Operation Pawn Storm Ramps up its Activities; Targets NATO, White House | Trend Micro Security Intelligence Blog

blog.trendmicro.com

Operation Pawn Storm Ramps up its Activities; Targets NATO, White House

Long-running APT campaign Operation Pawn Storm has begun the year with a bang, introducing new infrastructure and zeroing in on targets including North Atlantic Treaty Organization (NATO) members and even the White House. This is according to the latest intelligence gleaned from Trend Micro's ongoing research into the attack group, and comes as a follow-up to our widely publicized October 2014 report.

Operation Pawn Storm: A Background

Operation Pawn Storm is an active economic and political cyber-espionage operation that targets a wide range of entities, like the military, governments, defense industries, and the media.

The group is composed of a determined group of threat actors active since at least 2007 with a very specific modus operandi. We so named it due to the attackers' use of multiple connected tools and tactics to hit a specific target – a strategy mirroring the chess move of the same name.

The group used three very distinct attack scenarios. One was to send spear-phishing emails with malicious Microsoft® Office documents containing the information-stealing SEDNIT/Sofacy malware. Another was to inject selective exploits into legitimate Polish government websites, leading to the same malware. A final strategy was to send out phishing emails redirecting users to fake Microsoft Outlook Web Access (OWA) login pages.

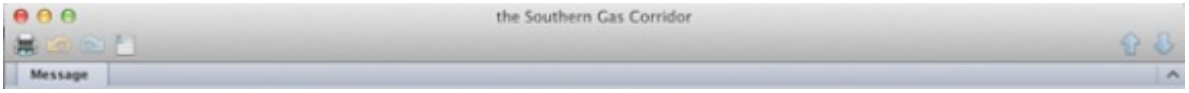
Pawn Storm targeted mainly military, government and media organizations in the United States and its allies. We determined that the group also aimed its attacks on Russian dissidents and those opposing the Kremlin, as well as Ukrainian activists and military, which has led some to speculate that there might be a connection with the Russian government.

We also observed another update to Pawn Storm's operations in February this year and found an iOS espionage app targeting Apple users.

What's New with Operation Pawn Storm?

The first quarter of 2015 has seen a great deal of activity from the group. Most notably this involved setting up dozens of exploit URLs and a dozen new command-and-control (C&C) servers targeting NATO members and governments in Europe, Asia and the Middle East.

In a slightly different modus operandi from the usual, we observed Pawn Storm attackers sending out specially-crafted emails designed to trick users into clicking on a malicious link.



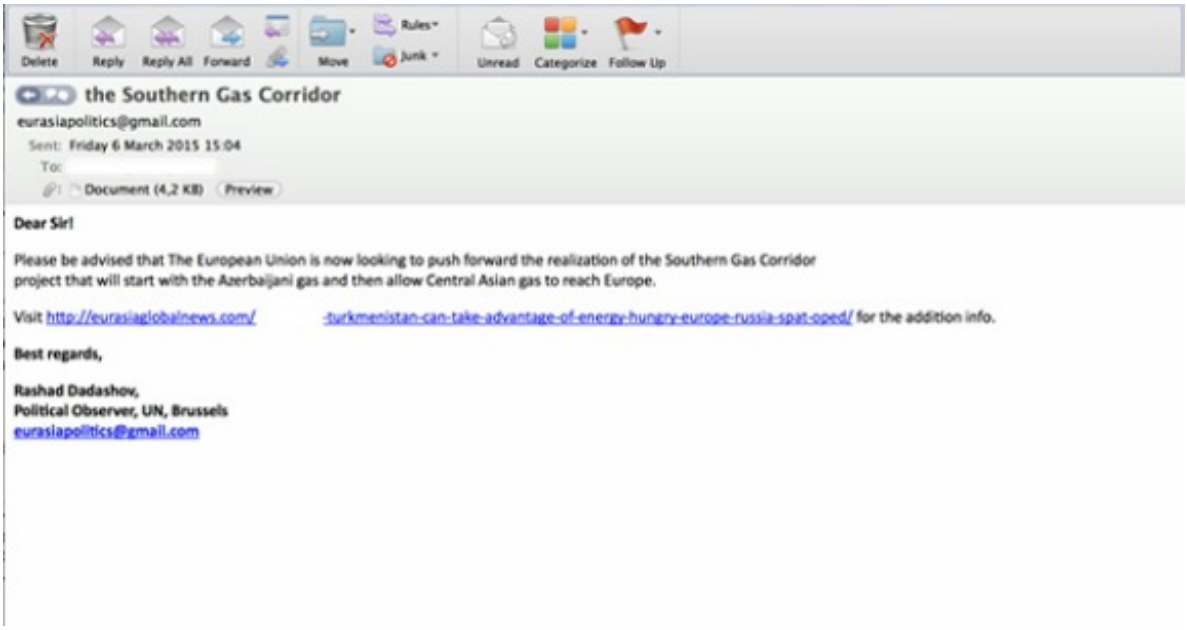


Figure 1. Sample spear-phishing email

In one case, the subject of the spam e-mail is the Southern Gas Corridor that the European Union initiated to become less dependent on Russian Gas. Other e-mails have similar geopolitical subjects, for example the Russian-Ukrainian conflict and the Open Skies Consultative Commission of the OSCE.

The emails usually have a link to what looks like a legitimate news site. When the target clicks on the link he will first load a fingerprinting script that feeds back details like OS, time zone, browser and installed plugins to the attackers. When certain criteria are met the fake news site may respond with a message that an HTML5 plugin has to be installed to view the contents of the site. The add-on in question turns out to be a version of X-Agent or Fysbis spyware if you're a Linux user, and Sednit if you're running Windows.

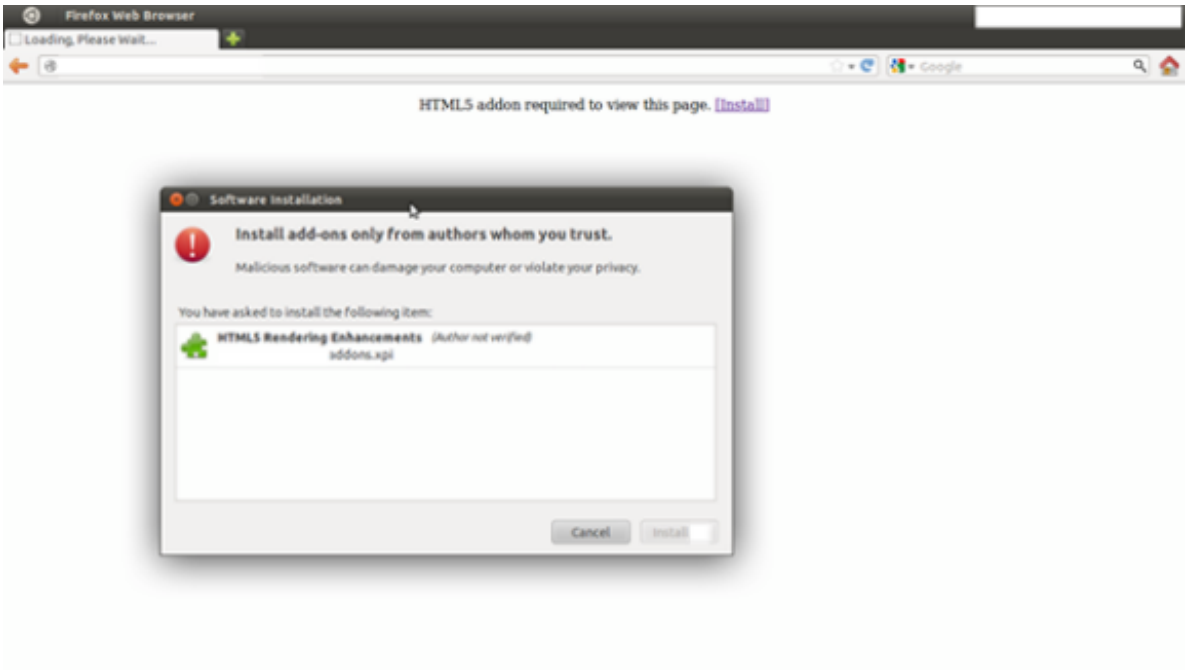


Figure 2. Screenshot of malicious HTML5 plugin

Same Old Tricks

Pawn Storm threat actors are also continuing with their phishing strategy. In fact, in autumn 2014 they set up a fake OWA webmail for a large US company which sells nuclear fuel to power stations.

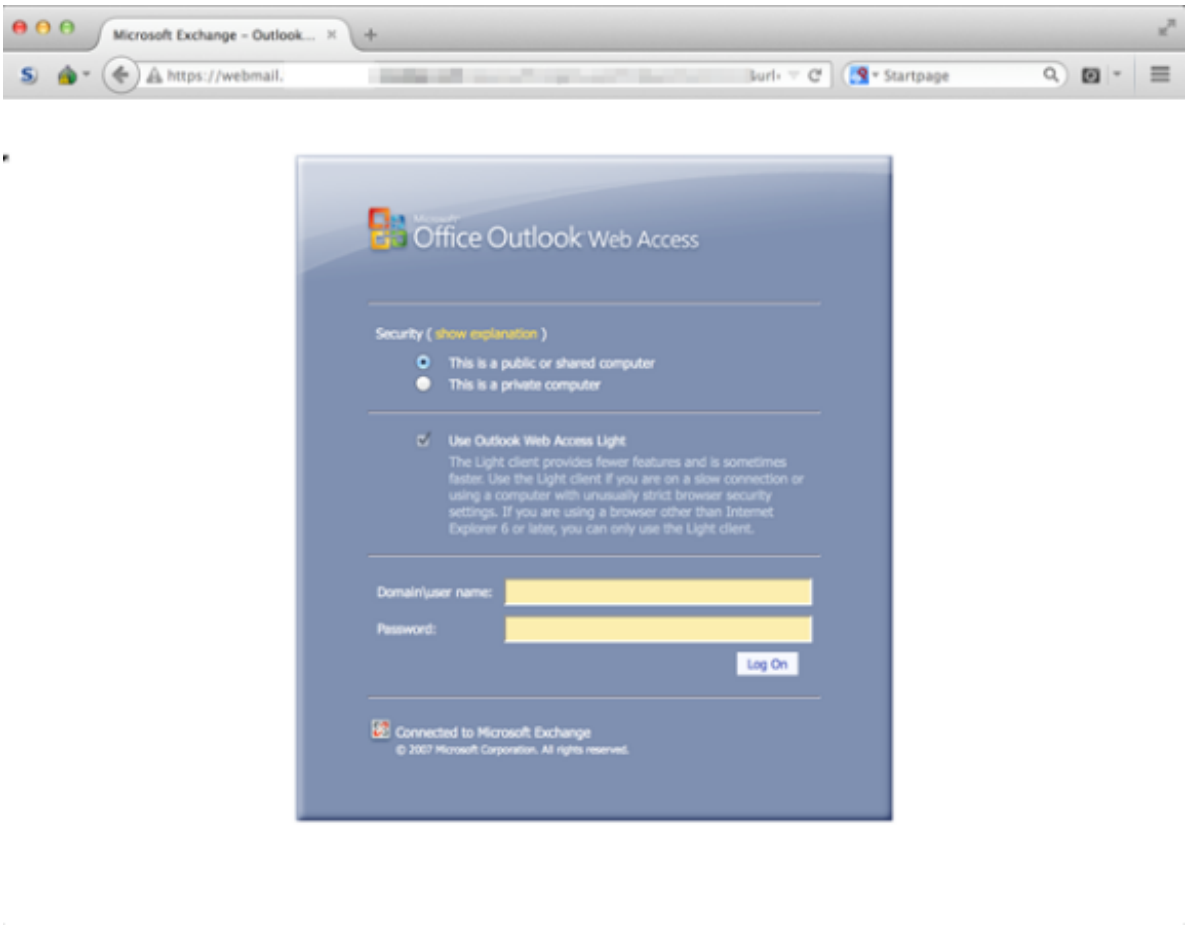


Figure 3. Fake webmail login page of US company selling nuclear fuel

It's not hard to see that a successful breach of this firm could lead to serious consequences. Other fake OWA servers include new ones targeting the armed forces of two European NATO members. A fake version of the webmail system of the NATO Liaison in the Ukraine was also put online in February this year.

White House Under Attack

Trend Micro has gathered evidence that the same group is eyeing the White House as a target. They targeted three popular YouTube bloggers with a Gmail phishing attack on January 26, 2015, four days after the bloggers had interviewed president Obama at the White House. This is a classic island hopping technique, in which attackers focus their efforts not on the actual target but on companies or people that might interact with that target, but which may have weaker security in place.

In a similar way, a well-known military correspondent for a large US newspaper was hit via his personal email address in December 2014, probably leaking his credentials. Later that month Operation Pawn Storm attacked around 55 employees of the same newspaper on their corporate accounts.

Organizations must remain on high alert for these kinds of attack, as Operation Pawn Storm hackers go to great lengths to make their emails appear legitimate. Military and government bodies in the US, Europe and Asia especially must invest in the right advanced cyber security tools to block phishing and malware downloads, and improve user training and education to mitigate the risk of attack.