Íránští hackeři nyní využívají chybu Windows ke zvýšení oprávnění

bleepingcomputer.com/news/security/oilrig-hackers-now-exploit-windows-flaw-to-elevate-privileges

Bill Toulas

Podle
Bill Toulas

- 13. října 2024
- 10:17
- 1

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

V těchto útocích, které zaznamenali výzkumníci Trend Micro, OilRig nasadil nová zadní vrátka zaměřená na servery Microsoft Exchange ke krádeži přihlašovacích údajů a také využila chybu Windows CVE-2024-30088 ke zvýšení svých oprávnění na kompromitovaných zařízeních.

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

Nejnovější útočný řetěz OilRig

Útoky, které zaznamenala společnost Trend Micro, začínají zneužitím zranitelného webového serveru k nahrání webového shellu, což útočníkům dává možnost spouštět vzdálený kód a příkazy PowerShellu.

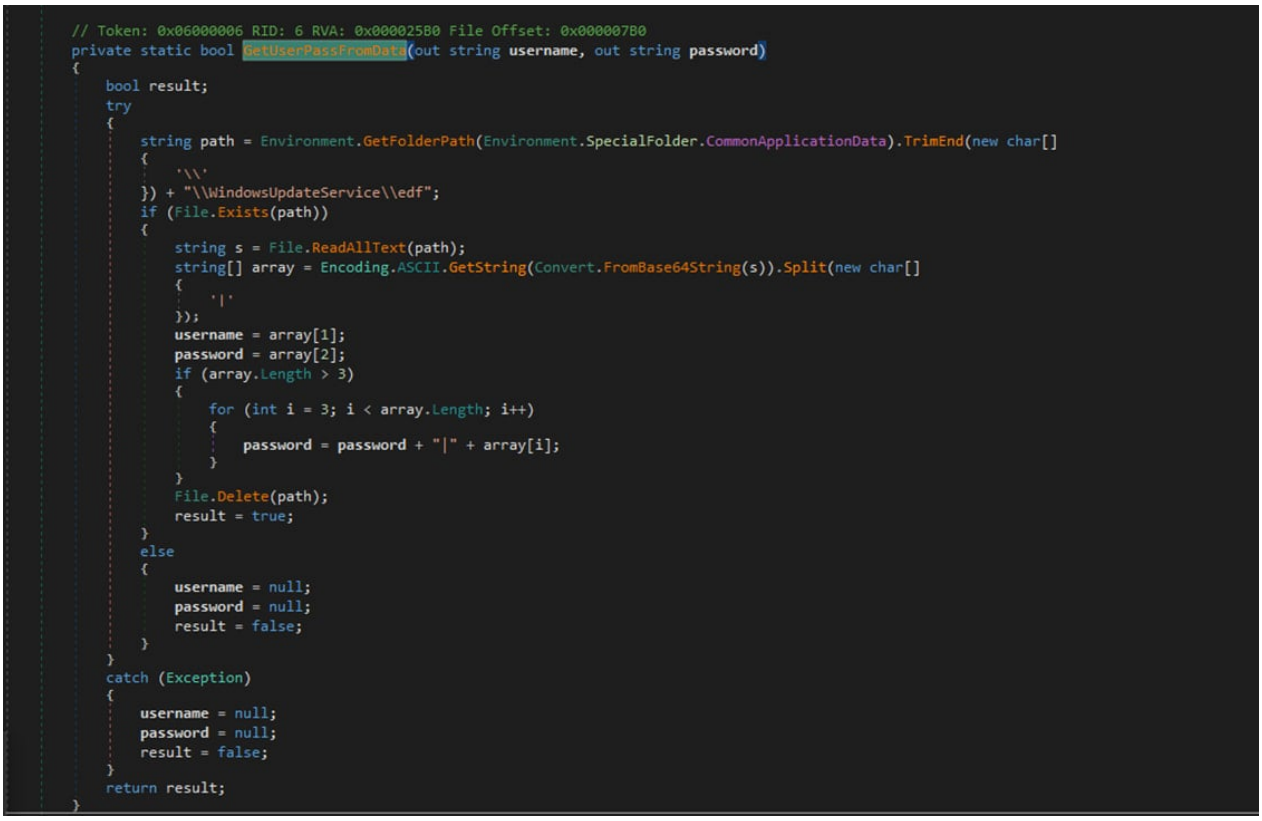
Jakmile je webový shell aktivní, OilRig jej využije k nasazení dalších nástrojů, včetně komponenty navržené k využití chyby Windows CVE-2024-30088.

CVE-2024-30088 je velmi závažná chyba zabezpečení týkající se eskalace oprávnění, kterou společnost Microsoft opravila v červnu 2024 a umožňuje útočníkům eskalovat svá oprávnění na úroveň SYSTÉMU, což jim poskytuje významnou kontrolu nad napadenými zařízeními.

Společnost Microsoft přiznala zneužití CVE-2024-30088 v rámci proof-of-concept, ale zatím tuto chybu na svém bezpečnostním portálu neoznačila jako aktivně využívanou. CISA ji také nenahlásila jako dříve zneužitou v katalogu ts Known Exploited Vulnerability.

Dále OilRig zaregistruje knihovnu DLL filtru hesel, která zachytí pověření ve formátu prostého textu během událostí změny hesla, a poté stáhne a nainstaluje nástroj pro vzdálené monitorování a správu „ngrok“, který se používá pro tajnou komunikaci prostřednictvím zabezpečených tunelů.

Další novou taktikou aktérů hrozeb je zneužívání on-premise serverů Microsoft Exchange ke krádeži přihlašovacích údajů a exfiltraci citlivých dat prostřednictvím legitimního e-mailového provozu, který je těžké odhalit.



```
// Token: 0x06000006 RID: 6 RVA: 0x00002580 File Offset: 0x00000780
private static bool GetUserPassFromData(out string username, out string password)
{
    bool result;
    try
    {
        string path = Environment.GetFolderPath(Environment.SpecialFolder.CommonApplicationData).TrimEnd(new char[]
        {
            '\\'
        }) + "\\WindowsUpdateService\\edf";
        if (File.Exists(path))
        {
            string s = File.ReadAllText(path);
            string[] array = Encoding.ASCII.GetString(Convert.FromBase64String(s)).Split(new char[]
            {
                '|'
            });
            username = array[1];
            password = array[2];
            if (array.Length > 3)
            {
                for (int i = 3; i < array.Length; i++)
                {
                    password = password + "|" + array[i];
                }
            }
            File.Delete(path);
            result = true;
        }
        else
        {
            username = null;
            password = null;
            result = false;
        }
    }
    catch (Exception)
    {
        username = null;
        password = null;
        result = false;
    }
    return result;
}
```

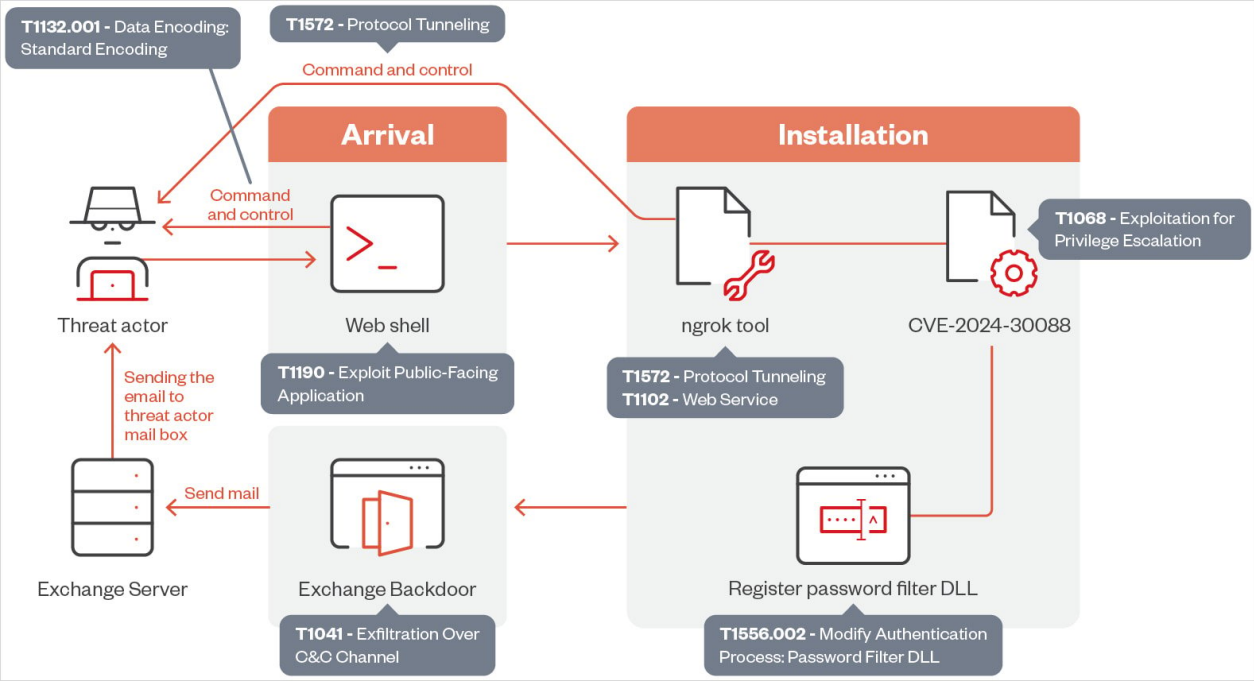
Backdoor kradení hesel z Exchange

Zdroj: Trend Micro

Exfiltraci usnadňují nová zadní vrátka s názvem „StealHook“, zatímco Trend Micro říká, že vládní infrastruktura se často používá jako klíčový bod, aby se proces zdál legitimní.

„Klíčovým cílem této fáze je zachytit ukradená hesla a předat je útočníkům jako přílohy e-mailů,“ vysvětluje Trend Micro ve zprávě .

"Navíc jsme zjistili, že aktéři hrozeb využívají legitimní účty s ukradenými hesly k směrování těchto e-mailů přes vládní servery Exchange."



Nejnovější útočný řetězec OilRig

Zdroj: Trend Micro

TrendMicro říká, že existují podobnosti kódu mezi StealHook a backdoors OilRig používanými v minulých kampaních, jako je Karkoff , takže nejnovější malware se zdá být spíše evolučním krokem než novým vytvořením od nuly.

Není to také poprvé, co OilRig použil servery Microsoft Exchange jako aktivní součást svých útoků. Téměř před rokem společnost Symantec oznámila , že APT34 nainstaloval backdoor PowerShell nazvaný „PowerExchange“ na místní servery Exchange schopné přijímat a spouštět příkazy prostřednictvím e-mailu.

Aktér ohrožení zůstává vysoce aktivní v regionu Středního východu a jeho spojení s FOX Kitten, i když není v tuto chvíli jasné, znepokojuje potenciál přidání ransomwaru do jeho útočného arzenálu.

Vzhledem k tomu, že většina cílových subjektů je v energetickém sektoru, podle Trend Micro by provozní výpadky v těchto organizacích mohly vážně ovlivnit mnoho lidí.

Související články:

CISA říká, že kritická chyba Fortinet RCE se nyní využívá při útocích

Mozilla opravuje Firefox zero-day aktivně zneužívaný při útocích

Ivanti varuje před třemi dalšími nultými dny CSA zneužitými při útocích

Qualcomm opravuje vysoce závažné zero-day útoky

Přes 4 000 obchodů Adobe Commerce a Magento bylo napadeno útoky CosmicSting

Bill Toulas

Bill Toulas je technický spisovatel a zpravodaj infosec s více než desetiletými zkušenostmi s prací na různých online publikacích, které pokrývají open-source, Linux, malware, incidenty narušení dat a hacky.

- Předchozí článek
- Další článek

Komentáře

blackhatcat - Před 1 dnem

proč se obtěžovat používáním exploitů, když existují nástroje jako nsudo/nanarun a snadno umožňují spuštění eskalace jako systémový nebo důvěryhodný instalační program

Fotogra
blackha

Přidat komentářPravidla komunity

Pro přidání komentáře se musíte přihlásit

Ještě nejste členem? Zaregistrujte se nyní

Také by se vám mohlo líbit: