T.C.

BİLGİ ÜNİVERSİTESİ

BİLİŞİM VE TEKNOLOJİ HUKUKU YÜKSEK LİSANS DERSİ ÖDEVİ

HACKER GRUBU ARAŞTIRMASI: FIN7

Hazırlayan: Şeymanur Sağınç

Öğrenci No:125691018

A. Giriş

Teknolojinin gelişmesi, internetin artık hayatımızın her yerinde yer alması avantajların yanında dezavantajları ve riskleri de getirmektedir. Bu riskleri oluşturanların başında hacker grupları gelmektedir. Özellikle olumsuz faaliyetlerde bulunan hacker gruplarının meydana getirdiği zararlar günden güne artarak devam etmektedir. Son yılların en gelişmiş siber suç örgütlerinden biri olan FIN7 de zararlı faaliyetlerde bulunan hacker grupları arasında yer almakta olup, işbu ödevde FIN7'nin yapısı, faaliyetleri, eylem türleri ve bu eylemler karşısında zarara uğrayan kişiler ile meydana gelen hukuki sorunlar ele alınmıştır.

B. FIN7'nin Yapısı ve Faaliyetleri

FIN7, 2013 yılından bu yana faaliyet gösteren bir hacker grubudur. Amerika Birleşik Devletlerinde (ABD) finansal hizmetler, yazılım, bulut hizmetleri, medya, perakende gibi birçok sektörü hedef alan FIN7, "Combi Security" adında paravan bir şirket kurmak suretiyle birçok faaliyetini yerine getirmiştir.[1]

FIN7'nin faaliyetlerinin daha çok Rusya ve Ukrayna ile bağlantılı olduğu söylense de hangi devlete bağlı oldukları belirsizliğini sürdürmektedir. Aynı şekilde üye sayısı da belirsiz olup, yasadışı faaliyetlerini gizlenmesi ve üye toplaması için Combi Security gibi paravan şirketler aracılığı ile kendilerini kamufle etmişlerdir.[2]

FIN7, siber saldırılarını genellikle oltalama saldırısı (phishing), fidye virüsleri ve sosyal mühendislik aracılığı ile yapmaktadır.[3]

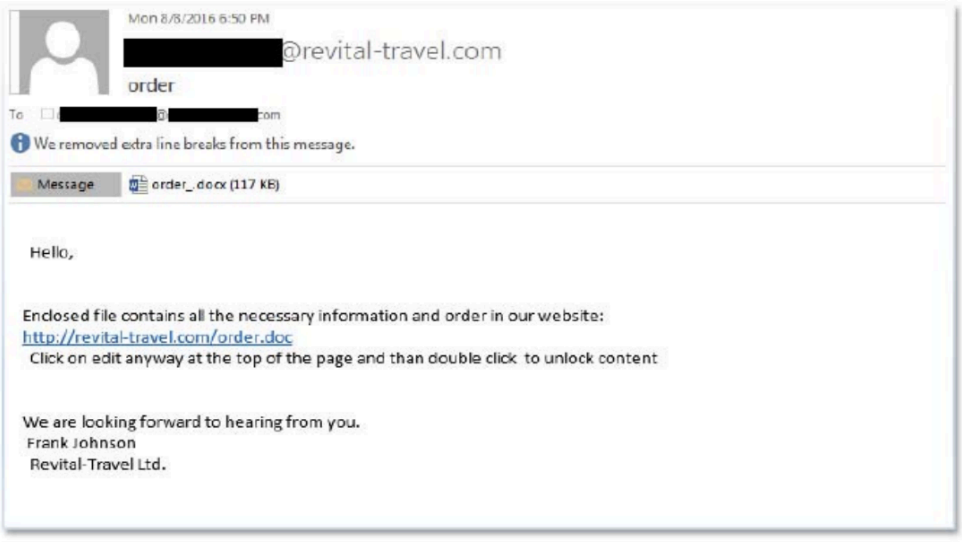
1. Oltalama Saldırısı (Phishing) ve Zıpkınlama Saldırı (Spear Phishing)

[1] MITRE ATT&CK; "FIN7 (G0046)", Versiyon 4.1, https://attack.mitre.org/groups/G0046/
[2] HUNTRESS; "FIN7 Cybercrime Group - Tactics, Tools, and Threat Insights", Huntress Threat Library, https://www.huntress.com/threat-library/threat-actors/fin7
[3] GREGORY, Jennifer; "Hacker Group FIN7 Is Selling EDR Evasion Tools to Other Cyber Criminals", IBM Think, 5 Ağustos 2024,https://www.ibm.com/think/news/hacker-group-fin7-selling-edr-evasion-tools-other-cyber-criminals

Oltalama saldırıları; genel olarak kurbanların e-posta hesaplarına hediye, indirim veya benzeri cezbedici sahte iletiler gönderilerek parola, kimlik bilgisi veyahut benzeri hassas verilerin çalınmasına sebep olan saldırı türüdür.[4]

FIN7 hem oltalama saldırılarını hem de zıpkınlama saldırısı (spear phishing) denilen belirli bireyleri veya kuruluşları manipüle etmek için titizlikle tasarlanan, son derece hedefe odaklanan saldırıları kullanmaktadır. Bu saldırı türünde genel ileti içeriklerinin aksine kişiselleştirilmiş iletiler ile saldırının gerçekmiş gibi görünmesi sağlanarak hedefin kötü amaçlı bağlantıya tıklaması, eklentiyi indirmesi ve hatta hassas bilgileri paylaşması sağlanır. Özetle oltalama, "rastgele, belki tutar" iken; zıpkınlama saldırıları, sosyal medya, şirket web siteleri veya sızdırılmış verilerden elde edilen bilgiler kullanılarak belirli bir kişi veya kuruluşu hedef alan son derece kişiselleştirilmiş bir saldırıdır.[5]

FIN7'nin de en çok kullandığı bu teknikler olup, ilk teması sağlamak için kişiye özel zıpkınlama saldırıları düzenlemek suretiyle özel tasarlanmış kampanyalar aracılığı ile saldırılarını yapmaktadır. FIN7'nin saldırılarından örnek bir mail aşağıda yer almaktadır.[6] Bu e-postayı gönderdikten sonra arama yapmak suretiyle e-postalarını doğrulanmış gibi göstermektedirler.



[4] İstanbul Bilgi Üniversitesi; "Phishing Saldırısı", 2026, https://it.bilgi.edu.tr/tr/guvenlik/phishing/
[5] HUNTRESS; "What is Spear Phishing?", Huntress Cybersecurity 101, https://www.huntress.com/cybersecurity-101/topic/what-is-spear-phishing
[6] United States Department of Justice, U.S. Attorney's Office, Western District of Washington; "How FIN7 Attacked and Stole Data", 2018, https://www.justice.gov/usao-wdwa/press-release/file/1084436/dl?inline

2. Fidye Virüsleri

En büyük tehditlerden olan fidye virüsleri (ransomware), zararlı bir yazılım olup, sistemi kilitleyen ve tüm verilere erişimi engelleyen kötü amaçlı bir yazılım türüdür.

FIN7; Carbanak, NetSupport RAT, POWERTRASH ve DICELOADER gibi kendine özgü zararlı yazılımlar geliştirip kullanmaktadır. Bu yöntemleri erişim düzeylerini yükseltmek, ağlar arasında geçiş yapmak ve POS sistemlerini hedef almak için kullanmaktadırlar. Son zamanlarda FIN7, fidye yazılımı faaliyetlerine yönelerek veri hırsızlığı ile fidye taleplerini birleştirip mali şantajın etkisini de artırmaya başlamışlardır.[7] Ancak fidyeyi ödemenin de beraberinde çeşitli hukuki sorunları getirdiği göz önüne alınmalıdır. Ayrıca fidye ödemeleri yapıldıkça saldırıya açık hâle de gelinebilecektir. Öte yandan uluslararası terör finansmanı için de fidye toplanabileceğinden söz konusu fidyeyi ödeyenin hukuki sorumluluğu da gündeme gelebilecektir.

3. Sosyal Mühendislik

FIN7'nin en çok kullandığı yöntemlerden olan sosyal mühendislik; saldırganların hedef kişiyi kendi adlarına belirli bir eylemi gerçekleştirmeye yönlendirmek amacıyla güvenilir bir kişi ya da kuruluşu taklit eden bir manipülasyon yöntemidir. Saldırganlar, hedeflerle iletişim kurarken yönetici, iş arkadaşı veya üçüncü taraf tedarikçi gibi bilinen bir kimliği taklit edebilmektedirler. Böylece oluşturulan sahte güven ilişkisi, saldırganın nihai hedeflerine ulaşmak için kullanılmaktadır.[8]

C. FIN7'nin Eylemleri ve Eylem Türleri

Amerika Birleşik Devletleri Başsavcılığı'na göre, 2015 ile 2018 yılları arasında FIN7, Chipotle Mexican Grill, Chili's, Arby's, Red Robin ve Jason's Deli de dahil olmak üzere 100'den fazla ABD şirketinin sistemlerine sızmış, 3.600'den fazla ayrı işletme lokasyonunda bulunan 6.500'den

[7] HUNTRESS; "FIN7 Cybercrime Group - Tactics, Tools, and Threat Insights", Huntress Threat Library, https://www.huntress.com/threat-library/threat-actors/fin7
[8] MITRE ATT&CK; "Social Engineering: Impersonation (T1684.001)", https://attack.mitre.org/techniques/T1684/001/

fazla POS cihazından 15 milyondan fazla müşteri kart bilgisini ele geçirmiştir. Sadece 2020-2021 yılı içerisinde gerçekleştirdikleri faaliyetler aşağıdaki tabloda yer almaktadır.[9]

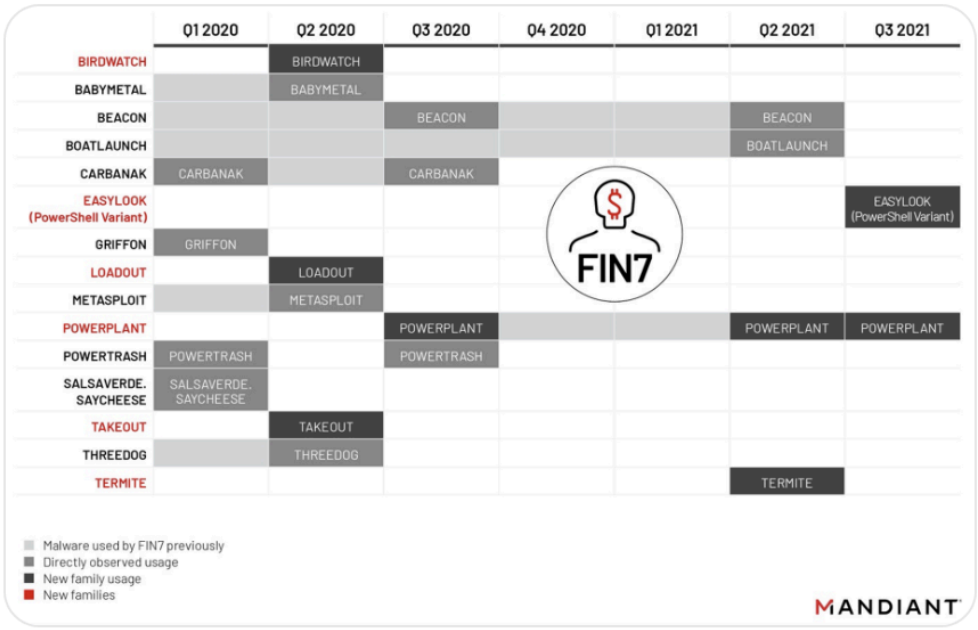


Figure 1: FIN7 Activity in 2020-2021

D. Mağdurlar

FIN7'nin dikkat çeken mağdurları arasında Chipotle, Chili's, Arby's, Jason's Deli ve Red Robin gibi zincirler restoranlar yer alıyor. Restoran sektörünün ötesinde, mağdurlar küresel olarak perakende, gıda zincirleri, POS sahipleri ve konaklama sektörlerini de kapsamakta olup, saldırgan grup özellikle Amerika Birleşik Devletleri'ndeki kuruluşlara odaklanmaktadır.[10]

E. Hukuki Sorunlar

FIN7'nin eylemleri itibariyle doğurduğu birçok hukuki sorun bulunmakta olup, bunlardan ilki fidye ödemesidir. FIN7'nin talep ettiği/edeceği fidyenin kimin tarafından hangi amaçla

[9] ABDO, Bryce; WORK, Zander; TEACA, Ioana; McKEAGUE, Brendan; "FIN7 Power Hour: Adversary Archaeology and the Evolution of FIN7", Mandiant / Google Cloud Blog, 4 Nisan 2022, https://cloud.google.com/blog/topics/threat-intelligence/evolution-of-fin7

[10] HUNTRESS; "FIN7 Cybercrime Group - Tactics, Tools, and Threat Insights", Huntress Threat Library, https://www.huntress.com/threat-library/threat-actors/fin7

kullanılacağı belirsiz olduğundan, söz konusu fidyenin terörizmin finansmanı için kullanılması hâlinde ödemeyi yapanın da sorumluluğu gündeme gelebilecektir. Başka bir hukuki sorun ise yetkisiz bir şekilde ele geçirilen verilerdir. Oltalama, sosyal mühendislik gibi yollarla hukuka aykırı bir şekilde ele geçirilen kişisel verilerin ve POS sistemlerinin ele geçirilmesi suretiyle yetkisiz bir şekilde erişilen finansal verilerin kullanılması sebebiyle veri hukuku ve siber güvenlik hukuku bakımından çeşitli hukuki sorunlar doğacaktır. Söz konusu saldırgan grubunun hangi ülke mensupları tarafından kurulduğunun net bir şekilde belirlenememesi sebebiyle de uygulanacak hukuk bakımından belirsizlik doğacaktır. Öte yandan Türk hukuku bakımından Cumhurbaşkanlığı Dijital Dönüşüm Ofisi'nin Bilgi ve İletişim Güvenliği Genelgesi kapsamında özellikle üretici firmalardan alınan arka kapı açıklığı taahhütnamesine benzer bir taahhüdün ilgili ülkelerde bulunması hâlinde bu taahhüde aykırılık da söz konusu olabilecektir. Son olarak hizmet sürekliliğin etkilenmesi sebebiyle de bilgi güvenliği hükümleri ve tüketicilerin mal ve hizmete erişiminin kesintiye uğraması sebebiyle de bilgi güvenliği hukuk kuralları ve tüketicinin korunması hükümleri uyarınca sorumluluk meydana gelebilecektir.

F. Sonuç

Yıllardır saldırılarda bulunan FIN7, saldırı çeşitliliği ile bilinen bir hacker grubu olup, her ne kadar ana kuruluş ülkesi bilinmese de birden fazla ülkede saldırı gerçekleştirmiş ve birçok kişi ve kurumu zarara uğratmıştır. Grubun bazı üyelerine yönelik soruşturmalar devam ederken, bir kısmına yönelik cezalar verilmeye başlanmıştır. Ancak henüz grubun faaliyetlerinin sona erdiğine dair net bir bilgi bulunmamaktadır. Günümüz itibariyle her ne kadar önemler geliştiyse de saldırı yöntemleri ve saldırganlar da bu hızda çoğalmaya devam etmektedir. Dolayısıyla güncel yazılımların kullanılması, çalışanlarla bu kapsamda eğitimlerin verilmesi, caydırıcı faaliyetlerin yürütülmesinin önemi de artmakta olup, tüm kurum ve kuruluşların bu kapsamda gerekli önlemleri alması gerekmektedir.

G. Kaynakça

- ABDO, Bryce; WORK, Zander; TEACA, Ioana; McKEAGUE, Brendan; "FIN7 Power Hour: Adversary Archaeology and the Evolution of FIN7", Mandiant / Google Cloud Blog, 4 Nisan 2022, https://cloud.google.com/blog/topics/threat-intelligence/evolution-of-fin7

- GREGORY, Jennifer; "Hacker Group FIN7 Is Selling EDR Evasion Tools to Other Cyber Criminals", IBM Think, 5 Ağustos 2024, https://www.ibm.com/think/news/hacker-group-fin7-selling-edr-evasion-tools-other-cyber-criminals

- HUNTRESS; "FIN7 Cybercrime Group - Tactics, Tools, and Threat Insights", Huntress Threat Library, https://www.huntress.com/threat-library/threat-actors/fin7

- HUNTRESS; "What is Spear Phishing?", Huntress Cybersecurity 101, https://www.huntress.com/cybersecurity-101/topic/what-is-spear-phishing

- İstanbul Bilgi Üniversitesi; "Phishing Saldırısı", 2026, https://it.bilgi.edu.tr/tr/guvenlik/phishing/

- KAYA, Mehmet Bedii; *Siber Güvenlik Hukuku*, 2026.

- United States Department of Justice, U.S. Attorney's Office, Western District of Washington; "How FIN7 Attacked and Stole Data", 2018, https://www.justice.gov/usao-wdwa/press-release/file/1084436/dl?inline

- United States Department of Justice, U.S. Attorney's Office, Western District of Washington; "Three Members of Notorious International Cybercrime Group 'Fin7' in Custody for Role in Attacking Over 100 U.S. Companies", 1 Ağustos 2018, https://www.justice.gov/usao-wdwa/pr/three-members-notorious-international-cybercrime-group-fin7-custody-role-attacking-over