ECHO
CYBER THREAT INTELLIGENCE

Son 6 Ayda Havacılık Sektörünü Hedef Alan APT Grupları

İçindekiler

Yönetici Özeti

Bu yönetici özeti, havacılık sektörünü hedef alan siber saldırıların önemini ve etkilerini ele almaktadır. Son yıllarda havacılık sektöründe gerçekleşen siber saldırılar, işletmeler için büyük bir tehdit haline gelmiştir. Bu saldırılar, havayolu şirketlerinin veri tabanları, rezervasyon sistemleri, uçuş sistemleri ve hatta hava trafik kontrol sistemleri gibi kritik altyapıları hedeflemektedir.

Havacılık sektörü, siber saldırılara karşı hassas bir hedef konumunda bulunmaktadır. Sektördeki kritik altyapıların ve verilerin korunması, operasyonel süreklilik ve yolcu güvenliği açısından büyük bir önem taşımaktadır. Siber saldırılar, veri hırsızlığı, operasyonel aksamalar, uçuş iptalleri ve hatta uçuş güvenliğinin tehlikeye atılması gibi ciddi sonuçlara yol açabilir.

Son yıllarda havacılık sektöründe gerçekleşen siber saldırıların sayısında bir artış gözlemlenmektedir. Eurocontrol raporlarından çıkarıldığı üzere siber saldırılar son dört yılda yıllık bazda en az %530 daha fazla gerçekleşiyor. Bir dikkat çeken durum ise, saldırı türlerinin %61'inde ciddi bir yoğunlaşma oluşmasıdır. Bu durum çok yönlü güvenlik önlemleri almayı gerektirmektedir.

Siber saldırganlar, sürekli olarak gelişen teknikler ve taktikler kullanarak güvenlik önlemlerini aşmayı hedeflemektedir. Saldırıların arkasında farklı motivasyonlar bulunmaktadır, bunlar arasında mali kazanç sağlama, ulusal güvenlik tehdidi, casusluk faaliyetleri veya siber saldırı yeteneklerini sergileme gibi amaçlar yer almaktadır.

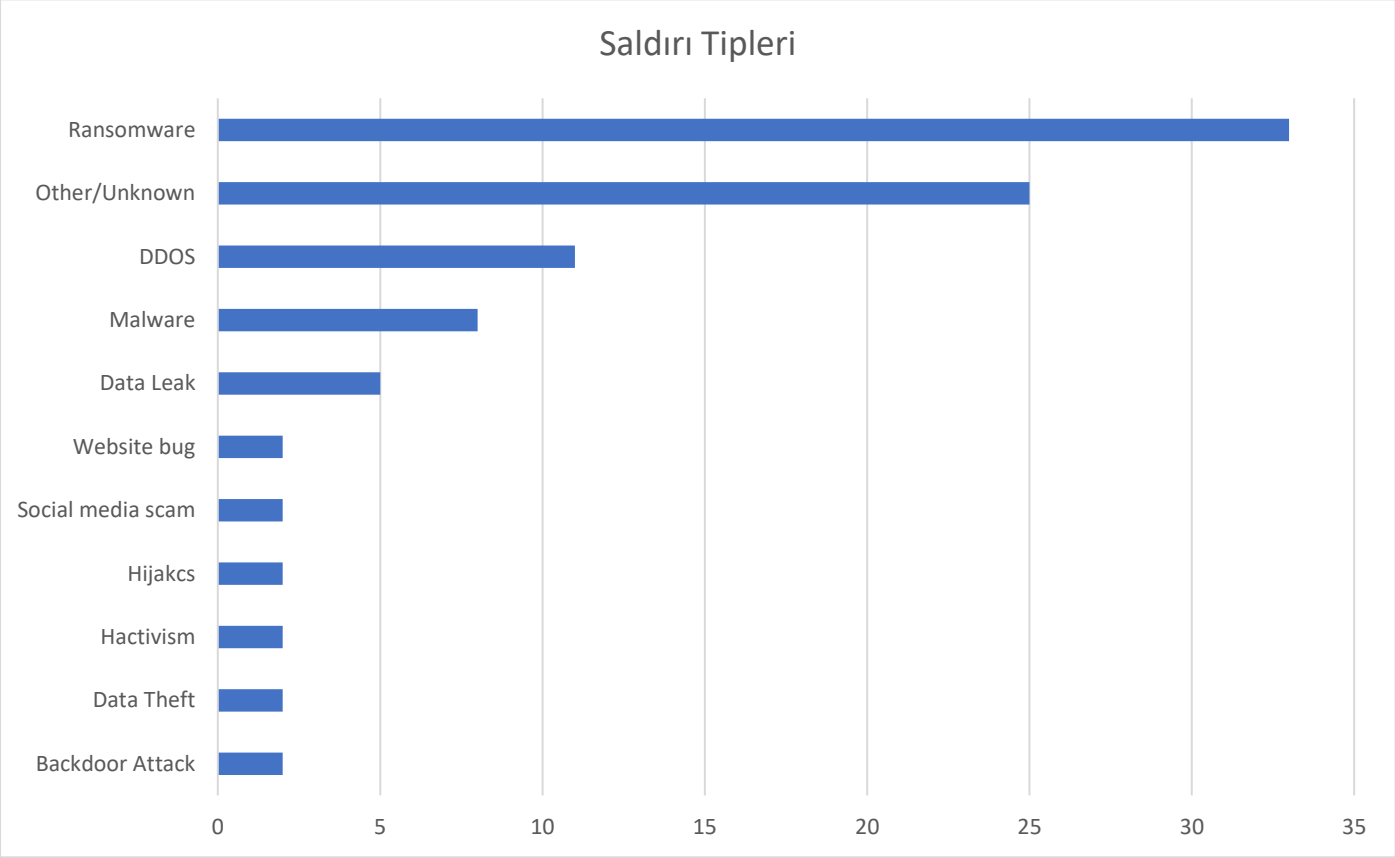
Havacılık sektörü, siber güvenlik konusunda sürekli olarak güncel kalması gereken bir alandır. Gelecekteki tehditlerin önlenmesi için sektör, güvenlik politikalarını sürekli gözden geçirmeli, personel eğitimine yatırım yapmalı ve teknolojik gelişmeleri yakından takip etmelidir.

Bu rapor, havacılık sektöründeki yöneticilerin, siber saldırı tehditlerine karşı bilinçlenmelerine ve gerekli önlemleri alarak şirketlerini korumalarına yardımcı olmayı amaçlamaktadır.

Havacılık Sektöründe Siber Tehditler

Son yıllarda, hızla gelişen teknolojiyle birlikte siber saldırılar giderek artan bir tehdit haline gelmiştir. Bu tehditler, hemen hemen her sektörü etkilese de havacılık sektörü gibi kritik altyapıları ve hassas bilgileri içeren sektörler özellikle hedef haline gelmektedir. Son altı ay içinde havacılık sektörüne yönelik gerçekleşen siber saldırılar, bu tehlikenin boyutlarını gözler önüne sermektedir.

Son altı ayda, havacılık sektöründe gerçekleşen siber saldırılar giderek artan bir endişe kaynağı haline gelmiştir. Önceden düşünülenden daha sofistike ve karmaşık hale gelen saldırılar, sektörün savunma mekanizmalarını zorlamış ve dikkatleri siber güvenliğe daha da yoğunlaştırmıştır. Bu saldırılar, farklı amaçlarla gerçekleştirilebilir. Örneğin, finansal kazanç elde etmek için hava taşımacılığından yararlanabilir, ulusal güvenliği tehlikeye atabilir veya itibar zararına yol açabilir.



Grafik 1 Saldırı Tipleri

Havacılık sektöründe gerçekleşen siber saldırıların etkileri de oldukça ciddi olabilir. Örneğin, hava trafik kontrol sistemlerine yapılan bir saldırı, uçakların seyrüseferinde aksamalara, kaos ortamlarına ve hatta potansiyel kazalara yol açabilir. Havayollarının müşteri bilgilerinin çalınması, kimlik hırsızlığı ve dolandırıcılık gibi sonuçlara yol açabilir. Ayrıca, uçak üreticileri veya diğer havacılık şirketlerine yapılan siber saldırılar, ticari sırların çalınması ve rekabet avantajının kaybedilmesi gibi ciddi ekonomik sonuçlar doğurabilir.

Bu rapor, son altı ay içinde havacılık sektörüne yönelik gerçekleşen siber saldırıları inceleyerek, bu tehdidin büyüklüğünü anlamayı ve sektörün gelecekteki güvenlik önlemlerini değerlendirmeyi amaçlamaktadır. Ayrıca, bu saldırıların ardındaki motivasyonları, saldırı türlerini ve sektörün bu tehditlere karşı mücadele etmek için aldığı önlemleri ele alacağız.

Havacılık sektörü, siber güvenlik açısından sürekli bir tehdit altında olmayı sürdürecektir. Ancak, bu alanda yapılan araştırmalar ve teknolojik gelişmeler, havacılık endüstrisinin siber saldırılara karşı daha dirençli hale gelmesini sağlayabilir. Bu rapor, havacılık sektöründe siber güvenlik konusundaki bilincin arttırılmasına ve önleyici önlemlerin güçlendirilmesine katkıda bulunmayı hedeflemektedir.

Yılın İlk Yarısında Yaşanan Saldırı ve Olaylar

Aer Lingus

Fidye yazılımı saldırısında 5.000 Aer Lingus personelinin verileri çalındı. MOVEit Transfer yazılımını ele geçirmenin bir yolunu bulduğunu ortaya çıkardı. Saldırının, endüstriyel kuruluşlara fidye yazılımı saldırılarıyla şantaj yapmasıyla tanınan Clop olarak bilinen üretken bir Rus siber suç çetesi tarafından düzenlendiği tespit edildi.

US Airlines

10 Ocak 2023 tarihinde yaşanan bu saldırı, saldırganlar tarafından US Airlines'a ait uçuşları iptal edip erteleyebilecek ve havayolu çalışanları için fiziksel kimlik kartı çıkarabileceklerini Uçuşa Yasak Listeyi ele geçirdiğini iddia etti.

Eurocontrol

Avrupa hava trafik kontrolü, web sitesinin Rusya yanlısı bilgisayar korsanları tarafından "saldırı altında" olduğunu doğruladı. Eurocontrol web sitesinin 19 Nisan'dan beri "saldırı altında" olduğunu doğruladı ve kesintinin sorumluluğunu "Rus yanlısı bilgisayar korsanlarının" üstlendiğini söyledi.

Scandinavian Airlines

İskandinav havayolu, bir siber saldırıya uğradığını söyledi ve müşterilerini uygulamasını kullanmaktan kaçınmaya çağırdı. Kuruma ait web sitesine ve uygulamasına yapılan saldırılar neticesinde müşteri bilgileri sızdırıldığı duyuruldu.

Colombia

10 Ocak 2023 tarihinde yaşanan bu saldırı, saldırganlar tarafından US Airlines'a ait uçuşları iptal edip erteleyebilecek ve havayolu çalışanları için fiziksel kimlik kartı çıkarabileceklerini Uçuşa Yasak Listeyi ele geçirdiğini iddia etti.

Safiran Airport

18 Haziran 2023 tarihinde "Hooshyaran-e Vatan" adlı bir hacker grubu, Safiran Airport Services veritabanı bilgilerini sızdırıldığı iddia etmektedir. Sızdırılan örnek veride, çeşitli e-postaları ve faturaları içermektedir.

British Air

18 Haziran 2023 tarihinde "Hooshyaran-e Vatan" adlı bir hacker grubu, Safiran Airport Services veritabanı bilgilerini sızdırıldığı iddia etmektedir. Sızdırılan örnek veride, çeşitli e-postaları ve faturaları içermektedir.

.

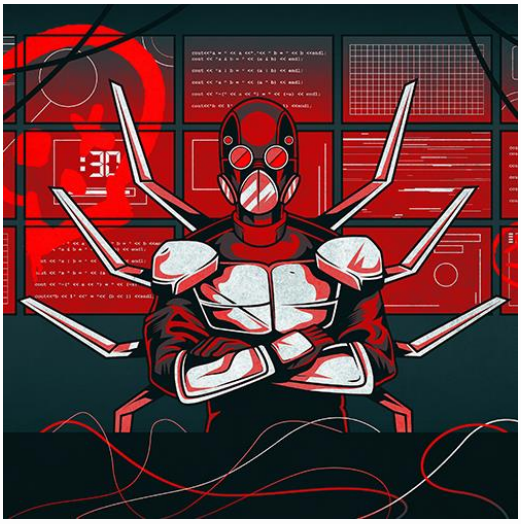
Kenya Airport Authority Medusa Ransomware

Mart 2023 yılında yaşanan bu saldırıda,Medusa ransomware grubu Kenya Airport şirketini hedef aldı.Medusa Ransomware 514 GB veri karşılığında 500.000 $ fidye talep etti.İddia edilen veriler içerisinde çalışanların kimlik fotoğrafları gibi önemli veriler olduğu söylenmektedir.

Son 6 Ayda Havacılık Sektörünü Hedef Alan APT Grupları

Ekibimiz tarafından yapılan incelemeler sonucunda, bazı APT gruplarının bu yılın ilk yarısından itibaren havacılık sektörünü hedef aldığı tespit edilmiştir. Raporun bilgilendirme amacı doğrultusunda söz konusu APT gruplarına ait bilgilere aşağıda yer verilmiştir.

Bitwise SPIDER



Bitwise Spider APT grubu, devlet kurumları, büyük şirketler ve kritik altyapıları olan ülkelerin özellikle savunma, enerji, iletişim ve teknoloji sektörlerini hedef bir APT (Advanced Persistent Threat) grubudur.

Saldırılarda kullanılan zafiyetler ve saldırı teknikleri:
- Active Directory
- Shadow copy
- UAC Bypass
- ESXI

Bitwise Spider, gelişmiş saldırı vektörleri kullanarak hedef ağlara sızar. Bunlar arasında phishing e-postaları, güvenlik açıklarını kullanma, zararlı yazılım enjeksiyonu, sosyal mühendislik ve gelişmiş süreç kaçırma teknikleri bulunur.

Bitwise Spider APT grubu, özelleştirilmiş zararlı yazılımlar kullanır. Bu zararlı yazılımlar, casusluk faaliyetleri için tasarlanmıştır ve genellikle gelişmiş zararlı yazılım analiz yöntemleriyle tespit edilmeleri zordur. Bitwise Spider grubunun geliştirdiği bilinen iki zararlı yazılım ailesi bulunmaktadır: LockBit Fidye Yazılımı ve StealBit InfoStealer Zararlı Yazılımı.

Bitwise Spider APT grubunun kurumlara etkileri:
1. Veri Hırsızlığı
2. Repütasyon Zararı
3. Finansal Kayıplar
4. Rekabet Avantajının Azalması
5. Saldırı Maliyetleri

Berserk Bear

Berserk Bear, ayrıca Energetic Bear veya Dragonfly olarak da bilinen, siber casusluk faaliyetleri yürüten bir Gelişmiş Sürekli Tehdit (APT) grubudur.

Berserk Bear'ın operasyonlarının odak noktası enerji sektöründeki kuruluşlardır, özellikle enerji şebekeleri, petrol ve gaz şirketleri ve diğer kritik altyapı sağlayıcıları.

Bu sistemlere izinsiz erişim sağlayarak grup, istihbarat toplamayı, operasyonları bozmak ve önemli kaynaklar üzerinde kontrol sağlamayı amaçlamaktadır.

Berserk Bear, hedeflerine ulaşmak için çeşitli gelişmiş teknik ve taktikler kullanmaktadır. Bunlar arasında, genellikle zararlı ekleri veya bağlantıları içeren özenle hazırlanmış e-postaların belirli kişilere gönderildiği **spear-phishing** kampanyaları bulunmaktadır. Grup **watering hole** saldırılarına başvurur, hedefledikleri kuruluşlar tarafından sıkça ziyaret edilen meşru web sitelerini tehlikeye atarak zararlı yazılım veya zafiyetleri kullanır.

Berserk Bear, özellikle endüstriyel kontrol sistemlerinde (ICS) kullanılan yazılım ve sistemlerdeki zafiyetleri sömürme yeteneğiyle dikkat çekmektedir. Kritik altyapıları ihlal etme kabiliyeti, hedeflenen kuruluşlara ve etkilenen sektörlerin genel istikrarına önemli riskler taşımaktadır.

Grup, 2015 ve 2016 yıllarında Ukrayna'daki enerji şebekelerini etkileme rolü nedeniyle uluslararası dikkat çekmiş ve yetenekleri ve potansiyel etkisi vurgulanmıştır. Enerji sektörü birincil odak noktası olsa da, Berserk Bear'ın Amerika Birleşik Devletleri ve Avrupa dahil diğer sektörler ve ülkelerdeki kuruluşlara yönelik saldırıları da bilinmektedir.

Faaliyetlerinin gizlilik gerektirmesi nedeniyle, Berserk Bear hakkında detaylı bilgilere genellikle sınırlı ve yakından korunan bir şekilde erişilmektedir. Güvenlik araştırmacıları ve hükümet kurumları, bu sürekli ve son derece yetenekli APT grubunun oluşturduğu tehditleri anlamak ve karşılamak için faaliyetlerini izlemeye devam etmektedir.

MuddyWater

MuddyWater APT grubu, çeşitli ulusal ve uluslararası hedeflere karşı saldırılar gerçekleştiren bir gelişmiş kalıcı tehdit (APT) grubudur.

Bu grup, ilk olarak 2017 yılında tespit edilen ve genellikle Orta Doğu ve Asya ülkelerindeki kamu kurumları, telekomünikasyon şirketleri, üniversiteler ve diğer sektörlere yönelik saldırılarında aktif olduğu bilinen bir grup olarak bilinir.

MuddyWater'ın saldırıları genellikle gelişmiş sosyal mühendislik teknikleri, karmaşık malware saldırıları ve hedeflenmiş phishing kampanyaları içerir. Bu grup, sahte belgeler, Word veya Excel dosyaları gibi güvenilir görünen iletiler aracılığıyla hedef sistemlere sızma girişiminde bulunur. Saldırılarında, gelişmiş gizlilik ve gizlenme tekniklerini kullanarak tespit edilmeyi önlemeye çalışır.

MuddyWater'ın hedeflediği amaçlar arasında bilgi toplama, casusluk, bilgi sızdırma ve ağların kontrolünü ele geçirme gibi faaliyetler bulunabilir. Bu grup, karmaşık saldırıları gerçekleştirme yeteneğine sahip olan uzman bir aktör olduğu bilinir ve sürekli olarak taktiklerini ve tekniklerini geliştirmeye devam eder.

MuddyWater APT grubu, bilgi güvenliği uzmanları ve siber güvenlik ekipleri tarafından yakından takip edilmekte ve analiz edilmektedir. Bu sayede yeni saldırı eğilimleri ve yöntemleri hakkında bilgi edinilerek savunma stratejileri oluşturulmaya çalışılmaktadır.

ALPHA SPIDER

Alpha Spider APT grubu, siber saldırılarda bulunan ve gizli kalma yeteneğine sahip olan bir gelişmiş kalıcı tehdit (APT) grubudur.

Alpha Spider'ın saldırıları genellikle hükümet kurumları, askeri kuruluşlar, enerji şirketleri ve finansal kuruluşlar gibi stratejik sektörlere odaklanmaktadır.

Bu grup, gelişmiş hedefli saldırı tekniklerini kullanarak sistemlere sızma girişiminde bulunur ve hassas verileri ele geçirmeyi hedefler.

Alpha Spider, siber casusluk faaliyetleriyle bilinir ve genellikle bilgi toplama, entelektüel mülkiyet hırsızlığı ve stratejik bilgilerin sızdırılması gibi amaçları güder. Grup, siber saldırılarında gelişmiş malware araçları, exploitler ve sosyal mühendislik taktiklerini kullanır. Ayrıca, ileri düzey gizlilik ve gizlenme teknikleriyle tespit edilmeden kalma yeteneğine sahiptir.

Alpha Spider APT grubu, sürekli olarak saldırı taktiklerini ve tekniklerini geliştirir ve günceller. Bu nedenle, bilgi güvenliği uzmanları ve siber güvenlik ekipleri, bu grubun faaliyetlerini takip etmek ve savunma stratejilerini güncellemek için sürekli olarak analizlerini yapmaktadır.

Alpha Spider APT grubunun hedefleri ve saldırı yöntemleri hakkında daha fazla bilgi edinmek, savunma mekanizmalarının güçlendirilmesi ve saldırılara karşı daha etkili önlemler alınması açısından büyük önem taşır.

ALPHA SPIDER

Cosmic Wolf APT grubu, siber saldırılarda bulunan gelişmiş bir kalıcı tehdit (APT) grubudur. Bu grup, çeşitli sektörlerdeki hedeflere karşı karmaşık ve sofistike saldırılar gerçekleştirerek bilgisayar korsanları tarafından yönetilir.

Cosmic Wolf'un hedefleri genellikle hükümet kurumları, askeri birimler, büyük şirketler ve kritik altyapılar gibi stratejik öneme sahip kuruluşlardır. Grup, finansal kazanç, casusluk veya politik amaçlarla saldırılar düzenleyebilir.

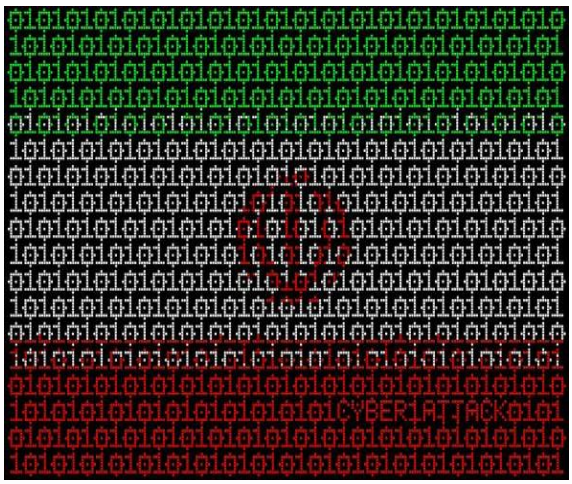
Cosmic Wolf, gelişmiş saldırı teknikleri kullanarak hedef sistemlere sızmayı hedefler. Bu grup, hedef kuruluşları belirlemek ve zayıflıkları tespit etmek için kapsamlı bir istihbarat toplama sürecinden geçer. Ardından, özel olarak tasarlanmış kötü amaçlı yazılımları, exploitleri ve sosyal mühendislik yöntemlerini kullanarak hedef sistemlere sızar.

Cosmic Wolf, saldırılarından önce ve sonra ağlarındaki izlerini gizlemek için gelişmiş gizlenme ve kötü amaçlı faaliyetlerini kamufle etme tekniklerini kullanır. Bu sayede tespit edilmelerini zorlaştırır ve izlerini takip etmek ve saldırılarını engellemek daha zor hale gelir.

Bu APT grubu, sürekli olarak saldırı tekniklerini geliştirir ve günceller. İleri düzey araştırma ve geliştirme çalışmalarıyla kendini yenileyerek savunma önlemlerini aşma girişiminde bulunur. Bu nedenle, güvenlik uzmanları ve siber güvenlik ekipleri, Cosmic Wolf'un faaliyetlerini izlemek, saldırılarını tespit etmek ve koruma stratejilerini güncellemek için sürekli olarak çalışmaktadır.

Cosmic Wolf APT grubunun faaliyetlerini anlamak ve koruma önlemlerini güçlendirmek, hedeflenen kuruluşlar için büyük önem taşır. Bu grupla ilgili güncel bilgilere erişmek ve saldırılarını engellemek için güvenlik topluluğunun iş birliği ve bilgi paylaşımı önemlidir.

APT39



APT39'un telekomünikasyon ve seyahat endüstrilerine odaklanması, belirli kişilere karşı izleme, izleme veya gözetleme operasyonları gerçekleştirme, ulusal önceliklere ilişkin stratejik gereksinimlere hizmet eden ticari veya operasyonel amaçlarla özel veya müşteri verilerini toplama veya kolaylaştırmak için ek erişimler ve vektörler oluşturmaktadır.

Saldırı Yaşam Döngüsü
APT39, saldırı yaşam döngüsünün tüm aşamalarında çeşitli özel ve herkese açık kötü amaçlı yazılımlar ve araçlar kullanır.

APT39 zararlı attachment veya hyperlinks olan kimlik avı e-postalarından yararlandığını ve tipik olarak bir POWBAT enfeksiyonuna yol açtığını gözlemlenmektedir. APT39, genellikle meşru web hizmetleri ve hedeflenen hedefle alakalı kuruluşlar gibi görünen domain adreslerini kaydeder ve bunlardan yararlanır. Ayrıca, bu grup, ANTAK ve ASPXSPY gibi web shelleri kurmak için hedeflenen kuruluşların savunmasız web sunucularını rutin olarak tanımlamış ve bunlardan yararlanmış ve çalınan meşru kimlik bilgilerini, dışarıdan bakan Outlook Web Access (OWA) kaynaklarını kullanmıştır.

APT39, hedef ortamda bir dayanak oluşturmak için SEAWEED, CACHEMONEY ve benzersiz bir POWBAT çeşidi gibi özel back-doorlardan yararlanmaktadır. Ayrıcalık yetki yükseltme sırasında, Windows Kimlik Bilgisi Düzenleyicisi ve ProcDump gibi yasal araçlara ek olarak, Mimikatz ve Ncrack gibi serbestçe kullanılabilen araçlar gözlenmiştir.Özel komut dosyaları ve hem serbestçe kullanılabilen hem de port tarayıcı, BLUETORCH gibi özel araçlar kullanılarak gerçekleştirildi.

APT39, Uzak Masaüstü Protokolü (RDP), Güvenli Kabuk (SSH), PsExec, RemCom ve xCmdSvc gibi sayısız araçla lateral movement tekniğini kolaylaştırmaktadır. Virüs bulaşmış ana bilgisayarlar arasında SOCKS5 proxy'leri oluşturmak için REDTRİP, PİNKTRİP ve BLUETRİP gibi özel araçlar da kullanılmıştır. Yanal hareket için RDP kullanmaya ek olarak, APT39 bu protokolü mağdur bir ortamda kalıcılığı korumak için kullanmıştır. APT39, görevini tamamlamak için genellikle çalınan verileri WinRAR veya 7-Zip gibi sıkıştırma araçlarıyla arşivlemektedir.

ECHO

CYBER THREAT INTELLIGENCE