1. What key evolutions happened with this campaign in its 4 main iterations?

Over the 4 main iterations, a couple key evolutions happened. Firstly, over the 4 iterations, the defense evasion techniques changed drastically. In campaign 1, the defense evasion techniques used were T1055, T1085, T1045, T1064 and T1158. No defense evasion techniques were used in campaign 2 while in campaign 3, only T1140. Finally, in campaign 4, T1099, T1112, T1045 and T1221 were used. The only technique that was used multiple times were T1045: Software packing and even this was only used in campaign 1 and 4. This could mean that either the techniques used in campaigns 1-3 were to some extent ineffective prompting the change or that SOFACY intends to consistently change their defense evasion techniques in order to make it difficult to detect them.

Another key evolution can be seen in the execution techniques used. In campaign 1, T1085, T1064 and T1204 were used. In campaign 2, T1204 was used and in campaign 3, T1059 and T1086 were used. Finally, in campaign 4, T1047 and T1204 were. This evolution is interesting because T1204 User Execution seems to be commonly used by SOFACY but the techniques they use along with it tend to differ including campaign 2 where they used no other technique for execution.

One final evolution can be seen in the command and control techniques used. In campaign 1, T1071, T1132 and T1105 were used. In campaign 2, T1024 and T1043 were used while in campaign 3, T1071 and T1105 were used. T1071, T1104, T1105 and T1094 were used in campaign 4. With the exception of campaign 2, SOFACY seems to prefer using T1071: Standard Application Layer Protocol and T1105: Remote File copy for command control. From campaign 1 to 4, T1132: Data Encoding was removed and eventually replaced by T1104: Multi-Stage channels and T1094: Custom Command and Control Protocol. This seems to imply that during this time, SOFACY may have implemented their own custom Command and Control technology.

1. What datasets/data feeds would we need to have coming into SIEM to detect SOFACY?

The most commonly used techniques by SOFACY are T1193: Spearphishing attachment being used in all 4 campaigns followed by T1204: User Execution, T1071: Standard Application Layer Protocol, T1105: Remote File Copy, T1113: Screen Capture, T1057: Process discovery and T1082: System Information Discovery. As a result, the datasets/data feeds that we need to have coming to detect SOFACY could consist of:

* T1193: Spearphishing Attachment
  + Detonation Chamber
  + Email gateway
  + File monitoring
  + Mail server
  + Network Intrusion detection system
  + Packet Capture
* T1204: User execution
  + Anti-virus
  + Process command-line parameters
  + Process monitoring
* T1071: Standard Application Layer Protocol
  + DNS records
  + Netflow
  + Network protocol analysis
  + Packet Capture
  + Process monitoring
  + Process use of network
* T1105: Remote File Copy
  + File monitoring
  + Netflow
  + Network protocol analysis
  + Packet capture
  + Process command-line parameters
  + Process monitoring
  + Process use of network
* T1113: Screen Capture
  + API monitoring
  + File monitoring
  + Process monitoring
* T1057: Process Discovery
  + API monitoring
  + Process command-line parameters
  + Process monitoring
* T1082: System Information Discovery
  + Cloud logs
  + Process command-line parameters
  + Process monitoring
  + Stackdriver logs

Since that is a lot of data, the data sources that appeared for more than 2 techniques are

* Appeared in 6
  + Process monitoring
* Appeared in 4
  + Process command-line parameters
* Appeared in 3
  + Packet capture

Since the above 3 detect multiple techniques that appear to be commonly used by SOFACY, they are likely the data sets would needed to be processed by the SIEM system.

1. Would we use static correlation or user/entity behavior analytics or both?

We would use both. For static correlation, a SIEM rules could be written based on the data sources discussed above. For process monitoring, a SIEM rule could be written to notify an analyst if a process or command line arguments are being used to gather network information. This would be effective if it this kind of activity is not common. However, if this is something that is done regularly on the network, it would still be useful to have a SIEM rule for it for user/entity behavior analytics. Similar rules could be written for the different techniques used by SOFACY.

For user/entity behavior analytics, we would be interested in defining behaviors around chains of techniques used by SOFACY. For example, a behavior around User Execution, Process Discovery and Remote File Copy. This could be someone from SOFACY installing software, performing discovery on the network and exfiltrating the data.

For populations of interest, if activities such as network scanning or remote file copy are only done by a small subset of the users, those activities should be locked behind a privilege. This means an attacker would have to escalate their privilege before being able to conduct certain activities which increases the chance of them being detected.

In this case, static correlation is used as an alert for potentially malicious activity. Behavior analytics are used to process the alerts as stricter indicator of compromise.

1. Thinking proactively, if we had some level of confidence that SOFACY was active in our environment, list and prioritize (triage) what incident response activities we would want to carry out?

Highest priority

* Review process and command-line logs for activity that could be SOFACY trying to gather system and network information
* Analyze unexpected network flows or packet captures to determine if it may be SOFACY
* Check network logs for file newly created files that were sent over the network
* Check user inboxes for potential spear phishing attacks that were successful

Lowest priority

The purpose of these activities is to attempt to confirm if SOFACY is in the system. If any of the analysis yields suspicious data, from there associated accounts that SOFACY may have been used can be locked down in order to remove SOFACY from the network.

1. How could we work ahead of the adversary? List some specific technical controls you would work with the IT/tech teams to implement in order to prevent key SOFACY techniques.

Detection tools

* Monitor processes and command-line arguments for actions that could be taken to gather system and network information
* Analyze network data for uncommon data flows
* Collect information from unusual processes using API calls
* Monitor for file creation and files transferred into the network

Mitigations

* Implement Anti-virus
* Implement Network Intrusion preventions system
* User Training around spear-phishing