PREMIUM reporty o APT zo služby ESET Threat Intelligence

UŽÍVAJTE SI BEZPEČNEJŠIE TECHNOLÓGIE™

VÝSKUM HROZIEB

SÚHRN AKTIVITY

Vydanie:

AS-2021-0007

1. apríla – 15. apríla 2021

SKUPINA LAZARUS

Prehľad skupiny

Skupina Lazarus, ktorá je aktívna minimálne od roku 2009, má na svedomí významné bezpečnostné incidenty, ako napríklad hackerský útok na filmové štúdio Sony Pictures Entertainment v roku 2016, kybernetické krádeže v hodnote desiatok miliónov dolárov v roku 2016 či šírenie malvéru WannaCryptor (tiež známeho ako WannaCry) v roku 2017. Táto skupina má za obdobie od roku 2011 po súčasnosť na svojom konte celú sériu útokov zameraných na širokú verejnosť aj kritickú infraštruktúru v Južnej Kórei. Skupina Lazarus je známa predovšetkým rozmanitosťou a početnosťou útočných kampaní, okázalosťou pri ich realizácii, ako aj tým, že u nej vidíme všetky tri piliere kybernetického zločinu: špionáž, sabotáž a honbu za finančným ziskom.

Súhrn aktivity

Operácia In(ter)ception

Operácia In(ter)ception je názov, ktorým spoločnosť ESET označuje sériu útokov pripisovaných skupine Lazarus. Tieto útoky pretrvávajú už minimálne od septembra 2019 a sú cielené na spoločnosti z oblasti letectva, armády a obrany. Operácia je zaujímavá tým, že pracuje s technikou spearphishingu využitím platformy LinkedIn a zároveň zapája špeciálne metódy, aby sa efektívne vyhýbala odhaleniu. Jej hlavným cieľom je podľa všetkého firemná špionáž.

Začiatkom apríla 2021 sa na stránke VirusTotal objavila nová verzia downloadera Stage 1. Hlavná funkcia a štruktúra malvéru zostala rovnaká, novinkou je jednobajtové XOR šifrovanie dôležitých reťazcov, ako sú URL, User-Agent a HTTP hlavičky, čo sťažuje ich čítanie počas statickej analýzy.

Viktimológia/Cieľové oblasti

Spoločnosti zo sféry letectva, armády a obrany

Vektor útoku

Nevzťahuje sa

Aktivita po napadnutí

Nevzťahuje sa

Indikátory IoC

Operácia In(ter)ception

Dátum	**2021-04-07 00:08:38**
MD5	2CBE0BEA035DB9240CEB338CF9EA7FE6
SHA-1	9A8B7F11104156F0DF4F07827EC12E5C2300C4EE
SHA-256	40B6CBCC594D3696952E90FA15CCD733EBC2777554092E8C15694334274E5B90
Názov súboru	c.exe
Popis	Stage 1 loader.
C&C	*https://kehot.com[.]ar/Pubs/menus.jpg* https://www.meisami[.]net/css/search.css https://www.sfaonweb[.]com/pdf/{A76E7D01-6BAF-4FE4-98E0-.pdf *https://amon-werbeartikel[.]de/Media/Uploaded/chrisen.png*
Detekcia	Win64/Interception.G
Čas kompilácie PE	2020-02-04 18:01:33 (podľa časovej pečiatky)

PREMIUM reporty o APT zo služby ESET Threat Intelligence

VÝSKUM HROZIEB

TECHNICKÁ ANALÝZA NETVULTURE A TURLACHOPPER

Vydanie:

TA-2021-0002

12. marca 2021

ZHRNUTIE

Turla je neslávne známa špionážna skupina, ktorá pôsobí v oblasti kybernetického zločinu už viac ako desaťročie. Zameriava sa hlavne na významné ciele ako vlády a diplomatické subjekty v Európe, Strednej Ázii a na Blízkom východe. Je známe, že stála za úspešnými útokmi na veľké organizácie, napríklad na americké ministerstvo obrany v roku 2008 a na švajčiarsku spoločnosť RUAG podnikajúcu v zbrojárstve v roku 2014. Počas posledných niekoľkých rokov sme *zdokumentovali veľkú časť arzenálu, ktorým táto skupina disponuje*, s cieľom zvýšiť povedomie o jej činnosti.

V januári 2021 sme zaznamenali podozrivú aktivitu na serveri Microsoft Exchange patriacom ministerstvu zahraničných vecí vo východnej Európe. Objavili sme dve nové rodiny malvéru, ktoré pripisujeme skupine Turla: TurlaChopper a NETVulture.

Kľúčové body tohto reportu:

- Server Microsoft Exchange Outlook Web Access bol napadnutý pravdepodobne zneužitím zraniteľnosti CVE-2020-0688.
- Na tento server útočníci nasadili vlastný škodlivý kód typu webshell, ktorý sme nazvali TurlaChopper.
- O dva mesiace neskôr útočníci nasadili dovtedy neznámy backdoor, ktorý sme pomenovali NETVulture, na iný Windows server rovnakej organizácie. Na jeho inštaláciu pravdepodobne využili TurlaChopper.
- NETVulture je backdoor vyvinutý na platforme .NET, ktorý používa Microsoft OneDrive ako svoj riadiaci C&C server.
- Inštancie NETVulture a TurlaChopper boli aktívne používané na škodlivé účely od začiatku roka 2020 do začiatku januára 2021.

PROFIL SKUPINY TURLA

Turla, tiež známa ako Snake, je neslávne známa špionážna skupina, ktorá pôsobí v oblasti kybernetického zločinu prinajmenšom desať rokov. Pre túto skupinu je príznačné používanie vlastných pokročilých nástrojov a schopnosť vykonávať vysoko cielené operácie.

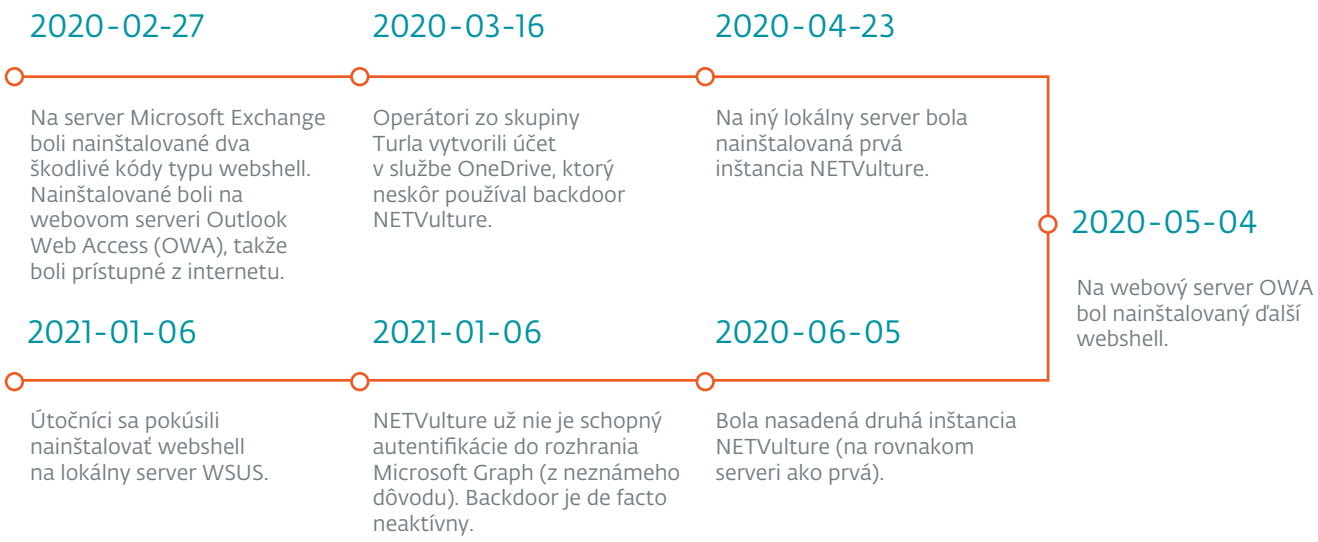
Za viac ako desaťročie sa Turla podpísala pod mnohé útoky na významné ciele, napríklad *Ústredné velenie Spojených štátov (CENTCOM)* v roku 2008, *fínske ministerstvo zahraničných vecí* v roku 2013, švajčiarsku zbrojársku spoločnosť RUAG v roku 2014 a *nemecké ministerstvo zahraničných vecí* v roku 2017. Z nedávnej minulosti má údajne na svedomí útoky na *francúzske ozbrojené sily* v roku 2018 a *rakúske ministerstvo zahraničných vecí* v roku 2019. Na časovej osi na obrázku 1 sú uvedené niektoré z hlavných útokov, ktoré sa verejne pripisujú skupine Turla.

Obrázok 1: Časová os útokov verejne pripisovaných skupine Turla

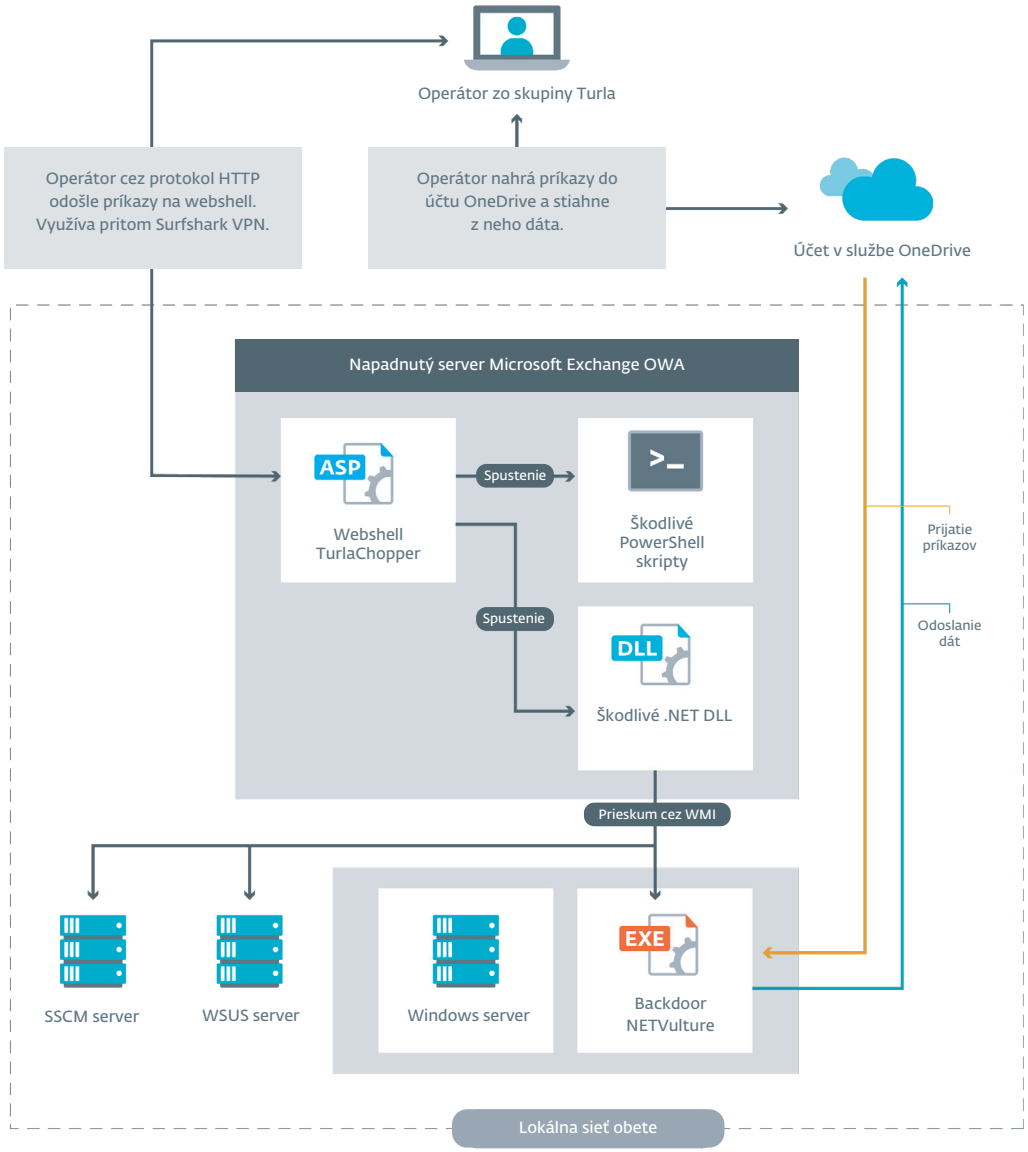
V uplynulých rokoch sa skupina Turla pomerne konzistentne zameriavala na tie isté cieľové oblasti:

- ministerstvá zahraničných vecí a diplomatické zastúpenia (veľvyslanectvá, konzuláty atď.),
- armádne organizácie,
- regionálne politické organizácie,
- dodávateľov tovarov a služieb zo sféry obrany.

Skupina má vo svojom arzenáli množstvo rôznych malvérových rodín, počnúc malvérom Skipper, ktorý sa často objavuje pri *útokoch uplatňujúcich techniku Watering Hole*, až po sofistikované backdoory, ako je napríklad *ComRAT v4* využívajúci Gmail na komunikáciu s C&C serverom, *LightNeuron* špeciálne navrhnutý pre e mailové servery Microsoft Exchange či backdoor *Crutch* používajúci Dropbox ako svoj C&C server.



Obrázok 2: Časová os dôležitých udalostí týkajúcich sa incidentu NETVulture



Obrázok 3: Prehľad fungovania TurlaChopper a NETVulture