‘Operation Sharpshooter’ Targets Global Defense, Critical Infrastructure

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

December 12, 2018

Ryan Sherstobitoff
Dec 12, 2018

4 MIN READ

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.

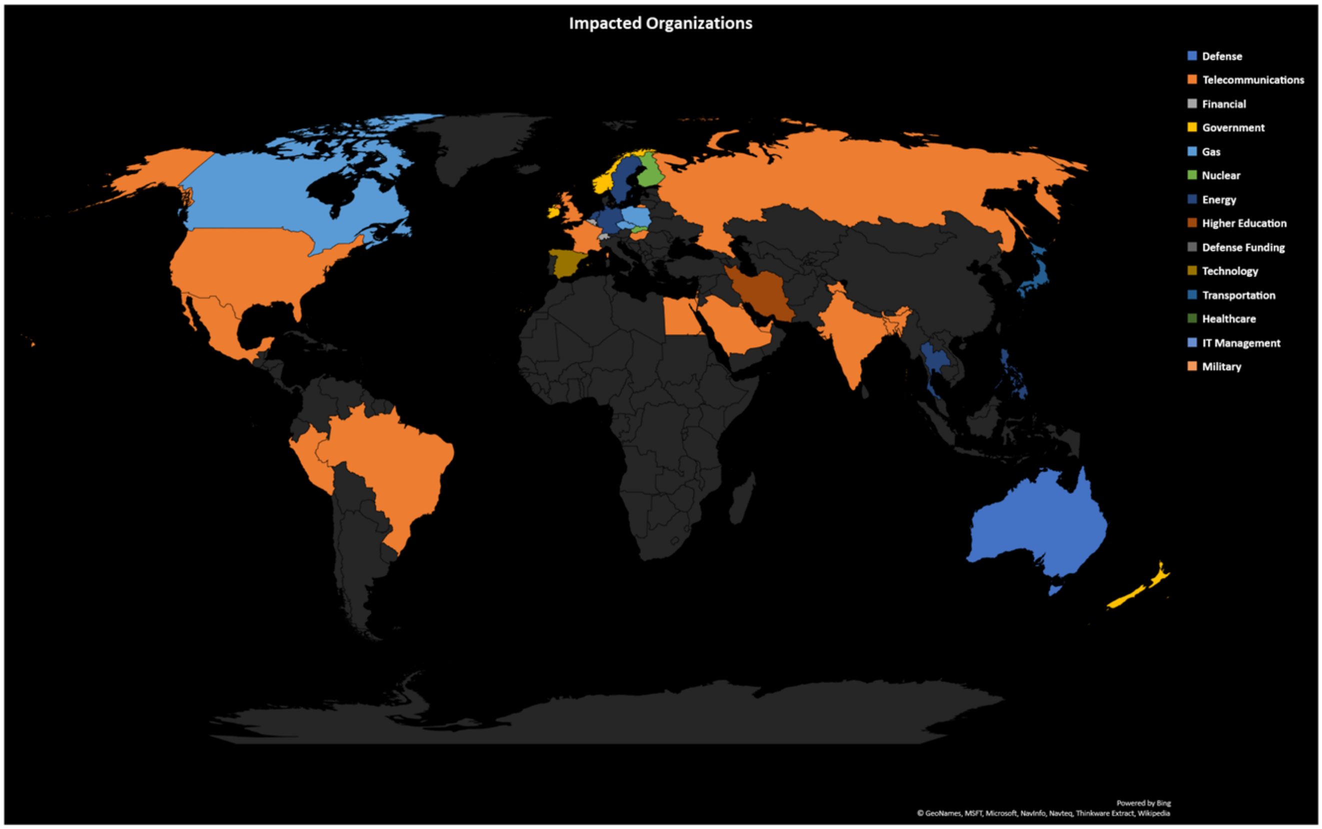
Read our full analysis of Operation Sharpshooter.

Have we seen this before?

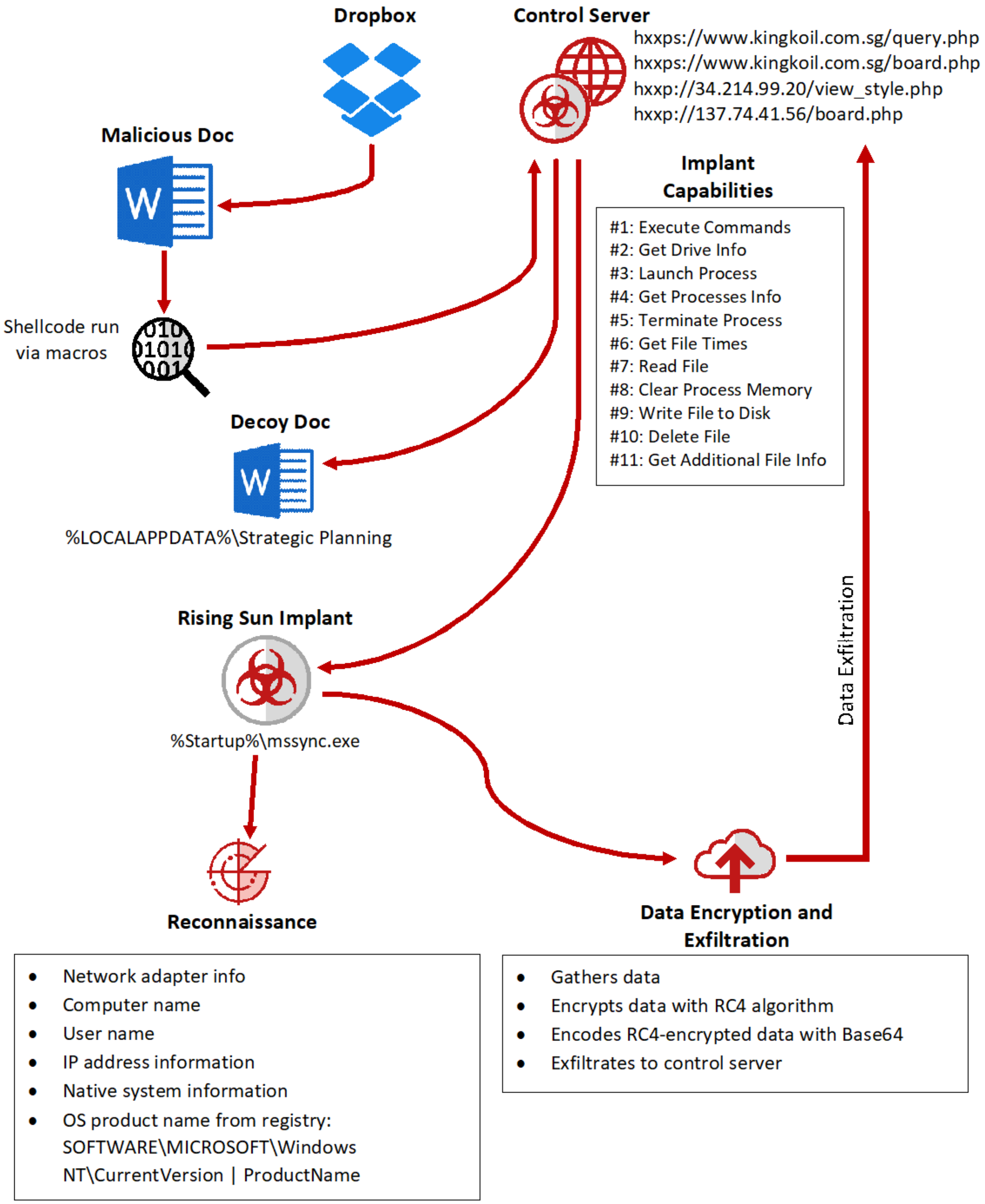
This campaign, while masquerading as legitimate industry job recruitment activity, gathers information to monitor for potential exploitation. Our analysis also indicates similar techniques associated with other job recruitment campaigns.

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.


Dropbox
Control Server
hxxps://www.kingkoil.com.sg/query.php
hxxps://www.kingkoil.com.sg/board.php
hxxp://34.214.99.20/view_style.php
hxxp://137.74.41.56/board.php
Malicious Doc
Implant Capabilities
Shellcode run via macros
Decoy Doc
%LOCALAPPDATA%\Strategic Planning
Rising Sun Implant
%Startup%\mssync.exe
Data Exfiltration
Reconnaissance
Data Encryption and Exfiltration

#1: Execute Commands
#2: Get Drive Info
#3: Launch Process
#4: Get Processes Info
#5: Terminate Process
#6: Get File Times
#7: Read File
#8: Clear Process Memory
#9: Write File to Disk
#10: Delete File
#11: Get Additional File Info

- Network adapter info
- Computer name
- User name
- IP address information
- Native system information
- OS product name from registry: SOFTWARE\MICROSOFT\Windows NT\CurrentVersion | ProductName

- Gathers data
- Encrypts data with RC4 algorithm
- Encodes RC4-encrypted data with Base64
- Exfiltrates to control server

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

Ryan Sherstobitoff
Ryan Sherstobitoff is a Senior Analyst for Major Campaigns – Advanced Threat Research in McAfee. Ryan specializes in threat intelligence in the Asia Pacific Region where he conducts cutting edge...

More from McAfee Labs

Crypto Scammers Exploit: Elon Musk Speaks on Cryptocurrency

By Oliver Devane Update: In the past 24 hours (from time of publication) McAfee has identified 15...

May 05, 2022 | 4 MIN READ

Instagram Credentials Stealer: Disguised as Mod App

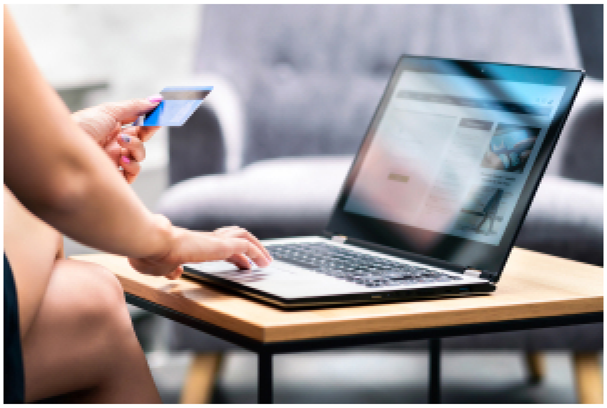
Authored by Dexter Shin McAfee's Mobile Research Team introduced a new Android malware targeting Instagram users who...

May 03, 2022 | 4 MIN READ

Instagram Credentials Stealers: Free Followers or Free Likes

Authored by Dexter Shin Instagram has become a platform with over a billion monthly active users. Many...

May 03, 2022 | 6 MIN READ



Scammers are Exploiting Ukraine Donations

Authored by Vallabh Chole and Oliver Devane Scammers are very quick at reacting to current events, so...

Apr 01, 2022 | 7 MIN READ

Imposter Netflix Chrome Extension Dupes 100k Users

Authored by Oliver Devane, Vallabh Chole, and Aayush Tyagi McAfee has recently observed several malicious Chrome Extensions...

Mar 10, 2022 | 8 MIN READ

Why Am I Getting All These Notifications on my Phone?

Authored by Oliver Devane and Vallabh Chole   Notifications on Chrome and Edge, both desktop browsers, are commonplace,...

Feb 25, 2022 | 5 MIN READ

Emotet's Uncommon Approach of Masking IP Addresses

In a recent campaign of Emotet, McAfee Researchers observed a change in techniques. The Emotet maldoc was...

Feb 04, 2022 | 4 MIN READ

HANCITOR DOC drops via CLIPBOARD

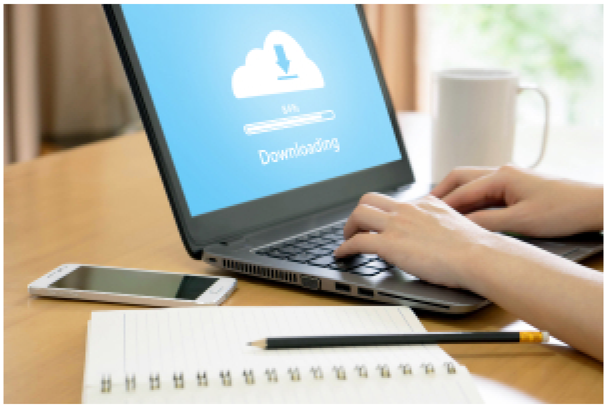
Hancitor, a loader that provides Malware as a Service, has been observed distributing malware such as FickerStealer,...

Dec 13, 2021 | 6 MIN READ

‘Tis the Season for Scams

‘Tis the Season for Scams

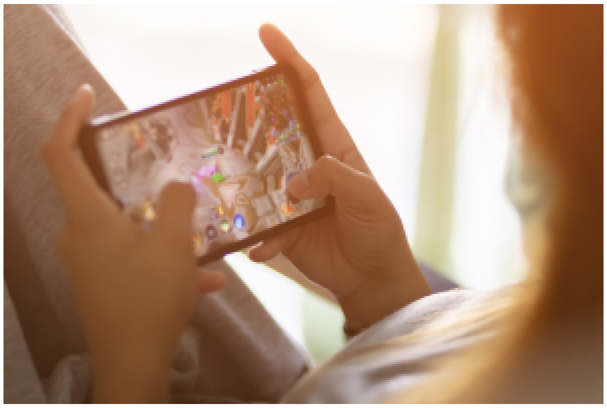
Nov 29, 2021 | 18 MIN READ



The Newest Malicious Actor: “Squirrelwaffle” Malicious Doc.

Authored By Kiran Raj Due to their widespread use, Office Documents are commonly used by Malicious actors...

Nov 10, 2021 | 4 MIN READ



Social Network Account Stealers Hidden in Android Gaming Hacking Tool

Authored by: Wenfeng Yu McAfee Mobile Research team recently discovered a new piece of malware that specifically...

Oct 19, 2021 | 6 MIN READ

Malicious PowerPoint Documents on the Rise

Authored by Anuradha M McAfee Labs have observed a new phishing campaign that utilizes macro capabilities available...

Sep 21, 2021 | 6 MIN READ