CryptoMix Ransomware Cyber Report

Overview

Earlier this month, the cyber intelligence community detected a new CryptoMix ransomware campaign that exploited real stories of children diagnosed with cancer.[1] The campaign pretended to represent a real children's charity and alleged that the victim's ransom payment was for a good cause.

This was not the first time a CryptoMix campaign used a theme pertaining to sick children, but this was the first one that used real photos and stories. Additionally, unlike previous campaigns, the ransomware was not delivered by email, but deployed after networks were breached in a remote desktop protocol (RDP) brute force attack.

Customer Impact

CryptoMix is a ransomware that targets Windows operating systems (OS) and was first discovered in March 2016.[2] It is not as widely distributed as other popular ransomware such as GandCrab or Dharma, and therefore has received less public attention.

CryptoMix borrows code from two other ransomware families: CyrptoWall and CryptXXX. It is also known to encrypt files using both the Rivest-Shamir-Adleman (RSA) and Advanced Encryption Standard (AES) algorithms.

CryptoMix has some unique characteristics for a ransomware. It does not change the desktop background image after encrypting files and does not provide a payment portal. Instead, it leaves a ransom note in the form of a text file that explains how to contact the threat actor by email for payment instructions.

To date, the ransom amounts for CryptoMix campaigns have been notably higher than those of other ransomware campaigns. While some estimates put the average ransom demand around $1,000 in 2017, CryptoMix ransoms have ranged from two to ten bitcoins ($7,000 to $35,000).[3]

Campaign Analysis

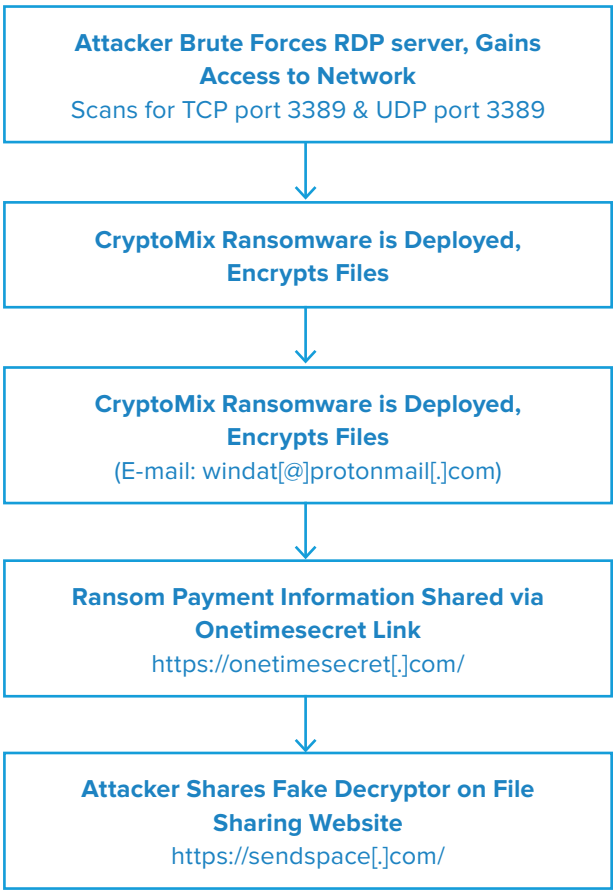
CryptoMix campaigns have tended to use e-mails, compromised websites embedded with malicious scripts, and Rig exploit kits to deliver the ransomware payloads. The campaign discovered this month, however, scanned the internet for public-facing RDP servers by searching for the default RDP port 3389. The threat actor then launched brute force attacks to break into servers with weak passwords.

Once a victim's network was breached, the attackers collected administrative credentials to further move across the network. Eventually, the ransomware was deployed and devices were encrypted. The ransomware generated a file named "_HELP_INSTRUCTION.txt" that contained instructions to contact the attackers in order to restore files. The file contained six email addresses and the victim was instructed to reply to all of them.[4]

Victims who responded to the emails received a reply message that claimed the attackers were part of a children charity organization. The message included real photos of children taken from legitimate crowdfunding websites. Victims were directed to visit a onetimesecret[.]com web page for payment instructions that included the attacker's bitcoin wallet information. Onetimesecret is a free online tool that is often used by cyber criminals to share information without exposing their identity. The tool allows users to share secret content with others through a one-time generated link that expires after a short time.

Finally, after submitting the payment, victims received an email that contained another onetimesecret link to a page that provided a url to download the decryptor software hosted at the file sharing website sendspace[.]com. Users have reported that these decryptors are fake.[5]

Chain Attack



Vulnerabilities & Mitigation

Infoblox recommends the following actions for combatting the brute force attacks described in this report. We also recommend reaching out to the third parties mentioned below to determine whether locked files can be recovered.

- Security vendor Avast provides a decryptor tool that can be applied to devices infected by CryptoMix variants that use offline keys for encryption.[6]
- The computer emergency response team (CERT) of Poland has found a way to decrypt files if provided the encrypted and unencrypted version of a file.[7]
- Unless it is absolutely necessary, do not expose an RDP server to the public. Set it behind a properly-configured firewall.
- Change the default RDP port numbers. Attackers scan for publicly-exposed RDP servers listening on TCP port 3389 and UDP port 3389.
- Frequently update the RDP software.
- Integrate two-factor authentication (2FA) for the RDP login.
- Limit the number of users who can access remote desktops.
- Always enable network level authentication (NLA). This is enabled by default for Windows 10 OS.

Appendix

Representative Indicators of Compromise	Description
windat[@]protonmail[.]com windat1[@]protonmail[.]com windat[@]dr[.]com windat[@]tuta[.]io windat1[@]yandex[.]com windat2[@]yandex[.]com	Email addresses belonging to the attacker
onetimesecret[.]com	Free secret content sharing tool
sendspace[.]com	File sharing site

Endnotes

1. https://www.coveware.com/blog/cryptomix-ransomware-exploits-cancer-crowdfunding
2. https://www.zdnet.com/article/this-old-ransomware-is-using-an-unpleasant-new-trick-to-try-and-make-you-pay-up/
3. https://www.webroot.com/blog/2016/07/22/about-cryptomix-ransomware/
4. https://www.pcrisk.com/removal-guides/9993-code-ransomware
5. https://www.bleepingcomputer.com/forums/t/690274/cryptomix-windatprotonmailcom-windat1protonmailcom/
6. https://blog.avast.com/cryptomix-avast-adds-a-new-free-decryption-tool-to-its-collection
7. https://www.cert.pl/en/about-us/

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com