BART Ransomware

This is a security alert for all TruShield clients, the financial services industry, and the community as a whole. We have learned about a new ransomware called Bart that is from the same developers behind Dridex and Locky.

About Bart Ransomware

Security researchers from Proofpoint discovered a new ransomware called Bart. For a user to get infected with Bart, a malicious actor will send them spam email with subjects to entice them into opening the malicious email. Then once the user opens the email with the attachments, it is downloaded and installed. It uses RockLoader to download Bart ransomware over HTTPS. Once a user is infected with the malware their files become encrypted.

The encryption used is not a cryptographic algorithm such as AES. Bart uses a password-protected ZIP file archive to encrypt the data of users that are a victim and adds .bart.zip as the extension to the new file. After the data is encrypted, a ransom note will display demanding users to pay three bitcoins to get the password to decrypt the user's zipped files. If the user does not pay, they will not get their file back. A unique thing about this ransomware is that it does not connect to a command and control server when it encrypts data. It uses the URL "id" parameter to transfer information that is necessary. And so far, according to the Proofpoint researchers, the first campaign of Bart seems to be largely targeting the US, but they don't believe that this will be the only country targeted because of available translations for the recovery files. Bart ransomware does not need internet communication to infect a computer because it does not communicate with any networks.

Files that are encrypted by Bart:

.123	.3dm	.3ds
.3g2	.3gp	.602
.aes	.ARC	.asc
.asf	.asm	.asp
.avi	.bak	.bat
.bmp	.brd	.cgm
.cmd	.cpp	.crt
.csr	.CSV	.dbf
.dch	.dif	.dip

.djv	.djvu	.DOC
.docb	.docm	.docx
.DOT	.dotm	.dotx
.fla	.flv	.frm
.gif	.gpg	.hwp
.ibd	.jar	.java
.jpeg	.jpg	.key
.lay	.lay6	.ldf
.m3u	.m4u	.max
.mdb	.mdf	.mid
.mkv	.mov	.mp3
.mp4	.mpeg	.mpg
.ms11	.MYD	.MYI
.NEF	.odb	.odg
.odp	.ods	.odt
.otg	.otp	.ots
.ott	.p12	.PAQ
.pas	.pdf	.pem
.php	.png	.pot
.potm	.potx	.ppam
.pps	.ppsm	.ppsx
.PPT	.pptm	.pptx
.psd	.rar	.raw
.RTF	.sch	.sldm
.sldx	.slk	.stc
.std	.sti	.stw
.svg	.swf	.sxc
.sxd	.sxi	.sxm
.sxw	.tar	.tbk
.tgz	.tif	.tiff
.txt	.uop	.uot
.vbs	.vdi	.vmdk
.vmx	.vob	.wav
.wb2	.wk1	.wks
.wma	.wmv	.xlc
.xlm	.XLS	.xlsb
.xlsm	.xlsx	.xlt
.xltm	.xltm	.xlw
.zip		

Files Bart will not zip:

Tmp	Winnt
Application Data	AppData
PerfLogs	Program Files (x86)
Program Files	ProgramData
Temp	Recovery
$Recycle.Bin	System Volume Information
Boot	Windows

How Does Bart Relate to Other Ransomware?

Bart is said to be created by the same developers as Locky and Dridex because of the intermediary loader that it uses known as RockLoader, the same loader employed by Locky. The payment screen that it uses is also like Locky's. It relates to Dridex because, according to researches, Bart uses the same email distribution mechanism and server that were hosting Locky and Dridex. It also shares similar code information to Locky.

Indicators of Compromise

Bart uses spam messages to infect its victims. Below are some of the signs of compromise:

Subject Line
Photos
Attachments
photos.zip
Image.zip
Photos.zip
photo.zip
Photo.zip
Picture.zip
Photos.zip email attachment SHA256
247e2c07e57030607de901a461719ae2bb2ac27a90623ea5fd69f7f036c4ea0d
FILE 21076073.js file inside Photos.zip SHA256
7bb1e8e039d222a51a71599af75b56151a878cf8bbe1f9d3ad5be18200b2286b
JavaScript Payload (RockLoader) URL
hxxp://camera-test.hi2[.]ro/89ug6b7ui?voQeTqDw=RUYEzU
Rockloader Payload SHA256
5d3e7c31f786bbdc149df632253fd538fb21cfc0aa364d0f03a79671bbaec62d

Rockloader C&C
hxxps://summerr554fox[.]su/api/
RockLoader Payload
hxxps://summerr554fox[.]su/files/6kuTU1.exe
6kuTU1.exe (Bart ransomware)
51ff4a033018d9343049305061dcde77cb5f26f5ec48d1be42669f368b1f5705

Mitigation

- Block zipped executables at the email gateway.
- Raise awareness among users about not opening email from unreliable sources.
- Be careful with emails that contain file extensions and do not open them.
- Keep computer software and browers up-to-date.
- Make sure backups are taking place.

Conclusion

Bart is a new ransomware that is similar to Locky and Dridex, but different in how it encrypts files, by not requiring C&C communication. Since the campaign for this malware has just started, the target country appears to be the US, but it may shortly start to target other countries. Please note that this ransomware is still under further analysis in order to gain more insight on how it encrypts files, and the communication that takes place during the process. The researchers at Proofpoint has said that due to the lack of communication with the C&C server, this malware may target corporate networks, due to its ability to bypass the corporate firewalls.

References

http://www.bleepingcomputer.com/news/security/bart-ransomware-being-spammed-by-the-same-devs-behind-locky/

https://www.proofpoint.com/us/threat-insight/post/New-Bart-Ransomware-from-Threat-Actors-Spreading-Dridex-and-Locky

http://www.securityweek.com/bart-ransomware-doesnt-require-cc-server-encrypt-files

TruShield Security Solutions

TruShield is a leading provider of Managed Security Services across the globe. We are dedicated to helping companies achieve success by making sure they are properly prepared against the current and emerging threats in today's digital world. Our service

offerings include: Continuous, 24/7/365 Monitoring, Penetration Testing and Vulnerability Assessments, Audit and Compliance, and many other Managed Services such as Managed Firewalls and Hosted Log Management. We also offer Security Awareness Training and Management Consulting services.
Contact us today to find out how we can help you protect your organization and safeguard your information.

Contact Information:

Email: support@trushieldinc.com
Web: www.trushieldinc.com
Phone: (877)-583-2841

Follow us on:

Twitter: @TruShield
LinkedIn: https://www.linkedin.com/company/trushield-security-solutions
Facebook: https://www.facebook.com/trushieldinc