Smash-and-grab: AstraLocker 2.0 pushes

ReversingLabs recently discovered instances of the AstraLocker 2.0 malware distributed directly from Microsoft Word files used in phishing attacks.

Executive Summary

ReversingLabs recently discovered of a new version of the AstraLocker ransomware (AstraLocker 2.0) that was being distributed directly from Microsoft Office files used as bait in phishing attacks. Our analysis suggests that the threat actor responsible for this campaign likely obtained the underlying code for AstraLocker 2.0 from a leak of the Babuk ransomware in September 2021. Links between the two campaigns include shared code and campaign markers, while a Monero wallet address listed for ransom payment is tied to the Chaos Ransomware gang.

The “smash and grab” attack methodology as well as other features suggest the attacker behind this malware is low-skill and looking to cause disruption, compared with the more patient, methodical, and measured approach to compromises used by Babuk and other, more sophisticated ransomware outfits. This underscores the risk posed to organizations following code leaks like that affecting Babuk, as a large population of low-skill, high-motivation actors leverage the leaked code for use in their own attacks.

Analysis

ReversingLabs threat analysts have looked at a number of samples of the AstraLocker 2.0 malware. This report reflects the conclusions of their analysis of the malware and associated attacks.

Background

First identified in 2021, AstraLocker is a fork of Babuk, ransomware used by the cybercriminal group of the same name. The Babuk group operated a Ransomware-as-a-Service (RaaS) platform and licensed its software to affiliates to carry out attacks.

Babuk first appeared in early 2021 and was linked to a string of high-profile attacks, including a ransomware attack and data leak targeting Washington D.C.'s Metro Police Department in April, 2021. By September of 2021, the Babuk group became a target itself, when the Babuk source code was stolen and leaked to a Russian hacking forum.

The AstraLocker malware also appeared in 2021, concurrent with Babuk. AstraLocker 2.0 was first seen in March 2022.

Significance

The AstraLocker 2.0 attack we observed was unusual in a number of ways. First: the attackers opted to push ransomware to victims at the very earliest stage of the attack, immediately after targets opened the malicious file attachment used as bait in the initial phishing attacks.

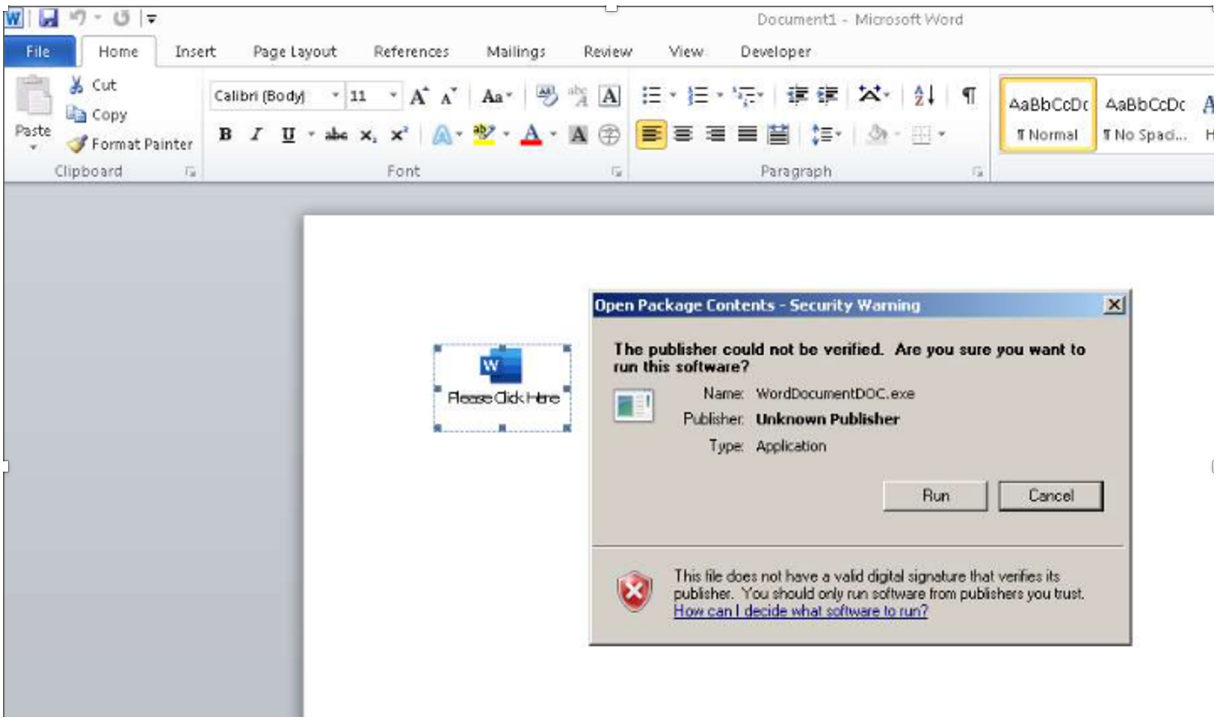
Typically, affiliate threat actors avoid pushing ransomware early, opting instead to push files that allow them to expand their reach within the target environment. Ransomware almost invariably is deployed last, after compromising the victim's Domain Controller(s), which enables the cybercriminals to use the domain controller (for example: Active Directory) to deploy a group policy object and encrypt all hosts in the affected domains. It's unusual to see a phishing document deliver ransomware immediately.

However, the samples ReversingLabs uncovered revealed a threat actor that was strictly interested in a big impact and a quick payout – a kind of "smash and grab" operation.

The lure

The AstraLocker samples we uncovered were hidden within Microsoft Word documents. Executing the malware took some doing: recipients who opened the malicious Word attachment were required to make multiple, additional clicks to activate the embedded ransomware. That's because the payload is stored in an OLE object; the lure only activates the ransomware if

the user double clicks the icon in the document and consents to running an embedded executable named "WordDocumentDOC.exe:"

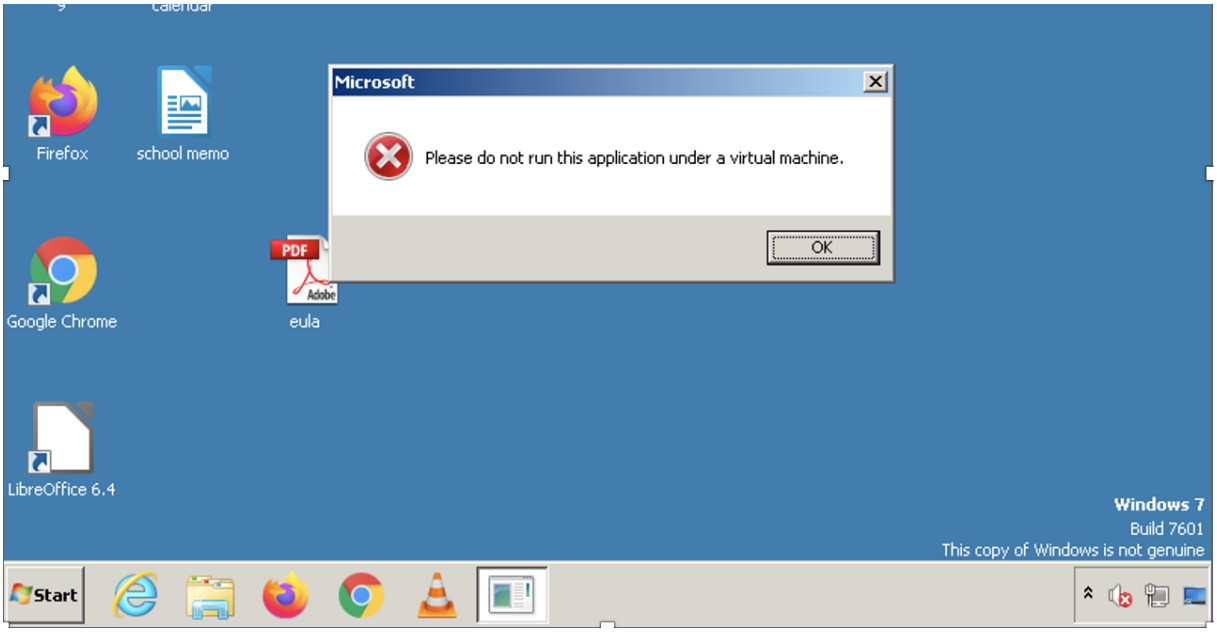


Needless to say: requiring so much user interaction increases the chances that victims will think twice about what they're doing. That's one reason OLE objects see less use in malware delivery, as opposed to the more popular VBA macro infection method, which only requires the user to enable macros in order to execute.

Unique features

In addition to the user-interaction intensive bait, the AstraLocker 2.0 samples used an outdated packer, the SafeEngine Shielden v2.4.0.0 protector, making them difficult to reverse engineer. This packer is so old that the legitimate version no longer appears to be sold, which means the threat actor likely obtained a cracked version. One of its tactics is to inject indirect jumps every 5-7 instructions, obfuscating the control flow of the program.

The malware also employs evasion tactics, checking whether the host is a virtual machine. If a VM is detected, the malware displays the following message (which is assuredly *not* from Microsoft).



The packer checks running processes to determine if it is in an analysis environment. To do this, it calls the NtQuerySystemInformation API, passing the ProcessInformation and EmulationProcessorInformation parameters.

In addition, the protector checks the names of open windows to determine if malware analysis tools are being run with different process names. One such window it searched for was **Regmonclass**, the window name associated with the tool Registry Monitor, before it became Process Monitor.

The packer attempts to hide its threads from debuggers by setting the thread information argument **HideFromDebugger**. It attempts to detect an evasive debugger by using rdtsc, an instruction which reads the system's Time Stamp Counter. Using rdtsc before and after a function, the malware can identify when a debugger has taken too long and is being debugged.

Impact

Once unpacked, AstraLocker 2.0 employs several tactics to avoid detection and hamper attempts to recover. Among them:

Stops a list of backup and anti-malware and security services:

Like many ransomware files, AstraLocker attempts to disable anti-malware and other endpoint security tools. These include the following:

vss, sql, svc$, memtas, mepocs, sophos, veeam, backup, GxVss, GxBlr, GxFWD, GxCVD, GxCIMgr, DefWatch, ccEvtMgr, ccSetMgr, SavRoam, RTVscan, QBFCService, QBIDPService, Intuit.QuickBooks.FCS, QBCFMonitorService, YooBackup, YooIT, zhudongfangyu, stc_raw_agent, VSNAPVSS, VeeamTransportSvc, VeeamDeploymentService, VeeamNFSSvc, PDVFSService, BackupExecVSSProvider, BackupExecAgentAccelerator, BackupExecAgentBrowser, BackupExecDiveciMediaService, BackupExecJobEngine, BackupExecManagementService, BackupExecRPCService, AcrSch2Svc, AcronisAgent, CASAD2DWebSvc, CAARCUpdateSvc

Kills a list of processes that could interfere with encryption:

The AstraLocker malware also attempts to disable applications that may block- or interfere with the encryption of data. These include:

sql.exe, oracle.exe, ocssd.exe, dbsnmp.exe, synctime.exe, agntsvc.exe, isqlplussvc.exe, xfssvccon.exe, mydesktopservice.exe, ocautoupds.exe, encsvc.exe, firefox.exe, tbirdconfig.exe, mydesktopqos.exe, ocomm.exe, dbeng50.exe, sqbcoreservice.exe, excel.exe, infopath.exe, msaccess.exe, mspub.exe, onenote.exe, outlook.exe, powerpnt.exe, steam.exe, thebat.exe, thunderbird.exe, visio.exe, winword.exe, wordpad.exe, notepad.exe

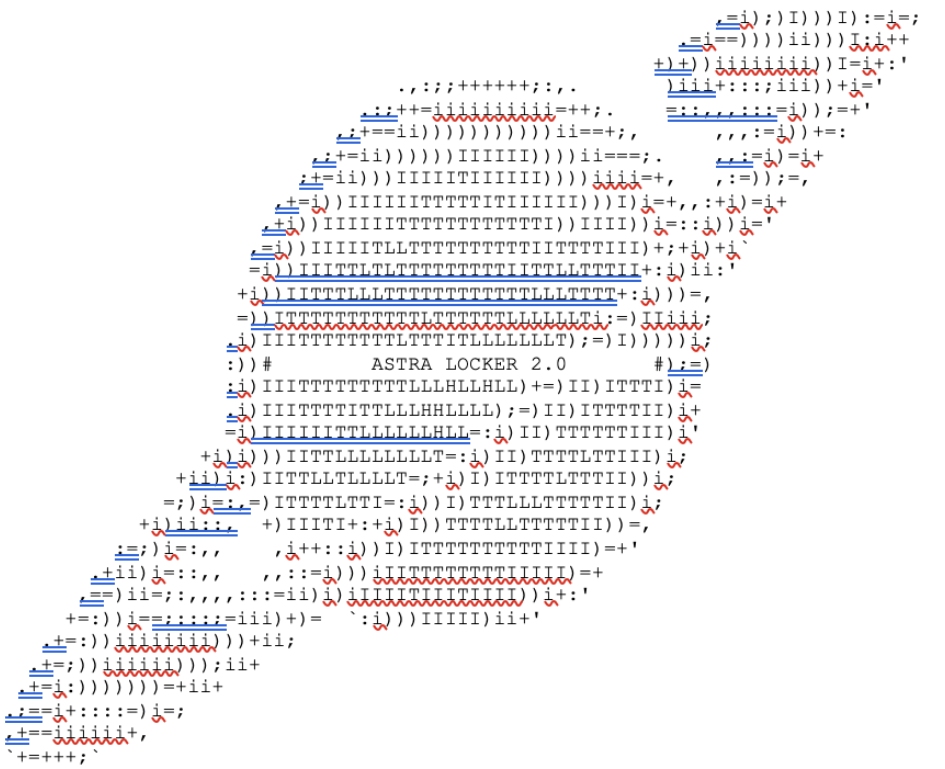
Deletes Volume Shadow Copies using the command
Sample command:
```
C:\Windows\System32\cmd.exe /c vssadmin.exe delete shadows /all /quiet.
```

Empties the Recycle Bin, rather than encrypting files there
Enumerates and attempts to mount all drives and network shares to ensure encryption occurs on all reachable resources
Encrypts files with the Elliptic Curve Cryptography algorithm Curve25519

Ransom note and FAQ

AstraLocker 2.0 displays the following ransom note, which closely resembles the standard Babuk ransomware note. This note has been modified by our threat actor to include new Monero and BitCoin wallets for payment. However, the attacker did not provide a contact email for victims, making it unclear how -or if -payments from victims were carried

out.




```
What happend?
------------------------------------------------
All Your files has been succesfully encrypted by AstraLocker 2.0

Can I get My files back?
------------------------------------------------
Sure! But You dont have much time for this.
Your computer is infected with a ransomware virus. Your files have been
encrypted and you won't be able to decrypt them without my help.

What can I do to get my files back?
------------------------------------------------
You can buy my decryption software, this software will allow you to recover
all of your data and remove the Ransomware from your computer.
The price for the software is about 50$ (USD). Payment can be made in Monero,
or Bitcoin (Cryptocurrency) only.

What guarantees?
------------------------------------------------
I value my reputation. If i do not do my work and liabilities, nobody will
pay me. This is not in my interests.
All my decryption software is perfectly tested and will decrypt your data.
```

Campaign markers

ReversingLabs analysis of AstraLocker revealed the following toolmarks, which your organization can use to identify the source of this new AstraLocker 2.0 campaign:

Mutex

Malware authors create a Mutex object to ensure only one encryptor is running at a time. The mutex created in this case was named `DoYouWantToHaveSexWithCuongDong`, while in other campaigns the mutex was called `EncryptedWithAstraLocker`. However, we did notice that the variant with the latter mutex was generating new files.

File footer

After encryption, AstraLocker 2.0 appends the text choung dong looks like hot dog!! to the end of the file. The corresponding decryptor searches for this footer to identify encrypted files.

Extension

In this campaign, AstraLocker 2.0 renames files with the **.babyk** extension, where in other instances it used **.AstraLocker**, **.piton**, **.Astra**, or a randomized extension.

Packer

Using the RHA similarity algorithm, we identified similar samples packed with SafeEngine Shielden, which are most likely in our campaign.

Ransom wallets

AstraLocker 2.0 uses a different set of cryptocurrency wallet addresses than were used in earlier versions of the malware and in the Babuk ransomware. In addition, the 2.0 version omits a working email address for contacting the threat actors.

Monero

The AstraLocker 2.0 lists the following Monero wallet address, which is notable for being the same wallet listed in the ransom note dropped by Chaos Ransomware, which was written in .NET.

```
47moe29QP2xF2myDYaaMCJHpLGsXLPw14aDK6F7pVSp7Nes4XDPMmNUgTeCPQi
5arDUe4gP8h4w4pXCtX1gg7SpGAgh6qqS
```

BitCoin (BTC)

The BitCoin wallet address used by AstraLocker 2.0 is associated with another AstraLocker 2.0 campaign.

```
bc1qpjftnrmahzc8cjs23snk2rq0vt6l0ehu4gqxus.
```

Email address

The original emails seem to have been removed. In this campaign, the AstraLocker emails are replaced with **AstraLocker@**. This could indicate that the threat actors are not tied to the original threat group.

Conclusions

ReversingLabs researchers have came to the conclusion that the threat actor responsible for this campaign likely obtained the builders for the AstraLocker 2.0 ransomware as a result of the Babuk leak in mid-2021. There are a number of elements of the campaign that lead us to that conclusion. Among them: the code and campaign markers in AstraLocker 2.0 are consistent with the encryptor used by the Babuk gang, as documented in this article. To that, the attackers added the SafeEngine Shielden packer and a slightly modified version of the Babuk ransom note.

While we do not have any conclusive evidence linking the AstraLocker “smash and grab” campaign to a specific individual, we know that the threat actors use a Monero wallet address that may be tied to Chaos Ransomware group. That makes it reasonable to assume that the threat actor behind this attack may have some affiliation with that group. This, however, is mere speculation.

What this attack makes clear is that the leak of the Babuk source code and builders in 2021 permits cybercriminals of any sophistication to launch their own operations, simply by making small modifications to the existing Babuk code. That is what we observe with the AstraLocker 2.0 malware. By leveraging the leaked code and dispensing with the “low and slow”

methodology that is common among sophisticated ransomware outfits, the attackers behind the AstraLocker 2.0 attacks have greatly shortened the time and investment needed to realize a profit off of infected hosts with their “smash and grab” approach.

However, as we see with actual “smash and grab” attacks – it is easy for attackers launching such hasty efforts to make mistakes. In this case, without a listed email to contact for victims, the AstraLocker 2.0 threat actor has no means of issuing the decryptor to victims even if a ransom is paid. This makes this attack both reckless and destructive.

Indicators of Compromise (IOCs)

Below are hashes of AstraLocker 2.0 indicators of compromise, as identified by ReversingLabs.

SHA256 Hash	File Type
cf3bdf0f8ea4c8ece5f5a76524ab4c81fea6c3a1715b5a86b3ad4d397fca76f3	AstraLocker 2.0 Ransomware
b0a010e5a9b353a11fb664501de91fc47878d89bf97cb57bc03428c7a45981b9	AstraLocker 2.0 Ransomware
17ea24ce8866da7ef4a842cba16961eafba89d526d3efe5d783bb7a30c5d1565	AstraLocker 2.0 Ransomware
08565f345878369fdbbcf4a064d9f4762f4549f67d1e2aa3907a112a5e5322b6	AstraLocker 2.0 Ransomware
5c061e188979d3b744a102d5d855e845a3b51453488530ea5dca6b098add2	AstraLocker

SHA256 Hash	File Type
821	2.0 Ransomware
60167b6a14b7da2257cb6cbdc7f1ebcb4bdfa16c76cc9a7539c9b8d36478d127	Malicious Word Document
71ba916a7f35fe661cb6affc183f1ce83ee068dbc9a123663f93acf7b5a4263e	Malicious Word Document