Sarwent has received little attention from researchers, but this backdoor malware is still being actively developed, with new commands and a focus on RDP.

functionality such as executing PowerShell commands.

- Updates also show a preference for using RDP
- Sarwent has been seen using the same binary signer as at least one TrickBot operator[1]

Background

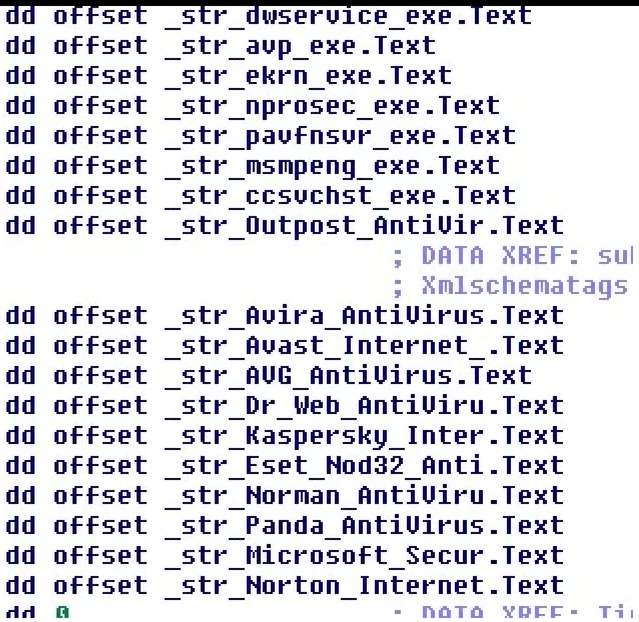
Sarwent appears to have been actively used since at least 2018 but not a lot has been publicly reported about it during that time period.

Research Insight

Sarwent functionality has historically revolved around being a loader, as shown by the limited number of original commands:

```
|download|
|update|
|vnc|
```

Some other functionality that has remained consistent is its AV(AntiVirus) checking.



```
dd offset _str_dwservice_exe.Text
dd offset _str_avp_exe.Text
dd offset _str_ekrn_exe.Text
dd offset _str_nprosec_exe.Text
dd offset _str_pavfnsvr_exe.Text
dd offset _str_msmpeng_exe.Text
dd offset _str_ccsvchst_exe.Text
dd offset _str_Outpost_AntiVir.Text
                        ; DATA XREF: sul
                        ; Xmlschematags
dd offset _str_Avira_AntiVirus.Text
dd offset _str_Avast_Internet_.Text
dd offset _str_AVG_AntiVirus.Text
dd offset _str_Dr_Web_AntiViru.Text
dd offset _str_Kaspersky_Inter.Text
dd offset _str_Eset_Nod32_Anti.Text
dd offset _str_Norman_AntiViru.Text
dd offset _str_Panda_AntiVirus.Text
dd offset _str_Microsoft_Secur.Text
dd offset _str_Norton_Internet.Text
dd 0                    ; DATA XREF: Ti
```

Figure 1: AV checks

Recent updates include a minor change to their C2 URI structure[2].

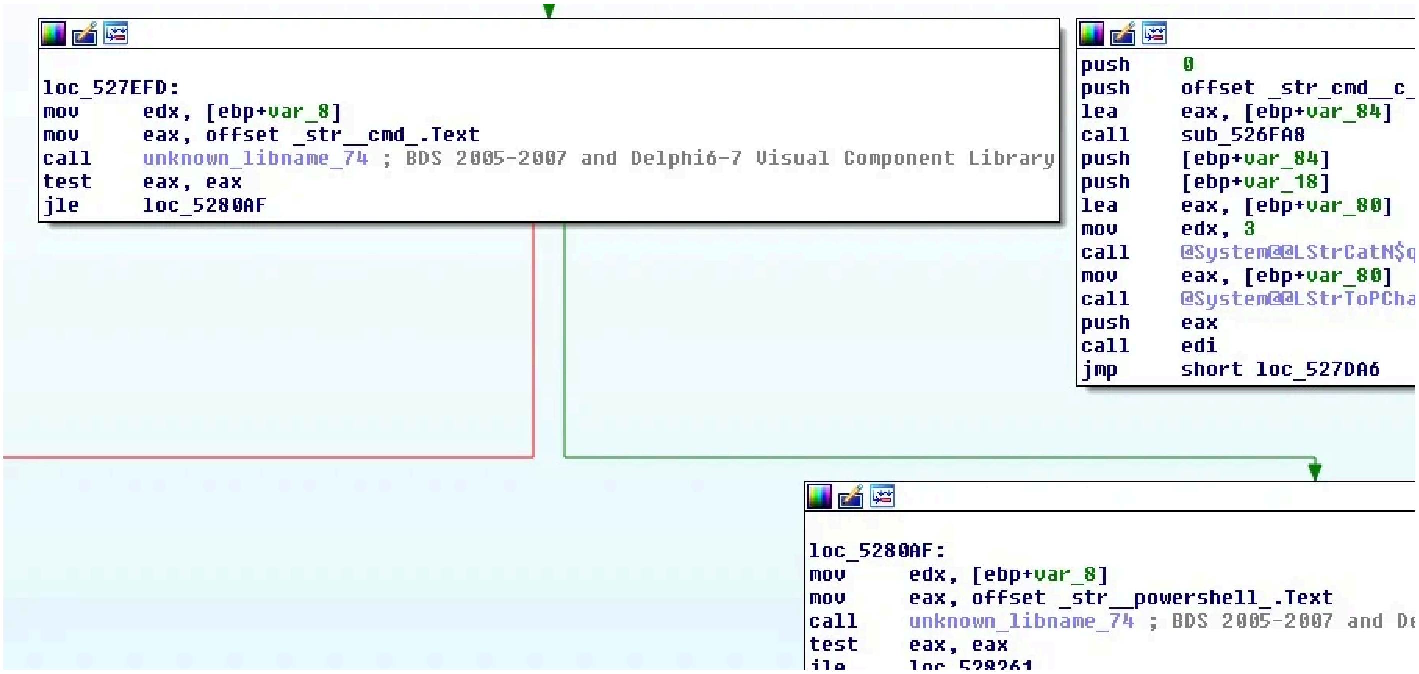
Figure 2: C2 checking update

Also, there has recently been the addition of a number of commands that would normally be seen in malware that focus more on backdoor or RAT like capabilities.

```
|cmd|
|powershell|
|rdp|
```

focus as can be seen in the recent proliferation of services selling access to systems[3].

The ‘cmd’ and ‘powershell’ commands are simply commands to be detonated.



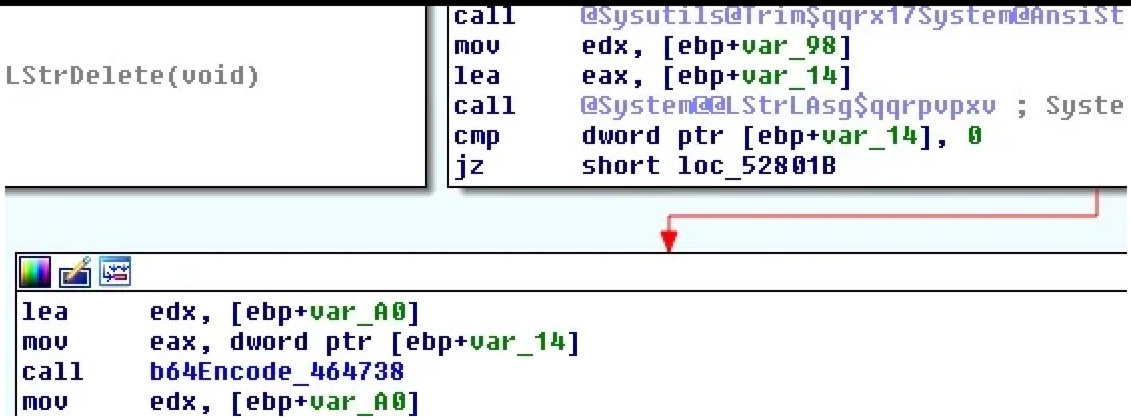
```
loc_527EFD:
mov     edx, [ebp+var_8]
mov     eax, offset _str__cmd_.Text
call    unknown_libname_74 ; BDS 2005-2007 and Delphi6-7 Visual Component Library
test    eax, eax
jle     loc_5280AF
```

```
push    0
push    offset _str_cmd__c_
lea     eax, [ebp+var_84]
call    sub_526FA8
push    [ebp+var_84]
push    [ebp+var_18]
lea     eax, [ebp+var_80]
mov     edx, 3
call    @System@@LStrCatN$q
mov     eax, [ebp+var_80]
call    @System@@LStrToPCha
push    eax
call    edi
jmp     short loc_527DA6
```

```
loc_5280AF:
mov     edx, [ebp+var_8]
mov     eax, offset _str__powershell_.Text
call    unknown_libname_74 ; BDS 2005-2007 and De
test    eax, eax
jle     loc_528261
```

Figure 3: Command line detonations

The results are base64 encoded and sent back to the C2 through the matching URL route.



```
LStrDelete(void)
```

```
call    @Sysutils@Trim$qqrx17System@AnsiSt
mov     edx, [ebp+var_98]
lea     eax, [ebp+var_14]
call    @System@@LStrLAsg$qqrpvpxv ; Syste
cmp     dword ptr [ebp+var_14], 0
jz      short loc_52801B
```

```
lea     edx, [ebp+var_A0]
mov     eax, dword ptr [ebp+var_14]
call    b64Encode_464738
mov     edx, [ebp+var_A0]
```

Figure 4: Base64 encode command results

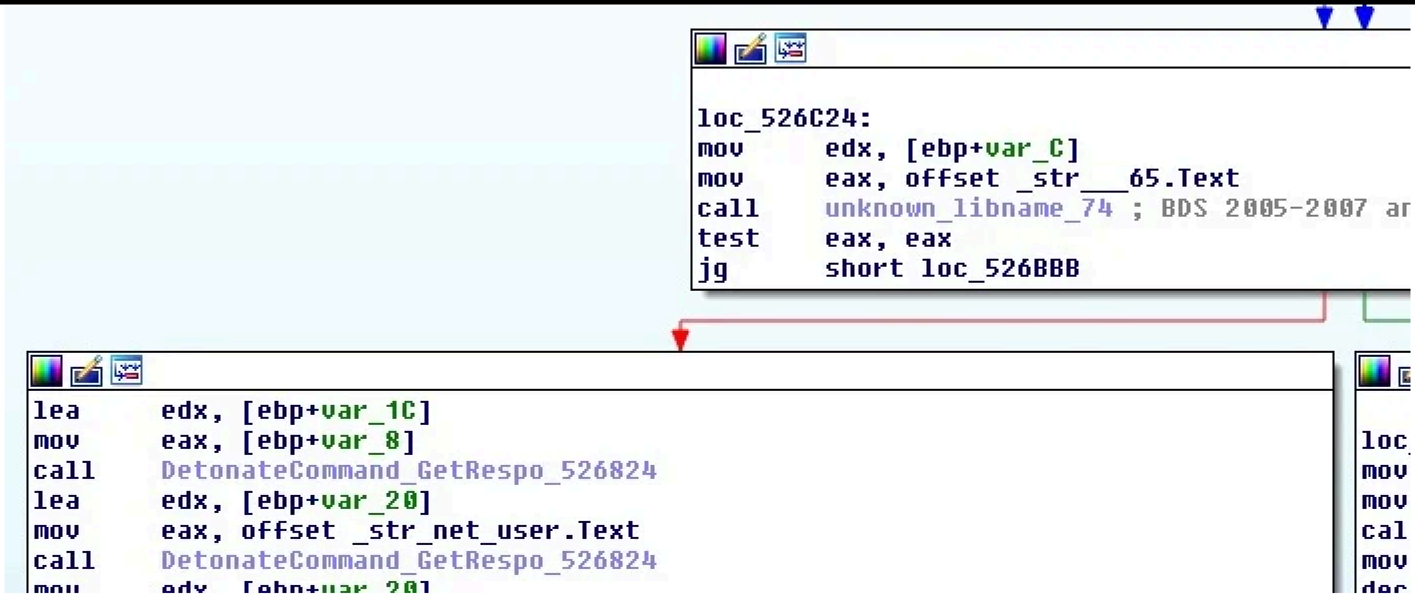
C2 routes for sending responses:

```
/gate/cmd_exec
/gate/powershell_exec
```

The ‘rdp’ command is a bit different; the code execution looks like it serves to tell the bot to perform a series of tasks:

- Add a new user
- List groups and users
- Punch hole in local firewall

Figure 5: Add new user



```
loc_526C24:
mov     edx, [ebp+var_C]
mov     eax, offset _str___65.Text
call    unknown_libname_74 ; BDS 2005-2007 ar
test    eax, eax
jg      short loc_526BBB
```

```
lea     edx, [ebp+var_1C]
mov     eax, [ebp+var_8]
call    DetonateCommand_GetRespo_526824
lea     edx, [ebp+var_20]
mov     eax, offset _str_net_user.Text
call    DetonateCommand_GetRespo_526824
mov     edx, [ebp+var_20]
```

```
loc
mov
mov
cal
mov
dec
```

Figure 6: List network groups and users

Figure 7: Allow firewall connections on RDP port

This command, then, is more related to setting up the system for RDP access at a later time.

Mitigation & Recommendations

Endpoint:

```
CommadLine="cmd /c ping localhost & regsvr32 /s *"
```

Suricata rules:

```
alert http $HOME_NET any → $EXTERNAL_NET any (msg:”Sarwent CMD response Post”; content:”POSt”; http_method; content:”/gate/cmd_exec”; http_uri; classtype:trojan-activity; sid:9000040; rev:1; metadata:author Jason Reaves;)

alert http $HOME_NET any → $EXTERNAL_NET any (msg:”Sarwent Powershell response Post”; content:”POST”; http_method; content:”/gate/powershell_exec”; http_uri; classtype:trojan-activity; sid:9000041; rev:1; metadata:author Jason Reaves;)

alert http $HOME_NET any → $EXTERNAL_NET any (msg:”Sarwent RDP exec response”; content:”GET”; http_method; content:”/gate/rdp_exec?command=”; http_uri; content:”&status=”; http_uri; classtype:trojan-activity; sid:9000042; rev:1; metadata:author Jason Reaves;)

alert http $HOME_NET any → $EXTERNAL_NET any (msg:”Sarwent update exe response”; content:”GET”; http_method; content:”/gate/update_exec?command=”; http_uri; content:”&status=”; http_uri; classtype:trojan-activity; sid:9000043; rev:1; metadata:author Jason Reaves;)

alert http $EXTERNAL_NET any → $HOME_NET any (msg:”Sarwent update command”; content:”200″; http_stat_code; content:”fHVwZGF0ZX”; startswith; http_server_body; flow:to_client, established; classtype:trojan-activity; sid:9000044; rev:1; metadata:author Jason Reaves;)
```

```
http_server_body; flow:to_client, established; classtype:trojan-activity; sid:9000045; rev:1; metadata:author Jason Reaves;)

alert http $EXTERNAL_NET any → $HOME_NET any (msg:”Sarwent powershell command”; content:”200″; http_stat_code; content:”fHBvd2Vyc2hlbGx8″; startswith; http_server_body; flow:to_client, established; classtype:trojan-activity; sid:9000046; rev:1; metadata:author Jason Reaves;)

alert http $EXTERNAL_NET any → $HOME_NET any (msg:”Sarwent rdp command”; content:”200″; http_stat_code; content:”fHJkcH”; startswith; http_server_body; flow:to_client, established; classtype:trojan-activity; sid:9000047; rev:1; metadata:author Jason Reaves;)
```

Indicators of Compromise

Download Location:

whatsmyhomeworthlondonontario[.]ca/wp-admin/version.exe

beurbn[.]com/install.exe

V2 samples

Hash:

3f7fb64ec24a5e9a8cfb6160fad37d33fed6547c

Domains

seoanalyticsproj.xyz

seoanalyticsproewj.xyz

seoanalyticsprojrts.xyz

seoanalyticspro32frghyj.xyz

Hash:

ab57769dd4e4d4720eedaca31198fd7a68b7ff80

Domains

vertuozoff.xyz

vertuozoff.club

vertuozofff.xyz

vertuozofff.com

vertuozofff.club

vertuozoffff.club

Hash:

d297761f97b2ead98a96b374d5d9dac504a9a134

Domains

rabbot.xyz

terobolt.xyz

tebbolt.xyz

rubbolt.xyz

rubbot.xyz

treawot.xyz

Hash:

3eeddeadcc34b89fbdd77384b2b97daff4ccf8cc terobolt.xyz

tebbolt.xyz

rubbolt.xyz

rubbot.xyz

treawot.xyz

Hash:

106f8c7ddbf265fc108a7501b6af292000dd5219

Domains

blognews-journal.com

startprojekt.pw

blognews-joural.com

blognews-joural.best

blognews-joural.info

startprojekt.pro

V1 Samples

Hash:

83b33392e045425e9330a7f009801b53e3ab472a

Domains

212.73.150.246

softfaremiks.icu

Hash:

2979160112ea2de4f4e1b9224085efbbedafb593

Domains

shopstoregame.icu

softfaremiks.icu

shopstoregamese.icu shopstoregamese.com shopstoregames.icu

References

1: https://twitter.com/VK_Intel/status/1228833249536987138

2: https://twitter.com/James_inthe_box/status/1228788661006659584

3: https://twitter.com/VK_Intel/status/1242587625409609731

4: https://github.com/silence-is-best/c2db

MALWARE SARWENT TRICKBOT

SHARE

PDF

in malware reverse-engineering. He has spent the majority of his career tracking threats in the Crimeware domain, including reverse-engineering data structures and algorithms found in malware in order to create automated frameworks for harvesting configuration and botnet data. Previously, he worked as a software developer and unix administrator in the financial industry and also spent six years in the U.S. Army. Jason holds multiple certifications related to reverse-engineering and application exploitation and has published numerous papers on topics such as writing malware scripts pretending to be a bot, unpackers, configuration data harvesters and covert channel utilities. He enjoys long walks in IDA and staring at RFCs for hours.

PREV

‹ **Deep Dive Into TrickBot Executor Module "mexec": Reversing the Dropper Variant**

NEXT

NetWalker Ransomware: No Respite, No English Required ›

RELATED POSTS

Exploring the VirusTotal Dataset | An Analyst's Guide to Effective Threat Research

📅 AUGUST 29 2024

Decoding the Past, Securing the Future | Enhancing Cyber Defense with Historical Threat Intelligence

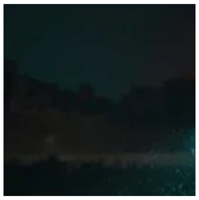
📅 NOVEMBER 28 2023

Search ...

SIGN UP

RECENT POSTS

Cloud Malware | A Threat Hunter’s Guide to Analysis, Techniques and Delivery
OCTOBER 24, 2024



China’s Influence Ops | Twisting Tales of Volt Typhoon at Home and Abroad
OCTOBER 16, 2024

Kryptina RaaS | From Unsellable Cast-Off to Enterprise Ransomware
SEPTEMBER 23, 2024

LABS CATEGORIES

Crimeware
Security Research
Advanced Persistent Threat
Adversary

SENTINELLABS

In the era of interconnectivity, when markets, geographies, and jurisdictions merge in the melting pot of the digital domain, the perils of the threat ecosystem become unparalleled. Crimeware families achieve an unparalleled level of technical sophistication, APT groups are competing in fully-fledged cyber warfare, while once decentralized and scattered threat actors are forming adamant alliances of operating as elite corporate espionage teams.

RECENT POSTS

Cloud Malware | A Threat Hunter’s Guide to Analysis, Techniques and Delivery

📅 OCTOBER 24, 2024

China’s Influence Ops | Twisting Tales of Volt Typhoon at Home and Abroad

📅 OCTOBER 16, 2024

SIGN UP

Get notified when we post new content.

Twitter LinkedIn