CERT-EU

Memo
16/09/2019 - TLP: WHITE

Big Game Hunting in the public sector

Reference: Memo [190916-1] – Version: 1.0
Keywords: Big Game Hunting, ransomware, extortion, disruption, Ryuk
Sources: Publicly available information

Key Points

- Big Game Hunting extortion campaigns by cybercriminals have become a significant threat to the public sector
- In the US, several ransomware attacks impacting local governments, cities, and public services were recently observed
- Cybercriminals are striking victims with greater precision and timing
- Their attacks are very well coordinated and they are demanding higher ransoms
- US Officials are worried of attacks against the 2020 Election

Summary

Big Game Hunting (BGH), where cybercriminals combine advanced, targeted attack techniques with ransomware to achieve substantial financial payoffs, has become a worldwide phenomenon, impacting both private and public sectors.

In the public sector, the number of targeted ransomware attacks has increased, especially since spring 2019 in the US. BGH has become a significant threat to local governments, cities and public services such as educational institutions. While the healthcare (more specifically hospitals) and the transportation sectors have historically been privileged targets of ransomware attacks, recent cases have shown that public services in general have become attractive for cybercriminals. The table in annex indicates some recent cases.

Several of the recent ransomware attacks aren't opportunistic and exhibit an increased coordination from attackers. In August for example, twenty-three local Texas governments were targeted by coordinated ransomware attacks[1]. The wave of attacks started in the morning of August 16 and security experts investigating the incidents believe that it was a coordinated campaign carried out by a single cybercriminal gang. Texas authorities along with the FBI have investigated the attacks.

Cybercriminals are striking victims with greater precision and timing. The attack against three public school districts in Louisiana is a good example. The timing of that attack was designed to inflict the most damage as it occurred just weeks before schools start in the autumn. Following the attack, the governor of Louisiana declared a state of emergency. This means that state resources will be made available and that assistance will be provided by experts from the Louisiana National Guard, Louisiana State Police, the Office of Technology Services and others in responding to the crisis and in preventing further data loss.

Criminals are demanding higher ransoms from authorities in charge of public services. In March 2018, the ransom demanded from the city of Atlanta was $50,000, while by summer 2019, it reached or exceeded $500,000 (Riviera Beach City $600,000; Lake City $600,000). Early September, the Mayor of the City of New Bedford said[2] that cybercriminals that had attacked its city on July 5, demanded $5.3 million in ransom. According to researchers[3], a few government authorities in the US have paid the ransom to get their files back. The restoration rate is about 25% among those who pay ransom. Often, the ransom payment is funded by cyber insurance.

US officials fear that ransomware attacks may be used against the 2020 election. Consequently, to prepare state election officials, the Cybersecurity Infrastructure Security Agency will provide educational material, remote computer penetration testing, vulnerability scans, and recommendations for preventing and recovering from a ransomware attack[4].

Comments

Considering the importance of the public sector and its institutions, they are likely to remain attractive targets for targeted ransomware campaigns.

As regards the question of the ransom payment, analysists are discussing[5] the role played by insurance companies in fuelling the rise in ransomware attacks. While cyber-insurance is usually designed to cover the mitigation of losses and protect against future attacks, paying the ransom could be a lot cheaper for the insurer. It at least one case, the victim's insurer pressured it to pay the ransom.

Organisations can reduce the impact of ransomware attacks by ensuring that proper backups are conducted on a routine schedule and that sensitive systems and data are properly segmented.

[1] https://securityaffairs.co/wordpress/90068/hacking/texas-governments-ransomware-attacks.html
[2] https://www.govtech.com/security/Ransomware-Hacker-Demands-53-Million-of-New-Bedford-Mass.html
[3] https://www.ivanti.com/blog/ransomware-in-the-public-sector
[4] https://www.itnews.com.au/news/us-officials-fear-ransomware-attack-against-2020-election-530205
[5] https://arstechnica.com/information-technology/2019/08/how-insurance-companies-are-fueling-a-rise-in-ransomware-attacks/

Date (2019)	Victim	Country	Affected Sector	Ransom Paid	Ransomware
2016					
Nov	San Francisco's light rail transit system's ticket machines	US	Local transportation	$73,000	
2017					
July	San Francisco's public TV and radio station	US	Public TV and radio	$27,000	
2018					
Feb	Colorado Department of Transportation	US	Local transportation		SamSam
March	Atlanta's network infrastructure	US	Local government (city)	$50,000	
2019					
March	Jackson County (Georgia)	US	Local government (county)	$400,000	
March 31	Albany (New York)	US	Albany police department		
April	Cleveland Hopkins International Airport	US	Airport		
April	City of Tallahassee (Florida)	US	Third-party vendor (payroll)	$498,000	
April	Augusta	US	Local government (city)	$100,000	
April 18	Maine	US	City's police department city's financial systems		
May 7	City of Baltimore	US	Local government (city)	$76,000	RobbinHood
June 20	Riviera Beach City (Florida)	US	Local government (city)	$600,000	
June 26	Lake City (Florida)	US	Local government (city)	$500,000	
July	LaPorte County (Indiana)	US	Local government (city)	$132,000	
July	New Bedford (Massachusetts)	US	Local government (city)	499 BTC ($5.3 million USD)	Ryuk
July	Finnish town of Kokemäki	Finland	Town		Most likely Phobos
July 23	Vigo County (Indiana)	US	Local government (County centre and courthouse)		Ryuk
July	Georgia state law enforcement agencies	US	Local government (State)		
July 25	Louisiana Governor declared a state of emergency	US	School districts		
July 25	City Power, the electric utility for Johannesburg	South Africa	Electric utility		
August 19	Coordinated attack against 23 Texas local agencies	US	Local government (State)		
August	Washington-based Grays Harbor Hospital	US	Hospitals	$1 M	
September	Numerous school districts in the states of Florida, Pennsylvania and Illinois	US	School district		