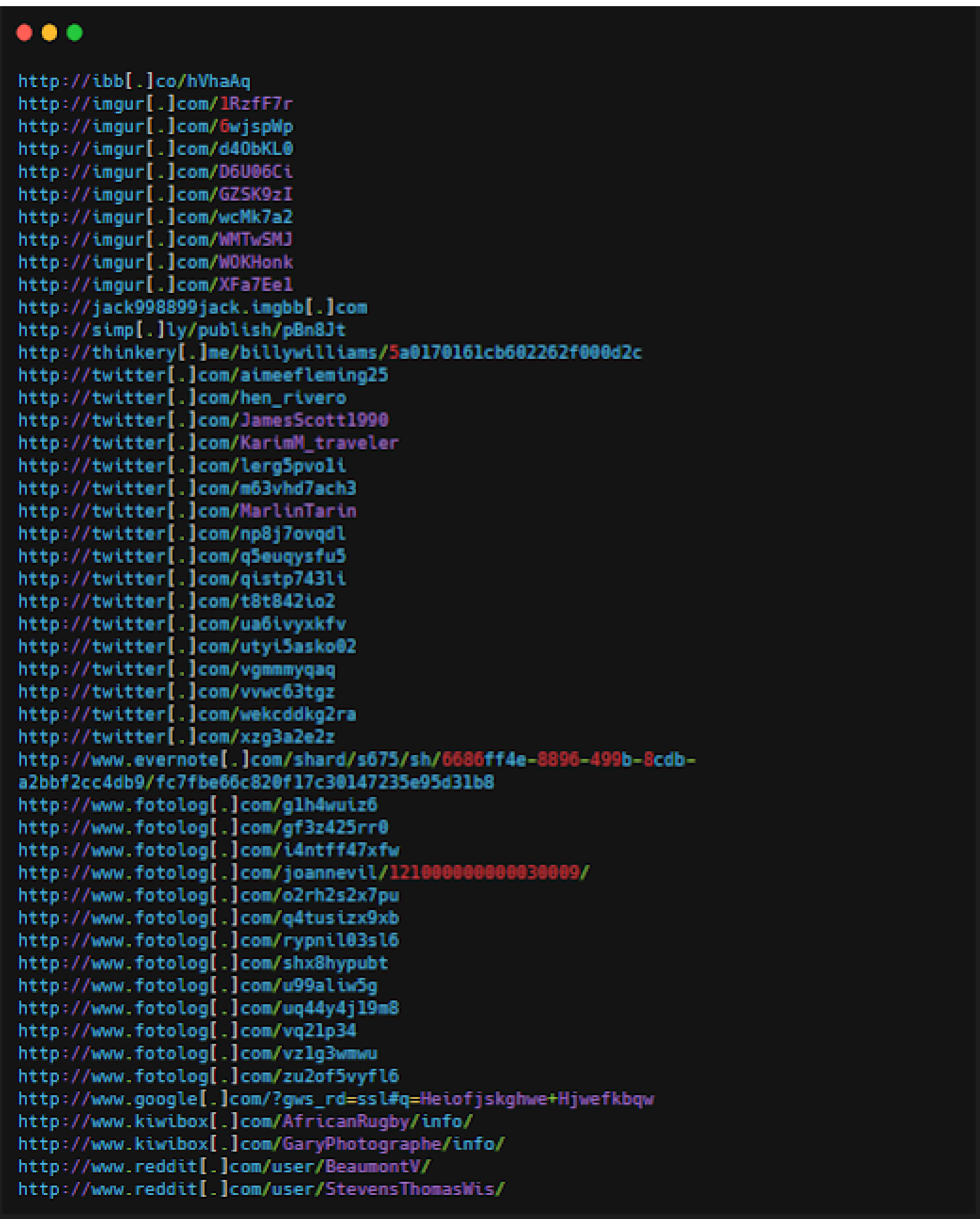
@BushidoToken Threat Intel

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”.

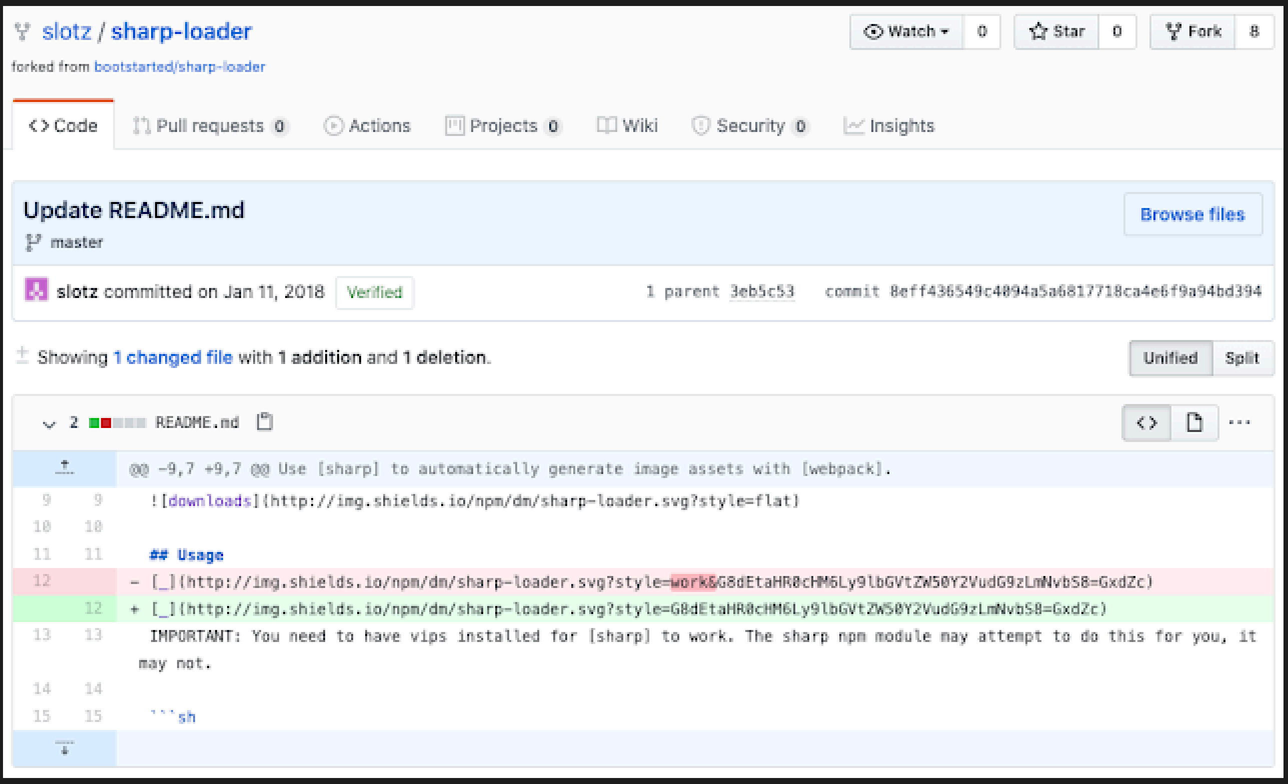
In October 2019, ESET Research disclosed a report on *Operation Ghost Dukes* which detailed the activities of an APT group known as TheDukes (also called APT29 or CozyBear). This particular group reportedly operates on behalf of the Russian foreign intelligence service (also known as the SVR). It was 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.



```
http://ibb[.]co/hVhaAq
http://imgur[.]com/1RzfF7r
http://imgur[.]com/6wjspWp
http://imgur[.]com/d40bKL0
http://imgur[.]com/D6U06Ci
http://imgur[.]com/GZSK9zI
http://imgur[.]com/wcMk7a2
http://imgur[.]com/WMTwSMJ
http://imgur[.]com/WOKHonk
http://imgur[.]com/XFa7Ee1
http://jack998899jack.imgbb[.]com
http://simp[.]ly/publish/pBn8Jt
http://thinkery[.]me/billywilliams/5a0170161cb602262f000d2c
http://twitter[.]com/aimeefleming25
http://twitter[.]com/hen_rivero
http://twitter[.]com/JamesScott1990
http://twitter[.]com/KarimM_traveler
http://twitter[.]com/lerg5pvoli
http://twitter[.]com/m63vhd7ach3
http://twitter[.]com/MarlinTarin
http://twitter[.]com/np8j7ovqdl
http://twitter[.]com/q5euqysfu5
http://twitter[.]com/qistp743li
http://twitter[.]com/t8t842io2
http://twitter[.]com/ua6ivyxkfv
http://twitter[.]com/utyi5asko02
http://twitter[.]com/vgmmmyqaq
http://twitter[.]com/vvwc63tgz
http://twitter[.]com/wekcddkg2ra
http://twitter[.]com/xzg3a2e2z
http://www.evernote[.]com/shard/s675/sh/6686ff4e-8896-499b-8cdb-
a2bbf2cc4db9/fc7fbe66c820f17c30147235e95d31b8
http://www.fotolog[.]com/g1h4wuiz6
http://www.fotolog[.]com/gf3z425rr0
http://www.fotolog[.]com/i4ntff47xfw
http://www.fotolog[.]com/joannevil/121000000000030009/
http://www.fotolog[.]com/o2rh2s2x7pu
http://www.fotolog[.]com/q4tusizx9xb
http://www.fotolog[.]com/rypnil03sl6
http://www.fotolog[.]com/shx8hypubt
http://www.fotolog[.]com/u99aliw5g
http://www.fotolog[.]com/uq44y4j19m8
http://www.fotolog[.]com/vq21p34
http://www.fotolog[.]com/vz1g3wmwu
http://www.fotolog[.]com/zu2of5vyfl6
http://www.google[.]com/?gws_rd=ssl#q=Heiofjskghwe+Hjwefkbqw
http://www.kiwibox[.]com/AfricanRugby/info/
http://www.kiwibox[.]com/GaryPhotographe/info/
http://www.reddit[.]com/user/BeaumontV/
http://www.reddit[.]com/user/StevensThomasWis/
```

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 using GitHub pages as the intermediary. This tactic had been employed by the GADOLINIUM group since 2018 to target organisations worldwide, with a focus on the maritime and health industries.



Update README.md

master

slotz committed on Jan 11, 2018 Verified 1 parent 3eb5c53 commit 8eff436549c4094a5a6817718ca4e6f9a94bd394

Showing 1 changed file with 1 addition and 1 deletion.

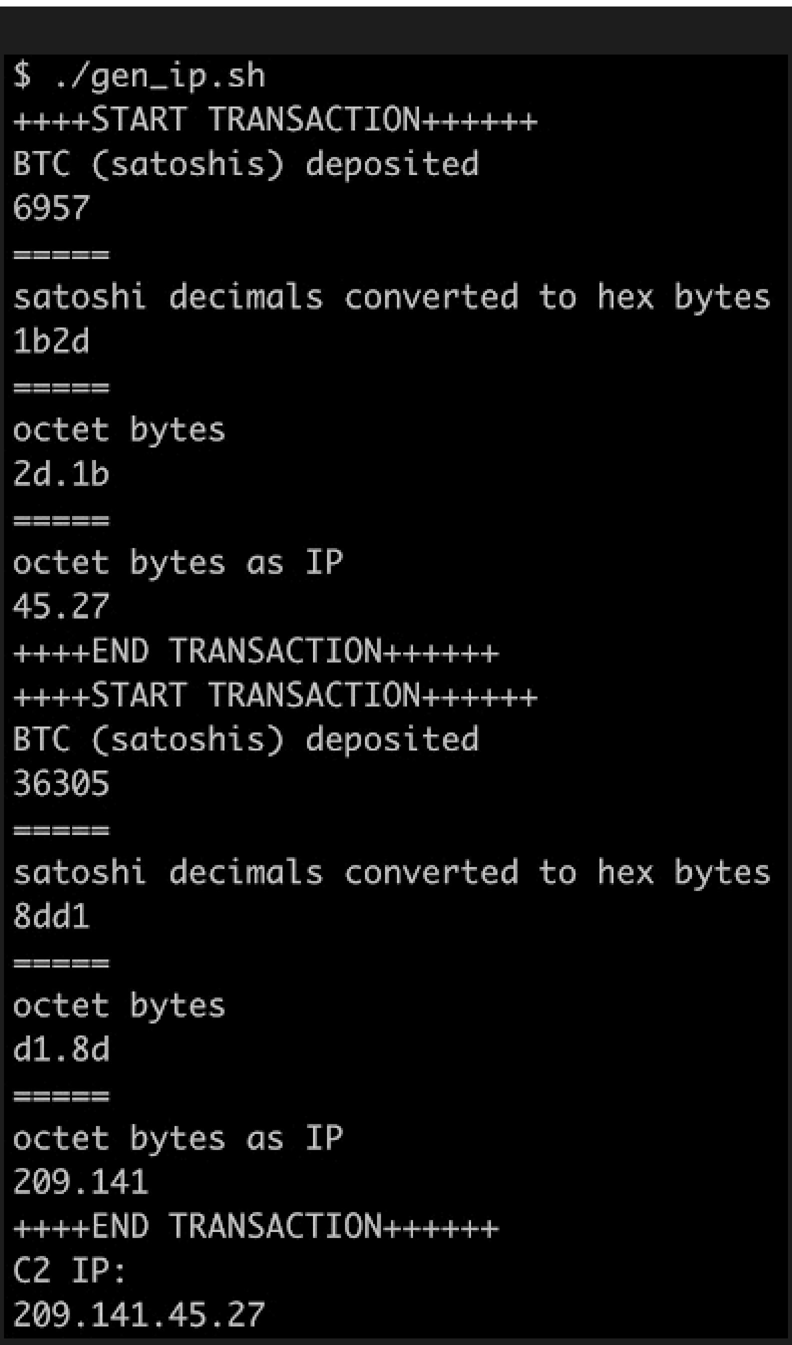
~~~
2 README.md
@@ -9,7 +9,7 @@ Use [sharp] to automatically generate image assets with [webpack].
  ![downloads](http://img.shields.io/npm/dm/sharp-loader.svg?style=flat)

  ## Usage
- [_](http://img.shields.io/npm/dm/sharp-loader.svg?style=work&G8dEtaHR0cHM6Ly9lbGVtZW50Y2VudG9zLmNvbS8=GxdZc)
+ [_](http://img.shields.io/npm/dm/sharp-loader.svg?style=G8dEtaHR0cHM6Ly9lbGVtZW50Y2VudG9zLmNvbS8=GxdZc)
  IMPORTANT: You need to have vips installed for [sharp] to work. The sharp npm module may attempt to do this for you, it
 may not.

  ```sh
~~~

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

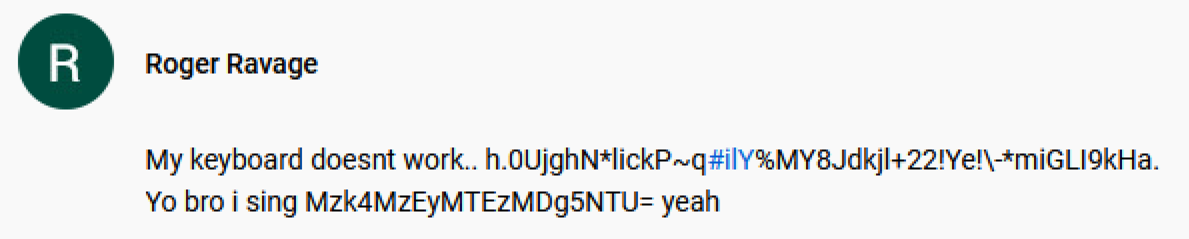
It is also worth noting that in February 2021, Akamai researchers wrote a blog on a crypomining botnet leveraging Bitcoin blockchain transactions in order to conceal its back up C&C server addresses. This specific dead drop resolver is interesting as it effectively can defeat takedown attempts. The blog 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.



```
$ ./gen_ip.sh
++++START TRANSACTION++++++
BTC (satoshis) deposited
6957
=====
satoshi decimals converted to hex bytes
1b2d
=====
octet bytes
2d.1b
=====
octet bytes as IP
45.27
++++END TRANSACTION++++++
++++START TRANSACTION++++++
BTC (satoshis) deposited
36305
=====
satoshi decimals converted to hex bytes
8dd1
=====
octet bytes
d1.8d
=====
octet bytes as IP
209.141
++++END TRANSACTION++++++
C2 IP:
209.141.45.27
```

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 Deceptikons and associated with the EvilNum group). The group heavily relied on dead drop resolvers to provide a way to store data at a fixed URL through public posts, comments, user profiles, content descriptions, etc. Messages left by the attackers follow the following patterns: “My keyboard doesn’t work… [string].” and “Yo bro I sing [Base64 encoded string] yeah”.



R

Roger Ravage

My keyboard doesnt work.. h.0UjghN*lickP~q#ilY%MY8Jdkjl+22!Ye!\-*miGLI9kHa.
Yo bro i sing Mzk4MzEyMTEzMDg5NTU= yeah

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.

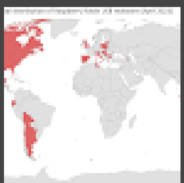
https://blogs.akamai.com/sitr/2021/02/bitcoins-blockchains-and-botnets.html
https://securelist.com/deathstalker-mercenary-triumvirate/98177/
https://sec0wn.blogspot.com/2018/12/powersing-from-lnk-files-to-janicab.html

APT C&C CTI Cybercrime dead drop espionage GitHub Intelligence Social Media threat intel Twitter YouTube

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 DEV-0856/Storm-0856) have covered the malware campaign in great detail. In fact, th …

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, leaked chat logs, amount of data, and corroboration from overlaps indicato …

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 procedures (TTPs) commonly used by ransomware and extortionist gangs. This reposit …

READ MORE

Powered by Blogger

Theme images by enot-poloskun