Update on Pawn Storm: New Targets and Politically Motivated Campaigns

blog.trendmicro.com/trendlabs-security-intelligence/update-pawn-storm-new-targets-politically-motivated-campaigns/

Feike Hacquebord (Senior Threat Researcher)

January 12, 2018

In the second half of 2017 Pawn Storm, an extremely active espionage actor group, didn't shy away from continuing their brazen attacks. Usually, the group's attacks are not isolated incidents, and we can often relate them to earlier attacks by carefully looking at both technical indicators and motives.

Pawn Storm has been attacking political organizations in France, Germany, Montenegro, Turkey, Ukraine, and the United States since 2015. We saw attacks against political organizations again in the second half of 2017. These attacks don't show much technical innovation over time, but they are well prepared, persistent, and often hard to defend against. Pawn Storm has a large toolset full of social engineering tricks, malware and exploits, and therefore doesn't need much innovation apart from occasionally using their own zero-days and quickly abusing software vulnerabilities shortly after a security patch is released.

In summer and fall of 2017, we observed Pawn Storm targeting several organizations with credential phishing and spear phishing attacks. Pawn Storm's modus operandi is quite consistent over the years, with some of their technical tricks being used repeatedly. For example, tabnabbing was used against Yahoo! users in August and September 2017 in US politically themed email. The method, which we first discussed in 2014, involves changing a browser tab to point to a phishing site after distracting the target.

We can often closely relate current and old Pawn Storm campaigns using data that spans more than four years, possibly because the actors in the group follow a script when setting up an attack. This makes sense, as the sheer volume of their attacks requires careful administration, planning, and organization to succeed. The screenshots below show two typical credential phishing emails that targeted specific organizations in October and November 2017. One type of email is supposedly a message from the target's Microsoft Exchange server about an expired password. The other says there is a new file on the company's OneDrive system.

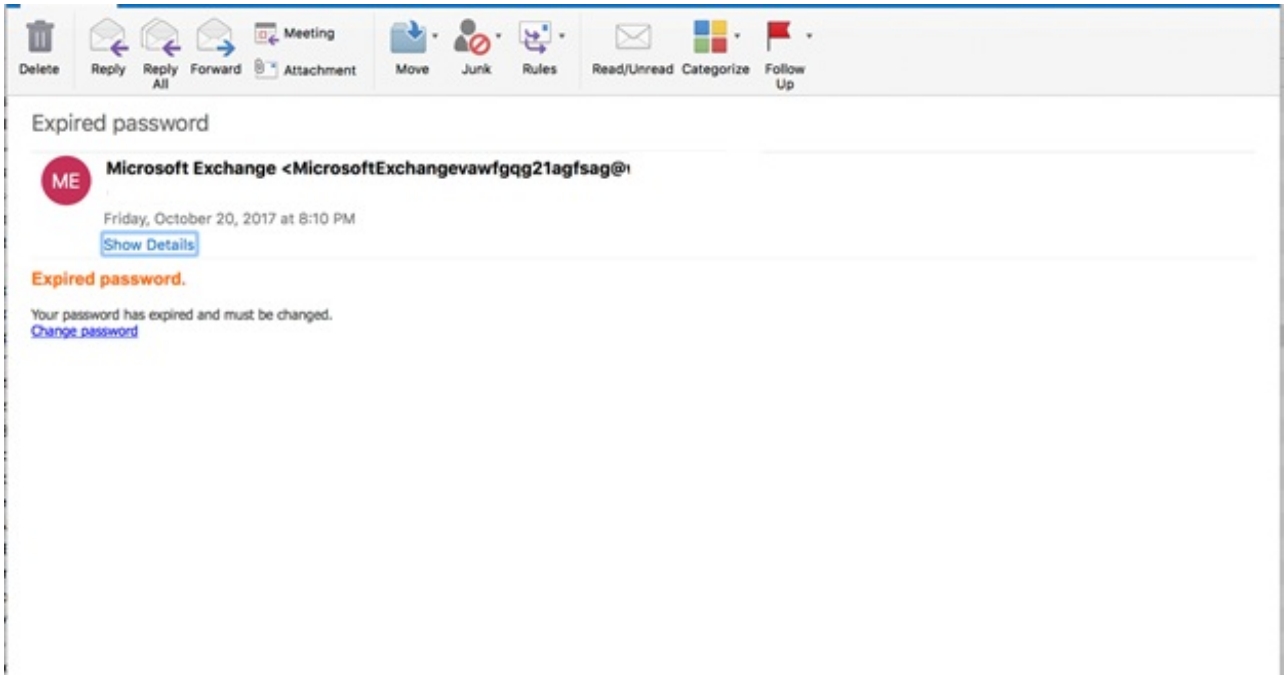

Figure 1. A sample of a credential phishing email Pawn Storm sent in October and November 2017

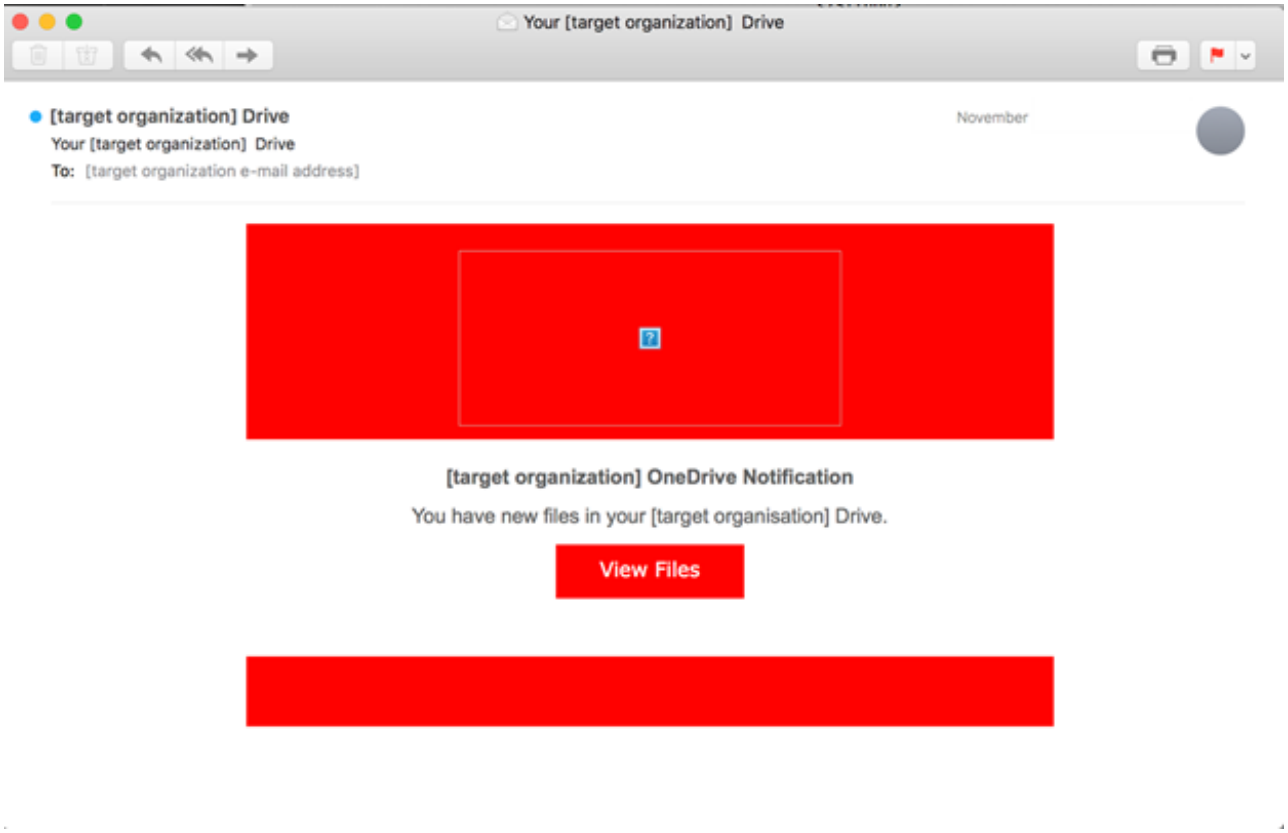

Figure 2. Second type of credential phishing email that was sent by Pawn Storm in November 2017. The logo of the target organization has been removed from the screenshot and the color was changed as not to reveal the source.

While these emails might not seem to be advanced in nature, we've seen that credential loss is often the starting point of further attacks that include stealing sensitive data from email inboxes. We have worked with one of the targets, an NGO in the Netherlands targeted twice, in late October and early November 2017. We successfully prevented both attacks from causing any harm. In one case we were able to warn the target within two hours after a dedicated credential phishing site was set up. In an earlier attack, we were able to warn the organization 24 hours before the actual phishing emails were sent.

Olympic Wintersports Federations

We have seen several International Olympic Wintersport Federations, such as the European Ice Hockey Federation, the International Ski Federation, the International Biathlon Union, the International Bobsleigh and Skeleton Federation and the International Luge Federation, among the group's targets in the second half of 2017. This is noteworthy due to the timing correlation between several Russian Olympic players being banned for life in fall, 2017. In 2016, Pawn Storm had some success in compromising WADA (the World Anti-Doping Agency) and TAS-CAS (the Court of Arbitration for Sport). At that time, Pawn Storm sought active contact with mainstream media either directly or via proxies and had influence on what some of them published.

Political targets

In the week of the 2017 presidential elections in Iran, Pawn Storm set up a phishing site targeting *chmail.ir* webmail users. We were able to collect evidence that credential phishing emails were sent to *chmail.ir* users on May 18, 2017, just one day before the presidential elections in Iran. We have previously reported similar targeted activity against political organizations in France, Germany, Montenegro, Turkey, Ukraine, and the United States.

Beginning in June 2017, phishing sites were set up mimicking the ADFS (Active Directory Federation Services) of the U.S. Senate. By looking at the digital fingerprints of these phishing sites and comparing them with a large data set that spans almost five years, we can uniquely relate them to a couple of Pawn Storm incidents in 2016 and 2017. The real ADFS server of the U.S. Senate is not reachable on the open internet, however phishing of users' credentials on an ADFS server that is behind a firewall still makes sense. In case an actor already has a foothold in an organization after compromising one user account, credential phishing could help him get closer to high profile users of interest.

The future of politically motivated campaigns

Rogue political influence campaigns are not likely to go away in the near future. Political organizations have to be able to communicate openly with their voters, the press and the general public. This makes them vulnerable to hacking and spear phishing. On top of that, it's also relatively easy to influence public opinion via social media. Social media platforms continue to form a substantial part of users' online experience, and they let advertisers reach consumers with their message.

This makes social media algorithms susceptible to abuse by various actors with bad intentions. Publishing stolen data together with spreading fake news and rumors on social media gives malicious actors powerful tools. While a successful influence campaign might seem relatively easy to do, it needs a lot of planning, persistence, and resources to be successful. Some of the basic tools and services, like ones used to spread fake news on social media, are already being offered as a service in the underground economy.

As we have mentioned in our overview paper on Pawn Storm, other actors may also start their own campaigns that aim to influence politics and issues of interest domestically and abroad. Actors from developing countries will learn and probably adapt similar methods quickly in the near future. In 2016, we published a report on C Major, an espionage group that primarily targets the Indian military. By digging deeper into C Major's activities, we found that this actor group not only attacks the Indian military, but also has dedicated botnets for compromised targets in Iranian universities, Afghanistan, and Pakistan. Recently, we have witnessed C Major also showing some interest in compromising military and diplomatic targets in the West. It is only a matter of time before actors like C Major begin attempting to influence public opinion in foreign countries, as well.

With the Olympics and several significant global elections taking place in 2018, we can be sure Pawn Storm's activities will continue. We at Trend Micro will keep monitoring their targeted activities, as well as activities of similar actors, as cyberpropaganda and digital extortion remain in use.

Indicators of Compromise (IoCs):

- adfs[.]senate[.]group
- adfs-senate[.]email
- adfs-senate[.]services
- adfs.senate[.]qov[.]info
- chmail.ir[.]udelivered[.]tk
- webmail-ibsf[.]org
- fil-luge[.]com
- biathlovvorld[.]com
- mail-ibu[.]eu
- fisski[.]ca
- iihf[.]eu