Telefónica

INSIDE ELECTIONS_

Threats to the German Electoral Process

21.09.2017

CYBER SECURED BY ElevenPaths

elevenpaths.com

Threats to the German Electoral Process

Analyst's View

In the last few months, different governmental agencies in Germany have been object of various cyber attacks perpetrated by groups such as APT28. In this regard, a spike of activity has been identified in the months of August and September of active sessions of malware associated with tools used by this group, and among those which were found, at least one had the specific target of Germany's governmental agencies. Given the nature of the evidence found, there is a real risk that the information potentially stolen from political actors in Germany can be used in the context of the upcoming elections. On the other hand, other generic samples detected have been found to have capabilities for information theft, the control of infected systems and different implementations to attack Windows, Mac and Android platforms. According to the work group developed by the European Union's East StratCom, disinformation campaigns allegedly linked to Russian government involvement in cyberspace have also been reported related to the management of the refugee crisis and against German soldiers part of a NATO contingent stationed in Lithuania.

Principal Country Keys

Official name	Federal Republic of Germany
Capital	Berlin
Official language	German
Religion	No official religion
Form of Government	**Federal, Constitutional and Democratic Welfare State.** The head of state is the Federal President, elected every 5 years. The **Bundestag** (lower house) represents the German people. The **Bundesrat** (Federal Council) is the house of representation of the Federated States.
Main issues at present	Negotiations on the programme "Designing the Future of Germany". Energy issues. Construction of the European Union, in which Germany is one of the key players. Refugee crisis.

Germany's regional references focus on:

Its ties with the **United States**, one of the pillars of its foreign policy, especially with regard to security and defence.

Germany is considered to be a valid interlocutor in relations with Russia. Despite this, it has come under criticism from Moscow as a result of the Ukraine crisis.

It has intensified its investments in **Brazil** and **Mexico**, as well as **China**.

Germany is taking on an increasingly relevant role on the African continent. It has a growing influence in both the **Mashriq** and **Maghreb** regions.

Types of Threats Identified

Threats Attributed to External Agents

Germany has previously endured attacks on different political agencies, mainly attributed to the APT28 Group (also known as Pawn Storm, Fancy Bear, Sofacy Group and Strontium). In June 2015, the Federal Office of Germany for Security in Information Technologies (BSI, in its German initials) accordingly confirmed that various political parties had been object of phishing attacks. In the same month, the head of the domestic intelligence agency similarly attributed the compromising of the networks of the Bundestag to this group [1].

Meanwhile, in April and May of 2016, investigators from TrendMicro identified that this same month had created false mail servers in order to launch phishing attacks against members of the Christian Democratic Union (CDU) political party, and thus obtain credentials and access to their accounts [2]. Although the German authorities confirmed that the attack was indeed perpetrated by Pawn Storm, it is unknown whether they were successful in their endeavour, as the emails have not been leaked to date. Some experts have raised the possibility that the potentially stolen information could have a specific purpose, such as to sway the German elections held on 24 September, similar to attempts made during the American elections.

On the other hand, the cybersecurity firm Fireeye has already issued a report earlier this year which pinpointed the malware "suite" used by this group, which includes the following tools: Chopstick, Eviltoss, Gamefish, Sourface, Oldbait and Coreshell. According to the threat database compiled by ElevenPaths, a spike in the number of active sessions linked to these threats have been identified in August and September (1,476 and 7,825 sessions, respectively) as shown in Figure 1.

Among all of these malware samples, one of them would have been using Coreshell and have affected governmental organisations in Germany.

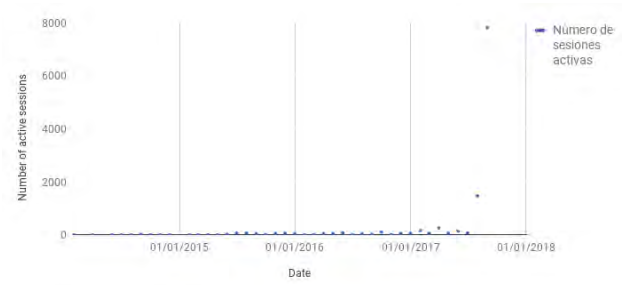

Figure 1. Number of active sessions in the malware parts linked to a suite of tools used by APT28.

Coreshell is a downloader which downloads in a second backdoor phase from a C2. Over time this downloader has evolved from Sourface to most recent Coreshell versions, normally compiled in a DLL (coreshell.dll).

It uses two sub-processes to communicate with its C2. The first sends beacons contained in the list of processes of the compromised host, while the second is responsible for downloading and executing two payloads. The messages are sent using HTTP POST requests, whose information is code in Base64 and also encrypted. As for the method itself, a personalised flow algorithm is used, which has a six-byte keyword. The commands from the C2 to the Coreshell implants utilise another type of flow encryption, this time using an eight-byte keyword.

Coreshell has used the same user-agent string ("MSIE 8.0) previously used by Sourface, but in most recent samples Coreshell was found to use the Internet Explorer user-agent string.

From another viewpoint, other more generic malware families not associated with known groups have been identified, or at least ones not attributed to these as part of their current tool arsenal. Among these, different types of malware have been found to have capabilities for information theft, the control of infected systems and different implementations to attack Windows, Mac and Android platforms.

Executable files, text documents and .pdf files with embedded exploits, Flash and applications developed in Java have also been identified. Below is a list of some samples which would be affecting German government offices:

- NetWireRAT. Remote administration tool (RAT) commonly used by various types of attackers to take remote control of a system.
- DarkComet. RAT used by various types of attackers to provide them with complete control over an infected system.
- Adwind. RAT in Java which has been distributed as a service.
- GearInformer. This is an updated and renamed version of the keylogger iSpy.
- H1N1. Downloader that affects Windows. This malware sends system information and accepts commands from a control server. Compatible commands permit the download and execution of files in the infected system. The malware injects its payloads in legitimate processes to hide its activities.
- KeyBase. A keylogger that also comes equipped with the theft of credentials and visualisation functionality of websites.
- MagnitudeEKFlashContainer. Sample supplied by the Magnitude exploit kit that exploits Adobe Flash Player versions.
- Matsnu. An x86 infector that acts as a back door once it gains access to the system, having the capacity to load and execute any code in the system, encrypt files and steal confidential data.
- NanoCoreRAT. Trojan that opens a back door and steals information from the compromised equipment. It also permits an attacker to execute various commands in the infected system.
- NeutrinoEKExploitsFlashContainer. Flash file used as part of the Neutrino exploit kit.
- PredatorPain. Trojan that aims to steal information, able to capture passwords, keystrokes, screen shots and other sensitive information.
- Recslurp. Trojan with capacity to extract FTP credentials and leak them to a remote server.
- SundownEKFlashContainer. Flash files that download malware in the victim's equipment as part of a Sundown exploit kit.
- Ursnif. Stealer and downloader with capacity to steal information from browsers and other application such as Microsoft Outlook. It also is capable of downloading additional malicious component from C2 servers from the attacker and dynamically load them into the memory.
- Zincite. Back door commonly installed by the Mydoom worm.
- RTF-OLE-Exploit. Multi-exploitation technique that tends to be found in HTML or JavaScript exploits, but rarely in RTF or Office exploits. The following vulnerabilities are exploited: CVE-2012-0158, CVE-2012-2539, CVE-2014-1761 and CVE-2015-1641.

The time frame in which these threats are situated runs from January 2015 to the most recent detections made whilst performing this investigation, September 2017. As for the infection vectors, these are email, web browsing, Flash, FTP, Owncloud and Mediafire.

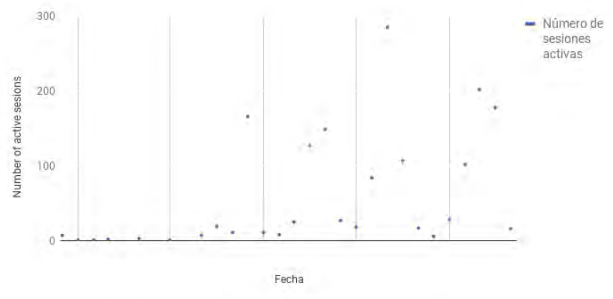

Figure 2. Number of active sessions of generic *malware* parts with an impact on German government agencies.

On the other hand, according to the German government, propaganda and disinformation campaigns from the Russian media have also been detected, similar to those identified in the American and French elections. In this sense, the European Union's East StratCom work group, created in 2015 to combat the disinformation campaigns of the Russian government, discovered that Chancellor Angela Merkel was a constant target of such attacks as a result of her refugee policy [3]. Another related case would be certain emails that were sent to the media regarding the "Lisa Case", in which German soldiers were accused of rape during their stationing in Lithuania as part of NATO military forces.[4]

Threats Attributed to Internal Agents

At the end of 2011, at the Chaos Computer Club [5], one of the most internationally important conferences on security, it was published that the trojan R2D2 (also known as Ozapftis or Bundestrojaner) was being used by German security corps and forces to intercept

communications. The capabilities of this tool include the intercepting of communications in Skype, MSN Messenger and Yahoo Messenger, the registering of key strokes in Firefox, Opera, Internet Explorer and SeaMonkey, the taking of screenshots of user screens and the remote communication with websites [6]. More recent appearances of similar threats have not been identified.

Bibliography

[1] «APT28: At the Center of the Storm « Threat Research Blog», *FireEye*, 11-ene-2017. [En línea]. Disponible en: https://www.fireeye.com/blog/threat-research/2017/01/apt28_at_the_center.html. [Accedido: 18-sep-2017].

[2] Trend Micro, «Two Years of Pawn Storm. Examining an Increasingly Relevant Threat», Research Paper, 2017.

[3] AFP, «Merkel faces more Russian disinformation ahead of poll: source», *Yahoo News*, 23-ene-2017. [En línea]. Disponible en: https://www.yahoo.com/news/merkel-faces-more-russian-disinformation-ahead-poll-source-201147963.html. [Accedido: 18-sep-2017].

[4] D. Welle (www.dw.com), «Why the "fake rape" story against German NATO forces fell flat in Lithuania | Europe | DW | 23.02.2017», *DW.COM*, 23-feb-2017. [En línea]. Disponible en: http://www.dw.com/en/why-the-fake-rape-story-against-german-nato-forces-fell-flat-in-lithuania/a-37694870. [Accedido: 18-sep-2017].

[5] «CCC | Chaos Computer Club analyzes government malware». [En línea]. Disponible en: https://ccc.de/en/updates/2011/staatstrojaner. [Accedido: 18-sep-2017].

[6] «'Government' backdoor R2D2 Trojan discovered by Chaos Computer Club», *Naked Security*, 09-oct-2011. .

About ElevenPaths

At ElevenPaths we believe in the idea of challenging the current state of security, a characteristic which should always be present in technology. We are continually rethinking the relationship between security and people, with the aim of creating innovative products capable of transforming the concept of security and thereby keeping one step ahead of our attackers, who are increasingly present in our digital lives.

Further Information

www.elevenpaths.com

@ElevenPaths

blog.elevenpaths.com