New in Ransomware: Seth-Locker, Babuk Locker, Maoloa, TeslaCrypt, and CobraLocker

trendmicro.com/en_us/research/21/b/new-in-ransomware.html

February 5, 2021

Ransomware

In this entry, we give an overview of new ransomware discoveries. This includes a new ransomware family dubbed Seth-Locker, and developments in the variants Babuk Locker, Maoloa, TeslaCrypt, and CobraLocker.

By: Raphael Centeno, Monte de Jesus, Don Ovid Ladores, Junestherry Salvador, Nikko Tamana, Llalum Victoria February 05, 2021 Read time: (words)

Ransomware is in constant state of development — this is true not only of ransomware families that are big-game hunters or ransomware families that have a targeted approach in their campaigns, but also for new ones.

In this entry, we look into a new ransomware family dubbed Seth-Locker, which was discovered while at large and is still under development. We also enumerate developments in Babuk Locker, Maoloa, and a possible TeslaCrypt variant. Lastly, we note the appearance of a CobraLocker variant that is at large and uses a popular game as a disguise to attract the attention of unwitting victims.

New ransomware Seth-Locker

We discovered a new ransomware named Seth-Locker at large. An interesting feature of this new ransomware is its inclusion a few backdoor routines in its malicious files, together with its ransom routine. These backdoor routines that have been observed so far are the following:

- open_link for reading content from the command-and-control (C&C) server
- down_exec for downloading and execute a file
- shell to run a command line shell command
- locker to run the ransomware routine
- kill to terminate a process or itself

Once executed, the ransomware follows the typical routine of encrypting files and appending them with the suffix .seth, before dropping a ransom note.

As its code contains several rookie mistakes and oversights, we surmise that it is still under development. For example, malware commands are easily visible and repetitions of file extensions to be checked are in its code. Additionally, another tell-tale sign that it is still under development is that it lacks sophistication in hiding its routines and techniques. In the future, however, it would be possible to encounter an improved version of this ransomware.

Developments in Babuk Locker

Babuk Locker is also a new ransomware family and the first enterprise ransomware discovered in 2021. It initially identified itself as Vasa Locker in December 2020. Babuk Locker is proving to be a fast-evolving and active ransomware. Early into 2021, it had already attacked several companies, utilizing the strategy of threatening to expose stolen information.

Even as a new ransomware-as-a-service (RaaS), its operations follow the methods of known targeted ransomware attacks. Its initial access likely involves compromised user accounts, exploitation of vulnerabilities, or malspam. Threat actors then move laterally to make an inventory of the victim's network and important files since they exfiltrate data as part of their double extortion method. Afterward, they finally proceed to deploying their ransomware payload. In addition, they eventually post the exfiltrated data on a blog or a Tor site that they operate.

Babuk Locker utilizes a ChaCha8 stream cipher for encryption and Elliptic-curve Diffie-Hellman (ECDH) for key generation, making the recovery of files without gaining access to the private key highly unlikely. Chuong Dong's blog gives further details on how this malware operates.

What's notable about Babuk Locker is the progression of its attacks and its threat actors' use of a Tor site to communicate with their victims. The oldest and first sample that we observed involved sending a typical ransom email to their target. Meanwhile, the second variant of the ransomware that we encountered used a Tor site, which showed a screenshot of the data that the threat actors had stolen from their target. Based on this development, we can see how the group behind Babuk Locker is making their extortion methods more personalized and aggressive.

Certain aspects of Babuk Locker have similarities with other known ransomware. In particular, the ransom note is striking as it matches that used by DarkSide. This is evidenced in Figure 1, which suggests that these two ransomware families could be linked together. With regard to techniques, Babuk Locker also seems to have taken a page out of older ransomware like Conti, Ryuk, and Ragnar Locker. For example, like these older malware, it terminates processes and services that are related to applications, back-up software, endpoint security, and servers. Given how effective these known ransomware are, it is no surprise that Babuk Locker has mimicked some of their techniques.

```
---------- [ Hello,                    ] ---------->

       ****BY BABUK LOCKER****


What happend?
-----------------------------------------------
Your computers and servers are encrypted, backups are deleted from your network and copied. We use strong encryption
algorithms, so you cannot decrypt your data.
But you can restore everything by purchasing a special program from us - a universal decoder. This program will restore
your entire network.
Follow our instructions below and you will recover all your data.
If you continue to ignore this for a long time, we will start reporting the hack to mainstream media and posting your
data to the dark web.

What guarantees?
-----------------------------------------------
We value our reputation. If we do not do our work and liabilities, nobody will pay us. This is not in our interests.
All our decryption software is perfectly tested and will decrypt your data. We will also provide support in case of
problems.
We guarantee to decrypt one file for free. Go to the site and contact us.

What information  compromised?
-----------------------------------------------
We copied more than 50 gb  from your internal network, here are some proofs, for additional confirmations, please chat
with us
In cases of ignoring us, the information will be released to the public.


How to contact us?
-----------------------------------------------
Using TOR Browser ( https://www.torproject.org/download/ ):
http://          e2p4wu4iq.onion/login.php?


!!! DANGER !!!
DO NOT MODIFY or try to RECOVER any files yourself. We WILL NOT be able to RESTORE them.
!!! DANGER !!
```

```
---------- [ Welcome to Dark ] ---------->

What happend?
-----------------------------------------------
Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data.
But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your
network.
Follow our instructions below and you will recover all your data.

Data leak
-----------------------------------------------
First of all we have uploaded more then 100 GB data.

Example of data:
 - Accounting data
 - Executive data
 - Sales data
 - Customer Support data
 - Marketing data
 - Quality data
 - And more other...

Your personal leak page: http://          xcftmqa.onion/blog/article/id/6/
The data is preloaded and will be automatically published if you do not pay.
After publication, your data will be available for at least 6 months on our tor cdn servers.

We are ready:
- To provide you the evidence of stolen data
- To give you universal decrypting tool for all encrypted files.
- To delete all the stolen data.

What guarantees?
-----------------------------------------------
We value our reputation. If we do not do our work and liabilities, nobody will pay us. This is not in our interests.
All our decryption software is perfectly tested and will decrypt your data. We will also provide support in case of problems.
We guarantee to decrypt one file for free. Go to the site and contact us.

How to get access on website?
-----------------------------------------------
Using a TOR browser:
1) Download and install TOR browser from this site: https://torproject.org/
2) Open our website: http://          cuhtk2.onion/
```

Figure 1. A Babuk ransom note (top) compared with a DarkSide ransom note (bottom)

Babuk Locker's leak site offers more clues. For example, we observed how the leak site has been modified recently to announce that Babuk has now been rebranded to "Babyk." The site also claims that the group behind the variant is not malicious, and that they aim to expose security issues in organizations.

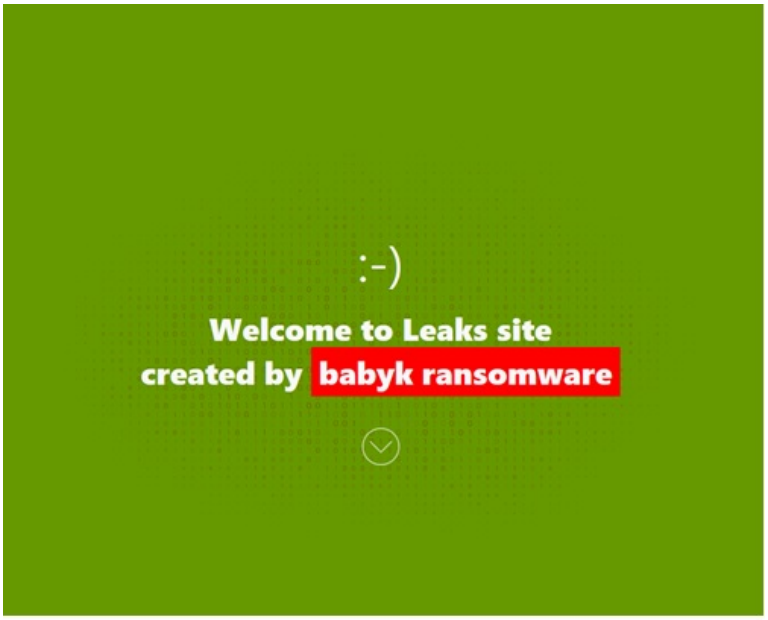
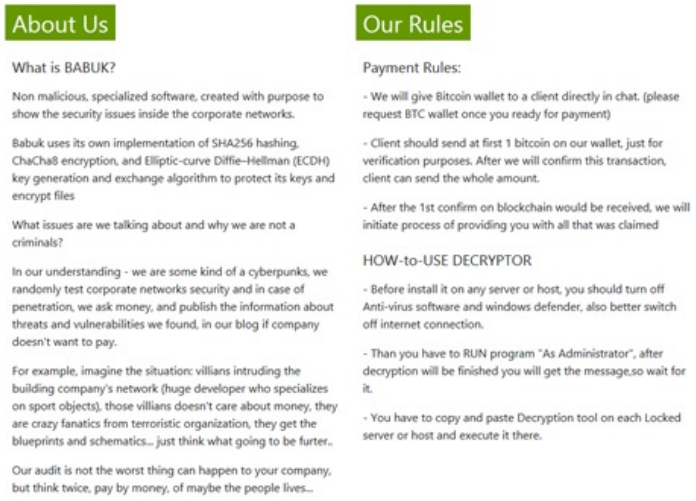


Figure 2. The leak site shows both the rebranding



About Us

What is BABUK?

Non malicious, specialized software, created with purpose to show the security issues inside the corporate networks.

Babuk uses its own implementation of SHA256 hashing, ChaCha8 encryption, and Elliptic-curve Diffie–Hellman (ECDH) key generation and exchange algorithm to protect its keys and encrypt files

What issues are we talking about and why we are not a criminals?

In our understanding - we are some kind of a cyberpunks, we randomly test corporate networks security and in case of penetration, we ask money, and publish the information about threats and vulnerabilities we found, in our blog if company doesn't want to pay.

For example, imagine the situation: villians intruding the building company's network (huge developer who specializes on sport objects), those villians doesn't care about money, they are crazy fanatics from terroristic organization, they get the blueprints and schematics... just think what going to be furter..

Our audit is not the worst thing can happen to your company, but think twice, pay by money, of maybe the people lives...

Our Rules

Payment Rules:

- We will give Bitcoin wallet to a client directly in chat. (please request BTC wallet once you ready for payment)

- Client should send at first 1 bitcoin on our wallet, just for verification purposes. After we will confirm this transaction, client can send the whole amount.

- After the 1st confirm on blockchain would be received, we will initiate process of providing you with all that was claimed

HOW-to-USE DECRYPTOR

- Before install it on any server or host, you should turn off Anti-virus software and windows defender, also better switch off internet connection.

- Than you have to RUN program "As Administrator", after decryption will be finished you will get the message,so wait for it.

- You have to copy and paste Decryption tool on each Locked server or host and execute it there.

from “Babuk” ransomware to “Babyk” and details about the malware.
Interestingly, the leak site also lists entities that are excluded from the group’s scope of interest. This list was present before the modification and is the first time that we have observed a ransomware variant showing this kind of discretion.

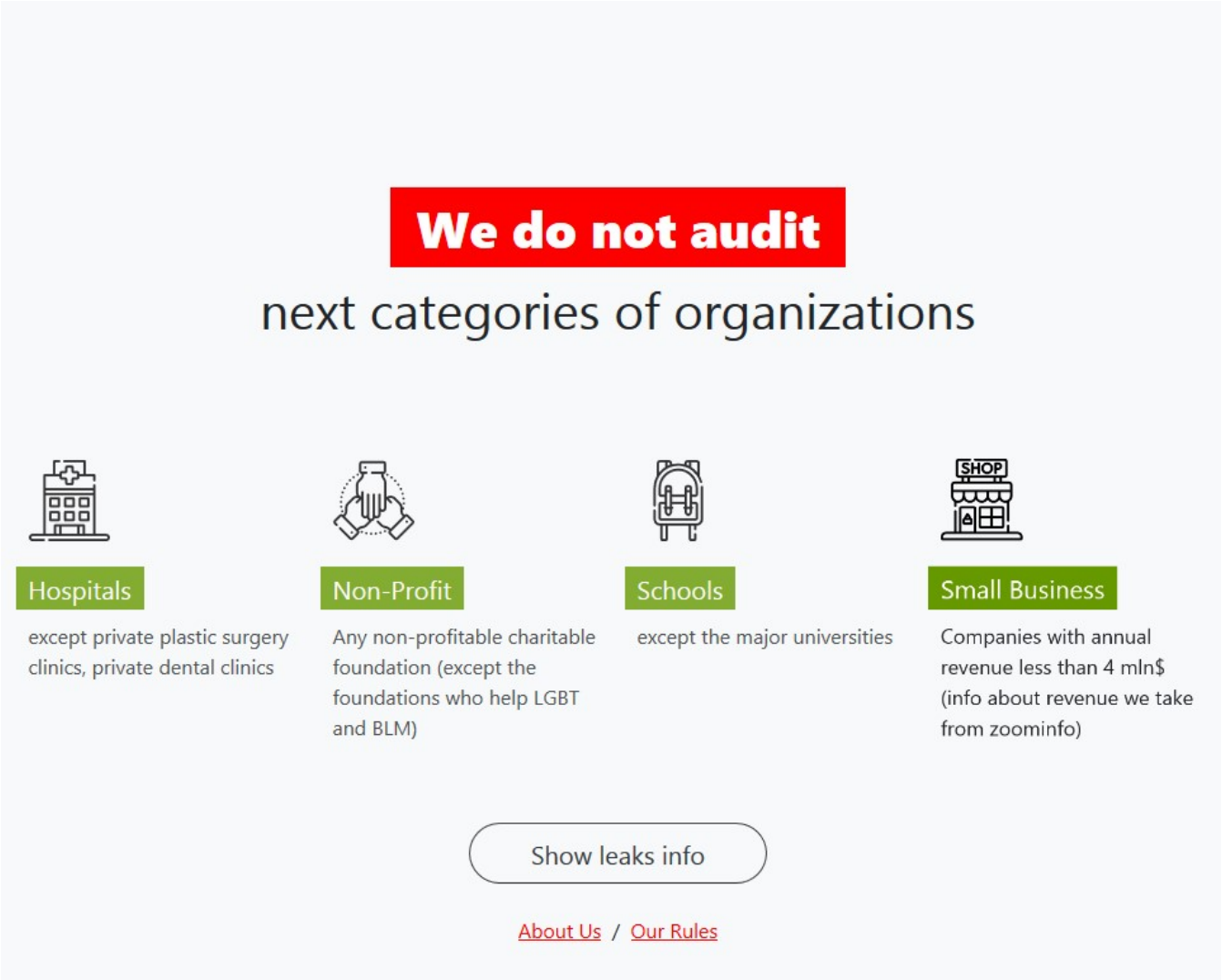


Figure 3. The list of organizations exempted from Babuk's attacks as posted on their leak site

Based on its code, the latest sample that we saw is already the third version of Babuk, which involves a more personalized ransom note that directly addresses the victim organization by name. It is likely that we will see more of this malware in the future, given the level of activity that we have described.

```
704a0fa7de1956►  ↓FRO --------          a32  PE.00408950|Hiew 7.20 (c)SEN
.00408950: 55                  push        ebp
.00408951: 8BEC                mov         ebp,esp
.00408953: 81EC80000000        sub         esp,0000000080 ;'    Ç'
.00408959: A1B0A14000          mov         eax,[0040A1B0]
.0040895E: 33C5                xor         eax,ebp
.00408960: 8945FC              mov         [ebp][-04],eax
.00408963: 68D0214000          push        0040021D0 ;'babuk_v3'
.00408968: 6A00                push        0
.0040896A: 6801001F00          push        001F0001  ;' ▼ ☺'
.0040896F: FF15C8B04000        call        OpenMutexA  ;KERNEL32
.00408975: 894588              mov         [ebp][-78],eax
.00408978: 837D8800            cmp         d,[ebp][-78],0
.0040897C: 7514                jne         .000408992   ---↓ (2)
.0040897E: 68DC214000          push        0040021DC ;'babuk_v3'
.00408983: 6A00                push        0
.00408985: 6A00                push        0
```

Figure 4. The Babuk Locker code showing that this sample is from the third version of Babuk

Possible TeslaCrypt disabling system security

The variant described here arrives through a spam email, which downloads a malicious binary that we detected as the ransomware TeslaCrypt. While Babuk is new, TeslaCrypt is an older ransomware family. Notably, TeslaCrypt's key was released in 2016 so it should now be considered a defunct ransomware; however, a new variant seems to have emerged (detected as Ransom.MSIL.TESLACRYPT.THABGBA). At present, we do not have enough information to say why the ransomware has made a reappearance. Additionally, we are not ruling out the possibility that the sample is simply a copycat version of TeslaCrypt.

Whatever the case might be, a notable feature of this malware is how it downgrades its victim's security. The malware initially disables Windows Defender before terminating a very long list of around 300 other services such as debuggers and security-related applications. Authors of this variant seem to be aiming to narrow down the availability of a recovery method for their victim's system.

For a ransomware variant, we very rarely see this many security-related processes and applications being closed in a campaign.

Operation	Info
new process	"net.exe" start FDResPub /y
new process	"net.exe" stop MSSQL$SQL_2008 /y
new process	"net.exe" stop EhttpSrv /y
new process	"net.exe" stop MMS /y
set registry value	key: HKU\S-1-5-21-1220815037-938734135-970455290-1001_CLASSES\Local Settings\MuiCache\46\52C64B7E value: LanguageList data: en-US, en
new process	"net.exe" stop MSSQL$SQLEXPRESS /y
new process	"net.exe" start upnphost /y
new process	C:\Windows\system32\net1 stop bedbg /y
new process	"net.exe" stop avpsus /y
new process	"net.exe" stop McAfeeDLPAgentService /y
new process	"net.exe" stop mfewc /y
new process	"net.exe" stop BMR Boot Service /y
new process	C:\Windows\system32\net1 start Dnscache /y
new process	"net.exe" stop NetBackup BMR MTFTP Service /y
new process	"net.exe" stop DefWatch /y
new process	"net.exe" start SSDPSRV /y
new process	"net.exe" stop YooBackup /y
new process	"net.exe" stop YooIT /y
new process	"net.exe" stop zhudongfangyu /y
new process	"net.exe" stop stc_raw_agent /y
new process	"net.exe" stop VSNAPVSS /y
set registry value	key: HKU\S-1-5-21-1220815037-938734135-970455290-1001_CLASSES\Local Settings\MuiCache\46\52C64B7E value: LanguageList data: en-US, en
new process	"net.exe" stop VeeamTransportSvc /y
new process	"net.exe" stop VeeamDeploymentService /y
new process	"net.exe" stop VeeamNFSSvc /y
new process	"net.exe" stop veeam /y

Figure 5. A screenshot showing a partial list of security-related applications terminated by the ransomware

Developments for Maoloa

The Maoloa ransomware was first seen in 2019. It is also one of the malware used in an attack on hospitals in Romania in July 2019. Maoloa has also been linked to the older GlobeImposter ransomware.

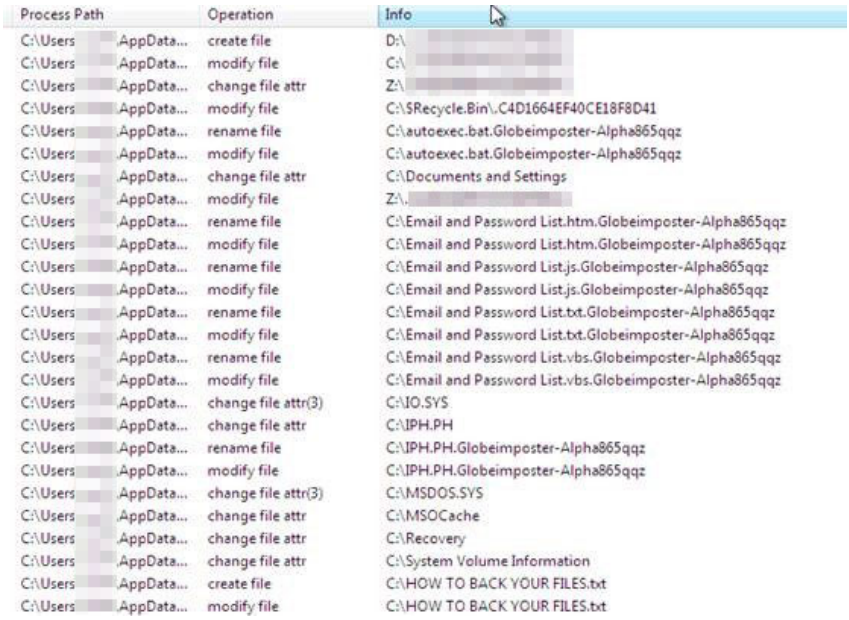
A newer sample that we encountered (detected as Ransom.Win32.MAOLOA.THAAHBA) was packaged inside a 7-Zip SFX file. This variant also used the legitimate tools certutil.exe and Autoit script. All of these additions are evasion tactics that we have not observed in previous variants. The older Maoloa variants that we encountered used a bare, unpackaged, binary.

Time	PID	Process Path	Operation	Info
17:12:05:873		C:\Users Desktop\...	create file	C:\Users AppData\Local\Temp\7ZipSfx.000\ rhi.com
17:12:05:888		C:\Users Desktop\...	modify file	C:\Users AppData\Local\Temp\7ZipSfx.000\ rhi.com
17:12:05:998		C:\Users Desktop\...	create file	C:\Users AppData\Local\Temp\7ZipSfx.000\ cee.com
17:12:05:998		C:\Users Desktop\...	modify file	C:\Users AppData\Local\Temp\7ZipSfx.000\ cee.com
17:12:05:998		C:\Users Desktop\...	create file	C:\Users AppData\Local\Temp\7ZipSfx.000\ ner.com
17:12:05:998		C:\Users Desktop\...	modify file	C:\Users AppData\Local\Temp\7ZipSfx.000\ ner.com
17:12:06:123		C:\Users Desktop\...	create file	C:\Users AppData\Local\Temp\7ZipSfx.000\ ttxh.com
17:12:06:123		C:\Users Desktop\...	modify file	C:\Users AppData\Local\Temp\7ZipSfx.000\ ttxh.com

Figure 6. Execution of the SFX file where the Maoloa ransomware is packaged

Once executed, the self-extracting archive carrying the Maoloa ransomware payload will drop four files as seen in Figure 6.

Among these files is the Maoloa ransomware which, once decrypted, will proceed with its encryption routine and dropping of ransom notes. Similar to past variants, this Maoloa sample's appended extension is ".Globeimposter-Alpha865qqz" despite belonging to the Maoloa ransomware family and not GlobeImposter's.



Process Path	Operation	Info
C:\Users .AppData...	create file	D:\
C:\Users .AppData...	modify file	C:\
C:\Users .AppData...	change file attr	Z:\
C:\Users .AppData...	modify file	C:\$Recycle.Bin\.C4D1664EF40CE18F8D41
C:\Users .AppData...	rename file	C:\autoexec.bat.Globeimposter-Alpha865qqz
C:\Users .AppData...	modify file	C:\autoexec.bat.Globeimposter-Alpha865qqz
C:\Users .AppData...	change file attr	C:\Documents and Settings
C:\Users .AppData...	modify file	Z:\
C:\Users .AppData...	rename file	C:\Email and Password List.htm.Globeimposter-Alpha865qqz
C:\Users .AppData...	modify file	C:\Email and Password List.htm.Globeimposter-Alpha865qqz
C:\Users .AppData...	rename file	C:\Email and Password List.js.Globeimposter-Alpha865qqz
C:\Users .AppData...	modify file	C:\Email and Password List.js.Globeimposter-Alpha865qqz
C:\Users .AppData...	rename file	C:\Email and Password List.txt.Globeimposter-Alpha865qqz
C:\Users .AppData...	modify file	C:\Email and Password List.txt.Globeimposter-Alpha865qqz
C:\Users .AppData...	rename file	C:\Email and Password List.vbs.Globeimposter-Alpha865qqz
C:\Users .AppData...	modify file	C:\Email and Password List.vbs.Globeimposter-Alpha865qqz
C:\Users .AppData...	change file attr(3)	C:\IO.SYS
C:\Users .AppData...	change file attr	C:\IPH.PH
C:\Users .AppData...	rename file	C:\IPH.PH.Globeimposter-Alpha865qqz
C:\Users .AppData...	modify file	C:\IPH.PH.Globeimposter-Alpha865qqz
C:\Users .AppData...	change file attr(3)	C:\MSDOS.SYS
C:\Users .AppData...	change file attr	C:\MSOCache
C:\Users .AppData...	change file attr	C:\Recovery
C:\Users .AppData...	change file attr	C:\System Volume Information
C:\Users .AppData...	create file	C:\HOW TO BACK YOUR FILES.txt
C:\Users .AppData...	modify file	C:\HOW TO BACK YOUR FILES.txt

Figure 7. Dropping of Maoloa encryption and ransom note components showing GlobeImposter file extensions

CobraLocker disguised as Among Us

Finally, part of our notable discoveries is a CobraLocker variant (detected as Ransom.MSIL.COBRALOCKER.B) that was found at large and that uses the popular game Among Us as a disguise to lure users. The file name used by this ransomware is “AmongUsHorrorEdition.”

Figure 8. The file name of CobraLocker that disguises itself as a version of Among Us

If executed, it will run an image in line with the “horror” aspect of the file and will display the text “Do you want to play?” It will then run typical malicious activities, such as terminating cmd.exe, regedit.exe, and Process Hacker, as well as adding registries for persistence.

How to secure against ransomware?

As shown by these ransomware families, threat actors will continue to hone their malware to ensure the success of their campaigns, be it by placing heavier pressure on their victims to comply to their demands or simply better disguising their malicious activities to evade detection.

- Ransomware of the present is undergoing rapid changes that need to be observed and prepared for. Here are measures that users and organizations can use to protect themselves from ransomware:
- Create an effective back-up strategy by following the 3-2-1 rule.
- Adopt strong passwords throughout the network.
- Consider network segmentation to separate important processes and systems from the wider access network.
- Increase both your awareness and the awareness of the members of your organization on how ransomware spreads (i.e., through spammed emails and attachments)
- Monitor and audit network traffic for any suspicious behaviors or anomalies.

Trend Micro solutions

Trend Micro solutions such as the Smart Protection Suite and Trend Micro™ Worry-Free™ Business Security Services solutions, which have behavior monitoring capabilities, can protect users and businesses from these types of threats by detecting malicious files, scripts, and messages as well as blocking all related malicious URLs. Our XGen™ security provides a cross-generational blend of threat defense techniques against a full range of threats for data centers, cloud environments, networks, and endpoints. It infuses high-fidelity machine learning (ML) with other detection technologies and global threat intelligence for comprehensive protection from advanced malware.

Indicators of Compromise (IOCs)

Detection name	SHA-256
Ransom.MSIL.COBRALOCKER.AA	88d55af8d84c1909e9ccf962e59f71dacf158eb9fd671920a23b7390103bd58f
Ransom.MSIL.COBRALOCKER.AA	ec621d94c847976baa8b3ead1bb98c2a0951432ba21181f09fb1c55dcddd98c3
Ransom.MSIL.COBRALOCKER.B	ba28a0615626a40254c4e4167e0b3f8bc82bdd83f42b225605c34268c38ef0b5
Trojan.MSIL.COBRALOCKER.A	bdcc8754a9f75c2fe1f909af669ac59f25d635139f3634f525e4189db604e3f0
Trojan.MSIL.COBRALOCKER.A	ff53667fe3745601d6d04668cd854813f650087be2872876de71d412b70eb0cd
Ransom.MSIL.TESLACRYPT.THABGBA	dcd725c415cebc7df170edf49af18d6f86e76ef75185737de5959405f4aecc56
Ransom.Win32.BABUK.YEBA-THAAEBA	704a0fa7de19564bc743fb68aa0652e38bf86e8ab694bc079b15f945c85f4320
Ransom.Win32.BABUK.YEBA-THAAEBA	8140004ff3cf4923c928708505754497e48d26d822a95d63bd2ed54e14f19766
Ransom.Win32.BABUK.YEBA-THAAEBA	afcf265a1dcd9eab5aab270d48aa561e4ddeb71c05e32c857d3b809bb64c0430
Ransom.Win32.BABUK.YNBA-THABGBA	3dda3ee9164d6815a18a2c23651a53c35d52e3a5ad375001ec824cf532c202e6
Ransom.Win32.BABUK.YNBA-THABGBA	c5167053129bd4a5542cfef9e739b0443e22e184cb4c0b57c049b448f030cf15
Ransom.Win32.MAOLOA.THAAHBA	94be0c4af61e979ad2064544708807fcdfc4b63115ed885ed0067ece04630a7b
Ransom.Win64.SETHLOCKER.THABEBAA	58c852525bf3bea185db34a79c2c5640c02f8291cdbdbe8dd7c0a9d4682f4b2c
Trojan.W97M.TESLACRYPT.THABGBA	c7e40628fb6beb52d9d73a3b3afd1dca5d2335713593b698637e1a47b42bfc71