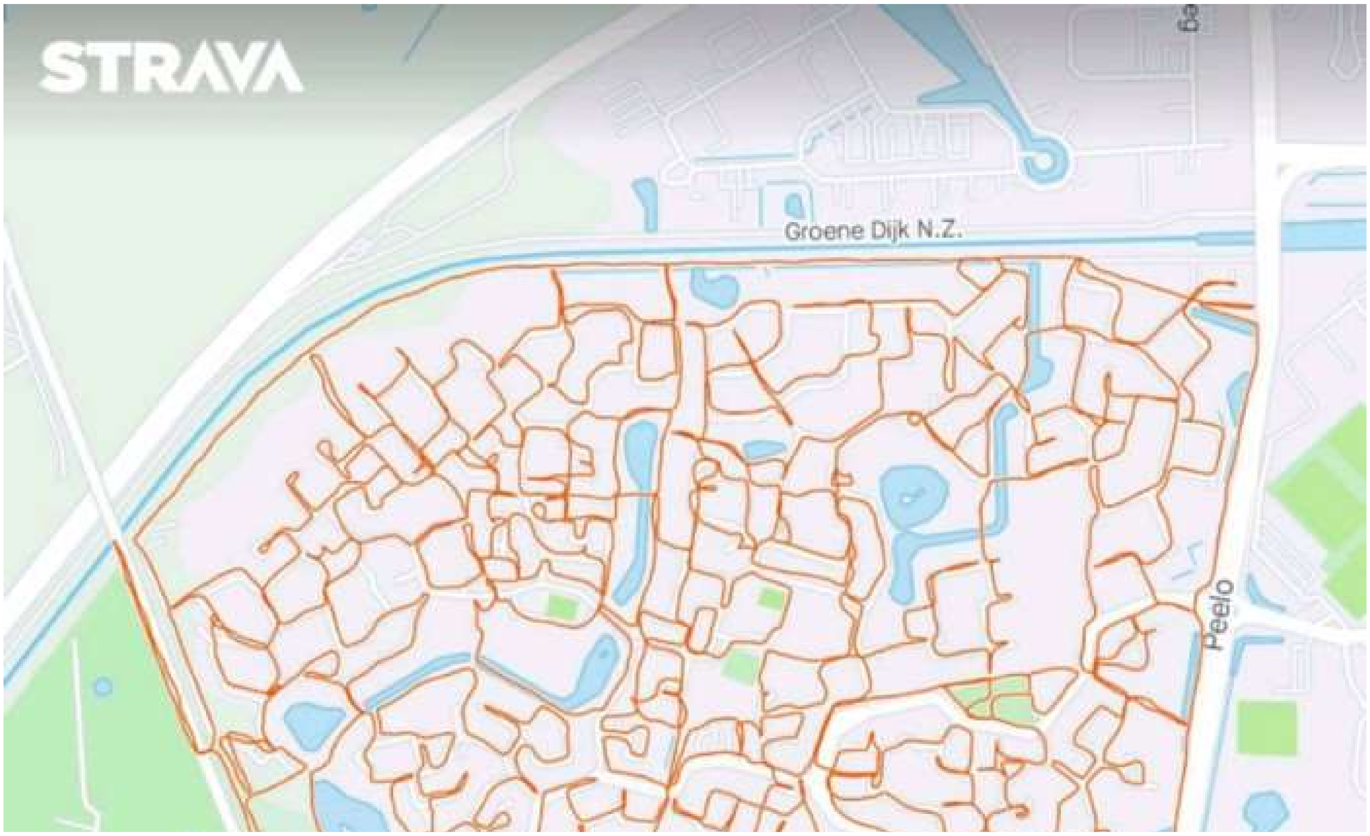
Peekaboo we see GRU

Peekaboo we see GRU 3 days ago · 2 min read

Peekaboo we see GRU (part 1)

This image shows the route a postal worker (mailman) takes each day to deliver mail to several hundred homes. If this delivery person was an “attacker”, this information would be essential to help catch them and identify homes that might have evidence that can be used to stop the criminal gang in the future.



For Microsoft Windows computers, Sysmon is free and one of the best tools an administrator can use to detect malicious events on host computers and throughout the company network.

When an email arrives in a users inbox, administrators hope that malicious emails have been filtered out. If a malicious (phishing) email is able to bypass those first layers of protection, we hope the user doesn't do something that allows the attacker to control the user's computer. Today it is common for attackers to gain code execution on user's systems. Once we have accepted this reality we need to think about how to detect these events.

In part one of this series, we won't repeat information about Sysmon setup and config that has already been explained well by others. If you don't have Sysmon installed, please check out these guides. One of the core data sources for this series is Sysmon. Without Sysmon, we won't know what parts of our network are under the attackers control.

How to install and use Sysmon for malware investigation (sophos.com)

Getting Started With Sysmon — Black Hills Information Security (blackhillsinfosec.com)

Splunking with Sysmon Series Part 1: The Setup | Hurricane Labs