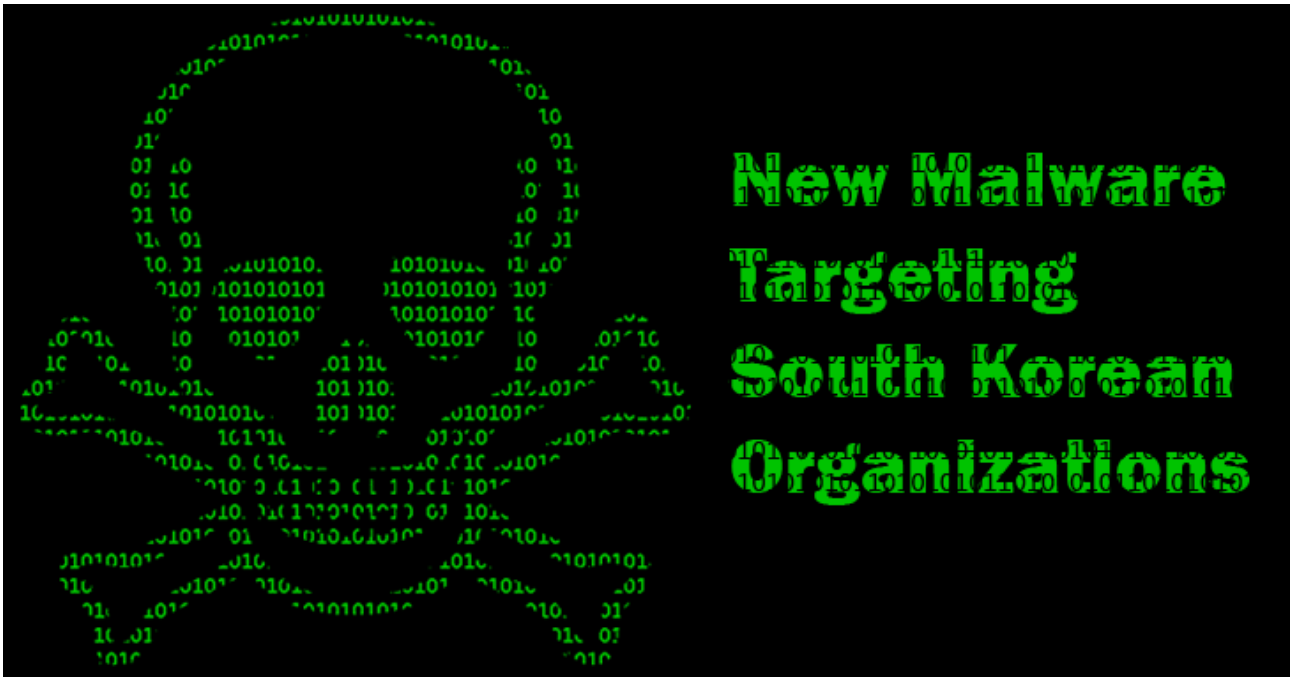
Duuzer Trojan: A New Backdoor Targeting South Korean Organizations

By The Hacker News

Published: 2015-10-27 · Archived: 2026-04-05 19:47:06 UTC



Security researchers at Symantec have uncovered a new Backdoor Trojan that grants hackers remote access and some control over infected machines.

"**Duuzer**," as dubbed by the researchers, has been targeting organizations in South Korea and elsewhere in an attempt to steal valuable information.

The Trojan is designed to infect both 32-bit and 64-bit computers running Windows 7, Windows Vista, and Windows XP.

Duuzer gives attackers remote access to the compromised computer, allowing them to:

- Collect system and drive information
- Create, enumerate, and end processes

- Access, modify and delete files
- Upload and Download additional files
- Change the time attributes of files
- Execute malicious commands
- Steal data from infected system
- Know about victim's Operating System

Duuzer Infects via Spear Phishing or Watering Hole Attacks

It is currently unclear how the malware is being distributed, but according to Symantec Researchers, the most obvious routes are **Spear Phishing** campaigns and **Watering Hole** attacks.

Once infected, Duuzer checks if the system is running on a virtual machine like **VMWare** or **Virtual Box** to ensure that security researchers are not analyzing the malware before performing its malicious routines.

Moreover, the Trojan identifies the existing software configured to run on startup and takes the name of that legitimate software on an infected computer and spread across the system.

Duuzer's first sets up a backdoor on the machine, allowing attackers physical access to the system.

The attackers then manually run commands through the backdoor on affected computers. They can perform a variety of operations mentioned above.

> *"Based on our analysis of Duuzer, the attackers behind the threat appear to be experienced and have knowledge about security researchers' analysis techniques,"* researchers said. *"Their motivation seems to be obtaining valuable information from their targets' computers."*

'Brambul' Worm and 'Joanap' Trojan also Detected

Research also discovered a dropper that infects computers with a worm known as **Brambul** and a Backdoor Trojan called **Joanap**. Both of them mostly work together and typically used to log and monitor infected systems remotely.

It is still unclear how the dropper is being distributed; however, it is believed that it comes from malicious emails.

The worm detected as **W32.Brambul** uses brute-force attacks via the **Server Message Block** (SMB) protocol to spread from one computer to another.

Once infected, the Brambul worm connects to random IP addresses on the local network and authenticates itself through SMB using common passwords, like 'password,' 'login,' '123123,' 'abc123' and 'iloveyou.'

Besides attacking other computers via SMB, Brambul creates a network share on compromised computers, usually the system drive, and then sends the computer's details and login credentials to a predefined email address.

Connection between Duuzer, Brambul and Joanap

According to Symantec, Duuzer has a connection with both Joanap and Brambul...But how?

Once infected, Brambul drops other pieces of malware on infected machines, either Duuzer or Joanap.

Systems infected with Brambul have been used as command-and-control (CnC) servers for Duuzer and have also been compromised with Duuzer.

If Joanap is dropped, the Trojan will register itself as a local OS service, named "SmartCard Protector." The Trojan opens a backdoor on the compromised machine and starts:

- Sending specific files to the attackers
- Saving or deleting files
- Downloading and executing files
- Executing or terminating processes
- Propagating instructions it receives from the C&C server

How to get rid of this ARMY?

Though Duuzer, Brambul, and Joanap are just a small selection of many threats affecting South Korean organizations with a very low-risk level.

But still, it is recommended for the users and businesses to keep themselves safe and protected by following these steps and prevent their systems from being compromised with this malware:

1. Use a firewall to block all incoming connections from the Internet to services that shouldn't be publicly available.
2. You should, by default, deny all incoming connections and only allow services you explicitly want to offer to the outside world.
3. Use Complex Passwords as it makes it difficult to crack.
4. Turned OFF Bluetooth if it is not required for mobile devices. Also, turn off other services not required at present.
5. Train your employees not to open email or messages attachments unless they are expecting them.

For more details, head on the Symantec's official blog.

Found this article interesting? Follow us on Google News, Twitter and LinkedIn to read more exclusive content we post.

Source: https://thehackernews.com/2015/10/computer-malware-attack.html