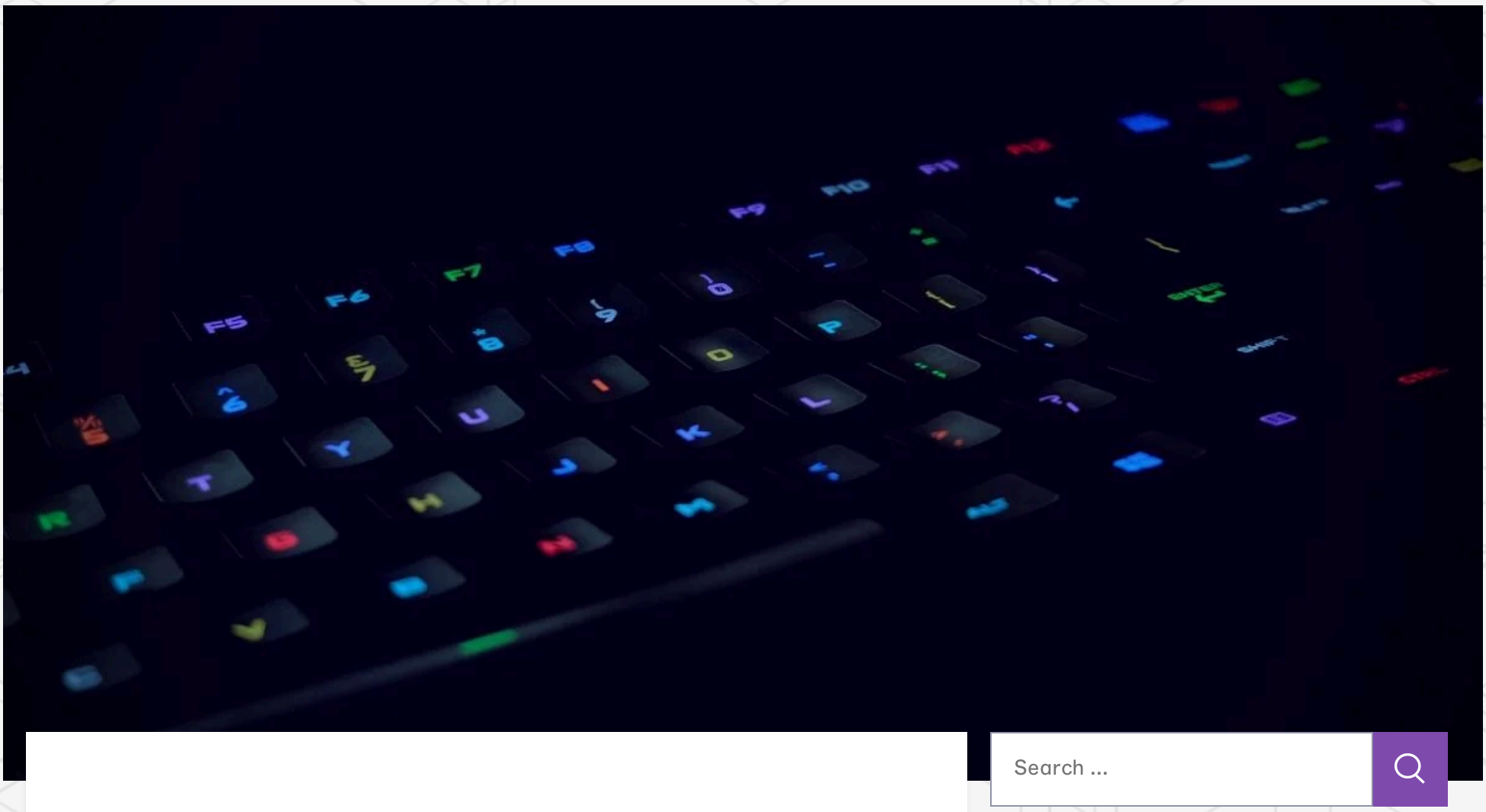


Sarwent has received little attention from researchers, but this backdoor malware is still being actively developed, with new commands and a focus on RDP.

Executive Summary

- Updates to Sarwent malware show a continued interest in backdoor 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]

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_acs_exe.Text ; DATA XREF
                            ; Xmlschematags
dd offset _str_sched_exe.Text
dd offset _str_avastsvc_exe.Text
dd offset _str_avgsvc_exe.Text
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: su
                            ; 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].

```
mov     fs:[eax], esp
push    offset _str_http____0.Text
push    ds:dword_532484
push    offset _str__gate_connect?.Text
push    offset _str_hwid_.Text
push    ds:dword_534598
push    offset _str__os_.Text
lea     eax, [ebp+var_38]
call    GetWindowsVersionString_523620
mov     eax, [ebp+var_38] ; this
lea     edx, [ebp+var_34] ; System::AnsiString
call    @Httpapp@HTTPEncode$qqrx17System@AnsiString ; Httpapp::HTTPEncode(System::An
push    [ebp+var_34]

_str__gate_connect? dd 0FFFFFFFFh           ; _top
                    dd 14                   ; Len
                    db '/gate/connect?',0   ; Text
```

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

for monetization and RDP continues to be a 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.

Figure 3: Command line detonations

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

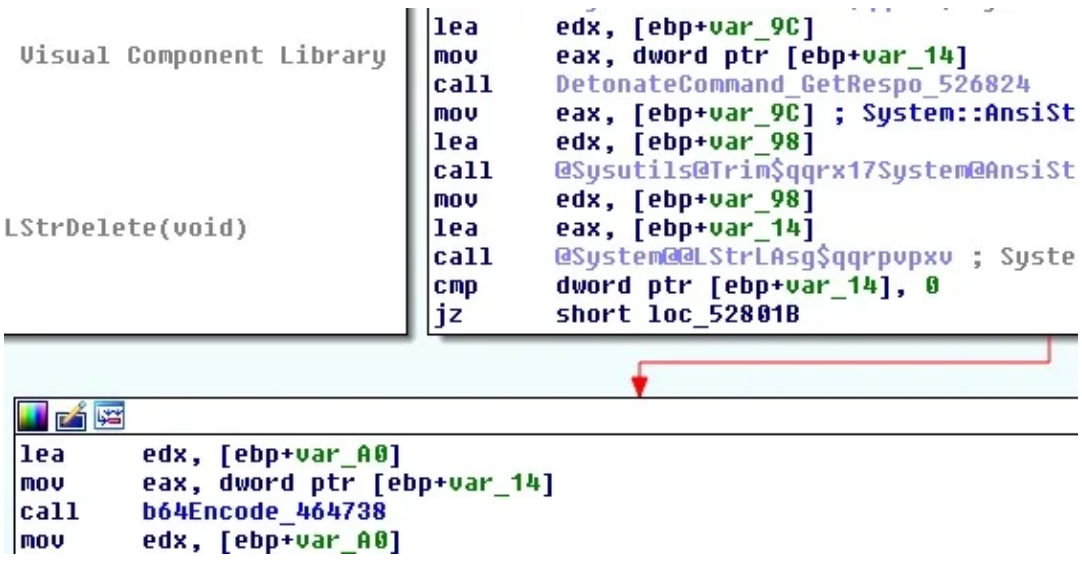


Figure 4: Base64 encode command results

C2 routes for sending responses:

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

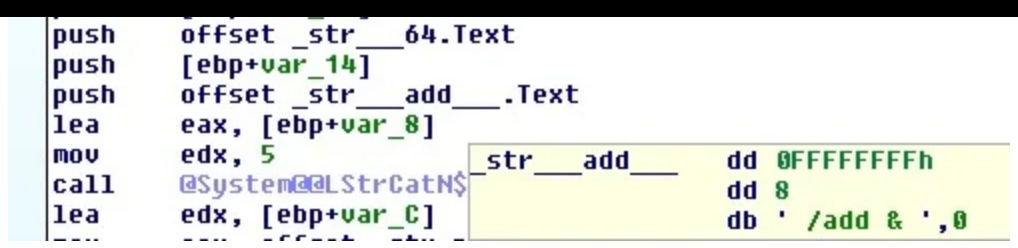


Figure 5: Add new user

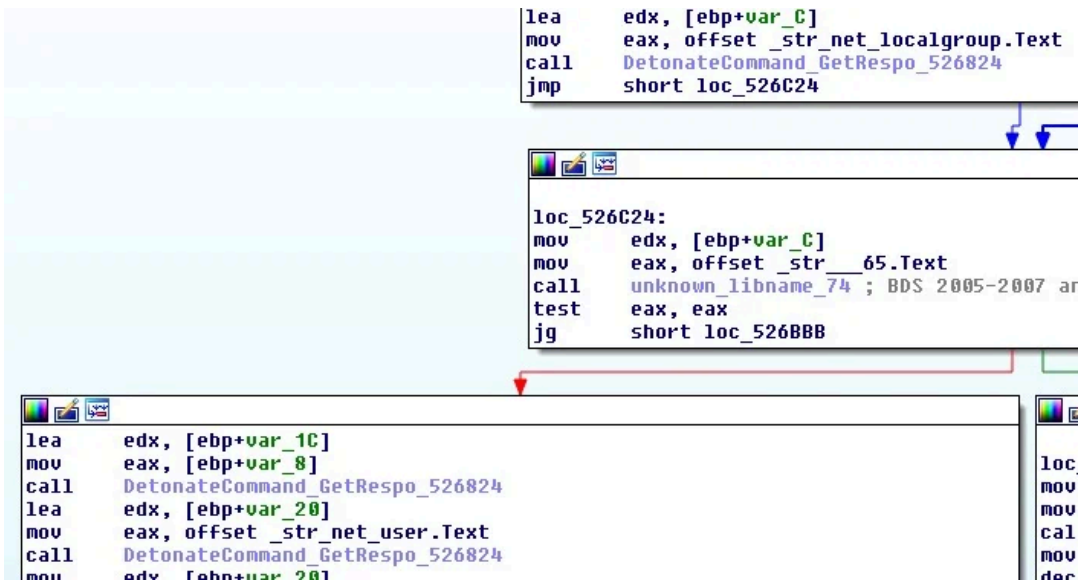


Figure 6: List network groups and users

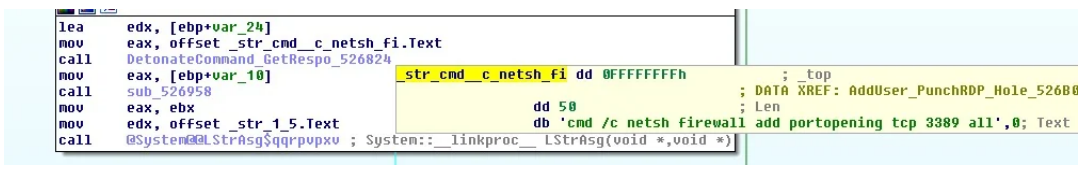


Figure 7: Allow firewall connections on RDP port

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 *"`

Network: A number of network rules already exist in Emerging Threats[4], so I decided to look at adding some Suricata rules that might not be currently covered.

Suricata rules:

```
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;)

alert http $EXTERNAL_NET any → $HOME_NET any
(msg:"Sarwent download command"; content:"200";
http_stat_code; content:"fGRvd25sb2Fkf"; startswith;
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;
```

beurbn[.]com/install.exe

V2 samples

Hash:

3f7fb64ec24a5e9a8cfb6160fad37d33fed6547c

Domains

seoanalyticsproj.xyz

seoanalyticsproewj.xyz

seoanalyticsp34roj.xyz

seoanalyticsptyrroj.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

Domains

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

shopstoregame.icu

shopstoregamese.icu

Hash:

2979160112ea2de4f4e1b9224085efbbedafb593

Domains

shopstoregame.icu

softfaremiks.icu

shopstoregamese.icu shopstoregamese.com

shopstoregames.icu

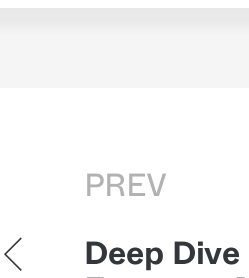
References

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



JASON REAVES

Jason Reaves is a Principal Threat Researcher at SentinelLabs who specializes 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

Cloud Malware | A Threat Hunter's Guide to Analysis

Exploring the VirusTotal Dataset | An Analyst's Guide

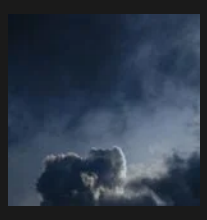
Decoding the Past, Securing the Future | Enhancing Cyber

SentinelLABS

SENTINELLABS

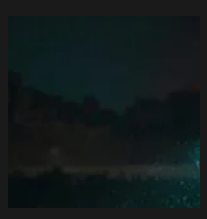
In the era of interconnectivity, when markets, geographies, and jurisdictions merge in the melting pot of the digital domain, the perils of the threat ecosystem become unparalleled. Crimeware families achieve an unparalleled level of technical sophistication, APT groups are competing in fully-fledged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

RECENT POSTS



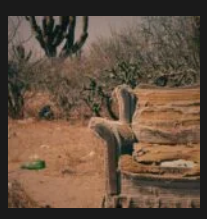
Cloud Malware | A Threat Hunter's Guide to Analysis, Techniques and Delivery

OCTOBER 24, 2024



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

OCTOBER 16, 2024



Kryptina RaaS | From Unsellable Cast-Off to Enterprise Ransomware

SEPTEMBER 23, 2024

SIGN UP

Get notified when we post new content.

Business Email >

By clicking Subscribe, I agree to the use of my personal data in accordance with SentinelOne Privacy Notice. SentinelOne will not sell, trade, lease, or rent your personal data to third parties. This site is protected by reCAPTCHA and the Google Privacy Policy and Terms of Service apply.

Twitter LinkedIn