RHYSIDA RANSOMWARE GANG

RANSOMWARE, CRYPTO VIRUS, , TROJAN, STEALER, FILES LOCKER

Vairav Advisory Report

6th September 2023

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977-1-4541540

Mobile: +977-9820105900

Email: mail@vairav.net

SUMMARY

In May 2023, the Ransomware-as-a-Service (RaaS) gang Rhysida first surfaced. This gang infiltrates networks and spreads its Rhysida-0.1 ransomware using phishing techniques and the Cobalt Strike framework. Their main method of operation includes threatening to leak stolen material to the public if a ransom is not paid. Rhysida lacks sophisticated features while being in its early phases of development. Infected files contain PDF messages attached to the ransomware and instruct users to contact the gang through their site and provide Bitcoin ransom payments. The victims of Rhysida come from all over the world, including Australia, North and South America, and Western Europe. Along with managed service providers, their main objectives are the manufacturing, technology, education, and government sectors. Notably, the Healthcare and Public Health (HPH) sector has recently seen intrusions. Organizations in a variety of industries are gravely concerned about this issue.

Introduction of Cyber Adversary

The origins or affiliations of the individuals who oversee Rhysida are only dimly known. Rhysida poses as a “cybersecurity team”, offering to assist victims in finding weaknesses in their network and systems, according to the Health Sector Cybersecurity Coordination Centre (HC3) notice. It's interesting to note that the group only surfaced after a victim chat support portal was established.

Key Points

- It is a RaaS group that spreads ransomware via phishing and Cobalt Strike.
- They utilize tools like PsExec and PowerShell to compromise security, delete backups, alter RDP settings, and change AD passwords.
- They encrypt files using a robust 4096-bit RSA key and AES-CTR.
- The .rhysida extension is added to the encrypted files.
- A multipurpose tool is used in the attack, PS1.SILENTKILL.A
- The report highlights the emergence of Rhysida as a significant ransomware threat targeting a wide range of sectors, including healthcare and public health, which have seen an alarming increase in ransomware attacks.

Tactics, Techniques, and Procedure

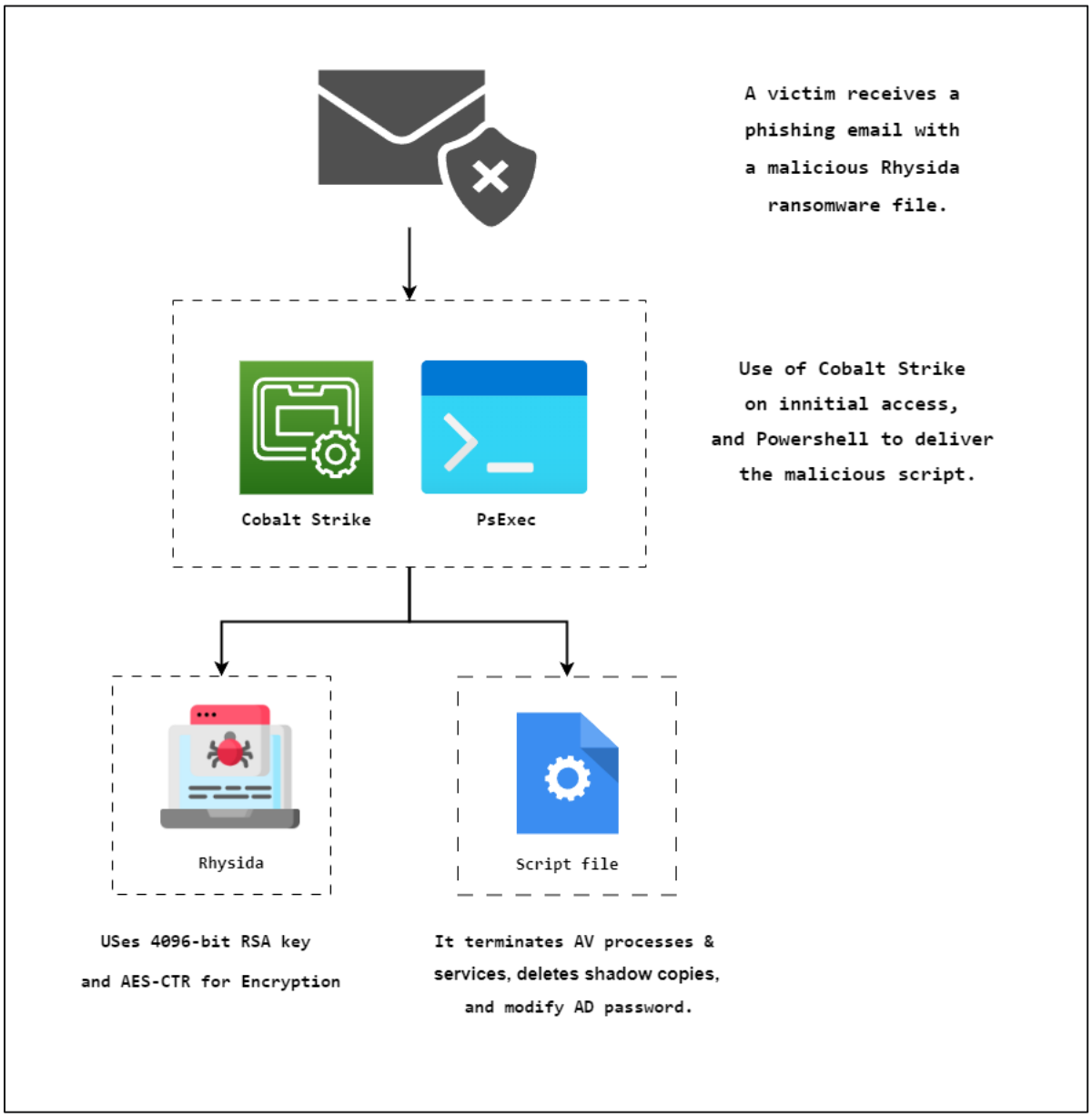

Figure 1: Infection chain of Rhysida ransomware.

Rhysida ransomware often gains access to a victim's computer by deceptive phishing techniques, and once inside, it uses Cobalt Strike for lateral system movement. When deploying the Rhysida ransomware payload itself and running PowerShell scripts, threat actors use PsExec. the PowerShell script, often known as Trojan, with the filename "g.ps1". A multipurpose tool is used in the attack, PS1.SILENTKILL.A. It is used to end antivirus software-related activities and services, remove shadow copies, change RDP configurations, and change the password for the active directory (AD).

Notably, it is discovered that the threat actors have updated the script (g.ps1) during execution, which finally results in the appearance of a PowerShell variant of the Rhysida ransomware. AES-CTR encryption and a strong 4096-bit RSA key are used by the Rhysida ransomware to lock victim files. The **.rhysida** extension is added to the encrypted files once the ransomware has successfully encrypted them, and it also leaves a ransom note with the filename **CriticalBreachDetected.pdf**.

The ransomware implements its encryption process using the open-source cryptography package LibTomCrypt.

```
if ( !init_prng(&prng, &PRNG_IDX) )
{
  for ( thread_i = 0; thread_i < PROCS; ++thread_i )
  {
    if ( init_prng(prngs + 17648 * thread_i, PRNG_IDXS + thread_i) )// Initialize ChaCha20 PRNG (Pseudo-Random Number Generator) for each thread
      goto LABEL_46;
  }
  if ( !rsa_import(&_PUB_DER, _PUB_DER_LEN, &key) )// Import RSA key
  {
    err = register_cipher(&refptr_aes_enc_desc);// Register AES cipher to the list of usable ciphers.
    if ( !err )
    {
      CIPHER = find_cipher("aes");          // Declaration of CIPHER to be used from the list
      if ( CIPHER != -1 )
      {
        err = register_hash(&refptr_chc_desc);// Register CHC Hash Algorithm
        if ( !err )
        {
          err = chc_register(CIPHER);       // Register AES to CHC Hash
          if ( !err )
          {
            HASH_IDX = find_hash("chc_hash");
            if ( HASH_IDX != -1 )
            {
              _aes_keysize = 32;
              err = rijndael_keysize(&_aes_keysize);
```

Figure 2: Rhysida's encryption setup process.

Rhysida generates keys and initialization vectors (IV) using LibTomCrypt's pseudorandom number generator (PRNG) features. The PRNG functions are initialized using the init_prng function. The ChaCha20 PRNG feature of the library is utilized by the malware.

```
*n = register_prng(refptr_chacha20_prng_desc);// Register ChaCha20 PRNG
if ( *n == -1 )
  return 1i64;
if ( chacha20_prng_start(prng_val) )          // Setup PRNG for future use
  return 2i64;
err = chacha20_prng_ready(prng_val);          // Check if PRNG is ready
if ( err )
  return 3i64;
for ( i = 0; i <= 39; ++i )
  prng_entr[i] = rand() * (*n + i + 1);
err = chacha20_prng_add_entropy(prng_entr, 40i64, prng_val);// Add Seed/Entropy to PRNG
if ( err )
  return 4i64;
v3 = rand();
v6 = (((v3 >> 31) >> 24) + v3) - ((v3 >> 31) >> 24) + 1;
Block = malloc(v6);
chacha20_prng_read(Block, 8u, prng_val);
free(Block);
```

Figure 3: Use of ChaCha20 PRNG functionality.

Rhysida imports the embedded RSA key when the PRNG is initialized, and it then specifies the encryption scheme it will employ to encrypt files. Initially, it employs the register_cipher function to formally enlist the "AES" algorithm within its roster of usable ciphers. Subsequently, the find_cipher function is utilized to retain this algorithm, still denoted as AES, within the variable named CIPHER. Following this, it proceeds to register and declare AES for its Cipher Hash Construction (CHC) functionalities.

Rhysida's encryption routine follows these steps:

Step 1: After reading the file contents for encryption, it employs the initialized PRNG's chacha20_prng_read function to create unique keys and IVs for each file.

Step 2: It initializes the cipher (in this case, AES from the variable CIPHER) for use in counter (CTR) mode using the ctr_start function.

Step 3: The generated key and IV are encrypted using the rsa_encrypt_key_ex function.

Step 4: Subsequently, Rhysida proceeds to encrypt the file using LibTomCrypt's ctr_encrypt function.

```
chacha20_prng_read(cipher_key, 32u, prngs + 17648 * thread_n);// Generate Key using chacha20 PRNG
chacha20_prng_read(cipher_iv, 16u, prngs + 17648 * thread_n);// Generate IV using chacha20 PRNG
v27 = ctr_start(CIPHER, cipher_iv, cipher_key, 32u, 14u, 16, ctr);// Initialize CTR Cipher
if ( v27 )
{
  pthread_mutex_unlock(&MUTEX_PRNG);
}
else
{
  v27 = ctr_setiv(cipher_iv);
  Size_4 = 32;
  ElementSize_4 = 4096;
  v27 = rsa_encrypt_key_ex(
          cipher_key,
          0x20ui64,
          Buffer,
          &ElementSize_4,
          "Rhysida-0.1",
          11,
          prngs + 0x44F0 * thread_n,
          PRNG_IDX,
          HASH_IDX,
          2,
          &key);                        // Encrypt Generated Key
```

Figure 4: Generation of Encrypt key.

The Rhysida ransom note stands out for its unique methodology. Unlike most ransom notes used by other ransomware families, the Rhysida ransom message seems to be a warning from the Rhysida cybersecurity team. It notifies victims that their data has been encrypted and that their machine has been hacked. Instead, then making a straightforward ransom demand, the message informs victims that they must pay to receive a "unique key" to retrieve their encrypted data.

MITRE ATT&CK techniques

The malware makes the usage of various attack tactics, techniques, and procedures based on the MITRE ATT&CK framework to attack victimized users or organizations.

Tactic	Technique
Initial Access	Phishing (T1566)
Execution	Command and Scripting Interpreter (T1059) • PowerShell (T1059.001) • Windows Command Shell (T1059.003)
Persistence	Boot or Logon Auto start Execution (T1547) • Registry Run Keys/ Startup Folder (T1547.001)
	Scheduled Task/ Job (T1053) • Scheduled Task (T1053.005)
Defense Evasion	Indicator Removal (T1070) • Clear Windows Event Logs (T1070.001) • File Deletion (T1070.004)
Discovery	File and Directory Discovery (T1083)
	System Information Discovery (T1082)
Impact	Data Encrypted for Impact (T1486)
	Inhibit System Recovery (T1490)
	Defacement (T1491) • Internal Defacement (T1491.001)

Indicators of Compromise (IOCs)

SHA1	Detection Names
69b3d913a3967153d1e91ba1a31ebed839b297ed	Ransom.Win64.RHYSIDA.THEBBBC
338d4f4ec714359d589918cee1adad12ef231907	Ransom.Win64.RHYSIDA.THFOHBC
b07f6a5f61834a57304ad4d885bd37d8e1badba8	Ransom.Win64.RHYSIDA.SM
7abc07e7f56fc27130f84d1c7935a0961bd58cb9	TrojanSpy.Win32.INVICTASTEALER.A
2543857b275ea5c6d332ab279498a5b772bd2bd4	TrojanSpy.Win32.INVICTASTEALER.A
eda3a5b8ec86dd5741786ed791d43698bb92a262	Trojan.LNK.DOWNLOADER.AA
rhysidaeverywhere@onionmail.org	Email
rhysidaofficial@onionpmail.org	Email
rhysidafohrhyy2aszi7bm32tnjat5xri65fopcxkdfxhi4tidsg7cad.onion	Domain
http://rhysidafohrhyy2aszi7bm32tnjat5xri65fopcxkdfxhi4tidsg7cad.onion	Email
ransom.win64.rhysida.sm	Hostname
ransom.ps1.rhysida.sm	Hostname
rhysidal.website	Domain
0220083d724fdb8a406d3e780497561590804281	YARA

Threat Summary	
Name	Rhysida Ransomware
Threat Type	Encryption
Detection Names	Ransomware, Crypto Virus, Trojan, Stealer, Files Locker
Symptoms	If names with an extension like "**.rhysida**" is found in the infected system.
Additional Information	It's important to keep in mind that it may not be the only malware present in an infected system. It can work in conjunction with other malicious samples and can be downloaded by notorious Trojans.
Distribution methods	Phishing techniques
Damage	Steal sensitive information, data loss, downtime, and financial loss.
Malware Removal (Windows)	Use reputable antivirus software to run a full system scan and remove all detected files and objects.

Vairav Recommendations

Here are several recommended measures that organizations should implement to protect their systems from ransomware attacks, along with brief explanations for each:

Create an inventory of assets and data: Organizations should maintain a comprehensive inventory of their digital assets and sensitive data. This helps in identifying potential vulnerabilities and prioritizing security efforts.

Review event and incident logs: Regularly monitoring event and incident logs allows organizations to detect suspicious activities and respond promptly to security incidents, potentially preventing ransomware attacks.

Manage hardware and software configurations: Properly configuring hardware and software reduces the attack surface and minimizes vulnerabilities that ransomware can exploit.

Grant administrative privileges and access only when relevant: Limiting administrative privileges to authorized personnel and providing access based on job roles and responsibilities helps prevent unauthorized access and reduces the risk of ransomware infections.

Enforce security configurations on network infrastructure devices: Implementing robust security configurations on network devices like firewalls and routers helps block malicious traffic and protect against ransomware attacks.

Establish a software whitelist: Creating a whitelist that permits only legitimate applications to run on the network helps prevent the execution of malicious software.

Perform routine vulnerability assessments: Regular vulnerability assessments identify weaknesses in the network, allowing organizations to proactively address and patch potential entry points for ransomware.

Apply patches or virtual patches: Promptly applying security patches and virtual patches for operating systems and applications closes known vulnerabilities, making it more difficult for ransomware to exploit them.

Keep software and applications up to date: Running the latest versions of software and applications ensures that organizations benefit from the latest security features and patches.

Integrate data protection, backup, and recovery protocols: Robust data protection, backup, and recovery strategies ensure that critical data can be restored in the event of a ransomware attack, reducing the incentive to pay a ransom.

Enable multifactor authentication (MFA): MFA adds an additional layer of security by requiring users to provide multiple forms of verification, making it more challenging for attackers to gain unauthorized access.

Utilize sandbox analysis: Implementing sandbox analysis for email attachments can help intercept and quarantine potentially malicious emails, preventing ransomware infections from spreading.

Regularly educate and evaluate employees' security aptitude: Employee training and awareness programs educate staff about ransomware threats and empower them to recognize and report suspicious activities.

Deploy security tools (such as XDR): Utilizing advanced security tools like Extended Detection and Response (XDR) can help detect and respond to ransomware attacks by identifying the abuse of legitimate applications and patterns of suspicious behavior.

It is important to remember that cyber adversaries are likely to constantly evolve their methods, tools, and techniques to evade detection and continue to be successful in their attacks. Therefore, organizations and individuals must stay informed about the latest TTPs and take proactive steps to protect themselves.

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-1-4541540

Mobile: +977-9820105900

Email: mail@vairav.net

Website: https://vairav.net