Notorious Cybercrime Gang, FIN7, Lands Malware in Law Firm Using Fake Legal Complaint Against Jack Daniels' Owner, Brown-Forman Inc.

esentire.com/security-advisories/notorious-cybercrime-gang-fin7-lands-malware-in-law-firm-using-fake-legal-complaint-against-jack-daniels-owner-brown-forman-inc

Despite multiple arrests and the conviction of several members of the notorious cybercrime gang, FIN7 [1][2] (a.k.a. Carbanak Group), the group continues to develop its business model and toolset throughout 2021 [3]. During the first week of June 2021, eSentire's Threat Response Unit (TRU) witnessed an opportunistic malspam campaign that was conducted by the FIN7 group. The criminal group used a fake legal complaint centering around Brown-Forman Inc. Brown-Forman is a large, U.S.-based wine and spirits company and the maker of the popular Jack Daniels whisky. (Figures 1 and 2). On June 10, external researchers observed a USPS mail delivery notification lure (Figure3). It was associated with the same infrastructure set as the legal complaint lure. Toward the end of June, a ProofPoint researcher documented a Windows 11 lure used to deliver JSSLoader.

One of the victims of the malicious legal complaint campaign was a law firm. The lure successfully bypassed the law firm's email filters, and it was not detected as suspicious by any of the firm's employees. eSentire's TRU team identified the malicious document through threat hunting activities.

The initial stage of the malware arrives as an Excel attachment, which downloads and executes a variant of the JSSLoader Remote Access Trojan (RAT). The variant has been reported as being used by the FIN7 group [3]. The malicious Excel document leverages Windows Management Instrumentation (WMI) to install the RAT. Once installed, JSSLoader provides the threat group with a backdoor to the victim's computer and the organization.

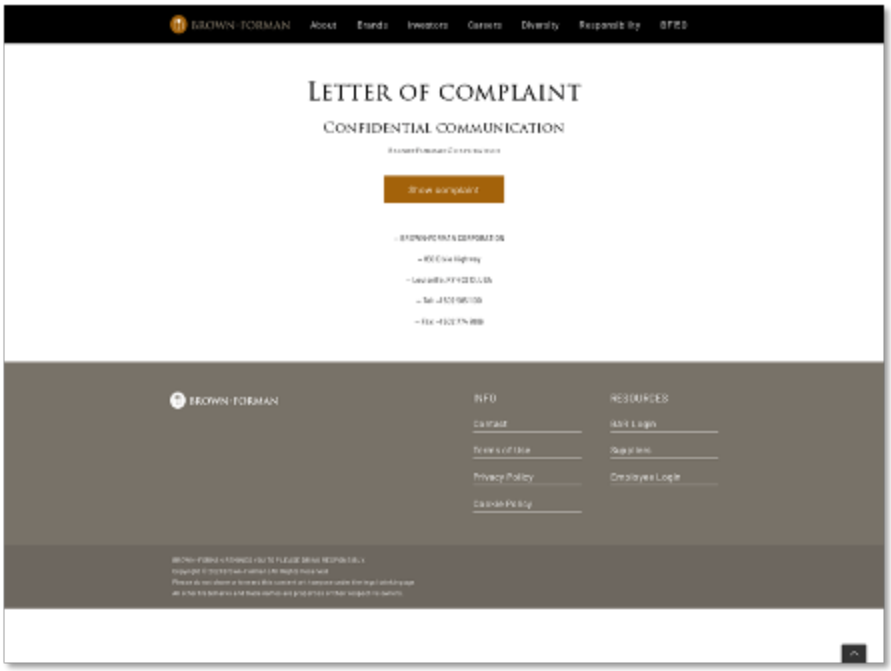

Figure 1: Brown-Forman Lookalike Landing Page (browm-forman[.]com)

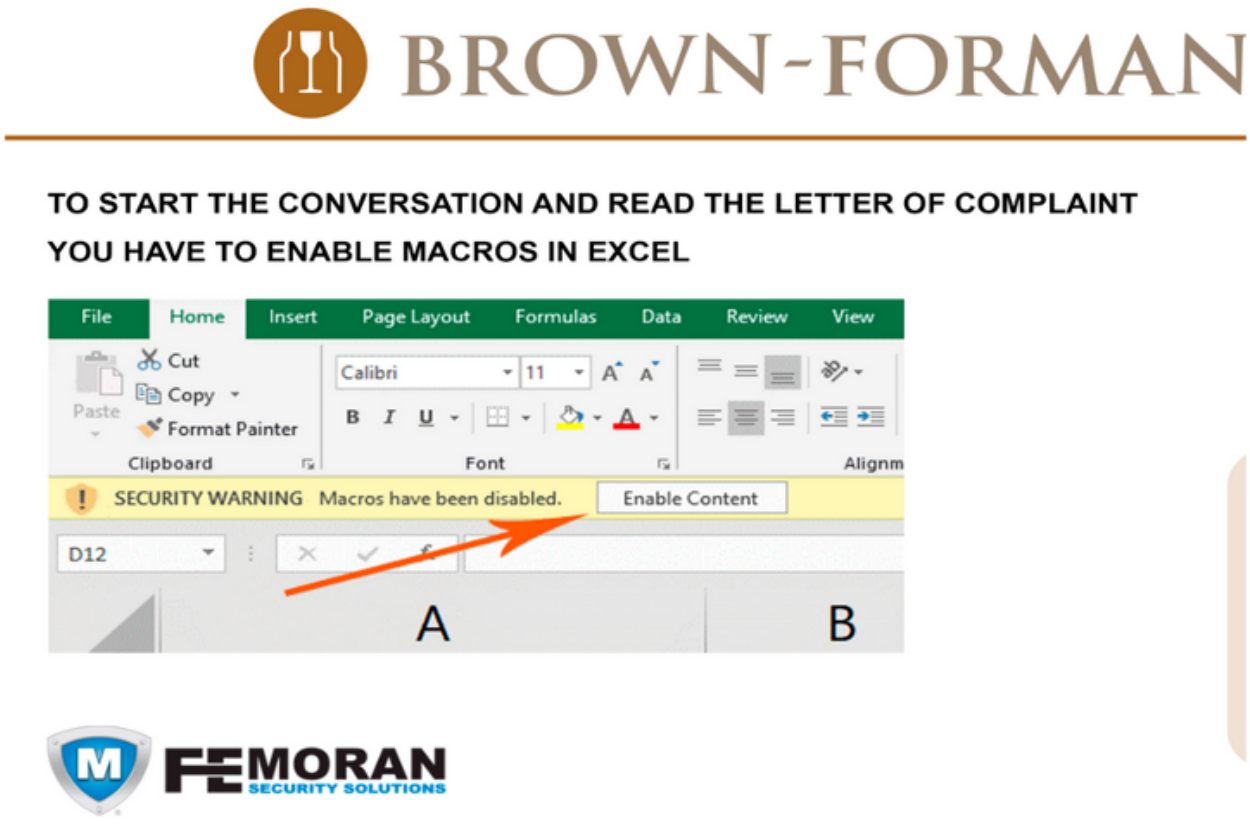

Figure 2: Legal Complaint lure observed by TRU on June 1, 2021 that led to an employee at a law firm downloading and executing a variant of JSSLoader.

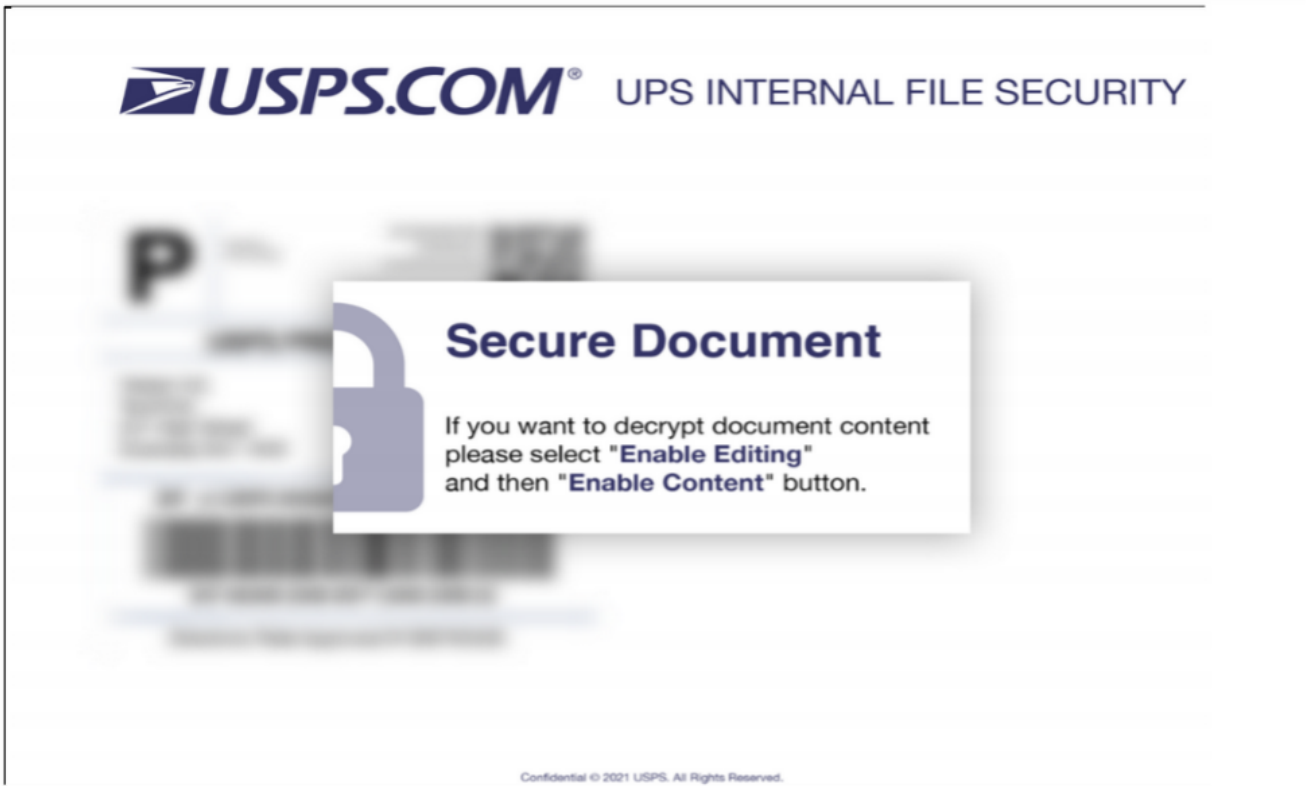

Figure 3: USPS lure associated with FIN7 infrastructure.

FIN7 Objectives

FIN7 is a financially motivated cybercrime group which gained notoriety for stealing millions of credit card numbers from businesses around the world. One security research team reported that the crime group stole more than a billion dollars between 2015 and 2018 from companies globally. U.S. federal law officials filed court documents on June 17, 2021 stating that FIN7 had more than 70 members, all assigned to various departments under the larger organization. The court documents went on to say that the FIN7 leaders would organize their personnel into different teams. These teams are tasked with creating malware, crafting phishing documents and collecting money from compromised victims. As for the U.S. victims, court officials stated that the group went after hundreds of U.S. companies infecting organizations ranging from the burrito chain Chipotle and the department store Saks Fifth Avenue. FIN7 is one of many cyber gangs observed participating in Magecart attacks [4]. Magecart is a consortium of malicious hacker groups who target online shopping cart systems, such as the Magento system, to steal customer payment card information.

FIN7 has also been associated with the Ryuk ransomware group[5]. In December 2020, security researchers at Trusec observed an attacker use the tools and techniques of FIN7 to gain a foothold into an enterprise. In a second attack against the company, almost six weeks later, that same foothold was used to launch Ryuk ransomware into the victim's environment. The Truesec researchers stated that this was the first instance where they had observed a combination of FIN7 tools and the RYUK ransomware. Until this incident, they said they had never seen FIN7 associated with ransomware attacks. The TRU has also never observed a connection between FIN7 and the Ryuk ransomware group. Truesec theorized "it was possible FIN7 simply sold the access to the Ryuk group, but it is probable that FIN7 and the Ryuk gang are more closely affiliated and may be part of the same organized crime network." [5]. No matter which theory is correct, this implies that few criminal organizations are out of scope for FIN7, since ransomware can often monetize intrusions regardless of the industry.

Similar conclusions can be drawn from the recent analysis on the victimology of the Avaddon ransomware group, which demonstrates a diverse set of victim targets, across business sectors and revenue volumes [6]. These observations are part of a trend of modern, financially motivated attacks which implement a threat model that is effective, regardless of an organization's industry. If FIN7 cannot make use of an organization they have compromised, they are likely to participate in the "initial access market," selling or trading access to the victim entity with another threat actor or threat group. Those threat actors are likely to be a ransomware group or its affiliates to monetize the access.

FIN7's Malicious Spam Campaign Using a Legal Lure Involving Brown-Forman Inc.

During this attack, the initial email arrives alleging a legal complaint for wine and spirits company, Brown-Forman, as observed by the TRU team, as well as other researchers [7]. Brown-Forman is one of the largest American-owned spirits and wine companies and among the top 10 largest global spirits companies.

Several researchers reported this lure, indicating that this was not a single incident, but most likely an opportunistic spam campaign. Corporate users might immediately suspect a random legal complaint, that arrives via email, from a large spirits and wine company. However, law firms deal with legal complaints across industry verticals regularly so the content would not be considered out of the ordinary. Thus, law firms may be more susceptible to this topic.

FIN7's Shifting Lures

On June 10, external researchers observed FIN7 using a USPS-themed email attachment[8]. The USPS lure is more generic and thus, more opportunistic in nature. And as mentioned previously, during the last week of June, a Proofpoint researcher saw a Windows 11 lure which led to the JSSLoader.

Whatever the specific intentions of FIN7, they appear to be actively adjusting their lures to maximize campaign success. For example, the legal complaint lure hit Internet users' email inboxes the first week of June, just one month before settlement claims were due for a class action suit against Brown-Forman regarding a ransomware breach the company suffered in August 2020 (Figure 5). The infamous REvil (Sodin) gang took credit for the ransomware attack. Although the company said they were able to disrupt the attack before their data could be encrypted, the REvil gang broadcasted on their blog/leak site that they had access to Brown-Forman's systems for over a month and stole a terabyte of their company data.

The fact that the TRU spotted FIN7 launching a malicious email campaign in June 2021, using the Brown-Forman legal complaint as a lure, and it was approximately one month before claim forms were due from victims (Figure 4.) is coincidental. Whether FIN7 is connected to the REvil (Sodinokibi) attack against Brown-Forman or whether they are simply capitalizing on public news regarding the case remains to be seen. In further examining potential connections between FIN7 and REvil, in August 2020 a Swiss security company promised to demonstrate connections between the two threat groups in a series of blog posts [9] but never provided sufficient evidence. It appears that they were left waiting for confirmation from the ransomware victims [10][11]. Regardless, what we do know for sure is that cybercriminals use well-timed lures and try to predict the susceptibility of a theme for their threat campaigns, and they will use lures built around social trends [12], global crises [13] and routine events [14].

Operating Infrastructure Tying FIN7's Malicious Email Lures Together

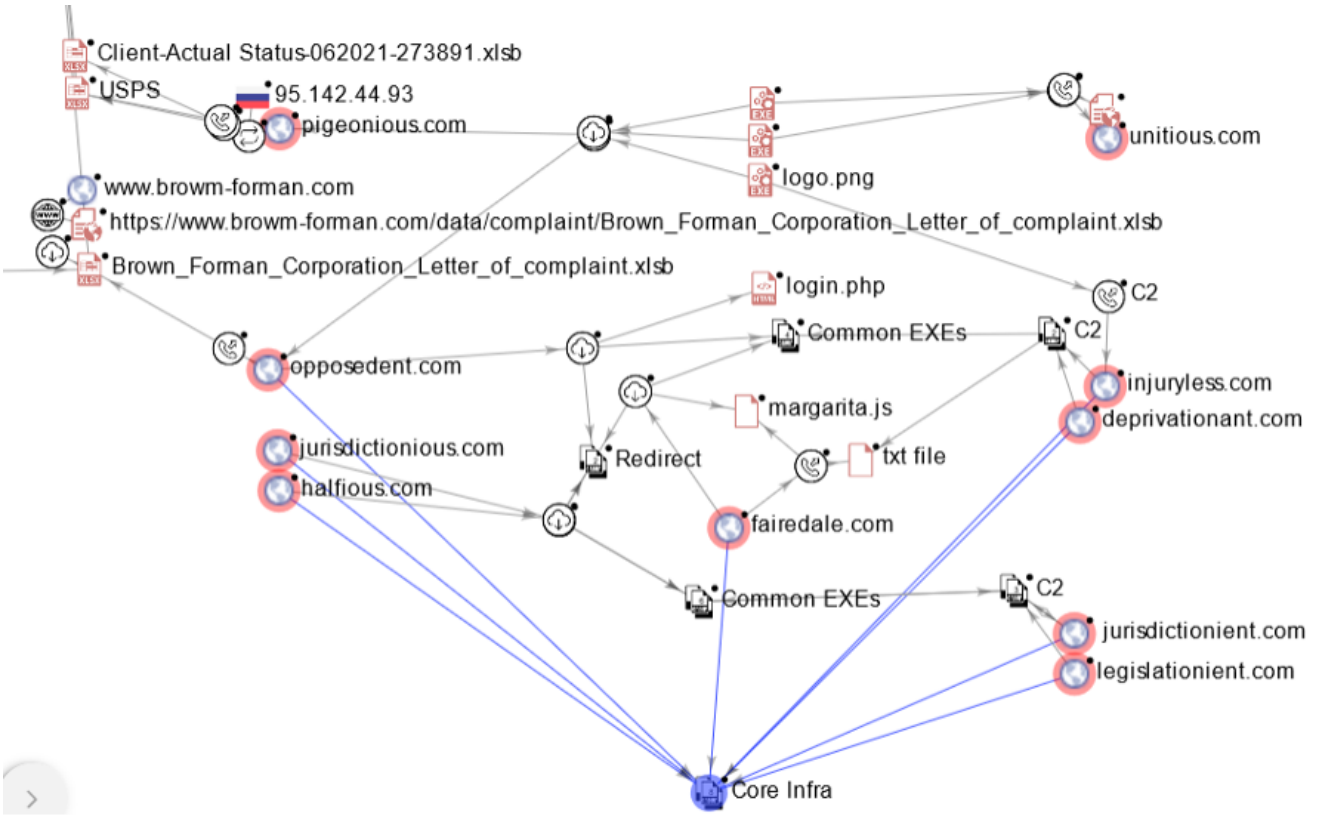

Figure 4: Infrastructure and malware used in the latest FIN7 campaigns

The most recent lures associated with FIN7 show connections in their supporting infrastructure. (Figure 3). The servers are observed performing three distinct functions. The primary download server, observed by TRU, was **browm-forman[.]com** which served as a starting point. First stage payloads are fetched from intermediate servers, such as **opposedent[.]com**, **jurisdictionious[.]com**, **halfious[.]com**, **pigeonious[.]com.** It is unclear what role **fairedale[.]com** plays, though given its position in redirection and JavaScript management, its role may be to test whether a visiting computer is a susceptible victim (and not, for example, a security researcher) before redirecting the user to the malicious payload. The command- and- control domains(C2s), for the first payload, appear to be **unitious[.]com**, **injuryless[.]com**, **deprivationant[.]com**, **jurisdictionient[.]com**, and **legislationient[.]com**. There is no apparent relationship with the infrastructure reported by previous research.

Another curious finding is that some infrastructure was not observed by TRU for months following domain registration. In the incident which leveraged the Brown-Forman lure, the landing page for the lookalike domain (browm-forman[.]com) was registered 2021-03-11, but not observed until June. VirusTotal submissions for this domain line up with the June observations. This gap between registration and operational use might have been to thwart website reputation filters which utilize domain age as input. This months-long time delta does not appear to carry over to C2 domains used by the weaponized Excel document and subsequent JSSLoader payload. Both contacted domains registered May 27th, a week prior to in- the-wild use.

Finally, TRU observed registration of a new lookalike domain (brown-formam[.]com) on June 9th. While in-the-wild use has not been observed, the registration and TLS certificate patterns match the previous landing page. We assess this domain will replace the prior one given that it has been exposed publicly.

Key Takeaways

The following key takeaways have been summarized by Spence Hutchinson, Manager of Threat Intelligence, eSentire:

- Despite several key members of the FIN7 group being incarcerated, the gang continues to mount successful threat campaigns, indicating that they have numerous members and extensive recruitment efforts.
- Notably for the Brown-Forman case, FIN7 threat actors registered the infrastructure months before the TRU saw it in action. Either the attackers were using it for months before eSentire saw the activity, or they weaponized it after a period of time to evade email filtering by newly registered domains. If that is the case, this shows a degree of planning and sophistication on the part of FIN7.

- The FIN7 group is very experienced. They have been involved in financial cybercrime for a long time, and they know how to use social engineering techniques that will lure computer users. Their success in compromising companies and individuals, via email, reiterates the importance of continually educating one's employees and partners to be on the lookout for malicious email campaigns.
- FIN7's regular shifting of infrastructure and lures is a testament to their knowledge on how to evade detection by security professionals.
- It is plausible that proficient financial cybercrime groups, such as FIN7, are providing initial access to seasoned ransomware groups, such as REvil (Sodinokibi), Ryuk, etc. as a way to monetize their access.

If you're not currently engaged with a Managed Detection and Response provider, we highly recommend you partner with us for security services in order to disrupt threats before they impact your business.

Want to learn more about how we protect legal firms globally? Connect with an eSentire Security Specialist.

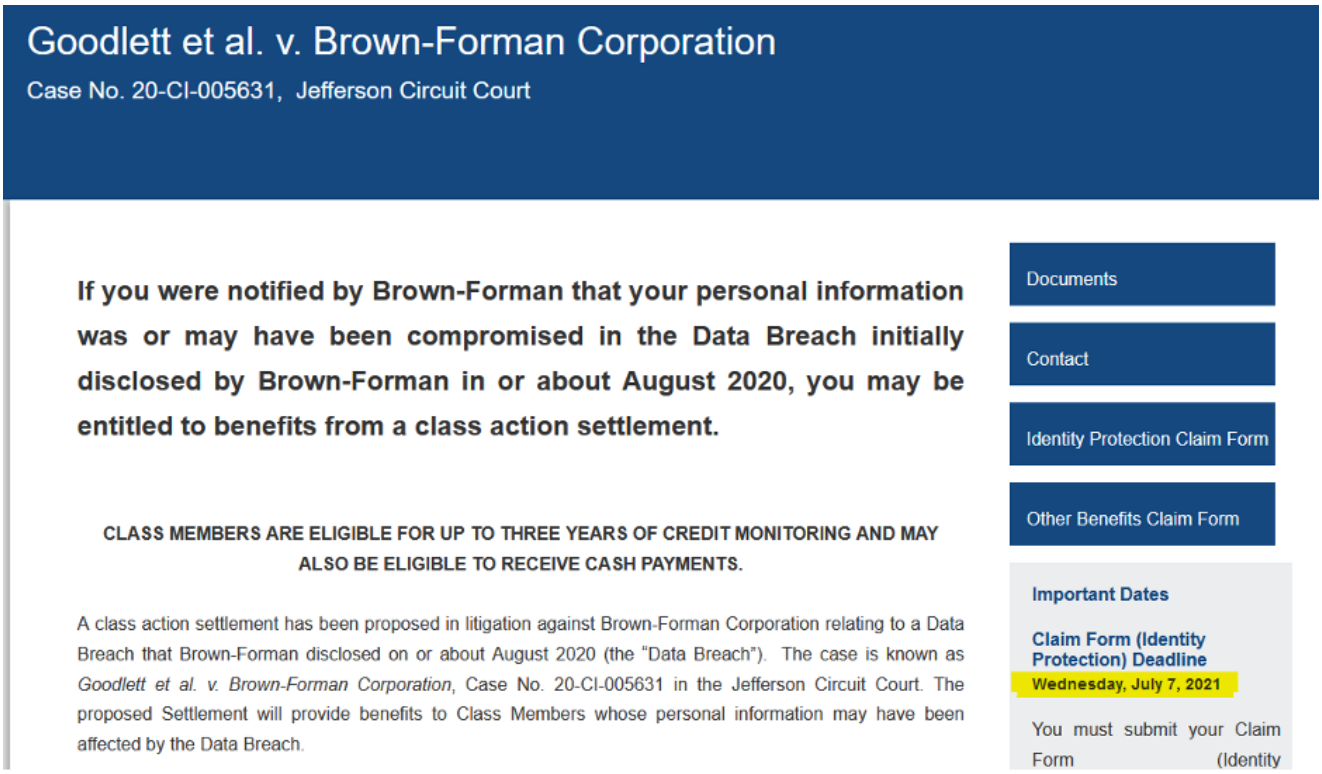

Figure 5: Brown-Forman Class Action Settlement. Note the Deadline aligns with the timing of the active campaigns by FIN7 using the Brown-Forman complaint lure.

Appendix of Domains Registered by the FIN7 Threat Group

Value	Creation Date

amusient[.]com	2021-06-29
brown-formam[.]com	2021-06-09
spectrummel[.]com	2021-06-08
pigeonious[.]com	2021-06-08
richesk[.]com	2021-06-07
unitious[.]com	2021-06-02
indulgology[.]com	2021-06-02
baradical[.]com	2021-05-31
deprivationant[.]com	2021-05-27
dullism[.]com	2021-05-27
injuryless[.]com	2021-05-27
opposedent[.]com	2021-05-27
capermission[.]com	2021-05-24
hemispherious[.]com	2021-05-17
jurisdictionient[.]com	2021-05-17
cannstattraction[.]com	2021-05-13
myofibrilliance[.]com	2021-05-12
migrationable[.]com	2021-04-15

shareholderery[.]com	2021-04-07
eyebrowaholic[.]com	2021-03-20
offspringance[.]com	2021-03-19
chyprediction[.]com	2021-03-17
browm-forman[.]com	2021-03-11
bank4america[.]com	2021-03-10
associationable[.]com	2021-03-09
discriminatoid[.]com	2021-03-09
shareholderma[.]com	2021-02-25
conglomeratoid[.]com	2021-02-11
domestickum[.]com	2021-01-26
fidespair[.]com	2021-01-22
executivance[.]com	2021-01-21
keywordsance[.]com	2021-01-20
cooperativology[.]com	2020-12-17
countrysidable[.]com	2020-12-14
bypassociation[.]com	2020-12-14
battlefieldant[.]com	2020-12-14

nonremittalable[.]com 2020-12-10

[1] https://www.cyberscoop.com/fin7-hacking-arrest-financial/
[2] https://www.justice.gov/opa/pr/three-members-notorious-international-cybercrime-group-fin7-custody-role-attacking-over-100
[3] https://blog.morphisec.com/the-evolution-of-the-fin7-jssloader
[4] https://socprime.com/news/fin7-group-involved-in-skimming-attacks/
[5] https://blog.truesec.com/2020/12/22/collaboration-between-fin7-and-the-ryuk-group-a-truesec-investigation/
[6] https://www.advanced-intel.com/post/the-rise-demise-of-multi-million-ransomware-business-empire
[7] https://mobile.twitter.com/Arkbird_SOLG/status/1400845444889120783
[8] https://twitter.com/ShadowChasing1/status/1403150596849295362
[9] https://threatintel.blog/OPBlueRaven-Part1/
[10] “Before disclosing the relationship between Fin7 and REvil groups, we are trying to reach the ransomware victims.”
[11] https://threatintel.blog/OPBlueRaven-Part2/
[12] eSentire | Cybercriminals Use Malicious Google Ads to Lure Computer…
[13] https://www.proofpoint.com/us/blog/threat-insight/attackers-use-covid-19-vaccine-lures-spread-malware-phishing-and-bec
[14] https://cofense.com/bah-humbug-5-recent-holiday-phishing-samples-need-watch/