EvilGrab Malware Family Used In Targeted Attacks

By Trend Micro (words)

Published: 2013-09-19 · Archived: 2026-04-05 23:13:14 UTC

Recently, we spotted a new malware family that was being used in targeted attacks - the *EvilGrab* malware family. It is called *EvilGrab* due to its behavior of grabbing audio, video, and screenshots from affected machines. We detect *EvilGrab* under the following malware families:

- BKDR_HGDER
- BKDR_EVILOGE
- BKDR_NVICM

Looking into the feedback provided by the Smart Protection Network, *EvilGrab* is most prevalent in the Asia-Pacific region, with governments being the dominant sector targeted. These are consistent with known trends in targeted attacks. The full report on *EvilGrab* may be found at the **Threat Intelligence Resource on Targeted Attacks** together with other resources discussing targeted attacks.

Attack Vectors

The most common arrival vector for *EvilGrab* malware is spear-phishing messages with malicious Microsoft Office attachments. In particular, malicious Word files and Excel spreadsheets that contain code that targets CVE-2012-0158 are a favored way to spread this new threat.

Information Theft

EvilGrab has three primary components: one .EXE file and two .DLL files. The .EXE file acts as the installer for all of the *EvilGrab* components. One of the .DLL files serves as a loader for the other .DLL file, which is the main backdoor component. Some variants of *EvilGrab* delete the .EXE file after installation to cover its tracks more effectively.

EvilGrab attempts to steal saved login credentials from both Internet Explorer and Outlook. The credentials of both websites and email accounts are targeted for theft by attackers. In addition to this, it can also "grab" any played audio and/or video on the system using standard Windows APIs. As part of its backdoor functionality, it can also take screenshots and log keystrokes. All of these are uploaded to a remote server to be accessed by the attacker.

Targeted Applications

EvilGrab has some unique behaviors if it detects certain installed applications. First of all, it is explicitly designed to steal information from *Tencent QQ*, a Chinese instant messaging application. It steals and uploads all the memory used by QQ. This may be able to reveal the contents of conversations or the members of the user's contacts list. EvilGrab will attempt to inject itself into the processes of certain security products. In the absence of

these security products, it will choose to inject itself into standard Windows system processes. ESET, Kaspersky, and McAfee have all been specifically targeted by EvilGrab for process injection.

Backdoor Activities

EvilGrab possesses backdoor capabilities that allows an attacker to carry out a wide variety of commands on the affected system. This grants them complete control over a system affected by *EvilGrab*. As part of its command-and-control traffic, *EvilGrab* contains two separate identifiers, which may serve as campaign codes and/or trackers. One of the identifiers has been seen with the following values:

- 006
- 007
- 0401
- 072002
- 3k-Ja-0606
- 3k-jp01
- 4k-lyt25
- 88j
- e-0924
- LJ0626
- RB0318

The other field has been seen with two values:

- V2010-v16
- V2010-v24

We have observed that the main backdoor component of those variants having the V2010-v24 identifier have a proper MZ/PE header. While most of those variants having the V2010-v16 identifier have some parts of their MZ/PE header overwritten with “JPEG” strings.

Update as of September 26, 2013

The MD5 hashes of the files involved in this attack are:

- 2E991260E42266DB9BCCFA40DC90AE16
- 7ED71CF0B98E60CC5D4296220F47C5A2
