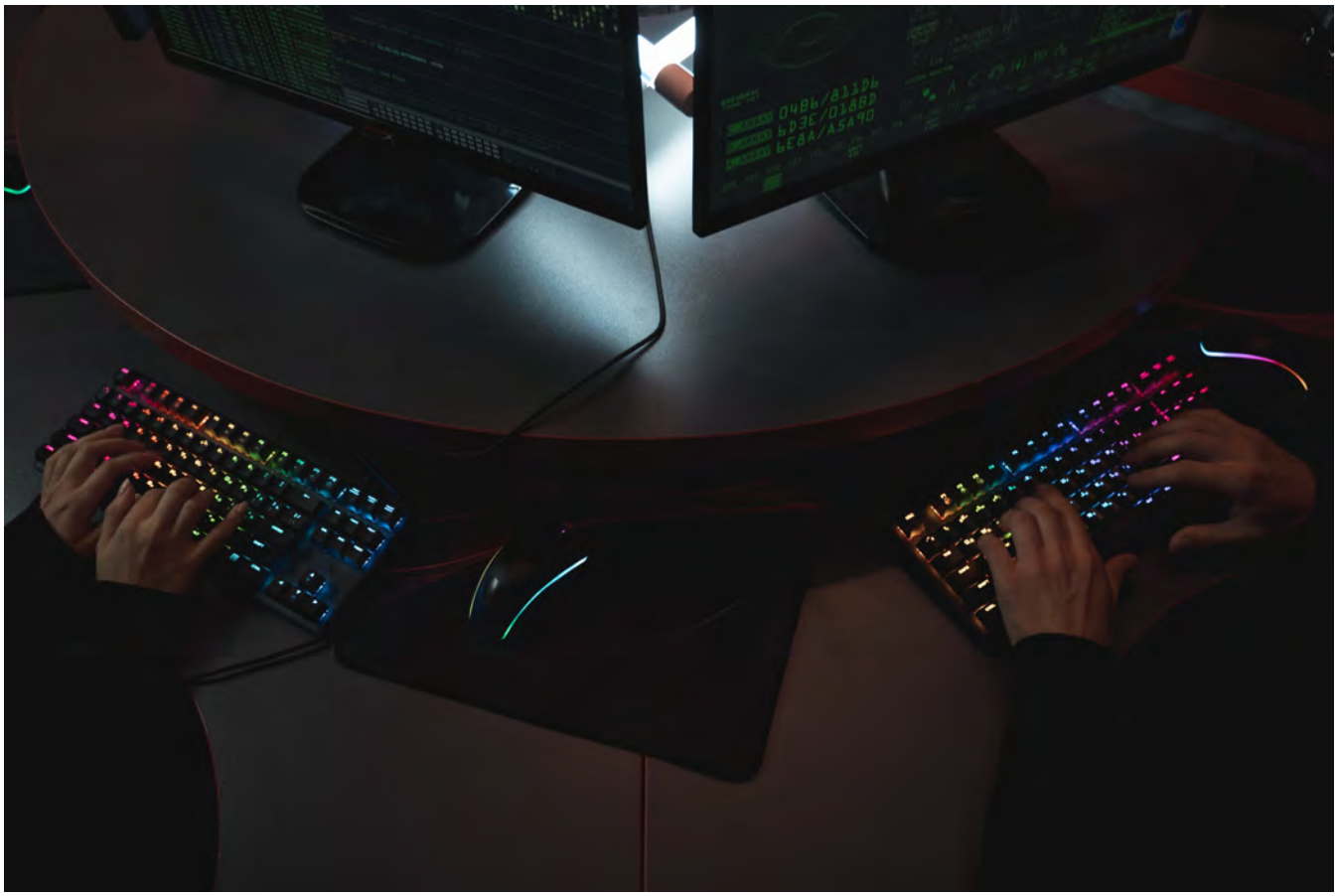
AURORA

Ransomware: A Cryptocurrency-Fueled Criminal Enterprise



aurorait.com
sales@aurorait.com
888-282-0696

Introduction

In today's fast-evolving and digitized world, cyber threats have become an unfortunate reality for businesses, governments, and individuals alike, causing notable financial damage for those unequipped to fight back or recover. The saying "crime never sleeps" does not escape cybercrime as cybercriminals constantly step up their games to generate higher returns faster with less effort. Meanwhile, businesses and governments try to keep up with the latest attack trends by investing in cybersecurity to lessen the financial, economic, environmental, safety, or reputational impact of a severe cyber-attack. One of the most ingenious attacks of all time is arguably ransomware, a software designed to encrypt computer files in exchange for a ransom payment. The first ransomware attack surfaced in the 1980s, but the technique did not get notoriety until the early 2000s following the emergence of Bitcoin. Before Bitcoin, ransomware cyberthieves operated on a small scale, receiving their fees for restoring their victims' files and computers through US dollars or online money transfer services, such as Ukash or PaySafeCard in the European Union and GreenDot MoneyPak in the United States. The cryptocurrency ecosystem allowed attackers to execute large-scale attacks with minimal risk of getting caught through a digitally distributed system designed to move money anonymously.

While most successful ransomware attacks create direct financial impact, some industries can also suffer socio-economic, environmental, and safety consequences, as attested by the recent fuel shortages across the nation caused by the Colonial Pipeline post-ransomware shutdown. Ransomware has proven to be very profitable for cybercriminals. It will likely continue to grow in popularity unless the issues enabling these attacks are addressed (lack of jurisdiction, anonymity, and unregulated currency). Therefore, organizations should design and implement defensible security programs to prevent or otherwise quickly recover from a ransomware attack, including developing disaster recovery plans and purchasing cyber insurance policies to alleviate the resulting financial and operational burden. ‘

From a petty crime thirty years ago to one of the most profitable criminal operations worldwide, this paper examines the evolution of ransomware, describing the anatomy of the infamous attack, the debate of paying the ransom, and the steps organizations can take to lessen the impact of a successful attack.

The Rise of Ransomware

Ransomware made its first debut in 1989 with the emergence of AIDS (AKA PC Cyborg virus), a trojan horse developed by Joseph Popp delivered to its victims in floppy disks after attending the World Health Organization's AIDS conference. The business model for ransomware was fundamentally different back then and far more straightforward than today, demanding smaller ransom payments sent via regular postal service.

The expansion and accessibility of the Internet combined with technology evolution allowed individuals and organizations to increase their digital footprint and become more connected. As Internet access rates and computer prices dropped, the number of Internet-connected devices increased proportionally, allowing attackers to deliver the ransomware in high volumes through massive phishing campaigns. In the low hundreds of dollars, the ransom demands were typically small, but attackers relied on high volumes of successful infections and payments to stay afloat.

Now, the operations are much more involved, and the stakes are much higher. Cybercriminals have shifted their focus to enterprises and government entities. Some organized groups now even hire experienced hackers to find and compromise big targets capable of paying out huge ransoms if infected. The hackers then sell the access credentials to the organized groups, who then carry out the ransomware attack. Everyone gets paid so abundantly that ransomware has become a multibillion-dollar industry.

According to a recent report by eSentire, more than 290 organizations have suffered different variants of damaging ransomware attacks during the first part of 2021, with an estimated associated financial loss of at least forty-five million dollars. Furthermore, according to Bitdefender, ransomware attacks increased 485% in 2020 globally, accounting for nearly one-quarter of all cyber incidents, with total global costs estimated at twenty billion dollars.

A new business model adopted by sophisticated attackers consists of developing and selling ransomware toolkits that can be downloaded and deployed by less skillful attackers. Ransomware-as-a-service is another common monetization technique that has led to some renowned ransomware attacks, including CryptoLocker, CryptoWall, Gandcard, and many more. Let's reflect on some of the ransomware variants that have claimed significant payouts over the years.

Sources:
https://www.esentire.com/resources/library/six-ransomware-gangs-claim-290-new-victims-in-2021-potentially-reaping-45-million-for-the-hackers
https://www.bitdefender.com/news/new-bitdefender-report-reveals-top-global-cyberthreats-3977.html

aurorait.com
sales@aurorait.com
888-282-0696

The Rise of Ransomware

In early May, a Russian hacking group by Darkside's name launched a successful ransomware attack against Colonial Pipeline, resulting in a significant socio-economic impact. The company's pipeline extends from Texas to New Jersey and delivers nearly half of the transport fuels for the Atlantic Coast. Colonial Pipeline pre-emptively shut down its pipeline upon detecting the attack, setting off a cascading crisis across the nation. Airlines were forced to make fuel stops on long-haul flights, gas prices increased, and people began panic-buying at the pumps. According to recent reports by The Wall Street Journal, Colonial Pipeline ended up paying a seventy-five Bitcoin ransom or nearly five million dollars to recover its inaccessible data.
Around the same time, JBS Meat Supplier was infected by ransomware by another major Russian hacking group, ReVIL. JBS paid eleven million dollars in ransom to get back their stolen data. Both attacks had dramatic socio-economic and financial impacts, causing supply constraints and panic.

In early June, the Biden administration made an unprecedented attempt to tackle this problem by bringing the ransomware crisis to the first face-to-face summit between Joe Biden and Vladimir Putin held in Villa La Grange in Geneva, Switzerland, proving the degree to which the threat of ransomware has grown.

Sources:
https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636

aurorait.com
sales@aurorait.com
888-282-0696

The Anatomy of a Ransomware Attack

Cybercriminals are undoubtedly in business to make money, using ransomware as extortion. While some criminals wait patiently for their ransom to clear, others go further to threaten organizations with leaking their information publicly unless the extortion is paid. Ransomware can find its way into organizations' systems through various vectors, including email phishing, Remote Desktop Protocol (RDP) connections, and technical software vulnerabilities. However, phishing has been the vector of choice to deliver the payload through malicious attachments and links. Power comes from knowledge, and knowledge provides information to take effective actions. Therefore, understanding the anatomy of ransomware is essential for building adequate countermeasures to prevent or otherwise detect and act on the threat.

Stage 1 - Recon and Initial Access

All cyber-attacks start with reconnaissance, where cybercriminals look for suitable organizations to target. Initial access follows reconnaissance and is the first active attack stage after cybercriminals have identified their target. In this stage, attackers attempt to deliver the payload via phishing or vulnerability exploitation or simply using valid credentials purchased from other criminals. The most commonly used vector is email phishing which attempts to trick victims into opening a malicious attachment that automatically infects their computer upon execution or clicking a link to a malicious site. Phishing links can take two forms, including a weaponized website designed to deliver the payload upon visiting it or a credential harvesting site created to steal users' credentials for later exploitation. Common countermeasures used in this phase include email and web security controls (e.g., secure email gateway and secure web gateway) and robust security awareness training programs to educate users on how to spot and report phishing emails.

Stage 2 - Infect & Persist

Infection and staging occur after the payload enters the target environment and is executed on the victim's system, where ransomware is installed. In this stage, the ransomware will embed itself in the target system and persist beyond a reboot.

At this stage, common preventive and detective measures include endpoint detection and response (EDR) software and security events monitoring.

Stage 3 - Scan and Encrypt

Scanning and encryption are the most damaging attack stages where ransomware scans local and network-attached file shares, searching for files to encrypt. Local files are encrypted almost immediately, and files stored in network shares quickly follow. Critical security measures at this stage include endpoint detection and response software, adequate access controls, and backups.

Stage 4 - Ransom

The last stage involves the ransomware generating a note for the victim containing the ransom demands, usually in Bitcoin, and the payment instructions. At the same time, the attackers wait to collect the payment in exchange for the key that will decrypt the hostage files.

aurorait.com
sales@aurorait.com
888-282-0696

Preventing Ransomware

While the saying "prevention is ideal, detection is a must" remains true for most cyber incidents, "prevention is ideal, recovery is a must" may be more appropriate for ransomware incidents. Organizations should consider ransomware a possible business continuity event and develop appropriate disaster recovery plans to overcome it quickly. Additionally, a defense-in-depth architecture will help slow the spread and lessen the impact. Below are some best practices that organizations can adopt to mitigate ransomware risks.

Perform Regular Backups
Availability of usable system backups is essential to enable quick recovery after suffering a ransomware attack. Organizations should conduct business impact assessments and establish recovery point and time objectives (RPO, RTO) for mission-critical systems to determine what to backup and for how long. Additionally, organizations should follow a regular backup testing schedule to ensure that they can successfully recover impaired systems to a known good state.

Conduct Security Awareness Training
Users are the first line of defense against social engineering attacks. Therefore, equipping information system users with the tools and knowledge needed to identify and report a phishing email could significantly increase the return on investment in terms of lowering the likelihood of initial compromise.

Enforce Least Privilege Access Control
Least privilege access control mechanisms ensure that only authorized entities (users, devices, and processes) can access resources needed to fulfill a specific task or objective. One of the most devastating stages of a ransomware attack is scanning and encrypting, where the ransomware scans local files and network shares, looking for files to encrypt.

Prioritize Vulnerability Management
Technical software vulnerabilities are another vector leveraged by attackers to deliver ransomware. Therefore, conducting regular vulnerability scans of information systems and adopting a strict patching regimen can greatly reduce the attack surface.

Enforce Network Segmentation
Network segmentation involves partitioning a network into smaller networks using mechanisms that control network traffic flow to make lateral movement more difficult. Organizations can limit the scope of a ransomware attack by granting users minimum permissions based on their roles.

Deploy an Endpoint Security Solution
Endpoint security continues to be one of the most effective ransomware mitigations. Symantec Endpoint Security is one solution we recommend to help protect your organization against all attack lifecycle phases. Pre-attack, Symantec Endpoint Security file-based protection quarantines notable ransomware file types or potentially unsafe files through its Virus and Spyware features, preventing their execution. During an attack, Symantec's Intrusion Prevention System (IPS) can help stop the file encryption process by blocking the command-and-control channel, preventing further damage to the system. Post-attack, the solution can provide targeted attack analysis, threat hunting, integrated response, and insights from expert SOC Investigators to help with breach recovery.

Fine-tune Security Event Detection
When everything else fails, detecting and responding to a security intrusion early in the attack kill chain is the last resort to prevent a ransomware attack.

aurorait.com
sales@aurorait.com
888-282-0696

Cryptocurrency and Ransomware

Cryptocurrency has undoubtedly fueled ransomware attacks during the last decade, creating a profitable criminal enterprise. And while some believe cryptocurrency is to blame for the ransomware rise and call on the Government to ban it, defending this position may be challenging. Necessity is the mother of innovation, and criminals are constantly finding new ways to exploit victims to increase and diversify their revenue streams. If the Government had banned cyrptocurrency ten years ago, would cybercriminals have found another equally profitable way to receive their fees? That is the question that bears asking.

Others call for Government regulations on cryptocurrency and its exchanges to provide protections similar to those regulating fiat currencies. Some cryptocurrency exchanges, such as Coinbase and Binance, have already implemented strong Know-Your-Customer (KYC) and Anti-Money Laundering (AML) processes similar to those used by banks to prevent fraud and stop money laundering.

aurorait.com
sales@aurorait.com
888-282-0696

The Future of Ransomware

Many of the cyberattacks observed in recent years have been attributed to Russian hacking organizations. Notorious groups like ReVIL (AKA Sodinokibi) and Darkside have already produced millions in ransom payments this year alone, and profits may continue to grow as cybercriminals grow more astute in refining their operations.

Ransomware is a globally evolving problem, affecting public and private organizations of all sizes across all industry sectors and promising potentially serious social, economic, financial, safety, and environmental consequences. The issue intensifies when basic human needs, such as water, food, and electricity, risk being obstructed by impaired critical infrastructure.

Ransomware tactics have evolved dramatically since the first-ever documented ransomware attack in 1989. Cybercriminals now employ double-extortion, threatening organizations with personal information disclosure unless the ransom is paid, which undoubtedly adds increasing pressure. Attackers know that companies without solid business continuity and disaster recovery plans are more likely to pay. Therefore, they are developing ransomware that persists on victim machines longer before encryption happens in an attempt to outlast backups.

Another tactic rising in popularity includes attackers cold-calling victims if they suspect the company will try to recover their systems from backups to suggest that any attempt at recovery will fail. The evilest tactic arguably involves targeting backup files directly, which would prevent successful restoration altogether, leaving organizations with no option but to pay.

On the positive side, a lot of information about ransomware, its variants, and how victim organizations failed to protect against the threat is available. With knowledge comes power, and with power comes the responsibility to learn from others' mistakes and take the necessary precautions to prevent becoming a victim or weather the storm and recover quickly and elegantly when all else fails.

About Aurora:

Aurora is an established premier partner of Symantec, a division of the Broadcom Software Group, and has deep knowledge and experience within Symantec's security portfolio. Our goal is to tailor Symantec's broad security solution sets to align with our clients' own needs and maximize their return on investment. At Aurora, we can help you improve your security posture to better prevent your organization against attacks like ransomware. Contact our sales team at sales@aurorait.com to learn more.

AURORA
A Plurilock Company

Symantec™
by Broadcom Software

aurorait.com
sales@aurorait.com
888-282-0696