Шардул Десаи
Holland & Knight компанияси партнери (АҚШ)

ТОВЛАМАЧИ-ДАСТУРЛАРНИНГ ИСТИҚБОЛЛАРИ

Шардул Десаи
Партнер компании Holland & Knight (США)

ПЕРСПЕКТИВЫ ПРОГРАММ-ВЫМОГАТЕЛЕЙ

Shardul Desai
Partner at Holland & Knight (USA)

PERSPECTIVES ON RANSOMWARE

Prior to working for Holland & Knight I spent 9 years working as a federal prosecutor in Western District, Pennsylvania. I handled some of the Department of Justice's most significant cybercrime cases, including a Gameover ZeuS and Evil Corp prosecution. Both involved organized Russian cybercriminals who were involved with some of the most pernicious malware. I also have a background in computer science and physics.

Going over ransomware we are looking at financially motivated cybercrimes. Cybercriminals are constantly evolving and changing their technique. As we develop new techniques for finance on the internet – cybercriminals are finding ways to attack those methods.

In early 2000s we were working on E-Commerce, where people could buy things online. The main cybercrime at that time was SQL Injection. That allowed them to access credit card data on these websites. As time moved towards online banking – cyber criminals became more sophisticated and moved towards banking Trojans which allow them to steal individual's usernames and IDs to access the online banking sites and send the wire transcripts.

With the conversion of cryptocurrency and the movement towards it in the late 2010s – we see the transition towards ransomware, allowing them to transfer money through Bitcoin to the cybercriminals without having to deal with banks and working with transfers. Overall there is a number of different financially motivated cybercrimes, based on the industry and the technologies in this particular industry.

Ransomware is a malware that will encrypt your system. When you get up on your computer on your server – you won't have access to anything and there might be one file that you can access. The file will look similar to a locked system that gives you instructions what to do and how to make payment in order to decrypt. In the last couple of years' cybercriminals also doing an exfiltration of

data engaging double extortion. Double extortion is essentially works for ransomed payment, decrypting your data and not publish your data online. As you can imagine for companies having a data published online is a significant concern that impacts their trade secrets, communication and trust among their clients.

We are also seeing in the last couple of years' ransomware as a service. Cybercriminals aren't simply engaging in ransomware, but they are packaging the ransomware as a service and making it available to all people.

This has some unique effects. Most significant impact – it is casing a massive increase in ransomware attacks, because no longer do sophisticated actors need to have access to ransomware. As a result, in 2019 was a 485% increase in ransomware attack and in the first half of 2021 – 93% increase. It mirrored with a lot of people telecommuting and working from home and use ransomware as a service.

Here are some statistics:

From January to September 2021: ~ 500 million attempted ransomware attacks (SonicWall)

2020: $312,493 average payment (Palo Alto Networks)

2020: $350 million payments (Chainanalysis)

This is a significant volume of money and it's a significant successful business.

When you are hit with ransomware – your systems are down and you need to hire a forensics team to immediately take measures, so you have lost time and opportunity costs and you will spend a lot of efforts and valuable business hours of your employees to get your system back to work. In addition, you are going to have to engage in negotiation and payments. Often time it is overwhelming and unknown to individuals. There are now third-party services to help on these aspects. There is also a reputational harm and adverse media attention.

– Legal considerations:

– Data Breach Notification Laws. Companies must provide notices to regulators, to individuals and that's true across multiple jurisdictions, not only in the US, and multiple countries are moving to that model.

– Litigation and Regulatory Enforcement Action. There is a significant increase in litigation for data breach matters and regulators are becoming far more aggressive in investigating companies – victim doing ransomware.

Overall ransomware's impact on victims is significant time, significant lost opportunity, significant headache and legal consequences and costs.

The last summer there was a major attack in USA, where there was a significant impact on supply chain and national security matters. As a result, law enforcement and government are concerned with the significant aggregate economic harm that ransomware has and national security harm.

The other significant impact is the overseas actors and organized criminal syndicates. Ransomware and cybercrime is unique in that and it requires a global approach.

– MLATs

– Budapest Convention

– Regulations on Cryptocurrency Exchanges.