‘Operation Sharpshooter’ Targets Global Defense, Critical Infrastructure

securingtomorrow.mcafee.com/blogs/other-blogs/mcafee-labs/operation-sharpshooter-targets-global-

December 12, 2018

By Ryan Sherstobitoff and Asheer Malhotra on Dec 12, 2018
This post was written with contributions from the McAfee Advanced Threat Research team.

The McAfee Advanced Threat Research team and McAfee Labs Malware Operations Group have discovered a new global campaign targeting nuclear, defense, energy, and financial companies, based on McAfee® Global Threat Intelligence. This campaign, Operation Sharpshooter, leverages an in-memory implant to download and retrieve a second-stage implant—which we call Rising Sun—for further exploitation. According to our analysis, the Rising Sun implant uses source code from the Lazarus Group’s 2015 backdoor Trojan Duuzer in a new framework to infiltrate these key industries.

Operation Sharpshooter’s numerous technical links to the Lazarus Group seem too obvious to immediately draw the conclusion that they are responsible for the attacks, and instead indicate a potential for false flags. Our research focuses on how this actor operates, the global impact, and how to detect the attack. We shall leave attribution to the broader security community.

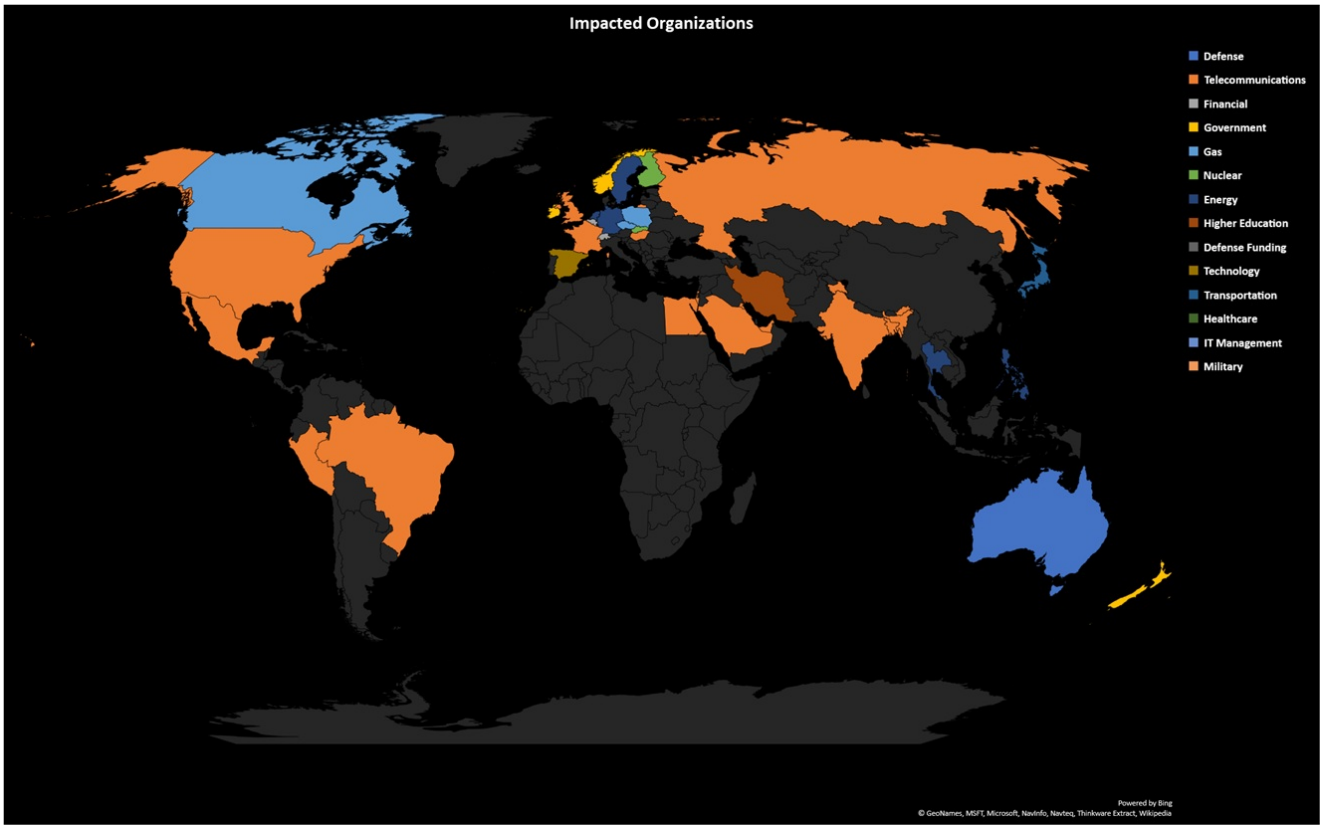
Read our full analysis of Operation Sharpshooter.

Have we seen this before?

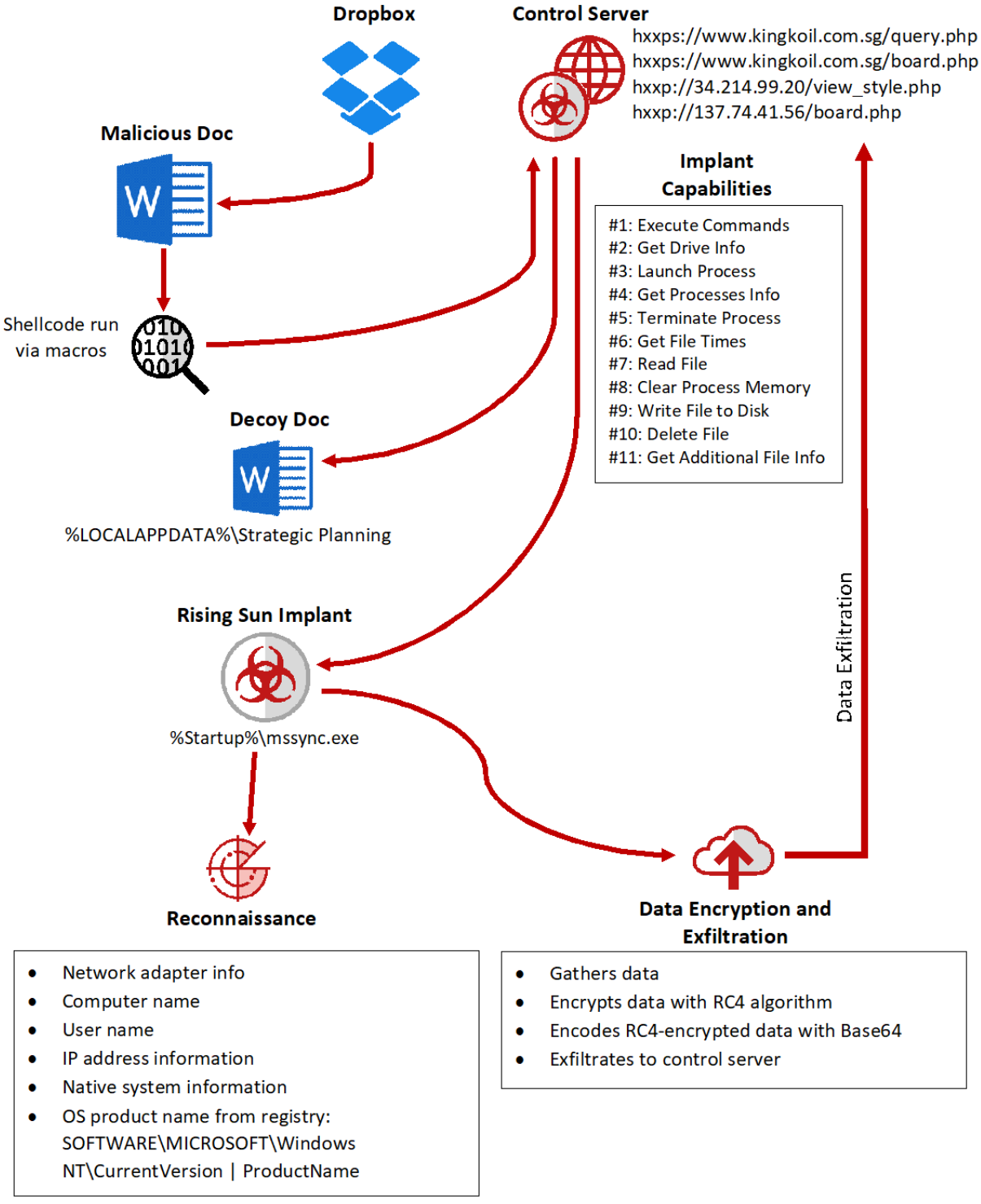
This campaign, while masquerading as legitimate industry job recruitment activity, gathers information to monitor for potential exploitation. Our analysis also indicates similar techniques associated with other job recruitment campaigns.

Global impact

In October and November 2018, the Rising Sun implant has appeared in 87 organizations across the globe, predominantly in the United States, based on McAfee telemetry and our analysis. Based on other campaigns with similar behavior, most of the targeted organizations are English speaking or have an English-speaking regional office. This actor has used recruiting as a lure to collect information about targeted individuals of interest or organizations that manage data related to the industries of interest. The McAfee Advanced Threat Research team has observed that the majority of targets were defense and government-related organizations.



Targeted organizations by sector in October 2018. Colors indicate the most prominently affected sector in each country. Source: McAfee® Global Threat Intelligence.



Infection flow of the Rising Sun implant, which eventually sends data to the attacker's control servers.

Conclusion

Our discovery of this new, high-function implant is another example of how targeted attacks attempt to gain intelligence. The malware moves in several steps. The initial attack vector is a document that contains a weaponized macro to download the next stage, which runs in

memory and gathers intelligence. The victim's data is sent to a control server for monitoring by the actors, who then determine the next steps.

We have not previously observed this implant. Based on our telemetry, we discovered that multiple victims from different industry sectors around the world have reported these indicators.

Was this attack just a first-stage reconnaissance operation, or will there be more? We will continue to monitor this campaign and will report further when we or others in the security industry receive more information. The McAfee Advanced Threat Research team encourages our peers to share their insights and attribution of who is responsible for Operation Sharpshooter.

Indicators of compromise

MITRE ATT&CK™ techniques

- Account discovery
- File and directory discovery
- Process discovery
- System network configuration discovery
- System information discovery
- System network connections discovery
- System time discovery
- Automated exfiltration
- Data encrypted
- Exfiltration over command and control channel
- Commonly used port
- Process injection

Hashes

- 8106a30bd35526bded384627d8eebce15da35d17
- 66776c50bcc79bbcecdbe99960e6ee39c8a31181
- 668b0df94c6d12ae86711ce24ce79dbe0ee2d463
- 9b0f22e129c73ce4c21be4122182f6dcbc351c95
- 31e79093d452426247a56ca0eff860b0ecc86009

Control servers

- 34.214.99.20/view_style.php
- 137.74.41.56/board.php
- kingkoil.com.sg/board.php

Document URLs

- hxxp://208.117.44.112/document/Strategic Planning Manager.doc
- hxxp://208.117.44.112/document/Business Intelligence Administrator.doc
- hxxp://www.dropbox.com/s/2shp23ogs113hnd/Customer Service Representative.doc?dl=1

McAfee detection

- RDN/Generic Downloader.x
- Rising-Sun
- Rising-Sun-DOC