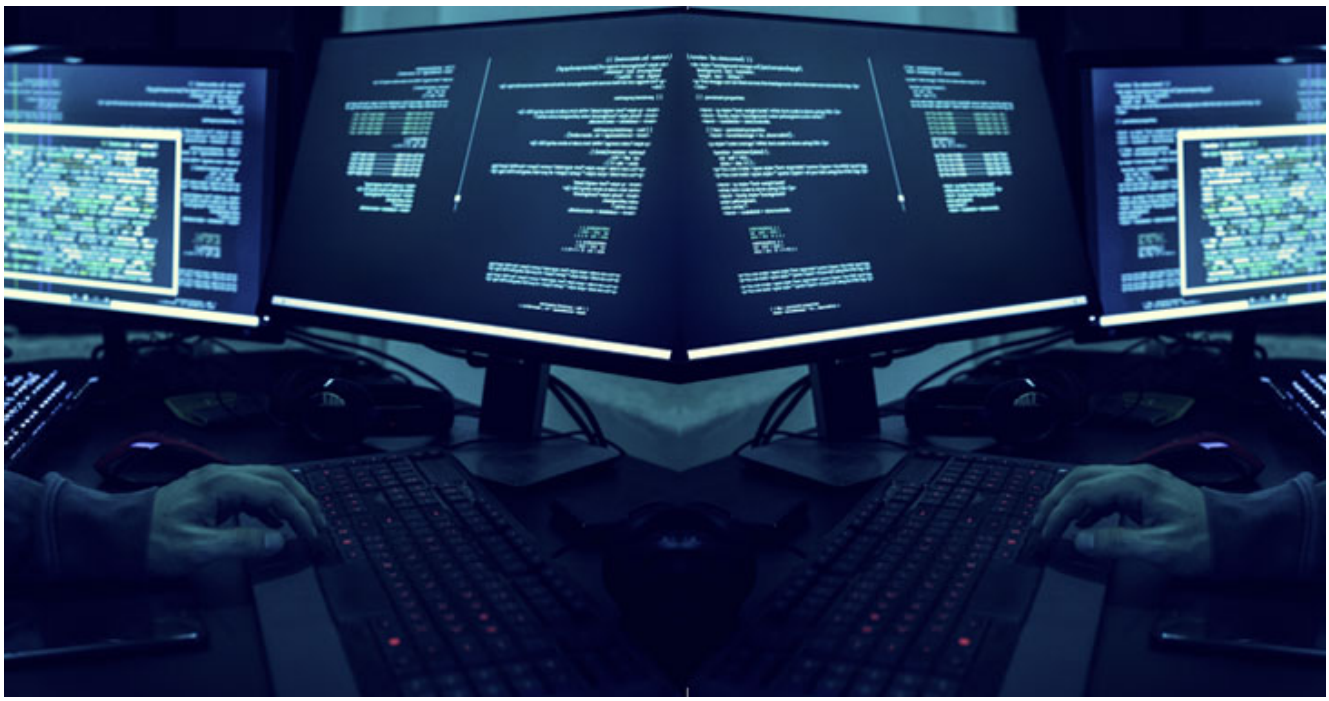
Researchers Find New Evidence Linking Kwampirs Malware to Shamoon APT Hackers

thehackernews.com/2022/03/researchers-find-new-evidence-linking.html

March 14, 2022



New findings released last week showcase the overlapping source code and techniques between the operators of Shamoon and Kwampirs, indicating that they "are the same group or really close collaborators."

"Research evidence shows identification of co-evolution between both Shamoon and Kwampirs malware families during the known timeline," Pablo Rincón Crespo of Cylera Labs said.

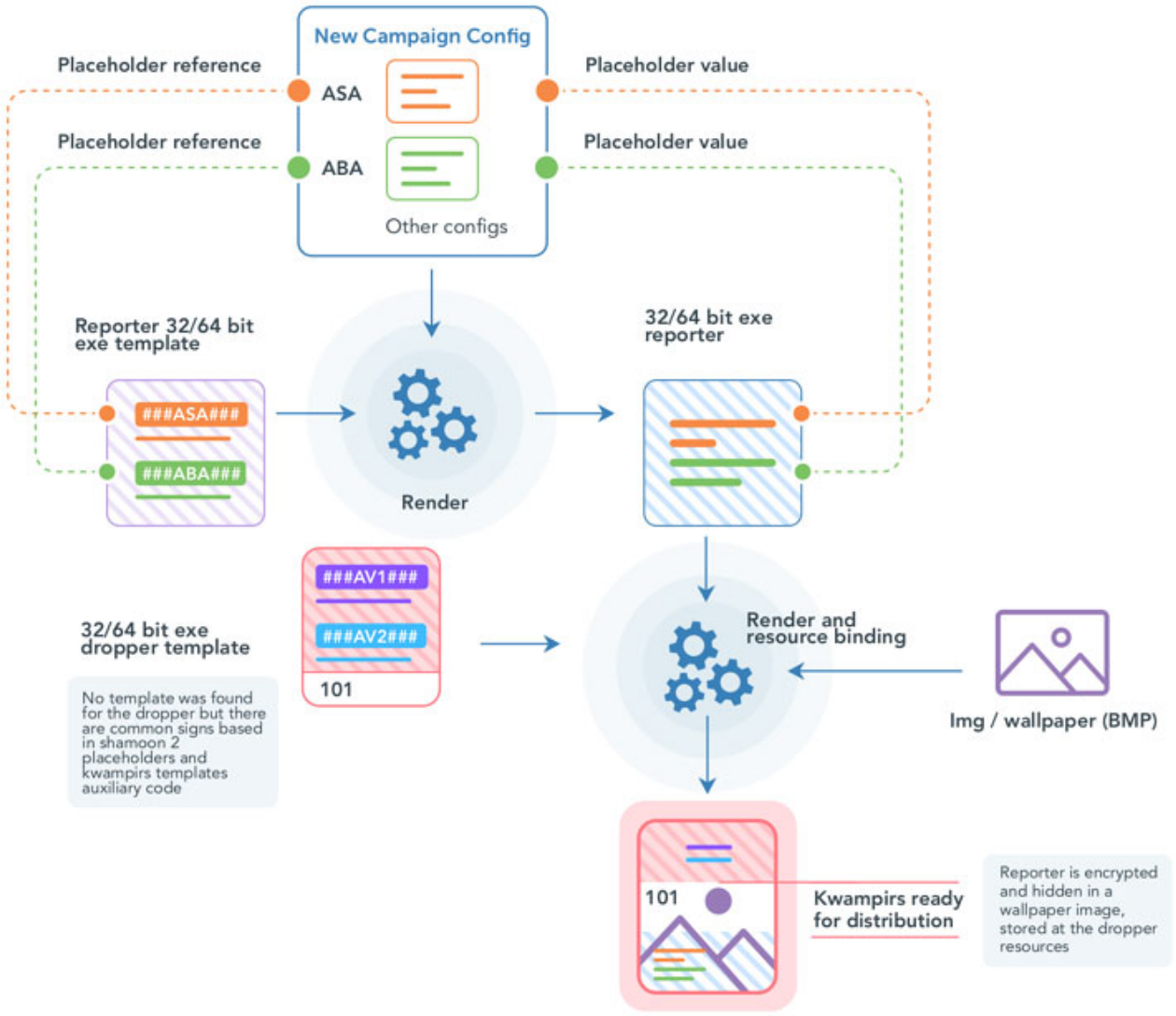
"If Kwampirs is based on the original Shamoon, and Shamoon 2 and 3 campaign code is based on Kwampirs, […] then the authors of Kwampirs would be potentially the same as the authors of Shamoon, or must have a very strong relationship, as has been seen over the course of many years," Rincón Crespo added.

Shamoon, also known as DistTrack, functions as an information-stealing malware that also incorporates a destructive component that allows it to overwrite the Master Boot Record (MBR) with arbitrary data so as to render the infected machine inoperable.

The malware, developed by the eponymous hacking crew also tracked as Magic Hound, Timberworm, COBALT GIPSY, was first documented by Broadcom-owned Symantec in August 2012. At least two updated versions of Shamoon have since emerged, Shamoon 2 in 2016 and Shamoon 3 in 2018.

In July 2021, the U.S. government attributed Shamoon as the handiwork of Iranian state-sponsored actors, linking it to cyber offensives targeting industrial control systems.

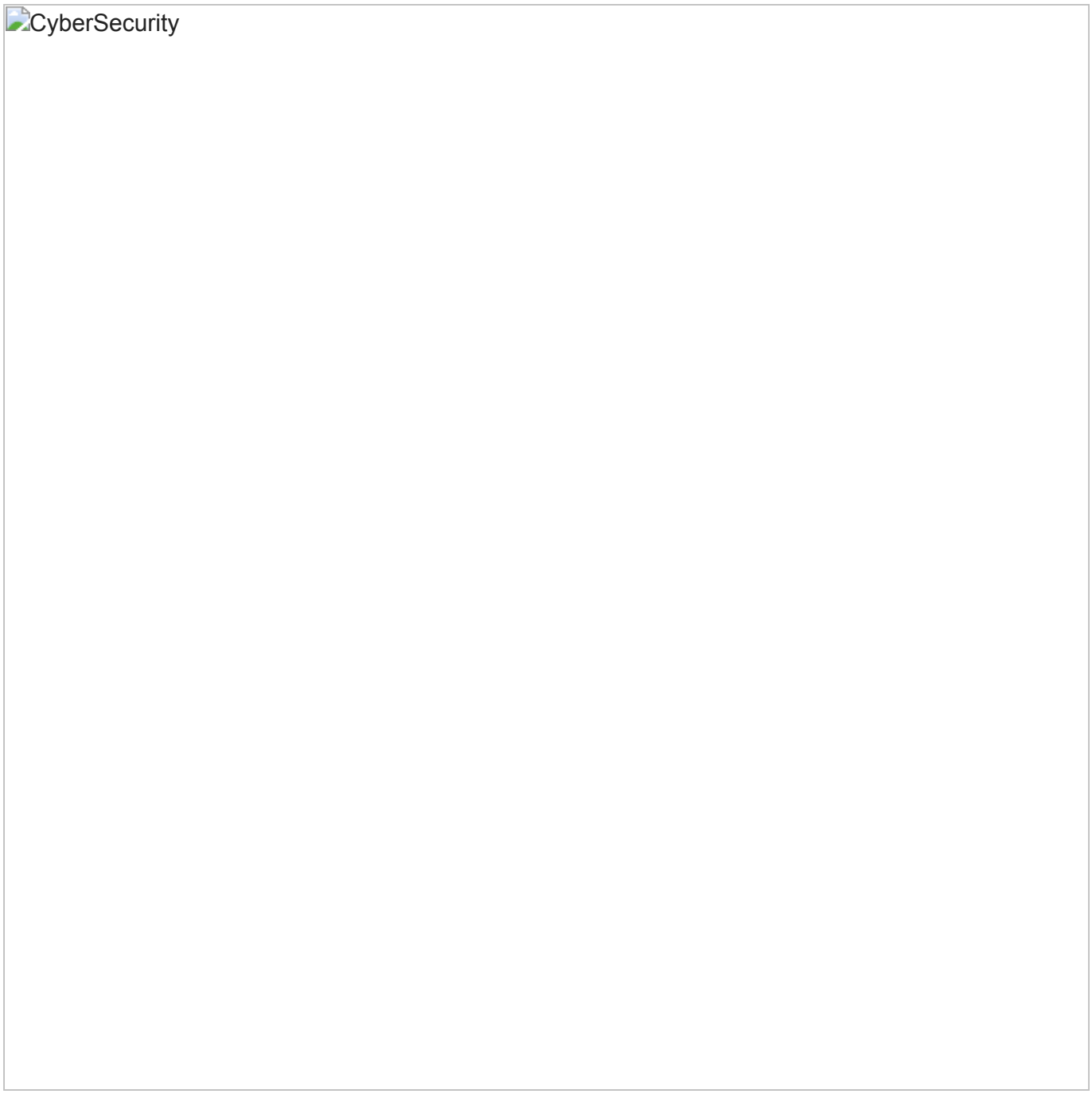
On the other hand, attack activity involving the Kwampirs backdoor has been connected to a threat group known as Orangeworm, with Symantec disclosing an intrusion campaign aimed at entities in the healthcare sector in the U.S., Europe, and Asia.



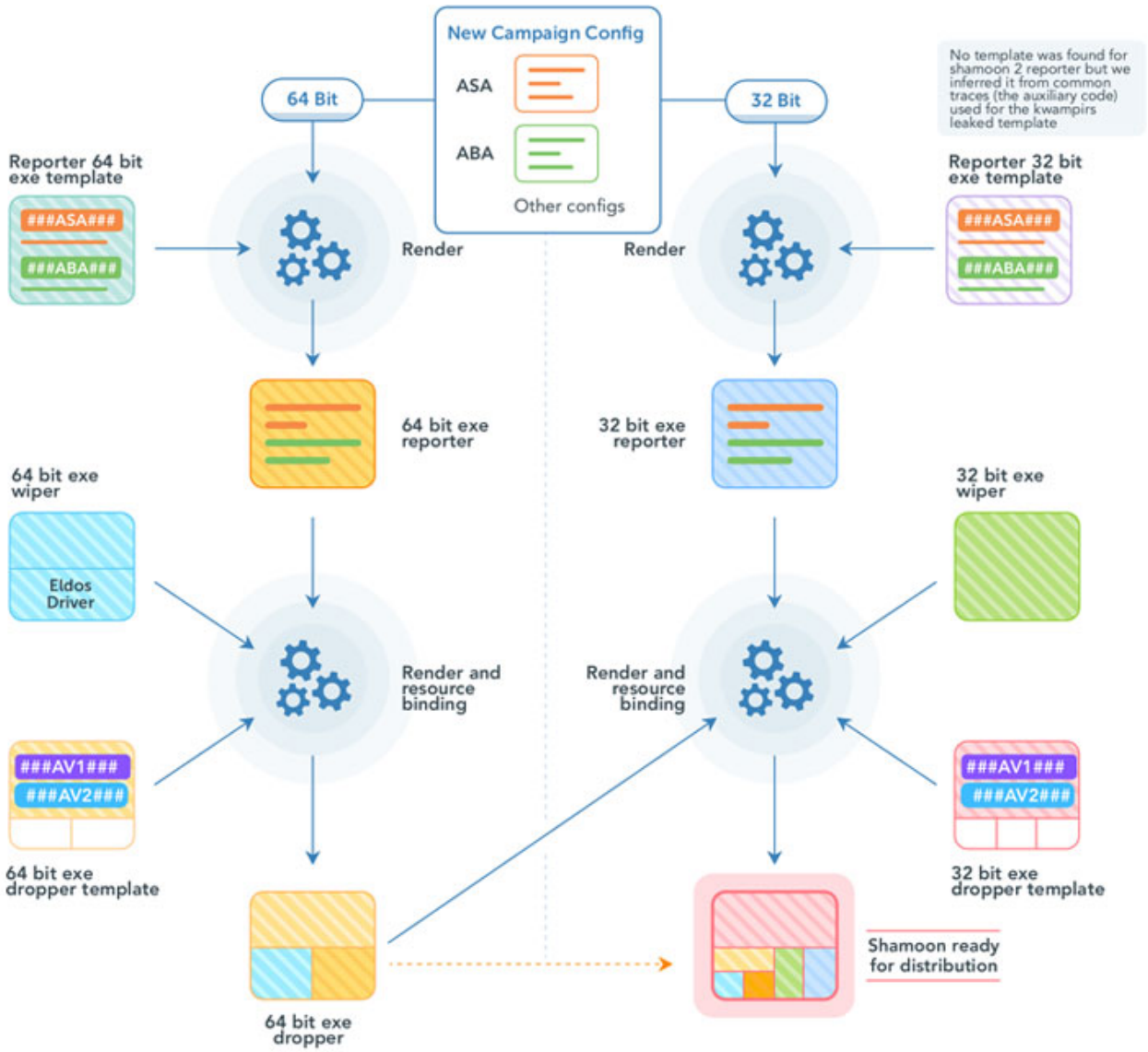
"Kwampirs New Campaign Building Process" explained by Cylera

"First identified in January 2015, Orangeworm has also conducted targeted attacks against organizations in related industries as part of a larger supply-chain attack in order to reach their intended victims," Symantec said in an analysis in April 2018.

Cylera Labs' uncovering of the connection stems from malware artifacts and previously unnoticed components, one of which is said to be an intermediary "stepping stone" version. It's a Shamoon dropper but sans the wiper feature, while simultaneously reusing the same loader code as Kwampirs.



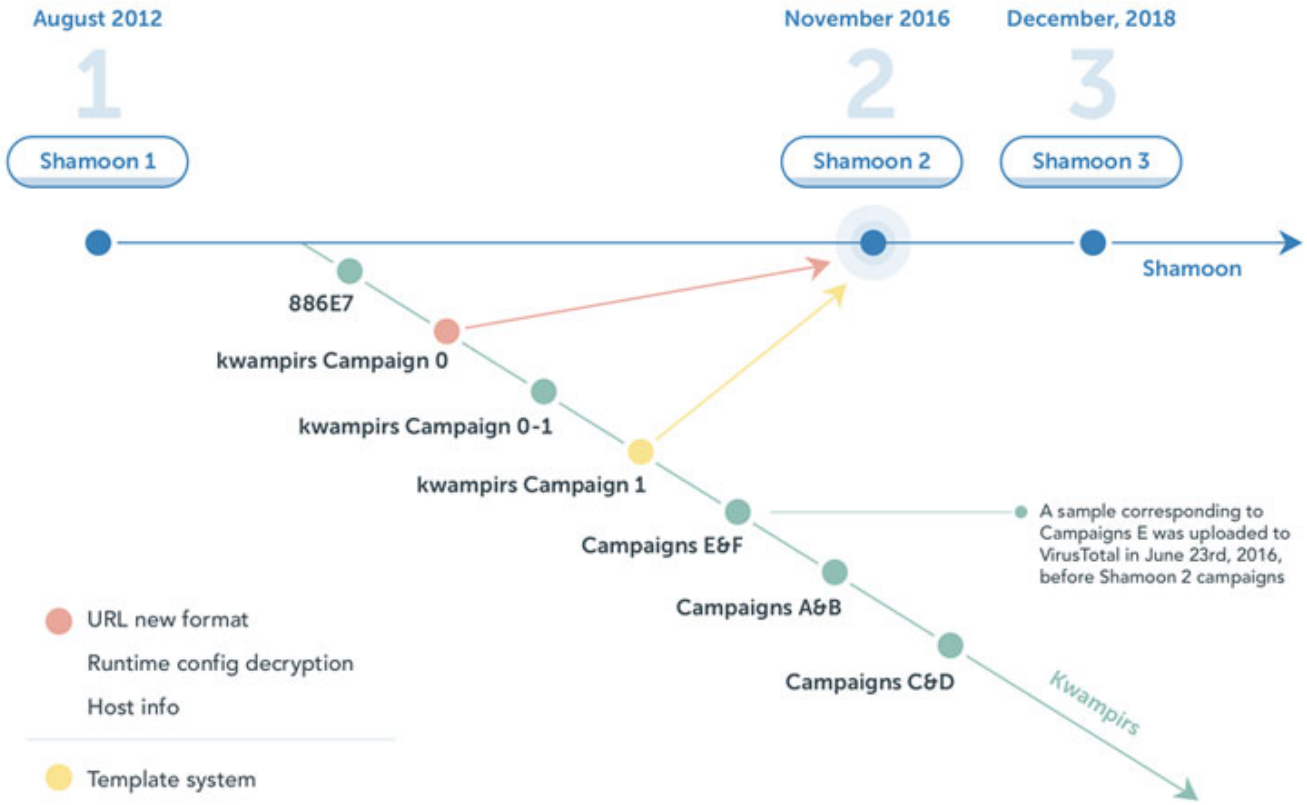
What's more, code-level similarities have been uncovered between Kwampirs and subsequent versions of Shamoon. This includes the functionality to retrieve system metadata, fetch MAC address, and the victim's keyboard layout information as well as the use of the same InternetOpenW Windows API to craft HTTP requests to the command-and-control (C2) server.



"Shamoon 2 New Campaign Building Process" explained by Cylera

Also put to use is a common template system to create the reporter module that houses capabilities to upload host information and download additional payloads to execute from their C2 servers, a feature that was missing in the first version of Shamoon.

In connecting the disparate dots, the investigation has led to the assessment that Kwampirs is likely based on Shamoon 1 and that Shamoon 2 inherited some of its code from Kwampirs, implying that the operators of both the malware are different sub-groups of a larger umbrella group or that it's the work of a single actor.



Such a claim isn't without precedence. Just last week, Cisco Talos detailed the TTPs of another Iranian actor called MuddyWater, noting that the nation-state actor is a "conglomerate" of multiple teams operating independently rather than a single threat actor group.

"These conclusions, if indeed correct, would recast Kwampirs as a large-scale, multi-year attack on global healthcare supply chains conducted by a foreign state actor," the researchers concluded.

"The data gathered and systems accessed in these campaigns have a wide range of potential usage, including theft of intellectual property, gathering of medical records of targets like dissidents or military leaders, or reconnaissance to aid in the planning of future destructive attacks."

SHARE □ □ □ □ ⅎ
SHARE □