CERT-EU

Ransomware in the transportation sector

Threat Memo - TM 20-009 - Date: 21/01/2020 - Version: 1.0
TLP:WHITE

FOR INFORMATION	Category	Type	Domain(s)	Sector(s)	Confidence
	Cybercrime	Ransomware	World	Transportation, aviation, maritime, ground transport	A1

Key Points

- Transportation and logistics are particularly attractive to operators of ransomware.
- Ransomware attacks against transportation operators usually correspond to the following scenarios: opportunistic criminal infections, hybrid attacks perpetrated by state-sponsored attacks, cybercriminal big game hunting.

Summary

Successful ransomware attacks in the transportation and logistics industry are happening frequently (see table annexed). For several reasons, ransomware operators find transportation and logistics temping as a lucrative target:

- They provide the opportunity to disrupt supply chains of hundreds or even thousands of other businesses
- The business is highly interconnected, presenting multiple potential points for malware infiltration (see for example Threat Memos on supply chain attacks, [190205-1] and [190326-1]).

In the **aviation sector**, attackers would most likely try to exploit air traffic control systems, cargo processes, and the aircraft themselves (incident examples below).

- The airport of Albany in New York state has already become victim of ransomware twice (Jan 2019 and Jan 2020),
- The Atlanta Int., Cleveland Int., and Bristol airports were all subject to ransomware attacks in 2018,
- The Int. airport of Odessa, in Ukraine was hit by the BadRabbit ransomware (related to NotPetya) in 2017,
- The aircraft parts manufacturer ASCO with sites all over the world was compromised with ransomware in June 2019.

In the **maritime sector**, large infrastructures like ports have shown to be attractive targets for cybercriminals (incident examples below).

- The US Coast Guard disclosed that the Ryuk ransomware had taken down a maritime facility in Dec 2019,
- XHunter ransomware attacks on a Kuwait shipping company and transport organisations were disclosed in Sept 2019,
- The San Diego harbour police department as well as the port itself were victim of a SamSam ransomware attack in Sept 2019.

Despite numerous occurrences, ransomware attacks were less prevalent in the **ground transport** sector, occurring mainly in the public transportation and in the US trucking industry (incident examples below).

- The Fresno COG (California), Spanish Transportation Agency, and Pinnacle Express (US) were all subject to ransomware attacks in 2019,
- The companies Truckstop.com (US), Bailey Trucking (DE), and Less-Than-Truckload computer systems (US) were infected with ransomware in 2019.

Comments

Ransomware attacks in the transportation sector typically match to 3 principal scenarios:

- Transportation organisations can be subject to *opportunistic criminal* infections like any organisation in any sector.
- Transportation infrastructures are seen as critical for a country's correct functioning and are therefore being targeted by state-sponsored cyber actors to create disruption and chaos in a foreign state. Operations may consist in testing new offensive cyber tactics, or be part of *hybrid threat campaigns*. The initial and primary victims of NotPetya, BadRabbit, and WannaCry have been targeted by likely state-actors who tried to conceal their real objective behind an apparent financial gain motive. The propagation across national boundaries and sectors was somehow employed as a way to blur analysis and attribution.
- Lately, there has been a rise in *big game hunting* (BGH) tactics. This scheme combines advanced, targeted attack techniques with ransomware to achieve substantial financial payoffs. BGH impacts both private and public sectors and the typical targets are organisations that cannot afford to have any downtime, a characteristic of transportation operators.

When it comes to ransomware, organisations in the transportation sectors are advised to be well prepared and have an incident response plan in place to help limit the potential damages, not only to production but also to customer trust and brand reputation. In these cases, prevention is always better than a cure.

Annex

Date	Victim	Country	Affected Sector	Ransom Demand	Ransomware
2020					
Jan 2020	Albany airport (New York)	US	Aviation		REvil, Sodinokibi
2019					
Dec 2019	RavnAir Dash 8 in Alsaka	US	Aviation		
Dec 2019	Exposing critical vessel control systems to significant vulnerabilities	US	Maritime		Ryuk
Dec 2019	Fresno COG (California)	US	Transportation services	$8000 (not paid)	
Dec 2019	Truckstop.com	US	Ground transport/Trucks		
Oct 2019	Spanish Transportation Agency	Spain	Transport		
Oct 2019	Bailey Trucking (NHK)	DE	Ground transport - Trucks		
Sep 2019	Kuwait Shipping and Transportation Organisations	Kuwait	Maritime & Transport		xHunter
July 2019	Albany (New York)	US	Maritime		
June 2019	ASCO cyber attack	World	Industry & Aviation		
June 2019	Less-Than-Truckload computer systems	US	Ground transport/Trucks		
Jan 2019	Trans4Cast system (Truckstop.com)	US	Ground transport/Trucks		
Jan 2019	Albany (New York): airport & metro	US	Aviation/Metro		
2018					
Nov 2018	Spanish airport operator Aena	Spain	Aviation		BitPaymer/ Dridex
Sep 2018	San Diego port	US	Maritime		-
Sep 2018	Bristol Airport	UK	Aviation		
Sep 2018	Port of Barcelona	Spain	Maritime		
July 2018	Chinese shipping firm Cosco	China	Maritime		
Apr 2018	Cleveland Hopkins International Airport	US	Aviation		
Mar 2018	Queensland Department of Transport	US	Transport		
Mar 2018	Hartsfield-Jackson Atlanta Int. Airport	US	Aviation		
Feb 2018	Colorado Department of Transportation cost $1.5 million	US	Transport		SamSam
2017					
Oct 2017	Metro system/Kiev & airport/Odessa and news media in Russia	UA, RU	Metro & Airport hundreds of victims	$6.000 per victim	BadRabbit
June 2017	Gov, advertising, transport, shipping (FedEx, Maersk)	UA, RU, EU	many organisations (shipping)		NotPetya
May 2017	Health service, telecom, transport…	World	+300,000 organisations	$300 per victim	WannaCry
May 2017	British shipping company Clarksons PLC	UK	Maritime		
2016					
Nov 2016	San Francisco transport system	US	Local transportation	$73.000	HDDCryptor