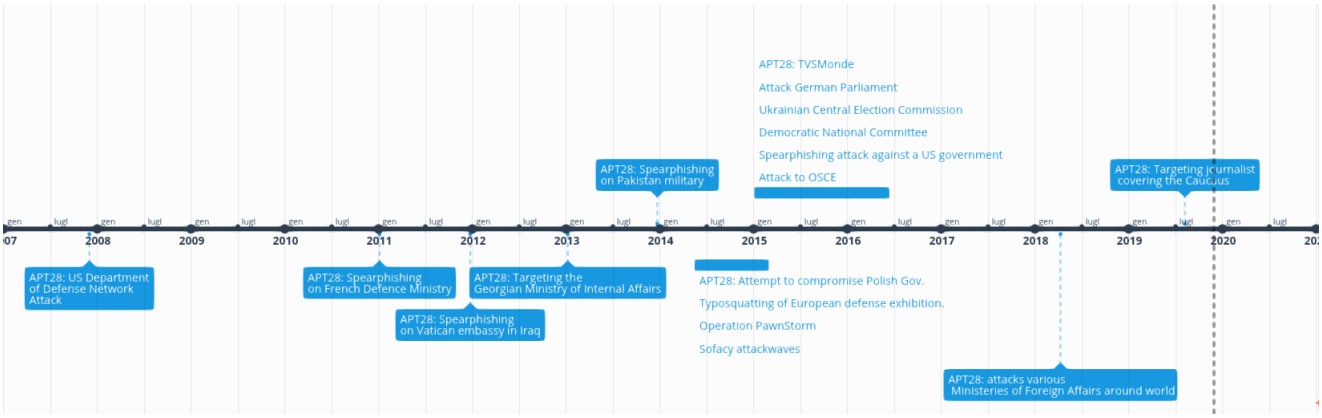
APT28 Attacks Evolution

marcoramilli.com/2019/12/05/apt28-attacks-evolution/

View all posts by marcoramilli December 5, 2019

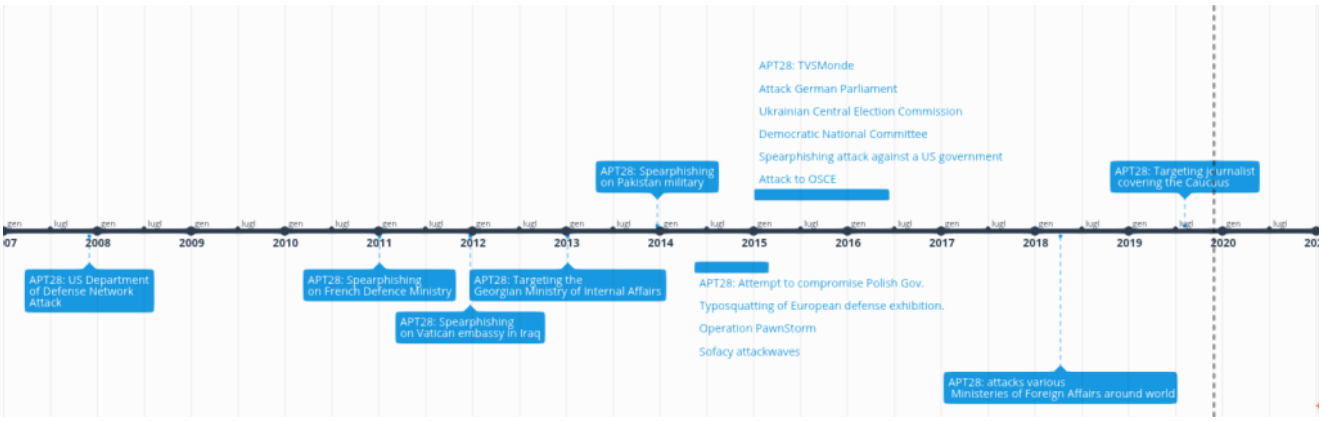


APT28 is a well known Russian cyber espionage group attributed, with a medium level of confidence, to Russian military intelligence agency **GRU** (by CrowdStrike). It is also known as **Sofacy Group** (by Kaspersky) or **STRONTIUM** (by Microsoft) and it's used to target Aereospace, Defence, Governmente Agencies, International Organizations and Media.

Today I'd like to share some personal notes after few years of collected evidences and readings on that topic.

Attack Timeline

The following timeline tracks APT28 back to 2008 and gives us a quick view on how big and organized is the threat group over the past decade.



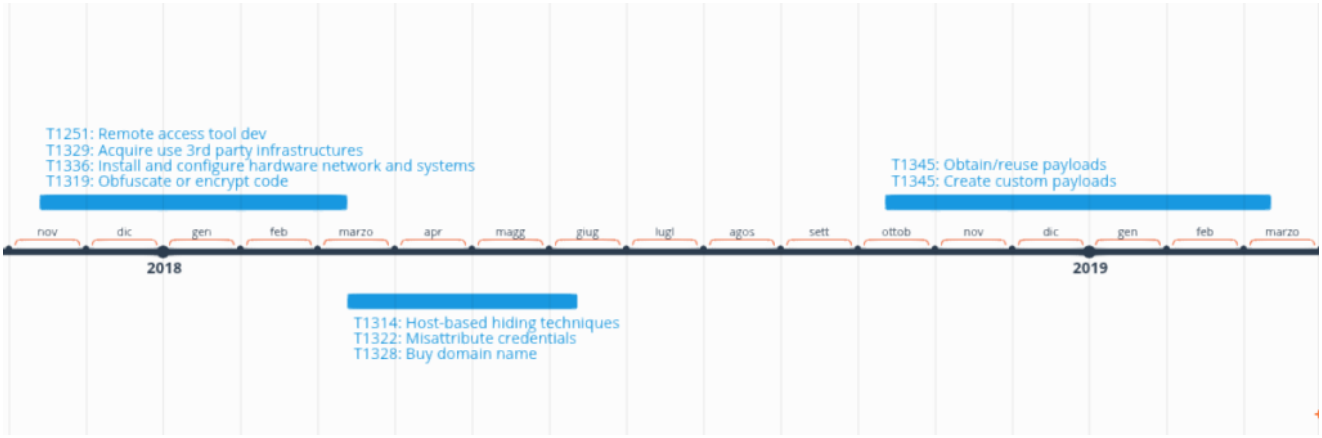
APT28 Timeline

According to the many analyses made by Unit42 (available **HERE**), FireEye (HERE, HERE) and TALOS (HERE, HERE) we might agree that APT28 has been very active (or at least very "spotted") during the time frame between 2012 to 2019. However most of the new attacks, qualitative speaking, happened during the time frame between 2018 to 2019. For

that reason it would be interesting to analyze how they've evolved over such a time frame in order to understand their change and their principal characteristics. From what I've tracked and from what I've read over the past few years it looks like APT28 changed in many areas, but today I'd like to focus mostly on the following three main areas: **Weaponization**, **Delivery**, **Installation**. Let's discuss one to one those areas.

Weaponization

Weaponization is a PRE-ATT&CK technique. It is classified as the operations needed to build and/or to prepare a complex attack. In other words all the infrastructures, the samples, the command and controls, the domains and IPs, the certificate, the libraries and, general speaking, all the operations that come before the attack phase in term of environments. Intelligence, humanInt, information gathering, informal test and so on, are not included in Weaponization since coming directly into the ATT&CK framework.



Weaponization Timeline

Observing the weaponization timeline it turns out there are three main blocks with few shared characteristics. For example from 2017 to early 2018 APT28 used specific techniques such as: T1251, T1329, T1336 and T1319. Those techniques are mainly focused on external – outsourcing (except for T1319) skills-set. Indeed acquiring 3rd parties infrastructures or Installing and configure hardware networks-systems and the usage of third party obfuscation libraries would definitely highlight a human resource depletion or the clear intent of false flag. On the other hand during early 2018 to mid-2018 the weaponization chain changed a lot moving to T1314, T1322 and to T1328. Those techniques enforced the idea the group moved from external professional resources and from hardware localized techniques to internal professional resources (indeed they started buy own domain for propagation and C2) . Finally from October 2018 to late march 2019 APT28 introduced a totally different weaponization technique: the T1345. It is not a direct consequence to the previous observed techniques, actually we might think they improved or forked an internal dev team. Those self-developing capabilities (implemented by T1345) were not observed during the past years and highlight a slightly significant change. We might think they enrolled a dedicated dev-team or they forked the actual one by running on two different paths.

Delivery

Delivery is the way attackers deploy the initial content to the victim. In other words how the adversary reach his victim by starting the infection chain. On one hand the delivery vector is often the only (or the first) artifact (such as: a Malware, a Link or exploit kit usage) that the cybersecurity analyst could observe. Unfortunately very often analysts don't have the possibility to track every single attack phase but they can just observe a small "portion" of it, and very often that "portion" is the "delivered artifact". Tracking the changes on Delivery would help cybersecurity analysts to build up the idea about threat actors by comparing likeness and differences in coding, styling and techniques. Indeed the delivery phase is a special key point to distinguish threat actors which usually tend to specialize their crafting capabilities over time rather than pivoting their capabilities on new delivery vectors. The following timeline shows how the delivery changed over the analyzed time frames.

Delivery Timeline

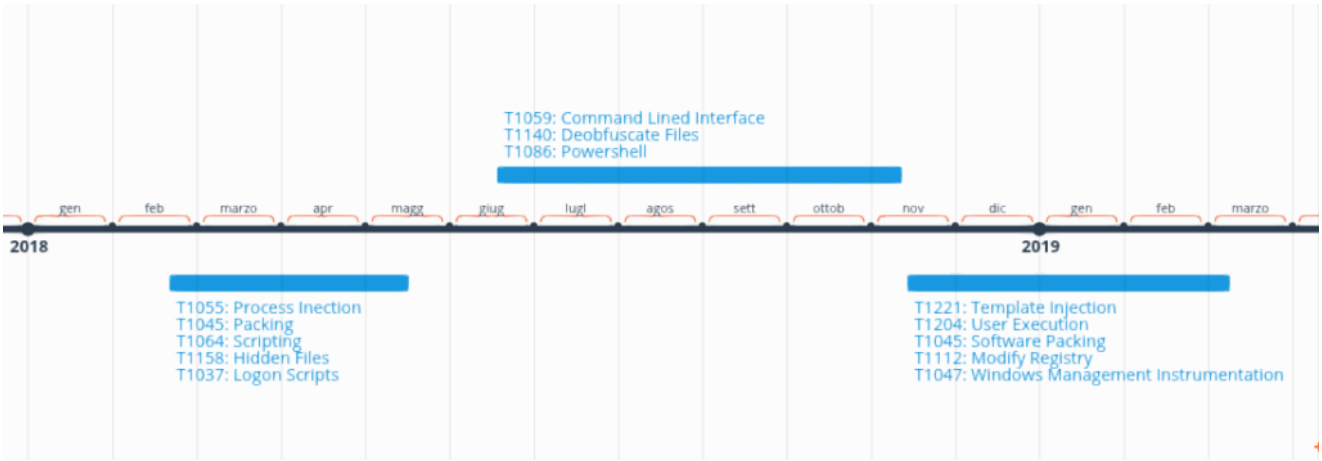
While in the previous section (weaponization section), three were the main macro blocks, in the delivery section everything looks like uniform and quite flat based on technique T1193: Spearphishing with a malicious attachment. But if we focus on the beginning of 2018 it looks like APT28 was using a more consolidated intelligence technique (T1376) by focusing on Human Intelligence in order to grab precious information used to deliver a well-crafted email campaign (government institutions related to foreign affairs). The delivery phase, at such time, was implementing a quite sophisticated dropper technology by exploiting vulnerabilities to "save and run" the payload in the desired place. The most exploited vulnerabilities by APT28 have been tracked as follows:

```
CVE-2017-0144 , CVE-2013-3897, CVE-2014-1776, CVE-2012-0158, CVE-2015-5119,
CVE-2013-3906, CVE-2015-7645, CVE-2015-2387, CVE-2010-3333, CVE-2015-1641,
CVE-2013-1347, CVE-2015-3043, CVE-2015-1642, CVE-2015-2590, CVE-2015-1701,
CVE-2015-4902, CVE-2017-0262, CVE-2017-0263
CVE-2014-4076, CVE-2014-0515
```

The most used tracked vulnerabilities are mainly focused on: "Windows", "Adobe Flash" and "Oracle" Technologies. During the past few months (almost one year from time writing) it was possible to observe a quick increment over Microsoft Office Vulnerabilities in order to drop second stages of payloads. This perfectly fits the new trend and the current infection chains.

Installation

While system persistence could be guaranteed in many different ways, for example by periodically exploiting a RCE vulnerability, persistence in case of Malware attacks is typically named: “Installation”. Since the main findings that I had analyzed for this post are Malware based, it makes sense to talk about Installation rather than talking about persistence. Moreover the installation procedure runs a key role into the infection chain. Observing the installation KPI would be meaningful to understand the developer team behind software, since developer teams do not like to change installation procedures over time because they used to focus on new features and/or to improve existing modules rather than change installation frameworks. The following timeline shows how Installation procedures changed over time on APT28 folks.



Installation Timeline

The observed time frame is focused on the past year since where the most interesting changes happened, at least in my personal opinion. Let’s start by observing that in early 2018 the most used techniques were: T1055, T1045, T1064, T1158 and T1037. Most of the used techniques belong to the “Scripting” world. In other words the most influential capabilities were based on Logon Scripts and JS/WB scripintg. From ~mid 2018 they group moves mostly on PowerShell scripting language (T1086 and T1140) widely used over the past two years (rif. HERE) ending up in early 2019 to advanced development techniques such as: T1221, T1204, T1045, T1047, T1112, which underline a quite interesting new develpment skillset.

Conclusions

As many groups are, APT28 is evolving over time. The group evolution is changing many TTPs (Tactics, Techniques and Procedures) but this time I decided to focus on: **Installation**, **Delivery** and **Weaponization**. Most of the tracked evolution indexes happened during the last one/two years showing a quick skill-sets enhancement on development, obfuscation and evasion techniques.