Postřehy z bezpečnosti: AI pomáhá tvořit malware, obcházení MFA u M365

root.cz/clanky/postrehy-z-bezpecnosti-ai-pomaha-tvorit-malware-obchazeni-mfa-u-m365

Monika Kutějová

Autor: Depositphotos

V tomto vydání Postřehů se podíváme na zneužívání chyby ve Windows, využití ChatGPT k psaní malwaru, ransomwarové skupiny zaměřené na Veeam Backup nebo únik 31 milionů údajů WaybackMachine.

Íránští hackeři zneužívají chybu ve Windows

Íránská státem sponzorovaná skupina APT34 alias OilRig nedávno vystupňovala své aktivity novými kampaněmi zaměřenými na vládní subjekty a subjekty kritické infrastruktury ve Spojených arabských emirátech a v oblasti Perského zálivu.

Útoků si všimli výzkumníci společnosti Trend Micro. Skupina OilRig při nich nasadila nový backdoor zaměřený na servery Microsoft Exchange za účelem odcizení přihlašovacích údajů, a zároveň zneužila chybu systému Windows CVE-2024–30088 ke zvýšení svých oprávnění na napadených zařízeních.

Kromě této aktivity společnost Trend Micro také zjistila spojení mezi OilRig a FOX Kitten, další íránskou APT skupinou zapojenou do ransomwarových útoků.

Útoky začínají zneužitím zranitelného webového serveru k nahrání web shellu, což útočníkům umožňuje spustit vzdálený kód a PowerShell příkazy. Jakmile je web shell aktivní, OilRig jej využívá k nasazení dalších nástrojů, včetně komponenty určené ke zneužití chyby CVE-2024–30088.

CVE-2024–30088 je zranitelnost s vysokou mírou eskalace oprávnění, kterou společnost Microsoft opravila v červnu 2024 a která útočníkům umožňuje eskalovat svá oprávnění na úroveň SYSTEM, což jim poskytuje významnou kontrolu nad napadenými zařízeními. Společnost Microsoft potvrdila, že pro CVE-2024–30088 existuje proof-of-concept exploitu, ale na svém bezpečnostním portálu zatím neoznačila tuto chybu jako aktivně zneužívanou.

V dalším kroku skupina OilRig zaregistruje knihovnu DLL filtru hesel, která zachytí přihlašovací údaje v prostém textu během změny hesla, a poté stáhne a nainstaluje nástroj pro vzdálené monitorování a správu `ngrok`, který se používá pro skrytou komunikaci prostřednictvím zabezpečených tunelů.
Další novou taktikou těchto útočníků je zneužívání lokálních serverů Microsoft Exchange ke krádeži přihlašovacích údajů a exfiltraci citlivých dat prostřednictvím legitimního e-mailového provozu, který je obtížné odhalit. Exfiltraci usnadňuje nový backdoor s názvem „StealHook“. „Klíčovým cílem této fáze je zachytit ukradená hesla a předat je útočníkům jako přílohy e-mailu,“ vysvětluje Trend Micro ve zprávě. „Navíc jsme vypozorovali, že aktéři hrozeb využívají legitimní účty s ukradenými hesly k tomu, aby tyto e-maily směrovali přes vládní servery Exchange.“

TrendMicro tvrdí, že mezi StealHookem a backdoory, které byly použity v minulých kampaních, existuje podobnost kódu, takže nejnovější malware se zdá být spíše evolučním krokem než novým výtvorem. Není to také poprvé, co

OilRig použil servery Microsoft Exchange jako aktivní součást svých útoků. Téměř před rokem společnost Symantec oznámila, že APT34 nainstalovala na lokální servery Exchange backdoor PowerShell nazvaný „PowerExchange“, který byl schopen přijímat a vykonávat příkazy prostřednictvím e-mailu.

Skupina OilRig je velmi aktivní v regionu Blízkého východu a její spojení s FOX Kitten je sice v tuto chvíli nejasné, ale znepokojující pro možnost přidání ransomwaru do jejího útočného arzenálu.

Vzhledem k tomu, že většina cílových subjektů působí v energetickém sektoru, by podle společnosti Trend Micro mohlo mít narušení provozu těchto organizací vážné dopady pro mnoho lidí.

OpenAI potvrdila používání ChatGPT k psaní malwaru

Společnost OpenAI narušila více než 20 škodlivých kybernetických operací zneužívajících jejího chatbota ChatGPT s umělou inteligencí k ladění a vývoji malwaru, šíření dezinformací, obcházení detekce a provádění spear-phishingových útoků.

Zpráva, která se zaměřuje na operace od začátku roku, představuje první oficiální potvrzení, že generativní nástroje AI jsou využívány k posílení útočných kybernetických operací. První známky takové činnosti ohlásila v dubnu společnost Proofpoint, která podezřívala skupinu TA547 (alias „Scully Spider“) z nasazení payloadu PowerShell napsaného umělou inteligencí pro jejich finální payload, infostealer Rhadamanthys.

Minulý měsíc výzkumníci společnosti HP Wolf s velkou jistotou oznámili, že kyberzločinci zaměřující se na francouzské uživatele využívají nástroje AI k psaní skriptů používaných v rámci vícekrokového infekčního řetězce.

Nejnovější zpráva společnosti OpenAI potvrzuje zneužívání nástroje ChatGPT a uvádí případy, kdy jej čínští a íránští aktéři hrozeb využívají ke zvýšení efektivity svých operací. Prvním aktérem, kterého OpenAI představila, je „SweetSpecter“ – čínský protivník, který byl poprvé zdokumentován analytiky společnosti Cisco Talos v listopadu 2023 jako kybernetická špionážní skupina zaměřená na asijské vlády. Společnost OpenAI uvádí, že SweetSpecter se zaměřil přímo na ni a na osobní e-mailové adresy zaměstnanců společnosti OpenAI zasílal spear phishingové e-maily se škodlivými přílohami

ZIP maskovanými jako žádosti o podporu. Pokud byly přílohy otevřeny, spustil se infekční řetězec, který vedl k tomu, že se do systému oběti spustil SugarGh0st RAT. Při dalším vyšetřování společnost OpenAI zjistila, že SweetSpecter používá skupinu účtů ChatGPT, které provádějí výzkum skriptování a analýzy zranitelností pomocí nástroje LLM.

Druhý případ se týká s íránskou vládou spřízněné skupiny kybernetických hrozeb „CyberAv3ngers“, která je známá tím, že se zaměřuje na průmyslové systémy v kritických infrastrukturách západních zemí. OpenAI uvádí, že účty spojené s touto skupinou požádaly ChatGPT o vytvoření výchozích pověření v široce používaných programovatelných logických automatech (PLC), vytvoření vlastních skriptů v jazycích bash a Python a obfuskaci kódu.

Íránští hackeři také používali ChatGPT k plánování svých aktivit po kompromitaci, k učení se, jak využívat konkrétní zranitelnosti, a k výběru metod krádeže uživatelských hesel v systémech macOS.

Třetí případ, na který upozorňuje zpráva OpenAI, se týká Storm-0817, rovněž íránských aktérů. Tato skupina údajně použila ChatGPT k ladění malwaru, vytvoření Instagram scraperu, překladu profilů LinkedIn do perštiny a vývoji vlastního malwaru pro platformu Android spolu s podpůrnou příkazovou a řídicí infrastrukturou. Malware vytvořený pomocí chatbota OpenAI dokáže ukrást seznamy kontaktů, protokoly hovorů a soubory uložené v zařízení, pořizovat snímky obrazovky, zkoumat historii procházení a zjistit přesnou polohu uživatele.

„Současně STORM-0817 používal ChatGPT k podpoře vývoje kódu na straně serveru, který je nezbytný pro zpracování připojení z napadených zařízení,“ uvádí se ve zprávě Open AI. „To nám umožnilo zjistit, že C2 server pro tento malware je konfigurace `WAMP` (Windows, Apache, MySQL & PHP/Perl/Python) a během testování používal doménu `stickhero[.]pro`.“

Všechny účty OpenAI používané výše uvedenými aktéry byly zakázány a související indikátory kompromitace, včetně IP adres, byly sdíleny s partnery v oblasti kybernetické bezpečnosti. Ačkoliv žádný z výše popsaných případů neposkytuje aktérům nové schopnosti při vývoji malwaru, představují důkaz, že nástroje generativní umělé inteligence mohou zefektivnit útočné operace aktérů s nízkou kvalifikací a pomáhat jim ve všech fázích, od plánování až po provedení.

Ukrajina zatkla provozovatele VPN poskytujícího přístup k Runetu

Ukrajinská kybernetická policie zatkla 28letého muže, který provozoval rozsáhlou službu virtuální privátní sítě (VPN), jež umožňovala lidem ze země přístup na ruský internet (Runet).

Runet je část internetu, která zahrnuje ruské stránky na doménách nejvyšší úrovně „ `.ru` “ a „ `.su` “, včetně vládních stránek, platforem sociálních médií, vyhledávačů a různých zpravodajských platforem z této země. Ruská vláda podnikla kroky ke kontrole, omezení, monitorování a izolaci od širšího globálního internetu.

Podle omezení a sankcí uvalených ukrajinskou Radou národní bezpečnosti a obrany (NSDC) je přístup na Runet zakázán. Proto ukrajinští poskytovatelé internetových služeb (ISP) blokují přístup k ruským platformám ze země. Služba VPN, která vznikla krátce po ruské invazi na Ukrajinu, umožnila Rusům na okupovaných územích i ruským sympatizantům po celé Ukrajině omezení obejít. Jedná se o porušení části 5 článku 361 ukrajinského trestního zákoníku, za což samouk hacker z Chmelnyckého čelí obvinění, za které mu hrozí až 15 let vězení.

Podle oznámení policie služba VPN nabízela přístup k více než 48 milionům IP adres Runetu a umožňovala síťový provoz, který denně přesahoval 100 gigabajtů.

Služba byla inzerována prostřednictvím kanálů Telegramu a souvisejících online komunit. Samotný hacker se představoval jako vývojář projektu. Podezřelý řídil podvodnou službu VPN z autonomního serveru umístěného v jeho bytě. Zároveň si pronajímal servery v Německu, Francii, Nizozemsku a Rusku, aby usnadnil přístup do ruské sítě. Z tohoto důvodu se ukrajinská policie domnívá, že agenti ruské rozvědky měli přístup k informacím o uživatelích služby VPN.

Při zatýkání a souvisejících prohlídkách v Chmelnyckém a Žytomyru policie zabavila serverové vybavení, počítače a mobilní telefony. Policie v současné době analyzuje získaná data a doufá, že se jí podaří identifikovat další komplice nebo ruské agenty úzce spolupracující s provozovatelem služby VPN.

Ransomware Akira a Fog zneužívají kritickou chybu Veeam RCE

Ransomwarové gangy nyní využívají kritickou bezpečnostní chybu, která útočníkům umožňuje vzdálené spuštění kódu (RCE) na zranitelných serverech Veeam Backup & Replication (VBR).

Bezpečnostní výzkumník společnosti Code White Florian Hauser zjistil, že bezpečnostní chyba, nyní sledovaná jako CVE-2024–40711, je způsobena slabinou v deserializaci nedůvěryhodných dat, kterou mohou neautentifikovaní aktéři zneužít při útocích s nízkou složitostí.

Společnost Veeam chybu odhalila a vydala aktualizace zabezpečení 4. září, zatímco společnost watchTowr Labs zveřejnila technickou analýzu 9. září. Společnost watchTowr Labs však odložila zveřejnění kódu proof-of-concept exploitu až na 15. září, aby poskytla správcům dostatek času na zabezpečení svých serverů.

Důvodem tohoto zpoždění byly podniky, které používají software VBR společnosti Veeam jako řešení pro ochranu dat a obnovu po havárii pro zálohování, obnovu a replikaci virtuálních, fyzických

a cloudových počítačů. To z něj činí velmi oblíbený cíl pro škodlivé subjekty, které se snaží získat rychlý přístup k zálohovaným datům společnosti.

Jak zjistili pracovníci společnosti Sophos X-Ops v průběhu minulého měsíce, chyba CVE-2024–40711 RCE byla rychle zachycena a zneužita při útocích ransomwaru Akira a Fog spolu s dříve kompromitovanými přihlašovacími údaji k přidání místního účtu „point“ do místních skupin Administrators a Remote Desktop Users.

„V jednom případě útočníci shodili ransomware Fog. Jiný útok ve stejném časovém rámci se pokusil nasadit ransomware Akira. Indikátory se ve všech 4 případech překrývají s dřívějšími útoky ransomwaru Akira a Fog,“ uvedla společnost Sophos X-Ops. „V každém z případů útočníci zpočátku přistupovali k cílům pomocí napadených bran VPN bez zapnuté vícefaktorové autentizace. Na některých z těchto VPN byly provozovány nepodporované verze softwaru. „V případě ransomwaru Fog jej útočník nasadil na nechráněný server Hyper-V a poté použil k exfiltraci dat nástroj `rclone`.“

V loňském roce, 7. března 2023, společnost Veeam rovněž opravila vysoce závažnou zranitelnost v softwaru Backup & Replication (CVE-2023–27532), kterou lze zneužít k narušení hostů zálohovací infrastruktury. O několik týdnů později, koncem března, zaznamenala finská společnost WithSecure zneužití CVE-2023–27532 nasazené v útocích spojených s finančně motivovanou skupinou FIN7, která je známá svými vazbami na ransomwarové operace Conti, REvil, Maze, Egregor a BlackBasta. O několik měsíců později byl stejný exploit Veeam VBR použit v ransomwarových útocích na Kubě proti americké kritické infrastruktuře a latinskoamerickým IT společnostem.

Společnost Veeam uvádí, že její produkty používá více než 550 000 zákazníků po celém světě, včetně nejméně 74 % všech společností z globální dvoutisícovky.

Únik dat WaybackMachine má dopad na 31 milionů uživatelů

Internetový archiv „The Wayback Machine“ utrpěl únik dat po napadení webových stránek a ukradení databáze ověření uživatelů obsahující 31 milionů unikátních záznamů.

Zpráva o narušení se začala šířit ve středu odpoledne poté, co se návštěvníkům stránek archive.org začalo zobrazovat hackerem vytvořené upozornění v JavaScriptu, které uvádělo, že Internet Archive byl narušen. „Měli jste někdy pocit, že internetový archiv běží jako na drátkách a je neustále na pokraji katastrofálního narušení bezpečnosti? Právě se to stalo. Uvidíme se s 31 miliony z vás na HIBP!“, stojí v upozornění JavaScriptu zobrazeném na napadené stránce `archive.org`.

Text „HIBP“ odkazuje na službu Have I Been Pwned pro oznamování narušení dat, kterou vytvořil Troy Hunt. Hunt sdělil serveru BleepingComputer, že aktér sdílel autentizační databázi Internet Archive před devíti dny a jedná se o 6,4GB soubor SQL s názvem „ `ia_users.sql` “. Databáze obsahuje autentizační informace o registrovaných členech, včetně jejich e-mailových adres, jmen, časových razítek změn hesel, hesel zašifrovaných šifrou Bcrypt a dalších interních údajů. Nejnovější časové razítko na ukradených záznamech je z 28. září 2024, tedy pravděpodobně z doby, kdy byla databáze ukradena.

Podle Hunta je v databázi 31 milionů unikátních e-mailových adres a mnoho z nich se přihlásilo k odběru služby HIBP pro oznamování narušení dat. Údaje budou brzy přidány do služby HIBP, což uživatelům umožní zadat svůj e-mail a potvrdit, zda byly jejich údaje při tomto narušení vystaveny.

Skutečnost, že údaje jsou pravé, byla potvrzena poté, co společnost Hunt kontaktovala uživatele uvedené v databázích, včetně výzkumníka v oblasti kybernetické bezpečnosti Scotta Helmeho, jenž povolil serveru BleepingComputer sdílet svůj odhalený záznam. Helme potvrdil, že heslo zašifrované šifrou bcrypt v datovém

záznamu se shoduje s heslem zašifrovaným šifrou brcrypt uloženým ve správci hesel. Potvrdil také, že časové razítko v databázovém záznamu odpovídá datu, kdy naposledy změnil heslo ve svém správci hesel.

Hunt tvrdí, že před třemi dny kontaktoval internetový archiv a zahájil proces zveřejnění s tím, že data budou do služby vložena do 72 hodin, ale od té doby se mu nikdo neozval. Není známo, jakým způsobem se aktéři do internetového archivu dostali a zda byla odcizena nějaká další data. Internet Archive navíc dne 9. října utrpěl útok DDoS, k němuž se přihlásila hackerská skupina BlackMeta s tvrzením, že bude provádět další útoky.

Ačkoliv internetový archiv čelí narušení dat i útokům DDoS současně, nepředpokládá se, že by tyto dva útoky spolu souvisely.

Nová služba Mamba 2FA bypass se zaměřuje na účty M365

V minulém týdnu byla pozorována nová platforma phishing-as-a-service (PhaaS) s názvem Mamba 2FA, která se zaměřuje na účty Microsoft 365 v rámci AiTM útoků pomocí dobře vytvořených přihlašovacích stránek. Mamba 2FA navíc nabízí aktérům hrozeb mechanismus AiTM (adversary-in-the-middle) k získání autentizačních tokenů oběti a obejití ochrany vícefaktorového ověřování (MFA) na jejich účtech.

Mamba 2FA se v současné době prodává kyberzločincům za 250 USD měsíčně, což je konkurenceschopná cena, která ji řadí mezi nejlákavější a nejrychleji rostoucí phishingové platformy v této oblasti. Mamba 2FA byla poprvé zdokumentována analytiky Any.Run koncem června 2024, ale společnost Sekoia uvádí, že sleduje aktivity spojené s touto phishingovou platformou již od května 2024.

Další důkazy ukazují, že Mamba 2FA podporovala phishingové kampaně od listopadu 2023. Po zprávě Any.Run o kampani podporované platformou Mamba 2FA provedli provozovatelé phishingové platformy několik změn ve své infrastruktuře a

metodách, aby zvýšili skrytost a životnost phishingových kampaní. Od října například Mamba 2FA zavedla proxy servery pocházející od komerčního poskytovatele IPRoyal, aby maskovala IP adresy relay serverů v ověřovacích protokolech. Dříve se relay servery připojovaly přímo k serverům Microsoft Entra ID, což odhalovalo IP adresy a usnadňovalo blokování. Domény odkazů používané ve phishingových adresách URL jsou nyní velmi krátkodobé a obvykle se střídají každý týden, aby se zabránilo jejich blokování bezpečnostními řešeními.

Další změnou bylo vylepšení příloh HTML používaných v phishingových kampaních neškodným výplňovým obsahem, který skrývá malý fragment JavaScriptu spouštějícího útok, což ztěžuje jeho odhalení bezpečnostními nástroji.

Mamba 2FA je speciálně navržena tak, aby cílila na uživatele služeb Microsoft 365, včetně firemních a spotřebitelských účtů. Stejně jako jiné podobné platformy PhaaS využívá k provádění phishingových útoků AiTM proxy relaye, které aktérům hrozby umožňují přístup k jednorázovým přístupovým kódům a ověřovacím souborům cookie. Mechanismus AiTM využívá knihovnu Socket.IO JavaScript k navázání komunikace mezi phishingovou stránkou a relay servery na backendu, které následně komunikují se servery společnosti Microsoft pomocí ukradených údajů. Mamba 2FA nabízí podvodné šablony pro různé služby Microsoft 365, včetně OneDrive, SharePoint Online, obecných přihlašovacích stránek Microsoftu a falešných oznámení hlasové schránky, která přesměrovávají na přihlašovací stránku Microsoftu.

U podnikových účtů podvodné stránky dynamicky přebírají vlastní přihlašovací značku cílové organizace, včetně loga a obrázků na pozadí, takže pokus vypadá autentičtěji. Zachycené přihlašovací údaje a ověřovací soubory cookie jsou útočníkovi předány prostřednictvím bota Telegramu, což mu umožní okamžitě zahájit relaci.

Mamba 2FA je také vybavena funkcí detekce sandboxu, která uživatele přesměruje na webové stránky Google 404, když usoudí, že je analyzován. Celkově je platforma Mamba 2FA další hrozbou pro organizace, která umožňuje málo kvalifikovaným aktérům provádět vysoce účinné phishingové útoky.

Chcete-li se chránit před operacemi PhaaS pomocí taktiky AiTM, zvažte použití hardwarových bezpečnostních klíčů, ověřování na základě certifikátů, zeměpisného blokování, IP allowlistingu, device allowlistingu a zkracování životnosti tokenů.

Ve zkratce

- CISA: Hackeři zneužívají soubory cookie F5 BIG-IP k mapování interních serverů
- Společnost Casio potvrdila krádež dat zákazníků při útoku ransomwaru
- USA a Spojené království varují před ruskými hackery APT29, kteří útočí na servery Zimbra a TeamCity
- CISA: kritická chyba RCE Fortinet je nyní zneužívána k útokům
- Mozilla opravuje zero-day Firefoxu aktivně zneužívaný při útocích
- Discord zablokován v Rusku a Turecku kvůli šíření nelegálního obsahu
- Microsoft opravil problémy se vzdálenou plochou způsobené aktualizací Windows Server
- Ukrajinec se přiznal k provozování malwaru Raccoon Stealer
- Společnost American Water po kybernetickém útoku vypnula online služby

O seriálu

Tento seriál vychází střídavě za pomoci pracovníků Národního bezpečnostního týmu CSIRT.CZ provozovaného sdružením CZ.NIC a bezpečnostního týmu CESNET-CERTS sdružení CESNET, bezpečnostního týmu CDT-CERT provozovaného společností ČD -

Telematika a bezpečnostních specialistů Jana Kopřivy ze společnosti Nettles Consulting a Moniky Kutějové ze sdružení TheCyberValkyries. Více o seriálu…