Global Phishing Attacks Spawn Three New Malware Strains

The never-seen malware strains have "professionally coded sophistication" and were launched by a well-resourced APT using nearly 50 domains, one hijacked.

Two waves of global financial phishing attacks that swamped at least 50 organizations in December have delivered three new malware families, according to a report from FireEye’s Mandiant cybersecurity team.

On Tuesday, the team said that they’ve dubbed the hitherto-unseen malware strains Doubledrag, Doubledrop, and Doubleback. What Mandiant called the “trifecta” spear-phishing campaign twice hit a wide swath of industries worldwide: first on Dec. 2, 2020, with a second wave launched between Dec. 11 and Dec. 18, 2020.

The US was the primary target for attacks in both waves, while EMEA and Asia and Australia shared equal suffering in the first wave.

These Are No Schlubs

Mandiant tracks the threat actor as UNC2529 and says that these guys are pros. Given the “considerable” infrastructure they have at their disposal, their carefully crafted phishing lures, and what the researchers called the “professionally coded sophistication” of the malware, the team says that the UNC2529 attackers seem “experienced and well-resourced.”

The UNC2529 gang researched their targets well, tailoring their phishing email subject lines to their intended victims. In one instance, the threat actors masqueraded as an account executive for a small, California-based electronics manufacturer, sending out seven phishing emails that targeted a slew of industries, from medical to defense. All of the emails contained subject lines that were specific to the products of the company that the threat actors were pretending to be associated with.

Three-Stage Process

The malware ecosystem used by UNC2529 consists of either a downloader (Doubledrag) or an Excel document with an embedded macro; a dropper (Doubledrop); and a backdoor (Doubleback).

The infection starts with phishing emails that are rigged with a link to download a malicious payload that contains a JavaScript downloader with code that’s heavily obfuscated in order to evade analysis. Once it’s executed, Doubledrag tries to download a dropper – Doubledrop – in the second stage of the attack chain. Doubledrop is an obfuscated PowerShell script designed to plant a backdoor into memory. It has two flavors: a 32-bit and a 64-bit instance of the Doubleback backdoor.

With all that set up, the backdoor gets to work inserting plugins and reporting back to its controllers.

“The backdoor, once it has the execution control, loads its plugins and then enters a communication loop, fetching commands from its C2 server and dispatching them,” Mandiant describes. “One interesting fact about the whole ecosystem is that only the downloader exists in the file system. The rest of the components are serialized in the registry database, which makes their detection somewhat harder, especially by file-based antivirus engines.”

50 Domains Chugging Away

UNC2529 used a lot of firepower to run the December phishing attacks, Mandiant says. Nearly 50 domains supported the various phases of the campaigns. Meanwhile, the attackers did their due diligence, researching their targets to concoct convincing lures that would entice recipients to click. As well, one legitimate third-party domain was compromised.

The threat actors also worked hard to obfuscate the malware components. One tactic was the use of fileless malware, which runs in memory after initial infection, instead of storing files on the hard drive. According to analysis of telemetry data from Cisco, fileless malware was the most common critical-severity cybersecurity threat to endpoints during the first half of 2020. This use of fileless malware helped to flummox detection so that the threat actors could deliver what Mandiant called “a well coded and extensible backdoor.”

Dimiter Andonov, Senior Principal Reverse Engineer with Mandiant, told Threatpost in an email on Tuesday afternoon that the techniques employed in this new malware ecosystem – specifically, the file-less serialization on compromised systems – isn’t new, but it’s effective. “While the technique is not novel per se, few malware are known to use it and the result is that the malicious components are much harder to be detected,” Andonov says.

Mandiant assumes that the point of all this effort is profit: “The identified wide-ranging targets, across geography and industry suggests a financial crime motive,” it says.

The researchers say that Doubleback appears to be “an ongoing work in progress.” The team expects to see UNC2529 continue to compromise victims in all industries, around the world.

To keep from being pulled in by what Mandiant calls this “double trifecta,” the standard-issue “don’t click on suspicious links” advice applies, Andonov says. “As all of the phishing initial vectors depend on convincing the user to click a link or execute an attached file, the ‘don’t click on the suspicious links’ advice is the first line of defense,” he says. “In some spear-phishing campaigns the malicious email might appear to be sent by a coworker or a person who is known by the receiver, and in such cases it’s always a good practice to reach back to the sender before opening any attached files.

References:

- hhttps://www.bleepingcomputer.com/news/security/worldwide-phishing-attacks-deliver-three-new-malware-strains/?&web_view=true
- https://threatpost.com/global-phishing-attacks-new-malware-strains/165857/
- https://www.zdnet.com/article/researchers-find-three-new-malware-families-used-in-global-finance-phishing-campaign/
- https://www.databreaches.net/worldwide-phishing-attacks-deliver-three-new-malware-strains/