



Ransomware

# An Overview of the New Rhysida Ransomware Targeting the Healthcare Sector

In this blog entry, we will provide details on Rhysida, including its targets and what we know about its infection chain.

By: Trend Micro Research

August 09, 2023

Read time: 7 min (1936 words)



*Updated on August 9, 2023, 9:30 a.m. EDT: We updated the entry to include an analysis of current Rhysida ransomware samples' encryption routine.*

*Updated on August 14, 2023, 6:00 a.m. EDT: We updated the entry to include Trend XDR workbench alerts for Rhysida and its components.*

## Introduction



RANSOMWARE (RHYSIDA.SM), which has been active since May 2023. In this blog entry, we will provide details on Rhysida, including its targets and what we know about its infection chain.

## Who is behind the Rhysida ransomware?

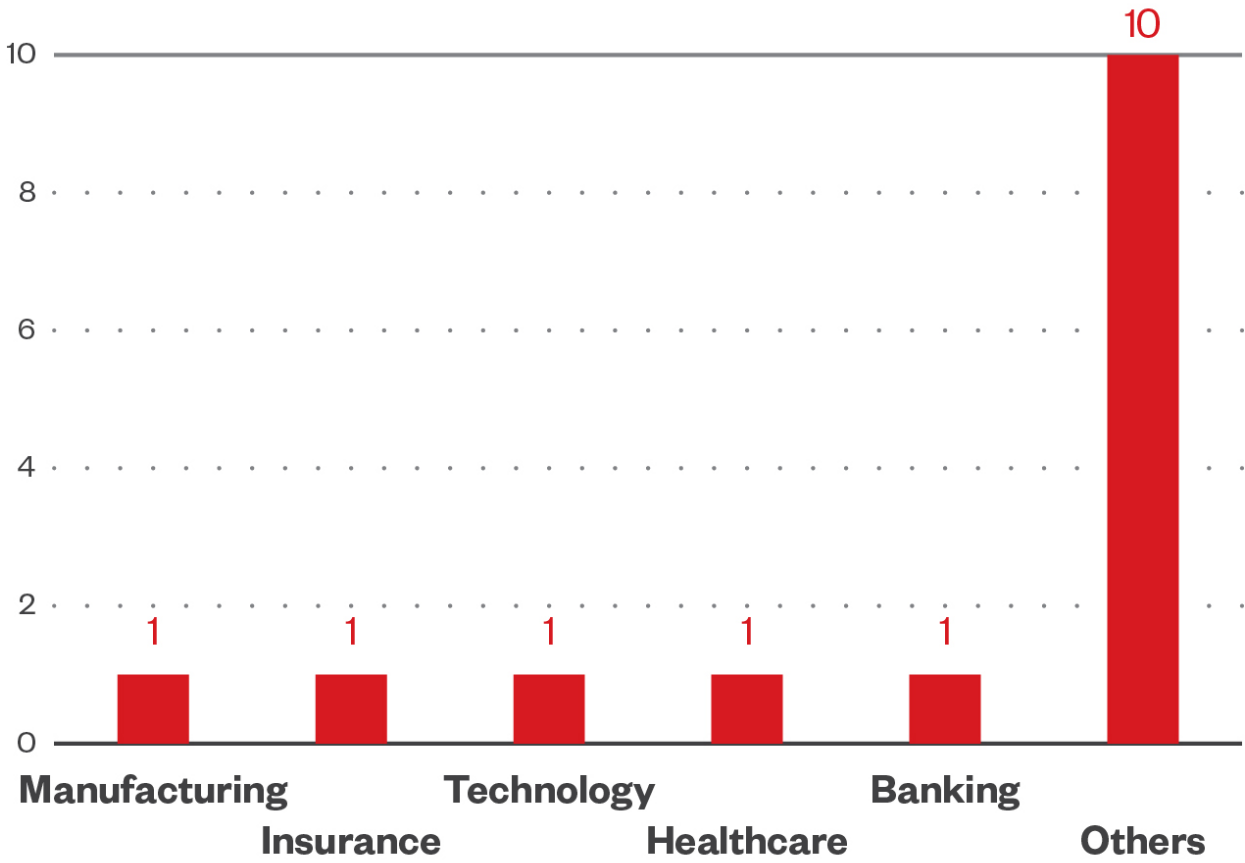
Not much is currently known about the threat actors behind Rhysida in terms of origin or affiliations. According to the HC3 alert, Rhysida poses itself as a “cybersecurity team” that offers to assist victims in finding security weaknesses within their networks and system. In fact, the group’s first appearance involved the use of a victim chat support portal.

## Who are Rhysida’s targets?

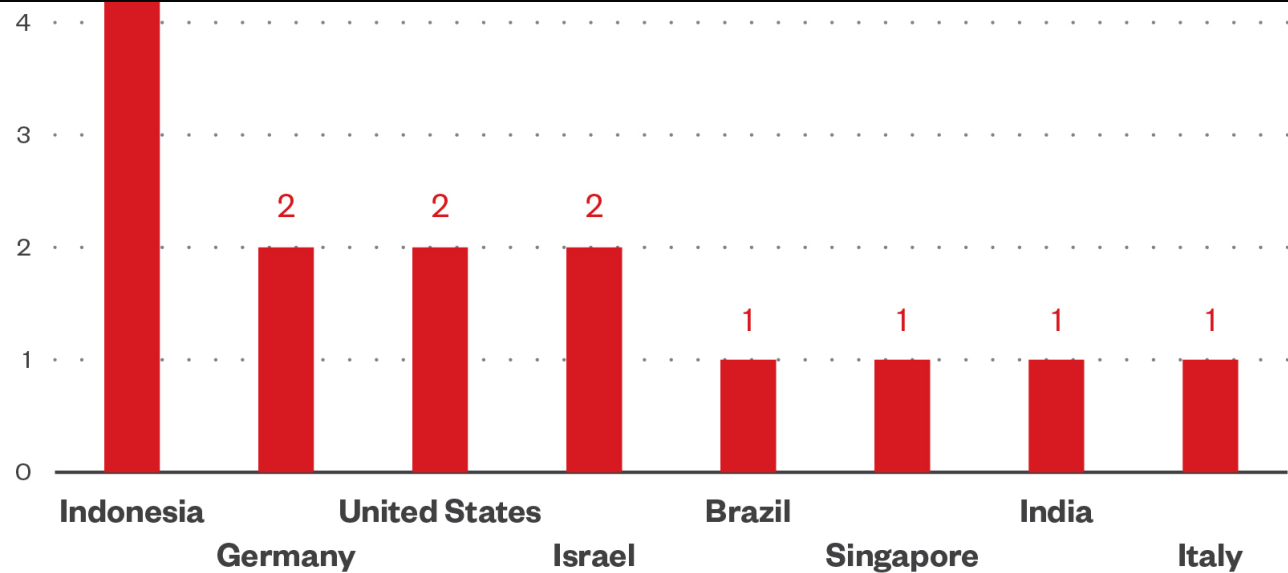
As mentioned earlier, Rhysida, which was previously known for targeting the education, government, manufacturing, and tech industries, among others — has begun conducting attacks on healthcare and public health organizations. The healthcare industry has seen an **increasing number of ransomware attacks** over the past five years. This includes a recent **incident** involving Prospect Medical Holdings, a California-based healthcare system, that occurred in early August (although the group behind the attack has yet to be named as of writing).

Data from Trend Micro™ Smart Protection Network™ (SPN) shows a similar trend, where detections from May to August 2023 show that its operators are targeting multiple industries rather than focusing on just a single sector.

and the United States.



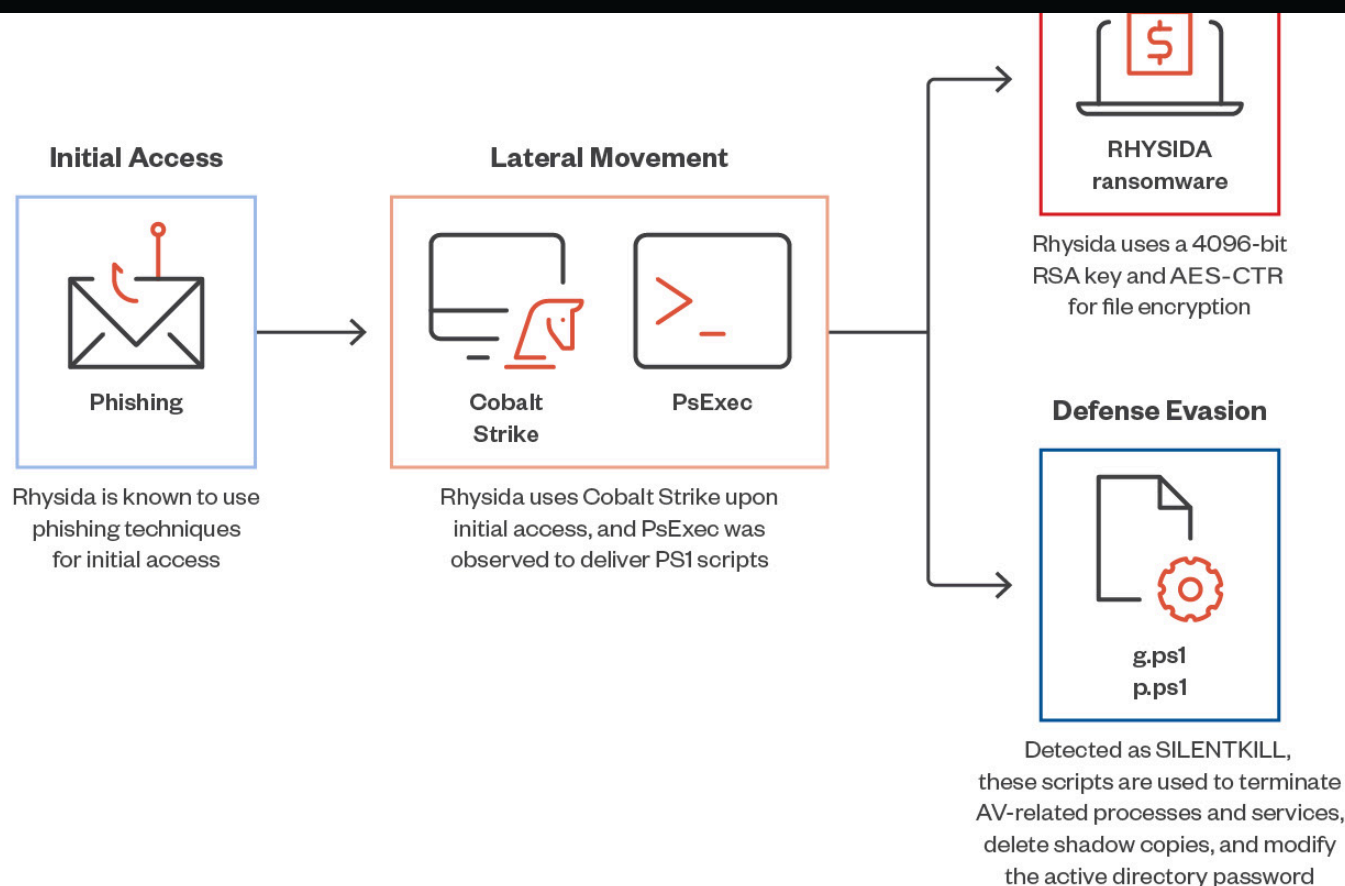
© 2023 TREND MICRO



© 2023 TREND MICRO

Figure 1. The industry and country detection count for Rhysida ransomware based on Trend SPN data from May to August 2023

# How does a Rhysida attack proceed?



© 2023 TREND MICRO

Figure 2. The Rhysida ransomware infection chain

Rhysida ransomware usually arrives on a victim's machine via phishing lures, after which Cobalt Strike is used for lateral movement within the system.

Additionally, our telemetry shows that the threat actors execute PsExec to deploy PowerShell scripts and the Rhysida ransomware payload itself. The PowerShell script (g.ps1), detected as Trojan.PS1.SILENTKILL.A, is used by the threat actors to terminate antivirus-related processes and services, delete shadow copies, modify remote desktop protocol (RDP) configurations, and change the active directory (AD) password.

Rhysida ransomware employs a 4096-bit RSA key and AES-CTR for file encryption, which we discuss in detail in a succeeding section. After successful encryption, it appends the .rhysida extension and drops the ransom note CriticalBreachDetected.pdf.

This ransom note is fairly unusual — instead of an outright ransom demand as seen in most ransom notes from other ransomware families, the Rhysida ransom note is presented as an alert from the Rhysida “cybersecurity team” notifying victims that their system has been compromised and their files encrypted. The ransom demand comes in the form of a “unique key” designed to restore encrypted files, which must be paid for by the victim.

## Summary of malware and tools used by Rhysida

- **Malware:** RHYSIDA, SILENTKILL, Cobalt Strike
- **Tools:** PsExec

|                  |                    |  |
|------------------|--------------------|--|
| Initial Access   | Phishing           | Based on external reports, Rhysida uses phishing lures for initial access  |
| Lateral Movement | PsExec             | Microsoft tool used for remote execution   |
|                  | Cobalt Strike      | 3 <sup>rd</sup> party tool abused for lateral movement   |
| Defense Evasion  | SILENTKILL         | Malware deployed to terminate security-related processes and services, delete shadow copies, modify RDP configurations, and change the AD password |
| Impact           | Rhysida ransomware | Ransomware encryption  |

## A closer look at Rhysida's encryption routine

After analyzing current Rhysida samples, we observed that the ransomware uses **LibTomCrypt**, an open-source cryptographic library, to implement its encryption routine. Figure 3 shows the procedures Rhysida follows when initializing its encryption parameters.

```
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 3. Rhysida's parameters for encryption

Rhysida uses LibTomCrypt's pseudorandom number generator (PRNG) functionalities for key and initialization vector (IV) generation. The *init\_prng* function is used to initialize PRNG functionalities as shown in Figure 4. The same screenshot also shows how the ransomware uses the library's ChaCha20 PRNG functionality.

```
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 4. Rhysida's use of the "init\_prng" function

After the PRNG is initialized, Rhysida then proceeds to import the embedded RSA key and declares the encryption algorithm it will use for file encryption:

- It will use the *register\_cipher* function to "register" the algorithm (in this case, aes), to its table of usable ciphers.
- It will use the *find\_cipher* function to store the algorithm to be used (still aes), in the variable CIPHER.

Afterward, it will proceed to also register and declare aes for its Cipher Hash Construction (CHC) functionalities.

Based on our analysis, Rhysida's encryption routine follows these steps:

1. After it reads file contents for encryption, it will use the initialized PRNG's function, *chacha20\_prng\_read*, to generate both a key and an IV that are unique for each file.
2. It will use the *ctr\_start* function to initialize the cipher that will be used, which is aes (from the variable CIPHER), in counter or CTR mode.
3. The generated key and IV are then encrypted with the *rsa\_encrypt\_key\_ex* 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 5. Rhysida's encryption routine

## How can organizations protect themselves from Rhysida and other ransomware families?



Although we are still in the process of fully analyzing Rhysida ransomware and its tools, tactics, and procedures (TTPs), the best practices for defending against ransomware attacks still holds true for Rhysida and other ransomware families.

Here are several recommended measures that organizations implement to safeguard their systems from ransomware attacks:

- Create an inventory of assets and data
- Review event and incident logs
- Manage hardware and software configurations.

TREND MICRO

Business



- Establish a software whitelist permitting only legitimate applications
- Perform routine vulnerability assessments
- Apply patches or virtual patches for operating systems and applications
- Keep software and applications up to date using their latest versions
- Integrate data protection, backup, and recovery protocols
- Enable multifactor authentication (MFA) mechanisms
- Utilize sandbox analysis to intercept malicious emails
- Regularly educate and evaluate employees' security aptitude
- Deploy security tools (such as XDR) which are capable of detecting abuse of legitimate applications

## Indicators of compromise

### Hashes

The indicators of compromise for this entry can be found [here](#).

## MITRE ATT&CK Matrix

|                |  |   |
|----------------|--|---|
| Initial Access | T1566 Phishing   | Based on external reports, Rhysida uses phishing lures for initial access.                |
| Execution      | T1059.003 Command and Scripting Interpreter: Windows Command Shell | It uses cmd.exe to execute commands for execution.  |
|                | T1059.001 Command and Scripting Interpreter: PowerShell            | It uses PowerShell to create scheduled task named <i>Rhsd</i> pointing to the ransomware. |

|                 |   |  |
|-----------------|---|--|
| Defense Evasion | T1070.004 Indicator Removal: File Deletion            | Rhysida ransomware deletes itself after execution. The scheduled task (Rhds) created would also be deleted after execution.  |
|                 | T1070.001 Indicator Removal: Clear Windows Event Logs | It uses wevtutil.exe to clear Windows event logs.  |
| Discovery       | T1083 File and Directory Discovery                    | It enumerates and looks for files to encrypt in all local drives.  |
|                 | T1082 System Information Discovery                    | <div>Obtains the following information:</div> <ul style="list-style-type: none"><li>• Number of processors</li><li>• System information</li></ul>  |
| Impact          | T1490 Inhibit System Recovery                         | It executes uses vssadmin to remove volume shadow copies   |
|                 | T1486 Data Encrypted for Impact                       | <div>It uses a 4096-bit RSA key and Cha-cha20 for file encryption.</div> <div>It avoids encrypting files with the following strings in their file name:</div> <ul style="list-style-type: none"><li>• .bat</li><li>• .bin</li><li>• .cab</li></ul> |

- .diagcab
- .diagcfg
- .diagpkg
- .drv
- .dll
- .exe
- .hlp
- .hta
- .ico
- .msi
- .ocx
- .ps1
- .psm1
- .scr
- .sys
- .ini
- .Thumbs.db
- .url
- .iso

It avoids encrypting files found in the following folders:

- \$Recycle.Bin
- Boot
- Documents and Settings
- PerfLogs
- ProgramData
- Recovery
- System Volume Information
- Windows



|  |  |   |  |
|--|--|---|--|
|  |  | <p>It appends the following extension to the file name of the encrypted files:</p> <p><i>.rhysida</i></p> <p>It encrypts all system drives from A to Z.</p> <p>It drops the following ransom note:</p> <p><i>{Encrypted Directory}\CriticalBreachDetected.pdf</i></p> |  |
|  | T1491.001 Defacement:<br>Internal Defacement | It changes the desktop wallpaper after encryption and prevents the user from changing it back by modifying the NoChangingWallpaper registry value.  |  |

## Trend Micro Solutions

Trend solutions such as [Apex One](#), [Deep Security](#), [Cloud One Workload Security](#), [Worry-Free Business Security](#), [Deep Discovery Web Inspector](#), [Titanium Internet Security](#), and [Cloud Edge](#) can help protect against attacks employed by the Rhysida ransomware.



| Trend Micro solutions   | Detection Patterns / Policies / Rules   |
|---|---|
| <ul style="list-style-type: none"><li>• Trend Micro Apex One</li><li>• Trend Micro Deep Security</li><li>• Trend Micro Titanium Internet Security</li><li>• Trend Micro Cloud One Workload Security</li><li>• Trend Micro Worry-Free Business Security Services</li></ul> | <ul style="list-style-type: none"><li>• Ransom.Win64.RHYSIDA.SM</li><li>• Ransom.Win64.RHYSIDA.THEBBBC</li><li>• Ransom.Win64.RHYSIDA.THFOHBC</li><li>• Trojan.PS1.SILENTKILL.SMAJC</li><li>• Trojan.PS1.SILENTKILL.A</li></ul>   |
| <ul style="list-style-type: none"><li>• Trend Micro Apex One</li><li>• Trend Micro Deep Security</li><li>• Trend Micro Worry-Free Business Security Services</li><li>• Trend Micro Titanium Internet Security</li></ul>   | <ul style="list-style-type: none"><li>• RAN4056T</li><li>• RAN4052T</li></ul>   |
| <ul style="list-style-type: none"><li>• Trend Micro Apex One</li><li>• Trend Micro Deep Discovery Web Inspector</li></ul>   | <ul style="list-style-type: none"><li>• DDI Rule ID: 597 - "PsExec tool detected"</li><li>• DDI Rule ID: 1847 - "PsExec tool detected - Class 2"</li><li>• DDI Rule ID: 4524 - "Possible Renamed PSEXEC Service - SMB2 (Request)"</li><li>• DDI Rule ID: 4466 - "PsExec Clones - SMB2 (Request)"</li><li>• DDI Rule ID: 4571 - "Possible Suspicious Named Pipe - SMB2 (REQUEST)"</li><br/><li>• DDI Rule ID: 4570 - "COBALTSTRIKE - DNS(RESPONSE)"</li><li>• DDI Rule ID: 4152 - "COBALTSTRIKE - HTTP (Response)"</li></ul> |

|  |   |
|--|---|
|  | <ul style="list-style-type: none"><li>• DDI Rule ID: 4153 - "COBALTSTRIKE - HTTP (Request) - Variant 2"</li><li>• DDI Rule ID: 2341 - "COBALTSTRIKE - HTTP (Request)"</li><li>• DDI Rule ID: 4390 - "CobaltStrike - HTTPS (Request)"</li><li>• DDI Rule ID: 4870 - "COBEACON DEFAULT NAMED PIPE - SMB2 (Request)"</li><li>• DDI Rule ID: 4861 - "COBEACON - DNS (Response) - Variant 3"</li><li>• DDI Rule ID: 4860 - "COBEACON - DNS (Response) - Variant 2"</li><li>• DDI Rule ID: 4391 - "COBEACON - DNS (Response)"</li></ul> |
| <ul style="list-style-type: none"><li>• Trend Micro Apex One</li><li>• Trend Micro Deep Security</li><li>• Trend Micro Worry-Free Business Security Services</li><li>• Trend Micro Titanium Internet Security</li><li>• Trend Micro Cloud Edge</li></ul> | <ul style="list-style-type: none"><li>• Troj.Win32.TRX.XXPE50FFF071</li></ul>   |

Trend Micro XDR uses the following workbench alerts to protect customers from Rhysida-related attacks:

Cobalt Strike

|   |                                      |
|---|--------------------------------------|
| Strike  |                                      |
| COBALT C2 Connection  | afd1fa1f-b8fc-4979-8bf7-136db80aa264 |
| Early Indicator of Attack via Cobalt Strike                     | 0ddda3c1-dd25-4975-a4ab-b1fa9065568d |
| Lateral Movement of Cobalt Strike Beacon                        | 5c7cdb1d-c9fb-4b1d-b71f-9a916b10b513 |
| Possible Cobalt Strike Beacon                                   | 45ca58cc-671b-42ab-a388-d972ff571d68 |
| Possible Cobalt Strike Beacon Active Directory Database Dumping | 1f103cab-9517-455d-ad08-70eaa05b8f8d |
| Possible Cobalt Strike Connection                               | 85c752b8-93c2-4450-81eb-52ec6161088e |
| Possible Cobalt Strike Privilege Escalation Behavior            | 2c997bac-4fc0-43b4-8279-6f2e7cf723ae |
| Possible Fileless Cobalt Strike                                 | cf1051ba-5360-4226-8ffb-955fe849db53 |

PsExec

| Workbench Alert   | ID                                   |
|---|--------------------------------------|
| Possible Credential Access via PSEXESVC Command Execution | 0b870a13-e371-4bad-9221-be7ad98f16d7 |
| Possible Powershell Process Injection via PSEXEC          | 7fe83eb8-f40f-43be-8edd-f6cbc1399ac0 |
| Possible Remote Ransomware Execution via PsExec           | 47fbd8f3-9fb5-4595-9582-eb82566ead7a |
| PSEXEC Execution By Process                               | e011b6b9-bdef-47b7-b823-c29492cab414 |
| Remote Execution of Windows Command Shell via PsExec      | b21f4b3e-c692-4eaf-bee0-ece272b69ed0 |



|   |                                      |
|---|--------------------------------------|
| Suspicious Mimikatz Credential Dumping via PsExec | 8004d0ac-ea48-40dd-aabf-f96c24906acf |
|---|--------------------------------------|

SILENTKILL

| Workbench Alert                           | ID                                   |
|---|--------------------------------------|
| Possible Disabling of Antivirus Software  | 64a633e4-e1e3-443a-8a56-7574c022d23f |
| Suspicious Deletion of Volume Shadow Copy | 5707562c-e4bf-4714-90b8-becd19bce8e5 |

Rhysida

| Workbench Alert                                 | ID                                   |
|---|--------------------------------------|
| Ransom Note Detection (Real-time Scan)          | 16423703-6226-4564-91f2-3c03f2409843 |
| Ransomware Behavior Detection                   | 6afc8c15-a075-4412-98c1-bb2b25d6e05e |
| Ransomware Detection (Real-time Scan)           | 2c5e7584-b88e-4bed-b80c-dfb7ede8626d |
| Scheduled Task Creation via Command Line        | 05989746-dc16-4589-8261-6b604cd2e186 |
| System-Defined Event Logs Clearing via Wevtutil | 639bd61d-8aee-4538-bc37-c630dd63d80f |



within their system:

```
processCmd:"powershell.exe*\\*$\?.ps1" OR (objectFilePath:"?:*\??\psexec.exe" AND processCmd:"*cmd.exe*\\?\?.bat")
```

Tags

[Endpoints](#) | [Ransomware](#) | [Research](#) | [Articles, News, Reports](#)

Authors

**Trend Micro Research**  
Trend Micro

[CONTACT US](#)

[SUBSCRIBE](#)

Related Articles

[Understanding the Initial Stages of Web Shell and VPN Threats: An MXDR Analysis](#)



Business



See all articles >

Experience our unified platform for free

Claim your 30-day trial



Resources

Support

About Trend

Country Headquarters

Trend Micro - United States (US)

225 East John Carpenter Freeway  
Suite 1500  
Irving, Texas 75062



Business



Select a country / region

United States

▼

[Privacy](#) | [Legal](#) | [Accessibility](#) | [Site map](#)

Copyright ©2024 Trend Micro Incorporated. All rights reserved