BOLETIM DE SEGURANÇA

Malware ValleyRAT, retorna com estratégias sofisticadas de extração de dados

heimdall
security research
A DIVISION OF ISH

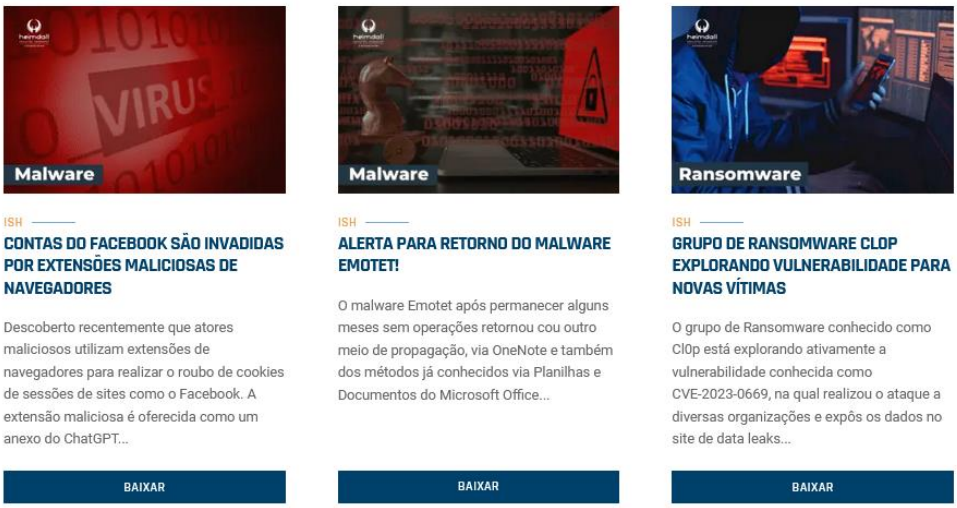
TLP: CLEAR

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 pesquisadores de segurança cibernética identificaram uma versão atualizada do malware ValleyRAT. Esta nova versão está sendo disseminada como parte de uma campanha inédita, representando uma ameaça potencial para a segurança digital.

2 INFORMAÇÕES SOBRE A AMEAÇA

O ValleyRAT, é um trojan de acesso remoto (RAT) descoberto pela primeira vez no início de 2023, ele tem como principal finalidade infiltrar-se e comprometer sistemas, permitindo que invasores remotos obtenham acesso não autorizado e controle sobre computadores infectados. A distribuição do ValleyRAT ocorre comumente através de e-mails de phishing ou downloads mal-intencionados. A versão mais recente do ValleyRAT apresenta novos comandos, incluindo captura de tela, filtragem de processos, desligamento forçado e limpeza de logs de eventos do Windows. Recentemente, foi detectada uma nova campanha que distribui a versão mais recente do ValleyRAT, envolvendo múltiplas etapas.

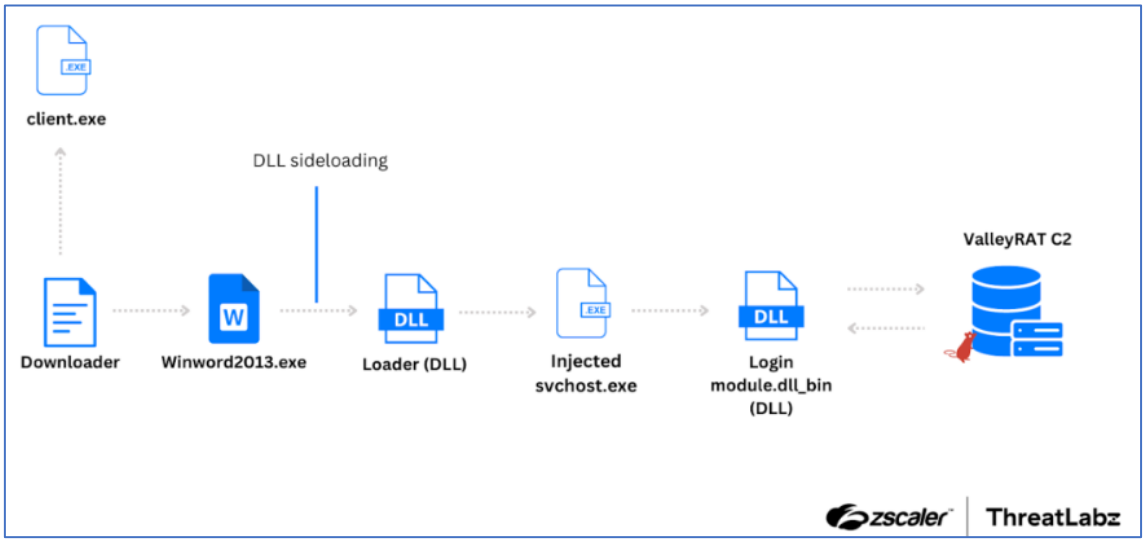


Figura 1 – Cadeia de ataque da campanha do ValleyRAT.

ValleyRAT emprega um downloader em sua fase inicial para obter cinco arquivos de um servidor HFS, que é posteriormente utilizado para comunicações C2.

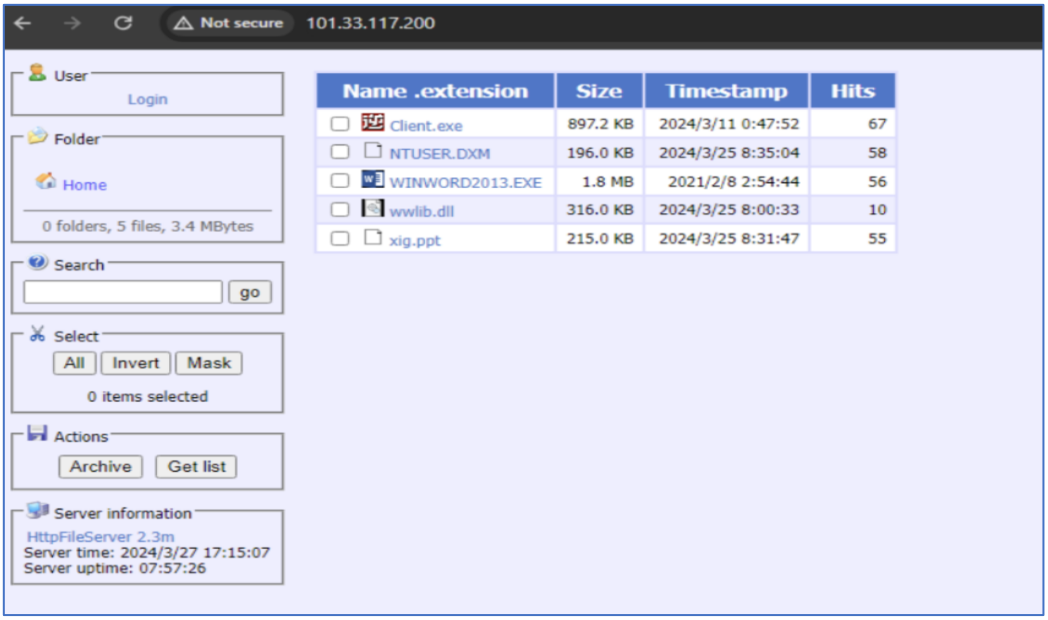


Figura 2 – Servidor HFS que hospeda arquivos do ValleyRAT.

Inicialmente, o downloader do ValleyRAT verifica se o arquivo NTUSER.DXM está presente. Caso contrário, ele baixa o arquivo da internet e o salva no disco usando as APIs URLOpenBlockingStreamW ,para baixar os arquivos como IStream e SHCreateStreamOnFileEx , para criar um arquivo e gravar o IStream baixado nele.

O arquivo NTUSER.DXM baixado é então descriptografado usando uma combinação de descriptografia XOR e RC4, com as chaves XOR e RC4 carregadas como strings de pilha. O arquivo descriptografado é uma DLL, que após a descriptografia, invoca a função de exportação _MainLogic@0. A DLL descriptografada verifica a existência do caminho C:\Program Files\TCLS. Se não existir, ela prossegue com o download do client.exe do servidor HFS usando a biblioteca WinINet, com Processkiller definido como o arquivo UserAgent.

A DLL também inclui uma verificação anti-AV para detectar e encerrar o software de segurança Qihoo e o utilitário Winrar. Ele recupera uma lista de todos os processos em execução no sistema e compara os nomes dos processos. Se o nome de um processo corresponder, o malware abre um identificador para o processo e envia uma mensagem WM_QUIT para todos os threads do processo, encerrando-os efetivamente.

Em seguida, o malware baixa WINWORD2013.EXE, wwlib.dll e xig.ppt do servidor HFS, salvando-os no disco no local C:\Users. O malware exclui o diretório C:\Program Files\TCLS e o arquivo client.exe. Por fim, o malware tenta executar WINWORD2013.EXE com privilégios administrativos usando o comando runas, levando ao segundo estágio. O arquivo WINWORD2013.EXE é o processador legítimo do Microsoft Word, mas o malware o utiliza para carregar uma DLL maliciosa chamada wwlib.dll. O wwlib.dll serve como um carregador malicioso, responsável por verificar a presença de C:\Users\xig.ppt (uma DLL criptografada) no disco. Se o arquivo for encontrado, o malware o carrega na memória e o descriptografa usando o mesmo algoritmo de descriptografia mencionado no primeiro estágio, usando as mesmas chaves XOR e RC4. O malware copia a DLL xig.ppt descriptografada para outro local de memória com permissão PAGE_EXECUTE_READ.

A partir deste momento, o descriptografado xig.ppt continua o processo de execução como um mecanismo para descriptografar e injetar shellcode no arquivo svchost.exe. O malware cria svchost.exe como um processo suspenso, aloca memória dentro do processo e grava shellcode nele. O malware usa a API SetThreadContext para alterar o ponteiro da instrução para o endereço do shellcode alocado. Finalmente, o malware chama a função ResumeThread, levando à próxima etapa do processo.

```
BVar4 = GetThreadContext(puVar12,(LPCONTEXT)ThreadContext);
if ((BVar4 != 0) &&
   (lpBaseAddress = VirtualAllocEx(processHandle,(LPVOID)0x0,0x98b,0x3000,PAGE_EXECUTE_READWRITE),
   lpBaseAddress != (LPVOID)0x0)) {
  BVar4 = WriteProcessMemory(processHandle,lpBaseAddress,&lpBuffer,0x98b,(SIZE_T *)&local_24);
  if ((BVar4 != 0) &&
     (local_280 = lpBaseAddress, BVar4 = SetThreadContext(local_1394,(CONTEXT *)ThreadContext),
     BVar4 != 0)) {
    ResumeThread(processInformation.hThread);
```

zscaler | ThreatLabz

Figura 3 – Processo de injeção utilizado pelo RAT.

O shellcode, que foi injetado, possui dados de configuração cruciais e decifra APIs para criar uma conexão com o servidor C2. Essa conexão é empregada para fazer o download da próxima fase do malware. Quando injetado no svchost.exe decifra APIs de forma dinâmica, percorrendo o Process Environment Block (PEB) e examinando os cabeçalhos PE por meio do algoritmo de hash BKDR.

```
def BKDRHashing(apiName):
finalHash = 0
for i in apiName:
  finalHash = (finalHash* 0x83) & 0xFFFFFFFF
  finalHash = (finalHash + ord(i)) & 0xFFFFFFFF
finalHash = finalHash & 0x7FFFFFFF
print(hex(finalHash))

>>>BKDRHashing("GetProcAddress")
0x1ab9b854
```

Figura 4 – Cabeçalhos PE usando o algoritmo de hash BKDR.

Após decifrar as APIs para kernel32.dll e ntdll.dll, o código examina a string codemark na memória do shellcode. Essa string atua como um espaço reservado para guardar a configuração do malware. A amostra usa TCP para se comunicar com o servidor C2. Em seguida, o malware envia os dados 32 para o C2 para obter um shellcode de 32 bits. Isso foi confirmado ao enviar dados 64 e receber um shellcode de 64 bits. O shellcode de 32 bits é recebido como dados criptografados de tamanho 0x4B00E. Os dados criptografados são descriptografados usando uma operação XOR simples com a chave de valor 0x36. O shellcode descriptografado de 32 bits é então executado, avançando para a próxima fase.

O shellcode utiliza o mesmo algoritmo de hash BKDR, já citado na terceira etapa, para resolver as APIs de forma dinâmica. Ele segue carregando uma DLL embutida de maneira reflexiva (utilizando as APIs resolvidas dinamicamente) a partir dos dados C2 descriptografados na memória. A DLL possui quatro exportações: DLL entrypoint, load, rune e zidingyixiugaidaochuhanshu. Dentre estas, as funções DLL entrypoint e load são executadas.

A função de exportação load copia a sequência de configuração observada em um formato específico, inverte a sequência e segue para a sua análise. A string é armazenada no formato |key:value|, onde a chave simboliza o atributo de configuração e o valor representa o seu valor correspondente.

```
|p1:101.33.117.200|o1:6666|t1:1|p2:101.33.117.200|o2:8888|t2:1|p3:127.0.0.1|o3:80|t3:1|
dd:1|cl:1|fz:默认|bb:1.0|bz:2024.3.20|jp:0|bh:0|ll:0|dl:0|sh:0|kl:0|bd:0||
```

Figura 5 – String armazenada no formato Key:Value.

O propósito desta fase é fazer o download e executar o payload final. Após a análise da configuração C2 e a implementação do tempo de sono especificado nos dados de configuração, o malware verifica a presença da carga final no host da vítima. Isso é realizado ao abrir a chave de registro HKEY_CURRENT_USER\Console\0 e consultar o valor nomeado d33f351a4aeea5e608853d1a56661059.

Se o tamanho do valor for superior a 0xA44, isso indica que a carga final já está no host da vítima. Nestes casos, o malware aloca uma seção de memória PAGE_EXECUTE_READWRITE e copia os dados do valor para ela. Caso a carga final ainda não estiver no host da vítima, o malware envia uma DLL chamada "登录模块.dll_bin (Login module.dll_bin)" para o C2 para fazer o download da carga final. O nome da DLL é criptografado através de uma operação XOR com a mesma chave (0x36) utilizada na terceira etapa. A resposta a este pedido contém a carga final incorporada. Estes dados são então copiados para uma seção de memória PAGE_EXECUTE_READWRITE e salvos no registro como um valor nomeado d33f351a4aeea5e608853d1a56661059 dentro da chave HKEY_CURRENT_USER\Console\0. A DLL incorporada é então carregada na memória e executada, atuando como a carga final.

O payload final entregue é o ValleyRAT, inicialmente identificado por Qi An Xin e atribuído ao ator de ameaça The Great Thief of Valley, também conhecido como Silver Fox. Neste contexto, discutiremos as alterações observadas no ValleyRAT. Na versão mais recente do ValleyRAT, os criadores de malware introduziram novos campos de dados para aprimorar a identificação digital do dispositivo.

Os criadores de malware também modificaram o processo de geração de ID do bot. Apesar do algoritmo de hash permanecer inalterado, os dados usados para o algoritmo foram modificados. Atualmente, o malware gera um hash MD5 utilizando os seguintes valores como argumentos:

- computerName
- numberOfProcessors
- ntdllVersion
- systemIP
- integrityLevelfollwedbyUsername
- profileGuid

```python
import hashlib
def botIDGeneration(computerName, numberOfProcessors, ntdllVersion, systemIP,
integrityLevelfollwedbyUsername, profileGuid):
   data = computerName.encode("utf-16le")
   data += ntdllVersion.encode("utf-16le")
   data += systemIP.encode("utf-16le")
   data += b'\x20\x00'
   data += numberOfProcessors.encode("utf-16le")
   data += "X86".encode("utf-16le")
   data += integrityLevelfollwedbyUsername.encode("utf-16le")
   data += profileGuid.encode("utf-16le")
   data += b'\x00\x00'
   result = hashlib.md5(data).hexdigest()
   print(result)
```

Figura 6 – Código utilizado escrito em Python.

3 MITRE ATT&CK - TTPs

Tática	Técnica	Detalhes
Defense Evasion	T1036 T1140	Consiste em técnicas que os adversários usam para evitar a detecção durante todo o seu comprometimento.
Persistence	T1574.002	Consiste em técnicas que os adversários usam para manter o acesso aos sistemas após reinicializações, alterações de credenciais e outras interrupções que podem interromper seu acesso.
Privilege Escalation	T1055	Privilege Escalation - Consiste em técnicas que os adversários usam para obter permissões de nível superior em um sistema ou rede.
Discovery	T1010 T1057 T1082 T1083 T1120 T1518.001	Consiste em técnicas que um adversário pode usar para obter conhecimento sobre o sistema e a rede interna.
Command and Control	T1071	Consiste em técnicas que os adversários podem usar para se comunicar com sistemas sob seu controle dentro de uma rede vítima.
Initial Access	T1659	Consiste em técnicas que utilizam vários vetores de entrada para obter sua posição inicial dentro de uma rede.
Collection	T1113	Consiste em técnicas que os adversários podem usar para coletar informações e nas fontes das quais as informações são coletadas que são relevantes para cumprir os objetivos do adversário.
Impact	T1529	Consiste em técnicas que os adversários usam para interromper a disponibilidade ou comprometer a integridade, manipulando processos comerciais e operacionais.

Tabela 1 – Tabela MITRE ATT&CK.

4 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:

Atualizações

- Mantenha o sistema operacional e os aplicativos sempre atualizados.

Antivírus

- Procure soluções de software antivírus que ofereçam proteção eficiente contra malwares.

Descriptografia

- Para combater efetivamente o aumento do tráfego criptografado malicioso, recomenda-se habilitar os recursos de descriptografia em firewalls de última geração.

Cuidado com links e anexos

- Evite clicar em links ou anúncios infectados e abrir anexos em e-mails de spam.

Educação

- Promova treinamentos e capacitações técnicas para todos na empresa, bem como atue junto do departamento de Comunicação Interna para gerar campanhas periódicas que relembrem os trabalhadores a respeito da importância de ficarem atentos.

Estratégias de vigilância

- Desenvolva ações de monitoramento e vigilância, pois a partir do momento em que a infecção ocorre, o software malicioso pode agir de forma indetectável e enfim roubar os dados de interesse ou promover a destruição dos sistemas.

Proteção contra malware

- A proteção contra malware é a melhor maneira de se proteger contra ameaças on-line.

5 INDICADORES DE COMPROMISSOS

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 do artefato	
md5:	984878f582231a15cc907aa92903b7ab
sha1:	d9ae9b2fa642658dc691442e197be96dc0dcd4c1
sha256:	470b18288f1fce4c024be7f7f01d66b062fbe41ff53d7fe50eef9d44ff79ad4b
File name:	984878f582231a15cc907aa92903b7ab.virus

Indicadores de compromisso do artefato	
md5:	81ab4d6b9a07e354b52a18690f98b8aa
sha1:	63d1d132dc05dd37e4f94dc8e22f3d0c3e700be0
sha256:	4215b084afa323f090c209518501d2ae0e9fa27cfc7cfe791a668e8802c6be61
File name:	81ab4d6b9a07e354b52a18690f98b8aa.virus

Indicadores de compromisso do artefato	
md5:	8995fbb4679ddd1516eacb3e453cb1ba
sha1:	857fa64483f911aaf2ed6238dec1b46d7017a1eb
sha256:	773a1cd04612e4e7346b200b46990d9ecc07aa9f917c0b0d7cc1975241d029ed
File name:	详情查看.exe

Indicadores de compromisso do artefato	
md5:	cc31928547ea412b9c7655ce958574bd
sha1:	44ffdbb03e7e0b49c39d80e58adb94830feea919
sha256:	8711dd15b2d9ef21c83cda2045bf360136e50399f817f59c21ead6f6d8e59a93
File name:	函数通知书.exe

Indicadores de compromisso do artefato	
md5:	abf0e40513a9d614266359e56ca54f90
sha1:	78eb03018194b7aadf859035d6092fcd7257ef77
sha256:	8b6694896f82a64ce6fd01d6f724c7ec64596577afd84e690377eb4c5bbe3ca3
File name:	abf0e40513a9d614266359e56ca54f90.virus

Indicadores de compromisso do artefato	
md5:	9aec2351a3966a9f854513a7b7aa5a13
sha1:	e11065431381023d16190b390504390dfeea16a9
sha256:	f5ebe440931d1d003a51133ad1f727daf2410ba50d9f51818938c269bb7fe806
File name:	wwlib.dll

Tabela 2 – Indicadores de Compromissos de artefatos

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
URL	hxxp[:]//hotshang[.]com/ hxxp[:]//119[.]28[.]41[.]143/ hxxp[:]//124[.]156[.]134[.]223/ hxxp[:]//101[.]33[.]117[.]200/ hxxp[:]//43[.]129[.]233[.]146/ hxxp[:]//43[.]132[.]212[.]111/ hxxp[:]//43[.]129[.]233[.]99/ hxxp[:]//119[.]28[.]32[.]143/ hxxp[:]//43[.]132[.]235[.]4/ hxxps[:]//2024aasaf[.]oss-cn-hongkong[.]aliyuncs[.]com/TARE961424[.]exe hxxp[:]//wenjian2024[.]com/57683653%E5%87%BD%E6%95%B0[.]exe hxxps[:]//2024aasaf[.]oss-cn-hongkong[.]aliyuncs[.]com/TARE965624%20[.]exe hxxps[:]//2024fapiao[.]oss-cn-hongkong[.]aliyuncs[.]com/82407836%E5%87%BD%E6%95%B0[.]exe hxxps[:]//scpgjhs[.]com/TARE965624[.]exe hxxps[:]//tzsxr[.]com/customer[.]exe hxxp[:]//mtw[.]so/6oAUvN hxxp[:]//kfurl[.]cn/kvukj hxxp[:]//mtw[.]so/5Fytvq hxxps[:]//fpwenj[.]zhangyaodong5[.]com/TARE985624[.]exe hxxps[:]//2024aasaf[.]oss-cn-hongkong[.]aliyuncs[.]com/TARE967124[.]exe

Tabela 3 – Indicadores de Compromissos de Rede.

Obs: Os *links* e endereços IP elencados acima podem estar ativos; cuidado ao realizar a manipulação dos referidos IoCs, evite realizar o clique e se tornar vítima do conteúdo malicioso hospedado no IoC.

6 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **ZScaler**
- **Thehackernews**

7 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH