From the Front Lines | Slam! Anatomy of a Publicly-Available Ransomware Builder

sentinelone.com/blog/from-the-front-lines-slam-anatomy-of-a-publicly-available-ransomware-builder/

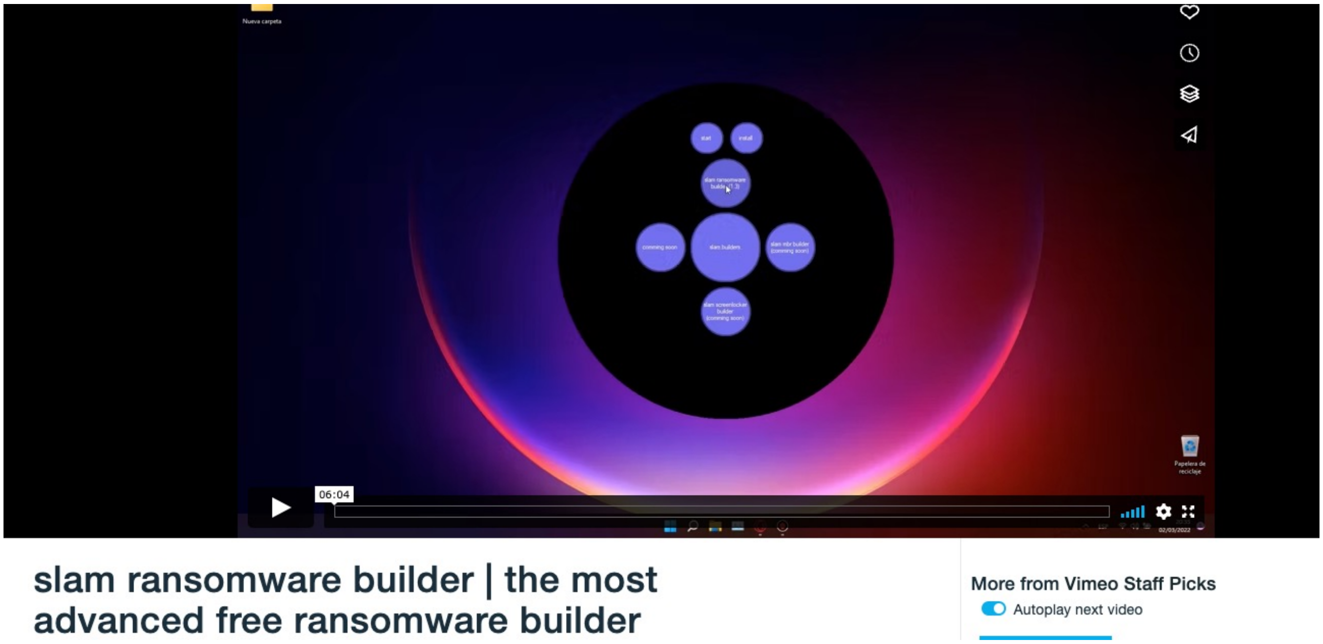
September 15, 2022

The barrier to entry for enterprising cybercriminals has been dropping considerably over recent years, in part due to the availability of RaaS (Ransomware as a Service) offerings on the darknet but also due to publicly-accessible code being shared for free. One such offering is the Slam Ransomware Builder, which had been hosted until recently on Github. In this post, we highlight how free ransomware builders like Slam offer an easy route into cybercrime and yet present a credible threat to organizations and enterprises. We provide a detailed list of indicators to help security teams detect and protect against Slam ransomware payloads.

Ransomware For “Educational Purposes Only”?

The Slam Ransomware Builder first appeared in late 2021, with Slam ransomware payloads appearing in the wild shortly after (e.g., ConsoleApp2.exe). During mid-2022, downloadable and executable versions of the Slam Ransomware Builder appeared on a publicly-visible repository on Github and were available for several months until Github admins removed the repository on September 1st, 2022.

The owner of the now-removed repository dubbed it “The Most Advanced Free Ransomware Builder” and has a history of providing “educational” videos on Vimeo, Youtube and KZHome, instructing viewers how to build ransomware and “virus payloads”.


Nueva carpeta
start
install
slam ransomware builder (1.3)
comming soon
slam builders
slam mbr builder (comming soon)
slam screenlocker builder (comming soon)
Papelera de reciclaje
06:04
02/03/2022

slam ransomware builder | the most advanced free ransomware builder

More from Vimeo Staff Picks

Autoplay next video

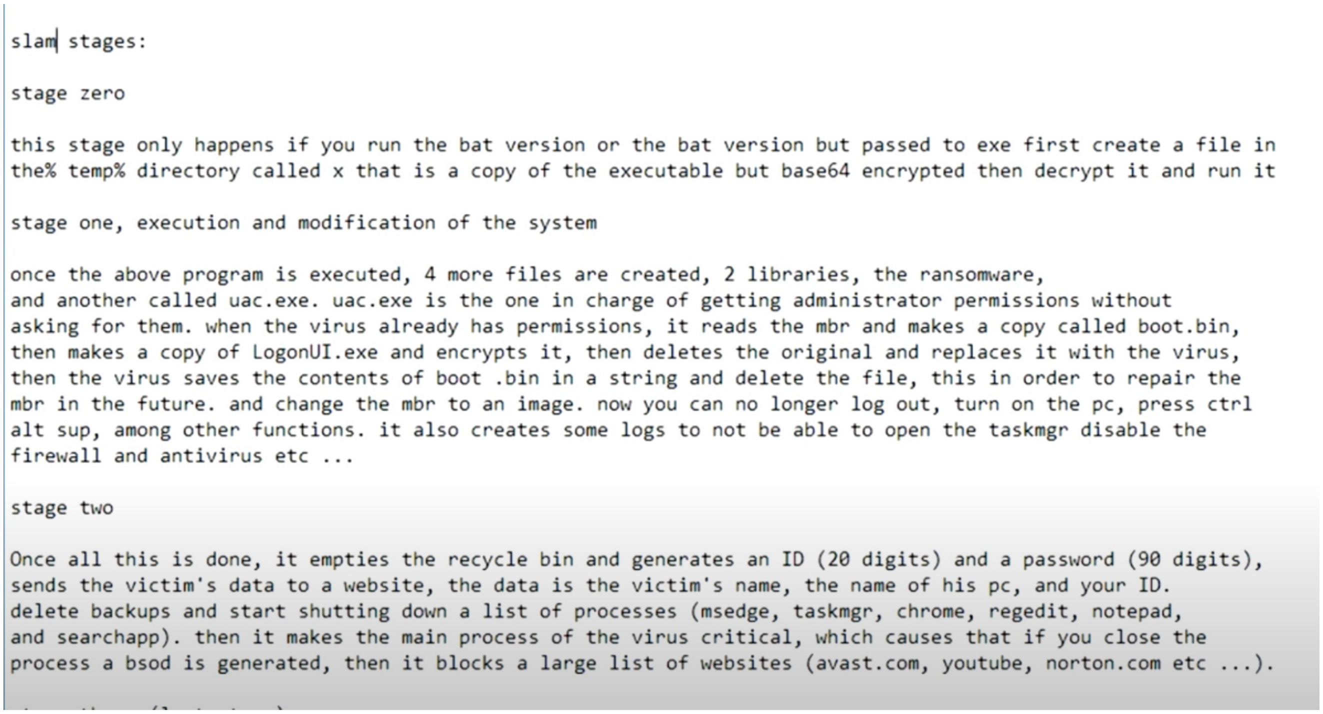
Source: Slam ransomware builder video hosted on Vimeo

While the author’s public postings contain the usual “for educational purposes only” and “don’t try this” disclaimers to avoid responsibility, they also contain language such as “most advanced ransomware” and “damage rate: destructive”.

SLAM.EXE
(RANSOMWARE)
DAMAGE RATE: DESTRUCTIVE

Source: Slam ransomware builder video hosted on Youtube

The author had described the ransomware’s behavior in detail in earlier publicly-posted videos, describing how victim data could be exfiltrated to an attacker-controlled site.



```
slam stages:

stage zero

this stage only happens if you run the bat version or the bat version but passed to exe first create a file in
the% temp% directory called x that is a copy of the executable but base64 encrypted then decrypt it and run it

stage one, execution and modification of the system

once the above program is executed, 4 more files are created, 2 libraries, the ransomware,
and another called uac.exe. uac.exe is the one in charge of getting administrator permissions without
asking for them. when the virus already has permissions, it reads the mbr and makes a copy called boot.bin,
then makes a copy of LogonUI.exe and encrypts it, then deletes the original and replaces it with the virus,
then the virus saves the contents of boot .bin in a string and delete the file, this in order to repair the
mbr in the future. and change the mbr to an image. now you can no longer log out, turn on the pc, press ctrl
alt sup, among other functions. it also creates some logs to not be able to open the taskmgr disable the
firewall and antivirus etc ...

stage two

Once all this is done, it empties the recycle bin and generates an ID (20 digits) and a password (90 digits),
sends the victim's data to a website, the data is the victim's name, the name of his pc, and your ID.
delete backups and start shutting down a list of processes (msedge, taskmgr, chrome, regedit, notepad,
and searchapp). then it makes the main process of the virus critical, which causes that if you close the
process a bsod is generated, then it blocks a large list of websites (avast.com, youtube, norton.com etc ...).
```

The author’s reasons for distributing free ransomware builders can only be guessed at, but despite being free, the builder and payloads are genuine threats that can cause real damage. As our analysis below shows, Slam is a full-featured ransomware with AES256 encryption, UAC bypass, shadow backup copy deletion and data exfiltration capabilities. In other words, everything needed to lock and steal enterprise data.

Slam Ransomware Builder Features

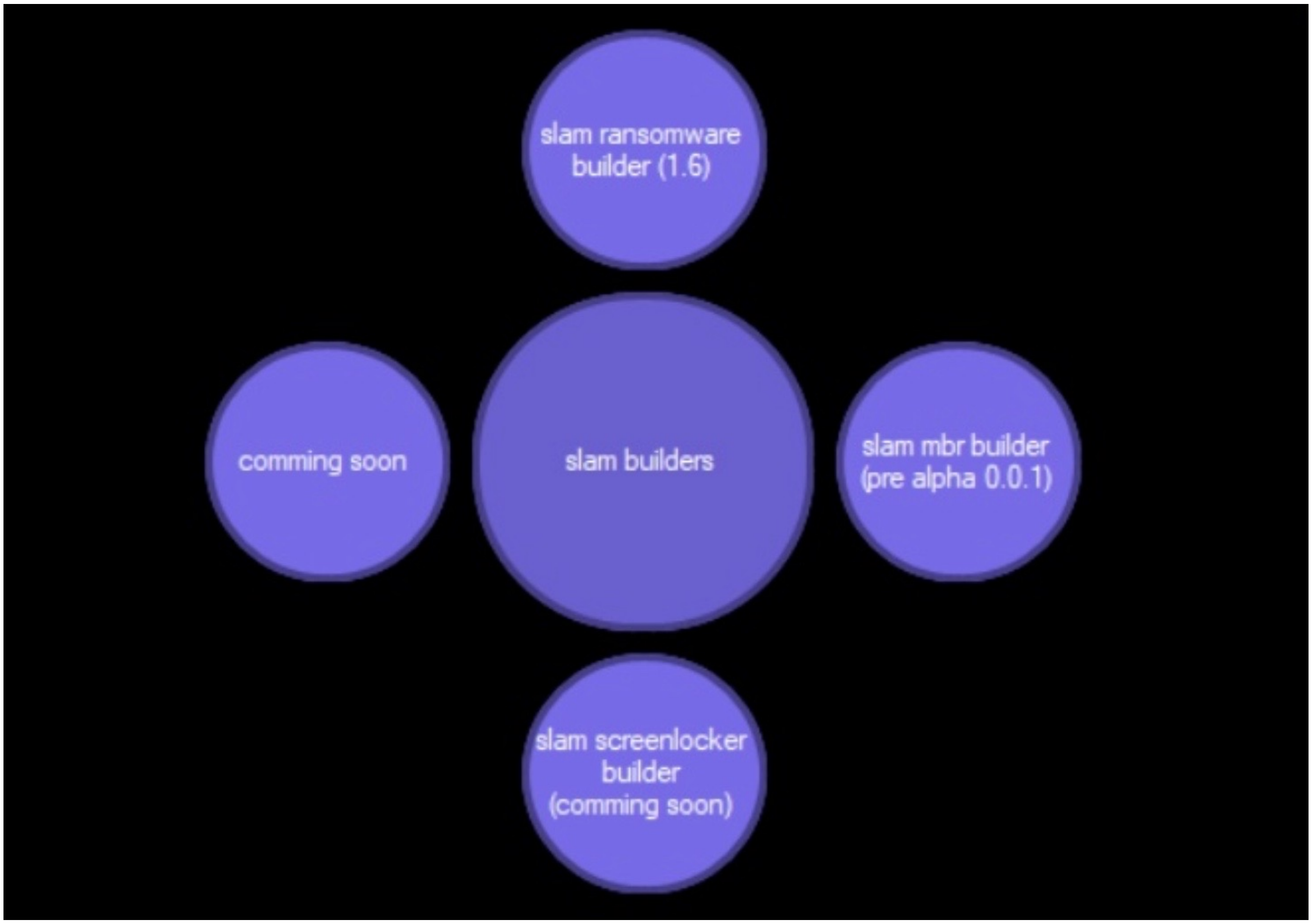
The most recent release of the Slam ransomware builder prior to being removed from Github was version 1.7. Earlier versions of the tool supported either English or Spanish locales, while later versions including 1.7 allow toggling between the two.

The existing feature set includes the following:

- Fully customizable ransom notes
- Custom encryption passphrases
- All ransomware to lay dormant until a network is available
- UAC Bypass (1)
- Run external commands with the ransomware launch
- VSS/ backup deletion
- Basic file transfers (HTTP) for exfiltration

Despite the code being removed from Github, it is possible the author intends to find or already has other distribution outlets. A list of features promised for the future include screen locking, MBR overwrites, and “LogonUI overwriting”.

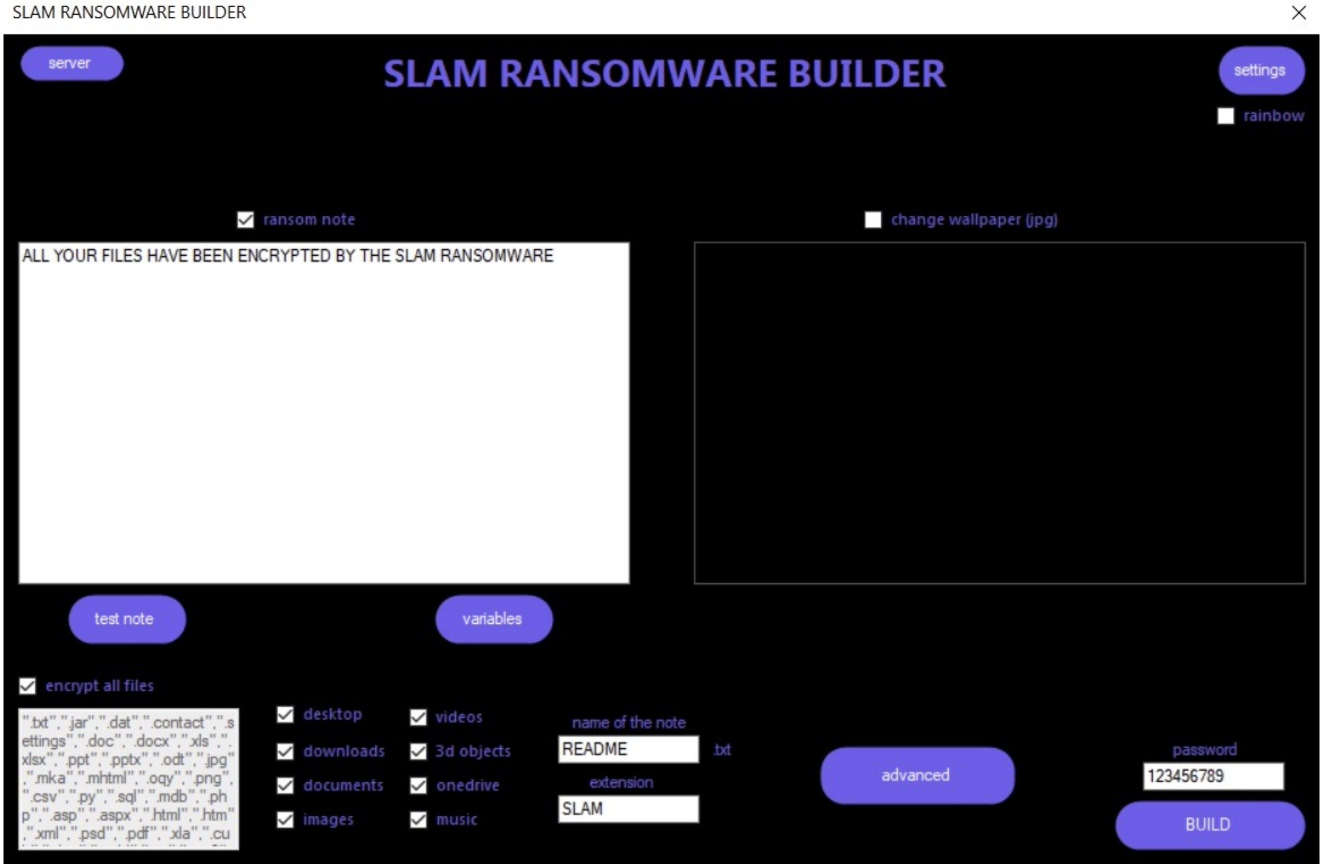
Upon running the code provided on Github, users of the builder are presented with a menu leading to different builder components or indications of their upcoming release.


slam ransomware builder (1.6)
comming soon
slam builders
slam mbr builder (pre alpha 0.0.1)
slam screenlocker builder (comming soon)

Version 1.6 of the Slam Ransomware Builder

When choosing the “slam ransomware builder” option, users must first “Install”, then “Start” to launch the builder interface. This installation essentially consists of writing the builder EXE to `c:\slam_ransomware_builder\` . Any other component requiring an “Install” step will also go to the root of the C drive (e.g., `c:\slam_mbr_builder)`

Once the main interface is launched, the user is presented with a standard set of options for building their ransomware payloads.



□ rainbow

☑ ransom note

ALL YOUR FILES HAVE BEEN ENCRYPTED BY THE SLAM RANSOMWARE

□ change wallpaper (jpg)

☑ encrypt all files

".txt",".jar",".dat",".contact",".settings",".doc",".docx",".xls",".xlsx",".ppt",".pptx",".odt",".jpg",".mka",".mhtml",".oqy",".png",".csv",".py",".sql",".mdb",".php",".asp",".aspx",".html",".htm",".xml",".psd",".pdf",".xla",".cu

☑ desktop ☑ videos
☑ downloads ☑ 3d objects
☑ documents ☑ onedrive
☑ images ☑ music

name of the note: README .txt

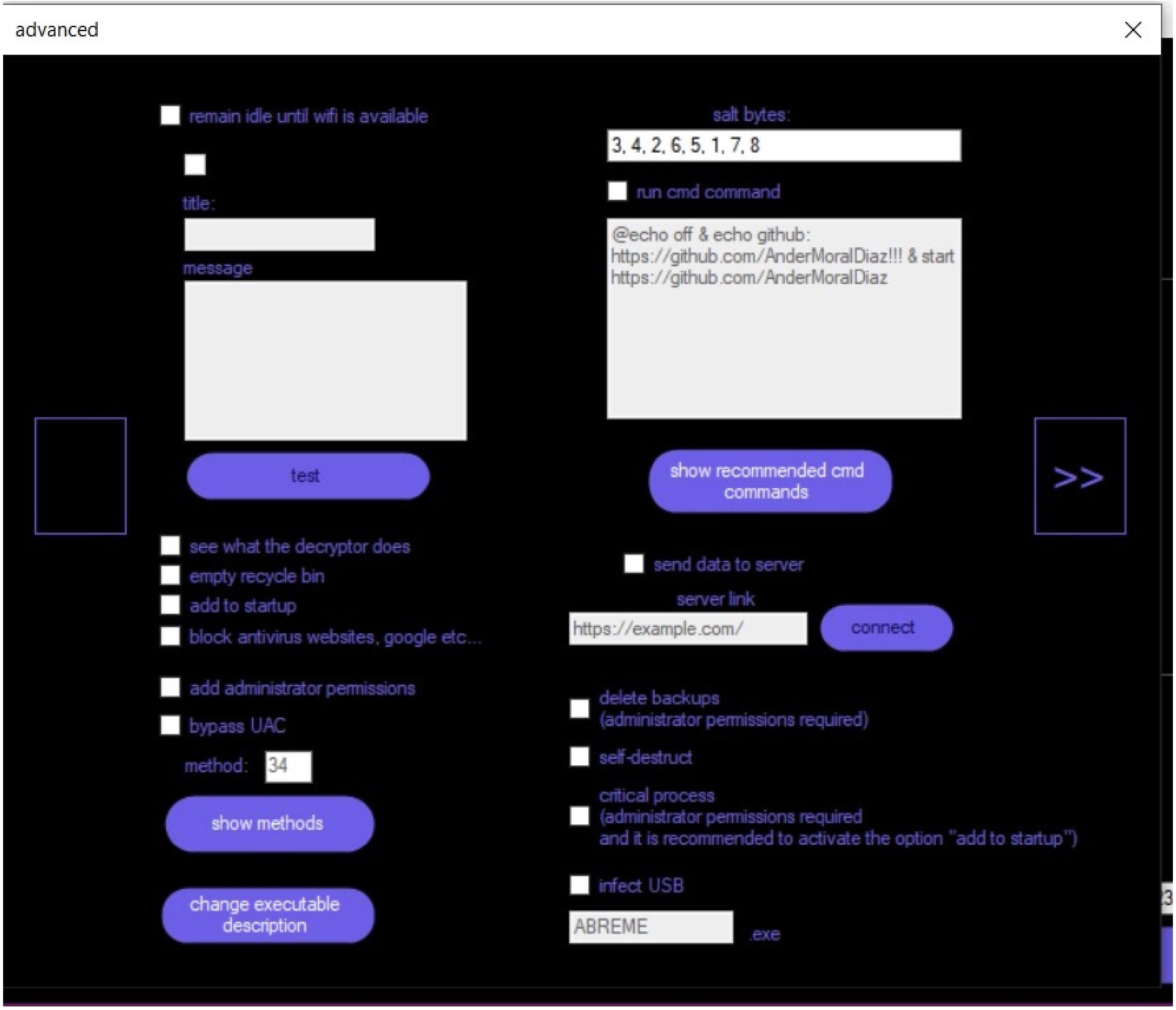
extension: SLAM

password: 123456789

Options including the following are present in this interface:

- Ransom note name and text
- Wallpaper modification options and images
- Affected file extensions
- File encryption (types / extensions to encrypt)
- Remote folder options (OneDrive)

The tool provides more ‘Advanced’ configuration options as well. These options are accessible via the “advanced” button.



advanced

□ remain idle until wifi is available

□

title:

message

□ see what the decryptor does

□ empty recycle bin

□ add to startup

□ block antivirus websites, google etc...

□ add administrator permissions

□ bypass UAC

method: 34

salt bytes:

3, 4, 2, 6, 5, 1, 7, 8

□ run cmd command

```
@echo off & echo github:
https://github.com/AnderMoralDiaz!!! & start
https://github.com/AnderMoralDiaz
```

□ send data to server

server link

https://example.com/

□ delete backups
(administrator permissions required)

□ self-destruct

□ critical process
(administrator permissions required
and it is recommended to activate the option "add to startup")

□ infect USB

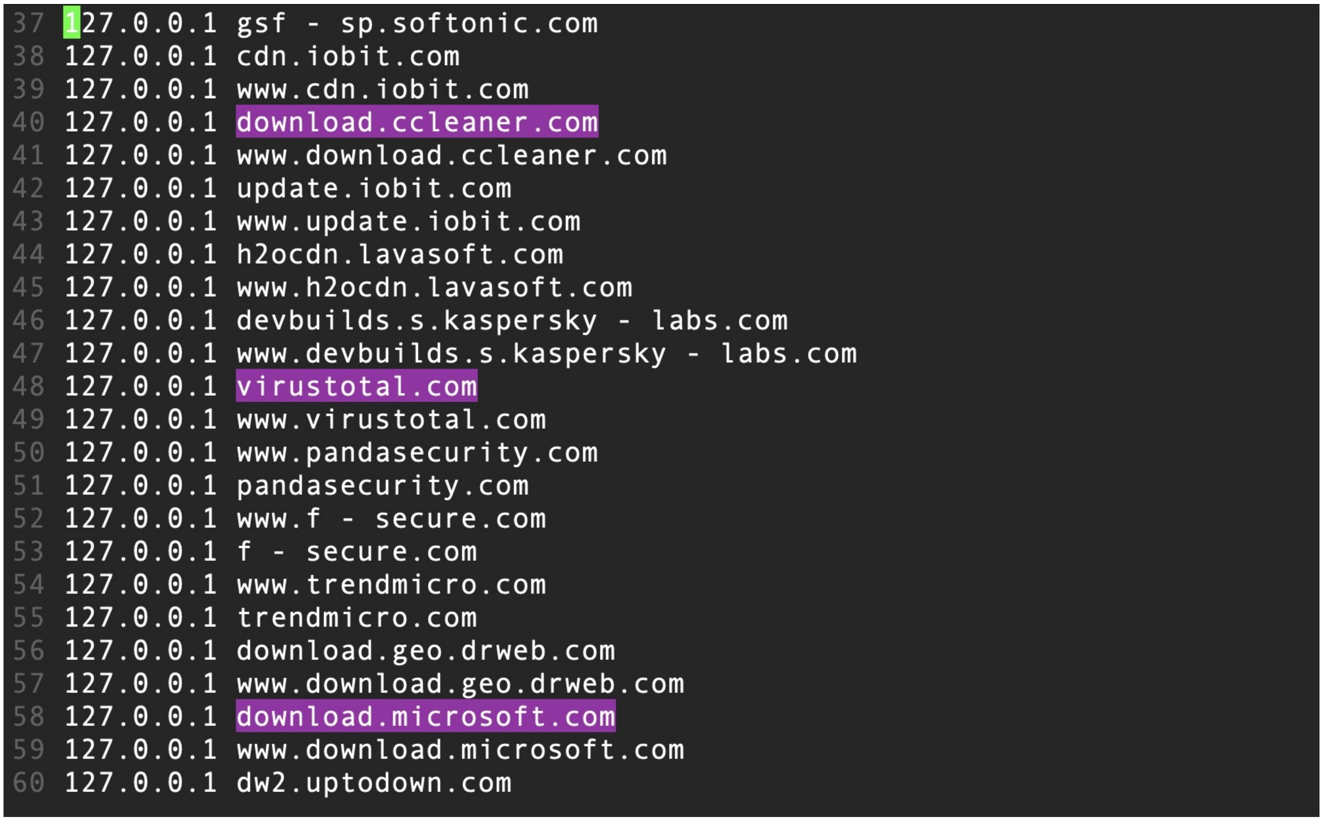
ABREME .exe

Options in this section include:

- Network awareness (remain idle until Wi-Fi is available)
- Verbose output options (decrypter)
- Persistence (add to startup)
- Inhibit recovery (website blocking, self-destruction, backup destruction).

The “block antivirus websites” option is meant to inhibit the victims from being able to download security software or check suspicious files on public malware repository sites such as VirusTotal.

The ransomware achieves this by modifying the device’s Hosts file, adding a long list of sites belonging to the likes of Avast, Avira, Bitdefender, CCleaner, Google, Kaspersky, McAfee, Microsoft, Panda Security, Trend Micro, VirusTotal, YouTube, and others. Each site is simply bound to the machine’s loopback address (typically, `127.0.0.1`), preventing the domain name from being resolved to an external IP address.



```
127.0.0.1 gsf - sp.softonic.com
127.0.0.1 cdn.iobit.com
127.0.0.1 www.cdn.iobit.com
127.0.0.1 download.ccleaner.com
127.0.0.1 www.download.ccleaner.com
127.0.0.1 update.iobit.com
127.0.0.1 www.update.iobit.com
127.0.0.1 h2ocdn.lavasoft.com
127.0.0.1 www.h2ocdn.lavasoft.com
127.0.0.1 devbuilds.s.kaspersky - labs.com
127.0.0.1 www.devbuilds.s.kaspersky - labs.com
127.0.0.1 virustotal.com
127.0.0.1 www.virustotal.com
127.0.0.1 www.pandasecurity.com
127.0.0.1 pandasecurity.com
127.0.0.1 www.f - secure.com
127.0.0.1 f - secure.com
127.0.0.1 www.trendmicro.com
127.0.0.1 trendmicro.com
127.0.0.1 download.geo.drweb.com
127.0.0.1 www.download.geo.drweb.com
127.0.0.1 download.microsoft.com
127.0.0.1 www.download.microsoft.com
127.0.0.1 dw2.uptodown.com
```

Some of the almost 100 domain names added to the Hosts file

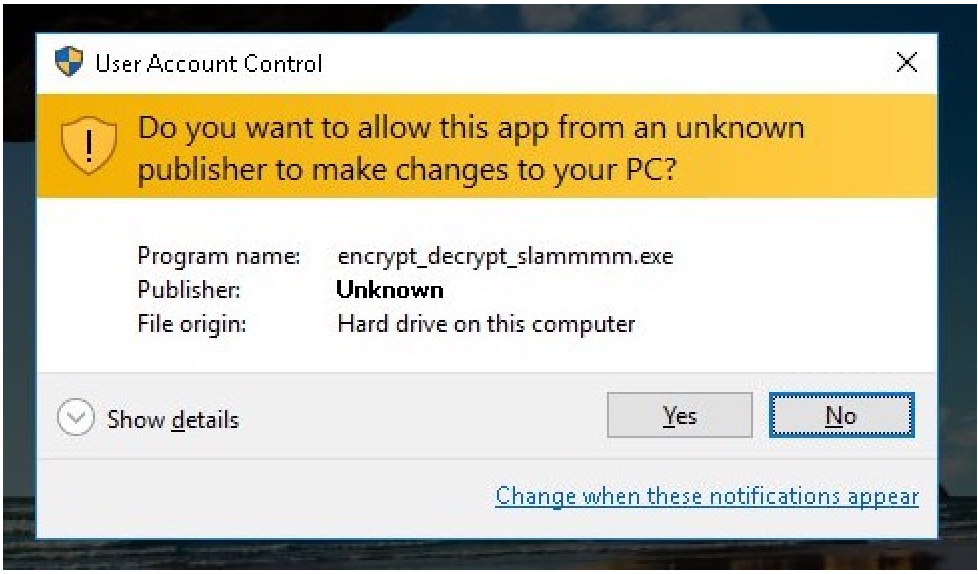
With regard to bypasses, the version of Slam we analyzed includes a single UAC bypass, based on UACMe, which attempts to defeat Windows User Account Control by abusing the built-in Windows AutoElevate backdoor. UACMe is a bypass technique that has been known for some years and widely abused by a number of other malware families including Multiplug adware, Dyre, Empercrypt and IcedID.

To exfiltrate victim data, the user can specify an HTTP server in the configuration interface, where a connection test can also be performed. If the connection test fails, an error is displayed. Other options available to the user include USB infection and execution of custom commands when the payload is detonated on the victim machine.

Slam Ransomware Payloads

With all options configured, the executable payloads generated are standard EXE files. The builder outputs both the encryptor and decryptor tools.

When executed with non-Administrator privileges, the UAC prompts and/or configured bypasses will come into play.



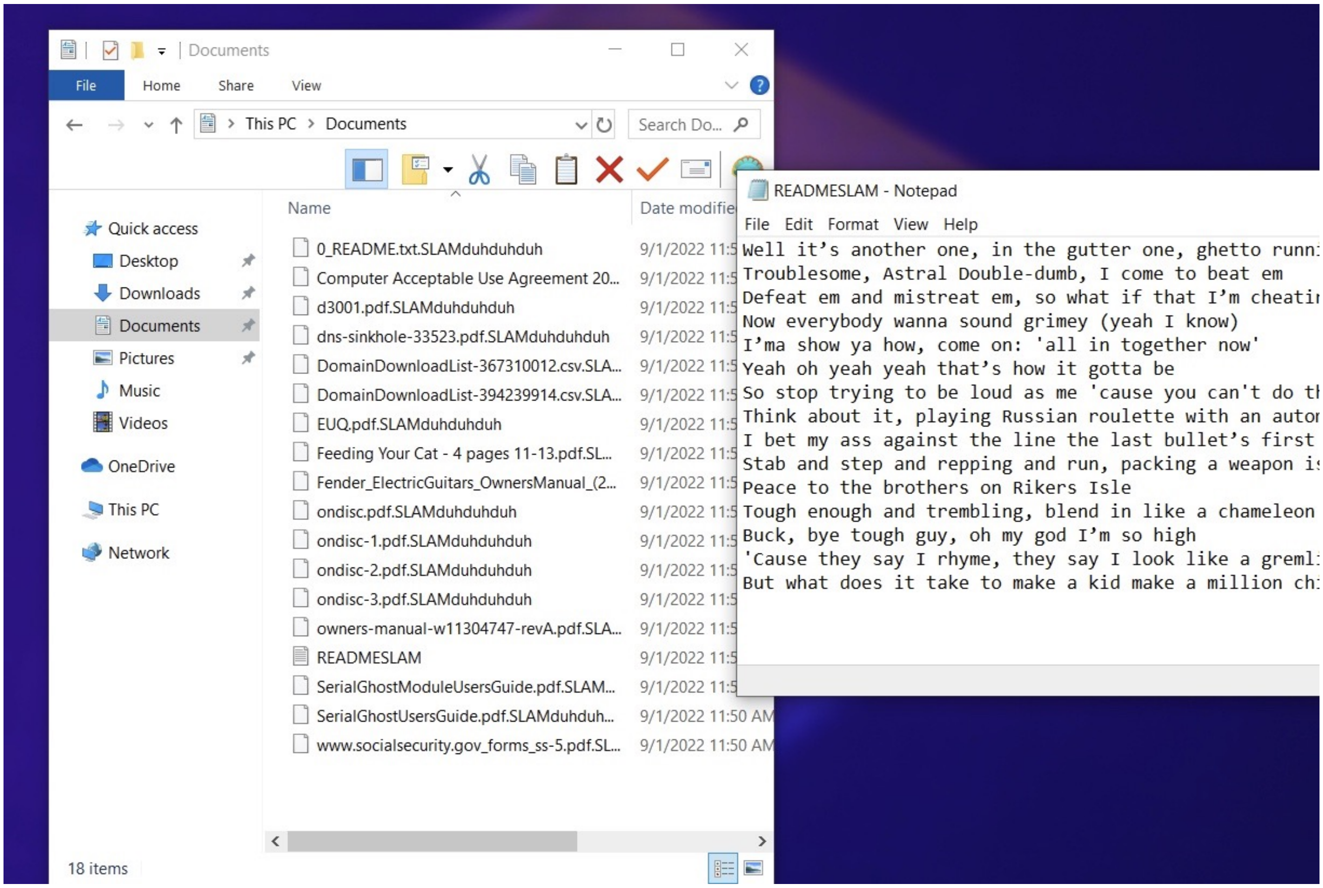
User Account Control

Do you want to allow this app from an unknown publisher to make changes to your PC?

Program name: encrypt_decrypt_slammmm.exe
Publisher: **Unknown**
File origin: Hard drive on this computer

Slam payload UAC prompt

Post-execution, the victim device is encrypted according to the options configured in the builder.

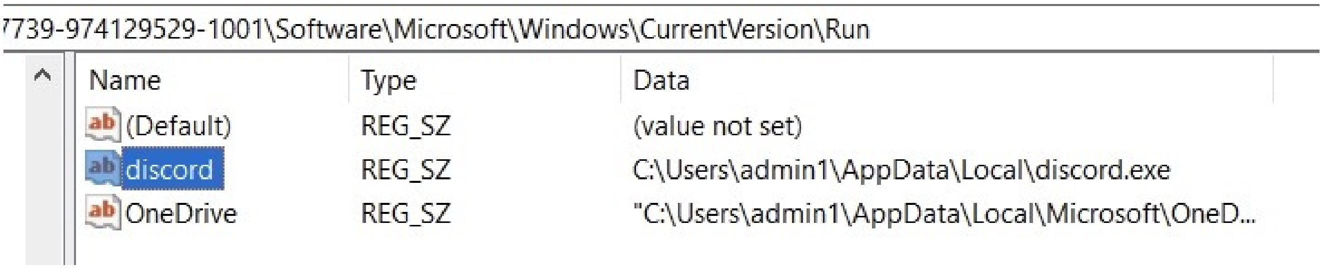


Name	Date modifie
0_README.txt.SLAMduhduhduh	9/1/2022 11:5
Computer Acceptable Use Agreement 20...	9/1/2022 11:5
d3001.pdf.SLAMduhduhduh	9/1/2022 11:5
dns-sinkhole-33523.pdf.SLAMduhduhduh	9/1/2022 11:5
DomainDownloadList-367310012.csv.SLA...	9/1/2022 11:5
DomainDownloadList-394239914.csv.SLA...	9/1/2022 11:5
EUQ.pdf.SLAMduhduhduh	9/1/2022 11:5
Feeding Your Cat - 4 pages 11-13.pdf.SL...	9/1/2022 11:5
Fender_ElectricGuitars_OwnersManual_(2...	9/1/2022 11:5
ondisc.pdf.SLAMduhduhduh	9/1/2022 11:5
ondisc-1.pdf.SLAMduhduhduh	9/1/2022 11:5
ondisc-2.pdf.SLAMduhduhduh	9/1/2022 11:5
ondisc-3.pdf.SLAMduhduhduh	9/1/2022 11:5
owners-manual-w11304747-revA.pdf.SLA...	9/1/2022 11:5
READMESLAM	9/1/2022 11:5
SerialGhostModuleUsersGuide.pdf.SLAM...	9/1/2022 11:5
SerialGhostUsersGuide.pdf.SLAMduhduh...	9/1/2022 11:50 AM
www.socialsecurity.gov_forms_ss-5.pdf.SL...	9/1/2022 11:50 AM

READMESLAM - Notepad

```
Well it’s another one, in the gutter one, ghetto runn
Troublesome, Astral Double-dumb, I come to beat em
Defeat em and mistreat em, so what if that I’m cheati
Now everybody wanna sound grimey (yeah I know)
I’ma show ya how, come on: 'all in together now'
Yeah oh yeah yeah that’s how it gotta be
So stop trying to be loud as me 'cause you can't do t
Think about it, playing Russian roulette with an auto
I bet my ass against the line the last bullet’s first
Stab and step and repping and run, packing a weapon i
Peace to the brothers on Rikers Isle
Tough enough and trembling, blend in like a chameleon
Buck, bye tough guy, oh my god I’m so high
'Cause they say I rhyme, they say I look like a greml
But what does it take to make a kid make a million ch
```

The payload is written to `%AppData%\Local\discord.exe` , which is called in the registry (Run key), ensuring the ransomware payload is persistent.



7739-974129529-1001\Software\Microsoft\Windows\CurrentVersion\Run

Name	Type	Data
(Default)	REG_SZ	(value not set)
discord	REG_SZ	C:\Users\admin1\AppData\Local\discord.exe
OneDrive	REG_SZ	"C:\Users\admin1\AppData\Local\Microsoft\OneD...

As advertised, the Slam payload successfully inhibits recovery via removal of VSS backups on an unprotected machine. Both `wmic` and `vssadmin` methods are utilized for VSS deletion.

```
/c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set
{default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled
no & wbadmin delete catalog -quiet

wmic shadowcopy delete
```

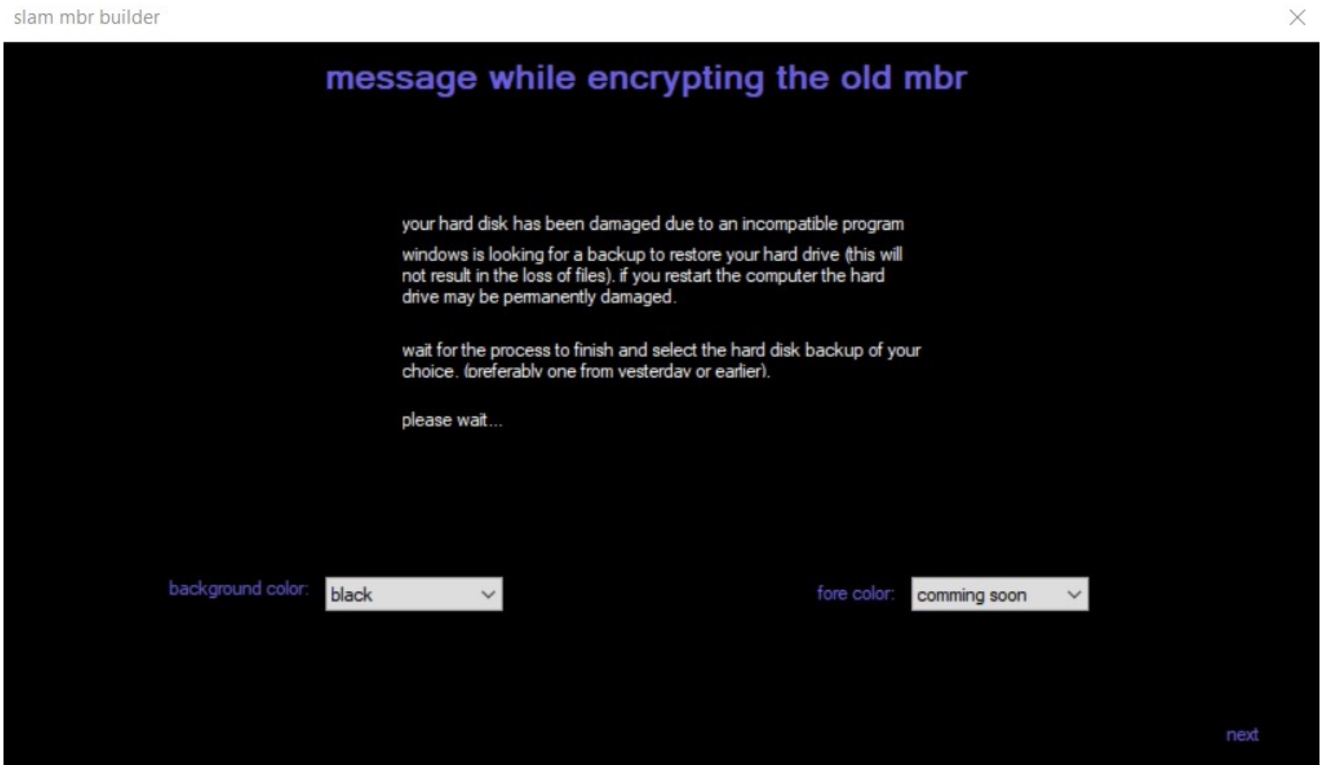
The ransomware also deletes various logs, Windows installation and recovery-related files via `cleanmgr.exe`. In the payload we analyzed, for example, a process named `wgMHhFHnkiczPUNfqaA8Cx4kqwVcRG.exe` issues the `cleanmgr.exe` command with the `/AUTOCLEAN` parameter, which executes Windows disk cleanup and removes Windows installation files on unprotected devices.

```
\system32\cleanmgr.exe /autoclean /d C:
```

Slam MBR Builder

The Slam builder also contains a very early stage “Alpha” MBR builder tool. Choosing to “Install” should write `start.exe` to `c:\slam_mbr_builder\start.exe`. This does not appear to occur in our testing and analysis, and the feature appears to be non-functional in the version of the Slam Builder we analyzed from Github.

However, we were able to obtain a copy of the builder from another source that allowed us to launch the builder and observe the output.



message while encrypting the old mbr

your hard disk has been damaged due to an incompatible program

windows is looking for a backup to restore your hard drive (this will not result in the loss of files). if you restart the computer the hard drive may be permanently damaged.

wait for the process to finish and select the hard disk backup of your choice. (preferablv one from vesterdav or earlier).

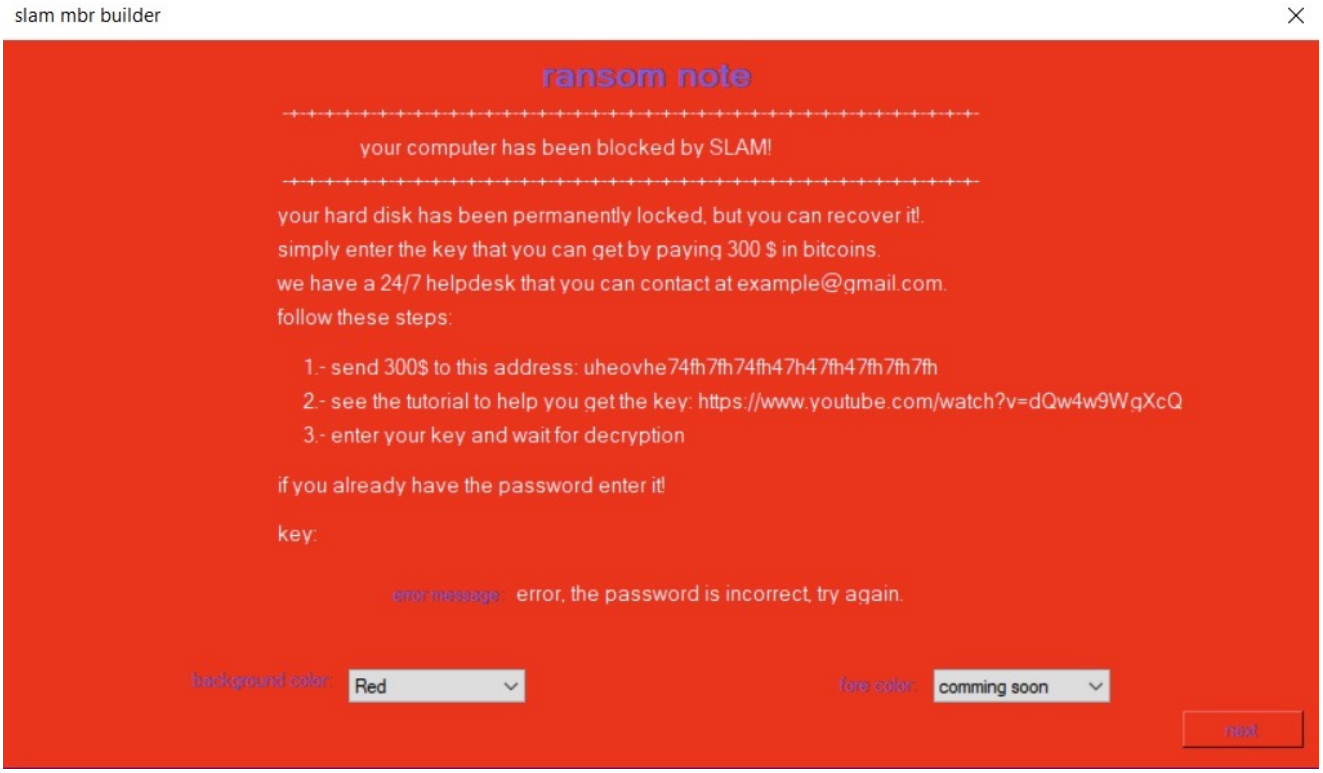
please wait...

background color: black

fore color: comming soon

Slam “Alpha” MBR builder

Within the MBR Builder interface, users are able to configure the message displayed to the victim.



ransom note

-+-

your computer has been blocked by SLAM!

-+-

your hard disk has been permanently locked, but you can recover it!.
simply enter the key that you can get by paying 300 $ in bitcoins.
we have a 24/7 helpdesk that you can contact at example@gmail.com.
follow these steps:

1.- send 300$ to this address: uheovhe74fh7fh74fh47h47fh47fh7fh7fh
2.- see the tutorial to help you get the key: https://www.youtube.com/watch?v=dQw4w9WgXcQ
3.- enter your key and wait for decryption

if you already have the password enter it!

key:

error message: error, the password is incorrect, try again.

background color: Red

fore color: comming soon

Slam MBR Builder Ransom Note Configuration

Prior to executing the build, a final screen allows the attacker to choose the “reboot mode” with the options being

- Do Nothing
- BSOD
- Reboot
- Shutdown
- Nothing

Payloads from the MBR builder have been observed in the wild with the following PDB string.

```
C:\slam_mbr_builder\MbrOverwriter\mbrcs\obj\Debug\mbrcs.pdb
```

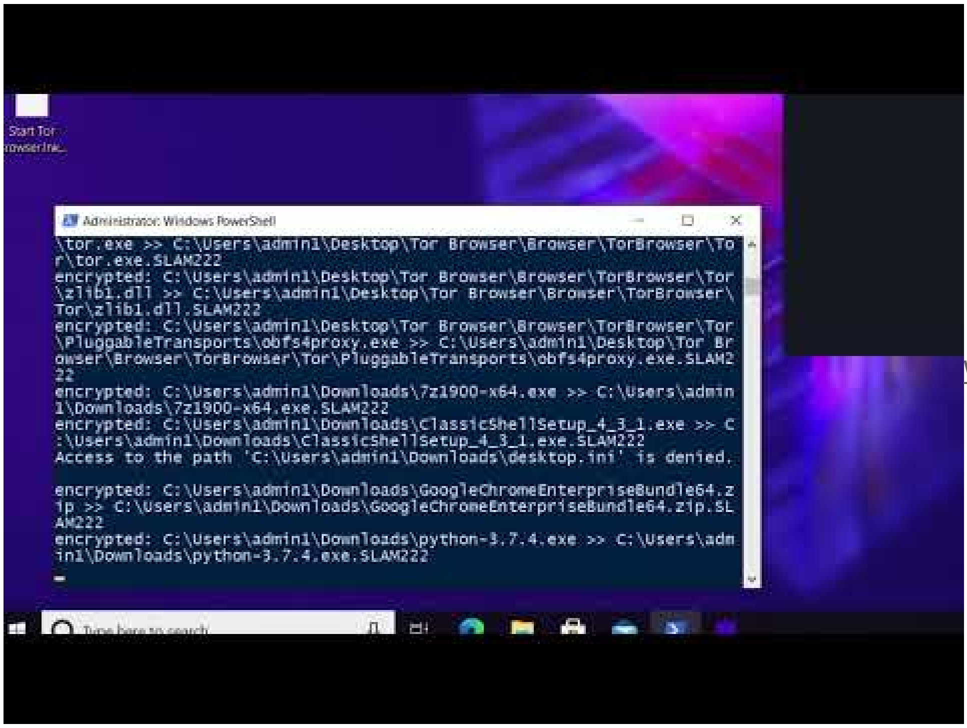
Conclusion

In this area and many others of infosec, there is a fine line between “education” and researcher-led offensive security that seeks to explore and improve weaknesses in enterprise defenses on the one hand, and simple, out-and-out malicious code designed to aid and abet criminal offenses on the other. We see no indications in the various public artifacts around the Slam ransomware builder (code, videos, Github repository) that suggest it could reasonably be interpreted as in the service of the former.

However that may be, once in the hands of unscrupulous actors, full-featured projects such as these represent a real risk to enterprises and organizations.

We applaud Github for removing this code and hope this post serves as a reminder to defenders to be vigilant as threat actors continue to simplify the ransomware-centric extortion process. The barrier to entry into the world of cybercrime has never been lower.

SentinelOne Singularity™ detects and prevents malicious behavior associated with Slam Ransomware and its associated artifacts.



```
\tor.exe >> C:\Users\admin1\Desktop\Tor Browser\Browser\TorBrowser\To
r\tor.exe.SLAM222
encrypted: C:\Users\admin1\Desktop\Tor Browser\Browser\TorBrowser\Tor
\zlib1.dll >> C:\Users\admin1\Desktop\Tor Browser\Browser\TorBrowser\
Tor\zlib1.dll.SLAM222
encrypted: C:\Users\admin1\Desktop\Tor Browser\Browser\TorBrowser\Tor
\PluggableTransports\obfs4proxy.exe >> C:\Users\admin1\Desktop\Tor Br
owser\Browser\TorBrowser\Tor\PluggableTransports\obfs4proxy.exe.SLAM2
22
encrypted: C:\Users\admin1\Downloads\7z1900-x64.exe >> C:\Users\admin
1\Downloads\7z1900-x64.exe.SLAM222
encrypted: C:\Users\admin1\Downloads\ClassicShellSetup_4_3_1.exe >> C
:\Users\admin1\Downloads\ClassicShellSetup_4_3_1.exe.SLAM222
Access to the path 'C:\Users\admin1\Downloads\desktop.ini' is denied.

encrypted: C:\Users\admin1\Downloads\GoogleChromeEnterpriseBundle64.z
ip >> C:\Users\admin1\Downloads\GoogleChromeEnterpriseBundle64.zip.SL
AM222
encrypted: C:\Users\admin1\Downloads\python-3.7.4.exe >> C:\Users\adm
in1\Downloads\python-3.7.4.exe.SLAM222
_
```

Watch Video At:

https://youtu.be/nI6LYb3yCi4

Indicators of Compromise

Observed File Names

ConsoleApp2.exe

mbrcs.exe

JpegMedic ARWE

slam ransomware builder.exe

Observed PDB Strings

```
C:\slam_mbr_builder\MbrOverwriter\mbrcs\obj\Debug\mbrcs.pdb
c:\slam_ransomware_builder\ConsoleApp2\ConsoleApp2\obj\Debug\ConsoleApp2.pdb
C:\Users\amdga\Desktop\UACME-master\Source\Akagi\output\Win32\Debug\Akagi.pdb
D:\agent\_work\20\s\\binaries\x86ret\bin\i386\\vcruntime140d.i386.pdb
c:\slam_ransomware_builder\uac\ConsoleApp2\obj\Debug\ConsoleApp2.pdb
c:\slam_ransomware_builder\ConsoleApp2\ConsoleApp2\obj\Debug\ConsoleApp2.pdb
C:\slam_mbr_builder\MbrOverwriter\mbrcs\obj\Debug\mbrcs.pdb
C:\Users\amdga\source\repos\conect\conect\obj\Debug\conect.pdb
C:\Users\ander\source\repos\slam ransomware builder\slam ransomware
builder\obj\Debug\slam ransomware builder.pdb
```

SHA1 Hashes

1ba9043ac164c6c60de4a1ee2ca50b2e7f4ebaf5

2037d9f2e7cd15930e83f5142c5a48adecd3b617

272566e8b5880e32cefb7a165a833652815a003f

27b1ca0793caa19edabfbc49e6cffc05b73093da

2c41f64557056e69541acf5ba52313869122f625
336371f4200af680f73c0b9c51fca5a25dd5754a
35ab1d4924990bf98a8e2e1026f91b5c9052de8e
3fa6705ca1b056a66f25a689dff72af0893f5b86
40bfa92e86484c09f2f7668121a1c4047c17ae72
44aaef83b79f4e963c4fee56250bc053eae5ec64
4879bd193dd73681c977371c857217257f141c92
4cff2b02cb6c1f866499125c003af1032a81b480
5a28f787cc73cffa7b5786faf3298d43e00d12aa
61e8ba86725ec3f4e034c51950cabc6254c5cca5
6325c42719b1aa3a48dd39b8add200054d3e0118
669ce00937bde782a88526205f083861e6d71be1
6e420a6c7b8e2d144df66dcbbae1afba62c82f4b
7429fdf9151dfa9e4d4dc8ef86528313d13dc73f
7690c273c8164a65602ed8f4284f0d50966d27c6
863edff3c71e89349674df35ab07f27ecb6702ef
880c343e75e7e8731f185ce756357599c37be065
8b46ce2ffa24a377ff30ea094e02bc3ba3e808da
8f3dc8437563182e06699763581fd6f7923b7582
9edd3d920fbe89240d52cc8b300a90e5bf576f73
b031d4c3747b58d930f33fe73abbf518dac63a31
be82474f54f49249c43c701c12907ec730e2a723
c5351846988ef5d6e7b95f564416138f59e2092a
c84aeb8c0b3939fd7f6beb9d73e72cc5ed8745db
c998384c7b8cfd2ca881f282dfdbc104d8402bac
ca2999c9c5a17b0253579194f651b4aafdce16f1
cb243b61a8d43816e1de7f0767b1377d0276dd71
cf30cc1e653043df81aa9d8974f2f927ceadc826
d187d81f4d021839e8f6e925dc192e231eb4679c
d635103117daaf2a2b93d465e32e7b722dd4d367
d6c9a556f5770f0a8f8ad05c5d46becd0cd021d3
d94eb94bb3c2c6c0c70916f8be2417ac616e8b43
dc327f3afbb6c770656be16fc885e1090f8395a3
ddba71aae3b8139210f71e835e1b89e90b0bd1dc
e0868fdb2f09d3a4aefe4c79d6af88c2f9b55ce2
e2052995d368355e899a518dbbbab716045abbd1
e9a5b40d0ba5a8bb5c4a1c5471616c93e0851558
ea4f7dda5a64a740a9c5570870ccba2788c69ea6
ee144154139619b8c1d890e5b6f9bf130d929e6f
eeafbbfaaf05d8b7a8a1dc3f7858a21e7fdb0531
f31855a1d5509b1e906caee75db3326515488cbc
fcd90af249796fc3c40e1e94d558b6f2d61304b5

MITRE ATT&CK

T1542.003 – Pre-OS Boot: Bootkit
T1047 – Windows Management Instrumentation
T1547.001 – Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
T1564.003 – Hide Artifacts: Hidden Window
T1112 – Modify Registry
T1490 – Inhibit System Recovery
T1486 – Data Encrypted for Impact
T1491.001 – Defacement: Internal Defacement
T1083 – File and Directory Discovery
T1005 – Data from Local System
T0809 – Data Destruction