1. MỤC TIÊU CHUNG

Tiến hành nghiên cứu toàn diện về nhóm Salt Typhoon, tập trung vào chiến thuật, kỹ thuật và thủ tục của họ. Sử dụng khung MITRE ATT&CK để vạch ra các hoạt động của nhóm và cung cấp những hiểu biết có thể hành động.
Phát hiện của bản báo cáo này đóng một vai trò quan trọng trong việc củng cố khả năng phòng thủ chống lại kẻ thù này.

2. Salt Typhoon

Salt Typhoon là một nhóm do Nhà nước Cộng hòa Nhân dân Trung Hoa (PRC) hậu thuẫn, đã hoạt động ít nhất từ năm 2019 và chịu trách nhiệm cho nhiều vụ xâm nhập vào hạ tầng mạng của các nhà cung cấp dịch vụ internet (ISP) lớn tại Hoa Kỳ. [1]

JumbledPath

Nhóm này custom nhiều loại mã độc khác nhau, một trong số đó là JumbledPath với ID S1206. [2]

JumbledPath là một tiện ích (utility) được xây dựng tùy chỉnh bằng ngôn ngữ **GO**, đã được **Salt Typhoon** sử dụng ít nhất từ năm 2024 để thực hiện packet capture trên các thiết bị Cisco từ xa. **JumbledPath** được biên dịch dưới dạng ELF binary sử dụng kiến trúc x86-64, điều này khiến nó có khả năng được sử dụng trên các hệ điều hành Linux và các thiết bị mạng từ nhiều nhà cung cấp khác nhau.[3]

Một trong các kỹ thuật mà **JumbledPath** thực hiện đó là hành vi xóa log tại ID **T1070.002.** [4]

JumbledPath Techniques Used

Domain	ID	Name	Use
Enterprise	T1560	Archive Collected Data	JumbledPath can compress and encrypt exfiltrated packet captures from targeted devices.
Enterprise	T1665	Hide Infrastructure	JumbledPath can use a chain of jump hosts to communicate with compromised devices to obscure actor infrastructure.

Enterprise	T1562	Impair Defenses	JumbledPath can impair logging on all devices used along its connection path to compromised hosts.
Enterprise	T1070	Indicator Removal: Clear Linux or Mac System Logs	JumbledPath can clear logs on all devices used along its connection path to compromised network infrastructure.
Enterprise	T1104	Multi-Stage Channels	JumbledPath can communicate over a unique series of connections to send and retrieve data from exploited devices.
Enterprise	T1040	Network Sniffing	JumbledPath has the ability to perform packet capture on remote devices via actor-defined jump-hosts.

GHOSTSPIDER

GHOSTSPIDER được xem như là một backdoor đa mô hình tinh vi được thiết kế với nhiều lớp để load các mô-đun khác nhau dựa trên các mục đích cụ thể. Backdoor này giao tiếp với C2 của mình bằng giao thức tùy chỉnh được bảo vệ bởi bảo mật lớp vận chuyển (TLS), đảm bảo giao tiếp an toàn. [5]

Dưới đây là list domain mà **GHOSTSPIDER** kết nối về C2, có thể nói đa phần đều gửi về .com, đặc biệt tròn đó có 1 doamin đuôi .dev

Domain
materialplies.com
news.colourtinctem.com
api.solveblemten.com
esh.hoovernamosong.com
vpn114240349.softether.net
imap.dateupdata.com
pulseathermakf.com
www.infraredsen.com
billing.clothworls.com
helpdesk.stnekpro.com
jasmine.lhousewares.com
private.royalnas.com
telcom.grishamarkovgf8936.workers.dev
vpn305783366.softether.net
vpn487875652.softether.net
vpn943823465.softether.net

GHOSTSPIDER Techniques Used

Mặc dù đã có mã định danh là **FGS5008** trên MITRE nhưng chưa có nội dung chi tiết công khai [6]

3. Salt Typhoon Techniques Used

Domain	ID		Name	Use
Enterprise	T1098	.004	Account Manipulation: SSH Authorized Keys	Salt Typhoon has added SSH authorized_keys under root or other users at the Linux level on compromised network devices.
Enterprise	T11	.002	Brute Force:	Salt Typhoon has cracked

	10		Password Cracking	passwords for accounts with weak encryption obtained from the configuration files of compromised network devices.
Enterprise	T1136		Create Account	Salt Typhoon has created Linux-level users on compromised network devices through modification of /etc/shadow and /etc/passwd.
Enterprise	T1602	.002	Data from Configuration Repository: Network Device Configuration Dump	Salt Typhoon has attempted to acquire credentials by dumping network device configurations.[
Enterprise	T1587	.001	Develop Capabilities: Malware	Salt Typhoon has used custom tooling including JumbledPath.
Enterprise	T1048	.003	Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol	Salt Typhoon has exfiltrated configuration files from exploited network devices over FTP and TFTP.
Enterprise	T1190		Exploit Public-Facing Application	Salt Typhoon has exploited CVE-2018-0171 in the Smart Install feature of Cisco IOS and Cisco IOS XE software for initial access.
Enterprise	T1590	.004	Gather Victim Network Information: Network Topology	Salt Typhoon has used configuration files from exploited network devices to help discover upstream and downstream network segments.

Enterprise	T1562	.004	Impair Defenses: Disable or Modify System Firewall	Salt Typhoon has made changes to the Access Control List (ACL) and loopback interface address on compromised devices.
Enterprise	T1070	.002	Indicator Removal: Clear Linux or Mac System Logs	Salt Typhoon has cleared logs including .bash_history, auth.log, lastlog, wtmp, and btmp.
Enterprise	T1040		Network Sniffing	Salt Typhoon has used a variety of tools and techniques to capture packet data between network interfaces.
Enterprise	T1588	.002	Obtain Capabilities: Tool	Salt Typhoon has used publicly available tooling to exploit vulnerabilities.
Enterprise	T1572		Protocol Tunneling	Salt Typhoon has modified device configurations to create and use Generic Routing Encapsulation (GRE) tunnels.
Enterprise	T1021	.004	Remote Services: SSH	Salt Typhoon has modified the loopback address on compromised switches and used them as the source of SSH connections to additional devices within the target environment, allowing them to bypass access control lists (ACLs).

4. References

[1] Salt Typhoon. https://attack.mitre.org/groups/G1045/

[2] JumbledPath. https://attack.mitre.org/software/S1206/

[3] Weathering the storm: In the midst of a Typhoon. https://blog.talosintelligence.com/salt-typhoon-analysis/

[4] Indicator Removal: Clear Linux or Mac System Logs. https://attack.mitre.org/techniques/T1070/002/

[5] Game of Emperor: Unveiling Long Term Earth Estries Cyber Intrusions. https://www.trendmicro.com/en_vn/research/24/k/earth-estries.html

[6] Ghost Spider. https://fight.mitre.org/software/FGS5008/