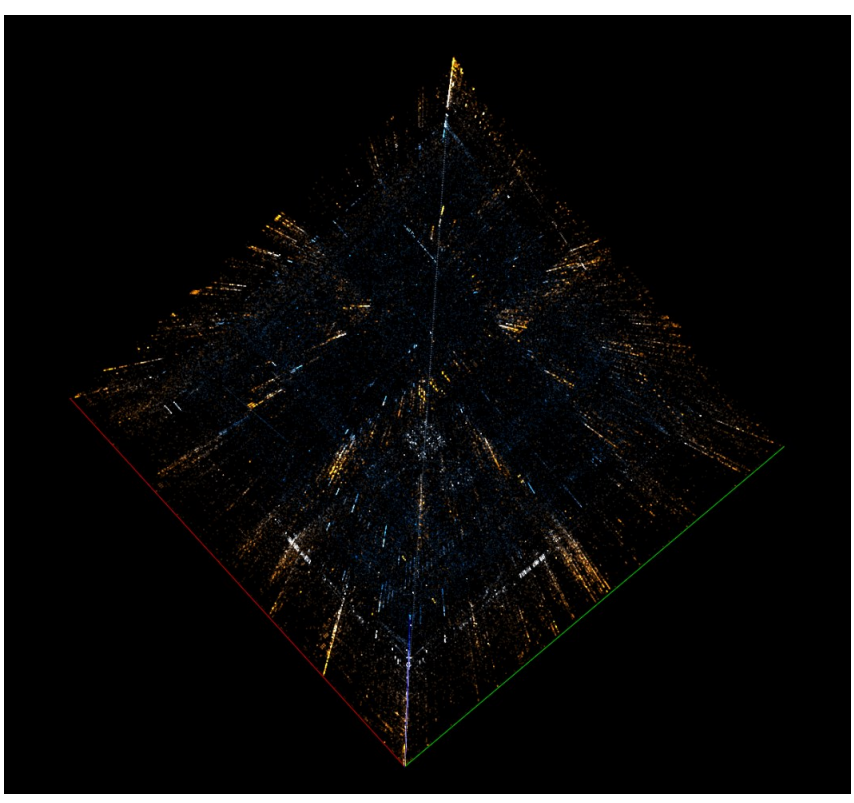
‘Operation Oceansalt’ Delivers Wave After Wave

By Raj Samani and Ryan Sherstobitoff on Oct 17, 2018

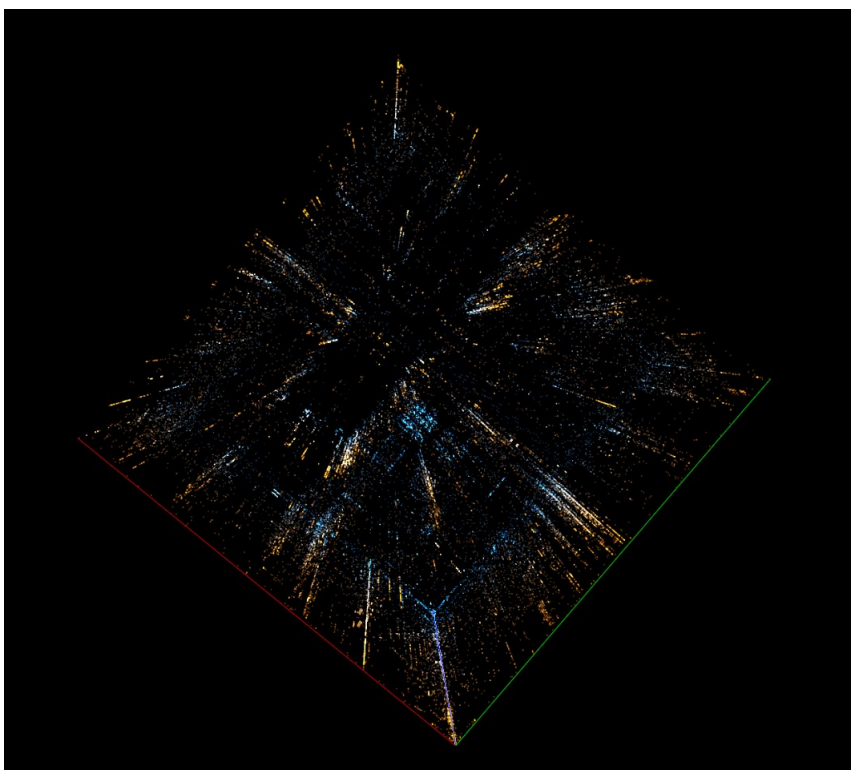
A wall eight feet high with three strands of barbed wire is considered sufficient to deter a determined intruder, at least according to the advice offered by the CISSP professional certification. Although physical controls can be part of a multifaceted defense, an electronic attack affords the adversary 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.

About the Author

Raj Samani

Raj Samani is Chief Scientist and McAfee Fellow for cybersecurity firm McAfee. He has assisted multiple law enforcement agencies in cybercrime cases, and is a special advisor to the European Cybercrime Centre in The Hague. Samani has been recognized for his contribution to the computer security industry through numerous awards, including the Infosecurity Europe hall ...

Read more posts from Raj Samani ›

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 research into new adversarial techniques and adapts those to better monitor the threat landscape. He formerly was the Chief Corporate Evangelist at Panda Security, where ...

Read more posts from Ryan Sherstobitoff ›

‹ Previous Article
Next Article ›

Categories: McAfee Labs
Tags: malware, endpoint protection, cybersecurity, Advanced Threat Research

Leave a reply

Facebook Comments Comments (0)

Similar Blogs