ST. KITTS BRANCH
Financial SERVICES Regulatory Commission
NewsLetter

August 2023
Issue No. 111

Countering Ransomware Financing

What is Ransomware?

According to the Financial Action Task Force (FATF), ransomware is a malicious software (malware) that is developed by criminals to deny access to data, systems or networks while demanding a ransom payment in exchange. Common attack methods include **data encryption**, **data exfiltration** and the disruption of operations. Attacks often involve more than one method and may include a threat to publish the victim's data.

Ransomware attacks have caused major disruption and damage for governments, public institutions, businesses and citizens, in some cases impacting healthcare and threatening national security. Ransomware criminals have developed techniques to increase the profitability of their attacks and the chances of success. As a result, the threat of illicit flows related to ransomware continues to grow. Ransom amounts can range from hundreds of dollars to millions targeting individuals to large corporations.

Sectors that may be involved in Ransomware Financial Flows

The financial flows related to ransomware often involve multiple traditional Financial Institutions (FIs) as well as Virtual Asset Service Providers (VASPs). Other third party establishments such as cyber insurance companies, incident response companies or cybersecurity companies may also be involved in the response to a ransomware attack.

- *Financial Institutions:* FIs may act as intermediaries that ransomware victims use for sending funds to a VASP for the purchasing of virtual assets.
- *Insurance Companies:* These companies may cover and pay a ransom as part of the cyber insurance coverage.
- *Virtual Asset Service Providers:* Victims use VASPs to purchase and transfer the particular type and amount of virtual asset specified by the ransomware criminal.
- *Incident Response Companies:* These are often contracted by ransomware victims to negotiate the ransom payment with attackers.
- *Cybersecurity Companies:* These may be contracted after the ransomware attack to safeguard the client from further attacks.

Common Ransomware Typologies

Conducting successful investigations into ransomware attacks require a sound understanding of the methods and techniques used to launder funds.

1. Ransomware criminals demand payment almost exclusively in virtual assets.
2. Over half of all reported ransomware attacks are against victims in the government/ public sector, healthcare and industrial goods and services sectors.
3. Ransomware criminals often use anonymity enhancing technologies, techniques and tokens to receive illicit proceeds such as wallets and privacy coins.
4. Money Mules are also used to convert virtual currency to fiat currency by using off-ramps which are platforms that allow for the exchange of virtual assets to fiat currency. These accounts are often created using stolen or fake identification.
5. Ransomware criminals often send the virtual assets to VASPs in high risk jurisdictions or to a VASP with weak or non existent AML/CFT controls.

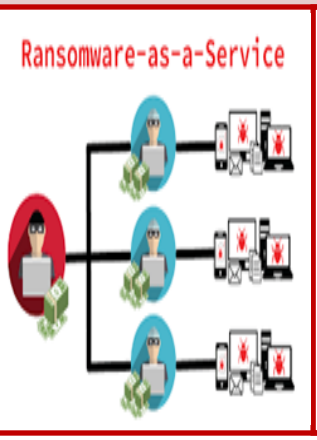
IN THIS ISSUE

RANSOMWARE TECHNIQUES

Big Game Hunting

This practice involves ransomware criminals targeting large, high-value organizations or high-profile entities that they think are more likely to pay a ransom to resume business operations or avoid public scrutiny.

Ransomware criminals also target organizations holding sensitive or valuable information. Attackers believe that these organizations have a higher propensity to pay ransoms compared to other victims.

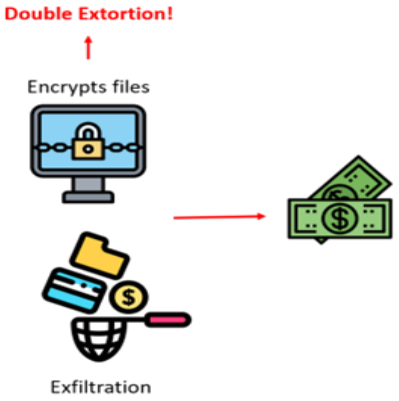


Ransomware-as-a-Service (RaaS)

This model involves criminals providing ransomware software kits on the Dark Web or outsourcing elements of ransomware attacks for a fee. These elements can include the distribution of malware, the initial compromising of a victim's network or ransom negotiation. The RaaS model has reduced the cost and necessary expertise to conduct ransomware attacks lowering the barriers to entry thereby allowing less sophisticated criminals to conduct ransomware attacks.

Double Extortion

This refers to a practice in which ransomware operators exfiltrate (steals or removes) a victim's data before encrypting it and then threaten to publish the stolen data if the ransom demands are not met. The additional threat of publication may put additional pressure on the victims to pay the ransom demands even if they are able to restore operations.



Triple Extortion

This refers to a practice where ransomware operators seek money not only from the victim that was first targeted but also from a victim who might be implicated by the disclosures of the original victim's data such as protected health information, personally identifiable information, account credentials and intellectual property.

Multiple Extortion

This practice involves more than two (2) methods of extortion. It is based on double extortion using encryption and exfiltration but includes additional pressure tactics such as denial of service, contacting the victim's customers, short selling the victim's stocks and disrupting systems.

Good Practices in Disrupting Ransomware Attacks on Your Organization

Being aware and following these steps can help to prevent ransomware attacks in your organization.

A. Educate Employees: Knowing about the warning signs and safe practices aid tremendously in preventing ransomware attacks.

B. Manage the Use of Privileged Accounts: Restrict the installation of software applications on network devices to limit network exposure to malware.

C. Employ a Data Backup and Recovery Plan for all critical data.

D. Ensure that all business devices are updated.

Discussion Question: What is the difference between data exfiltration and data encryption?

CONTACT US
For More Information

References:

Countering Ransomware Financing: Financial Action Task Force (FATF) Report March 2023

South Independence Square Street, P.O. Box 898, Basseterre, St. Kitts
Tel: (869) 466-5048 | 467-1019/1591 Fax: (869) 466-5317
Website: www.fsrc.kn / Email: info@fsrc.kn