Diamond Model of Intrusion Analysis – Travelex Ransomware Attack

Constantine Caras
caras6@gatech.edu

Introduction
Travelex had been operating as a prominent foreign currency exchange service until its demise came at the hands of the Ransomware Evil (aka REvil/Sodinokibi) cybercriminal group on New Year’s Eve, 2019. The debilitating cyber-attack compromised virtually every Travelex customer-facing system and took the London-based firm offline for over two weeks, ultimately rendering its trustworthiness and service provision irreparable. Despite negotiating down and eventually complying with REvil’s payment demands, the lack of preemptive security measures resulted in acute impact to the business and imposed major hindrance to recovery efforts.

Through the application of the Diamond Model of Intrusion Analysis, this paper identifies and intricately examines all core features of the incident, highlighting the hacker’s modus operandi and defining causal relationships between every phase of the attack. Furthermore, a policy assessment is conducted to illustrate which societal layer could best address this variant of intrusion to support stronger proactive security defense in the future.

I. Diamond Model Application and Analysis
To effectively inspect the flow of events from an overarching perspective, the following Diamond Model (Figure 1.1) depicts REvil’s ransomware hack of Travelex and is used as the basis for this paper’s investigation of the security incident.

---

**Figure 1.1**
Travelex/REvil – Diamond Model

**Adversary** – REvil (Sodinokibi)
- Performs remote code execution through
- Identify weakness and edge vector for intrusion
- Capabilities –
  - Advanced recon
  - Privilege escalation
  - CVE-2019-11510 exploitation
  - Lateral network infiltration

**Victim** – Travelex services and assets
- Victim discovers the malware
- File inaccessibility takes services offline
- Infrastructure –
  - Unpatched VPN servers
  - Internet facing services
- On-prem Pulse Secure servers enable access to internal network
- SIEM logs and ransomware prompts reveal adversary
Adversary
In examining our initial Diamond Model element, Russian-based REvil is identified as
the intrusion actor, or agent, attributed with conducting this ransomware attack. This
can be deemed factual as the Ransomware as a Service (RaaS) group themselves went
public amid the heist with their monetary demands, and additionally, reported their
involvement to several media outlets post-breach, including WSJ & BBC [1, 2].
However, despite their coming forward, the adversary can also be systematically
discerned through the analyzation of the entire Diamond Model and its threads.

REvil’s operations were still in their infancy at the time of this December 2019 breach,
lacking any malevolent track record/notoriety garnered from the public, or understanding
of procedural tactics used to compromise entities. This obscurity allowed for execution
of several attacks of similar flow against a myriad of organizations, from which parallels
can now be drawn to pinpoint REvil’s involvement on a cross-case basis [3].

As part of REvil’s operating model, affiliates were recruited to deploy their crafted
malware stack to targeted organizations. It is believed that these affiliates were also
Russian based, as the group was yet to target any Russian corporations. These hired
individuals ‘press the buttons’ of the attack, so to speak, acting as the ‘operator’, or
actual hacker in the process. REvil, the ringleader from which directive to attack is
delineated to affiliates, acts as the ‘customer’. Monetary gains are distributed amongst
REvil and its affiliates, and fund the resources required to execute future attacks.

Victim
The Travelex organization – a worldwide foreign currency exchange service utilized by
millions via airport kiosks and international brick and mortar stores – serves as the
victim persona. Its employees also fall into this category, many of which had their
positions cut due to organizational restructure prompted by the attack. Victim asset
comprises of 5GB of exfiltrated sensitive customer data, web servers delivering content
to 30 countries, and additional systems that were air-gapped to halt the malware
spread, rendering them useless [2]. During the two-week outage, Travelex was forced
to resort to an ad-hoc pen and paper model of operation, severely hindering customers’
ability to exchange cash.

Although Pulse-provisioned servers were the hop-through point to which attackers
gained internal network access to Travelex, Pulse is not a victim. Their systems resided
in Travelex’s datacenter to act as VPN single sign on mechanisms, and did not store
any customer data or proprietary intellectual property. Pulse itself (and its parent
organization, Ivanti) was unaffected by the intrusion.

It is likely that Travelex’s renown as the global currency exchange leader [1], paired with
their vast customer base, instigated REvil’s prospective recon and ultimate execution
against them. The firm can be defined as an ‘easy’ target, handling large amounts PCI
& PII while exhibiting potential intrusion vectors to their sensitive network, such as
vulnerable VPN systems and public-facing RDP [4, 5].
Capabilities
REvil group’s modus operandi is predicated on their advanced methods of reconnaissance, vulnerability exploitation, stealthy privilege escalation, and file encoding/encrypting. This expert capability not only allows for seamless target vetting and selection, but obscuresness throughout hacking operations, enabling more systematic and impactful attacks due to its Advanced Persistent Threat (APT) technique. Intricacies in REvil’s malware allow for under-the-radar baking, in which they can familiarize themselves with a target’s internal network and data sets while disguising their presence [6].

To put it technically, REvil specializes in exploiting system weaknesses the Pulse Server vulnerability, CVE 2019-11510: Pre-auth Arbitrary File Reading, the specific medium for intruding Travelex’s network. Their pattern consists of obtaining domain admin access after utilizing PsExec to install a Virtual Network Compute (VNC) to laterally traverse their target’s network and disable endpoint security tools, enabling the exfiltration of data and installation/propagation of REvil ransomware [6].

Through the incapacitation of business-critical systems invariably arises the capability to leverage monetary demands for system restoration. Demands come in the form of Bitcoin requests, since the decentralized block-chaining currency allows for more anonymity and avoids tipping off investigating officials. This, of course, is how REvil monetizes its operations.

Infrastructure
This element describes the physical and logical methods of which communication and control occurred between adversary and victim, emphasizing the target’s weak points and the systems by which mechanisms and exploits granted access to the bad actor(s).

Weak, unpatched Pulse Connect Secure VPN servers acted as the exploitable vector for malicious network infiltration of the ransomware strain, enabling connectivity between the actor and victim. The affected servers were on-premise Pulse boxes in Travelex’s datacenter which, despite ample notification from the vendor, were left unpatched by the firm’s system administrators for over eight months [2]. Whether due to oversight or lack of resources, this shortcoming presented a single point of failure – or entry – and enabled REvil to ‘deploy its capabilities’ to the Travelex environment, infiltrating their network and pivoting to critical systems.

The attack involves Type 2 infrastructure – Pulse VPN servers that are housed by Travelex were exploited, leading to the compromise of the Travelex’s entire network. This hop-through took place via the Pulse Connect Secure federation client, due to the unpatched vulnerability (CVE 2019-11510) on the Pulse IdP system. Figure 1.2 [7] portrays a standard on-premise Pulse Secure setup, similar to the integration configuration of Pulse in Travelex. The breach vector is indicated.
**Activity Threads**

Through the diamond schematic, several chronologically linked events and meta-features are observed across the vertices of the model.

**Social-Political Meta-Feature**

In highlighting the adversary – victim relationship, the intent of the actor must first be examined. The foremost motivating factor is recognizably financial gain through the maintenance of a network foothold on the victim, Travelex, in order drive costs or timeliness of payments. REvil’s mantra is operating through ‘negotiation to decrypt’ with the threat of exposing exfiltrated user data if the victim fails to comply within a certain window. The group doesn’t appear to have any political backing or incentive in its process; merely an independent entity looking to line their pockets by way of vulnerable, high-capital corporations – the ‘service’ which Travelex provides them. Like many adversarial cyber groups, REvil has a need for money to compensate members and affiliates, fund operations/computing resources, and maintain secretive status – with a goal of perpetuating its malfeasant dominance over vulnerable corporations.

The designation of an APT is applied to the function of the REvil group, as they compromised Travelex servers eight months before and remained dormant on the systems, unnoticed by sysadmins. On the surface, the event seems to be an ephemeral, ‘smash and grab’ attack, due to the swift onset of file encryption and threatening ransomware messages taking place in a single evening. However, this relationship between adversary and victim had been persistent since April 2019 [2]. REvil had been performing intuitive, authenticated reconnaissance since that time, and exfiltrated over 5GB of customer data over the eight-month span [2]. Through REvil’s patience, a well-planned attack commenced as intended on December 31st. Diligence
through long-term association served as leverage against Travelex, and the APT had manifested in a time-sensitive ultimatum for its executives – pay the $6 million asking price for unguaranteed data restoration within or have your customer’s data leaked. As a slight consolation to the currency exchange firm, hackers settled for a negotiated 285 Bitcoin ($2.3 million), however the incident still proved costly – lack of first party cyber insurance resulted in the firm embracing 100% of the ransom [8].

Technology Meta-Feature
To best describe the capability-infrastructure relationship between REvil and Travelex, identification of utilized and misused technologies is imperative. The cyber kill chain can also be incorporated into this feature’s analysis, and is beneficial in reviewing the phases of intrusion. Initial recon methods entailed port scanning on UDP 4500 (PulseSecure / SSL VPN port) to examine the response for CVE 2019-11510 [9]. After discovering Travelex as a candidate for attack, hackers utilized their skillsets and malware to authenticate to the corporate network without credentials, commencing in the intrusion, exploitation, privilege escalation, and lateral movement phases via the insecure Pulse VPN endpoints. By way of this entry vector, we see an actual activity thread spanning four phases of the kill chain, arriving at the ‘obfuscation’ phase. While idle for months, the ‘thread’ is still active, and will serve as a key factor on the day of the availability attack. 5 GB of customer data is secretively downloaded, and ransomware logic bombs are set to encrypt on REvil’s execution day – the ‘denial of service’ phase. Capability had overpowered infrastructure through an evolving sequence of successive phases, and prepared the adversary to achieve the desired result.

II. Policy Assessment
A type of intrusion such as REvil’s attack on Travelex is most appropriately addressed through level 8, or the organizational layer, of the societal governance model. The exclusiveness of this type of breach on Travelex and other firms attacked through this same medium – equating to a minute percentage of companies utilizing Pulse Secure VPN services – poses several questions about their respective information security postures and standards: Why were the VPN servers left unpatched, despite receiving timely and ample warning? Who was governing regulatory compliance of these critical systems and their mitigating controls, and why weren’t these lackadaisical measures flagged as material requiring attention? Post attack, why weren’t full backups available to be immediately restored post server airgap? It is of my opinion that redress to these uncertainties is to be established by the respective organization through corporate security policies.

The global threat of ransomware is more widespread than ever, but it’s unnecessary for policymaking to rise to the ranks of the transnational or even the national level for rule enactment. From a technical perspective, instating organizational regulations at a company’s remote access ICT domain to patch all systems adequately and consistently, regardless of their estimated criticality, will assist in thwarting this type of contemporary attack from being as prevalent. Also, in this realm, corporate data backup policies should be formulated and adhered to for all storage devices, expectedly in conjunction with the organization’s ransomware policy. Performing full backups will increase MTTR
in the case of a ransomware hostage situation, and is a procedure commensurate with global best practices. Adopting a compliance framework such as NIST or ISO is necessary to form these standards.

From a legal standpoint, Travelex and similar REvil/ransomware victims should purchase cyber-insurance in the interim, and build their legal teams up to deal with fallout from the breach. Class-action lawsuits and investigations from governments/attorneys will most likely inundate the organization following potential customer data loss, and though seemingly reactive, will result in a standard operating procedure and provide for legal defense against any future threats on the corporation. Following regulatory guidelines – i.e. patching systems on a common cycle and utilizing as minimal amount of internet-facing services as possible operation – should be the key takeaway for Travelex to achieve reparation.
References


[9] “KB8569 - how does network connect / pulse secure client work when ESP is enabled versus NCP/oncp (SSL)?,” *Public KB - KB8569 - How does Network Connect / Pulse Secure client work when ESP is enabled versus NCP/onNCP (SSL)*? [Online]. Available: