TLP: CLEAR

BOLETIM DE SEGURANÇA

Black Basta Ransomware amplia arsenal com e-mails em massa, QR codes e táticas de engenharia social

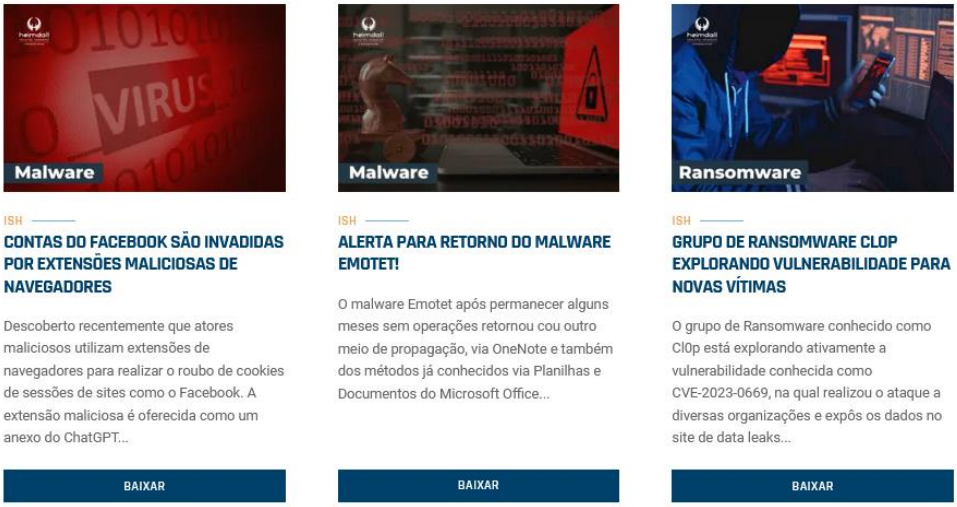
heimdall
security research

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 SUMÁRIO EXECUTIVO

Os operadores associados ao ransomware Black Basta têm demonstrado uma evolução em suas táticas de ataque, especificamente no uso de técnicas de engenharia social. Desde o início de outubro de 2024, esses agentes começaram a empregar uma estratégia mais diversificada, introduzindo novas cargas úteis, como Zbot e DarkGate, em suas campanhas. Essa mudança sugere um esforço contínuo para maximizar a eficácia de suas operações, possivelmente visando ampliar seu alcance ou contornar medidas de segurança mais robustas.

2 CADEIA DE ATAQUES OBSERVADA

De acordo com informações da Rapid7, os ataques de engenharia social seguem com o agente de ameaça bombardeando os usuários do ambiente alvo com **e-mails massivos**, uma prática viabilizada ao inscrever os endereços de e-mail das vítimas em diversas listas de discussão simultaneamente. Após esse ataque de "*mail bomb*", o agente estabelece contato direto com os usuários impactados. Observou-se que esse contato inicial ainda ocorre predominantemente através do **Microsoft Teams**, onde o atacante, utilizando-se de uma conta externa, tenta realizar chamadas ou enviar mensagens às vítimas, oferecendo ajuda como parte de sua abordagem maliciosa. Também em vários casos, o agente de ameaça frequentemente se passou por um membro do **help desk**, da equipe de suporte ou da equipe de TI da organização-alvo.

Exemplos de nomes de exibição usados no Microsoft Teams foram observados, incluindo casos em que os nomes podem ser preenchidos com caracteres de espaço em branco. Além disso, é comum que os atacantes utilizem combinações de nome e sobrenome como nome de exibição no chat e/ou nome de usuário da conta, representando um suposto membro da equipe de TI da organização-alvo.

- ***Help Desk***
- ***HELP DESK***
- ***Help Desk Manager***
- ***Technical Support***
- ***Administracion***

Caso o usuário interaja com a isca, seja atendendo a chamada ou respondendo à mensagem, o agente da ameaça buscará induzi-lo a instalar ou executar uma ferramenta de gerenciamento remoto (RMM). Entre as ferramentas observadas estão Quicasses, AnyDesk, TeamViewer, Level e ScreenConnect. Também foram identificadas tentativas de utilizar o cliente OpenSSH, um utilitário nativo do Windows, para estabelecer um shell reverso. Em pelo menos uma ocasião, o agente compartilhou um código QR com a vítima. Embora o propósito exato do código QR não tenha sido confirmado, acredita-se que ele possa ter sido usado como parte de uma estratégia para contornar a autenticação multifator (MFA) após obter as credenciais do usuário.

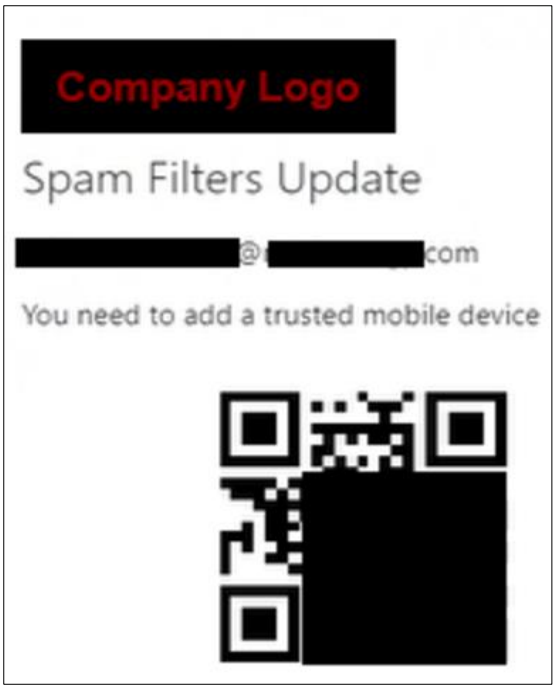


Figura 1 – QR Code (ofuscado) enviado por um operador.

Na maioria das situações, foi observado que, após obter acesso ao dispositivo do usuário por meio da ferramenta RMM, o operador tenta fazer o download e executar cargas úteis de malware adicionais. Em um caso específico, o atacante chegou a pedir mais tempo, possivelmente para transferir o acesso a outro integrante do grupo criminoso. Os métodos utilizados para entregar payloads variam de acordo com o caso e incluem o uso de instâncias comprometidas do SharePoint, plataformas populares de compartilhamento de arquivos, servidores alugados de provedores de hospedagem ou até uploads diretos para dispositivos comprometidos por meio do controle remoto de ferramentas RMM. Em outro incidente, o operador utilizou um coletor de credenciais personalizado do grupo para capturar as credenciais do usuário, que foram posteriormente carregadas em um site de compartilhamento de arquivos, expondo-as publicamente. O SharePoint também foi empregado para distribuir versões portáteis do AnyDesk, possivelmente como estratégia para contornar restrições de segurança que impediriam o download direto do site oficial anydesk[.]com, embora tentativas semelhantes tenham sido bloqueadas por proxies da web em casos anteriores.

O objetivo principal após o acesso inicial parece ser consistente: mapear rapidamente o ambiente e capturar as credenciais do usuário. Sempre que possível, os operadores também buscam roubar arquivos de configuração de VPN armazenados no dispositivo. Com as credenciais obtidas, informações de VPN da organização e, potencialmente, a superação de medidas de MFA, os atacantes podem autenticar-se diretamente no ambiente de destino.

3 MITRE ATT&CK - TTPs

Tática	Técnica	Detalhes
Resource Development	T1587.001: Develop Capabilities: Malware	O agente da ameaça está desenvolvendo ativamente novos malwares para distribuir.
Initial Access	T1566.004: Phishing: Spearphishing Voice	O agente da ameaça liga para os usuários afetados e finge ser um membro da equipe de TI da organização para obter acesso remoto.
Credential Access	T1649: Steal or Forge Authentication Certificates	O agente da ameaça distribuiu diversas cargas de malware assinadas.
Credential Access	T1056.001: Input Capture: Keylogging	O agente da ameaça executa um executável que coleta as credenciais do usuário.
Credential Access	T1558.003: Steal or Forge Kerberos Tickets: Kerberoasting	O agente da ameaça realizou o Kerberoasting após obter acesso inicial.
Discovery	T1033: System Owner/User Discovery	O agente da ameaça enumera informações de ativos e usuários no ambiente após obter acesso.
Defense Evasion	T1140: Deobfuscate/Decode Files or Information	O agente da ameaça criptografa algumas cargas de arquivo zip com uma senha.
Defense Evasion	T1055.002: Process Injection: Portable Executable Injection	Várias cargas úteis executadas pelo agente da ameaça utilizam injeção de PE local.
Defense Evasion	T1620: Reflective Code Loading	Várias cargas úteis executadas pelo agente da ameaça carregam e executam o shellcode.
Impact	T1498: Network Denial of Service	O agente da ameaça sobrecarrega as soluções de proteção de e-mail com spam.
Command and Control	T1572: Protocol Tunneling	O agente da ameaça tentou usar túneis reversos SSH.
Command and Control	T1219: Remote Access Software	O agente da ameaça usou QuickAssist, AnyDesk, ScreenConnect, TeamViewer, Level e muito mais para facilitar o acesso remoto.

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:

Atualização de sistemas

- Mantenha sistemas operacionais, softwares e firmwares atualizados para corrigir vulnerabilidades conhecidas que podem ser exploradas por atacantes.

Autenticação Multifator (MFA)

- Implemente MFA em todos os serviços compatíveis para adicionar uma camada extra de proteção contra acessos não autorizados.

Conscientização sobre Phishing

- Realize treinamentos regulares para que os colaboradores identifiquem e relatem tentativas de phishing, reduzindo a eficácia de ataques de engenharia social.

Backups regulares

- Estabeleça rotinas de backup de sistemas críticos e configurações, assegurando a capacidade de restauração em caso de incidentes.

Configuração de ferramentas de segurança

- Garanta que as ferramentas de segurança de endpoint estejam corretamente configuradas e atualizadas para detectar e prevenir ameaças.

Monitoramento contínuo

- Implemente sistemas de detecção e resposta a intrusões para identificar e mitigar atividades suspeitas na rede.

Gestão de privilégios

- Restrinja privilégios de usuários com base em suas necessidades operacionais, minimizando o potencial de escalonamento de privilégios por atacantes.

Proteção de dados sensíveis

- Utilize criptografia para proteger dados sensíveis, tanto em trânsito quanto em repouso, dificultando o acesso não autorizado.

5 INDICADORES DE COMPROMETIMENTO (IOC)

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.

Indicadores do artefato	
md5:	1e801dfcf3f38c4d642bd6905b2a8c4e
sha1:	5a95b69c11018420b17b469771c8ec07458fda23
sha256:	5e9fbae0b94f6e36717bbd2c997981ba438d7efd800e76924f73452a69c04051
File name:	test.vbs

Indicadores do artefato	
md5:	fea6aea9de998c82840fc0fbe9256233
sha1:	640640d6651c4ac2f66ed8312084849ad9f0124e
sha256:	db34e255aa4d9f4e54461571469b9dd53e49feed3d238b6cfb49082de0afb1e4
File name:	SyncSuite

Indicadores do artefato	
md5:	0615dd42e9468cffe31c7febe206f62f
sha1:	ab1271b4316eb4a5d6ea03b4c24d56cef1e8524a
sha256:	49405370a33abbf131c5d550cebe00780cc3fd3cbe888220686582ae88f16af7
File name:	OmniScript

Indicadores do artefato	
md5:	a4e3345491eaca250f1cc139db05a015
sha1:	f09804b59a3aac7c1dd47c7e027182fb54f9a277
sha256:	22c5858ff8c7815c34b4386c3b4c83f2b8bb23502d153f5d8fb9f55bd784e764
File name:	PixelSignal

Indicadores do artefato	
md5:	fb426a4f80f7792ff46d04884ec80b8c
sha1:	8af2eab50e77706cec0f1416a51c171088d26ed6
sha256:	1656c55c8516bd650fe59b71a5886ecf508deb927ed3c8465cf0ad5923c35958
File name:	ProtectConnectEU.dll

Tabela 2 – Indicadores de Comprometimento

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
URL	-
Domínio	-
IP	185.130.47[.]96 65.87.7[.]151 66.78.40[.]86

	184.174.97[.]32 212.232.22[.]140 8.209.111[.]227 8.211.34[.]166 109.172.88[.]38 109.172.87[.]135 188.130.206[.]243 46.8.232[.]106 46.8.236[.]61 91.212.166[.]91 93.185.159[.]253 94.103.85[.]114 193.29.13[.]60 88.214.25[.]32 45.61.152[.]154 185.229.66[.]224 172.81.60[.]122 145.223.116[.]66 185.238.169[.]17 179.60.149[.]194

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**
- **Rapid7**
- **Thehackernews**

7 AUTORES

- **Ismael Rocha**

heimdall
security research
A DIVISION OF ISH