The Newly-Named FIN11 Cybercrime Group Moves into Ransomware and Extortion

Executive Summary

Mandiant recently elevated a tracked threat cluster to the named threat group FIN11. Beginning in 2016 with phishing campaigns, this group has moved into double extortion ransomware operations utilizing CLOP ransomware. They indiscriminately attack organizations in every sector, including the pharmaceutical industry, via large phishing campaigns. Mitigations for the Healthcare and Public Health (HPH) sector can be found at the end of the report.

Report

On October 14, 2020, FireEye Mandiant published a blog post introducing a new threat group, dubbed FIN11. Mandiant has been tracking them as a threat cluster since 2016, noting their high-volume phishing campaigns that have targeted nearly every sector. In 2019, the group was seen shifting to CLOP ransomware, to include utilizing 'double extortion'. This technique occurs when a cybercriminal gang first steals an organizations information before encrypting it. The actors then demand payment to decrypt the data and to ensure they do not leak the organization's data. In early 2020, they began targeting pharmaceutical companies.

FIN11's tactics, techniques, and procedures (TTP) are constantly evolving. The below chart shows an almost monthly change in TTP from September 2019 to June 2020, with the only constant being the initial delivery of a phishing email and the eventual execution of a malicious Office document.

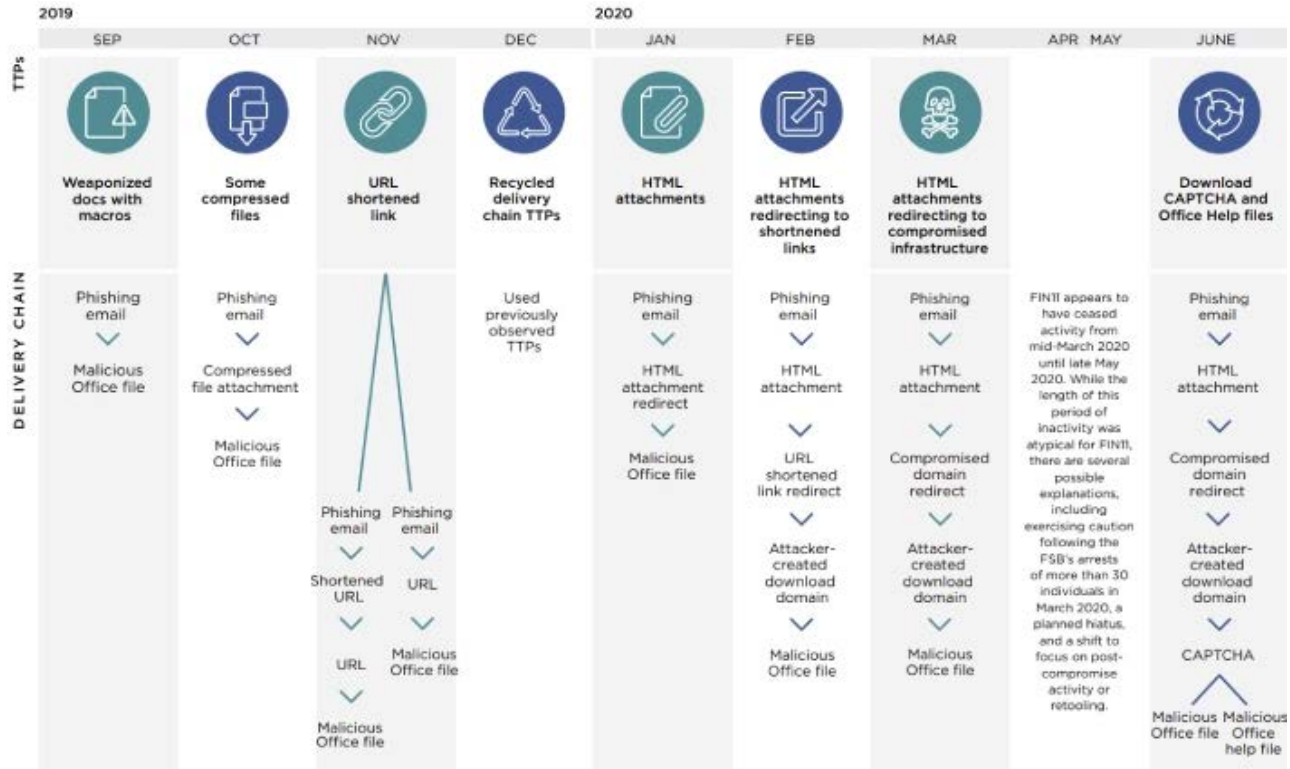

Figure 1 FIN11 TTPs

Mandiant researchers following FIN11 have assessed with moderate confidence that the group operates from somewhere within the Commonwealth of Independent States (CIS), which comprise most of the former Soviet Union countries. This assessment is based on FIN11's avoidance of systems utilizing CIS-country keyboard layouts and the

use of Russian-language file metadata.

Researchers believe that FIN11 outsources many of their services via underground, criminal communities. This includes using bulletproof hosting services, signed certificates, publicly available malware, and domain registration services. Attribution efforts are hampered when a cybercrime organization uses many of the same publicly-available services as other cybercriminals.

Figure 2 FIN11's use of publicly-available services

While the group uses a wide variety of malware purchased from underground sites, the use of malware code families FlawedAmmyy, FRIENDSPEAK, and MIXLABEL appear to be unique to FIN11. Due to an overlap in their TTPs, primarily its use of large-scale phishing campaigns, many organizations track FIN11 activity as the threat group TA505, famous for its use of the Dridex Trojan and Locky ransomware. While FIN11 and TA505 share TTPs, some of which have not been publicly reported, Mandiant researchers caution against conflating them as the same group, and are tracking them as two separate entities.

FIN11 should be treated the same as any other ransomware/extortion cybercrime group when it comes to safeguarding against their attacks. The Cybersecurity and Infrastructure Security Agency (CISA) recently published Alert (AA20-302A) - Ransomware Activity Targeting the Healthcare and Public Health Sector, in conjunction with the Department of Health and Human Services and the Federal Bureau of Investigations. This end of this Alert contains a section titled 'General Ransomware Mitigations – HPH Sector' and contains numerous best practices regarding ransomware along with points of contact should you become a victim. The link to this alert is in the References section.

References

https://www.fireeye.com/blog/threat-research/2020/10/fin11-email-campaigns-precursor-for-ransomware-data-theft.html
https://www.lineaedp.it/files/2020/10/report-prodotto.pdf
https://www.bleepingcomputer.com/news/security/fin11-hackers-jump-into-the-ransomware-money-making-scheme/
https://www.securityweek.com/fin11-spun-out-ta505-umbrella-distinct-attack-group
https://thehackernews.com/2020/10/fin11-hackers-spotted-using-new.html
https://us-cert.cisa.gov/ncas/alerts/aa20-302a