FIN7 Spear Phishing Campaign Targets Personnel Involved in SEC Filings

fireeye.com /blog/threat-research/2017/03/fin7_spear_phishing.html

In late February 2017, FireEye as a Service (FaaS) identified a spear phishing campaign that appeared to be targeting personnel involved with United States Securities and Exchange Commission (SEC) filings at various organizations. Based on multiple identified overlaps in infrastructure and the use of similar tools, tactics, and procedures (TTPs), we have high confidence that this campaign is associated with the financially motivated threat group tracked by FireEye as FIN7.

FIN7 is a financially motivated intrusion set that selectively targets victims and uses spear phishing to distribute its malware. We have observed FIN7 attempt to compromise diverse organizations for malicious operations – usually involving the deployment of point-of-sale malware – primarily against the retail and hospitality industries.

Spear Phishing Campaign

All of the observed intended recipients of the spear phishing campaign appeared to be involved with SEC filings for their respective organizations. Many of the recipients were even listed in their company's SEC filings. The sender email address was spoofed as EDGAR <filings@sec.gov> and the attachment was named "Important_Changes_to_Form10_K.doc" (MD5: *d04b6410dddee19adec75f597c52e386)*. An example email is shown in Figure 1.

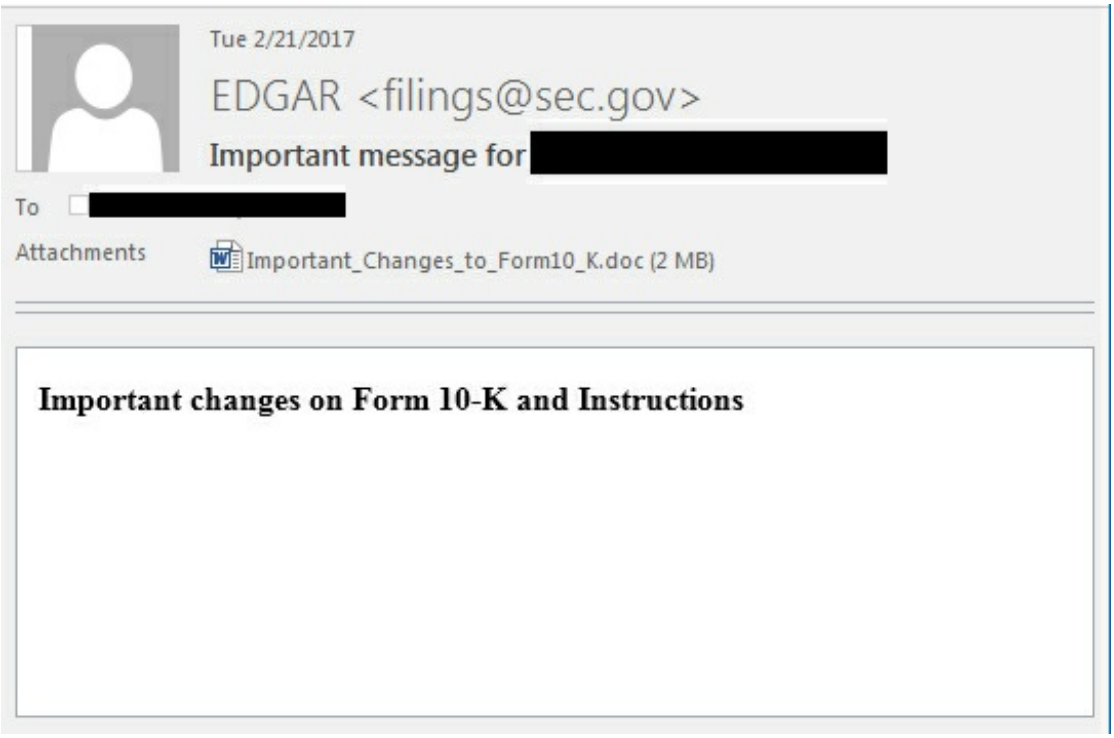

Figure 1: Example of a phishing email sent during this campaign

We have observed the following TTPs with this campaign:

- The malicious documents drop a VBS script that installs a PowerShell backdoor, which uses DNS TXT records for its command and control. This backdoor appears to be a new malware family that FireEye iSIGHT

Intelligence has dubbed POWERSOURCE. POWERSOURCE is a heavily obfuscated and modified version of the publicly available tool DNS_TXT_Pwnage. The backdoor uses DNS TXT requests for command and control and is installed in the registry or Alternate Data Streams. Using DNS TXT records to communicate is not an entirely new finding, but it should be noted that this has been a rising trend since 2013 likely because it makes detection and hunting for command and control traffic difficult.

- We also observed POWERSOURCE being used to download a second-stage PowerShell backdoor called TEXTMATE in an effort to further infect the victim machine. The TEXTMATE backdoor provides a reverse shell to attackers and uses DNS TXT queries to tunnel interactive commands and other data. TEXTMATE is "memory resident" – often described as "fileless" malware. This is not a novel technique by any means, but it's worth noting since it presents detection challenges and further speaks to the threat actor's ability to remain stealthy and nimble in operations.
- In some cases, we identified a Cobalt Strike Beacon payload being delivered via POWERSOURCE. This particular Cobalt Strike stager payload was previously used in operations linked to FIN7.
- We observed that the same domain hosting the Cobalt Strike Beacon payload was also hosting a CARBANAK backdoor sample compiled in February 2017. CARBANAK malware has been used heavily by FIN7 in previous operations.

Victims

Thus far, we have directly identified 11 targeted organizations in the following sectors:

- Financial services, with different victims having insurance, investment, card services, and loan focuses
- Transportation
- Retail
- Education
- IT services
- Electronics

All these organizations are based in the United States, and many have international presences. As the SEC is a U.S. regulatory organization, we would expect recipients of these spear phishing attempts to either work for U.S.-based organizations or be U.S.-based representatives of organizations located elsewhere. However, it is possible that the attackers could perform similar activity mimicking other regulatory organizations in other countries.

Implications

We have not yet identified FIN7's ultimate goal in this campaign, as we have either blocked the delivery of the malicious emails or our FaaS team detected and contained the attack early enough in the lifecycle before we observed any data targeting or theft. However, we surmise FIN7 can profit from compromised organizations in several ways. If the attackers are attempting to compromise persons involved in SEC filings due to their information access, they may ultimately be pursuing securities fraud or other investment abuse. Alternatively, if they are tailoring their social engineering to these individuals, but have other goals once they have established a foothold, they may intend to pursue one of many other fraud types.

Previous FIN7 operations deployed multiple point-of-sale malware families for the purpose of collecting and exfiltrating sensitive financial data. The use of the CARBANAK malware in FIN7 operations also provides limited evidence that these campaigns are linked to previously observed CARBANAK operations leading to fraudulent

banking transactions, ATM compromise, and other monetization schemes.

Community Protection Event

FireEye implemented a Community Protection Event – FaaS, Mandiant, Intelligence, and Products – to secure all clients affected by this campaign. In this instance, an incident detected by FaaS led to the deployment of additional detections by the FireEye Labs team after FireEye Labs Advanced Reverse Engineering quickly analyzed the malware. Detections were then quickly deployed to the suite of FireEye products.

The FireEye iSIGHT Intelligence MySIGHT Portal contains additional information based on our investigations of a variety of topics discussed in this post, including FIN7 and the POWERSOURCE and TEXTMATE malware. Click here for more information.