Sunday, 3 March 2019

Threat Hunting #26 - Remote Windows Service Creation / Recon

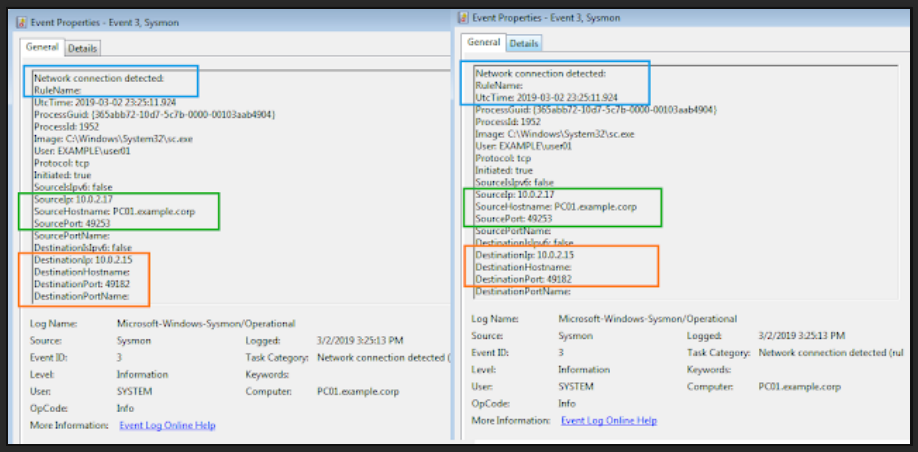
Interacting remotely with windows services is one way to execute programs remotely as well as persisting across system reboots. It can be done via different utilities (sc.exe, WMI etc.) but in this post we will be focusing more on artifacts and methods to detect this based on static behavioral indicators and independently from the used utilities.

A) Create remotely a service using legit windows built-in utilities:

Example of a command to create remotely a new service "remotesvc" on host 1.2.3.4 that persist system reboot and executes cmd.exe:

```
sc \\1.2.3.4 create remotesvc binpath= cmd.exe type= own start= auto
```

From the source machine, we can see clearly sc.exe is connecting to a remote host and source|destination ports are both dynamic RCP port numbers [TCP 49152-65535]:



Monitoring sc.exe process execution command line and network connections is good but not resilient enough and can be bypassed easily as a detection (a.k.a rename sc.exe to something else and run it from another folder).

On the target machine, the most interesting observed events are:

Windows Built-in:

- [System Events] Event-ID 7045: A service was installed on the system (expected, since we've created a service)
- [Security Events] Event-ID 5156: The Windows Filtering Platform has allowed a connection

If you enable System> Security System Extension in your Advanced Audit Policy GPO you will be able to see eventid 4697 in your security events and which is equivalent to 7045.

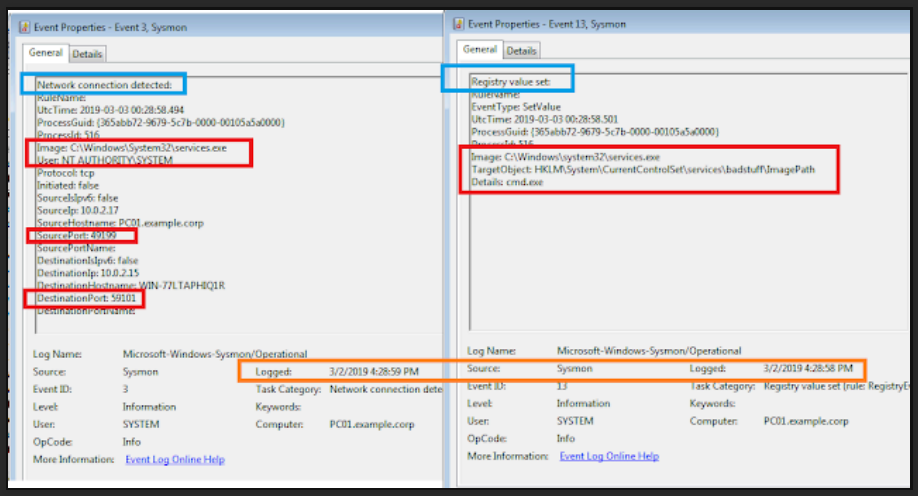
Sysmon:

- [Sysmon RegValueSet] ID 13: Registry Value Set (HKLM\System\CurrentControlSet\services\<svcname>*, which is expected since we've created a service)

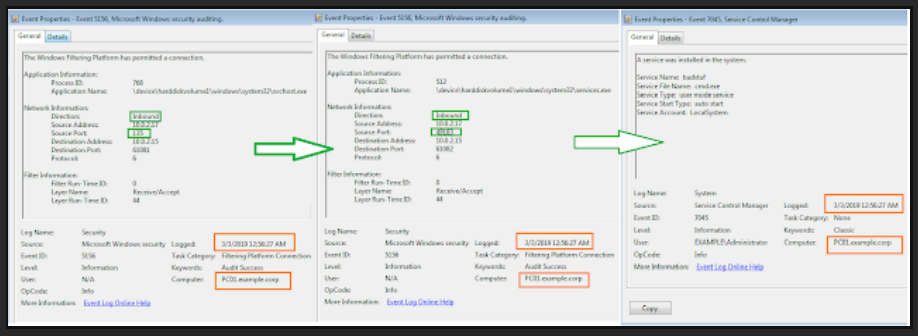
- [Sysmon Network Connect] ID 3: Network Connection Detected

Both events 5156 and 3 (sysmon) contain same information and indicates incoming and/or outgoing network connections from services.exe process to the source machine of our command. Which is a good indication of remote interaction with the service control manager on the target machine.

Sysmon's observed key events:



Windows's builtin observed key events:



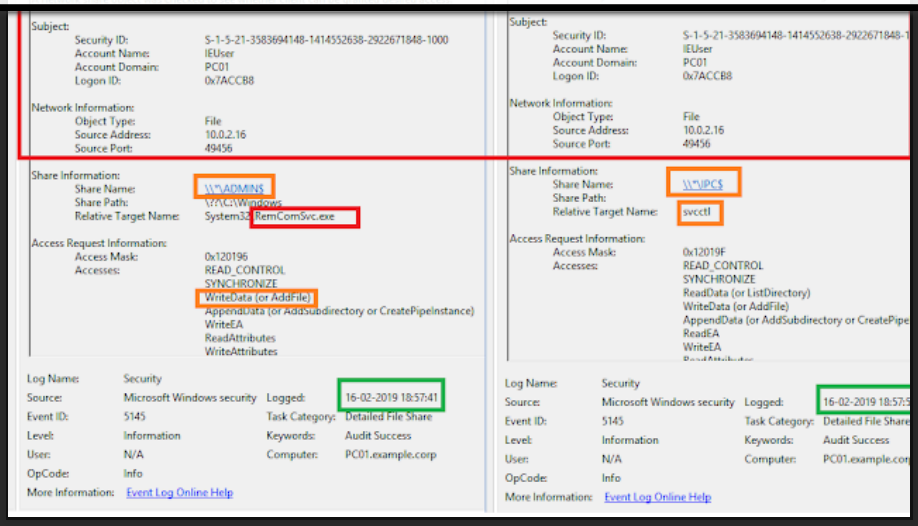
B) Creating a remote service using external utilities (i.e. psexec, paexec, psexec_psh, remcom etc.):

The aforementioned third party utilities are extremely useful for an attacker to move laterally and expand the compromise. High level modus operandi is quite simple and similar across this category of utilities:

1. Extract a service PE from it's resource section or download it from elsewhere
2. Copy the extracted PE to the destination host
3. Register a service on the destination machine (with binpath pointing to the PE extracted in step 2) and send a start control to begin execution
4. Start Interacting with the remote machine

To detect reliably the above steps we will be using our best friend event 5145:

- [Security] EventID 5145 - A network share object was checked to see whether client can be granted desired access - > will help us to detect step 2 and 3 from the destination host security events:



Detection & Takeaways:

Correlation Rule 1 (standard remote service creation - windows builtin):

[EventID=5156 and ApplicationName like "*\services.exe" and SourceAddress != DestinationAddress and SourcePort>=49152 and DestinationPort>=49152 and SourceAddress!=Null and DestinationAddress!=Null] followed by (EventID=7045 or EventID=4697) within 1 min and same ComputerName.

Correlation Rule 2 (standard remote service creation - sysmon) :

[EventID=13 and TargetObject like "HKLM\System\CurrentControlSet\services*"] followed by [EventID=3 and SourceIP != DestinationIP and SourcePort>=49152 and DestinationPort>=49152 and Image like "*\services.exe" and SourceIP!=Null and DestinationIP !=Null] within 1 minute and Same ComputerName.

Correlation Rule 3 (psexec family):

[EventID=5145 and ShareName=(*\ADMIN$ or *\C$) and event.payloads contains "WriteData"] followedby [EventID=5145 & ShareName='*\IPC$' and RelativeTargetName:'svcctl')] within 1min and with Same [AccountName, SourceAddres,Port] and Same ComputerName

Posted by MENASEC at 11:28

Labels: persistence, remote execution, w indow s services

21 comments:

james john 2 October 2019 at 12:42

The article was up to the point and described the information very effectively. Thanks to blog author for wonderful and informative post.
Security System Provider

Reply

for ict 99 6 October 2019 at 20:49

Great Article
Network Security Projects for CSE

JavaScript Training in Chennai

Project Centers in Chennai

shanewarner 21 April 2020 at 16:46

The post is written in very a good manner and it contains many useful information for me.

gexton advance security solution

Reply

FERHAT YILDIZ 24 June 2021 at 02:50

instagram takipçi satın al - instagram takipçi satın al - tiktok takipçi satın al - instagram takipçi satın al - instagram beğeni satın al - instagram takipçi satın al - instagram takipçi satın al - instagram takipçi satın al - binance güvenilir mi - binance güvenilir mi - binance güvenilir mi - binance güvenilir mi - instagram beğeni satın al - instagram beğeni satın al - polen filtresi - google haritalara yer ekleme - btcturk güvenilir mi - binance hesap açma - kuşadası kiralık villa - tiktok izlenme satın al - instagram takipçi satın al - sms onay - paribu sahibi - binance sahibi - btcturk sahibi - paribu ne zaman kuruldu - binance ne zaman kuruldu - btcturk ne zaman kuruldu - youtube izlenme satın al - torrent oyun - google haritalara yer ekleme - altyapısız internet - bedava internet - no deposit bonus forex - erkek spor ayakkabı - webturkey.net - minecraft premium hesap - karfiltre.com - tiktok jeton hilesi - tiktok beğeni satın al - microsoft word indir - misli indir

Reply

Unknown 23 July 2021 at 13:41

instagram takipçi satın al
aşk kitapları
tiktok takipçi satın al
instagram beğeni satın al
youtube abone satın al
twitter takipçi satın al
tiktok beğeni satın al
tiktok izlenme satın al
twitter takipçi satın al
tiktok takipçi satın al
youtube abone satın al
tiktok beğeni satın al
instagram beğeni satın al
trend topic satın al
trend topic satın al
youtube abone satın al
instagram takipçi satın al
beğeni satın al
tiktok izlenme satın al
sms onay
youtube izlenme satın al
tiktok beğeni satın al
sms onay
sms onay
perde modelleri
instagram takipçi satın al
takipçi satın al
tiktok jeton hilesi
instagram takipçi satın al pubg uc satın al
sultanbet
marsbahis
betboo
betboo
betboo

Reply

Unknown 13 August 2021 at 17:41

marsbahis
betboo
sultanbet
marsbahis
betboo
sultanbet

Reply

Nice & Informative Blog ! We offer welcome to yorkie puppies nearme. Check it out!...
puppies for sale near me
yorkie puppies with home training
where to buy Yorkie
Yorkie Female Puppies for sale
Yorkie puppies ready for their forever homes

Reply

sdsaaa 8 February 2022 at 02:05

The breed became very popular in the early 1900s, and in 1913 and 1914, https://oneshoppharmacy.com they were among the 10 most popular entries in the Westminster Kennel Club Show. During World War I, however, the breed fell on hard times in the U.S. and England because they were poodle for sale closely associated with Germany. Dachshund owners sometimes were called traitors and their dogs stoned. After
World War I, some U.S. breeders dachshunds for sale imported some Dachshunds from Germany and the breed started to become popular once again. The breed faced a similar fate during World War II, but not nearly so severely as during World War I.
In the 1950s, Dachshunds became one of the most popular family dogs in the U.S. again, a status they have enjoyed ever https://Greenlandpuppies.com
since. While Dachshunds mini dachshund puppy for sale rarely are used as hunting dogs in the U.S. or Great Britain, in other parts of Europe, especially France, they still are considered hunting dogs. mini dachshund puppies for sale Dachshunds also love a challenge, and as long as you incorporate plenty of opportunities to chase and find things, you'll miniature dachshund for sale have a happy dog. These dogs love their human parents, and really don't want them to leave.

Reply

sdsaaa 8 February 2022 at 02:06

Dachshunds are bred and shown in two sizes: Standard and Miniature. https://www.cutespupsforsale.com/ Standard Dachshunds of all varieties (Smooth, Wirehair, and Longhair) usually weigh between 16 and 32 pounds. Miniature Dachshunds of all varieties weigh 11 pounds and under at teacup poodle for sale maturity. Dachshunds that weigh between 11 and 16 pounds are called Tweenies. Some people who breed exceptionally small Dachshunds advertise them as Toy Dachshunds, but this is purely a poodles for sale marketing term, not a recognized designation. He's bred for perseverance, which is another way of saying that he can be stubborn. Dachshunds have a reputation for being dachshund puppies sale entertaining and fearless, but what they want most is to cuddle with their people. Longhairs are calm and quiet, and Smooths have dachshund for sale a personality that lies somewhere in between. https://Greenlandpuppies.com Some Mini Dachshunds can be nervous or shy, but this isn't correct for the breed. Avoid puppies that show these characteristics.Like every dog, Dachshunds need early socialization-exposure to many different people, dachshund puppies for sale near me sights, sounds, and experiences-when they're young. Socialization helps ensure that your Dachshund puppy grows up to be a well-rounded dog. .

Reply

sdsaaa 8 February 2022 at 02:07

The dachshund was bred in Germany hundreds of years ago to hunt badgers. https://www.poodlespring.com/ "Dach" means badger and "hund" means dog. The three varieties of dachshund, smooth-,As family dogs, dachshunds are loyal companions and good watchdogs.
https://Greenlandpuppies.com They are good with children if treated well. They can be slightly difficult to train. Dachshund puppies for sale wire-,and long-coated, originated at different times. The smooth was the first and arose from a mixture of a miniature French pointer and a pinscher. The breed also comes in two sizes: standard and miniature, with the standard the original size.
The dachshund has short, strong legs that enable the dog to dig out prey and go inside burrows. Larger versions of the breed were used to chase deer or fox..
Smaller dachshunds Dachshund puppy for sale were bred for hunting hares and ferrets.
The breed is still used for hunting, primarily in Europe, nine in dachshunds puppies for sale ches in height.All three types are known
The dachshund's coat may be shades of red, black, chocolate, white or gray. Some have tan markings or are spotted or dappled. Dachshunds live about 12 to 15 years. toy poodle for sale espite their size, dachshunds are known for their courageous nature and will take on animals much larger than themselves. Some may be aggressive toward strangers and other dogs
Some dachshund fanciers say there are personality differences among the different varieties of the breed. For instance, the long-coat dachshund is reportedly calmer teacup poodles for sale than the smooth-coat variety,

Reply

uniqueaiminc 24 March 2022 at 00:07

Kevin 29 March 2022 at 13:19

Very nice. This is exactly the same information. which I was looking for .Turkey visa for Americans is a visa which is made specifically for American Citizens. It is very helpful for all the American citizens.

Reply

Unknown 6 April 2022 at 21:28

seo fiyatları
saç ekimi
dedektör
instagram takipçi satın al
ankara evden eve nakliyat
fantezi iç giyim
sosyal medya yönetimi
mobil ödeme bozdurma
kripto para nasıl alınır

Reply

WB Sales and Service 12 April 2022 at 19:53

I am impressed with your work and skills for **WB Sales and Service**

Reply

Unknown 27 April 2022 at 20:17

bitcoin nasıl alınır
tiktok jeton hilesi
youtube abone satın al
gate io güvenilir mi
referans kimliği nedir
tiktok takipçi satın al
bitcoin nasıl alınır
mobil ödeme bozdurma
mobil ödeme bozdurma

Reply

2015 SECURITY SERVICES LTD 7 May 2022 at 21:53

Thanks for sharing this valuable information about **London Security Services**. I have gone through your post and got meaningful information.

Reply

dennishcaraid 14 May 2022 at 13:24

Hii guys, this is excellent information! You can travel to India. But first you need an Indian visa. You can never enter India without a visa. I am using India visa website services. This website helps a lot and provides fast visa services.

Reply

Unknown 31 May 2022 at 18:42

Smm Panel
Smm Panel
iş ilanları
instagram takipçi satın al
https://www.hirdavatciburada.com/
beyazesyateknikservisi.com.tr
SERVİS
Jeton hile

Reply

Unknown 3 June 2022 at 05:47

ataşehir vestel klima servisi
maltepe toshiba klima servisi
maltepe beko klima servisi
kadıköy beko klima servisi
kartal lg klima servisi
ümraniye lg klima servisi
kartal alarko carrier klima servisi
ümraniye alarko carrier klima servisi
pendik lg klima servisi

Reply

Unknown 6 July 2022 at 07:01

bostansepeti.com
site kurma
ürünler
vezirsosyalmedya.com
postegro
sosyal medya yönetimi
surucukursuburada.com

Reply

Unknown 7 July 2022 at 12:24

patent sorgula
yorumbudur.com
yorumlar
tiktok jeton hilesi
mobil ödeme bozdurma
mobil ödeme bozdurma
mobil ödeme bozdurma
pubg uc satın al
pubg uc satın al

Reply

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)