New Backdoor Targeting Taiwan Employs Stealthy Communications

symantec-enterprise-blogs.security.com/threat-intelligence/taiwan-malware-dns

Threat Hunter TeamSymantec

A previously unseen backdoor (Backdoor.Msupedge) utilizing an infrequently seen technique was deployed in an attack against a university in Taiwan.

The most notable feature of this backdoor is that it communicates with a command-and-control (C&C) server via DNS traffic. While the technique is known and has been used by multiple threat actors, it is nevertheless something that is not often seen.

Msupedge analysis

Msupedge is a backdoor in the form of a dynamic link library (DLL). It has been found installed in the following file paths:

- csidl_drive_fixed\xampp\wuplog.dll
- csidl_system\wbem\wmiclnt.dll

While wuplog.dll is loaded by Apache (httpd.exe), the parent process for wmiclnt.dll is unknown.

Msupedge uses DNS tunneling for communication with the C&C server. The code for the DNS tunneling tool is based on the publicly available dnscat2 tool. It receives commands by performing name resolution. The host names that are resolved are structured as follows:

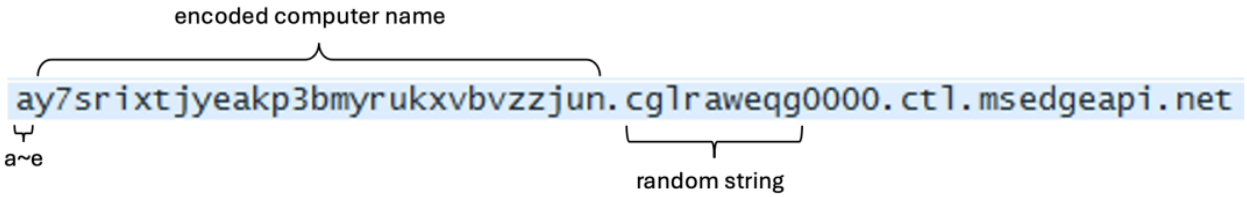

Figure 1. Host name for initial name resolution.

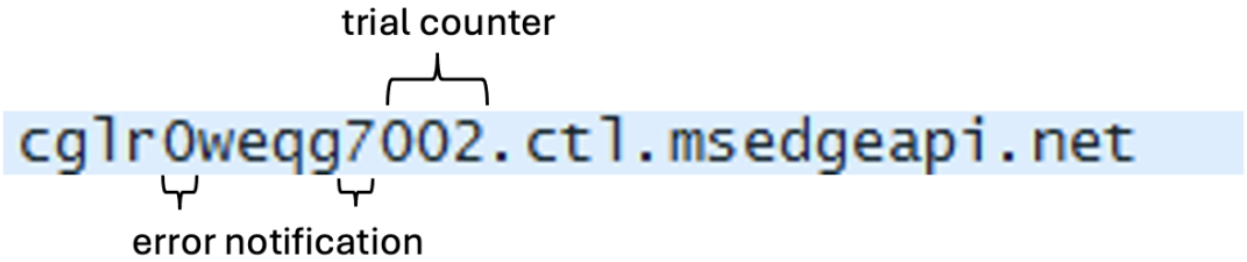

Figure 2. Host name used once computer name is sent.

Error notifications include the success or failure of the following:

- Memory allocation
- Decompression of received commands
- Execution of received commands

The backdoor also appears to encode the result of the command execution as a fifth-level domain and send it.

Msupedge not only receives commands via DNS traffic but also uses the resolved IP address of the C&C server (ctl.msedeapi[.]net) as a command. The third octet of the resolved IP address is a switch case. The behavior of the backdoor will change based on the value of the third octet of the resolved IP address minus seven. For example, if the third octet is 145, this translates to 138 (expressed in hexadecimal as 0x8a)

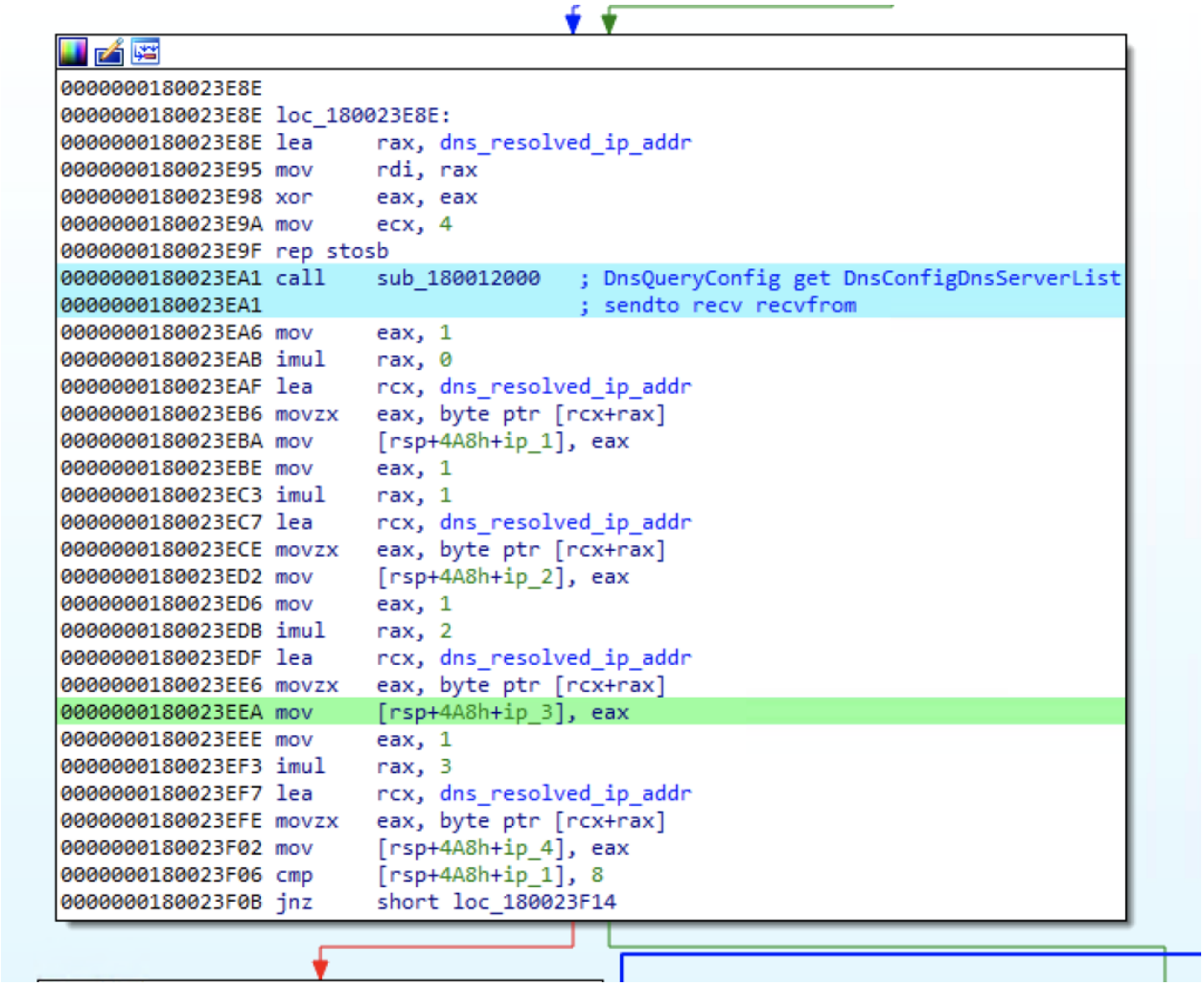

Figure 3. Retrieving the resolved IP address.

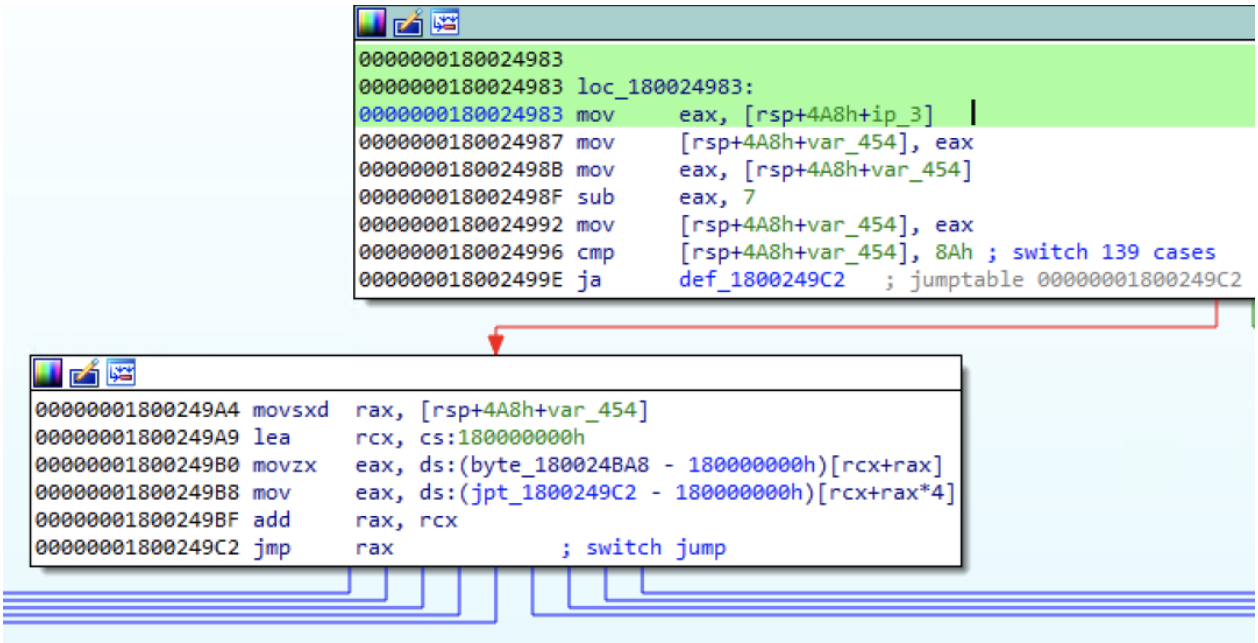

Figure 4. The behavior of the backdoor changes based on the values of the third octet of the resolved IP address minus seven.

Msupedge supports the following commands:

- Case 0x8a : Create process. The command is receive via DNS TXT record.
- Case 0x75 : Download file. The download URL is received via DNS TXT record.
- Case 0x24 : Sleep (ip_4 * 86400 * 1000 ms).
- Case 0x66 : Sleep (ip_4 * 3600 * 1000 ms).
- Case 0x38 : Create %temp%\1e5bf625-1678-zzcv-90b1-199aa47c345.tmp. The purpose of this file is unknown.
- Case 0x3c: Remove %temp%\1e5bf625-1678-zzcv-90b1-199aa47c345.tmp.

Infection vector

The initial intrusion was likely through the exploit of a recently patched PHP vulnerability (CVE-2024-4577). The vulnerability is a CGI argument injection flaw affecting all versions of PHP installed on the Windows operating system. Successful exploitation of the vulnerability can lead to remote code execution.

Symantec has seen multiple threat actors scanning for vulnerable systems in recent weeks. To date, we have found no evidence allowing us to attribute this threat and the motive behind the attack remains unknown.

Protection/Mitigation

For the latest protection updates, please visit the Symantec Protection Bulletin.

Indicators of Compromise

If an IOC is malicious and the file is available to us, Symantec Endpoint products will detect and block that file.

e08dc1c3987d17451a3e86c04ed322a9424582e2f2cb6352c892b7e0645eda43 – Backdoor.Msupedge

f5937d38353ed431dc8a5eb32c119ab575114a10c24567f0c864cb2ef47f9f36 – Backdoor.Msupedge

a89ebe7d1af3513d146a831b6fa4a465c8edeafea5d7980eb5448a94a4e34480 – Web shell

About the Author

Threat Hunter Team

Symantec

The Threat Hunter Team is a group of security experts within Symantec whose mission is to investigate targeted attacks, drive enhanced protection in Symantec products, and offer analysis that helps customers respond to attacks.

Want to comment on this post?