would get a message like this:

Figure 2. A phony email from Pawn Storm

The email poses as an advisory from Gmail and prompts potential victims to install an "official" application called "Google Defender". Normally an internet user will know better than to readily install an application that wasn't asked for.

If the user clicks on the link, it will lead to a page on accounts.google.com that looks like this:

Figure 3. A request to grant access from "Google Defender"

At this point, the user is faced with a legitimate Google site—since all OAuth approvals are done on the site of the service provider—but the application itself is part of a phishing scheme.

"Google Defender" is actually a third party application made by Pawn Storm. After abusing the screening process for OAuth approvals, Pawn Storm's rogue application operates like every other app accepted by the service provider. If the user falls for the scam and clicks the "Allow" button, an OAuth token is provided to the app, giving Pawn Storm semi-permanent access to the target's mailbox.

Apart from targeting Gmail users, Pawn Storm has also abused OAuth in credential phishing attacks against high profile Yahoo users. Here is an example from 2015 where "McAfee Email Protection" is offered.

Figure 4. A convincing Yahoo phishing email

Clicking on the "Try McAfee Email Protection" button would lead to this legitimate website:

Figure 5. This gives the third party app OAuth access

However the application is not a service of Yahoo or a legitimate product of McAfee, but a rogue application used by Pawn Storm. Clicking on the "Agree" button would give Pawn Storm an OAuth token and access to the targets' mailbox. The group then gains access to the mailbox until the token gets revoked by the service provider or the target.

Pawn Storm apparently had some success with this type of attack as it kept sending this kind of social lure during the end of November and the first half of December 2015, as indicated in the next figure.

Figure 6. Overview of Pawn Storm's Yahoo credential phishing campaigns. The blue boxes indicate when Pawn Storm used OAuth lures while red boxes indicate other phishing email strategies

OAuth enhances the user experience on the web. For example, by allowing social networks access to your webmail contact list, it is easier to find friends who are subscribed to the same social network. But while we believe that internet service providers have enhanced security checks of applications that are allowed to use OAuth, internet users are urged to never accept OAuth token requests from an unknown party or a service they did not ask for. Regularly review the applications you have granted access to your mailbox in the security settings of your free webmail or social media service. In case you see a suspicious application immediately revoke the OAuth token.

These are known rogue applications of Pawn Storm that have been used in credential phishing attacks against high profile users (variants of these names are likely to have been used by Pawn Storm as well):

-
-
-
-
-

For more information about Pawn Storm, check out *From Espionage to Cyber Propaganda: Pawn Storm's Activities over the Past Two Years*news article.

Tags
