The Siesta Campaign: A New Cybercrime Operation Awakens

In the past few weeks, we have received several reports of targeted attacks that exploited various application vulnerabilities to infiltrate various organizations. Similar to the Safe Campaign, the campaigns we noted went seemingly unnoticed and under the radar. The attackers orchestrating the campaign we call the Siesta Campaign used multicomponent malware to target certain institutions that fall under the following industries:

- Consumer goods and services
- Energy
- Finance
- Healthcare
- Media and telecommunications
- Public administration
- Security and defense
- Transport and traffic

Threat actors don't always rely on complex attack vectors to infiltrate an organization's network. Attackers can also make use of basic social engineering techniques for their victims to take the bait, such as in our case study below.

The Siesta Campaign: A Case Study

We are currently investigating an incident that involved attackers sending out spear-phishing emails addressed to executives of an undisclosed company. These emails were sent from spoofed email addresses of personnel within the organization. Instead of using attachments and document exploits, this specific campaign served their malware through a legitimate-looking file download link.

To lure the target into downloading the file, the attacker serves the archive under a URL path named after the target organization's name as cited below:

> *http://{malicious domain}/{organization name}/{legitimate archive name}.zip*

This archive contains an executable (TROJ_SLOTH) disguised as a PDF document. When executed, it drops and opens a valid PDF file, which was most probably taken from the target organization's website. Along with this valid PDF file, another malicious component is also dropped and executed in the background.

This backdoor component is named *google{BLOCKED}.exe*. (Due to the ongoing investigation, we are

unfortunately unable to share hashes and filenames at this time.) This backdoor connects to *http://www.micro{BLOCKED}. com/index.html*, which are its command-and-control (C&C) servers. Trend Micro identifies these samples as BKDR_SLOTH.B.

At this point, the malware begins waiting for additional commands from the attacker. The encrypted commands that are accepted are:

- Sleep:
  - Commands the backdoor to sleep for specified number of minutes
  - We have received a sleep command of "sleep:120" during our analysis which means that the malware will wait for 2hrs before establishing a connection again to the C&C server
- Download: <download_url>
  - Commands the backdoor to download and execute a file (most probably another Win32 executable) from a specified URL

The C&C servers used in this campaign are found to be newly registered and also short-lived, making it difficult for us to track the malware's behavior.

Based on our research, we found 2 variants of the malware used in this campaign. Although not exactly alike, the behaviors are nearly identical.

One of the similar samples is a file named *Questionaire Concerning the Spread of Superbugs February 2014.exe* (SHA1: 014542eafb792b98196954373b3fd13e60cb94fe). This sample drops the file *UIODsevr.exe*, its backdoor component which behaves similarly as BKDR_SLOTH.B with the addition of communicating to its C&C at *skys{BLOCKED}com*. These samples are identified by Trend Micro as BKDR_SLOTH.A.

Both variants excessively use *Sleep* calls, which renders the malware dormant for varying periods of time, hence the campaign name "*Siesta"* (which means to take a short nap in Spanish). Commands are being served through HTML pages using different keywords as listed below:

> ***Variant 1***
> *prefix: ">SC<"*
>
> ***Variant 2***
> *prefix: "longDesc="*
> *suffix: ".txt"*

Listed below are the backdoor commands we were able to see from our analysis:

Variant 1

"run1" – open a remote shell

"run2" – pipe shell commands from URL1

"run3" – pipe shell commands from URL2

"http" – pipe shell commands from C2

"x_" – sleep for specified number of minutes

Variant 2

"sleep:" – sleep for specified number of minutes

"download:" – download and execute another executable from C2

Attribution

Attribution of campaigns and attack methods can often be difficult. We were able to identify this new campaign through inspecting hashes, C&Cs, registrants, commands, and additional information.

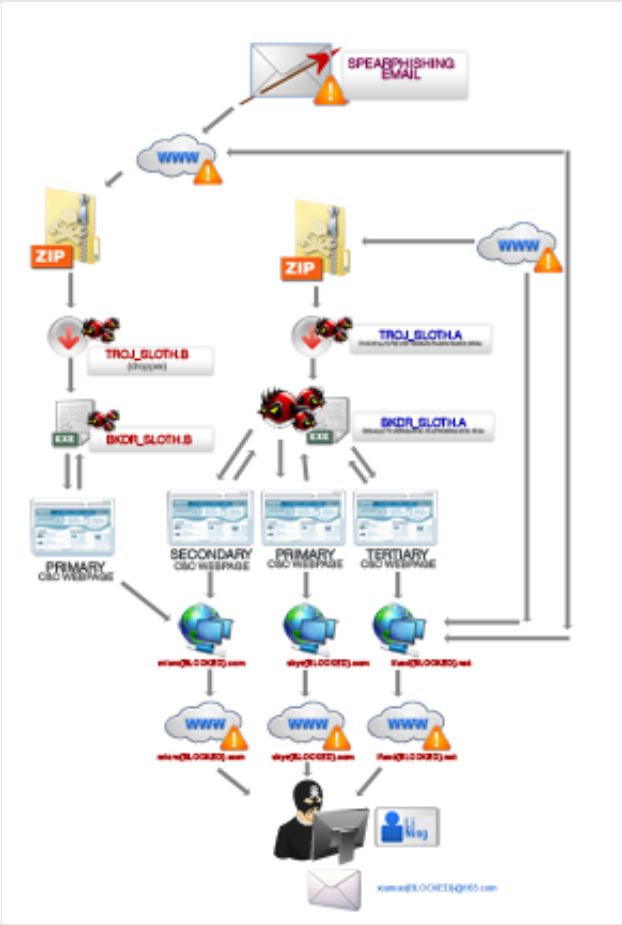

Figure 1. Attribution Graph (click the thumbnail for full view)

During the course of our investigation into this new campaign, we investigated the malware dropped. We quickly noticed the registrant of *sky{BLOCKED}.com* is also the same registrant as

micro{BLOCKED}.com and *ifued{BLOCKED}.net*. This individual used the name Li Ning and others with an email address of *xiaomao{BLOCKED}@163.com*. This individual also recently registered 79 additional domains. There are a total of roughly 17,000 domains registered with this same email address.

Figure 2. Domains registered under the name Li Ning, based on Whois data

Conclusion

Early detection is crucial in preventing targeted attacks from exfiltrating confidential company data. Organizations and large enterprises need an advanced threat protection platform like Trend Micro™ Deep Discovery, which can mitigate the risks posed by targeted attacks through its various security technologies and global threat intelligence. At the heart of our Custom Defense solution is Deep Discovery which provides real-time local and global intelligence across the attack life cycle. This can help IT administrators understand the nature of the attack they are dealing with.

Trend Micro blocks all related threats, emails and URLs associated with these attacks. As always, we advise users to exercise caution when opening emails and links.

With additional insights and analysis from Kervin Alintanahin, Dove Chiu, and Kyle Wilhoit.