'Hangover' Persists, More Mac Malware Found

By Kelly Jackson Higgins

Published: 2013-07-18 · Archived: 2026-04-05 18:32:14 UTC

Researchers who this spring unearthed details of a diverse cyberespionage campaign out of India recently discovered it using additional malware targeting Mac OS X machines, as well as telltale signs that some of the suspected actors behind the hacks know they are being watched online.

The so-called Operation Hangover attacks targeting Pakistan, China, the U.S., and other nations is unusual in its global, franchise-style approach: It appears to be run by an independent cyberspying organization that hires out different aspects of the campaign. There were no zero-day bugs used, no earmarks of nation-state sponsorship, but the campaign for three or more years has been targeting multiple national-interest and industrial entities around the globe, mostly Pakistan and U.S. organizations, but also Norwegian telecom provider Telenor and the Chicago Mercantile Exchange.

Norman Shark researchers at Black Hat USA later this month will provide details on new Mac malware they found in the attacks, as well as an inside look into what went on behind the scenes as they tracked this campaign -- including proof that the attackers are trying to hide their tracks in the wake of Norman Shark's report about them.

"We have come across more domains and IP addresses to help us illuminate more of the bad guys' network," says Jonathan Camp, who, along with fellow Norman Shark researcher Snorre Fagerland, headed up the research on Operation Hangover.

"Two things came to light as we published the report. The very nature of the research in this is iterative: We find one small thing that looks interesting, and it leads to three more interesting things. We keep following those paths -- domains or user names, for example, or parts of a social media network ... and we continue to get more information."

Camp, who won't reveal all of the details until his presentation at Black Hat, says some of the actors in the attack campaign began pulling their resumes and other information offline after Norman Shark's report was published in late May. "We noticed quite a few resumes started disappearing from the Web. A small bit of information would be removed," he says. "We were able to correlate between when the report was released and the changes made. The people responsible for this had the report and changed things."

Spotting the actors taking down online information just confirmed some of Norman Shark's findings, he says. "It showed us we were absolutely on the right path, that our assertions were valid because of all of the changes we saw," he says.

[Operation Hangover signals new franchise model in cyberespionage with cyberspying services for hire. See 'Commercialized' Cyberespionage Attacks Out Of India Targeting U.S., Pakistan, China, And Others.]

Operation Hangover works in a model unlike other publicized advanced persistent threat-style attacks. "This is a model that is different from what we've seen before ... it's a lot more difficult to track," Fagerland, principal security researcher in the malware detection team at Norman Shark, told Dark Reading in late May. "My concern is that this shows just how commercialized this seems to have been and how lucrative it possibly is. So you get these APTs growing up everywhere."

Hangover appears to employ freelance code-writers, and uses a "standardized" approach with regular patterns of establishing domains and placing images in them. F-Secure this spring blogged about a targeted attack dropping Mac spyware on an Angolan dissident's computer, an attack Norman Shark attributed to Operation Hangover as well.

Meanwhile, Norman Shark found "more Mac malware" after publishing the late May report, according to Camp.

He says it was interesting to drill down into how the actors in the campaign were organized and who was responsible for which piece of code or spearphish, for example. "They were not just focused on one specific target. And they have lots of different people" working on various elements of the campaign, he says.

The big question mark with the op, however, is whether Indian security firm Appin Security Group is involved. Norman says the word "Appin" and "AppinSecurity Group" appear inside executables, and an alleged Hangover coder's professional profile was found on an online employment website for freelance programmers that said he works for Appin.

The Norman Shark report says it could be a case of falsified evidence trying to pin nefarious behavior on Appin, or "maybe someone has tried to hurt Appin by falsifying evidence to implicate them. Maybe some rogue agent within Appin Security Group is involved, or maybe there are other explanations."

Other security firms, such as CrowdStrike, that have studied the attacks say it's no coincidence that Appin's name came up in the research. Adam Meyers, director of intelligence at CrowdStrike, which has been studying the same attacks but under the moniker of Viceroy Tiger, said in an interview in May that Appin appears to have some connection: "But it would be extremely unlikely that they are innocent victims in this. The likelihood that they developed and were using the software is extremely high," he told Dark Reading

Appin, meanwhile, has disputed any connection to the cyberattacks.

The attacks target various entities and industries, mainly in Pakistan. But organizations in the U.S., Norway, Iran, China, Taiwan, Thailand, Jordan, Indonesia, the U.K., Germany, Austria, Poland, Romania, and other nations also have been in the bull's eye. Operation Hangover has gone after military and government organizations, mining, telecommunications, law firms (in the U.S. as well), food and restaurants, and manufacturing industries.

Have a comment on this story? Please click "Add Your Comment" below. If you'd like to contact Dark Reading's editors directly, send us a message.

About the Author

Editor-in-Chief, Dark Reading

Kelly Jackson Higgins is the Editor-in-Chief of Dark Reading and VP, cybersecurity editorial at Informa TechTarget, where she leads editorial strategy for the company's three cybersecurity media brands: Dark Reading, SearchSecurity and Cybersecurity Dive. She is an award-winning veteran technology and business journalist with three decades of experience in reporting and editing for various technology and business publications and major media properties. Jackson Higgins was selected three consecutive times as one of the Top 10 Cybersecurity Journalists in the U.S., and was named as one of Folio's 2019 Top Women in Media. She has been with Dark Reading since its launch in 2006.
