‘Operation Oceansalt’ Delivers Wave After Wave

securingtomorrow.mcafee.com/other-blogs/mcafee-labs/operation-oceansalt-delivers-wave-after-wave/

October 18, 2018

Raj Samani

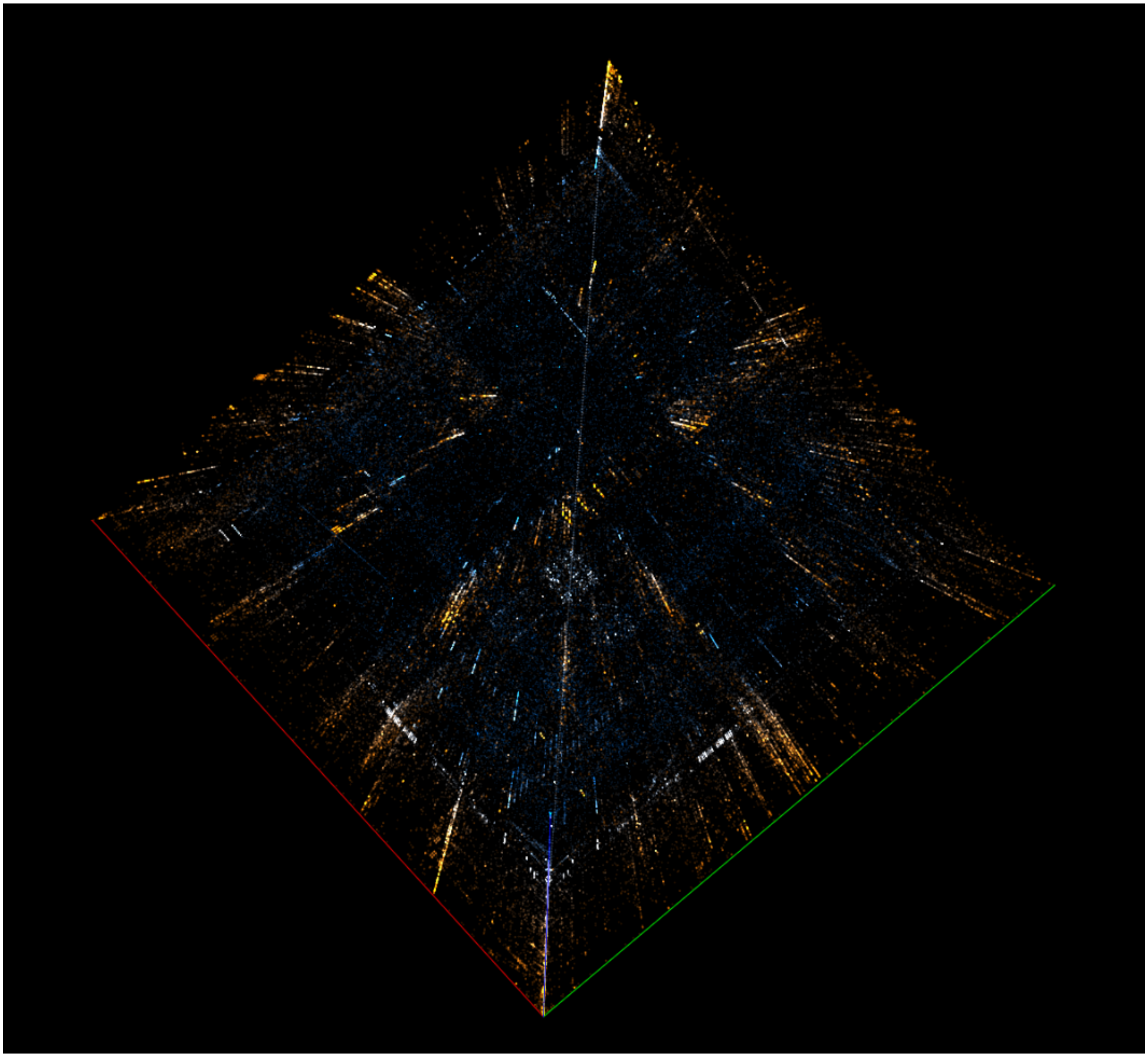
Oct 17, 2018

4 MIN READ

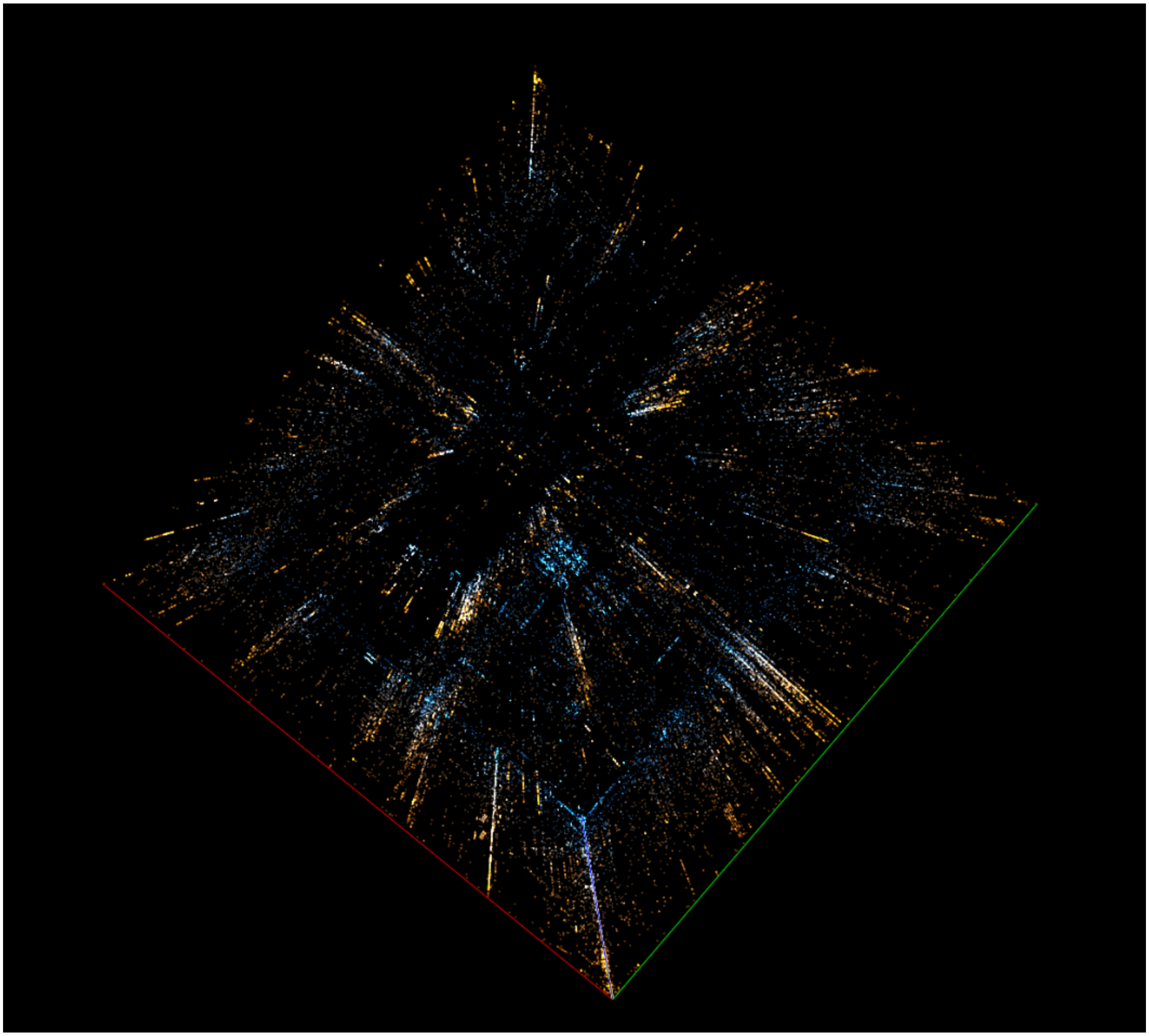
A wall eight feet high with three strands of barbed wire is considered sufficient to deter a determined intruder, at least according to the advice offered by the CISSP professional certification. Although physical controls can be part of a multifaceted defense, an electronic attack affords the adversary time to develop the necessary tools to bypass any logical wall set before them. In the latest findings from the McAfee Advanced Threat Research team, we examine an adversary that was not content with a single campaign, but launched five distinct waves adapted to their separate targets. The new report “Operation Oceansalt Attacks South Korea, U.S., and Canada with Source Code from Chinese Hacker Group” analyzes these waves and their victims, primarily in South Korea but with a few in the United States and Canada.

Although one reaction is to marvel at the level of innovation displayed by the threat actor(s), we are not discussing five new, never-before-seen malware variants—rather the reuse of code from implants seen eight years prior. The Oceansalt malware uses large parts of code from the Seasalt implant, which was linked to the Chinese hacking group Comment Crew. The level of reuse is graphically depicted below:

Code Visualization of Recent Oceansalt with Older Seasalt



Oceansalt, 2018.



Seasalt, 2010.

Who is Behind the Oceansalt Attack?

Originally taking the title APT1, the Comment Crew was seen as the threat actor conducting offensive cyber operations against the United States almost 10 years before. The obvious suspect is Comment Crew and, although this may seem a logical conclusion, we have not seen any activity from this group since they were initially exposed. Is it possible that this group has returned and, if so, why target South Korea?

It is possible that the source code developed by Comment Crew has now been used by another adversary. The code to our knowledge, however, has never been made public. Alternatively, this could be a "false flag" operation to suggest that we are seeing the re-emergence of Comment Crew. Creating false flags is a common practice.

What Really Matters

It is likely that reactions to this research will focus on debating the identity of the threat actor. Although this question is of great interest, answering it will require more than the technical evidence that private industry can provide. These limitations are frustrating. However, we can focus on the indicators of compromise presented in this report to detect, correct, and protect our systems, regardless of the source of these attacks.

Perhaps more important is the possible return of a previously dormant threat actor and, further, why should this campaign occur now? Regardless of whether this is a false flag operation to suggest the rebirth of Comment Crew, the impact of the attack is unknown. However, one thing is certain. Threat actors have a wealth of code available to leverage new campaigns, as previous research from the Advanced Threat Research team has revealed. In this case we see that collaboration not within a group but potentially with another threat actor —offering up considerably more malicious assets. We often talk about partnerships within the private and public sector as the key to tackling the cybersecurity challenges facing society. The bad actors are not putting these initiatives on PowerPoint slides and marketing material; they are demonstrating that partnerships can suit their ends, too.

Raj Samani VP, Chief Technical Officer EMEA
Raj Samani is Chief Scientist and Fellow for the Enterprise business. He has assisted multiple law enforcement agencies in cybercrime cases and is a special advisor to the European Cybercrime...

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

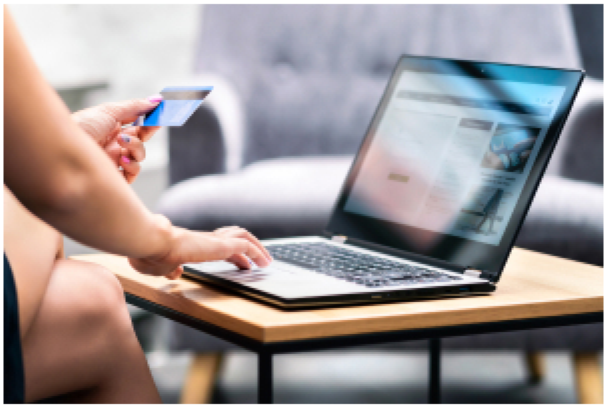
Authored by Dexter Shin McAfee's Mobile Research Team introduced a new Android malware targeting Instagram users who...

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

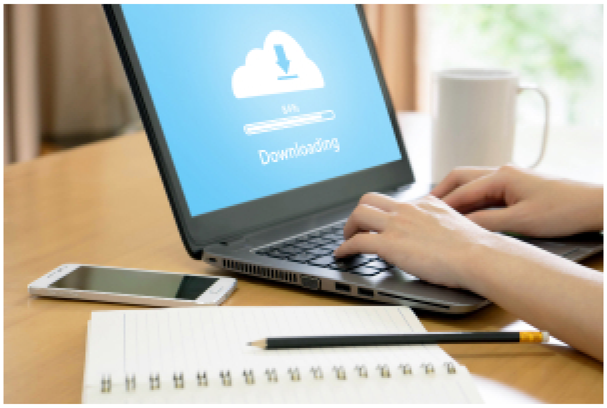
Hancitor, a loader that provides Malware as a Service, has been observed distributing malware such as FickerStealer,...

Dec 13, 2021 | 6 MIN READ

‘Tis the Season for Scams

‘Tis the Season for Scams

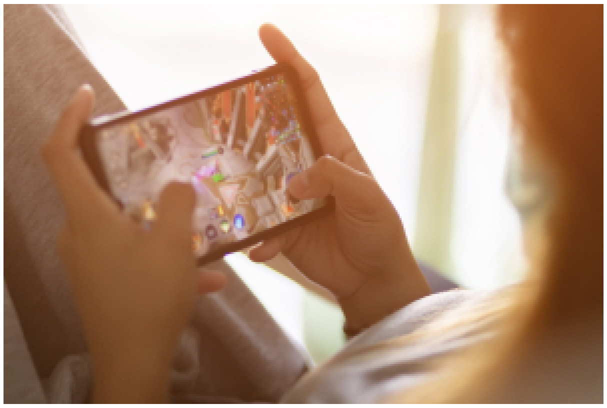
Nov 29, 2021 | 18 MIN READ



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