FIN11: Widespread Email Campaigns as Precursor for Ransomware and Data Theft

fireeye.com/blog/threat-research/2020/10/fin11-email-campaigns-precursor-for-ransomware-data-theft.html

Breadcrumb

Threat Research

Genevieve Stark, Andrew Moore, Vincent Cannon, Jacqueline O’Leary, Nalani Fraser, Kimberly Goody

Oct 14, 2020

3 mins read

Ransomware

Threat Research

Mandiant Threat Intelligence recently promoted a threat cluster to a named FIN (or financially motivated) threat group for the first time since 2017. We have detailed FIN11's various tactics, techniques and procedures in a report that is available now by signing up for Mandiant Advantage Free.

In some ways, FIN11 is reminiscent of APT1; they are notable not for their sophistication, but for their sheer volume of activity. There are significant gaps in FIN11's phishing operations, but when active, the group conducts up to five high-volume campaigns a week. While many financially motivated threat groups are short lived, FIN11 has been conducting these widespread phishing campaigns since at least 2016. From 2017 through 2018, the threat group primarily targeted organizations in the financial, retail, and hospitality sectors. However, in 2019 FIN11's targeting expanded to include a diverse set of sectors and geographic regions. At this point, it would be difficult to name a client that FIN11 hasn't targeted.

Mandiant has also responded to numerous FIN11 intrusions, but we've only observed the group successfully monetize access in few instances. This could suggest that the actors cast a wide net during their phishing operations, then choose which victims to further exploit based on characteristics such as sector, geolocation or perceived security posture. Recently, FIN11 has deployed CLOP ransomware and threatened to publish exfiltrated data to pressure victims into paying ransom demands. The group's shifting monetization methods—from point-of-sale (POS) malware in 2018, to ransomware in 2019, and hybrid extortion in 2020—is part of a larger trend in which criminal actors have increasingly focused on post-compromise ransomware deployment and data theft extortion.

Notably, FIN11 includes a subset of the activity security researchers call TA505, but we do not attribute TA505's early operations to FIN11 and caution against using the names interchangeably. Attribution of both historic TA505 activity and more recent FIN11 activity is complicated by the actors' use of criminal service providers. Like most financially motivated actors, FIN11 doesn't operate in a vacuum. We believe that the group has used services that provide anonymous domain registration, bulletproof hosting, code signing certificates, and private or semi-private malware. Outsourcing work to these criminal service providers likely enables FIN11 to increase the scale and sophistication of their operations.

To learn more about FIN11's evolving delivery tactics, use of services, post-compromise TTPs, and monetization methods, register for Mandiant Advantage Free. The full FIN11 report is also available through our FireEye Intelligence Portal (FIP). Then for even more information, register for our exclusive webinar on Oct. 29 where Mandiant threat intelligence experts will take a deeper dive into FIN11, including its origins, tactics, and potential for future activity.