BOX 1

Technology Focus—Legacy Infrastructure

Financial services firms, from central banks to retail banks and insurers, have been grappling with legacy infrastructure for many years. While this is true of many, if not all, other sectors, the problem is especially acute in finance due to the widespread reliance on core systems that are many decades old and that have often been joined together as a result of various mergers and acquisitions. The industry's reliance on software programmed in common business-oriented language (COBOL) is well-known, with the number of qualified engineers that can maintain these codebases dropping each year.

A recent report by the United Kingdom's Treasury Committee into information technology (IT) failures in the financial services sector found that not enough was being done to mitigate operational risks posed by legacy technology and that organizations must ensure that the use of legacy systems remains appropriate.[7]

Many have argued that overhaul of legacy systems should be coupled with taking advantage of cloud technology.[8] However, this requires careful planning and is not as simple as a so-called lift-and-shift. For example, legacy login credentials quickly result in current breaches if systems are inadvertently exposed to the internet. Organizations need to sort out such skeletons in the closet before migrating to the cloud.

A notable project in upgrading legacy infrastructure is the Bank of England's Real Time Gross Settlement Renewal Programme (RTGS2).[9] Many central banks around the world are monitoring this closely, with expected completion for the project around 2024. Among the main principles driving RTGS2 are higher levels of resilience and blending current needs with future-proofing—for example, retaining the financial messaging service SWIFT for connectivity and messaging services but being message-network agnostic in design.[10] Notably, the use of blockchain-type Distributed Ledger Technology (DLT) was considered for RTGS2, but it was found insufficiently mature for use.[11]

Evolving Techniques

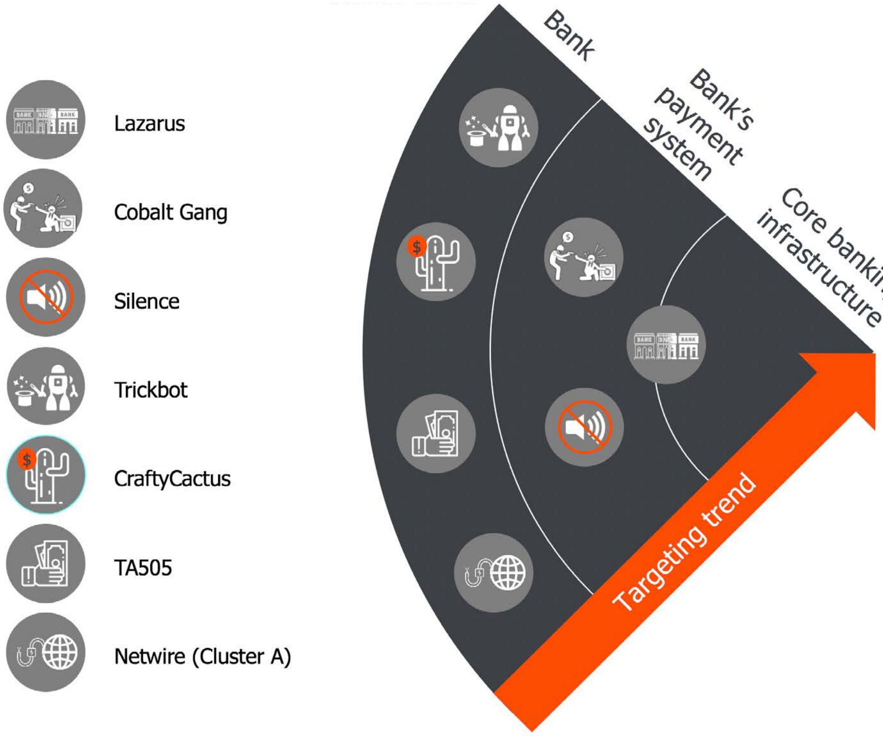
While the motivations of the various threat groups have not changed much, the techniques used to achieve their goals continue to evolve. This section highlights two areas that are key concerns to financial services sector firms today: targeted intrusions and ransom and extortion attacks.

Targeted Intrusions

Some of the most significant threats to the financial system come from state or organized criminal groups seeking to steal funds. An overarching trend among threat actors in recent years has been their steady progression into deeper levels of financial infrastructure. Figure 2 highlights different threat groups that specifically target banks and their capability and intent to target different levels of financial infrastructure.

FIGURE 2

Many Threat Groups Can Compromise Bank Networks but Only Some Reach Core Infrastructure



SOURCE: BAE Systems, 2020

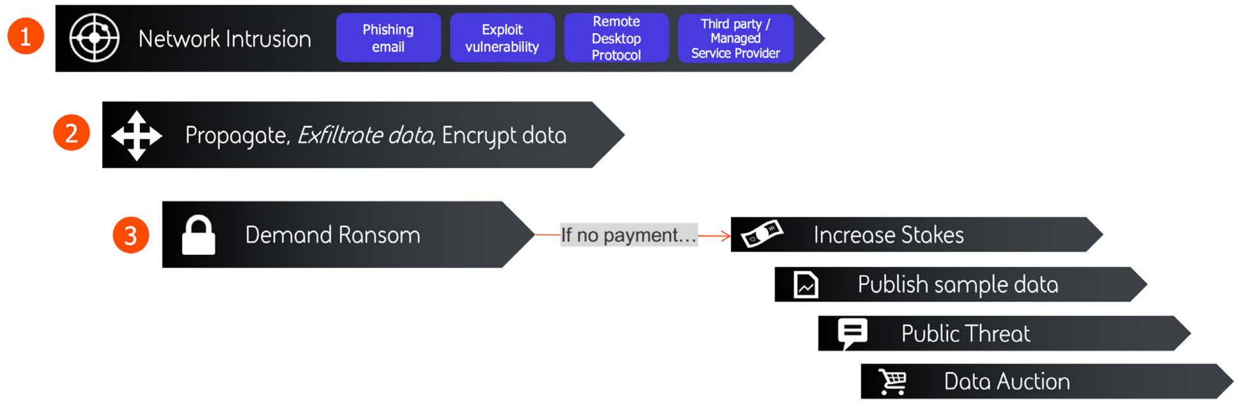
Several of these groups are expert at using sophisticated penetration testing tools, such as Cobalt Strike and PowerShell Empire.[12] These tools have advanced significantly in recent years. They contain features that make detection on enterprise networks particularly difficult. Such features include: living-off-the-land techniques, which leverage preexisting Windows tools such as PowerShell; in-memory infection, where the malware doesn't write any files to disk, in order to hamper antivirus detection; and domain name system (DNS) command-and-control modules, which can effectively evade web-proxy controls and intrusion detection tools.

Ransom and Extortion

Ransomware has evolved from the early years of basic locker malware targeting millions of end users via phishing emails to today's sophisticated attacks against large corporations and public institutions causing millions of dollars of damages on an increasingly regular basis (see figure 3). In another recent shift in tactics, criminal groups now steal data from company networks prior to encryption and threaten to publicly release the data on their ransomware blogs if the victim does not pay up.

FIGURE 3

Simplified Stages of a Modern Ransomware Attack with Data Theft and Extortion



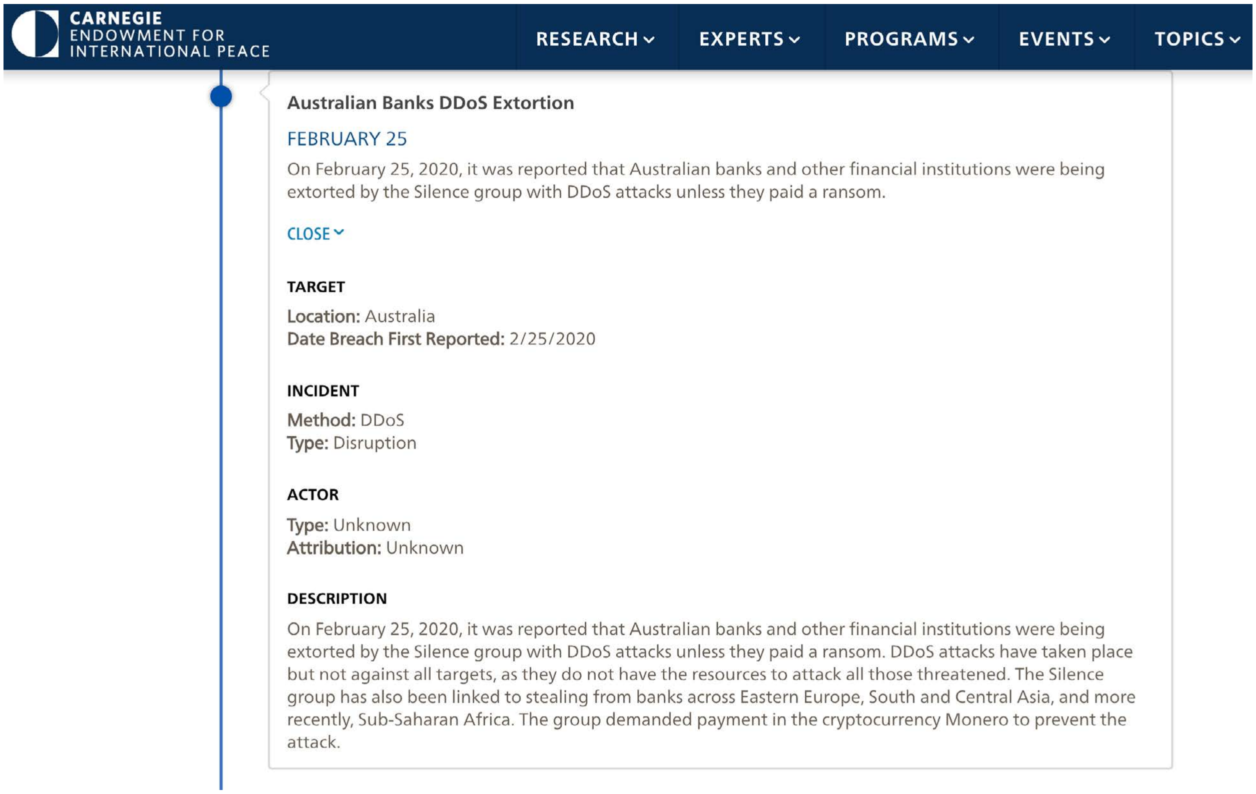
SOURCE: BAE Systems, 2020

The most commonly targeted sector for this type of ransomware attack is industrial and manufacturing organizations. However, as discussed in the opening section of this paper, financial services and the financial services supply chain have also been targeted recently (see figure 4). Criminals' use of new data-leaking tactics in 2020 has put increased pressure on their victims to pay, for fear that sensitive customer or commercial information will be publicly released. This could do far more damage than a traditional encryption attack, where the costs (if no ransom is paid) are purely for remediation and IT cleanup. Additional data privacy requirements (such as the European Union's General Data Protection Regulation [GDPR]) and the publicity that these attacks generate can also cause significant reputational damage to an organization.

A different twist on a ransom attack is where DDoS techniques are used to create the attack against an organization, rather than ransomware. In recent months there has been an increase in this so-called DDoS for extortion attack mode (see figure 4).

FIGURE 4

Australian Bank DDoS Extortion



Australian Banks DDoS Extortion

FEBRUARY 25

On February 25, 2020, it was reported that Australian banks and other financial institutions were being extorted by the Silence group with DDoS attacks unless they paid a ransom.

TARGET

Location: Australia
Date Breach First Reported: 2/25/2020

INCIDENT

Method: DDoS
Type: Disruption

ACTOR

Type: Unknown
Attribution: Unknown

DESCRIPTION

On February 25, 2020, it was reported that Australian banks and other financial institutions were being extorted by the Silence group with DDoS attacks unless they paid a ransom. DDoS attacks have taken place but not against all targets, as they do not have the resources to attack all those threatened. The Silence group has also been linked to stealing from banks across Eastern Europe, South and Central Asia, and more recently, Sub-Saharan Africa. The group demanded payment in the cryptocurrency Monero to prevent the attack.

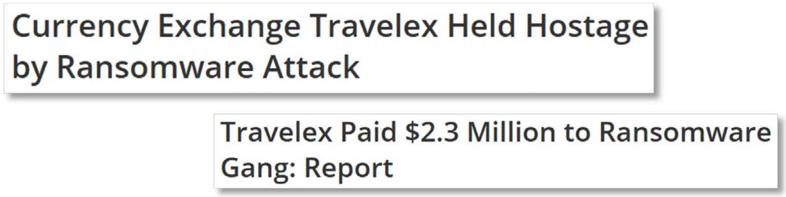
SOURCE: "Timeline of Cyber Incidents Involving Financial Institutions," Carnegie Endowment for International Peace, updated August 2020, https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline.

The following case study demonstrates the damage a successful ransomware attack can have on a financial services organization.

Case Study: Travelex & REvil

On December 31, 2019, the London-based foreign currency exchange Travelex was hit by a ransomware attack that crippled its network and allegedly stole five gigabytes of documents. The attackers demanded Travelex pay $6 million to restore its systems and prevent the stolen data from being leaked online. This attack had a devastating effect on Travelex, reducing their operations to pen and paper transactions and impacting a wide range of high street banks that relied upon its currency services. Reports estimated that the attack ultimately cost the firm almost $30 million and put their parent company, Finablr, under significant financial pressure, with $2.3 million reportedly paid in ransom (see figure 5).[13] Travelex subsequently filed for bankruptcy, citing the coronavirus pandemic and the cyber attack as key factors.[14]

FIGURE 5
Headlines to a Ransomware Attack Can Be as Damaging as the Intrusion



Currency Exchange Travelex Held Hostage by Ransomware Attack

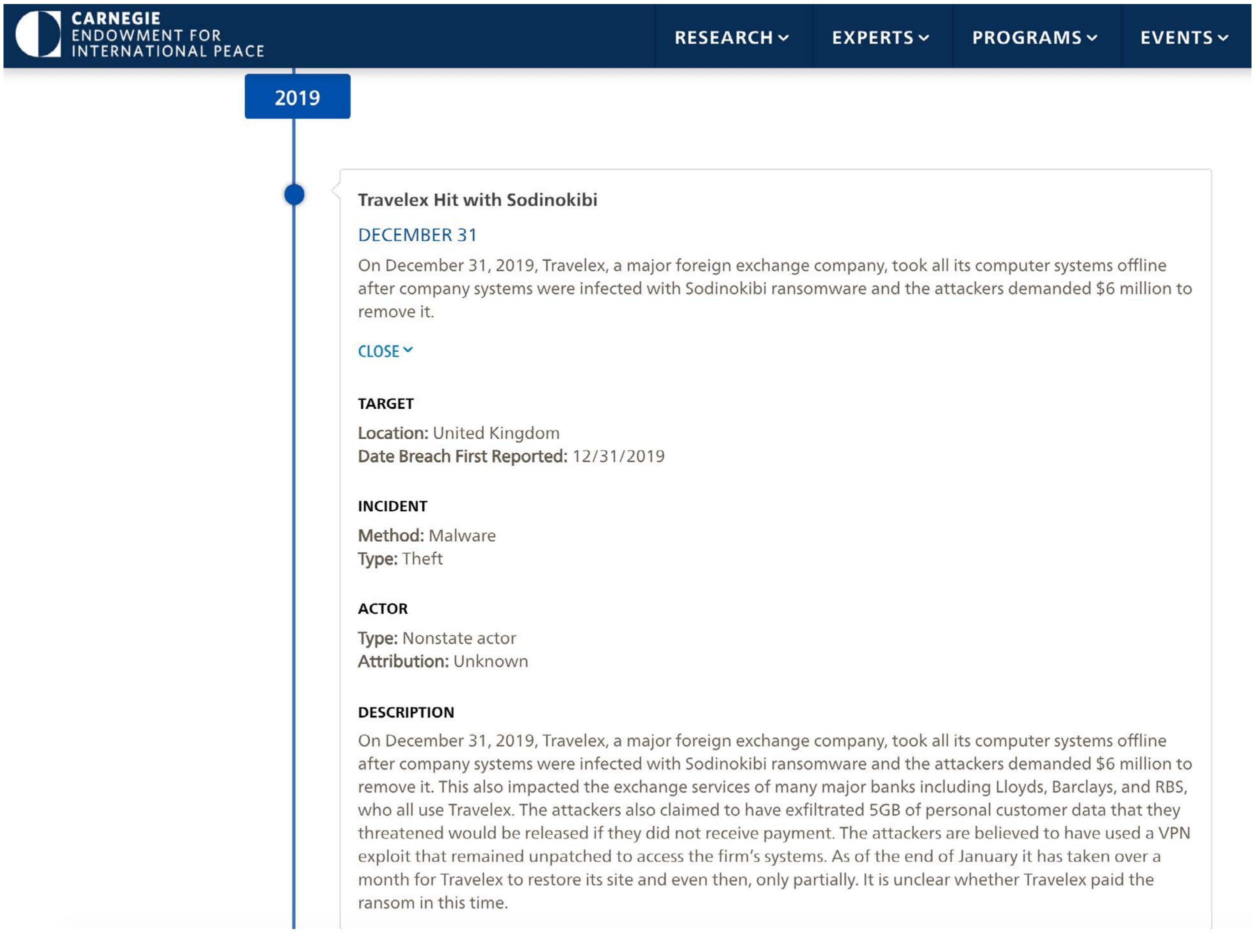
Travelex Paid $2.3 Million to Ransomware Gang: Report

SOURCE: BAE Systems, 2020

The threat actors responsible for this attack used a prolific ransomware variant called REvil, one of the pioneers in this new wave of data theft ransomware attacks. The threat group, also called REvil, has since gone on to undertake similar attacks against a wide range of victims. The attackers work on an affiliate model whereby attackers can purchase a subscription to use the malware to perform their own attacks but publish stolen data to a central blog (see figure 6). REvil affiliates predominantly favor attacks on the financial and insurance sector.

FIGURE 6

Travelex Hit with Sodinokibi



Travelex Hit with Sodinokibi

DECEMBER 31

On December 31, 2019, Travelex, a major foreign exchange company, took all its computer systems offline after company systems were infected with Sodinokibi ransomware and the attackers demanded $6 million to remove it.

CLOSE

TARGET

Location: United Kingdom
Date Breach First Reported: 12/31/2019

INCIDENT

Method: Malware
Type: Theft

ACTOR

Type: Nonstate actor
Attribution: Unknown

DESCRIPTION

On December 31, 2019, Travelex, a major foreign exchange company, took all its computer systems offline after company systems were infected with Sodinokibi ransomware and the attackers demanded $6 million to remove it. This also impacted the exchange services of many major banks including Lloyds, Barclays, and RBS, who all use Travelex. The attackers also claimed to have exfiltrated 5GB of personal customer data that they threatened would be released if they did not receive payment. The attackers are believed to have used a VPN exploit that remained unpatched to access the firm's systems. As of the end of January it has taken over a month for Travelex to restore its site and even then, only partially. It is unclear whether Travelex paid the ransom in this time.

SOURCE: "Timeline of Cyber Incidents Involving Financial Institutions," Carnegie Endowment for International Peace, updated August 2020, https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline.

Although most ransom and extortion attacks target enterprise networks, regardless of where these services are hosted, cloud services have been specifically exploited by criminal groups.[15] This is just part of a growing concern over threats to cloud technology, another focus area for many financial services firms (see box 2).

BOX 2

Technology Focus—Cloud

Undoubtedly the major technology trend for the finance industry in the last decade is the shift to cloud services. As more and more companies move to a cloud-first strategy or make some level of transition to the cloud and as the range of services that are available via cloud deployment continues to increase, this trend is likely to remain at the top of C-suite lists for many years to come.

Outside of the technical challenges of making this shift, there are a number of security-related concerns that consistently come into play and will feature on many internal risk registers. Each of the following concerns brings a level of complexity and a requirement for in-house expertise:

- Concerns over data residency are tangible on a backdrop of increased data regulation and a concern that businesses could—without paying attention to cloud platform terms and conditions—fall foul of data retention or privacy laws in different countries.

- The (albeit unlikely) scenario of a major cloud provider suffering a major outage that exceeds their own redundancy measures and an ability to meet customer-service-level agreements on availability has led to many companies adopting a multicloud approach, running services from Amazon Web Services, Azure, Google, and the like.

- The shared responsibility model for different cloud platforms can be a sticking point, and fully understanding which responsibilities rest with the organization, as well as how to achieve an appropriately secure configuration, can require extensive expertise. Many organizations have needed to train their staff in different cloud models, with larger organizations requiring hundreds of trained personnel in different areas.

The question of configuration remains the main security issue for cloud adoption. Examples of data breaches arising from inappropriately configured cloud storage have been seen in recent years. Despite improvements by cloud service providers trying to make it harder for these errors to occur, they are still happening. According to the 2020 Verizon Data Breach Investigations Report, 22 percent of data breaches in 2019 involved cloud assets, and misconfiguration errors (many of which are related to cloud) are now the most common type of error reported in Verizon's data.[16]

The major cloud platforms each have very high standards of security and extensive resources at their disposal. To date, their security records have been very strong. The question of whether and how a data breach at a cloud provider might occur is an interesting one, but a common viewpoint held across many industry sectors is that data and services are safer in the hands of a major cloud provider than they would be on premises. However, while that may well be correct from an individual organization's perspective, from a sector and financial services regulatory perspective, concerns around aggregation risk come to the fore, with many firms reliant on a few core IT service providers for so many critical financial services.

It is inevitable that as more and more assets are in the cloud, the threat landscape will shift to focus on technology supply chains and cloud providers—as has already begun to happen. It is highly likely that critical vulnerabilities that allow for hypervisor or virtual machine breakout (meaning that a threat actor on one public cloud instance can compromise others) will arise in the future. The arms race between these being discovered by security teams and researchers versus threat actors will be similar to that which plays out in major operating systems and software products.

Emerging Challenges

Threat Group Collaboration and Facilitation

The evolution of the threat landscape features greater collaboration among threat actors. In 2018, several infections from the North Korea–based Lazarus Group coincided on networks within the same time frames as a Russian-speaking criminal group known as TA505.[17] Forensic evidence from incident response work confirmed the overlap wasn't purely coincidental; the criminal actors were found to have effectively handed over access to Lazarus. A few theories on the nature of the relationship between TA505 and Lazarus were considered, but the most likely one was a transactional relationship where TA505 sold victim network access to Lazarus.[18]

While instances of TA505 and Lazarus overlap may have subsided, overlaps between Lazarus and other criminal operations have come to light. Other incidents of transactional relationships or collaboration appeared again in 2020. Infections with the criminal malware Trickbot led to the deployment of Lazarus malware, which might indicate a similar scenario of Lazarus buying access from another party. Others have reported that a Trickbot-related framework called Anchor was also associated with Lazarus malware.[19]