BOLETIM DE SEGURANÇA

Agencias governamentais alertam usuários do Ubiquiti EdgeRouter para a ameaça MooBot do APT28

heimdall
security research
A DIVISION OF ISH

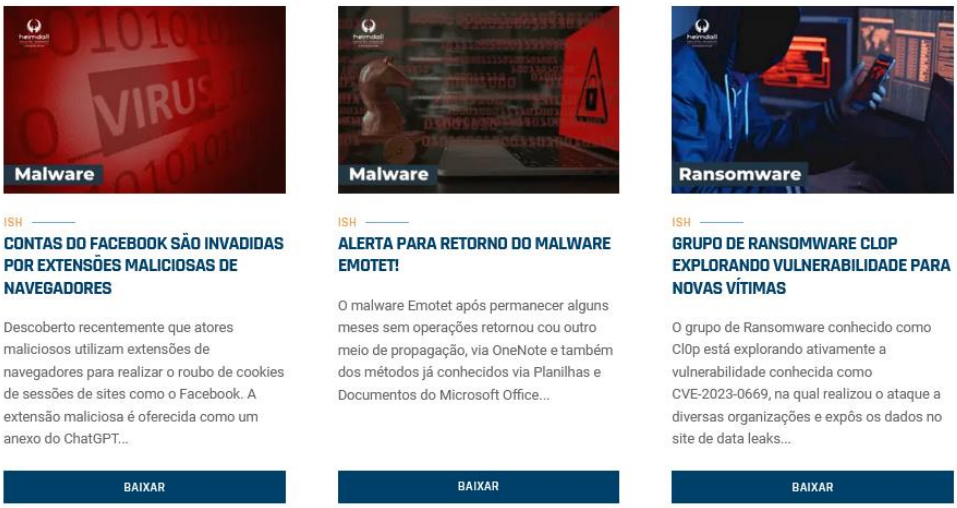
TLP: CLEAR

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

1 SUMÁRIO EXECUTIVO

Agências de segurança cibernética e de inteligência de várias nações, em um recente pronunciamento conjunto, estão recomendando aos usuários do **Ubiquiti EdgeRouter** que adotem medidas de segurança adicionais. O comunicado informa que a botnet, chamada **MooBot**, foi usada por um ator de ameaça ligado à Rússia, conhecido como **APT28**, para coletar credenciais, coletar resumos NTLMv2, tráfego de rede proxy e hospedar páginas de destino de spear-phishing e ferramentas personalizadas. O APT28, afiliado à Diretoria Principal do Estado-Maior General (GRU) da Rússia, é conhecido por estar ativo pelo menos desde 2007.

Isso ocorre após a desativação de uma botnet formada por roteadores comprometidos pelas autoridades, como parte de uma operação denominada Dying Ember, destacada algumas semanas atrás.

2 ATIVIDADE ASSOCIADA AO ATOR DE AMEAÇA

Conforme o documento conjunto, em 2022, os atores do APT28 utilizaram EdgeRouters comprometidos para facilitar ataques cibernéticos secretos, operações contra governos, militares e organizações em todo o mundo. Essas operações têm como alvo vários setores, incluindo Aeroespacial e Defesa, Educação, Energia e Serviços Públicos, Governos, Hotelaria, Manufatura, Petróleo e Gás, Varejo, Tecnologia e Transporte. Os países-alvo incluem República Checa, Itália, Lituânia, Jordânia, Montenegro, Polónia, Eslováquia, Turquia, Ucrânia, Emirados Árabes Unidos e os EUA.

Uma investigação do FBI revelou que atores do APT28 acessaram EdgeRouters comprometidos pelo Moobot, um botnet que instala trojans OpenSSH em hardware comprometido. Embora o comprometimento dos EdgeRouters tenha sido documentado em relatórios de código aberto, a investigação do FBI revelou que cada roteador comprometido acessado por atores APT28 abrigava uma coleção de scripts Bash e binários ELF projetados para explorar daemons OpenSSH backdoor e serviços relacionados para diversos fins. Os atores do APT28 usaram EdgeRouters comprometidos para coletar credenciais, tráfego de rede proxy e hospedar páginas de destino falsificadas e ferramentas pós-exploração personalizadas.

Por exemplo, no início de 2023, os atores criaram scripts Python personalizados para coletar credenciais de contas para usuários de webmail direcionados especificamente. Os atores do APT28 enviaram esses scripts Python personalizados a um subconjunto de roteadores Ubiquiti comprometidos para validar credenciais de contas de webmail roubadas coletadas por meio de scripts entre sites e campanhas de spear-phishing no navegador.

Em resumo, com acesso root aos Ubiquiti EdgeRouters comprometidos, os atores do APT28 acessaram a sistemas operacionais baseados em Linux para instalar ferramentas e ofuscar sua identidade durante a realização de campanhas maliciosas.

3 DETECÇÃO DA AMEAÇA EM DISPOSITIVOS

Para localizar arquivos maliciosos relacionados em EdgeRouters, pode ser pesquisado nos históricos Bash de todos os usuários por downloads de arquivos do domínio *packinstall[.]kozow[.]com*, consulte o tráfego de rede para conexões com o domínio *packinstall[.]kozow[.]com* e faça referência ao tabela de hash de arquivo abaixo para localizar artefatos no disco.

Além disso, se o diretório */usr/lib/libu.a/* existir em um EdgeRouter, é provável que tenha ocorrido uma infecção.

File path	SHA-256
/usr/sbin/cl	3B5ED45345193B06F40515DA342FF146267E8340B2E1AB6D55A257D2E3554A2B
/usr/sbin/cl	ADAE1BD8938B9A0D825A2EF7E7C4E000F01966C397306027119F20D7ECCE955D
/usr/sbin/cts	C09F8D0A9FA0F9BB3E19556182A95782DAEC2F2F532CAB5EEB5528F2CD783583
/usr/sbin/env	1CC20155517860557C94308EC913E4C3BFC072C34CE33449641CC9FB1D571B21
/usr/sbin/events	551EB82D82B7A8830549C9183EB39ACF19719C84B9BCCC7FB443504B093F6BB9
/usr/sbin/events	CD83DD9470603B1A1951EEFA95B602E34207C4D5E62C649642E7160574A9C50D
/usr/sbin/events	FBC2E6820C874ED102BAB304382EDEFFB9708E7B8445E126C227A6C289D92708
/usr/sbin/ptty	C9E06C7C62395DA32C91CC0C4ACB95F29A0AA3380A833E7C7B24B8D4DB50C0C6
/usr/sbin/ptty	5FACBE53B4C63DBC865F3713385358DF490A4BAD9211337241D85F0554CCA40A
/usr/sbin/ptty	C7C40CDCDD65E468EE29D330A34E8EE94C26AA8B3F1830E0A8DFEA8ACA3CDD50
/usr/sbin/sshd	A4A95807F1C5B200D5D94E3E811A7C4AF2D0D9CA88CA4D7F9D02015574F4716F
/usr/sbin/sshd	104E3EA9A190BA039488F5200824FE883B98F6FE01D05A1B55E15ED2199C807A

Tabela 1 – Hashes e caminhos para verificação.

Algumas versões do trojan OpenSSH criam usuários maliciosos systemd e systemx em /etc/shadow e /etc/passwd em EdgeRouters infectados. O trojan também introduz um endereço IP de servidor OpenDNS em /etc/resolv.conf, *208[.]67[.]220[.]222*, e um processo de usuário chamado .kworker para se disfarçar como um thread de kernel legítimo.

Os defensores da rede também podem consultar o tráfego da rede em busca de conexões com os seguintes domínios, que foram identificados pelo FBI e estão associados ao trojan OpenSSH. Os beacons HTTP para esses domínios seguem o formato fornecido após a lista.

- *matbaiteahe[.]mooo[.]com*
- *lalapoc[.]kozow[.]com*
- *gneivaientga[.]ignorelist[.]com*
- *antotehlant[.]theworkpc[.]com*
- *onechoice[.]gleeze[.]com*
- *mumucnc[.]kozow[.]com*

/srv.php?type=${type}&ip=${ip}&sshd_port=${sshd_port}&sshd_backup_miss ing=${sshd_backup_missing}&sshkey=${SSHKEY}&ptty_ver=${ptty_ver}&ctry=${CTRY}&id_ unic=${id_unic}&os=${os}&arch=${arch}&kernel=${kernel}&upt=${upt}&serverspeed=${s erverspeed}&lan=${lan}&lan_ip=${lan_ip}&rk_date=${rk_date}&socks_value=${socks_va lue}

EdgeRouters comprometidos pelo trojan OpenSSH exibem uma string de identificação SSH exclusiva, SSH-2.0- OpenSSH_6.7p2. É indicado o uso do Netcat ou ferramentas semelhantes para coletar strings de identificação de EdgeRouters e outro hardware para localizar infecções.

(local) $ nc <IP address of EdgeRouter> <SSH listening port on EdgeRouter>

SSH-2.0-OpenSSH_6.7p2 # this version indicates infection.

4 MITRE ATT&CK - TTPs

Técnica	ID	Detalhes
Develop Capabilities	T1587	Os agentes de ameaças APT28 criaram scripts Python personalizados para coletar credenciais de contas para usuários de webmail direcionados especificamente
Obtain Capabilities	T1588	Os atores do APT28 acessaram EdgeRouters comprometidos pelo Moobot, um botnet que instala trojans OpenSSH em hardware comprometido.
Compromise Infrastructure	T1584	Atores de ameaças APT28 acessaram EdgeRouters anteriormente comprometido por um trojan OpenSSH
Phishing	T1566	Os atores da ameaça APT28 conduziram scripts entre sites e campanhas de spear-phishing navegador-no-navegador.
Exploitation for Client Execution	T1203	Os atores da ameaça APT28 exploraram o CVE-2023-23397.
Event Triggered Execution	T1546	O roteador comprometido abrigava uma coleção de scripts Bash e binários ELF projetados para backdoor de daemons OpenSSH e serviços relacionados.
Adversary-in-theMiddle	T1557	Os atores da ameaça APT28 instalaram as ferramentas disponíveis publicamente Impacket ntlmrelayx.pyvi e Respondervii em roteadores Ubiquiti comprometidos para executar ataques de retransmissão NTLM.
Modify Authentication Process	T1556	Os atores da ameaça ATP28 hospedaram servidores de autenticação não autorizados NTLMv2 para modificar o processo de autenticação de credenciais roubadas coletadas durante os ataques de retransmissão NTLM.
Automated Collection	T1119	APT28 utiliza CVE-2023-23397 para automatizar a coleta de hash NTLMv2.
Automated Exfiltration	T1020	APT28 utiliza CVE-2023-23397 para automatizar a exfiltração para infraestrutura controlada por atores.

Tabela 2 – Tabela MITRE ATT&CK.

5 RECOMENDAÇÕES

Conforme nota, o FBI e seus parceiros recomendam que as seguintes etapas sejam tomadas para remediar EdgeRouters comprometidos:

1. Execute uma redefinição de fábrica do hardware para liberar arquivos maliciosos nos sistemas de arquivos
2. Atualize para a versão de firmware mais recente
3. Altere quaisquer nomes de usuário e senhas padrão
4. Implementar regras estratégicas de firewall nas interfaces do lado WAN para evitar a exposição indesejada de serviços de gerenciamento remoto.

Além disso, todos os proprietários de redes devem manter seus sistemas operacionais, software e firmware atualizados. A aplicação oportuna de patches é uma das medidas mais eficientes e econômicas que uma organização pode tomar para minimizar sua exposição a ameaças à segurança cibernética. Para CVE-2023-23397, a atualização do Microsoft Outlook atenua a vulnerabilidade. Para mitigar outras formas de retransmissão NTLM, todos os proprietários de rede devem considerar desabilitar o NTLM quando possível, ou habilitar a assinatura do servidor e configurações de Proteção Estendida para Autenticação.

6 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Comunicado conjunto FBI**
- **Mitre ATT&CK**
- **Thehackernews**

heimdall
security research
A DIVISION OF ISH