



Dead Drop Resolvers - Espionage Inspired C&C Communication



- April 07, 2021

A “dead drop” is a well-known espionage tactic of passing items or information between two parties using secret locations. The two parties never meet and any sign of communication is concealed. This tactic is commonly used by intelligence officers to interact with their assets in the field to avoid any suspicious meetings or either caught talking to each other. For decades, intelligence agencies have used dead drops. Two infamous double agents from the CIA and FBI - [Aldrich Ames](#) and [Robert Hanssen](#) respectively - both used dead drops to supply information to their handlers from the Soviet Union. Cyber adversaries have also come to adapt this technique into their espionage campaigns. However, instead of a human source, state-backed computer network operations (CNOs) have leveraged legitimate services for covert communications or so-called “dead drop resolvers”.

In October 2019, ESET Research disclosed a report on *Operation Ghost Dukes* which detailed the activities of an APT group known as TheDukes (also called APT29 or CozyBear). This particular group reportedly operates on behalf of the Russian foreign intelligence service (also known as the SVR). It was made infamous for compromising the Democratic National Committee (DNC) in 2016 during the run-up to the US election. *Operation Ghost Dukes* likely began in 2013 and targeted government entities for years whilst attracting very little attention. One key reason why TheDukes were able to go undetected for this length of time was partly due the use of online services as dead drop resolvers including Twitter, Imgur, and Reddit. These acted as primary command and control (C&C) channels for the first stage of their malware.

Ce site utilise des cookies provenant de Google pour fournir ses services et analyser le trafic. Votre adresse IP et votre user-agent, ainsi que des statistiques relatives aux performances et à la sécurité, sont transmis à Google afin d'assurer un service de qualité, de générer des statistiques d'utilisation, et de détecter et de résoudre les problèmes d'abus.

EN SAVOIR PLUS OK !

Figure 1 - C&C Dead Drop Resolvers used by TheDukes.

In September 2020, the Microsoft Threat Intelligence Center (MSTIC) reported that a Chinese state-sponsored threat actor known as GADOLINIUM used GitHub Commits to issue new commands to victim computers. These acted as dead drop resolvers to conceal any communications to attacker infrastructure by

Ce site utilise des cookies provenant de Google pour fournir ses services et analyser le trafic. Votre adresse IP et votre user-agent, ainsi que des statistiques relatives aux performances et à la sécurité, sont transmis à Google afin d'assurer un service de qualité, de générer des statistiques d'utilisation, et de détecter et de résoudre les problèmes d'abus.

EN SAVOIR PLUS **OK !**

Figure 2 - GitHub repository controlled by GADOLINIUM used as a Dead Drop Resolver

It is also worth noting that in February 2021, Akamai researchers wrote a blog on a cryptomining botnet leveraging Bitcoin blockchain transactions in order to conceal its back up C&C server addresses. This specific dead drop resolver is interesting as it effectively can defeat takedown attempts. The blog does describe a singular method of causing disruption, however, as a disruptor can send funds to the wallets the group uses to generate invalid C&C server addresses.

Ce site utilise des cookies provenant de Google pour fournir ses services et analyser le trafic. Votre adresse IP et votre user-agent, ainsi que des statistiques relatives aux performances et à la sécurité, sont transmis à Google afin d'assurer un service de qualité, de générer des statistiques d'utilisation, et de détecter et de résoudre les problèmes d'abus.

EN SAVOIR PLUS OK !

Figure 3 - Bitcoin transactions used to generate C&C server addresses

In August 2020, Kaspersky GReAT disclosed information on a mercenary APT group dubbed DeathStalker (previously called the Decentikens and associated with the EvilNum group). The group heavily relied on dead

Ce site utilise des cookies provenant de Google pour fournir ses services et analyser le trafic. Votre adresse IP et votre user-agent, ainsi que des statistiques relatives aux performances et à la sécurité, sont transmis à Google afin d'assurer un service de qualité, de générer des statistiques d'utilisation, et de détecter et de résoudre les problèmes d'abus.

EN SAVOIR PLUS **OK !**

Figure 4 - Strings containing C&C addresses left as YouTube comments

Analysis

Defenders attempting traffic analysis would only see connections to these legitimate sites and it would not flag any suspicious alerts. This tradecraft has often been favoured by state-sponsored adversaries for intelligence gathering and long term persistence. Although this TTP of dead drop resolvers has been leveraged by the cyber arm of the Russian SVR since at least 2013 - and the idea by spies decades earlier - it is still an effective tool to bypass basic traffic analysis. It is always worth remembering that many APT groups are either directly associated with intelligence and security agencies or do contract work for them. As shown with cryptomining campaigns and the DeathStalker group, these TTPs can often transfer to the cybercriminal underground.

Dead drops resolvers are free for threat actors to create and provide simple yet effective cover. It can also hinder defenders from disrupting the attacker's campaign as takedown requests can be a difficult and time-consuming process. The online services like YouTube and Twitter also cannot be blocked at the company level. However, this tactic comes at a price. Once an analyst has uncovered the attacker's dead drops, it can lead to unraveling other parts of the campaign as it can also be difficult for the attackers to remove their infrastructure and evidence of their attacks.

References:

<https://www.wired.com/story/what-is-dead-drop/>
<https://www.microsoft.com/security/blog/2020/09/24/gadolinium-detecting-empires-cloud/>
https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Operation_Ghost_Dukes.pdf
<https://github.com/eset/malware-ioc/blob/master/dukes/README.adoc>
<https://attack.mitre.org/techniques/T1102/001/>
<https://blogs.akamai.com/sitr/2021/02/bitcoins-blockchains-and-botnets.html>
<https://securelist.com/deathstalker-mercenary-triumvirate/98177/>
<https://sec0wn.blogspot.com/2018/12/powersing-from-lnk-files-to-janicab.html>



APT

C&C

CTI

Cybercrime

dead drop

espionage

GitHub

Intelligence

Social Media

threat intel

Twitter

YouTube

Ce site utilise des cookies provenant de Google pour fournir ses services et analyser le trafic. Votre adresse IP et votre user-agent, ainsi que des statistiques relatives aux performances et à la sécurité, sont transmis à Google afin d'assurer un service de qualité, de générer des statistiques d'utilisation, et de détecter et de résoudre les problèmes d'abus.

EN SAVOIR PLUS OK !

Popular posts from this blog

Raspberry Robin: A global USB malware campaign providing access to ransomware operators

- May 02, 2023



Logo credit: RedCanary Ever since it first appeared in late 2021, the Raspberry Robin malware campaign has been propagating globally. A number of threat intelligence reports by vendors such as RedCanary (who named it) and Microsoft (who track it as ...

[READ MORE](#)

Lessons from the iSOON Leaks

- February 22, 2024



Introduction A Chinese Ministry of Public Security (MPS) contractor called iSOON (also known as Anxun Information) that specializes in network penetration research and related services has had its data leaked to GitHub. Based on the level of detail, ...

[READ MORE](#)

The Ransomware Tool Matrix

- August 15, 2024



Introduction Ransomware attacks are becoming increasingly damaging, but one thing remains consistent: the tools these cybercriminals rely on. The Ransomware Tool Matrix is a comprehensive resource that sheds light on the tactics, techniques, and ...

[READ MORE](#)

Ce site utilise des cookies provenant de Google pour fournir ses services et analyser le trafic. Votre adresse IP et votre user-agent, ainsi que des statistiques relatives aux performances et à la sécurité, sont transmis à Google afin d'assurer un service de qualité, de générer des statistiques d'utilisation, et de détecter et de résoudre les problèmes d'abus.

[EN SAVOIR PLUS](#) [OK !](#)