ESET: Čínští útočníci ze skupiny Webworm rozšířili svůj kybernetický arzenál, škodlivé aktivity zacílili na Evropu

28.5.2026 - Lucie Mudráková, Vítězslav Pelc | ESET software

Kyberbezpečnostní experti z výzkumné divize společnosti ESET odhalili a analyzovali nejnovější aktivity a nástroje APT skupiny Webworm, která je napojená na Čínu. APT skupiny se zaměřují na pokročilé přetrvávající hrozby (Advanced Persistent Threats). Jedná se obvykle o seskupení útočníků z řad státních organizací nebo organizací, které pracují na objednávku států.

- Tato APT skupina začala v roce 2025 používat tzv. zadní vrátka (backdoory), která využívají Discord a Microsoft Graph API pro komunikaci se serverem útočníků (Command and Control – C&C). Experti z ESETu v souvislosti s tím dešifrovali více než 400 zpráv na platformě Discord.
- Mezi nejnovějšími nástroji skupiny vynikají zejména dva nové backdoory: EchoCreep, který využívá platformu Discord, a GraphWorm využívající rozhraní Microsoft Graph.
- Útočníci z Webworm nedávno přesunuli svou pozornost na evropské vládní organizace a rozšířili své aktivity v Jihoafrické republice.

Praha, 28. května 2026 — Bezpečnostní experti ze společnosti ESET se ve své analýze zaměřili na aktivity skupiny Webworm z roku 2025. Jedná se o tzv. APT skupinu, pokročilou přetrvávající hrozbu, která je napojená na Čínu. Skupina se původně zaměřovala na organizace v Asii, v poslední době však cílí na Evropu. Podle zjištění ESETu cílila skupina Webworm na vládní organizace v Belgii, Itálii, Polsku, Srbsku a Španělsku. V České republice zatím aktivity skupiny experti nepozorují, byť je do budoucna nelze úplně vyloučit. Zároveň s tím útočníci provedli operaci v Jihoafrické republice, kde kompromitovali místní univerzitu. Od loňského roku skupina používá tzv. zadní vrátka (backdoory), která využívají Discord a Microsoft Graph API pro komunikaci se serverem útočníků. Bezpečnostní experti dešifrovali více než 400 zpráv z Discordu a odhalili server, který útočníci využívali k průzkumu více než 50 jedinečných cílů.

„V rámci analýzy se nám podařilo získat příkazy, které útočníci zadali na svém serveru. Poskytly nám vhled do jejich technik, které využívají k získání počátečního přístupu, nebo do toho, jak využívají open-source skener zranitelností. Informace nám pomohly také identifikovat některé z jejich cílů," vysvětluje Robert Šuman, vedoucí pražské výzkumné a vývojové pobočky společnosti ESET.

Na základě informací získaných z dešifrovaných zpráv na platformě Discord ESET přisuzuje kampaň z roku 2025 APT skupině Webworm. Útočníci využili platformu Discord také pro backdoor EchoCreep, který zajistil komunikaci s jejich kontrolním serverem. Tyto informace dovedly experty až k repozitáři na GitHubu, který obsahoval připravené soubory a data, například aplikaci SoftEther VPN. V konfiguračním souboru SoftEther nalezli IP adresu, která odpovídá známé IP adrese používané skupinou Webworm.

Mezi nejnovější nástroje skupiny patří zejména dva nové backdoory: EchoCreep využívající Discord a GraphWorm využívající Microsoft Graph. Útočníci přidali k doposud využívaným proxy řešením vlastní proxy nástroje WormFrp, ChainWorm, SmuxProxy a WormSocket. Na základě jejich počtu a komplexity může Webworm vytvářet mnohem rozsáhlejší skrytou síť, a to tak, že oběti lstí přiměje ke spuštění těchto proxy nástrojů.

Mimo to začala skupina Webworm zneužívat Discord a Microsoft Graph API k ovládání a příkazům. Backdoor EchoCreep využívá Discord k nahrávání souborů, odesílání reportů o stavu fungování a přijímání příkazů. Backdoor GraphWorm využívá Microsoft Graph API pro komunikaci s kontrolním serverem. Experti z ESETu zjistili, že backdoor GraphWorm používá výhradně koncová zařízení OneDrive, a to konkrétně pro získávání nových zakázek a nahrávání dat obětí.

„Během vyšetřování kampaní z roku 2025 jsme dále zjistili, že skupina Webworm začala používat své vlastní proxy řešení WormFrp k získávání konfigurací z kompromitovaného úložiště AWS S3. Jedná se o veřejné cloudové úložiště dostupné v rámci Amazon Web Services, přičemž S3 znamená Simple Storage Service. Je zřejmé, že prostřednictvím tohoto úložiště můžou útočníci provádět exfiltraci dat, zatímco nic netušící oběť hradí náklady za tuto službu," doplňuje Šuman z ESETu.

Mezi prosincem 2025 a lednem 2026 nahráli útočníci do této služby 20 nových souborů, z nichž dva byly exfiltrovány ze španělské státní instituce. Skupina rovněž nadále ukládá soubory na GitHub a ESET předpokládá, že v tom bude pokračovat i v budoucnu.

Více informací

Více informací o popsaných aktivitách čínské APT skupiny Webworm najdete v článku na webu WeLiveSecurity.cz.

O společnosti ESET

Společnost ESET®, která byla založena v Evropě, je předním dodavatelem řešení kybernetické bezpečnosti s pobočkami po celém světě. Poskytuje špičková řešení kybernetické bezpečnosti, která pomáhají předcházet útokům ještě před jejich vznikem. ESET kombinuje technologie umělé inteligence (AI) a lidskou odbornost, čímž pomáhá předejít nově vznikajícím globálním kybernetickým hrozbám, ať již známým či dosud neznámým. Poskytuje zabezpečení pro firmy, kritickou infrastrukturu a jednotlivce. Ať už jde o ochranu koncových zařízení, cloudu nebo mobilních zařízení, řešení a služby společnosti ESET, které využívají technologie umělé inteligence a kladou důraz na cloudové prostředí, zůstávají vysoce efektivní s minimálními nároky na uživatele.

Technologie ESET jsou vyvíjeny v EU a zahrnují robustní systém detekce a reakce, ultra-bezpečné šifrování a multifaktorovou autentizaci. S nepřetržitou obranou v reálném čase a silnou místní podporou udržuje ESET uživatele v bezpečí a firmy v chodu bez narušení jejich provozu. Neustále se vyvíjející digitální prostředí vyžaduje progresivní přístup k bezpečnosti. Jen v České republice nalezneme tři výzkumná a vývojová centra společnosti, a to v Praze, Jablonci nad Nisou a Brně. Výzkumné pobočky po celém světě podporují aktivity společnosti v rámci Threat Intelligence, stejně jako její silná globální síť partnerů.

Více informací

Více informací o trendech v kyberbezpečnosti pro širokou veřejnost naleznete například v online magazínu Dvojklik.cz nebo v online magazínu o IT bezpečnosti pro firmy Digital Security Guide. Nejčastějším rizikům pro děti na internetu se věnuje iniciativa Safer Kids Online, která má za cíl pomoci nejen jejich rodičům, ale také například učitelům či vychovatelům zorientovat se v nástrahách digitálního světa.

Vysvětlení aktuálních kyberbezpečnostních pojmů a trendů najdete dále na stránkách Slovníku ESET, v podcastu RESET a na našich sociálních sítích Facebook, Instagram, LinkedIn a X.

Kontakt pro media:

Lucie Mudráková
Specialistka PR a komunikace
ESET software spol. s r.o.
tel: +420 702 206 705
lucie.mudrakova@eset.com

Vítězslav Pelc
Senior manažer PR a komunikace
ESET software spol. s r.o.
tel: +420 720 829 561
vitezslav.pelc@eset.com

https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/eset-cinsti-utocnici-ze-skupiny-webworm-rozsirili-svuj-kyberneticky-arzenal-skodlive-aktivity-zacilili-na-evropu